KINDLE FORENSICS: ACQUISITION & ANALYSIS

Peter Hannay
SECAU
School of Computer and Security Science
Edith Cowan University
Perth, Australia
p.hannay@ecu.edu.au

Abstract

The Amazon Kindle eBook reader supports a wide range of capabilities beyond reading books. This functionality includes an inbuilt cellular data connection known as Whispernet. The Kindle provides web browsing, an application framework, eBook delivery and other services over this connection. The historic data left by user interaction with this device may be of forensic interest. Analysis of the Amazon Kindle device has resulted in a method to reliably extract and interpret data from these devices in a forensically complete manner.

Keywords: forensics, digital forensics, kindle, mobile, embedded, ebook, ereader

1. INTRODUCTION

The Amazon Kindle eBook reader provides significant functionality aside from that of simply reading eBooks. As the Kindle is an embedded computing platform it is possible to deploy a wide range of functionality due to the use of general computing hardware (see Table 1 for details). The Kindle platform has grown to include a web browser, which utilizes an inbuilt cellular data connection, an application framework, music player, image viewer, AGPS and numerous other capabilities. The presence of this functionality leads to a situation where the ability to provide forensic analysis of these devices would be quite desirable due to the potential for nefarious use of such features.

Table 1 - Comparison of Kindle Hardware (Amazon, 2010)

Kindle Specifications					
	Kindle	Kindle 2	Kindle DX	Kindle DX 2	Kindle 3
CPU	Freescale 532 MHz, ARM-11	Freescale 532 MHz, ARM-11	Freescale 532 MHz, ARM-11	Freescale 532 MHz, ARM-11	Freescale 532 MHz, ARM-11
Flash	256MB	2GB	4GB	4GB	4GB
Comms	Cellular/3G	Cellular/3G	Cellular/3G	Cellular/3G + WiFi	Cellular/3G and/or WiFi
Kernel	Linux-2.6.26	Linux-2.6.26	Linux-2.6.26	Linux-2.6.26	Linux-2.6.26

The 2GB of flash storage is divided into four file systems (see figure 1), the last of these is mapped to act as a USB mass storage device and is the only file system that can be accessed, viewed or in any other way interacted with when the kindle is in its secure state. The other three partitions contain the root Linux file system, configuration files and a debug file system respectively.

```
$ fdisk kindle.img
Disk: kindle    geometry: 995/64/63 [4014080 sectors]
Signature: 0xAA55
         Starting       Ending
 #: id  cyl  hd sec -  cyl  hd sec [     start -       size]
------------------------------------------------------------------------
*1: 83    0   1   1 - 1023   3  16 [        16 -     819248] Linux files*
 2: 83 1023   3  16 - 1023   3  16 [    819264 -      49152] Linux files*
 3: 83 1023   3  16 - 1023   3  16 [    868416 -      16384] Linux files*
 4: 0B 1023   3  16 - 1023   3  16 [    884800 -    3129280] Win95 FAT-32
```

Figure 1 - Partition Structure of the Kindle

Existing digital forensics software packages have implemented limited support for Kindle devices, however there are is currently no support for examination of the flash memory other than the FAT32 partition (MacForensicsLab, 2010). In the same vein research has been performed by a number of individuals in an attempt to derive forensic methodology for the Kindle, however this research has also only focused on the FAT32 partition exposed as a USB mass storage device (Huber, 2010b; Hughes, 2010; newinforensics, 2010).

2. SECURITY

The Kindle utilizes a firmware update mechanism that allows for over the air (OTA) or manual updates. In the case of both the update file is placed in the root of the mass storage portion of the file system. The update is then applied once the user activates this functionality from the system menu of the device.

The update files themselves are essentially signed TAR archives, these are extracted and a shell script contained within executed to facilitate the update functionality. The signing mechanism relies on RSA encryption in which the update is signed with amazon's private key and verified with amazon's public key, which is pre-installed on the Kindle device (Hannay, 2010).

The security functionality can however be defeated as the tar archive is extracted prior to signature verification. The most commonly employed exploit to leverage this involves setting the absolute path to the public key store in the tar archive, as such prior to signature validation a new public key is added to the store. The result of this exploit is that the ability to sign arbitrary updates is gained. The jailbreak process described here is illustrated below in Figure 2.

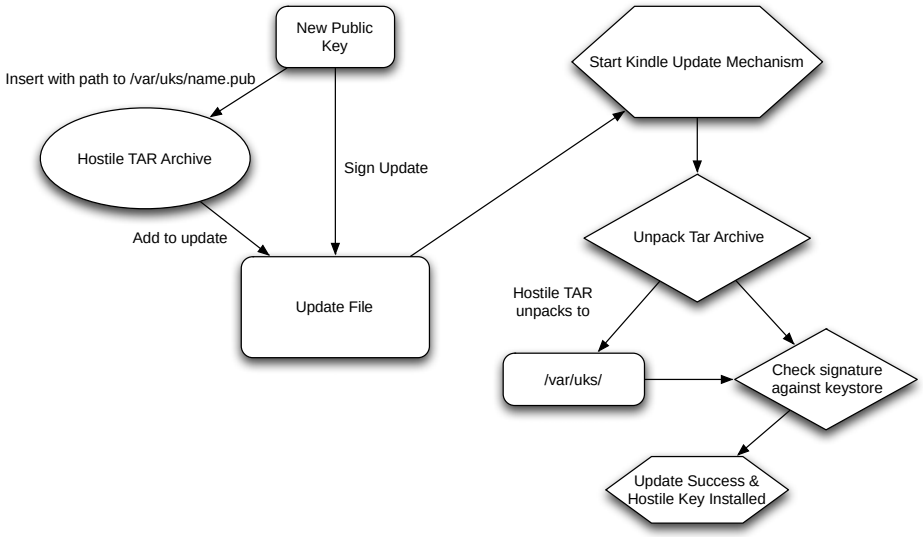

Figure 2 - Illustration of Jailbreak Process

3. ACQUISITION METHODOLOGY

Prior to commencement of this section it is important to note that knowledge of best practice in terms of hashing, evidence preservation and documentation are assumed and as such are out of scope of this paper. The investigator should ensure that he/she understands the impact that writing data to a device can have and the implications on forensic integrity.

In order to accomplish the acquisition and analysis of the Kindle we must first gain access to the device beyond what is available by default. This access is achieved through use of the exploit identified in the previous section, the implementation we will be using in this example is the Kindle Jailbreak (based on AVNard's earlier work), this utility includes a standard public/private key pair which is known publicly as well as an installation framework (NiLuJe, 2010). At this stage in the process we now have the ability to install custom software via the update system.

In order to gain complete access to the device it is necessary to install some form of remote access software on the device. In our case a telnet & SSH server will be installed along side scripts which allow for the USB port to be remapped as a USB Ethernet Gadget. The package commonly used to achieve this is the "USBNetwork" package, so named as it restores the USB networking functionality that was originally present in early versions of the Kindle firmware (NiLuJe, 2010). Once this has been accomplished it is possible to establish to start the USBNetwork service by issuing the ";debugOn" and "`usbNetwork" commands on the device (without quotes) as

shown in Figure 3.

Figure 3 - The ";debugOn" command being issued

Once the USBNetworking package is installed and enabled it is possible to start acquisition. This is accomplished through the use of telnet, dd and netcat, this methodology has been commonly implemented in live system acquisitions (Burdach, 2005). In this configuration the host system is configured to listen for the data transmission, piping the output to dd. Then a telnet connection is established to the kindle and data transfer initiated, this process is shown in Figure 4 below.

```
1. Connect to kindle
$ telnet 192.168.2.2
Trying 192.168.2.2...
Connected to 192.168.2.2.
Escape character is '^]'.
 [root@kindle root]#

2. Listen for connection on host sytem
$ nc -l 55555 | dd of=kindle.img
3185454+1385484 records in
4014080+0 records out
2055208960 bytes transferred in 915.234125 secs (2245555 bytes/sec)

3. Initiate transfer of data from kindle
[root@kindle /dev]# dd if=/dev/mmcblk0 | nc 192.168.2.1 55555
4014080+0 records in
4014080+0 records out
```

Figure 4 - Acquiring image of NAND memory

Once this acquisition is complete it may be desirable to split this file into the four file systems that are contained within. The details of these can be extracted using fdisk as shown in Figure 1. Once these partition boundaries are known we can extract the individual partitions into their own files for subsequent analysis as shown in Figure 5.

```
$ dd if=kindle.img of=kindlep1.img skip=16 count=819248
819248+0 records in
819248+0 records out
419454976 bytes transferred in 23.742699 secs (17666693 bytes/sec)
$ dd if=kindle.img of=kindlep2.img skip=819264 count=49152
49152+0 records in
49152+0 records out
25165824 bytes transferred in 1.661936 secs (15142477 bytes/sec)
$ dd if=kindle.img of=kindlep3.img skip=868416 count=16384
16384+0 records in
16384+0 records out
8388608 bytes transferred in 0.315741 secs (26568018 bytes/sec)
$ dd if=kindle.img of=kindlep4.img skip=884800 count=3129280
3129280+0 records in
3129280+0 records out
1602191360 bytes transferred in 141.444850 secs (11327322 bytes/sec)
```

Figure 5 - Splitting disk image into individual partition images

The completion of this splitting leads us to the point where these images can be analysed using traditional computer forensics methodologies. The next section includes information on the various file systems and location of data that has been deemed to be of forensic interest.

4. DATA OF INTEREST

Partition 1 (root file system)

Location	Description
/opt/wan/firmware/mt-3/version.dat	Firmware version indicator
/opt/amazon/ebook/config/	Configuration files
/opt/amazon/ebook/prefs/	Preferences files
/etc/uks/	Public key store, keys other amazon's and the key created during jailbreak may indicate tampering

Partition 2 (/var/local)

Location	Description
/audio/	Audio settings
/eink/screen_saver_last	The a reference to the last screen saver image displayed
/java/prefs/cookies	Cookies used to uniquely identify this device to amazon. These are persistent.
/java/prefs/DevicePasswordData.pw	Password data for this device
/java/prefs/browser/bookmarks	Web browser bookmarks
/java/prefs/browser/cookie.dat	Web browser cookies (no cache is present, this may provide limited historical evidence of web access
/java/prefs/browser/settings	Web browser configuration
/java/prefs/com.amazon.ebook.booklet.reader/social-clipping/social-prefs	Credentials and accounts associated with social networking services (twitter, facebook, etc) that have been set up for use with the device
/java/prefs/com.amazon.ebook.framework	User settings including: country, timezone & WAN status
/java/prefs	Details of the user, kindle name & user name
/log/	Detailed logs of users interaction with the device, including time stamps
/wan/	Network configuration

Partition 4 (User file system – available via USB mass storage)

Location	Description
/documents	Books and other publications for consumption on device
/music	Music and other audio for consumption on device
/system/Search Indexes/	History of each search conducted on the device
/system/com.amazon.ebook.booklet.reader/reader.pref	Contains details of last book read, font size selected and dictionary currently in use.

Note: On all test systems partition 3 was zero filled. Based on investigation it has been determined that this area is used for diagnostic purposes and likely will not contain information outside of the development environment.

5. CONCLUSION

eBook devices such as the Kindle are gathering increased interest from the forensic community as they become increasingly popular. The included cellular data capability of the Kindle specifically may make it a candidate for nefarious purposes, as the there is no data cost associated with the global data service (Hannay, 2010). In addition to data functionality the inclusion of an application framework and development kit in beta release will only lead to increased use of the product for purposes that were once met by the traditional computing paradigm.

The initial efforts of the forensic community have focused on acquisition of only a portion of the internal storage of the device as this area is readily accessible as a USB mass storage device (Huber, 2010a, 2010b; Hughes, 2010; MacForensicsLab, 2010; newinforensics, 2010). This paper has gone beyond the existing methodologies and provided a mechanism for the acquisition of the complete internal NAND memory and analysis of same. In order for this result to be achieved however some data must be written to the device and in doing so there is the possibility of data being overwritten. However aside from invasive hardware based acquisition there are no current known techniques that would allow for complete acquisition without this approach.

Research into small and embedded device forensics is ongoing, with increased focus on complete acquisition of all relevant data from these systems, including flash storage, memory and data stored on individual microcontrollers.

6. REFERENCES

Amazon. (2010). Kindle Wireless Reading Device, Wi-Fi, Graphite, 6" Display with New E Ink Pearl Technology. Retrieved January 7th, 2011, from http://www.amazon.com/gp/product/B002Y27P3M?ie=UTF8&tag=10inchlaptop-20&linkCode=as2&camp=1789&creative=390957&creativeASIN=B002Y27P3M

Burdach, M. (2005). Digital forensics of the physical memory. *Warsaw University*.

Hannay, P. (2010). Hooray for Reading: Hacking the Kindle. Retrieved January 3rd, 2011, from http://openduck.com/2010/11/27/hooray-for-reading-hacking-the-kindle/

Huber, E. (2010a). Additional Thoughts on Kindle Forensics Retrieved January 19th, 2011, from http://ericjhuber.blogspot.com/2010/04/additional-thoughts-on-kindle-forensics.html

Huber, E. (2010b). A Cursory Look at Kindle Forensics. Retrieved January

19th, 2011, from http://ericjhuber.blogspot.com/2010/04/cursory-look-at-kindle-forensics.html

Hughes, A. (2010). Forensics Beyond the Hard Drive: Kindle 2 Logging. Retrieved Febuary 6th, 2011, from http://inforensics.vidocrazor.com/2009/06/26/forensics-beyond-the-hard-drive-kindle-2-logging/

MacForensicsLab. (2010). Forensic Imaging of the Amazon Kindle. Retrieved January 12th, 2011, from http://www.macforensicslab.com/ProductsAndServices/index.php?main_page=document_general_info&cPath=5_18&products_id=338&zenid=be461f672b245e5f78e3800158c920e5

newinforensics. (2010). Kindle 3G Wireless Reading Device - forensically speaking. Retrieved January 9th, 2011, from http://newinforensics.blogspot.com/2010/10/kindle-3g-wireless-reading-device.html

NiLuJe. (2010). Fonts & ScreenSavers hacks for Kindles Retrieved Janurary 2nd, 2011, from http://www.mobileread.com/forums/showthread.php?t=88004