

PAPER • OPEN ACCESS

Forensic Analysis of Xbox One

To cite this article: Ying Zhang and Feng Gao 2019 *IOP Conf. Ser.: Earth Environ. Sci.* **252** 042097

View the [article online](#) for updates and enhancements.

Forensic Analysis of Xbox One

Ying Zhang^a, Feng Gao^b

The Third Research Institute of Ministry of Public Security Shanghai, China

^azhangying@stars.org.cn, ^bgaofeng@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, data on hardware, network data 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.

Table 1. Image List

<i>Name</i>	<i>Description</i>	<i>Created Time</i>
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.

Table 2. Partitions

<i>Numble</i>	<i>Partition</i>	<i>File System</i>	<i>Size (GB)</i>
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.

File system: NTFS Name: Temp Content Total capacity: 44023414784 bytes = 41.0 GB Sector count: 85983232 Bytes per sector: 512 Bytes per cluster: 4096 Free clusters: 6309252 = 59% free Total clusters: 10747903 NTFS version: 3.1 Volume flags: 0x0000 Serial No.: FB3FEDF8 (hex) Serial No.: F8ED3FFB (hex, rev) Serial No.: 4176297979 (dec, rev)	File system: NTFS Name: User Content Total capacity: 391915765760 bytes = 365 GB Sector count: 765460480 Bytes per sector: 512 Bytes per cluster: 4096 Free clusters: 95653872 = 100% free Total clusters: 95682559 NTFS version: 3.1 Volume flags: 0x0000 Serial No.: 5BA4EEE8 (hex) Serial No.: E8EEA45B (hex, rev) Serial No.: 3907953755 (dec, rev)	File system: NTFS Name: System Support Total capacity: 42949672960 bytes = 40.0 GB Sector count: 83886080 Bytes per sector: 512 Bytes per cluster: 4096 Free clusters: 8080888 = 77% free Total clusters: 10485759 NTFS version: 3.1 Volume flags: 0x0000 Serial No.: 8934F0C0 (hex) Serial No.: C0F03489 (hex, rev) Serial No.: 3236967561 (dec, rev)
File system: NTFS Name: System Update Total capacity: 12884901888 bytes = 12.0 GB Sector count: 25165824 Bytes per sector: 512 Bytes per cluster: 4096 Free clusters: 2631879 = 84% free Total clusters: 3145727 NTFS version: 3.1 Volume flags: 0x0000 Serial No.: DE0CFC76 (hex) Serial No.: 76FC0CDE (hex, rev) Serial No.: 1996229854 (dec, rev)	File system: NTFS Name: System Update 2 Total capacity: 7516192768 bytes = 7.0 GB Sector count: 14680064 Bytes per sector: 512 Bytes per cluster: 4096 Free clusters: 1822792 = 99% free Total clusters: 1835007 NTFS version: 3.1 Volume flags: 0x0000 Serial No.: 4303FD42 (hex) Serial No.: 42FD0343 (hex, rev) Serial No.: 1123877699 (dec, rev)	

Figure 1. Partition Information.

Considering previous and current studies [3], it is found that different Xbox one owns the same partition structure, including name, size and file system.

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.

xbox_one_1.001

Name	Type	Path	Size	Created	Modified	Record changed	Accessed
\$Extend		\	9.0 MB	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05
(Root directory)		\		2013/05/26 00:00:05	2013/05/26 00:00:08	2013/05/26 00:00:08	2013/05/26 00:00:08
\$AttrDef		\	2.5 KB	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05
\$BadClus		\	0 B	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05
\$Bitmap		\	1.3 MB	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05
\$Boot		\	8.0 KB	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05
\$LogFile		\	64.0 MB	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05
\$MFT		\	256 KB	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05
\$MFTMirr		\	4.0 KB	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05
\$Secure		\	0 B	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05
\$sosrst.xvd	xvd	\	96.6 MB	2013/05/26 00:00:05	2013/05/26 00:01:42	2013/05/26 00:01:42	2013/05/26 00:00:05
\$UpCase		\	128 KB	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05
\$Volume		\	0 B	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05	2013/05/26 00:00:05
appswapfile.xvd	xvd	\	2.0 GB	2013/05/26 00:00:08	2013/05/26 00:01:42	2013/05/26 00:01:42	2013/05/26 00:00:08
AppTempStorage		\	3.0 GB	2013/05/26 00:00:55	2013/05/26 00:01:42	2013/05/26 00:01:42	2013/05/26 00:00:55
AppUserStorage		\	1.5 GB	2013/05/26 00:00:47	2013/05/26 00:01:42	2013/05/26 00:01:42	2013/05/26 00:00:47
ConnectedStorage-retail		\	9.1 GB	2013/05/26 00:00:49	2013/05/26 00:01:42	2013/05/26 00:01:42	2013/05/26 00:00:49
GDVIndex.xvd	xvd	\	101 MB	2013/05/26 00:01:37	2013/05/26 00:01:42	2013/05/26 00:01:42	2013/05/26 00:01:37
ScreenShots.xvd	xvd	\	1.0 GB	2013/05/26 00:01:40	2013/05/26 00:01:42	2013/05/26 00:01:42	2013/05/26 00:01:40
Free space (ntfs)		\	34.1 GB				
Idle space		\					
Volume slack		\	4.0 KB				

xbox_one_factory_settings.001

Name	Type	Path	Size	Created	Modified	Record changed	Accessed
\$Extend		\	9.0 MB	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06
(Root directory)		\		2014/09/02 00:00:06	2014/09/02 00:00:50	2014/09/02 00:00:50	2014/09/02 00:00:50
\$AttrDef		\	2.5 KB	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06
\$BadClus		\	0 B	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06
\$Bitmap		\	1.3 MB	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06
\$Boot		\	8.0 KB	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06
\$LogFile		\	64.0 MB	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06
\$MFT		\	256 KB	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06
\$MFTMirr		\	4.0 KB	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06
\$Secure		\	0 B	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06
\$sosrst.xvd	xvd	\	46.1 MB	2014/09/02 00:00:07	2014/09/02 00:01:51	2014/09/02 00:01:51	2014/09/02 00:00:07
\$UpCase		\	128 KB	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06
\$Volume		\	0 B	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06	2014/09/02 00:00:06
appswapfile.xvd	xvd	\	2.0 GB	2014/09/02 00:00:15	2014/09/02 00:00:17	2014/09/02 00:00:17	2014/09/02 00:00:15
DeploymentSoftwareDistrib...	xvd	\	3.0 GB	2014/09/02 00:00:37	2014/09/02 00:02:00	2014/09/02 00:02:00	2014/09/02 00:00:37
GDVIndex.xvd	xvd	\	101 MB	2014/09/02 00:00:43	2014/09/02 00:02:00	2014/09/02 00:02:00	2014/09/02 00:00:43
ScreenShots.xvd	xvd	\	1.0 GB	2014/09/02 00:00:50	2014/09/02 00:01:21	2014/09/02 00:01:21	2014/09/02 00:00:50
Free space (ntfs)		\	34.7 GB				
Idle space		\					
Volume slack		\	4.0 KB				

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 Wnindows 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 from 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.

Table 3. Table Type Styles

File Name	User Logon	System Update
	<i>Hash Value (SHA256)</i>	<i>Hash Value (SHA256)</i>
\$Attr Def	D7DE5B1B2F79F45F235CEB1ADBC46908 ED64EAE174EB90ED66AEFE5F25165DA3	D7DE5B1B2F79F45F235CEB1ADBC46908 ED64EAE174EB90ED66AEFE5F25165DA3
\$Bitmap	4D1EE6E1567ADCAC4C0C468AE377EF9 DD3C04918D4963AA0B12FC883D01355F 7	90282754B5636E5A0E7E91BEDC9DA1B9 B788E88A5308471F960FC5FCC4C8B958
\$Boot	24F1DAB8C92E93032E526BB5134B89566 B9D85E80D5C9913F4D271331C1838D2	24F1DAB8C92E93032E526BB5134B89566 B9D85E80D5C9913F4D271331C1838D2
\$LogFile	CC60A9EC74F361023CB04652C533F6B1A 62A95FC96054E86C024C7CECD274ED2	D26777423BD8306FD66288F288FA9CCAE 74D580F2E813C3A94C5260126988582
\$MFT	7991E4E5C923FDD461E3ED5CE251D7962 9C2D4C3244275BA72BDB76FD5C96417	A8EDFF0CC5309E4E4CDEE0C297145294 26D1DCC37A7FA18ADCA20ED4198C079 0
\$MFTMirr	8F8C0E84A4EF4611D794F5F453B5042675 658C5C2588D73302F7CA6D99EEDFF2	8F8C0E84A4EF4611D794F5F453B5042675 658C5C2588D73302F7CA6D99EEDFF2
\$UpCase	41C26BC7A12BDAEB26025C93118697C7 E3EF81EE048B00FE5CCE2A472E0E0742	41C26BC7A12BDAEB26025C93118697C7 E3EF81EE048B00FE5CCE2A472E0E0742
updater.xvd	5468F999D21D97885930B5C31B8EFE46E1 9191613C496B513837441D37A4C681	10E4D9CC1549DF4594CE8484C4DAD8A CFA1620FAC69B0B4911C23D2D7B60A3E 4

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

DNS Protocol

1043	40.438743	192.168.253.9	192.168.253.1	DNS	87 Standard query 0xe18c A inference.location.live.net
1044	40.449541	192.168.253.1	192.168.253.9	DNS	260 Standard query response 0xe18c A inference.location.live.net CNAME inference.location.services.windowsphone.com CNAME inference.location.livenet.akadns.net
1160	42.863854	192.168.253.9	192.168.253.1	DNS	85 Standard query 0xc785 A leaderboards.xboxlive.com
1169	42.880833	192.168.253.1	192.168.253.9	DNS	299 Standard query response 0xc785 A leaderboards.xboxlive.com CNAME leaderboards.xboxlive.com.akadns.net CNAME leaderboards.xboxlive.com-c.edgekey.net CNAME
1368	44.668286	192.168.253.9	192.168.253.1	DNS	93 Standard query 0xef58 A v20.vortex-win.data.microsoft.com
1369	44.669979	192.168.253.1	192.168.253.9	DNS	210 Standard query response 0xef58 A v20.vortex-win.data.microsoft.com CNAME v20-asimov-win.vortex.data.microsoft.com.akadns.net CNAME geo.vortex.data.microsoft.com
1516	61.951898	192.168.253.9	192.168.253.1	DNS	85 Standard query 0xd9e4 A achievements.xboxlive.com
1517	61.962207	192.168.253.1	192.168.253.9	DNS	296 Standard query response 0xd9e4 A achievements.xboxlive.com CNAME achievements.xboxlive.com.akadns.net CNAME achievements.xboxlive.com-c.edgekey.net CNAME
1519	61.972906	192.168.253.9	192.168.253.1	DNS	85 Standard query 0xcac0 A titlstorage.xboxlive.com
1520	61.982335	192.168.253.1	192.168.253.9	DNS	291 Standard query response 0xcac0 A titlstorage.xboxlive.com CNAME titlstorage.xboxlive.com.akadns.net CNAME titlstorage.xboxlive.com-c.edgekey.net CNAME t
1539	62.043616	192.168.253.9	192.168.253.1	DNS	81 Standard query 0xc963 A titlehub.xboxlive.com
1545	62.058682	192.168.253.1	192.168.253.9	DNS	244 Standard query response 0xc963 A titlehub.xboxlive.com CNAME wildcard.xboxlive.com-c.edgekey.net CNAME wildcard.xboxlive.com-c.edgekey.net.globalredir.ak
1780	63.349333	192.168.253.9	192.168.253.1	DNS	80 Standard query 0xe148 A profile.xboxlive.com
1781	63.361770	192.168.253.1	192.168.253.9	DNS	276 Standard query response 0xe148 A profile.xboxlive.com CNAME profile.xboxlive.com.akadns.net CNAME profile.xboxlive.com-c.edgekey.net CNAME profile.xboxli
1782	63.368152	192.168.253.9	192.168.253.1	DNS	80 Standard query 0xbdbf A privacy.xboxlive.com
1784	63.378469	192.168.253.1	192.168.253.9	DNS	279 Standard query response 0xbdbf A privacy.xboxlive.com CNAME privacy.xboxlive.com.akadns.net CNAME privacy.xboxlive.com-c.edgekey.net CNAME privacy.xboxli
1787	63.424493	192.168.253.9	192.168.253.1	DNS	81 Standard query 0xbd82 A accounts.xboxlive.com
1790	63.434379	192.168.253.1	192.168.253.9	DNS	280 Standard query response 0xbd82 A accounts.xboxlive.com CNAME accounts.xboxlive.com.akadns.net CNAME accounts.xboxlive.com-c.edgekey.net CNAME accounts.xb
1794	63.451950	192.168.253.9	192.168.253.1	DNS	82 Standard query 0xba72 A userstats.xboxlive.com
1800	63.460329	192.168.253.1	192.168.253.9	DNS	287 Standard query response 0xba72 A userstats.xboxlive.com CNAME userstats.xboxlive.com.akadns.net CNAME userstats.xboxlive.com-c.edgekey.net CNAME userstat

DNS Protocol

2609	138.294873	192.168.253.9	192.168.253.1	DNS	85 Standard query 0xbf7d A titlstorage.xboxlive.com
2610	138.305495	192.168.253.1	192.168.253.9	DNS	291 Standard query response 0xbf7d A titlstorage.xboxlive.com CNAME titlstorage.xboxlive.com.akadns.net CNAME titlstorage.xboxlive.com-c.edgekey.net CNAME t
9132	155.012628	192.168.253.9	192.168.253.1	DNS	82 Standard query 0xb6b2 A xsts.auth.xboxlive.com
9133	155.025004	192.168.253.1	192.168.253.9	DNS	145 Standard query response 0xb6b2 A xsts.auth.xboxlive.com CNAME xsts.auth.xboxlive.com.akadns.net A 66.119.149.145
9167	155.670948	192.168.253.9	192.168.253.1	DNS	86 Standard query 0xb695 A mods.services.bethesda.net
9170	155.713096	192.168.253.9	10.0.1.1	DNS	86 Standard query 0xb695 A mods.services.bethesda.net
9180	155.029063	10.0.1.1	192.168.253.9	DNS	97 Standard query 0xb2f38 A services.bethesda.net
9182	156.048588	192.168.253.1	192.168.253.9	DNS	81 Standard query 0xb2f38 A services.bethesda.net
9173	155.855349	192.168.253.9	192.168.253.1	DNS	85 Standard query 0x28b0 A userpresence.xboxlive.com
9174	155.864123	192.168.253.9	10.0.1.1	DNS	81 Standard query 0x2f38 A services.bethesda.net
9175	155.865985	192.168.253.1	192.168.253.9	DNS	299 Standard query response 0x28b0 A userpresence.xboxlive.com CNAME userpresence.xboxlive.com.akadns.net CNAME userpresence.xboxlive.com-c.edgekey.net CNAME
9176	155.866873	10.0.1.1	192.168.253.9	DNS	150 Standard query response 0xb695 A mods.services.bethesda.net A 13.35.121.48 A 13.35.121.54 A 13.35.121.114 A 13.35.121.81
9177	155.874340	192.168.253.1	192.168.253.9	DNS	97 Standard query response 0xb695 A mods.services.bethesda.net A 13.35.121.48 A 13.35.121.114 A 13.35.121.81 A 13.35.121.54
9180	155.029063	10.0.1.1	192.168.253.9	DNS	97 Standard query response 0xb2f38 A services.bethesda.net A 143.204.132.228
9182	156.048588	192.168.253.1	192.168.253.9	DNS	97 Standard query response 0xb2f38 A services.bethesda.net A 13.32.134.252
9208	156.406209	192.168.253.9	192.168.253.1	DNS	68 Standard query 0xcfc2 A o.s.s2.us
9209	156.413389	192.168.253.1	192.168.253.9	DNS	132 Standard query response 0xcfc2 A o.s.s2.us A 13.33.227.228 A 13.33.227.3 A 13.33.227.53 A 13.33.227.123
9234	159.461180	192.168.253.9	192.168.253.1	DNS	87 Standard query 0xd06e A o.scp.root2.amazontrust.com
9235	159.472660	192.168.253.1	192.168.253.9	DNS	151 Standard query response 0xd06e A o.scp.root2.amazontrust.com A 143.204.132.119 A 143.204.132.7 A 143.204.132.193 A 143.204.132.211
9255	160.590053	192.168.253.9	192.168.253.1	DNS	88 Standard query 0xcce6 A o.scp.rootcal.amazontrust.com
9256	160.600761	192.168.253.1	192.168.253.9	DNS	152 Standard query response 0xcce6 A o.scp.rootcal.amazontrust.com A 143.204.132.211 A 143.204.132.7 A 143.204.132.193 A 143.204.132.119

DNS Protocol

No.	Time	Source	Destination	Protocol	Length	Info
68	0.842274	192.168.253.9	192.168.253.1	DNS	74	Standard query 0xe331 A login.live.com
69	0.852447	192.168.253.1	192.168.253.9	DNS	174	Standard query response 0xe331 A login.live.com CNAME login.msa.akadns6.net CNAME vs.login.msa.akadns6.net A 131.253.61.64 A 131.253.61.84 A 131.253.61.66
127	1.616326	192.168.253.9	192.168.253.1	DNS	82	Standard query 0x05f9 A peoplehub.xboxlive.com
128	1.620624	192.168.253.9	192.168.253.1	DNS	81	Standard query 0xedd1 A comments.xboxlive.com
129	1.626491	192.168.253.1	192.168.253.9	DNS	247	Standard query response 0x05f9 A peoplehub.xboxlive.com CNAME peoplehub.xboxlive.com-c.edgekey.net CNAME peoplehub.xboxlive.com-c.edgekey.net.globalredir
131	1.633633	192.168.253.1	192.168.253.9	DNS	282	Standard query response 0xedd1 A comments.xboxlive.com CNAME comments.xboxlive.com.akadns.net CNAME comments.xboxlive.com-c.edgekey.net CNAME comments.xb
133	1.638415	192.168.253.9	192.168.253.1	DNS	83	Standard query 0xe849 A usertitles.xboxlive.com
135	1.646719	192.168.253.1	192.168.253.9	DNS	284	Standard query response 0xe849 A usertitles.xboxlive.com CNAME usertitles.xboxlive.com.akadns.net CNAME wildcard.xboxlive.com-c.edgekey.net CNAME wildcard
144	1.658220	192.168.253.9	192.168.253.1	DNS	79	Standard query 0x2e05 A social.xboxlive.com
150	1.668188	192.168.253.1	192.168.253.9	DNS	275	Standard query response 0x2e05 A social.xboxlive.com CNAME social.xboxlive.com.akadns.net CNAME social.xboxlive.com-c.edgekey.net CNAME social.xboxlive.c
295	3.347532	192.168.253.9	192.168.253.1	DNS	82	Standard query 0xfc2c A editorial.xboxlive.com
298	3.357312	192.168.253.1	192.168.253.9	DNS	247	Standard query response 0xfc2c A editorial.xboxlive.com CNAME editorial.xboxlive.com-c.edgekey.net CNAME editorial.xboxlive.com-c.edgekey.net.globalredir
402	4.341641	192.168.253.9	192.168.253.1	DNS	80	Standard query 0xb485 A clubhub.xboxlive.com
407	4.350858	192.168.253.1	192.168.253.9	DNS	278	Standard query response 0xb485 A clubhub.xboxlive.com CNAME clubhub.xboxlive.com.akadns.net CNAME wildcard.xboxlive.com-c.edgekey.net CNAME wildcard.xbox
416	4.379915	192.168.253.9	192.168.253.1	DNS	79	Standard query 0x2b0c A chatfd.xboxlive.com
420	4.387254	192.168.253.1	192.168.253.9	DNS	276	Standard query response 0x2b0c A chatfd.xboxlive.com CNAME chatfd.xboxlive.com.akadns.net CNAME wildcard.xboxlive.com-c.edgekey.net CNAME wildcard.xboxli
474	4.660522	192.168.253.9	192.168.253.1	DNS	82	Standard query 0xf04e A title.mgt.xboxlive.com
477	4.674086	192.168.253.1	192.168.253.9	DNS	145	Standard query response 0xf04e A title.mgt.xboxlive.com CNAME title.mgt.xboxlive.com.akadns.net A 66.119.149.146
562	9.329951	192.168.253.9	192.168.253.1	DNS	76	Standard query 0xf01f A rt.a.xboxlive.com
563	9.340021	192.168.253.9	192.168.253.1	DNS	81	Standard query 0xf068 A notifier.xboxlive.com

DNS Protocol

No.	Time	Source	Destination	Protocol	Length	Info
563	9.340021	192.168.253.9	192.168.253.1	DNS	81	Standard query 0xf068 A notifier.xboxlive.com
564	9.357337	192.168.253.1	192.168.253.9	DNS	263	Standard query response 0xbaf1 A rt.a.xboxlive.com CNAME rt.a.xboxlive.com.akadns.net CNAME rt.a.xboxlive.com-c.edgekey.net CNAME rt.a.xboxlive.com-c.edgekey
565	9.364687	192.168.253.1	192.168.253.9	DNS	223	Standard query response 0xf068 A notifier.xboxlive.com CNAME notifier.xboxlive.com.akadns.net CNAME chat.xboxlive.com CNAME chat.xboxlive.com-c.natc.net C
572	9.405124	192.168.253.9	192.168.253.1	DNS	83	Standard query 0x2009 A ctldl.windowsupdate.com
573	9.415628	192.168.253.1	192.168.253.9	DNS	235	Standard query response 0x2009 A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.nsatc.net CNAME ctldl.windowsupdate.edgesuite.net CNAME a1621.g.ak
595	10.568859	192.168.253.9	192.168.253.1	DNS	90	Standard query 0x2c09 A notificationinbox.xboxlive.com
596	10.582415	192.168.253.1	192.168.253.9	DNS	161	Standard query response 0x2c09 A notificationinbox.xboxlive.com CNAME notificationinbox.xboxlive.com.akadns.net A 104.43.128.98
645	12.244481	192.168.253.9	192.168.253.1	DNS	78	Standard query 0x5244 A xncsi.xboxlive.com
666	13.244926	192.168.253.9	10.0.1.1	DNS	78	Standard query 0x5244 A xncsi.xboxlive.com
667	13.256660	10.0.1.1	192.168.253.9	DNS	271	Standard query response 0x5244 A xncsi.xboxlive.com CNAME xncsi.xboxlive.com.akadns.net CNAME xncsi.xboxlive.com-c.edgekey.net CNAME xncsi.xboxlive.com-c
670	13.320653	192.168.253.1	192.168.253.9	DNS	271	Standard query response 0x5244 A xncsi.xboxlive.com CNAME xncsi.xboxlive.com.akadns.net CNAME xncsi.xboxlive.com-c.edgekey.net CNAME xncsi.xboxlive.com-c
672	16.233589	192.168.253.9	10.0.1.1	DNS	77	Standard query 0xb9a0 A avty.xboxlive.com
673	16.249367	10.0.1.1	192.168.253.9	DNS	267	Standard query response 0xb9a0 A avty.xboxlive.com CNAME avty.xboxlive.com.akadns.net CNAME avty.xboxlive.com-c.edgekey.net CNAME avty.xboxlive.com-c-edg
690	22.236106	192.168.253.9	192.168.253.1	DNS	76	Standard query 0xf0f0 A www.xboxlive.com
695	22.440784	192.168.253.1	192.168.253.9	DNS	122	Standard query response 0xf0f0 A www.xboxlive.com CNAME xboxlive.com A 52.164.206.56 A 104.215.95.187
696	22.455411	192.168.253.9	10.0.1.1	DNS	80	Standard query 0x644a A xmotify.xboxlive.com
697	22.470888	10.0.1.1	192.168.253.9	DNS	215	Standard query response 0x644a A xmotify.xboxlive.com CNAME xmotify.xboxlive.com.nsatc.net CNAME wildcard.xboxlive.com-c.edgekey.net CNAME e07.g.akamaedge
750	23.381085	192.168.253.9	10.0.1.1	DNS	93	Standard query 0xbda9 A v10.vortex-win.data.microsoft.com
755	23.393790	10.0.1.1	192.168.253.9	DNS	283	Standard query response 0xbda9 A v10.vortex-win.data.microsoft.com CNAME v10-win.vortex.data.microsoft.com.akadns.net CNAME geo.vortex.data.microsoft.com
903	33.965772	192.168.253.9	10.0.1.1	DNS	82	Standard query 0xb447 A xsts.auth.xboxlive.com

DNS Protocol

755	23.393790	10.0.1.1	192.168.253.9	DNS	283	Standard query response 0xbda9 A v10.vortex-win.data.microsoft.com CNAME v10-win.vortex.data.microsoft.com.akadns.net CNAME geo.vortex.data.microsoft.com
903	33.965772	192.168.253.9	10.0.1.1	DNS	82	Standard query 0xb447 A xsts.auth.xboxlive.com
904	33.982021	10.0.1.1	192.168.253.9	DNS	145	Standard query response 0xb447 A xsts.auth.xboxlive.com CNAME xsts.auth.xboxlive.com.akadns.net A 66.119.149.145
1021	40.392566	192.168.253.9	10.0.1.1	DNS	71	Standard query 0x43e0 A arc.msn.com
1022	40.392731	192.168.253.9	192.168.253.1	DNS	71	Standard query 0x43e0 A arc.msn.com
1023	40.392733	192.168.253.9	10.0.1.1	DNS	82	Standard query 0x37e1 A xsts.auth.xboxlive.com
1024	40.393320	192.168.253.9	10.0.1.1	DNS	71	Standard query 0x43e0 A arc.msn.com
1025	40.393323	192.168.253.9	192.168.253.1	DNS	82	Standard query 0x37e1 A xsts.auth.xboxlive.com
1027	40.393784	192.168.253.9	10.0.1.1	DNS	82	Standard query 0x37e1 A xsts.auth.xboxlive.com
1028	40.393785	192.168.253.9	192.168.253.1	DNS	71	Standard query 0x43e0 A arc.msn.com
1029	40.393787	192.168.253.9	10.0.1.1	DNS	71	Standard query 0x43e0 A arc.msn.com
1030	40.396707	10.0.1.1	192.168.253.9	DNS	122	Standard query response 0x43e0 A arc.msn.com CNAME arc.msn.com.nsatc.net A 52.229.207.60
1031	40.398447	10.0.1.1	192.168.253.9	DNS	122	Standard query response 0x43e0 A arc.msn.com CNAME arc.msn.com.nsatc.net A 52.229.207.60
1032	40.399740	10.0.1.1	192.168.253.9	DNS	122	Standard query response 0x43e0 A arc.msn.com CNAME arc.msn.com.nsatc.net A 52.229.207.60
1033	40.401957	192.168.253.1	192.168.253.9	DNS	122	Standard query response 0x43e0 A arc.msn.com CNAME arc.msn.com.nsatc.net A 52.229.207.60
1034	40.405540	192.168.253.1	192.168.253.9	DNS	145	Standard query response 0x37e1 A xsts.auth.xboxlive.com CNAME xsts.auth.xboxlive.com.akadns.net A 66.119.149.145
1035	40.409826	10.0.1.1	192.168.253.9	DNS	145	Standard query response 0x37e1 A xsts.auth.xboxlive.com CNAME xsts.auth.xboxlive.com.akadns.net A 66.119.149.145
1036	40.410342	10.0.1.1	192.168.253.9	DNS	145	Standard query response 0x37e1 A xsts.auth.xboxlive.com CNAME xsts.auth.xboxlive.com.akadns.net A 66.119.149.145
1043	40.438743	192.168.253.9	192.168.253.1	DNS	87	Standard query 0xe18c A inference.location.live.net
1044	40.449541	192.168.253.1	192.168.253.9	DNS	260	Standard query response 0xe18c A inference.location.live.net CNAME inference.location.services.windowsphone.com CNAME inference.location.livenet.akadns.n

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, Armino 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>