Digital Investigation, Volume 28, March 2019, pp. 112-118
DOI:10.1016/j.diin.2019.01.003

Sifting through the Ashes: Amazon Fire TV Stick Acquisition and Analysis

M.Hadgkiss, S.Morris, S.Paget

Digital Forensics Unit, Cranfield University

Defence Academy

Shrivenham, SN6 8LA

digitalforensics@cranfield.ac.uk

Keywords: Amazon Fire TV Stick, Digital Forensics, Chip Off

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Abstract

The Amazon Fire TV Stick is a popular device that is the centre of entertainment for many homes. Its collection of functions and features generates a considerable amount of data, giving this device the potential to be included in a multiple investigations. Highlighting a clear requirement for a forensic analysis of the device.

Previous research of smart entertainment devices focuses on the larger areas of the market including Smart TV's, smart speakers and smart watches. All have provided potential forensic artefacts that can be used in investigations. However, data is often acquired using methods that can compromise the forensics of the data.

An Amazon Fire TV Stick was populated with data following a methodology that captured the multiple uses of the device. A chip off acquisition method was then applied to acquire a forensic image. Analysis demonstrated there were a number of artefacts recoverable relating to the system, users and Kodi. The majority of the relevant artefacts identified were located in SQLite3 databases and XML files.

1 Introduction

The business for internet of things (IoT) is ever growing, with new devices continually populating the market. More consumers are striving for smart technology and it has imposed a great need for forensic research of such devices. Initially the market for IoT was heavily entertainment based with companies creating different sticks or boxes that allowed users to access online entertainment. One popular device is the Amazon Fire TV Stick which is part of the amazon ecosystem, that offers a collection of entertainment features.

The purpose of this paper is to formulate a method to acquire and analyse the Amazon Fire TV Stick in a forensically sound manner. Therefore, preventing alterations and changes to the data and keeping to ACPO guidelines. This was achieved by populating an Amazon Fire

TV Stick encapsulating the device's many uses creating a relevant dataset. Applying a chip off acquisition method to the device to acquire physical forensic image. The resulting image was analysed using a variety of Digital Forensic software to establish whether there are any artefacts stored on the device and to assess the forensic relevance of those artefacts.

The rest of this paper is structured as follows: Section 2 identifies related research; the methodology is discussed in Section 3. Section 4 highlights the chip off process identified and section 5 working with the data. Section 6 focuses on analysis and artefacts identified are discussed in Section 7. Conclusions are described in section 8.

2 Related Research

2.1 Smart Device Forensics

Previous research of smart devices has identified there are potential artefacts on the devices that could be used in forensic investigations. Currently, the main focus of smart entrainment device research has been Smart TV's. There have been many papers discussing how to approach an investigation of these devices and artefacts that maybe present. **(Sutherland, Read and Xynos, 2014)** Through to technical forensic analysis of the device, identifying acquisition methods and present artefacts. **(Boztas, Riethoven and Roeloffs, 2015).**

With Smart TV's initially being unaffordable, entertainment sticks and boxes were produced to allow a standard TV to access and perform smart functions. Other studies has shown these devices also provide data that could have forensic relevance. Research conducted on the Amazon Fire TV Stick focused on experimenting with acquisition methods and analysis of the data acquired. The EXT4 filesystem and partition structure was identified using an android debug bridge acquisition method. However, in order to gain further data manual acquisition was used, ultimately compromising the forensic integrity of the evidence. **(Morrison et al., 2017)** An analysis of the Google Chromecast discovered the NAND memory was encrypted, therefore requires decrypting before analysis. **(Van Bolhuis and Van Bockhaven, 2014)**. Even though there has been previous research in this area there has been limited research that has been able to keep the forensic integrity of the data acquired, demonstrating a clear area for new research.

2.2 Fire TV Stick Features

The Fire TV Stick is predominantly an entertainment device, allowing users to access a range of applications from media content, games and books. **(James, 2016)** This is all facilitated through the Amazon application store, allowing users to customise and increase the capability of the device. User's wanting additional content or access can install third party applications by configuring developer settings on the device. These applications typically have avoided any regulation, making the device vulnerable to potential attacks and giving users access to content they shouldn't.

Alexa, Amazon's voice assistant is also available on the second-generation Amazon Fire TV Stick. Alexa responds to many user voice commands, including opening applications, play

and pause streaming etc. **(Burgess, 2018)** Making it simple to navigate through the Fire TV Stick features however, is only available after initiating the voice command button on the remote, demonstrating that a user would have had to intended to initiate or complete the action.

2.3 Modification And Criminal Relevance

Due to the Fire TV Sticks compact nature, it is very easy to conceal and hide as well as being very mobile and having 8GB of onboard storage media, users can easily customise their device. This could be uploading or downloading images and video or using various applications to communicate with people. Due to these characteristics this device could easily be used for nefarious purposes an example of which is a mobile incident image device.

As discussed in 2.2 software modifications can be made to the Fire TV Stick, the predominant modification is installing Kodi **(McNeal, 2017)**. Kodi is an open source media player that enables a user to stream online videos from a third-party plugins and repositories. This can result in users streaming copyrighted material or illicit content. Many people manipulated this modification for both personal use and financial gain, constructing businesses that sold modified devices to the general public and other businesses. In 2016, Terry O'Reilly was sentenced with conspiracy to defraud, due to selling over a thousand devices with modifications. **(R v. Terry O'Reilly, 2016)** There have been multiple cases like this that have resulted in custodial sentences. However, despite arrests these devices are still easily purchased online, demonstrating there is still a clear market for devices with software modifications.

2.4 Acquisition

The standard digital forensics acquisition method involves creating an exact copy of the target device. The method involves removing the storage media from the device, then creating a forensically sound bit for bit copy of the storage media using software. **(Craiger, 2017)** This becomes more complex with mobile devices, as the storage media is typically not removable, which prevents the use of the standard methods.

The Fire TV Stick's main connection is HDMI which is used to transfer audio and video data, therefore could not be used to obtain data from the device. A micro USB port is also present on the device, its predominant purpose is to power the device. The second generation of the Fire TV Stick supports the use of USB devices and storage media through this port, whereas the first generation the device had to be rooted, before these devices would be recognised. **(Saba, 2018)** Therefore could be utilised for acquisition purposes, previous research has explored this option. Various methods were tested including Android Debug Bridge extraction, UFED Touch Test, Rooting, custom python scripts and manual extraction. **(Morrison et al., 2017)** Some methods yielded data, however the forensic soundness was compromised in most cases, demonstrating a need for alternative acquisition method.

2.5 Chip Off and Direct EMMC

Chip off is an alternative acquistion process that involves physically removing flash memory chips from a device, allowing for a raw physical acquisition of the device. **(Billard and Vidonne, 2017)** This invasive process is broken down to three parts: removal, restoration and acquisition. Each of these steps require specific equipment and technical methods, therefore is considered one of the last resort acquisition methods. However, for some mobile devices it is the optimum way to gather the most quality data from the device as the standard method is unusable. Due to the Amazon Fire TV Stick having these quality's this method was considered to produce a forensically sound image.

Another method, direct EMMC or In System Programming (ISP) can be implemented to prevent and mitigate some of the problems that occur with chip off acquisition. This method involves directly connecting to the device's PCB at specific points. However, this method requires knowing the points of connection in order to function and the ability to control the processor. This method has been implemented on previous research on smart TV's, **(Boztas, Riethoven and Roeloffs, 2015)** but discovered an image could not be taken due to the processor accessing the chip. Demonstrating that this method can reduce the invasive nature of acquisition but is not always successfully implemented.

3 Methodology

The aim of this research is to demonstrate a standard acquisition of the Fire TV Stick is not a viable option and to test alternative acquisition methods to gain a forensic image of the Amazon Fire TV Stick. After acquisition the image will be analysed, looking for relevant system and user artefacts using a range of digital forensic tools.

3.1 Testing Environments

The Amazon Fire TV Stick used during experimentation was a second-generation device with Alexa voice remote, which was purchased directly from Amazon. Two mobile devices were used to test the application remote feature an Apple iPhone SE running iOS 9.3.2 and LG Nexus 4 running Android 5.1.1. On both devices, Amazon Fire TV Remote Application was downloaded from the Apple and Google application stores.

3.2 Dataset

Given the invasive nature of the chip-off acquisition process it was not feasible to generate a large number of individual experiments, therefore the decision was taken to replicate a range of user activity in a single data set. During experimentation Amazon Fire TV Stick was running Fire OS 5.2.4.2 and device developer options and ability to download applications from third party sources were enabled.

For each action taken on the device, date and time was recorded, and contemporaneous notes were made. The actions were as follows:

- Sign in with one user account
- Connected to WIFI

    - Two Wi-Fi connection were connected to

- Download and use applications from Amazon App store
    - Six applications were installed
    - Two game applications were used
    - Two video applications were installed, and multiple videos were watched
    - One casting application was installed
    - One downloader application was installed and used

- Watch Amazon Video content
    - Seven TV series episodes and movies were watched
    - Content was paused, played, fast forward and rewound. These actions were initiated by the Fire TV Stick remote and phone application on both phones.

- Connect iPhone SE and Google Nexus 4 to Fire TV Stick via Amazon Fire TV application
    - Remote features: home, play, pause, fast forward and rewind. Alexa commands were also issued to initiate these actions.
- Alexa commands
    - Used on both the Fire TV Stick remote and both mobile phones
    - Open applications
    - play, pause, fast forward and rewind Amazon video content

- Use Kodi application with connect repository
    - Kodi was downloaded on Android Nexus 4 and installed on the Fire TV Stick via Apps2Fire.
    - Two repositories were installed
    - Four TV shows and movie were watched through the repository
    - One TV show was downloaded to the Fire TV Stick

3.3 Analysis Tools

Access Data FTK Imager 3.4.2.6 was used to acquire the data from the chip. Primary viewing and analysis were completed using WinHex 18.5 and X-Ways 17.7 hexadecimal editor software. Therefore, allowing the exploration through each of the partitions at the binary level. When artefacts of relevance were located, they were exported out of the software and other tools were used. Secondary tools used were DB Browser for SQLite 3.10.1 and XML Marker 1.1. A virtual machine (VM) was used to mount and display the data, it was created using VMware Workstation 14 and Linux Mint 18.3 Cinnamon OS was installed using default options.

4 Acquisition

In order to justify using the chip-off acquisition, a standard acquisition method was attempted in order to show there was acquisition issues. The initial acquisition method attempted used the micro USB port. A Tableau USB bridge was connected to the device using a male micro USB cable to male USB lead. After this connection is made, FTK Imager

software 4.1.1 was used to attempt acquisition of the device. This was attempted multiple times however the Fire TV Stick was not recognised by the imaging system.
The Fire TV Stick was disassembled to reveal the device's PCB. See figure 1.

Figure 1 – Amazon Fire TV Stick Disassembled

Once the PCB was exposed, metal shielding was visibly covering parts of the PCB. The shielding must be removed in order to reveal the chips below, allowing for identification of the correct data chip.

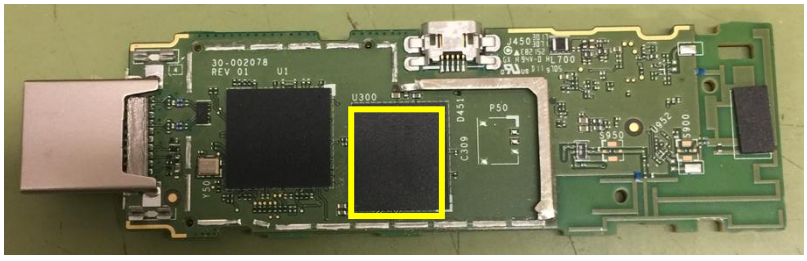

Figure 2 – Amazon Fire Stick Without Shielding

Removing the shielding exposed three ball grid array (BGA) surface mount chips. Typically, BGA's have both manufacture details and serial numbers printed on the top side of the chip. However, sometimes manufactures tamper with these details to obscure the chips function or manufacturer i.e. removing the serial numbers, making identification harder. The names and serial numbers had not been tampered with on the Amazon Fire TV Stick we examined so an internet search was conducted to gather further information about the chip and functionality. From the information gathered the chip highlighted in yellow in figure 2 was identified as the data storage chip. The data chip was a SK Hynix BGA 221 embedded Multi-Media Controller (eMMC).

Following identification, the chip is then removed from the PCB. This is completed by applying heat to the chip and lifting it off the PCB using a suction tool. The equipment used was: heat gun, thermocouple, suction pen, PCB board, stopwatch and clamps. Once the set up was secure heat could start to be applied to the chip. Initially temperature started at

200°, then after 30 seconds the heat was removed, and the suction tool was applied to try and remove the chip. After 2 minutes the heat was increased up a further 10°. The chip was removed at 290°C-300°C after 27 minutes.

After the removal, the excess solder is removed and the chip is re-tipped, by reapplying a small amount of solder to the chip. Allowing the pads to make contact with the pogo pins in the chip reader. See figure 4.

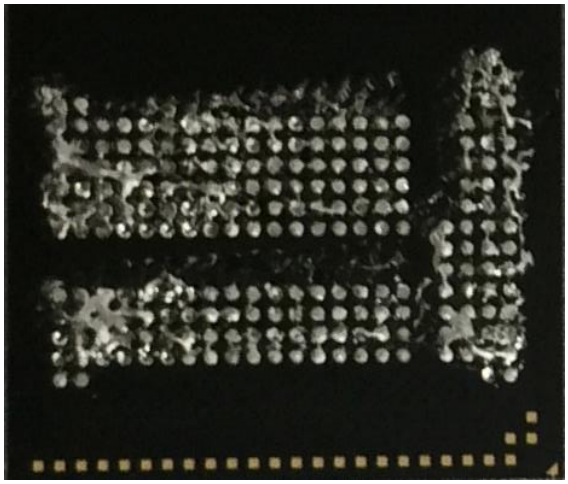

Figure 3 – Chip Removed From PCB

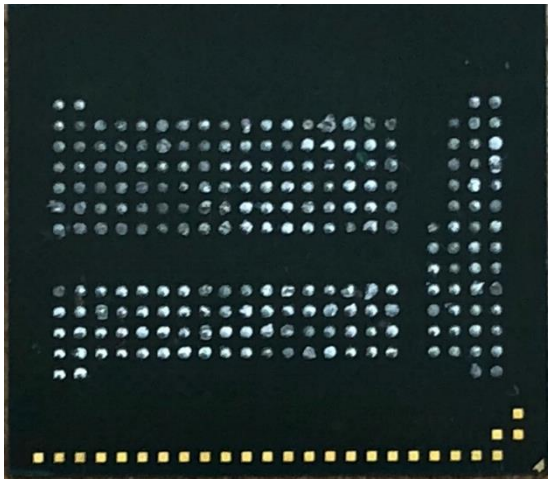

Figure 4 – Cleaned, Re-tipped Chip

After the cleaning process, the chip was placed in an MOORC E-Mate Pro adapter tool see figure 5. Once connected to the imaging machine, the chip is was recognised as a device and Access Data FTK imager was used to acquire the data in a raw format.

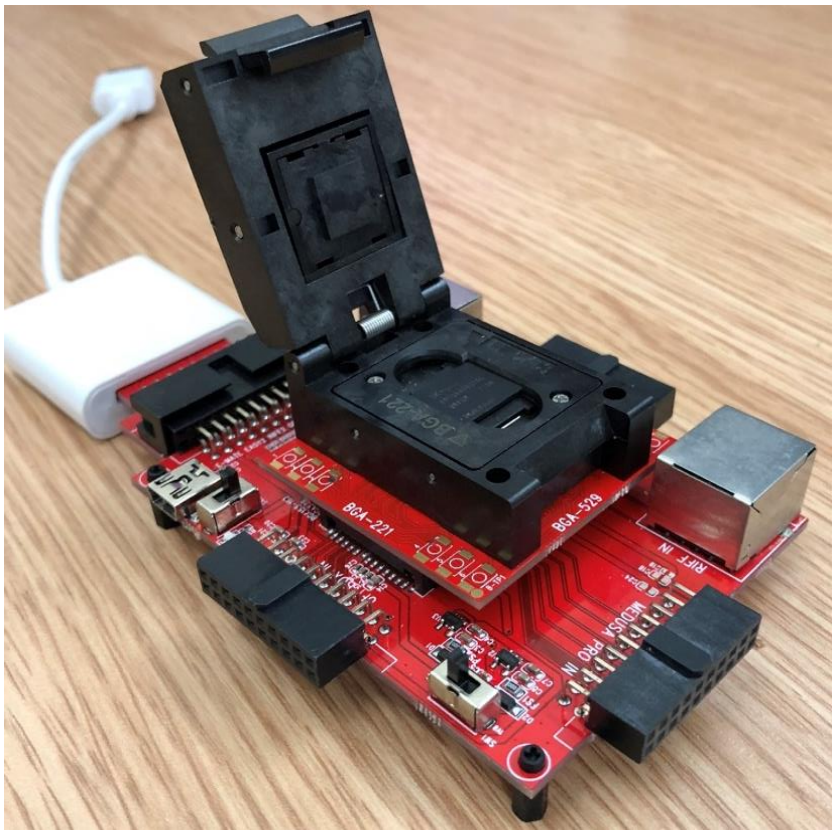

Figure 5 – MOORC E-Mate Pro EMMC Adapter Tool

5 Working With The Data

After finishing acquisition, WinHex was used to display the Fire TV Stick data. By analysing the Master Boot Record (MBR), there was a one partition entry which pointed to a GUID partition header, indicating the Fire TV Stick chip had a GUID Partition Table (GPT) partitioning scheme. The GPT header was used to locate the partition table, it showed that there were 13 partitions, conforming **(Morrison et al., 2017)** previous research's findings.

Opening partitions 11, 12 and 13 the same structure was being displayed. (See figure 7). An Ext4 WinHex template was applied to each partition start sector revealing that partition 11, 12 and 13 all had the same universally unique identifier (UUID). Therefore, the software could have been presuming each partition was the same. This occurred until a refined volume snapshot was taken of each partition with the Ext3/Ext4 Parse journal option off, forcing the software to update the details. To further verify this, each partition was mounted in a virtual Linux Mint 18.3 Cinnamon environment.

Name	Ext.	Size	Created	Modified	Inode changed	Attr.	1st sector
securedStorageLocation		4.0 KB		20/09/2017 11:13:15 +1	20/09/2017 11:13:15 +1	rwxrwx--x	262,008
misc		4.0 KB	01/01/2010 00:00:02 +0	01/01/2010 00:00:03 +0	01/01/2010 00:00:01 +0	rwxrwx--t	7,344,112
lost+found		4.0 KB			01/01/2010 00:00:01 +0	rwxrwx---	202,144
hwval		4.0 KB		01/01/2010 00:00:30 +0	01/01/2010 00:00:01 +0	rwxrwx---	261,992
dontpanic		4.0 KB	01/01/2010 00:00:02 +0	01/01/2010 00:00:02 +0	01/01/2010 00:00:01 +0	rwxr-x---	11,538,416
dalvik-cache		4.0 KB		01/01/2010 00:00:02 +0	01/01/2010 00:00:01 +0	rwxrwx--x	202,152
(Root directory)		4.0 KB		01/01/2010 00:00:57 +0	01/01/2010 00:00:01 +0	rwxrwx--x	202,136
.journal		95.2 MB				rw-------	7,160
Volume slack		1.0 MB					12,856,536
Indirect blocks							
Idle space							
Free space (net)		4.2 GB					

Figure 6 – WinHex Partition Structure Being Displayed For Partitions 11, 12 And 13

fdisk -l command was used to display the sector size and start sector of each of the partition, allowing us to gain the information required to mount each partition. See figure 7.

```
melissa@firestick ~/Desktop $ fdisk -l Firestick.dd
Disk Firestick.dd: 7.3 GiB, 7818182656 bytes, 15269888 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 222FB76B-B3C5-41DF-9DD0-2650CF1303C2

Device           Start      End  Sectors  Size Type
Firestick.dd1     2048     4095     2048    1M Linux filesystem
Firestick.dd2     4096     6143     2048    1M Linux filesystem
Firestick.dd3     6144    41727    35584 17.4M Linux filesystem
Firestick.dd4    41728    43775     2048    1M Linux filesystem
Firestick.dd5    43776    76543    32768   16M Linux filesystem
Firestick.dd6    76544   109311    32768   16M Linux filesystem
Firestick.dd7   109312   110335     1024  512K Linux filesystem
Firestick.dd8   110336   117503     7168  3.5M Linux filesystem
Firestick.dd9   117504   127743    10240    5M Linux filesystem
Firestick.dd10  127744   137983    10240    5M Linux filesystem
Firestick.dd11  137984  1899263  1761280  860M Linux filesystem
Firestick.dd12 1899264  2411263   512000  250M Linux filesystem
Firestick.dd13 2411264 15269854 12858591  6.1G Linux filesystem
```

Figure 7 – Fire Stick Structure In A Linux Environment

The required partitions were mounted in a read only state keeping it forensically sound using the commands in Table 1. Each of the individual flags are explained in Table 2.

Partition Number	Mount Offset	Commands
11	70647808	sudo mount –t ext4 –o ro,noload,loop, offset=70647808 Firestick.dd /mnt/amazon_partition_11
12	972423168	sudo mount –t ext4 –o ro,noload,loop, offset= 972423168 Firestick.dd /mnt/amazon_partition_12
13	1234567168	sudo mount –t ext4 –o ro,noload,loop, offset=1234567168 Firestick.dd /mnt/amazon_partition_13

Table 1 – Fire Stick Partition Mount Commands

Flag	Description
-t	Allows you to specify the partition type
noload	Prevents the loading of the journal once the image has mounted
loop	Allows the device to become accessible as a block device
offset	Offset of partition start in bytes
Firestick.dd	Image file name
/mnt/amazon_partition_XX	Mount point of the image file

Table 2 – Fire TV Stick Mount Command Flag Explained

The blkid command was used on the mounted partitions to display the UUID seen in figure 8, confirming and verifying the duplicated UUID.

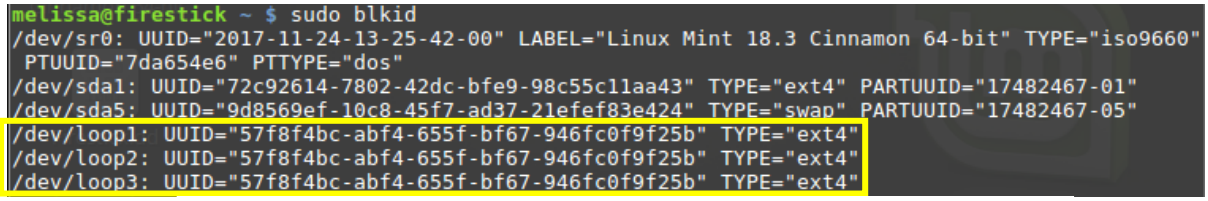

Figure 8 – Using blkid Command To Display Partition UUID

6 Analysis

The artefacts in this section were identified following an analysis looking for activity relating to those carried out in section 3.2. The artefacts were found within the Fire TV Stick image mainly located in partition 13. All artefacts are presented in table 3. The file path provided in the structure [PXX, where p is the partition number] followed by the partition absolute path.

There were multiple system and user level artefacts found, which were located in SQLite databases, XML files and text files.

Location	Type	Information Contained Within The Artefact
P13\data\com.android.providers.settings\databases\settings.db	SQlite3	Device name, Wi-Fi device name, time zone, country
P13\system\users\userlist.xml	XML	User ID's that are associated with the Fire TV Stick
P13\system\users\[user id].xml	XML	User names, user icon location, user restrictions
P13\system\users\[user id]\accounts.db	SQlite3	Users associated with the Fire TV Stick
P13\misc\wifi\networkHistory.txt	Text file	Wi-Fi SSID's, BSSIS's
P13\data\com.amazon.wifilocker\shared_prefs\com.amazon.wifilocker.PREFERENCE_WIFI_NETWORK.xml	XML	SSID's of Wi-Fi
P13\securedStorageLocation\com.amazon.kindleautomatictimezone\TimeZoneCacheManager.db	SQlite3	Time Zone, day light saving SSID if Wi-Fi was used to predict the time zone
P13\data\com.amazon.device.controllermanager\databases\devices.db	SQlite3	Devices that have been connected to the Fire TV Stick.
P13\system\usagestats\[user id]	XML	Contain information on user's usage stats
P13\data\com.amazon.avod\files\databases\dbplaybackhistory.db	SQlite3	Name of Amazon video content, last accessed time, watched position, length of video
P13\system\recent_tasks\	XML	The package that has been called, last time moved, last time active, first time active, user id, task id and activity.
P13\media\[user id]\Android\data\org.xmbc.kodi\files\.kodi\temp\kodi.log	Text file	Locations of other files related to Kodi application processes
P13\media\[user id]		Standard area where Kodi suggests to download files.
P13\media\[user id]\Android\data\org.xbmc.kodi\files\.kodi\userdata\profiles.xml	XML	User id associated with Kodi
P13\media\[user id]\Android\data\org.xbmc.kodi\files\.kodi\userdata\Database\Addons27.db	SQlite3	Installed add-ons and repository's

Table 3 – Summary Of Artefacts

7 Discussion

7.1 Acquisition

The Amazon Fire TV Stick PCB was separated from the casing with ease with correct tools, revealing the shielded chips on the PCB. The most effective way to remove the shielding was filing the top edges, causing the top of the shielding to separate from the rest of the shielding, therefore exposing the chips on the PCB. This method removed the need of applying heat to the PCB before attempting the chip off method, protecting and reducing the vulnerability of the chip and the PCB to heat exposure. Discovering the data chip was EMMC, we could have explored acquisition in both chip off and direct EMMC methods. However direct EMMC required further research in identifying the ports of interest and the using the need for specialised tools. Therefore, a chip off acquisition method was chosen, however future work of the device could consider this acquisition method.

To ensure the chip was removed at the correct temperature we started at 200°C working up at small intervals of temperature and time, trying to get an accurate removal temperature. This method caused the chip to be exposed to heat for 27 minutes which could have created damage to the chip and therefore effected the potential stored data. From 2006 all consumer devices sold in the EU should not contain lead, therefore prior to the removal of the chip an estimate of the melting point of the solder was around 217°C, this was the reasoning behind our initial temperature of 200°C. In older devices it is essential to raise the temperature in small increments otherwise the component will fail. In BGA chips there is a lower thermal resistance, allowing heat to flow through to the PCB, therefore removing the requirement to slowly increase temperature. In the future the chip is only required to be heated to 300°C for removal, reducing the heat contact time down.

7.2 Artefacts

System, user and Kodi Artefacts were located through performing key word searches and browsing through the file structure in WinHex. All artefacts, located in table 3 where found in SQLite3 databases, XML and text files, which were all human readable and examined using secondary tools mentioned in 3.3.

Various system level artefacts were found, giving a broad overview of the device. This included device name, time zone, users, network connections and connected devices. These artefacts were spanned across various file paths and in different file formats, highlighting a potential area for automation in the future. All of these areas provided an insight to how the device was set up and how users were operating the device.

User level data was present on the device, including Amazon Video content and user statistics. These artefacts collectively gave a view of how the user was interacting with the device and an indication on what had been used and when it was used. Producing a clear indication of a user's behaviour whilst using the device.

Several Kodi artefacts were identified, demonstrating whether the application had been installed and how the application was being used after installation. This is particularly

important as many users were buying devices from third party sellers with Kodi preloaded. Therefore the artefacts located can help establish whether users had actually used the application or not.

Collectively all artefacts provide an insight into actions the user or users have completed on the device. However, using a dataset method actions could only be controlled to a certain degree. Therefore, to strengthen the forensics value of each of the artefacts identified smaller experiments should be explored. This will allow certain features to be individually tested, providing more control of the experimentation. A much larger dataset would also be beneficial, mimicking a real life scenario assisting with testing the capacity of the files and seeing how often data is being overwritten.

8 Conclusion

This paper has provided a suitable way to create a forensically sound image of the Amazon Fire TV Stick, allowing for analysis. Various artefacts were identified relating to all of the Fire TV Stick features including streaming videos, connecting additional devices and using a third-party applications. Each providing an indication how a user has interacted with the device and what actions they have completed.

After this research, we aim to strengthen the artefacts located by completing further experimentation on the Amazon Fire TV Stick increasing the number of datasets examined. Building upon this research the new generation Amazon Fire TV Stick could be compared to demonstrate any changes or similarities between the devices. Furthermore, the Amazon Fire TV could be tested to see whether they have a similar structure and artefacts compared to the Amazon Fire TV Stick, establishing if Amazon devices have similarities between each device.

Bibliography

Amazon.co.uk. (2017). Available at: https://www.amazon.co.uk/Stick-Alexa-Remote-Streaming-Player/dp/B01ETRIFOW [Accessed 9 Nov. 2017].

Billard, D. and Vidonne, P. (2017). [online] Lerti.fr. Available at: http://www.lerti.fr/web/pdf/20150930-Chip-off-by-Matter-Subtraction-Frigida-Via.pdf [Accessed 18 Dec. 2017]

Boztas, A., Riethoven, A. and Roeloffs, M. (2015). Smart TV forensics: Digital traces on televisions. Digital Investigation, [online] 12, pp.S72-S80. Available at: https://www.sciencedirect.com/science/article/pii/S1742287615000134.

Burgess, M. (2018). Amazon's new £40 Fire TV Stick has launched in the UK. [online] Wired.co.uk. Available at: http://www.wired.co.uk/article/amazon-alexa-fire-stick-tv-control [Accessed 21 Mar. 2018].

Craiger, J. (2017). [online] Cyberace.org. Available at: http://www.cyberace.org/Publications/craiger.forensics.methods.procedures.DRAFT.pdf [Accessed 18 Dec. 2017].

Developer.amazon.com. (2018). Developer Tool Options | Amazon Fire TV. [online] Available at: https://developer.amazon.com/docs/fire-tv/system-xray-developer-tools.html [Accessed 21 Mar. 2018].

ISO/IEC 27037:2012 (2018). ISO/IEC 27037:2012 - Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence. [online] Iso.org. Available at: https://www.iso.org/standard/44381.html [Accessed 21 Mar. 2018

James, F. (2016). Fire Stick: The 2016 User Guide and Manual. 1st ed. CreateSpace Independent Publishing Platform, pp.1-24.

Kodi (2017). About Kodi. [online] Available at: https://kodi.tv/about [Accessed 18 Dec. 2017].

Kodi | Open Source Home Theater Software. (2017). Kodi | Open Source Home Theater Software. [online] Available at: https://kodi.tv [Accessed 12 Dec. 2017].

McNeal, I. (2017). Is Kodi popularity to blame for shortage of Amazon Fire TV sticks?. [online] gazettelive. Available at: http://www.gazettelive.co.uk/news/teesside-news/kodi-popularity-blame-shortage-amazon-12694560 [Accessed 18 Dec. 2017].

Saba, E. (2018). Amazon Fire TV Stick 2 supports USB Storage, Keyboards/Mice, and Ethernet Adapters via USB OTG without Root. [online] AFTVnews. Available at: http://www.aftvnews.com/amazon-fire-tv-stick-2-supports-usb-storage-keyboardsmice-and-ethernet-adapters-via-usb-otg-without-root/ [Accessed 21 Mar. 2018].

Sutherland, I., Read, H. and Xynos, K. (2014). Forensic analysis of smart TV: A current issue and call to arms. Digital Investigation, 11(3), pp.175-178.

R v. Terry O'Reilly [2016] (Nottingham Crown Court).

Van Bolhuis, P. and Van Bockhaven, C. (2014). Forensic analysis of Chromecast and Miracast devices. MSc. University of Amsterdam.

Sifting through the ashes: Amazon Fire TV stick acquisition and analysis

Hadgkiss, Melissa

2019-01-14

Hadgkiss M, Morris S, Paget S. Sifting through the ashes: Amazon Fire TV stick acquisition and analysis. Digital Investigation, Volume 28, March 2019, pp. 112-118
https://doi.org/10.1016/j.diin.2019.01.003