Forensic Analysis of Dropbox® Application File Artifacts Recovered on Android and iOS Mobile Devices

Treleven Sara, BS[1], Christopher Vance, BS[1], Terry Fenger, PhD[1],
Josh Brunty, MS[1], Jenniffer Price[2]

[1]Department of Forensic Science, Marshall University
[2]Wisconsin Department of Justice

Abstract

Forensic examination of smartphone mobile devices is hindered not only by the amount of information stored on the device itself, but also the location of the application files used on different operating systems. Dropbox® was installed on a 4th generation Apple iPod Touch running iOS 5.1.1 and an Android smartphone emulator running Android 2.3.3 to examine the file structure layout and data organization of the application files. Physical dumps of both file systems were done and analyses took place using Physical Analyzer version 3.0 and FTK version 4.0.2.33. File structures of both operating systems were very similar; however more user data was able to be recovered from the iOS device. Possessing a better understanding of file structures from this application on different operating systems can help investigators and analysts in future work, as well as possibly expediting present casework. Future studies should be conducted to confirm that files recovered from the Android emulator are identical to files recovered from an actual Android smartphone.

Introduction

It comes as no surprise that smartphone sales are continuously on the rise in the United States. Of the world's almost five billion mobile phones in use, 1.08 billion are smartphones and

approximately 100 million of these smartphones are present in the United States alone (Pew 2012). This number continues to increase as current feature phone users decide to make the jump to smartphones and prices of smartphones themselves decrease. Smartphone users have recently become more prevalent within the overall population than owners of more basic mobile phones by 13% (Pew 2012). Smartphones are becoming increasingly popular not only with middle aged adults, which holds the majority (72%) of the market, but also younger children and older adults. 13% of adults over the age of 65, 31% of 14-17 year olds, and 8% of 12-13 year olds now own smartphones as well (Pew 2012). As of May 2011, the average number of apps per smartphone has jumped 28 percent, from 32 apps to 41 (PC Mag 2011). Not only are smartphone owners downloading more apps, but they are spending about ten percent more time than last year on the mobile web (Digital Buzz 2011).

With greater advancements in technology come more evidence to be collected at a scene. Where collection of a single PC would have been sufficient in the past, now evidence collection includes multiple desktops, laptops, cell phones, USB devices, SD cards, microSD cards, cameras, gaming systems, GPS devices, and more. In regards to digital evidence, most information relates to that found on cell phones, especially smartphones, since they are hand-held and can hold enormous amounts of potentially useful information.

While the majority of activities done on mobile devices are innocuous, criminals now have an added advantage than in the past. Illegal pictures and videos can be taken and distributed within seconds, kept on hand at all times, and stored in vast amounts on inconspicuous storage devices that are easily concealed. The advent of file sharing applications available for mobile devices has made the information stored using the app more accessible with each device synched to the user's account. However, with the development and exponential

growth of so many smartphone applications come complexities when dealing with forensic analyses in criminal cases. Increasingly, organizations encounter data that cannot be analyzed with today's tools because of format incompatibilities, encryption, or simply a lack of training (Garfinkel 2010). The location of the stored files also plays a role in forensic analysis as the cloud becomes a larger storage medium than an actual physical hard drive. Applications of forensic interest include apps that allow the synching and sharing of files, images, and videos that may have suspected illegal activity associated. These crimes can include financial and business account records, documents and images related to drug offenses and homicides, as well as images and videos relating to child pornography. Many of these applications are available through Apple iOS mobile devices using the App Store and on Android mobile devices using Android Marketplace.

Android is currently the most popular operating system, accounting for 48.6% of all smartphones while Apple's iOS is the second most popular with 29.5% of the market (Phonedog 2012). For this reason these two operating systems were used for research purposes to examine the file locations of the Dropbox® application.

Android OS

Android is a Linux-based operating system for mobile devices such as smartphones and tablet computers. Android, Inc. was developed in California in 2003 and was then acquired by Google in 2005, making Android, Inc. a subsidiary of Google, Inc. At the time of writing, Android is still owned by Google, Inc. under the Open Handset Alliance which develops open standards for mobile devices (Android, Wiki 2012). The first version of Android written was "Astro," and has been updated frequently. Each proceeding version has been named alphabetically after a dessert, starting with 1.5 "Cupcake." 2.3 "Gingerbread" and 3.0

"Honeycomb" have followed, with 4.0 "Ice Cream Sandwich" being the most used version as of October 19, 2011. 4.0 "Jelly Bean" is the most recent version that debuted in July 2012 on the Nexus 7 tablet. While research done in this paper is on an Android smartphone emulator, the Android operating system is also used on laptops, netbooks, smartbooks, e-readers, tablets, and smart TVs. Even though using an emulator looks identical to an actual Android smartphone, it cannot be assumed that all virtual machine file systems will be identical to that of the actual smartphone (Bem 2007). Android applications are usually developed in the Java language using the Android Software Development Kit and can be purchased from Google Play or the Amazon Appstore. As of October 2011, there were more than 500,000 apps available for Android and the operating system itself was installed on over 130 million total devices. There are currently six manufacturers — Dell, HTC, Kyocera, LG, Motorola, and Samsung — making 42 smartphones using the Android operating system (Android, Wiki 2012).

iOS

iOS is a mobile operating system developed and distributed by Apple, Inc. that is Unix based and derived from OS X. It was originally released in 2007 for the iPhone and iPod Touch, and is now extended to the iPad and Apple TV (OS X, Wiki 2012). Originally, the operating system went unnamed with devices stating "iPhone runs OS X." In October 2007, a Software Development Kit (SDK) was developed and with it came Apple's first named operating system: "iPhone OS." Versions that followed were: iPhone OS 2.0, OS 3.0, iOS 4.0, and the current iOS 5.0 which supports all iPad models, iPhone 3GS, iPhone 4 and iPhone 4S (GSM and CDMA), and the iPod Touch 3rd and 4th generation. Applications can be acquired through Apple's App Store which contains more than 550,000 iOS applications (OS X, Wiki 2012).

Dropbox® File Sharing Application

Dropbox® was founded in 2007 and is a file sharing service operated by Dropbox®, Inc. Dropbox® provides cloud storage, file synchronization, and client software (Dropbox, Wiki 2012). Client software is provided for Microsoft, Windows, Mac OS X, Linux, Android, iOS, Blackberry OS, and web browsers. Dropbox® was started by two MIT graduates who frequently misplaced or had forgotten their USB devices and originally planned on developing Dropbox® for their own personal use. However, as of October 2011, Dropbox® has over 50 million users worldwide storing over 20 billion files and occupying petabytes of storage (Dropbox, Wiki 2012).

Dropbox® allows users to place their files or folders inside the Dropbox® folder where they can be viewed on any device as long as the device has Dropbox® installed along with a username and password. Files placed in the Dropbox® folder can be found on mobile devices and any other device that allows downloading of applications and each user is given two gigabytes of free storage, with the option of buying up to one terabyte of storage space. Dropbox® offers storing files in the standard Dropbox® folder, a "Photos" folder, a "Public" folder, or a "Shared" folder. Other Dropbox® users must be invited and accept the Dropbox® Shared folder request to access and edit files. A public link is created on files inside the 'Public' folder where items can be downloaded, but are read-only.

By default, Dropbox® saves all deleted and earlier versions of files for thirty days; a feature that is supported with a free Dropbox® account. A paid monthly subscription to Dropbox® also offers an additional add-on called "Packrat," a feature that saves all files indefinitely.

Dropbox® uses Amazon's S3 (Simple Storage Service) storage system to store the files and SSL transfers for synchronization. An AES-256 encryption is used to ensure privacy of

data. Almost 33% of Dropbox® users are from the United States, making up the largest share. Sixty-six percent of Dropbox® users primarily use Windows® while 20.9% use Macs only. (Dropbox, Wiki 2012).

Until recently, Dropbox® has claimed that a user's files are actually safer in a Dropbox® account than when stored on a local drive, stating "We use the same secure methods as banks and the military to send and store your data...Nobody can see your private files in Dropbox® unless you deliberately invite them or put them in your Public folder" (Beta News 2012). Since then, Dropbox® Terms of Service have changed be in compliance with the US legal procedures and allow law enforcement access to a private Dropbox® account when warranted (Beta News 2012).

With the Dropbox® application, it is likely that the same file will be synched to multiple devices collected at a scene. This research is prudent because the location of questionable documents, files, videos, etc. is needed to convict or exonerate the suspect in question, in as little time as possible. Having a clear knowledge of what information can be found on the device as well as what will most likely be excluded would not only expedite current casework, but would also assist in decreasing backlog in digital laboratories. Mobile forensics usually requires procedures that are very specific to the device manufacturer and/or model for both collection and analysis since each mobile device has unique software, memory layouts, and storage techniques (Vidas et al. 2011). Certain forensic software may be more beneficial in acquiring needed information from the device than other software, so knowing what to expect when dealing with a certain application's data is not only helpful in analysis but is also more time efficient.

Materials and Methods

Dropbox® Standard Research Folder

A 2012 MacBook Pro laptop running OS X Mountain Lion was used to download Dropbox® application version 1.4.7 from the iTunes App Store and given an account name (misde.ethan@me.com) specific to research purposes only. A standard folder was created on the MacBook Pro that included a set of .JPG images, one uploaded video, two Microsoft Word documents, and one Microsoft Word Excel document. The shared folder, in this case renamed to "untitled folder," was created that allowed specific images to be shared publicly with other email addresses linked to Dropbox® accounts. In addition, two .JPG images were put into the folder labeled "Public." One of the Microsoft Word documents was downloaded, opened and viewed, and then intentionally deleted from the Dropbox® account. All of the .JPG images, the undeleted Microsoft Word document, and the Microsoft Excel document had the word "sloth" associated with them. This was done with intentions of facilitating searches of Dropbox® images and documents. The goal of the folder organization was to analyze the files using forensic software to see if public and shared folders could be distinguished, and more importantly, to see if the shared email addresses could be recovered. Recovery of deleted data on mobile devices is always an area of interest, making the ability to recover the deleted document from the standard folder a high priority as well. This standard folder was then synched to the iPod Touch and to the Android emulator so that the files on each were identical.

Apple iPod Touch

An Apple 4th Generation 32GB iPod Touch running iOS version 5.1.1 was purchased and used for research purposes only. Being the most recent version at the time of analysis, Dropbox® version 1.5.7 for iOS was downloaded and installed using the research account name misde.ethan@me.com. Dropbox® offers automatic synching of images taken with the iPod Touch to the associated Dropbox® account, which was manually disabled. By default, iTunes is configured to synchronize automatically with a device when connected via USB. This was also disabled to prevent back and forth exchange between laptop and iPod Touch. All attempts at producing a forensically controlled environment were taken. During research analysis, the laptop and iPod Touch were removed from the wireless network to keep a forensically sound environment by preventing possible cross contamination to evidence.

Android Emulator

A virtual machine was created on the MacBook Pro laptop, emulating an Android smartphone. Eclipse was downloaded onto the MacBook Pro, a software development environment written in Java and a basis for creating applications. Eclipse has an IDE, or Integrated Development Environment, used to develop applications in Java or by using different plug-ins. The appropriate plug-in, ADT or Android Developer Tools was then downloaded. This provided a collection of tools that were integrated with the Eclipse IDE.

The SDK, or Software Development Kit, was downloaded from the Android Developer website. The Android SDK included a mobile device emulator, a virtual mobile device capable of running on a computer. This emulator lets a user develop and test Android applications

without actually having a physical phone in hand and also provides documentation and utilities that can assist in the forensic analysis of a device.

Next, by using the Android Virtual Device (AVD) manager, a choice of different Android platforms was given to install and run. Version 2.3.3 (Gingerbread) and all of the necessary components to create a working emulator were installed with an API (application programming interface) level 10. Version 2.3.3 was chosen over newer versions including 3.0 (Ice Cream Sandwich) and 4.0 (Jelly Bean) because at the time of writing it was the most commonly run version of the Android operating system on mobile devices. As of July 2012, version 2.3.3 was present on 64% of Android smartphones (Android Developers 2012).

With the Android SDK and the necessary platform, an AVD (Android Virtual Device), or emulator, was created which ran on the Apple MacBook Pro. The Android emulator was created from developer.android.com/ and ran a full Android system stack, down to the kernel level, including the basic level of preinstalled applications found on a newly purchased Android smartphone. The AVD was fully functional and allowed the user to surf the web, set up email accounts, and even send text messages to other AVDs or to other mobile devices. A 2 GB virtual SD card was also created to store application data downloaded on the Android emulator.

Next, Dropbox® was installed and synched with the research account. The Amazon.com AppStore was downloaded and used to install the Dropbox® application. This was then synched with the research account so that the Dropbox® files on the iPod Touch and the Dropbox® files on the Android emulator were completely identical to each other. Dropbox® version 2.1.2 for Android was used and Dropbox® version 1.5.7 for iOS was used, as they were the most recent versions at the time of analysis.

Data Extraction

The iPod Touch was put into DFU (Device Firmware Upgrade) to bypass the operating system, making sure that data would not be overwritten on the device and a physical dump was done using Cellebrite's Physical Analyzer version 3.0. These files were then analyzed using both Physical Analyzer as well as FTK (Forensic Toolkit) version 4.0.2.33. Starting with iOS 4, Apple introduced a hardware-based encryption of user data, so Elcomsoft Phone Password Breaker software was downloaded from elcomsoft.com/download.html and the iOS image file was decrypted. This decrypted image file was then used analyzed with FTK.

Once the standard Dropbox® folder was synched to the Android emulator, these files needed to be extracted from the MacBook Pro laptop. This was accomplished by using the SDK push/pull feature. There were three folders found under the file explorer tab: "data," "mnt," and "system." The Dropbox® stored user data was found within the subfolder "sdcard" of the "mnt" main folder. These files were transferred using the "pull" feature on Eclipse to move the virtual SD card data files to the research USB drive to be forensically analyzed with Physical Analyzer and FTK.

Results

iOS Dropbox® Analysis Using Physical Analyzer

After the iPod Touch was put into DFU mode and a physical extraction was performed, files were analyzed using Physical Analyzer version 3.0. The Extraction Summary revealed important initial information. Under "Device Info" was a tab named "Sync Data" where the Sync Host Name was labeled as "AlsoMISDE's MacBook Pro." This was the device synched

with the research iPod Touch. The last sync was also shown with a date and time stamp, along with the iPod Touch being synched to "Computer: AlsoMISDE's MacBook Pro\User: AlsoMISDE." This can be pertinent information to an investigation with multiple users. Applications downloaded to the device are named by their SHA-1 value, in this case Dropbox® is referred to as "3FA61474-D20E-445B-8D3F-8EF67E18E815."

Following the path *File Systems/HFS/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E18E815* four folders were examined for Dropbox® application artifacts. These folders were: "Documents," "Dropbox.app," "Library," and "tmp." Under *File Systems/HFS /Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E18E815/Documents* were three databases: "Dropbox.sqlite," "Persist_DBUniqueID," and "Uploads.sqlite."

Data/mobile Applications/3FA61474-D20E-445B-8D3F-8EF67E18E815/Documents

Dropbox.sqlite Database

A full list of data stored on the Apple iPod Touch's Dropbox® application was found at *File Systems/HFS/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E18E815/Documents/Dropbox.sqlite*, including the deleted Microsoft Word document file "Data Archiving Plan." However, there was no notification that the file had been deleted. A view count, size, revision, and the last view date are also associated with each file. Located under the "ZPATH" column, the exact location of files as they are stored on the Dropbox® application locally on the iPod Touch is shown. For example, "photo-2.JPG" was stored in the Public folder in Dropbox® on the iPod Touch. When observed under the "ZPATH" column of Physical Analyzer, it is shown as "/Public/photo-2.JPG." However, the Shared

Dropbox folder, in this case named “untitled folder,” shows no indication of being shared. The .JPG stored in the Shared folder is found under the “ZPATH” column as “/untitled folder/Photo Jun 24, 10 54 43.jpg.”

Uploads.sqlite Database

A video (.MOV) that had been taken with the Apple iPod Touch device and uploaded to the Dropbox® account was found in this database following the path *File Systems/HFS/Data/ mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E18E815/Documents/Uploads.sqlite.* Also noted in the database view were the file size, date added, date created, date uploaded, video type, and full path. The full path, under “ZPATH,” was shown as */Video Jun 26, 10 04 26 AM (1).mov.* The video did not show any association to the Dropbox® account, but only that it had been uploaded using the iPod Touch device.

Persist_DBUniqueId Database

In this database was a unique identifier specific to the Dropbox® application; however there was no apparent forensic significance and no further examinations were done.

Data/mobile Applications/3FA61474-D20E-445B-8D3F-8EF67E18E815/Dropbox.app

The Dropbox.app did not seem to possess any forensic significance. This folder mainly stored data specific to the Dropbox® application itself, but nothing related to the user or to stored data on the application.

Data/mobile Applications/3FA61474-D20E-445B-8D3F-8EF67E18E815/Library

The Library folder has four subfolders that were examined: “Caches,” “Cookies,” “Preferences,” and “WebKit.” The subfolder “Caches” showed an area of forensic significance. Following the path *Data/mobile Applications/3FA61474-D20E-445B-8D3F-8EF67E18E815/Library/Caches/Dropbox,* a full list of Dropbox® stored data exactly how it was stored locally on the device itself was displayed. The deleted Microsoft Word document “Data Archiving Plan.docx” was also present. A full list of recovered items can be seen in Table 1. Associated with this deleted file are the creation, modified, and last access times, along with a file size and data offset. Each .JPG image file has two files associated with it: a smaller 150x150 “fit_one” and a larger 960x640 “bestfit.” Images of the stored Microsoft Word and Excel documents are also seen, stored as .JPGs. The Dropbox® username as well as the Dropbox® ID were also recovered. Full paths of these items can be seen in Table 2.

iOS Dropbox® Analysis Using FTK

The decrypted image made from Elcomsoft Phone Passcode breaker was put into FTK and the files were analyzed there. Dropbox® application files were stored under the path *\Data [HFS]\mobile\Applictions\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox.* The main application folder itself had four subfolders: “Documents,” “Dropbox.app,” “Library,” and “tmp.”

Data [HFS]\mobile\Applictions\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches \Dropbox\Documents

The “Documents” subfolder contained the Dropbox.sqlite database. This contained names and paths of some stored Dropbox® data, but not all downloaded data from the

application. A subfolder of the Dropbox.sqlite folder named “tables” was examined for possible significant data. Following the path *\Data [HFS]\mobile\Applictions\3FA61474-D20E-445B-8D3F-8EF67E815\Documents\Dropbox.sqlite\tables\ZCACHEDFILE*, a table was shown of 19 items stored on Dropbox®. Each item had a size, view count, last viewed date, and a path associated with it, as seen in Fig. 1. The Dropbox® “Sample Photos” in Fig. 1 were not included in the research project, as they had no forensic significance.

Data [HFS]\mobile\Applictions\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches \Dropbox\Dropbox.app

The “Dropbox.app” folder had many subfolders, but none of them housed any stored user data that was thought to be forensically significant.

Data [HFS]\mobile\Applictions\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches \Dropbox\Library

This main “Library” folder stored the most useful user data. Following the path *Data [HFS]\mobile\Applictions\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches \Dropbox\Library\Caches\Dropbox* showed a complete listing of how data was stored locally on the iPod Touch device. The folder structure can be seen in Fig. 2. All .JPGs were recoverable and had two image sizes present, a 150x150 and a 960x640. All Microsoft Word and Excel documents were recovered as well as the deleted Microsoft Word document, “Data Archiving Plan.docx.” This deleted document was able to be seen easily; however shows no evidence that the document was originally removed from Dropbox®. The video file, .MOV, was not recovered

in either the main Dropbox® folder or the Public folder. All recovered items and full paths can be seen in Table 3. The Dropbox® account username and Dropbox® ID were also recovered using FTK. This information is shown in Table 4.

Data [HFS]\mobile\Applictions\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches \Dropbox\tmp

The "tmp" folder housed a run.log that showed a listing of Dropbox® files stored on the device. It did list the deleted Microsoft Word document, "Data Archiving Plan.docx" but not the .MOV video file.

FTK Index Search Results

Running an Index Search for possible shared email address contacts did not result in any hits in allocated or unallocated space. Another search was done to find more possible locations of the user's Dropbox® ID, but no additional locations were found in allocated or unallocated space besides the ones already listed in this paper. A final search was done for ".MOV" to see if a result would show association with the .MOV file and Dropbox®. One result was shown as the video being synched to the icloud, since the video was originally taken and uploaded with the Apple iPod; however, the search result did not show any association with Dropbox®.

Android Dropbox® Analysis Using Physical Analyzer

Data found on the virtual SD card was examined with Physical Analyzer. The initial Extraction Summary showed very little useful information, only accounting for twenty images present. The images accounted for are shown in Table 5. Since there were two files saved of each image, a 960x640_bestfilt.jpg and a large.jpg, only ten of the actual files were recovered.

/sd pull/sdcard/Android/

The "sdcard" folder had two subfolders: "Android" and "LOST.DIR." All stored user data was found primarily in subfolders of the "Android" folder. A full listing of the stored user files on Dropbox® as shown on Physical Analyzer exactly as they were stored locally on the Android emulator. However, only the .JPG files were recovered. There is no indication of any Microsoft Word or Excel documents being stored on Dropbox®. Images could be found easily using the path */sd pull/sdcard/Android/data/com.dropbox.android/cache/thumbs.*

The "com.dropbox.android" folder had two subfolders: "cache" and "files." All stored data was found in the "cache" folder; however the "files" folder did have subfolders named "Photos," "Public," and "untitled folder." No actual data was found in these folders and it was thought to be a directory of the main Dropbox® folders and not house any user data. No actual Dropbox® user data was recovered, such as a Dropbox® ID or the Dropbox® user email address.

/sd pull/sdcard/LOST.DIR

The role of this directory was unclear, but thought to be a possible recovery directory for deleted data. No data was found in this folder.

Physical Analyzer Search Results

Searches were done in Physical Analyzer for the Dropbox® user ID, possible shared email addresses, and for the .MOV file. No evidence was found after conducting all three searches, as shown in Table 6.

Android Dropbox® Analysis Using FTK

The contents of the virtual SD card were analyzed using FTK version 4.0.2.33. Under the main folder labeled "sd card" were two subfolders named "Android" and "LOST.DIR." These were both analyzed in-depth for forensically significant content and the full file structure can be seen in Fig. 3. The contents of the "Android" folder were analyzed first following the path */Android/data/com.dropbox.android*. Android emulator files stored on the virtual SD card that were able to be analyzed on FTK were only .JPGs. The video was not able to be recovered, along with any Microsoft Word and Excel documents including the deleted Microsoft Word document, "Data Archiving Plan.docx." Recovered items are shown in Table 7.

/Android/data/com.dropbox.android/cache/

Within the "cache" folder were two subfolders labeled "thumbs" and "tmp." The contents of the "thumbs" folder show a full listing of Dropbox® stored data, with two images of each .JPG, a "large.jpg" and a "960x640_bestfit.jpg." The folder structure was intact as it was locally on the Android emulator, showing the main Dropbox® file structure as well as the subfolders "Photos," "Public," and the Shared folder, "untitled folder." Each individual file on FTK had a column showing Name, Item #, Extention, Path, Category, and Created, Modified, and Accessed dates and times. No data was found in the temporary, or "tmp" folder using the path */Android/data/com.dropbox.android/cache/tmp.*

The second folder present under the com.dropbox.android named "files," which was a subfolder of the "cache" folder, was also examined. The "files" folder had a subfolder, "scratch," with three subfolders within that: "Photos," "Public," and "untitled folder." The only folder of the three that had any stored data was the "Photos" folder, which housed another folder labeled "Sloths Riding Bikes." However, no data was present in this folder.

/Android/LOST.DIR/

No data was found in this folder.

FTK Index Search Results

Running an Index Search for the Dropbox® ID and possible shared email address did not result in any hits in allocated or unallocated space, as shown in Table 8. An additional search was done to find more possible locations of the .MOV file, but showed no results.

Discussion and Conclusions

The work done in this paper is a good indication of what to expect and what not to expect when forensically analyzing a Dropbox® account. Since the Dropbox® user data was not stored locally on any device, but rather in the cloud, it was initially unknown whether or not any data could be recovered using forensic software. Data analysis of each operating system was unique; however both files systems did have multiple similarities. The Dropbox® files stored on the iOS device and on the Android device both showed a similar file structure when analyzed with forensic software. Files from both devices were shown as they were stored locally on each device, and in their appropriate folders ("Photos," "Public," and "Shared"). However, the "Shared" folder was able to be renamed by the user (in this case was renamed to "untitled folder") and after analysis of both Android and iOS data, it was not obvious that data stored in this folder were associated with a shared folder. The shared folder had also been shared with the author's personal email address and the images were downloaded by the author on her own mobile device, but no record of this sharing had been found after analysis.

Much more pertinent information was recovered on the iOS device than from the Android emulator pertaining to the user itself. This may have to do with the actual iPod device being used in analysis, rather than an emulator. The stored Microsoft Word and Excel documents were fully recovered from the iPod Touch, however they were not present when the Android emulator files were analyzed. The reason why is unknown, and further testing should and will be done to find the location of these files. The iPod Touch did show a record of the deleted "Data Archiving Plan.docx" Microsoft Word document while the Android emulator did not show any indication of it being stored on Dropbox®. The .MOV video file associated with Dropbox® was also unrecoverable from either the iOS or Android files.

Using an emulator such as this is especially helpful for forensic analysts because the execution of applications on a device can be easily seen. This helps in validating findings in an investigation, or testing how a forensic tool affects an Android device (Hoog 2011). However, future studies should be conducted to confirm that Dropbox® mobile application files found on the Android emulator are identical to the Dropbox® files found on an actual Android smartphone. At the time of writing all current versions of applications were used, as well as the most used versions of iOS and Android. As technology advances, file storage will likely change and future studies should be done to ensure pertinent information is not overlooked and still recoverable. Currently, iOS presents problems with their encryption of deleted data and also with the inability to crack initial passcodes. Applications that can encrypt texts and images are becoming more and more popular, as well as remote wiping of entire devices. Problems such as this will surely add frustration and hinder forensic investigations in the future. Studies such as this are important to stay up-to-date on advancements, as criminals always seem to be one step ahead of the investigator.

References

1. Android (operating system) [Internet]. 2012. Wikipedia. [cited 2012 June 5]. Available from: http://en.wikipedia.org/wiki/Android_%28operating_system%29

2. Android Developers. 2012. [Internet]. Android. [cited 2012 June 3]. Available from: http://developer.android.com/index.html

3. Bem, D. 2007. Computer forensic analysis in a virtual environment. International Journal of Digital Evidence 6(2).

4. Beta News. [Internet]. Now Anyone, Not Just Cops With a Warrant Can Peek Inside Your Dropbox®. 2012. [cited 2012 July 24]. Available from: http://betanews.com/2011/06/16/now-anyone-not-just-cops-with-a-warrant-can-peek-inside-your-Dropbox /

5. Digital Buzz. [Internet]. Infographic: Mobile Statistics, Stats & Facts 2011. 2011. [cited 2012 July 25]. Available from: http://www.digitalbuzzblog.com/2011-mobile-statistics-stats-facts-marketing-infographic/

6. Dropbox ® (Service). [Internet]. 2012. Wikipedia. [cited 2012 June 5]. Available from: http://en.wikipedia.org/wiki/Dropbox _%28service%29

7. Garfinkel, SL. 2010. Digital forensics research: The next 10 years. Journal of Digital Investigation 7:64-73.

8. Hoog A. 2011. Android forensics: Investigation, analysis, and mobile security for Google Android. 1st Ed. Massachusetts. Syngress. p. 102-20.

9. OS X [Internet]. 2012. Wikipedia; [cited 2012 June 5]. Available from: http://en.wikipedia.org/wiki/OS_X

10. Pew Internet. [Internet]. Nearly Half of American Adults are Smartphone Owners. 2012. [cited 2012 July 23]. Available from: http://pewinternet.org/Reports/2012/Smartphone-Update-2012.aspx

11. Phonedog. [Internet]. Number of U.S. Smartphone Subscribers Surpass 100 million, Says ComScore. 2012. [cited 2012 June 25]. Available from: http://www.phonedog.com/2012/03/08/number-of-u-s-smartphone-subscribers-surpasses-100-million-says-comscore/

12. PC Mag. [Internet]. Smartphone App Downloads Jump 28 Percent 2011. [cited 2012 June 26]. Available from: http://www.pcmag.com/article2/0,2817,2404502,00.asp

13. Vidas, T., Zhang, C., and C. Nicolas. 2011. Toward a general collection methodology for Android devices. Journal of Digital Investigation 8:14-24.

Acknowledgements

The author would like to thank Christopher Vance, Dr. Terry Fenger, Dr. Pamela Staton, and Josh Brunty from the Marshall University Forensic Science Center in their guidance and instruction, as well as Special Agent in Charge Jenniffer Price, Lead Criminal Analyst Tim Lokrantz, and Criminal Analysts Mark Howard, Chris Kendrex, Florian Berger, Toby Carlson, and Christine Byars at the Department of Justice's Division of Criminal Investigation Computer Forensics Unit in Wisconsin.

Appendix

Table 1. Dropbox® iOS files analyzed with Physical Analyzer showing file name, location, and path, if recovered.

Dropbox® File Name	Folder Location	Recovered?	Path
Che_Slothera_..._by_j_a_x.jpg	Main	Yes	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Caches/Dropbox/Che_Slothera_Revolucion_by_j_a_x.jpg*
Goonies_sloth.jpg	Main	Yes	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Caches/Dropbox/goonies_sloth.jpg*
Il_570xN.29573039.jpg	Main	Yes	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Cache /Dropbox/il_570xN.29573039.jpg*
Sloth.jpg	Main	Yes	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Caches/Dropbox/sloth.jpg*

Sloth_333322_481808.jpg	Main	Yes	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Caches/Dropbox/Sloth_333322_481808.jpg*
Sloths.jpg	Main	Yes	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Cache/Dropbox/sloths.jpg*
Video Jun 26,…6AM (1).mov	Main	No	NA
Video Jun 26, …4 26 AM.mov	Shared (untitled folder)	No	NA
Photo Jun 24,… 54 43 PM.jpg	Shared (untitled folder)	Yes	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Cache/Dropbox/untitled folder/Photo Jun 24, 10 43 43 PM.jpg*
Woo Hoo Do…e Sloths.docx	Main	Yes	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Cache /Dropbox/Woo Hoo Do I Love Sloths.docx*
Workbook1.xlsx	Main	Yes	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Cache/Dropbox/Workbook 1.xlsx*
Data Archiving Plan	Main (deleted)	Yes (link only)	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Cache /Dropbox/Data Archiving Plan.docx*
Mr January.JPG	Public	Yes	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Cache/Dropbox/Public/Mr January.JPG*
Photo-2.JPG	Public	Yes	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Cache/Dropbox/Public/photo-2.JPG*
Sloths Riding Bikes IMG_5031.jpg	Photos	Yes	*/Data/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Cache/Dropbox/Photos/Sloths Riding Bikes/IMG_5031.jpg*

Table 2. Dropbox® iOS account user information recovered using Physical Analyzer.

Dropbox® Info	**Recovered?**	**Path**
User name (misde.ethan @me.com)	Yes	*Apple_iPod Touch.zip/Backup Service/var/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Preferences/com.getDropbox .Dropbox*
Dropbox® ID (83845009)	Yes	*Apple_iPod Touch.zip/Backup Service/var/mobile/Applications/3FA61474-D20E-445B-8D3F-8EF67E815/Library/Caches/LogPool /ios_iPod4,1_5.1.1_1.5.2_008BFF5B-EFD3-4C2C-BCA2-2F9F681BE291_1342535629_ANALYTICALS_83845009_2 19624249.log*
Dropbox® ID (83845009)	Yes	*System(Apple:HFS [+])/Analyzed Data/Passwords*
Shared email addresses	No	NA

rowid	Z_PK	Z_ENT	Z_OPT	ZFAVORITE	ZREVISION	ZSIZE	ZVIEWCOUNT	ZLASTVIEWEDDATE	ZENCODINGNAME	ZMIMETYPE	ZPATH
1	1	1	4	0	11	55525	3	364148795.243116	[NULL]	[NULL]	/il_570xN.29573039.jpg
2	2	1	4	0	13	52157	3	364160496.551781	[NULL]	[NULL]	/Sloth_333322_481808.jpg
3	3	1	4	0	15	49714	3	364160496.575007	[NULL]	[NULL]	/sloth.jpg
4	4	1	4	0	14	12637	3	364148795.266823	[NULL]	[NULL]	/goonies_sloth.jpg
5	5	1	4	0	12	70537	3	364160496.516544	[NULL]	[NULL]	/sloths.jpg
6	6	1	4	0	10	40340	3	364148795.215599	[NULL]	[NULL]	/Che_Slothera_Revolucion_by_j_a_x.jpg
7	7	1	2	0	8	567	1	361736309.655061	ascii	text/plain	/Photos/How to use the Photos folder.txt
8	8	1	2	0	4	339773	1	361736334.414792	[NULL]	[NULL]	/Photos/Sample Album/Boston City Flow.jpg
9	9	1	1	0	6	354633	0	361736335.960187	[NULL]	[NULL]	/Photos/Sample Album/Costa Rican Frog.jpg
10	10	1	3	0	18	27526	2	361737299.115401	[NULL]	[NULL]	/Woo Hoo Do I Love Sloths.docx
11	11	1	4	0	19	28811	3	364402208.156082	[NULL]	[NULL]	/Workbook1.xlsx
12	12	1	4	0	34	2918633	3	368641234.26122	[NULL]	[NULL]	/Photos/Sloths Riding Bikes/IMG_5031.jpg
13	13	1	3	0	29	2419275	2	364224971.795685	[NULL]	[NULL]	/Public/photo-2.JPG
15	15	1	3	0	39	46091	2	364224971.837655	[NULL]	[NULL]	/Public/Mr January.JPG
16	16	1	2	0	9	675	1	361913279.233444	ascii	text/plain	/Public/How to use the Public folder.txt
17	17	1	2	0	24	12772	1	361913312.131797	[NULL]	[NULL]	/Data Archiving Plan.docx
18	18	1	4	0	41	94152	3	362678522.63128	[NULL]	[NULL]	/Photo Jun 24, 10 54 43 PM.jpg
19	19	1	2	0	1	94152	1	362678541.927289	[NULL]	[NULL]	/untitled folder/Photo Jun 24, 10 54 43 PM.jpg

Figure 1. ZCACHEDFILE listing of iOS Dropbox® files analyzed with FTK.

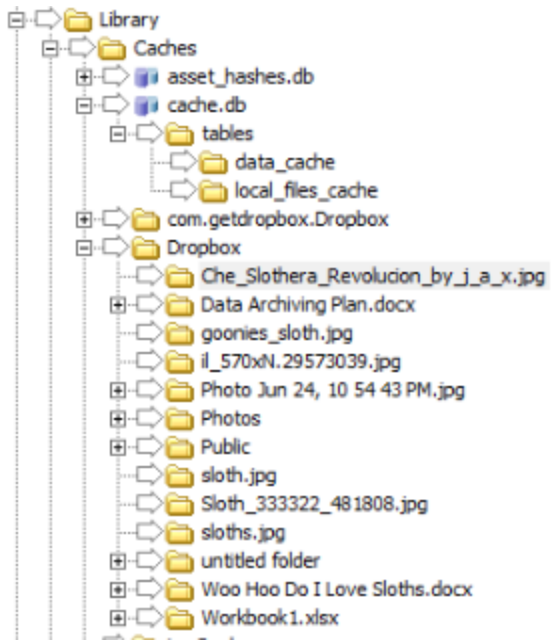

Figure 2. Dropbox® iOS file structure using FTK analysis.

Table 3. Dropbox® iOS files analyzed with FTK showing file name, location, and path, if recovered.

Dropbox® File Name	Folder Location	Full Recovery?	Path
Che_Slothera_..._by_j_a_x.jpg	Main	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\Che_Slothera_Revolucion_by_j_a_x.jpg*
Goonies_sloth.jpg	Main	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\goonies_sloth.jpg*
Il_570xN.29573039.jpg	Main	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\Il_570xN.29573039.jpg*
Sloth.jpg	Main	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\sloth.jpg*

Sloth_333322_481808.jpg	Main	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\Sloth_333322_481808.jpg*
Sloths.jpg	Main	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\sloths.jpg*
Video Jun 26,…6AM (1).mov	Main	No	NA
Video Jun 26, …4 26 AM.mov	Shared (untitled folder)	No	NA
Photo Jun 24,… 54 43 PM.jpg	Shared (untitled folder)	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\Photo Jun 24, 10 54 43PM.jpg*
Woo Hoo Do…e Sloths.docx	Main	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\Woo Hoo Do I Love Sloths.docx*
Workbook1.xlsx	Main	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\Workbook1.xlsx*
Data Archiving Plan	Main (deleted)	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\Data Archiving Plan.docx*
Mr January.JPG	Public	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\Public\Mr January.JPG*
Photo-2.JPG	Public	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\Public\photo-2.JPG*
Sloths Riding Bikes IMG_5031.jpg	Photos	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\Dropbox\Photos\Sloths Riding Bikes\IMG_5031.jpg*

Table 4. Dropbox® iOS account user information recovered using FTK

Dropbox® Info	Recovered?	Path
User name (misde.ethan @me.com)	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Preferences \com.getdropbox.Dropbox.plist*
Dropbox® ID (83845009)	Yes	*\Data\[HFS]\mobile\Applications\3FA61474-D20E-445B-8D3F-8EF67E815\Library\Caches\LogPool*
Shared email addresses	No	NA

Table 5. Dropbox® Android files analyzed with Physical Analyzer showing file name, location, and path, if recovered.

Dropbox® File Name	Folder Location	Recovered?	Path
Che_Slothera_..._by_j_a_x.jpg	Main	Yes	*/sd pull/sdcard/Android/data /com.dropbox.android/cache/thumbs/Che_Slothera_Revolucion_by_j_a_x.jpg*
Goonies_sloth.jpg	Main	Yes	*/sd pull/sdcard/Android/data /com.dropbox.android/cache/thumbs/goonies_sloth.jpg*
Il_570xN.29573039.jpg	Main	Yes	*/sd pull/sdcard/Android/data /com.dropbox.android/cache/thumbs/ Il_570xN.29573039.jpg*
Sloth.jpg	Main	Yes	*/sd pull/sdcard/Android/data /com.dropbox.android/cache/thumbs/sloth.jpg*
Sloth_333322_481808.jpg	Main	Yes	*/sd pull/sdcard/Android/data /com.dropbox.android/cache/thumbs/Sloth_333322_481808.jpg*
Sloths.jpg	Main	Yes	*/sd pull/sdcard/Android/data /com.dropbox.android/cache/thumbs/goonies_sloth.jpg*

Video Jun 26,…6AM (1).mov	Main	No	NA
Video Jun 26, …4 26 AM.mov	Shared (untitled folder)	No	NA
Photo Jun 24,… 54 43 PM.jpg	Shared (untitled folder)	Yes	*/sd pull/sdcard/Android/data /com.dropbox.android/cache/thumbs/untitled folder/Photo Jun 24, 10 54 43PM.jpg*
Woo Hoo Do…e Sloths.docx	Main	No	NA
Workbook1.xlsx	Main	No	NA
Data Archiving Plan	Main (deleted)	No	NA
Mr January.JPG	Public	Yes	*/sd pull/sdcard/Android/data /com.dropbox.android/cache/thumbs/Public/Mr January.jpg*
Photo-2.JPG	Public	Yes	*/sd pull/sdcard/Android/data /com.dropbox.android/cache/thumbs/Public/Photo-2.jpg*
Sloths Riding Bikes IMG_5031.jpg	Photos	Yes	*/sd pull/sdcard/Android/data /com.dropbox.android/cache/thumbs/Photos/Sloths Riding Bikes IMG_5031.jpg*

Table 6. Dropbox® Android account user information recovered using Physical Analyzer

Dropbox® Info	**Recovered?**	**Path**
User name (misde.ethan @me.com)	No	NA
Dropbox® ID (83845009)	No	NA
Shared email addresses	No	NA

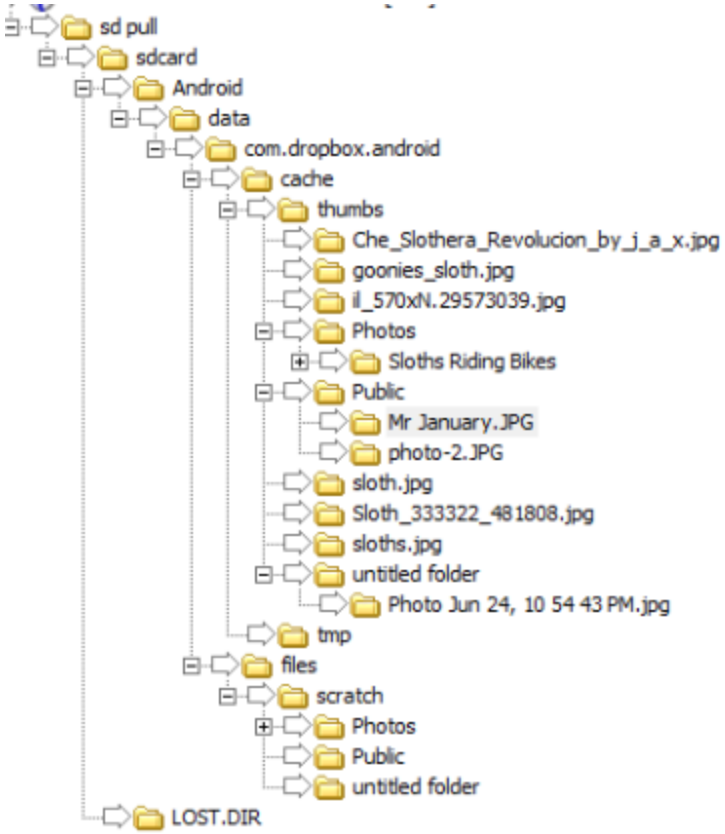

Figure 3. Android Dropbox® file structure using FTK analysis.

Table 7. Dropbox® Android files analyzed with FTK showing file name, location, and path, if recovered.

Dropbox® File Name	Folder Location	Recovered?	Path
Che_Slothera_..._by_j_a_x.jpg	Main	Yes	*/Android/data/com.dropbox.android/cache/thumbs/Che_Slothera_Revolucion_by_j_a_x.jpg*
Goonies_sloth.jpg	Main	Yes	*/Android/data/com.dropbox.android/cache/thumbs/goonies_sloth.jpg*
Il_570xN.29573039.jpg	Main	Yes	*/Android/data/com.dropbox.android/cache/thumbs/il_570xN.29573039.jpg*

Sloth.jpg	Main	Yes	*/Android/data/com.dropbox.android/cache/thumbs/Che_Slothera_Revolucion_by_j_a_x.jpg*
Sloth_333322_481808.jpg	Main	Yes	*/Android/data/com.dropbox.android/cache/thumbs/sloth_333322_481808.jpg*
Sloths.jpg	Main	Yes	*/Android/data/com.dropbox.android/cache/thumbs/sloths.jpg*
Video Jun 26,…6AM (1).mov	Main	No	NA
Video Jun 26, …4 26 AM.mov	Shared (untitled folder)	No	NA
Photo Jun 24,… 54 43 PM.jpg	Shared (untitled folder)	Yes	*/Android/data/com.dropbox.android/cache/thumbs/untitled folder/Photo Jun 24, 10 54 43PM.jpg*
Woo Hoo Do…e Sloths.docx	Main	No	NA
Workbook1.xlsx	Main	No	NA
Data Archiving Plan	Main (deleted)	No	NA
Mr January.JPG	Public	Yes	*/Android/data/com.dropbox.android/cache/thumbs/Public/Mr January.JPG*
Photo-2.JPG	Public	Yes	*/Android/data/com.dropbox.android/cache/thumbs/Public/photo-2.JPG*
Sloths Riding Bikes IMG_5031.jpg	Photos	Yes	*/Android/data/com.dropbox.android/cache/thumbs/Photos/Sloths Riding Bikes/IMG_5031.jpg*

Table 8. Dropbox® Android account user information recovered using FTK

Dropbox® Info	**Recovered?**	**Path**
User name (misde.ethan @me.com)	No	NA
Dropbox® ID (83845009)	No	NA
Shared email addresses	No	NA