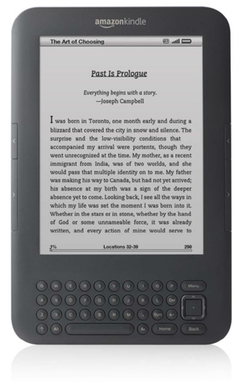
CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Amazon Kindle Forensics

Marcus Thompson



Abstract

The Amazon Kindle is becoming an increasingly popular e-book reader. This examination of the Kindle Keyboard is important for law enforcement investigators who have seized a Kindle; however, documented forensic acquisition methods for the Kindle do not exist. This research explores possible forensic processes including privilege escalation and documents locations of items of interest for investigations.

Significance

Jeff Bezos, the founder, president, CEO and chairman of the board of Amazon.com, reports that the Kindle is the bestselling, most wished for, and most gifted product on Amazon.com. A user can use the Kindle to play music, play games, browse the web, and store about three gigabytes of data, and not necessarily e-books. It supports conversion for many file extensions , and can store any other file much like a flash drive. Currently, the Kindle Development Kit (KDK) is in beta testing to allow users to develop their own active content, such as games, calendars, or photo galleries . As features are added, to make life more convenient for its users, some decide to use these conveniences to further their criminal trade craft. Books and other files contained can be considered associative evidence, which can give insight to a suspect, victim, or person of interest or can help build a case in conjunction with other evidence. The Kindle can contain more 3500 books, hundreds of .mp3 songs, or other files. It will give an investigator a large picture of an active user.

Method

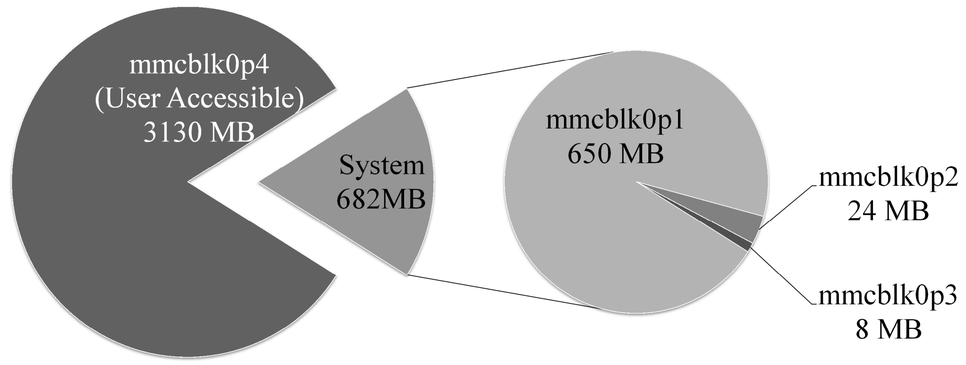
For this research a Kindle Keyboard was populated with various types of files a typical user may introduce using several methods:

- wireless download purchases
- wireless download of archived content
- content transfer from a computer host via USB
- downloading documents through Amazon's Kindle Personal Document Service

The Kindle was imaged with AccessData's Forensic ToolKit and compared with images of the same Kindle after several common user file deletion methods to determine evidence recoverability:

- hardware deletion
- Amazon.com deletion
- set to factory defaults

Kindle Partitions



Kindle Content at a Glance

Content	Location
Current Location in Last Book Read	Kindle-FAT32\system\userannotlog
Device Email Address	mmblk0p2\LocalVars-ext3\java\prefs\reginfo
Downloaded Books	Kindle-FAT32\documents\<title>-asin_<Amazon Standard Identification Number>-type_EBOK-v_0.azw
Firmware Version	Kindle-FAT32\Update_<previous version>-<current version>.bin
Kindle Time	Kindle-FAT32\system\com.amazon.ebook.booklet.reader\reader.pref
Screenshots	Kindle-FAT32\documents\screen_shot-<number>.gif
Serial Number	Kindle-FAT32\system\AudibleActivation.sys
User Highlights and Notes	Kindle-FAT32\documents\My Clippings.txt

Selected References

Amazon Kindle User's Guide. Retrieved from http://kindle.s3.amazonaws.com/Kindle_User's_Guide_English.pdf.

Kindle Wireless Reading Device, Wi-Fi, Graphite, 6" Display with New E Ink Pearl Technology. (n.d.). Retrieved from http://www.amazon.com/dp/B002Y27P3M/ref=btech_kindle_wifi

Marsico, C., Rogers, M. (2005). iPod forensics. *International Journal of Digital Evidence*. *4* (2).

Discovery Park e-Enterprise Center