Amazon Kindle Fire HD Forensics

Asif Iqbal[1,3(✉)], Hanan Alobaidli[1,2], Andrew Marrington[3], and Ibrahim Baggili[4]

[1] Athena Labs, Dubai, UAE
asif@babariqbal.com
[2] University of Sharjah, Sharjah, UAE
[3] Zayed University, Dubai, UAE
marrington@computer.org,
[4] University of New Haven, Connecticut, USA
ibaggili@newhaven.edu

Abstract. This research presents two developed approaches for the forensic acquisition of an Amazon Kindle Fire HD. It describes the forensic acquisition and analysis of the Amazon Kindle Fire HD device. Two developed methods of acquisition are presented; one requiring a special cable to reflash the boot partition of the device with a forensic acquisition environment (Method A), and the other exploiting a vulnerability in the device's Android operating system (Method B). A case study is then presented showing the various digital evidence that can be extracted from the device. The results indicate that Method A is more favorable because it utilizes a general methodology that does not exploit a vulnerability that could potentially be patched by Amazon in future software updates.

Keywords: Amazon Kindle Fire HD · Digital · Forensics · Analysis · Acquisition · Android forensics · Forensic flashing

1 Introduction

Tablets, also considered to be mobile devices, are the new computers of this decade. The portability of mobile devices provide users with the ability to use them anywhere and anytime in a variety of ways such as organizing their contacts, appointments, electronic correspondence, playing games etc. Over time, mobile devices accumulate a wealth of information about their users and their behavior, which is valuable in a course of an investigation. According to Fabio Marturana et al. [1] and NIST (National Institute of Standards and Technology) [2] it is more likely that law enforcement will encounter a suspect with a mobile device in his/her possession than a PC or laptop.

Scientific literature discusses various forensic research into small scale devices such as iDevices [3–6] and Android devices [7, 8, 20] from mobiles to tablets because of their importance in any investigation. Although there are many tablets that have been released in recent years, the competitive price of the Amazon Kindle Fire HD makes it attractive for consumers in the tablet sector.

The aim behind this research was to investigate forensically sound methodologies that could be used to acquire and analyze an Amazon Kindle Fire HD.

P. Gladyshev et al. (Eds.): ICDF2C 2013, LNICST 132, pp. 39–50, 2014.
DOI: 10.1007/978-3-319-14289-0_4

This paper is divided into several sections – Sects. 1 and 2 contain an introduction and a literature review, while Sects. 3 and 4 discuss the developed acquisition methods and the analysis of the acquired Amazon Kindle Fire HD image to identify the possible sources of evidence respectively. Finally, in Sect. 5 we conclude and give direction for future work.

2 Literature Review

Small Scale Digital Device (SSDD) forensics appeared alongside the invention of mobile devices such as PDAs, mobiles, smartphones and now tablets such as the iPad and Amazon Kindle Fire HD. The main reason for the forensic community's interest in SSDD research the valuable digital evidence that can be found on these devices. The SDDD forensics field can be defined as a sub-field of digital forensics that is concerned with the acquisition and analysis of evidence found on mobile devices such as cell phones, smartphones and now tablets like the iPad and Amazon Kindle Fire HD.

In 2011 the Amazon Kindle Fire e-reader was released as a new version of the long established Kindle e-reader. The Kindle Fire device contained new features compared to the older e-reader devices, as it included web browsing and applications – moving the Kindle out of the e-reader market segment into the tablet space. Despite the success of the various Amazon Kindle devices, and the appearance of the Amazon Kindle Fire tablet, there has been little published forensics research on these devices. With respect to the older e-reader Amazon Kindle devices, some blogs discussed the forensic investigation of these e-readers in order to provide insight into the inner working of the device and the possible evidence that can be found on it.

A blogger by the name Allyn Stott provided a brief discussion about the forensic investigation of one of the older Kindle devices, the Kindle Touch 3G. The blog identified the imaging method used along with a set of valuable information found on the device [9]. Another blog written by Marcus Thompson attempted to provide a baseline for the forensic study of the Amazon Kindle, the blog represented data acquired after imaging and analyzing the data on a Kindle device. Thompson has identified that the device image included fifty-nine books, three games, forty-five converted .pdf files, sixteen Kindle screenshots, two audio books, two book samples, one blog subscription, one magazine subscription, and one newspaper subscription. There are several other valuable information has been identified such as the browser cookies, settings and bookmarks along with information regarding the last book being read and the last time an audio book was listened to [10]. There are other blogs that tried to provide information about Amazon Kindle forensics such as [11, 12] along with these blogs MacForensicsLab have identified that its software can be used to image and analyze an Amazon Kindle keyboard [13].

The first notable published research on Kindle Forensics was by Peter Hannay at Edith Cowan University [14]. His research offered insight into forensically examining the various partitions on a Kindle by enabling the debug mode and then enabling usb networking – thus treating the Kindle like a network device to acquire data from it.

Iqbal et al. [15] conducted a study that discussed the forensic acquisition and analysis of the Amazon Kindle Fire, the first such study on an Amazon Kindle Fire.

In this research, the acquisition process required the Kindle Fire Device to be connected to a forensic workstation that contains a payload to be injected into the device using ADB (Android Debug Bridge) to a temporary location. This Payload is then executed on the device in order to reboot the device with a temporary root access using an exploit in Android Gingerbread. A bitwise image of the data partition is acquired using the Linux "dd" utility. The analysis of this image produced valuable digital artifacts, similar to the possible evidence that can be found on iDevices and any powered Android device. The research showed that the Amazon Kindle Fire is a potential source of more digital evidence (both in terms of variety and quantity) than the older Kindle e-reader devices because besides being an e-reader this version of the Amazon Kindle Fire provided tablet functionality.

In 2012 Oxygen Forensics, which offers forensic data examination tools for smartphones and mobile devices, released Oxygen Forensic Suite 2012 providing forensic support for the new Kindle Fire HD. The Oxygen team investigated the specifics of the new device, analyzed the new and unique apps, and determined types and locations of user data that can be stored by these apps [16]. However, proprietary software like Oxygen is effectively, a "blackbox" which obscures the process of acquisition and analysis of digital evidence from the examiner. Consequently questions may be raised as to the reliability of scientific testimony provided to a court by that examiner.

Currently, there has been no published research that investigated the forensic analysis and acquisition of a Kindle Fire HD. This work aims to fill this gap with regards to Kindle Fire HD forensics.

3 Acquisition Methodologies

While investigating the Amazon Kindle Fire HD, the researchers found two viable acquisition methodologies. These methodologies are discussed in the sections that follow.

3.1 Acquisition Methodology A

The first acquisition methodology required the creation of a "Factory Cable" also known as "Active Power Cable" see Fig. 1. A factory cable boots the Kindle Fire HD device to bootloader (u-boot) and awaits for commands from a host PC. For the creation of the "Factory Cable" a USB Micro-B to A cable used for Android data transfer was modified to provide +5 V to unused pin #4 on the Micro-B connector side.

Later on a custom boot image was sent to the device (overwriting the boot partition) and is booted by executing "fastboot -i 0x1949 flash boot boot.img", "fastboot -i 0x1949 flash system boot.img" and "fastboot -i 0x1949 reboot", where boot.img is a boot disk image containing a minimal Linux forensic acquisition environment, and the "i" switch is the manufacturer unique ID. Initially, we had intended to employ an approach based on that of Vidas et al., where the recovery partition is reflashed with a forensic acquisition environment [8], however, we found that the recovery partition

was not available on the Kindle Fire HD device. The implementation of specific partitions can vary between different Android devices. However, the reasoning which motivated the selection of the recovery partition in the work of Vidas et al. [8] equally applies to the boot partition – the normal boot sequence of the device is still interrupted, and the user data partitions have not been overwritten. The difference is that the device would need to be reflashed after the examination in order to restore its original boot partition (which would apply equally to the recovery partition in Vidas et al. [8], only changes to that partition are less likely to be noticed by end users). In both cases, the use of the recovery partition in Vidas et al. [8] and the use of the boot partition in this work, the Android device is booted into a known "safe" acquisition environment, roughly analogous to the use of a forensic boot CD such as Helix in computer forensics.

After the recovery has finished booting, the ADB (Android Debug Bridge) server is started on the host PC. Android Debug Bridge (ADB) is a command line tool that facilitates the communication with an emulator instance or connected Android device [18] such as the Amazon Kindle Fire. ADB is used from the host PC to connect to the ADB client running on the Kindle Fire HD device. Using adb the following commands are executed on the Kindle Fire HD device to acquire an image of the "userdata" partition:

- adb shell -c "chmod 777/dev/block/"
- adb pull/dev/block/mmcblk0p13

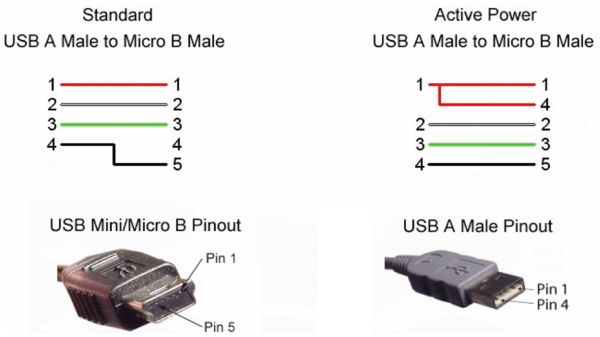


Fig. 1. The difference between a standard and an Active power cable

3.2 Acquisition Methodology B

Another method of acquisition is to use a known exploit in the Kindle Fire HD software to gain root access. In order for this method to work USB Debugging must be enabled on the Kindle Fire HD device from the setting menu (Menu-> More>Security-> Android Debugging). This acquisition methodology is dependent on the software version of the Android Kindle Fire HD device - we employed software version 7.2.3 (the latest at time of writing). Future Kindle software versions may address the vulnerability which permits this form of acquisition to work. This method works by making it seem as though the system is running in a virtualized qemu environment

which enables debugging and root access in ADB (Android Debug Bridge). This exploit known as "qemu automated root" was, to our best knowledge, discovered by "sparkym3", a member of xda-developers.com forums [17].

In order to gain root access to the Amazon Kindle Fire HD device, the following commands are executed from the host workstation after connecting ADB to the device:

- adb shell mv/data/local/tmp/data/local/tmp.bak
- adb shell ln -s/data/data/local/tmp
- adb reboot
- adb wait-for-device
- adb shell rm/data/local.prop > nul
- adb shell "echo ro.kernel.qemu=1 > /data/local.prop"
- adb reboot

After the device has finished rebooting ADB will be running with root privileges. Following commands are executed to acquire an image of the user data partition:

- adb shell -c "chmod 777/dev/block/"
- adb pull/dev/block/mmcblk0p13

3.3 Discussion of the Acquisition Methodologies

Of the two acquisition methodologies we have employed, acquisition methodology A is preferred since it is independent of the software version and does not interfere with the partitions which are most likely to contain valuable digital evidence. Acquisition methodology B worked in our own experiment, but future software changes (to address the vulnerability which permits the qemu automated root exploit [17], for example) may make methodology B non-viable. Another advantage of acquisition methodology A as we see is that the examiner provides a known safe minimal Linux-based forensic acquisition environment and does not depend on any software installed on the device. Acquisition methodology B may be subject to interference from malware or an otherwise modified kernel on the Amazon Kindle Fire HD device. The downside of acquisition methodology A is that it requires specialized hardware (in the form of the factory cable), but this is not unique in digital forensics, especially with respect to small scale digital devices.

In investigations concerned with only with the primary storage of the Amazon Kindle Fire HD device, like Vidas et al. [8] we have a clear preference for avoiding the use of root kits to modify the device. However, we note that for live memory acquisition, neither of the acquisition methodologies we have described above are suitable, as they require the rebooting of the Kindle Fire HD device. In cases where live memory acquisition is necessary, it remains necessary to root the device [19]. In our analysis, described in Sect. 4 below, we have constrained ourselves to the examination of images acquired from the Kindle Fire HD device's secondary storage.

4 Case Study

The aim of the case study was to simulate the activities done by a regular user of this device and study the possible traces of evidence. In the case study the user uses the

Table 1. Amazon Kindle Fire HD Partition Table

No.	Start	End	Size	File system	Name
1	131 kb	262 kb	131 kb		Xloader
2	262 kb	524 kb	262 kb		Bootloader
3	524 kb	590 kb	65.5 kb		Idme
4	590 kb	606 kb	16.4 kb		Crypto
5	606 kb	608 kb	294 b		Misc
6	1049 kb	11.5 mb	10.5 mb		Dkernel
7	11.5 mb	213 mb	201 mb	Ext4	dfs
8	213 mb	230 mb	16.8 mb	Ext4	Efs
9	230 mb	238 mb	8389 kb		recovery
10	238 mb	246 mb	8389 kb		boot
11	246 mb	1175 mb	929 mb		system
12	1175 mb	1857 mb	682 mb	Ext4	cache
13	1857 mb	15.6 gb	13.8 gb	Ext4	userdata

device to log into his/her Amazon Account, after getting the access the user performs several activities which were as follows:

- Downloaded the book "Siddhartha by Herman Hesse" and read 10 %, then we downloaded book "SQL Server Forensic Analysis", placed a bookmark at 72 % and added several annotations.
- Downloaded and listened to some Music Albums from Amazon MP3.
- Accessed Amazon audio book service Audible.
- Accessed email from built-in email application. Several emails with attachments were accessed.
- Took a picture using the device's camera.
- Browsed slashdot.org > pcpro.com and zu.ac.ae > abpoutzu in a different tab.zu.ac.ae tab was left open.
- Installed and logged into recommended "Skype Kindle Fire Edition" app. Initiated a few videos and text chat sessions with some contacts.

After performing these activities the Amazon Kindle Fire HD device was imaged using the developed acquisition methods. The acquired image was studied and analyzed to identify the possible sources of evidence.

4.1 Acquired Data

The array of information provided by a device such as Amazon Kindle Fire HD can provide the investigator with valuable evidence. To study any device the first step was to identify the device structure in order to understand and analyze the possible sources of evidence see Table 1.

All application data is stored in the data directory of "userdata" partition, which is mounted at "/data". Every application has a directory with a unique identifier, which

itself has the following sub-directories 'files', 'database', 'shared_prefs' and 'cache'. With exception of few cases most database files are stored in the database sub - directory of application data.

All user data (Documents, Books etc.) are stored on media directory of the "userdata" partition. The media directory is mounted as "/sdcard" using a fuse virtual file-system. This virtual file-system is also made available to the PC when the device is connected via a USB cable for data transfer.

Along with that all system apps, the Kindle Fire HD has a database file "cmsapi.db" with table "sync_hashes" that indicates the cloudsync status of the applications. Cloudsync status indicates that the device syncs to Amazon cloud servers either to store data or make use of the computational resources provided by the cloud.

Photos taken by the device can be recovered from "data/media/Pictures" in the "userdata' partition. The photo taken in the case study was found in that directory.

In the case of browsing history, all the browsing history from our case study was recovered from the device. History was stored in the data directory "com.amazon. cloud9" specifically in the pages table of the browser.db database file (see Fig. 2). All open tabs were stored in tabs table of browser.db (see Fig. 3). Page thumbnails and preview images were stored in the files directory of the application data with a unique id (see Fig. 4).

Table: pages

	i	title	url	visits	visited_on	boo	thumbnail	touch_icon_url
1	1	Amaz	http://www.amazon.com/			1	content://com.an	
2	2	Googl	http://www.google.com/			0	content://com.an	
3	3	Faceb	http://www.facebook.com/			0	content://com.an	
4	4	Yahoc	http://www.yahoo.com/			0	content://com.an	
5	5	Wikip	http://www.wikipedia.org/			0	content://com.an	
6	6	YouTu	http://youtube.com/			0	content://com.an	
7	7	Slash	http://slashdot.org/	1	1360621813547	0	content://com.an	http://slashdot.org/
8	8	Zaye	http://www.zu.ac.ae/main/en/	1	1360621822723	0	content://com.an	http://www.zu.ac.a
9	9	Can y	http://www.pcpro.co.uk/features,	1	1360621839759	0	content://com.an	
10	10	Abou	http://www.zu.ac.ae/main/en/exp	1	1360621861355	0	content://com.an	http://www.zu.ac.a

Fig. 2. com.amazon.cloud9/browser.db – pages Table contains browsing History on Amazon Kindle Fire HD

Table: tabs

	i	app	url	positio	selected	hist	is_home	title
1	1			0	0		1	
2	3		http://www.zu.ac.ae/main/en/exp	1	1	1	0	

Fig. 3. com.amazon.cloud9/browser.db – tab Table list open tabs

Another valuable source of potential evidence may relate to Kindle Books. The Kindle ebook library data was recovered from the "com.amazon.kindle" data directory. Library information was stored in the "KindleContent" table of the "kindle_library.db"

database file; while Books themselves were stored in "/sdcard/Books/{id}" (see Fig. 5). The current position of the book was from the information recovered regarding the ebooks along with all annotation data that were recovered from "annotations.db" (see Fig. 6).

The music player history may also provide information for certain investigations. Analyzing the Amazon Kindle Fire HD structure showed that Music player history was stored in the recent table of "NowPlaying.db" database file in the "com.amazon.mp3" data directory. The history was stored with a unique id and a timestamp. Along with Music player history streaming music cache was also recovered with the metadata of cache being stored in the "PlaybackStreamCache.db" database file. This information is valuable in an investigation as it can provide a source for profiling the user behavior and habits.

Other applications such as Skype left traces on the device. These traces included all Skype contacts, text chats and video chats, and were recovered from the "com.skype.raider" data directory.

All relevant information to an investigation were being stored in the "main.db" database file in "files/{screenname}" sub-directory. Some chat excerpts were also recovered from "files/chatsync" and its sub-directories (see Fig. 7).

Kindle Fire HD uses a standard Android 4 email application; email messages sent or accessed on the device were located in the "com.android.email" data directory as expected. These Email messages were being stored in the "EmailProvider.db" database file in the databases sub-directory (see Fig. 8), while Attachments were cached in the databases/1.db_att directory.

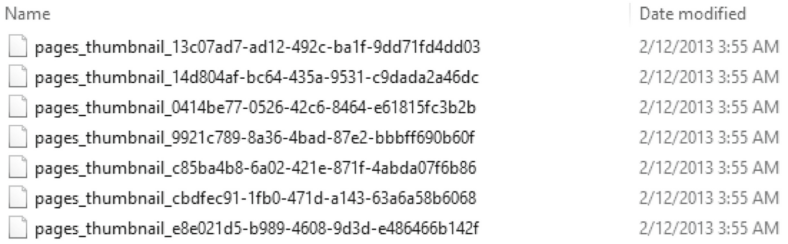
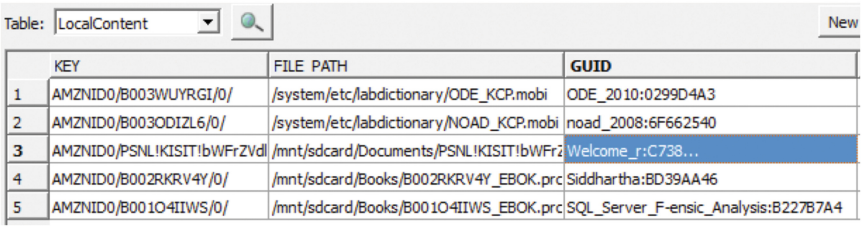


Fig. 4. com.amazon.cloude9/files - Page thumbnails and preview images stored in files directory of the application data with a unique id



	KEY	FILE_PATH	GUID
1	AMZNID0/B003WUYRGI/0/	/system/etc/labdictionary/ODE_KCP.mobi	ODE_2010:0299D4A3
2	AMZNID0/B003ODIZL6/0/	/system/etc/labdictionary/NOAD_KCP.mobi	noad_2008:6F662540
3	AMZNID0/PSNL!KISIT!bWFrZVdl	/mnt/sdcard/Documents/PSNL!KISIT!bWFr	Welcome_r:C738…
4	AMZNID0/B002RKRV4Y/0/	/mnt/sdcard/Books/B002RKRV4Y_EBOK.prc	Siddhartha:BD39AA46
5	AMZNID0/B001O4IIWS/0/	/mnt/sdcard/Books/B001O4IIWS_EBOK.prc	SQL_Server_F-ensic_Analysis:B227B7A4

Fig. 5. Books stored in "/sdcard/Books/{id}"

Table: Annotations

New Record | Delete Record

	USERID	BOOKID	TYPE	START_P	END_POS	USER_TEXT
1	amzn1.account.AHF	AMZNID0/B002RKR\	0	28293	28293	
2	amzn1.account.AHF	AMZNID0/B001O4II'	0	130848	130848	illustrates the structure of a
3	amzn1.account.AHF	AMZNID0/B001O4II'	0	124005	124005	• MSDB: Holder of a
4	amzn1.account.AHF	AMZNID0/B001O4II'	0	121855	121855	processing requirements or database users
5	amzn1.account.AHF	AMZNID0/B001O4II'	0	116399	116399	Server in upcoming chapters, you
6	amzn1.account.AHF	AMZNID0/B001O4II'	0	106582	106582	User Mode Scheduler An integrated
7	amzn1.account.AHF	AMZNID0/B001O4II'	0	38944	38944	firsthand how databases insert, delete,
8	amzn1.account.AHF	AMZNID0/B001O4II'	0	24286	24286	Preface During a forensic investigation,
9	amzn1.account.AHF	AMZNID0/B001O4II'	0	1163590	1163590	

Fig. 6. Annotation data that were recovered from "annotations.db"

Name	Object	Type	Schema
Videos	table		CREATE TABLE Videos (id I...
SMSes	table		CREATE TABLE SMSes (id I...
CallMembers	table		CREATE TABLE CallMember...
ChatMembers	table		CREATE TABLE ChatMemb...
Alerts	table		CREATE TABLE Alerts (id I...
Conversations	table		CREATE TABLE Conversati...
Participants	table		CREATE TABLE Participants...
VideoMessages	table		CREATE TABLE VideoMessa...
LegacyMessages	table		CREATE TABLE LegacyMes...
Calls	table		CREATE TABLE Calls (id IN...
Accounts	table		CREATE TABLE Accounts (i...
Transfers	table		CREATE TABLE Transfers (i...
Voicemails	table		CREATE TABLE Voicemails (i...
Chats	table		CREATE TABLE Chats (id I...
Messages	table		CREATE TABLE Messages (i...
ContactGroups	table		CREATE TABLE ContactGro...
sqlite_autoindex_DbMeta_1	index		
IX_Contacts_skypename	index		CREATE INDEX IX_Contact...

Fig. 7. main.db/files/chatsync - Some chat excerpts recovered from files/chatsync and its sub-directories

Name	Object	Schema
android_metadata	table	CREATE TABLE android_metadata (locale TEXT)
Message	table	CREATE TABLE Message (_id integer primary key autoincrement, sy...
QuickResponse	table	CREATE TABLE QuickResponse (_id integer primary key autoincrem...
sqlite_sequence	table	CREATE TABLE sqlite_sequence(name,seq)
Message_Updates	table	CREATE TABLE Message_Updates (_id integer unique, syncServerI...
Message_Deletes	table	CREATE TABLE Message_Deletes (_id integer unique, syncServerId...
Attachment	table	CREATE TABLE Attachment (_id integer primary key autoincrement,...
Mailbox	table	CREATE TABLE Mailbox (_id integer primary key autoincrement, dis...
HostAuth	table	CREATE TABLE HostAuth (_id integer primary key autoincrement, p...
Account	table	CREATE TABLE Account (_id integer primary key autoincrement, dis...
Policy	table	CREATE TABLE Policy (_id integer primary key autoincrement, pass...
sqlite_autoindex_Message_Updates_1	index	
sqlite_autoindex_Message_Deletes_1	index	
message_timeStamp	index	CREATE INDEX message_timeStamp on Message (timeStamp)
message_flagRead	index	CREATE INDEX message_flagRead on Message (flagRead)
message_flagLoaded	index	CREATE INDEX message_flagLoaded on Message (flagLoaded)
message_mailboxKey	index	CREATE INDEX message_mailboxKey on Message (mailboxKey)
message_syncServerId	index	CREATE INDEX message_syncServerId on Message (syncServerId)
attachment_messageKey	index	CREATE INDEX attachment_messageKey on Attachment (message...
mailbox_serverId	index	CREATE INDEX mailbox_serverId on Mailbox (serverId)
mailbox_accountKey	index	CREATE INDEX mailbox_accountKey on Mailbox (accountKey)

Fig. 8. com.android.email/EmailProvider.db/databases - Email messages were being stored in "EmailProvider.db" database file in databases sub-directory

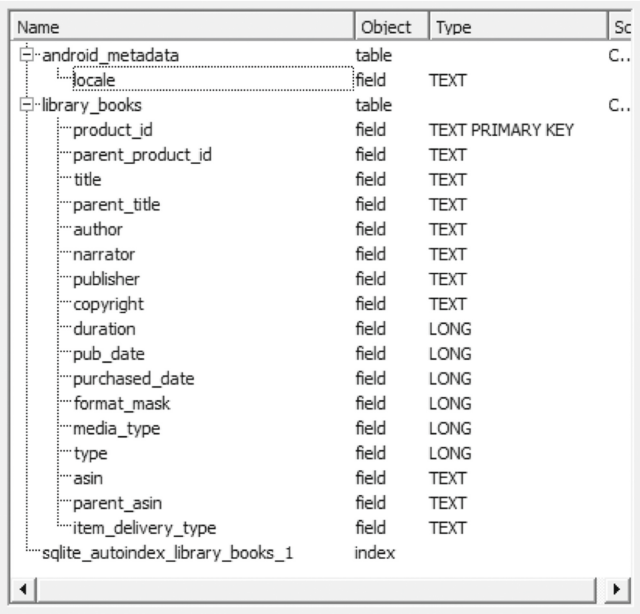


Fig. 9. com.audible.application.kindle/library.db - library_books table contains Audio book library

In addition to the discussed sources of evidence, Audible which is an amazon service for audio books that is integrated into Kindle Fire HD device may be relevant information to an investigation. Analyzing the image of the Amazon Kindle Fire HD identified that audio book library was stored in the "library.db" database file of the "com.audible.application.kindle" data directory in the table "library_books" see Fig. 9.

5 Conclusion and Future Work

The concept of mobility has transformed the computing technology market. With the introduction of devices such as the iPod, iPhone and later the iPad the tablet market continues to grow. Amazon Kindle Fire HD is a tablet with similar features to the iPad, and has been introduced to the market at a competitive price point, with an ecosystem for multimedia and ebook distribution provided by Amazon comparable to Apple's iTunes platform. The differences between the Amazon Kindle Fire HD and other Android-based tablets make it worthy of particular attention.

This research described the digital forensic acquisition and analysis of the Amazon Kindle Fire HD device. The paper presents two developed methods of acquisition, one requiring a special cable to reflash the boot partition of the device with a forensic acquisition environment, and the other exploiting a vulnerability in the device's Android operating system. After acquisition, the investigation of the system resulted in the identification of the system structure as well as the possible artifacts that could be used in a course of an investigation.

To the best of our knowledge, this is the first scientific paper discussing digital investigations of Amazon Kindle Fire HD devices. Our contributions are two techniques for physical acquisition (one of which, methodology A, we clearly prefer) of these devices, and a "road map" of storage locations on the device of key digital evidence items which may prove a useful starting point for digital forensic examiners.

This research targeted the acquisition and analysis of data on Amazon Kindle Fire HD, but still there is a lot of room for improvement and research. One of the possible areas is to explore third party applications and the artifacts left by them on the device. With devices such as Amazon Kindle Fire HD and iPads the door is open for research as they represent a move from the traditional computing era to the mobile computing era. There are many other areas of future work within the broader field of Android device forensics, such as live memory acquisition without the need for rooting the device, which will also have direct applicability to the Amazon Kindle Fire HD device.

References

1. Marturana, F., Me, G., Berte, R., Tacconi, S.: A quantitative approach to triaging in mobile forensics. In: 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 582–588, 16–18 November 2011
2. Mobile Security And Forensics. NIST, 23 February 2009, Cited: 1, 19, 2013. http://csrc.nist.gov/groups/SNS/mobile_security/index.html
3. Zdziarski, J.: iPhone Forensics: Recovering Evidence. Personal Data and Corporate Assets, s.l. O'Reilly (2008)
4. Bader, M., Baggili, I.: iPhone 3GS forensics: Logical analysis using apple iTunes backup utility. Small Scale Digital Device Forensics J. **4**(1) (2010)
5. Husain, M.I., Baggili, I., Sridhar, R.: A Simple Cost-Effective Framework for iPhone Forensic Analysis. In: Baggili, I. (ed.) ICDF2C 2010. LNICST, vol. 53, pp. 27–37. Springer, Heidelberg (2011)
6. Iqbal, B., Iqbal, A., Al Obaidli, H.: A novel method of iDevice(iPhone,iPad,iPod) forensics without jailbreaking. In: International Conference on Innovations in Information Technology (IIT), pp. 238–243, Abu Dhabi, Al Ain. IEEE (2012). doi:10.1109/INNOVATIONS.2012.6207740
7. Hoog, A.: Android forensics: investigation, analysis and mobile security for Google Android. Syngress (2011)
8. Vidas, T., Zhang, C., Christin, N.: Toward a general collection methodology for Android devices. Digital Invest. **8**, S14–S24 (2011). doi:10.1016/j.diin.2011.05.003
9. Allyn S.: Amazon kindle forensics. A Safe Blog, 9 June 2011, Cited: 1, 19, 2013. www.blog.asafewebsite.com/2011/06/amazon-kindle-forensics.html
10. Thompson, M.: Introduction to kindle forensics. Practical Digital Forensics. 5 September 2011, Cited: 1, 19, 2013. http://practicaldigitalforensics.blogspot.com/2011/09/introduction-to-kindle-forensics.html
11. Eric H.: A cursory look at kindle forensics. In: A Fistful of Dongles. 13 April 2010, Cited: 1, 19, 2013. www.ericjhuber.com/2010/04/cursory-look-at-kindle-forensics.html
12. Kindle 3G Wireless Reading Device - forensically speaking. Computer Forensics and IR - what's new? 3 October 2010, Cited: 1, 19, 2013. newinforensics.blogspot.com/2010/10/kindle-3g-wireless-reading-device.html

13. Forensic Imaging of the Amazon Kindle. MacForensicsLab, Cited: 1, 19, 2013. http://www.macforensicslab.com/ProductsAndServices/index.php?main_page=document_general_info&cPath=5_18&products_id=338&zeni%ED%AF%80%ED%B2%AB
14. Hannay, P., Kindle forensics: Acquisition and analysis. In: Proceedings of the ADFSL 2011 Conference on Digital Forensics, Security and Law (2011)
15. Iqbal, B., Iqbal, A., Guimaraes, M., Khan, K., Al Obaidli, H.: Amazon kindle fire from a digital forensics perspective. In: 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 323–329, 10–12 October 2012. doi:10.1109/CyberC.2012.61
16. Oxygen Forensic Suite 2012 Adds Support for Amazon Kindle Fire HD, PRweb, 23 October 2012, Cited: 1, 19, 2013. http://www.prweb.com/releases/kindle-fire-hd/forensic-tools/prweb10040657.htm50442462&pf_rd_i=B005890
17. qemu automated root, exploit, Cited: 14, 5, 2013. http://forum.xda-developers.com/showthread.php?t=1893838
18. Android Debug Bridge, Developer Android. Cited: 14, 5, 2013. http://developer.android.com/tools/help/adb.html
19. Sylve, J., Case, A., Marziale, L., Richard, G.G.: Acquisition and analysis of volatile memory from android devices. Digital Invest. **8**(3–4), 175–184 (2012). doi:10.1016/j.diin.2011.10.003
20. Lessard, J., Kessler, G.C.: Android forensics: simplifying cell phone examinations. In: Small Scale Digital Device Forensics J. **4**(1) September 2010