

2014-03-31

## Cloud-Based Storage Applications for Smart Phones: Forensic Investigation of Cloud Storage Applications

Radoslaw Ochrymowicz  
*Technological University Dublin*

Follow this and additional works at: <https://arrow.tudublin.ie/scschcomdis>



Part of the [Computer Engineering Commons](#)

---

### Recommended Citation

Ochrymowicz, R. Cloud-based storage applications for smart phones: Forensic investigation of cloud storage applications. Submitted in partial fulfilment of the requirements of Technological University Dublin for the degree of M.Sc. in Computing (Information Technology) May 2014. DOI: 10.21427/c9p6-xh08

This Dissertation is brought to you for free and open access by the School of Computer Science at ARROW@TU Dublin. It has been accepted for inclusion in Dissertations by an authorized administrator of ARROW@TU Dublin. For more information, please contact [arrow.admin@tudublin.ie](mailto:arrow.admin@tudublin.ie), [aisling.coyne@tudublin.ie](mailto:aisling.coyne@tudublin.ie), [vera.kilshaw@tudublin.ie](mailto:vera.kilshaw@tudublin.ie).

# **Cloud-based storage applications for smart phones: Forensic investigation of cloud storage applications**

**Radoslaw Ochrymowicz**

A dissertation submitted in partial fulfilment of the requirements of  
Dublin Institute of Technology for the degree of  
M.Sc. in Computing (Information Technology)

**May 2014**

I certify that this dissertation which I now submit for examination for the award of MSc in Computing (Information Technology), is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

This dissertation was prepared according to the regulations for postgraduate study of the Dublin Institute of Technology and has not been submitted in whole or part for an award in any other Institute or University.

The work reported on in this dissertation conforms to the principles and requirements of the Institute's guidelines for ethics in research.

***Signed:*** \_\_\_\_\_

***Date:***                    ***20 May 2014***

## **ABSTRACT**

The proliferation of smart phones across the globe, development of 4G network standards and its progressing implementation along with shift towards cloud computing bring risks to smart phone users who avail of these service. Security of cloud storage mobile applications should be essential to smart phone users. Enterprises' move to huge data centres and availing of their infrastructure, platform and service is an advantage but poses a risk. Users use corporate resources managed and administered with security in mind of policy makers but it is still possible to use unsecure, designed for users services without business being aware of it.

This research aims to analyse concerns of data storage providers and services they provide on smart phone devices in the form of mobile cloud applications. The investigation of data stored on smart phones upon simulation of real life test case scenarios will be undertaken. Data recovered from smart phones using mobile cloud applications using forensic tools will be examined for any artefacts that may lead to the discovery of any security vulnerabilities. This will lead to the formulation of conclusions.

Recommendations for future research and work as well as suggestions for users and cloud storage vendors will supplement this study in order to increase security of data used by smart phone users and their mobile devices as gateways to gain access to this data.

**Key words:** *cloud storage, mobile application, security, forensics software*

## **ACKNOWLEDGEMENTS**

I would like to express my sincere thanks to the following people.

Brian Keegan – my supervisor, for his patience, provision of valuable feedback and support throughout my work on this project.

Alan Claffey – Vodafone, for supply of smart phones that I used for testing purposes as well as insight to mobile networks.

Sylwia Ochrymowicz – my wife, for her patience, support throughout my work on the project and the time that we both sacrificed.

Martin Choluj – my friend, for his determination and ambition that he infected me with and thanks to him I went back to college for the second time.

Max and Adam – my sons, for being there for me.

## TABLE OF CONTENTS

ABSTRACT .....	ii
TABLE OF CONTENTS .....	iv
TABLE OF FIGURES .....	viii
TABLE OF TABLES.....	ix
1. Introduction.....	10
1.1 Research problem.....	10
1.2 Introduction.....	11
1.3 Background .....	12
1.4 Intellectual challenge .....	12
1.5 Research objectives.....	13
1.6 Research methodology.....	13
1.7 Resources .....	13
1.8 Scope and limitations .....	14
1.9 Organisation of the dissertation .....	14
2 Security of cloud storage providers .....	16
2.1 Introduction.....	16
2.2 Dropbox .....	19
2.2.1 Security of Dropbox service .....	20
2.2.2 Dropbox user interfaces .....	23
2.2.3 Dropbox security breaches .....	23
2.3 Box.....	25
2.3.1 Security of Box service.....	25
2.4 SugarSync .....	27
2.4.1 Security of SugarSync service .....	27
2.5 Conclusion .....	29

3	iPhone Operating System .....	30
3.1	Introduction.....	30
3.2	Apple’s iOS.....	32
3.2.1	History of iPhone Operating System .....	32
3.2.2	Operating System.....	37
3.2.3	File System and memory .....	37
3.2.4	Security of iOS .....	38
3.2.4.1	System Security .....	39
3.2.4.2	Encryption and Data Protection .....	40
3.2.4.3	Application Security .....	41
3.2.4.4	Network Security .....	42
3.2.4.5	Internet Services.....	43
3.2.4.6	Device Controls .....	44
3.3	Conclusion .....	44
4	Forensic software.....	46
4.1	Introduction.....	46
4.2	Classification of Forensic Tools .....	46
4.2.1	Manual Extraction .....	47
4.2.2	Logical Extraction .....	47
4.2.3	Physical Extraction .....	48
4.2.4	Chip-Off Extraction.....	49
4.2.5	Microread.....	49
4.3	BlackLight.....	50
4.3.1	BlackLight features.....	50
4.4	EnCase Forensic.....	52
4.4.1	EnCase Forensic features.....	52
4.5	Oxygen Forensic Suite .....	53

4.5.1	Oxygen Forensic Suite Standard Edition features .....	53
4.5.2	Oxygen Forensic Suite Analyst Edition features .....	54
4.6	Conclusion .....	57
5	Literature Review .....	58
5.1	Introduction.....	58
5.2	Mobile Cloud Computing .....	58
5.3	Conclusion .....	60
6	Experimentation & Evaluation .....	61
6.1	Introduction.....	61
6.2	Forensic Software Installation .....	62
6.2.1	BlackLight forensic software installation .....	62
6.2.2	EnCase Forensic software installation.....	62
6.2.3	Oxygen Forensic software Standard Edition installation .....	63
6.3	Experimentation.....	64
6.3.1	Data Set.....	64
6.3.2	Transactions on files .....	64
6.3.3	Smart phone device state .....	65
6.3.4	Tests expectations.....	66
6.3.5	Analysis of database files for individual cloud storage applications.....	67
6.3.6	Hardware and software .....	67
6.4	Test Outcomes .....	68
6.4.1	iOS Applications.....	68
6.4.1.1	Dropbox .....	69
6.4.1.2	Box.....	70
6.4.1.3	SugarSync .....	71
6.4.2	iOS Test Outcomes .....	72
6.4.3	Box follow up tests on iPhone.....	74



6.5	Conclusion .....	78
7	Conclusion .....	79
7.1	Introduction.....	79
7.2	Research Definition & Research Overview .....	79
7.3	Contributions to the Body of Knowledge .....	80
7.4	Experimentation, Evaluation and Limitation .....	80
7.5	Future Work & Research .....	81
7.6	Conclusion .....	82
	BIBLIOGRAPHY .....	83
	APPENDIX A .....	91
	APPENDIX B .....	93
	APPENDIX C .....	96
	APPENDIX D .....	99

## TABLE OF FIGURES

Figure 2.1 Global spending forecast on cloud computing.....	17
Figure 2.2 Increase in outsourcing of IT systems to the cloud.....	18
Figure 2.3 Current and planned use of IaaS/PaaS in industry.....	18
Figure 2.4 Dropbox Architecture.....	22
Figure 2.5 Security audit page for Dropbox user.....	24
Figure 2.6 Box infrastructure.....	26
Figure 2.7 Simplified SugarSync architecture.....	28
Figure 3.1 Security architecture of iOS.....	39
Figure 4.1 Forensic analysis tools classification.....	37
Figure 6.1 Script to download files from Box cloud storage.....	68

## TABLE OF TABLES

Table 3.1 Smartphone Sales to End Users by Operating System, 4Q 2008.....	31
Table 3.2 Smartphone Sales to End Users by Vendor, 4Q 2008.....	31
Table 3.3 Top Five Smartphone Operating Systems, Shipments and Market Share, 2013.....	32
Table 6.1 File names and file transactions.....	65
Table 6.2 Smartphone features.....	67
Table 6.3 Cloud storage mobile and PC client versions.....	68
Table 6.4 Forensic software tools and versions.....	68
Table 6.5 Results off file recovery for iPhone device.....	74

# 1. INTRODUCTION

Very often smart phones users, regardless if they are corporate users or consumers, do not consider the important issues concerning security of their devices. In majority, they are focused on usability of their device and applications installed on them. They are not aware of terms and conditions of applications they use, mostly by their own choice, as well as how these applications operate in the background, which for non-technical users may prove to be cumbersome. Users are not concerned if they actually own data they upload to the cloud storage , where exactly it is stored, how secure it is, what details the provider of an application is collecting to name a few.

## *1.1 Research problem*

Global rapid growth of smart phone users (Statista, 2014) which has seen growth from 40 million smart phone user globally in first quarter of 2009 to nearly 250 million users in third quarter 2013 along with proliferation of cloud storage services (Gartner, 2013) which allow user to store data elsewhere rather than on their devices brings up a challenges and concerns. Providers must guarantee data integrity and availability at all times. On the other hand users need to be aware of the cost of data usage and most importantly how secure their data is.

All cloud storage providers have security measures in place in their environment whether servers are hosted by them or third party data centres. However, how secure are mobile applications and data related to operation of these applications on users' mobile devices. If cloud storage data is not properly secured this may lead to an individual accessing the data and potentially compromising users' cloud storage.

The aim of this dissertation is to evaluate security implications of using Dropbox, Box and SugarSync cloud-based storage applications on smart phones running Apple's iOS and Android operating system.

## ***1.2 Introduction***

On 29<sup>th</sup> June 2007 the first iPhone was released (Apple, 2007). The phone was able to run third party applications based on Web 2.0 framework. Over a year later on 11<sup>th</sup> July 2008 iPhone 3G was released that allowed users to connect with internet over mobile phone connections (Apple, 2008). iPhone 3G came preloaded with App Store. This is when the revolution in mobile phones started and changed the design, interface and users' interaction with mobile devices irrevocably. iPhone has not been the first touchscreen device or the device that was able to run application that comes with operating system (Buxton, 2014). However, it was the first device with revolutionary touch interface and its own application store. This framework triggered a huge increase in development of the third party applications on the iPhone. By March 2008 Apple's software development kit (SDK) has been downloaded 100,000 times and three months later the number of SDK downloads reached 250,000. In April 2009 there were 100,000 applications available on App Store. Within next few years these numbers increased algorithmically. On 22 October 2013 Tim Cook informed that there were over 1,000,000 applications available on the App store with over 60 billion downloads since the App store has been made available to users.

Similarly to Apple's path, Android platform has been developed and made 3<sup>rd</sup> party applications available to users. First branded smart phone with Android operating system was launched on 24 January 2008 (Ricker, 2008). It was HTC Dream. Since then, market share of Android Operating System (OS) based devices has been increasing to become the world's most popular smart phone operating system (IDC, 2014). Android operating system in comparison to Apple's Operating System (iOS) is open source software and a number of manufacturers release their smart phones with Android OS such as HTC, LG, Samsung or Sony. Smart phones became personal mobile computers through which information and resources can be accessed on the go at any given moment and anywhere.

The other aspect along with proliferation of smart phone devices is cloud computing, in particular cloud storage services. Providers like Dropbox, Box, SugarSync, Google or Microsoft to name a few allow consumers to use their servers to store data with assurance of data availability, integrity and back-up functionality. Initially service

provided to consumers, it expanded to corporate users in the same shape and format as for consumers. Now, there are options for businesses to set up business accounts with premium service and support on them. These services find their way on to smart phones and tackle the storage limitation of devices. Provide back-up of data and allow to instantly sharing content. All of this seems to bring benefits to consumers and business users alike.

### ***1.3 Background***

Software development kits are available for both platforms and virtually any one can develop an application. Developers need to adhere to guidelines available on Android and Apple developer websites (Apple Developer, 2014; Android Developer, 2014). This is where issues may arise. Security and a proper vetting process of third party applications is a serious problem. The number of malware available on both App Store and Google Play is considerably high with some pointing at Android platform as being a leader (Svajcer, 2012). Even though, publication of applications on Android and iOS platforms undergo a vetting process it may be not good enough (Biswas, 2012). It does not address potential bugs in the software or what and how user's information relative to the application itself is stored i.e. logon details, password and any other relevant data.

### ***1.4 Intellectual challenge***

The intellectual challenges involved are detailed review of operating systems of two major providers of mobile operating platforms, familiarisation with forensic software and data acquisition in particular. Also study of cloud computing and cloud storage platforms that products were used this research. Finally, detailed analysis of data extracted from mobile devices and conclusions leading to recommendations and guidance on future research.

## ***1.5 Research objectives***

The following objectives have been set out to complete the dissertation and contribute to the overall outcome.

- Uncover any potential security flaws when using cloud storage applications on a mobile device.
- Extraction of data using forensic software.
- Detailed analysis of cloud storage files structure and hierarchy.
- Preparation of data set consisting of a number files that will be uploaded to cloud storage.
- Simulation of real life transaction of data stored in the cloud.
- Development of number of test cases to simulate real life scenarios.
- Detailed review of the forensic software tools.
- Install of the forensic software products and familiarisation with them.
- Thorough literature review.
- Recommendation of a solution to avoid any security flaws.

## ***1.6 Research methodology***

The primary research will focus on the analysis of extracted data from cloud storage applications installed and used on smart phones.

The secondary research, a follow up experimentation will be carried out in case there are findings that may lead to compromising user's account or data stored in the cloud.

## ***1.7 Resources***

Successful completion of the research requires a number of resources. The following is the list of the resources that will be utilised during the course of conducting the research project.

- Laptop computer for conducting the data acquisition, data set uploads and writing the dissertation.
- Smart phones for conducting file transactions and data acquisition.
- Forensic software products.
- Internet access.
- Access to DIT library to enable use of a variety of academic resources.

### ***1.8 Scope and limitations***

This study aims to identify security flaws of three different cloud storage smart phone applications used to upload, download, view and remove data stored in the cloud. It will be carried out by using smart phones to simulate real life usage of both, mobile devices and mobile application. Subsequently, forensic tools will be used to acquire file system off these smart phones and analysis of that data. There will be experiment expectations set out so that outcomes of the research can be referred to as well as to previous researches in this field.

Limitations may be down to forensic software tools made available to the researcher as well as the feature set and level of data acquisition that these tools will provide.

### ***1.9 Organisation of the dissertation***

Chapter 2 introduces the term of cloud computing and cloud storage. It also highlights vendor of the cloud storage service used for the purpose of this paper with characteristics particular to security measures implemented by these vendors.

Chapter 3 focuses on operating system of one of the most popular mobile operating systems provider on the market. A brief history is presented including major achievements in development of these operating platforms. Description of the behind the scene of mobile systems as well as their security features.



Examination of classification of forensic software tools is provided in Chapter 4. It also contains a description of forensic software products made available to the researcher.

Chapter 5 focuses on previous research. A review of work so far completed is conducted including highlights and critical review.

The experimentation and evaluation of test cases take places in Chapter 6. Detailed description of test cases, data set prepared, undertaken scenarios, forensic software tools installation process and versions description is achieved. Also, if required, any follow up experimentation will be carried out during experimentation and evaluation stage.

The entirety of this study is discussed and overall recommendations are concluded in last chapter. This will propose the contribution this project offers to both users and vendors of cloud storage solutions. Suggestions are proposed for future work and research in the field.

## 2 SECURITY OF CLOUD STORAGE PROVIDERS

### 2.1 Introduction

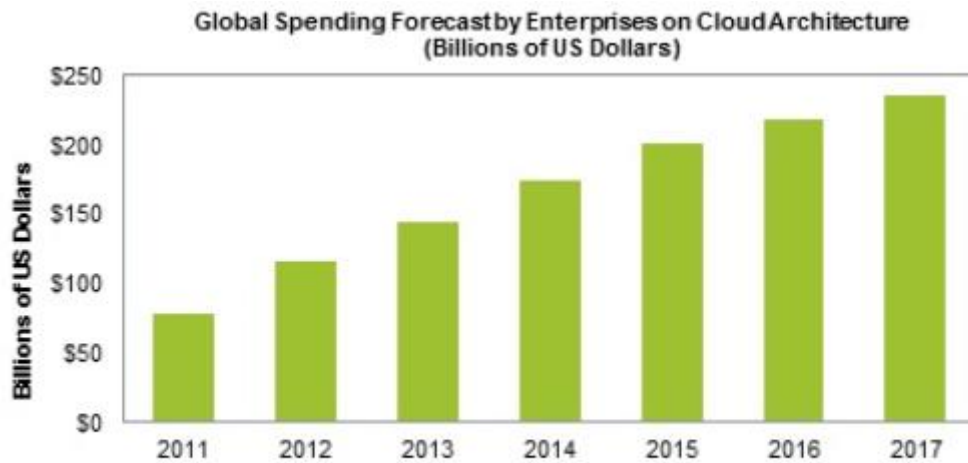
Cloud computing as a term became widely known and used in recent years. However, the roots of the concept go back to the sixties. J.C.R. Licklider, the man behind Advanced Research Projects Agency Network (ARPANET), came up with an idea of an “intergalactic computer network” in 1969 (Kandukuri., 2009). The term “cloud computing” itself was coined in the mid nineties’ by two Compaq staff members, market executive named George Favaloro and technologist Sean O’Sullivan (Regalado, 2011). Throughout the years, the evolution of cloud computing as a network-based service developed from application service provision to the following three main areas;

- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS).

Cloud storage is part of an Infrastructure as a Service.

The establishment of Salesforce in 1999, a provider of web-based applications, was one of first milestones in the area of cloud computing (Salesforce, 2014). Nowadays, huge multinational corporations provide their services in a cloud model. Google, Amazon, HP, IBM are a few of the companies who have their data centres located across the world (Google, 2014; Amazon; 2014).

Latest IHS Technology forecast showed that businesses will triple their investment in cloud-based services between 2011 and 2017 (IHS, 2014). The industry spend in 2011 was \$78.2 billion. In 2013 this amount almost doubled with business spend of \$145.2 billion. This year, it is estimated that the will be total of \$174.2 billion invested in cloud-based services. It is forecasted that in 2017 enterprise spending will reach \$235.1 billion as seen in figure 2.1.



Source: IHS, February 2014

**Figure 2.1 Global spending forecast on cloud computing (IHS, 2014)**

Also Gartner, Inc. predicted an increase in cloud-based services provisioning (Gartner, 2013). They forecasted that a bulk of new IT spend will be investment in cloud computing by 2016. In India, cloud computing will generate the annual growth rate of 33.2% from 2012 to 2017. Software as a Service and Infrastructure as a Service have higher projected growth rate of 34.4% and 39.8% respectively.

CompTIA's 4<sup>th</sup> Annual Trends in Cloud Computing Report showed an increase in outsourcing of businesses IT systems in the United States (CompTIA, 2013). Main IT processes that were moved to cloud are storage (59%), business continuity/disaster recovery (48%) and security (44%). In 2012 and 2013 10% of companies were using some sort of cloud-based systems as depicted in figure 2.2. 1-30% of IT systems were outsourced at the level of 44% in 2012 and this percentage dropped to 31% in 2013. However, increase was seen between 2012 and 2013 from 29% to 38% for companies with 31-60% cloud-based IT systems and for companies with 61-100% IT systems outsourced, increase from 16% to 22% respectively.

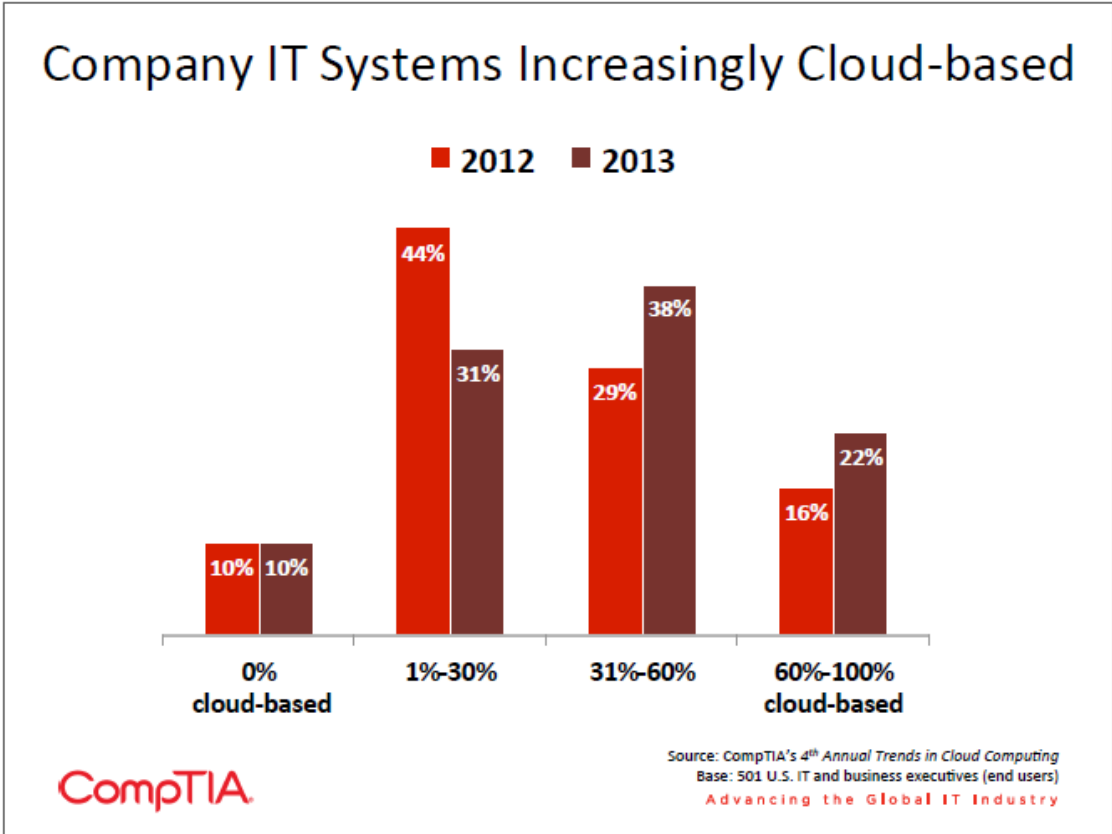


Figure 2.2 Increase in outsourcing of IT systems to the cloud (CompTIA, 2013)

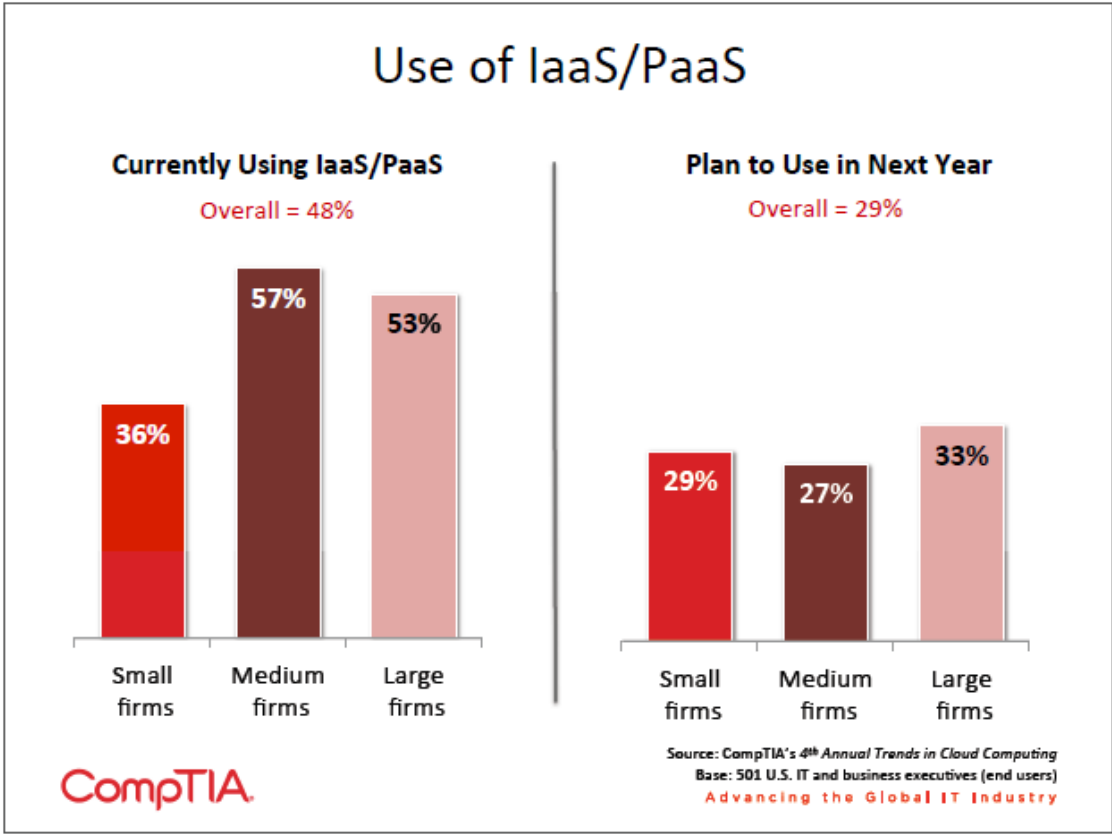


Figure 2.3 Current and planned use of IaaS/PaaS in industry (CompTIA, 2013)

As seen in figure 2.3, there were overall 48% of industry using Infrastructure as a Service and Platform as a Service with 36% of businesses being small firms (1-99 employees), 57% medium firms (100-499 employees) and 53% large firms (500+ employees). 29% of industry planned to move to IaaS and PaaS in 2014. This number consisted of 29% small firms, 27% medium firms and 33% large firms.

Consumer market for personal cloud storage was on the rise as well (IHS, 2012). The ISH iSuppli Mobile and Wireless Communication Service report published in 2012 showed number of personal cloud storage subscribers in 2011 to be less than 300 million with projected growth to 500 million users by the end of 2012. Furthermore, IHS forecasted steady growth of 25% in subscriptions until at least 2017, 1.3 billion.

More optimistic forecast was released at the end of 2013 by ABI Research that forecasted a growth of personal cloud storage subscription to 1 billion in 2013 (ABI Research, 2013).

This chapter will discuss the security of three cloud storage providers, whose services were used in this research. Also a review of known security breaches for Dropbox, Box and SugarSync is presented.

## ***2.2 Dropbox***

Two MIT students, Drew Houston and Arash Ferdowsi, founded Dropbox in June 2007 and launched their product in September 2008 (Dropbox, 2014).

According to the Dropbox official website (Dropbox, 2014) there are more than two hundred million users in over two hundred countries uploading one billion files every twenty four hours (Dropbox, 2014). Dropbox provides storage services to 4 million businesses of which 97% are in Fortune 500.

### 2.2.1 Security of Dropbox service

The following services are elementary to Dropbox architecture which diagram is presented in figure 2.4 (Dropbox, 2014).

- Encryption and application service.

Uploaded files are being split into blocks which are encrypted using a strong cipher. Only blocks that have been modified are synchronised. A new file or existing file that has been modified is identified by Dropbox application and information is sent to the encryption and application service. Service is responsible for new or changed blocks processing and transfer of these to the storage service.

#### Encryption

- Data in rest.

Data stored on Dropbox servers is encrypted using 256-bit Advanced Encryption Standard (AES). Files split into blocks are stored in multiple data centres.

- Data in transit.

Data is transferred using Secure Sockets Layer (SSL)/Transfer Layer Security (TLS). This secure tunnel is protected by 128-bit or higher AES encryption. SSL/TLS encryption is in place every time data is transferred between a Dropbox client. The client type can be a desktop client, mobile client, application programming interface (API) or web client, and hosted service. Desktop and mobile as well as modern browsers are end points under control of Dropbox. For these end points Dropbox uses strong ciphers and support perfect forward secrecy. An extra security measure on the web is flagging all authentication cookies as secure and enable HTTP Strict Transport Security (HSTS).

Dropbox front-end servers are authenticated through public certificates held by the client in order to prevent man-in-the-middle attacks. Secure transfer of data to Dropbox front-end servers for both file block and metadata storage is achieved by previously negotiated encrypted connection.

- Key management.

There are operational, technical and procedural security controls in place. Direct access to keys is very limited and their management is undertaken by Dropbox on behalf of users. This ensures strong cipher encryption, enables advanced features of the product and reduces complexity.
- Data centres.

Dropbox uses third-party organisation data centres and managed service providers. The physical, environmental and operational security controls of Dropbox infrastructure lies within third party service and storage provider. Dropbox looks after the logical, network and application security of the infrastructure hosted at third-party data centres. Third-party housed infrastructure for Dropbox is audited and reviewed at least once a year. Logical and network security is protected by firewall configured to a default deny-all mode. Furthermore, access restriction to the environment is limited to a number of IP addresses and employees.
- Storage service.

Users' content is stored in encrypted blocks. Dropbox client fragments files into blocks to prepare for the block storage utility. Each encrypted file block is recovered based on its hash value from a Content-Addressable Storage (CAS) system. Strong cipher is used to encrypt data at rest.
- Metadata service.

Metadata, specific to user, basic information including file names and types, is stored in its own storage service. It is indexed data for users' accounts. Dropbox metadata is kept in a MySQL database utility. In order to provide best user experience at performance and high availability level, metadata is shared and replicated.
- Notification service.

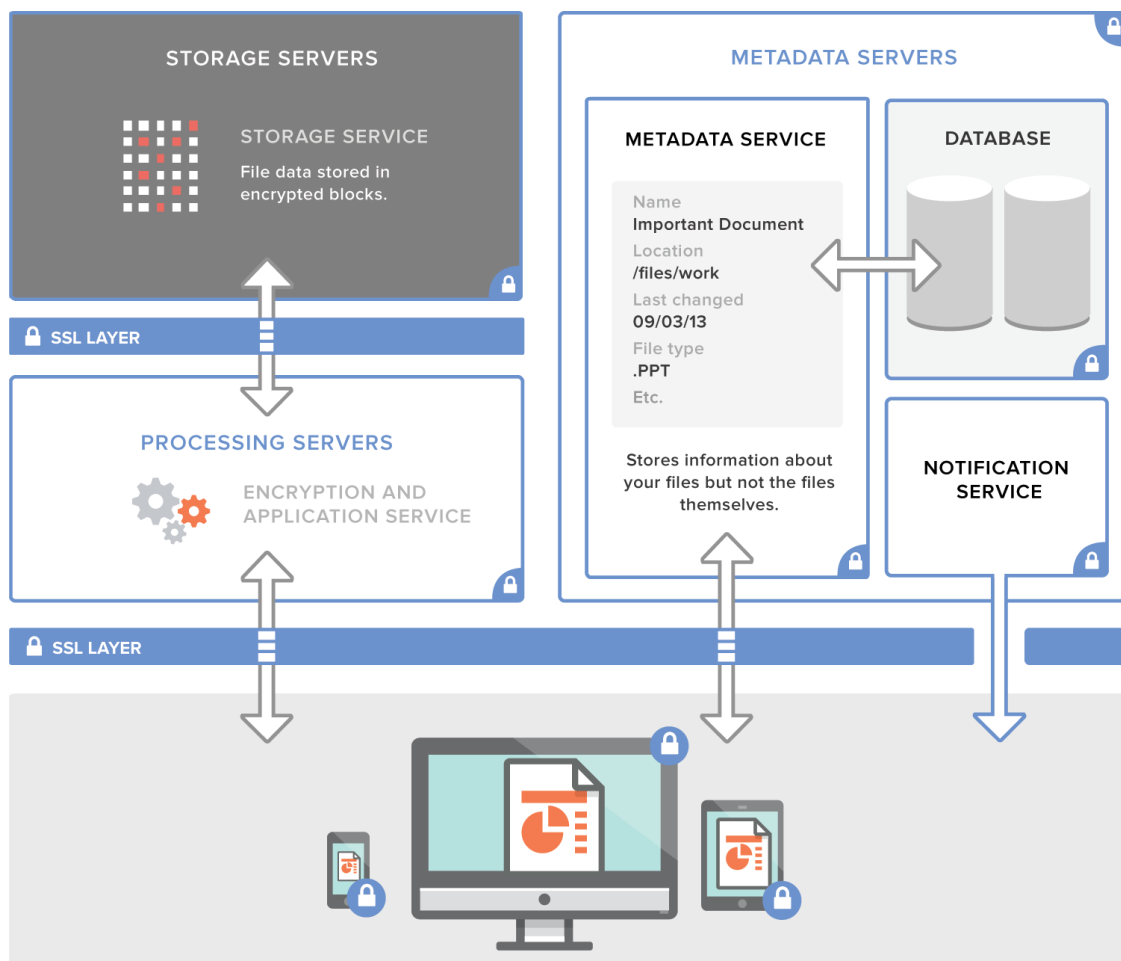
This dedicated service is responsible for monitoring of any changes applied to Dropbox accounts. Connections to these specific services are not encrypted since there are no files or metadata stored here or transferred. A long poll connection to the notification service is established with each client.

The long poll connection is described in XEP-0124: Bidirectional-streams Over Synchronous HTTP (BOSH) draft standard (Moffit et al., 2010). The standard describes a use of long polling with multiple synchronous HTTP request/response pairs to achieve efficiency and low latency.

The long poll connection is idle until a change to any file in Dropbox occurs. In this instance, the notification service beacons an alteration to the related client by terminating the long poll connection. Termination of the connection indicates that client must connect to the metadata service securely to synchronise any changes.

- Dropbox certification.

Dropbox storage is SSAE16/SOC1, SOC2, ISAE 3402 and ISO 27001 certified in Amazon S3 facilities.



**Figure 2.4 Dropbox Architecture (Dropbox, 2014)**



Model of various instances of the information distributed across these services not only improves speed of synchronisation process but makes it more consistent. It also enhances security of service.

Dropbox continuously performs automated and manual application security audits and testing to address any potential security vulnerabilities and bugs. Security and safety of the service is a common work of third party security specialists, industry security teams as well as the security research communities.

### ***2.2.2 Dropbox user interfaces***

There are three user interfaces that customers may utilise. All of them have security features and settings that protect users' data throughout process of users' interaction with the service (Dropbox, 2014).

- Web-based application.  
Upload, download, view and file share takes place via modern browsers.
- Desktop application.  
Dropbox desktop application is a powerful client that allows synchronisation of files stored locally for offline access. Users have full access to their Dropbox accounts. Clients can run on Mac, Linux and Windows operating systems.
- Mobile application.  
Dropbox synchronisation application is available for iOS, Android and Blackberry platforms. Users can access their files on the go as well as download files for offline access to their smart phones or tablets.

### ***2.2.3 Dropbox security breaches***

On 19 June 2011 a bug affected authentication mechanism allowing users to log in to their accounts with any password (Ferdowsi, 2011). Anyone knowing usernames of other Dropbox users could access their cloud storage for duration of almost four hours.


On 31 July 2012 Dropbox announced (Agarwal, 2012) that as a result of a hacked employee account, a number of email addresses were stolen and used for spam purposes. After this incident Dropbox introduced new security measures as follows.

- Two-factor authentication. Optional requirement to validate users' login details using two proofs; password and a temporary code sent to users' smart phones.
- Mechanisms to assist with identification of suspicious activities.
- A new page allowing users to track all active logins (figure 2.5).
- If users' passwords are considered to be common, Dropbox may require users to change them.

On 13 August 2013 at Usenix 2013 Workshop (Kholia and Wegrzyn, 2013) two developers claimed that they were able to hack Dropbox users' accounts via reverse engineering.

Sessions





These are the web browsers currently logged in to your Dropbox.

Browser	Country	Most recent activity
 Firefox on Windows	Ireland	in the last hour ⓘ

---

Devices

You've linked these devices.

Name	Country	Most recent activity	
 Test-PC	Ireland	about a week ago ⓘ	×
 Syl-PC	Ireland	about 4 months ago ⓘ	×
 iPhone	N/A	N/A ⓘ	×
 Android	N/A	N/A ⓘ	×

**Figure 2.5 Security audit page for Dropbox user (Dropbox, 2014)**

## 2.3 *Box*

Box was founded in 2005 by Aaron Levie, student at University of Southern California and Dylan Smith, student at Duke University (Box, 2014).

According to the latest Box announcement (Haig, 2014), there are 25 million active Box subscribers and one hundred thousand businesses of which 92% are in Fortune 500.

### 2.3.1 *Security of Box service*

The following are security measures implemented in Box service (Box, 2014).

- Encryption
  - Data in transit.

Business and Enterprise accounts are encrypted using 256-bit AES SSL encryption. Enterprise accounts benefit of multiple Content Delivery Networks (CDNs) such as Akamai (Akamai, 2014) or EdgeCast (EdgeCast, 2014) to increase upload speed from distributed locations. Once a file is being uploaded or downloaded an encrypted SSL tunnel is opened to a local CDN point. CDN then sends the encrypted data to the Box servers. This utilises the high bandwidth and TCP optimisation processes provided by CDNs for a better transfer performance.
  - Data at rest.

Enterprise account owners benefit from 256-bit AES encryption.
  - Key management.

A Key Encryption Key (KEK) is used to encrypt the AES encryption key. The key encryption key is stored in a secure fashion and independently from data as well as rotated frequently to meet the best practises for key management. Logs and audits are in place for all access to keys.
  - Data centres.

Data resiliency is assured by data replication to offsite storage. The encryption of the data is retained. The encryption key required to decrypt the data is not replicated to redundant storage.

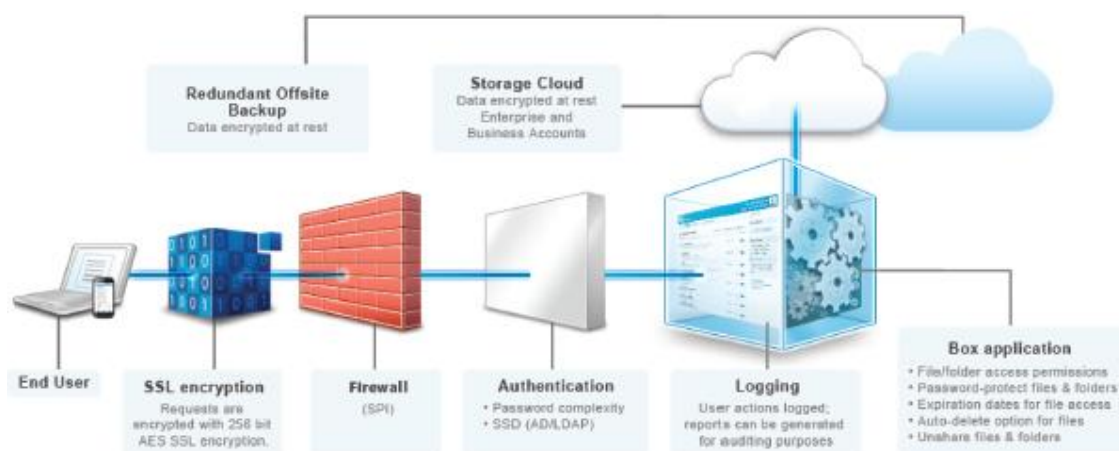
- Box industry certification.
  - Box fulfils Statement on Auditing Standards (SAS) No.70 requirements for both, third party data centre housing their infrastructure and the Box company itself. Current certification that Box holds is SAS 70 Type II.
  - Box is ISO 27001 complaint (Shirk, 2013) and Safe Harbor certified (Safeharbor, 2009).

- Security within a company.

There are a number of measures in order to assure security of the services provided by Box within a company's environment.

- Background checks of employees.
- Access privileges.
- Security training.
- Network and host intrusion detection.
- Vulnerability monitoring.
- Audit and log of systems, networks and applications.
- Third party network security testing.

Figure 2.6 shows Box network architecture and link between end user and cloud storage.



**Figure 2.6 Box infrastructure (Box, 2014)**

Users can interact with Box cloud storage service in the same manner as Dropbox users.

- Web-based application.  
Upload, download, view and file share takes place via modern browsers.
- Desktop application.  
Box desktop application is a powerful client that allows synchronisation of files stored locally for offline access. Users have full access to their Box accounts. Client can run on Mac and Windows operating systems.
- Mobile device application.  
Box synchronisation application is available for iOS, Android and Blackberry platforms. Users can access their files on the go as well as download files for offline access to their smart phones or tablets.

There are no known security breaches to the Box network or hosted data centres.

## ***2.4 SugarSync***

SugarSync was founded in 2008 (SugarSync, 2014). The company, formerly known as Sharpcast and established in 2004 (Venture Beat, 2009), provides paid-only cloud storage services unlike Dropbox and Box. According to SugarSync website (SugarSync, 2014), the company has millions of users worldwide. In December 2013 SugarSync announced (SugarSync, 2013) to move to paid-only model unlike its competitors who offer limited storage free of charge.

### ***2.4.1 Security of SugarSync service***

A simplified architecture diagram of SugarSync service is shown in figure 2.7. The following are security features of SugarSync service (SugarSync, 2014).

The following are features of SugarSync encryption.

- Data in transit.  
Transfer of files is secured using TLS/SSL encryption.
- Data at rest.  
Stored files are encrypted with 256-bit AES encryption. Data is replicated so that users' files are backed-up.
- Data Centres.  
SugarSync hosted services are provided by Amazon's S3 facilities.
- Data access.  
Access to users' data is limited to a few employees in SugarSync's escalation team. All personal data access is logged and audited.



**Figure 2.7 Simplified SugarSync architecture (SugarSync, 2014)**

Users can interact with SugarSync cloud storage service in the same manner as Dropbox and Box users.

- Web-based application.  
Upload, download, view and file share takes place via modern browsers.
- Desktop application.  
SugarSync desktop application is a powerful client that allows synchronisation of files stored locally for offline access. Users have full access to their SugarSync accounts. Client can run on Mac and Windows operating systems.
- Mobile device application.  
SugarSync synchronisation application is available for iOS, Android and Blackberry platforms. Users can access their files on the go as well as download files for offline access to their smart phones or tablets.

There are no known security breaches to SugarSync service and servers.

## ***2.5 Conclusion***

This chapter outlines cloud storage origins and discusses security frameworks of three cloud storage providers that services were used in this research. The reason to choose these three providers is that outcomes of the experimentation will be referred and checked against previous research. Also all of the companies share similar origins and their founders had the same idea when companies have been established. Provision of cloud storage for all three businesses was their sole goal at the time. Dropbox and Box provide their cloud storage services to majority of Fortune 500 companies, 97% and 92% respectively. SugarSync was the first out of these three to have a presence on the market.

Focus of the next chapter will be operating systems of smart phone devices on which cloud storage applications will be installed and tested. The security of the operating system will be discussed as well as it is essential to users and providers alike. Users want it to be secure since it is their data that is stored in the cloud. Providers want to ensure security of their services in this highly competitive market.

## **3 IPHONE OPERATING SYSTEM**

### ***3.1 Introduction***

Every operating system whether it is for a PC, laptop, tablet or smart phone has come a long way since its initial debut. Since the dawn of smart phones, they are under constant scrutiny and are the target of hackers that wish to exploit any security flaw that is possible. George Holtz was the first hacker to hack the iPhone (Lee, 2007). Apple had exclusive agreement with AT&T for iPhone sales; hence iPhone was locked to AT&T network. Holtz unlocked iPhone so that smart phone could be used on any network.

"It's a cat-and-mouse game. We try to stay ahead.  
People will try to break in, and it's our job to stop them breaking in."  
(Steve Jobs)

The first Android phone was released in 2008 (Ricker, 2008) and it was HTC Dream. Android operating system based phones were not in demand as depicted in table 3.1 (Gartner, 2009) thus they were not target of hackers. BlackBerry phones were widely used in the industry as they are famous for their security standards and still are. The company founded in Canada is the first one to secure United States Department of Defence device management approval (Whittaker, 2013). Nokia, market leader at the time as seen in table 3.2 haven't had a smart phone in their offering that would resemble iPhone.



Company	4Q08 Sales	Market Share 4Q08 (%)	4Q07 Sales	Market Share 4Q07 (%)	Growth 4Q07-4Q08 (%)
Symbian	17,949.1	47.1	22,902.5	62.3	-21.6
Research In Motion	7,442.6	19.5	4,024.7	10.9	84.9
Microsoft Windows Mobile	4,713.9	12.4	4,374.4	11.9	7.8
Mac OS X	4,079.4	10.7	1,928.3	5.2	111.6
Linux	3,194.9	8.4	2,675.9	7.3	19.4
Palm OS	326.5	0.9	449.1	1.2	-27.3
Other OSs	436.9	1.1	411.3	1.1	6.2
<b>Total</b>	<b>38,143.3</b>	<b>100.0</b>	<b>36,766.1</b>	<b>100.0</b>	<b>3.7</b>

**Table 3.1 Smartphone Sales to End Users by Operating System, 4Q 2008 (Gartner, 2009)**

Company	4Q08 Sales	Market Share 4Q08 (%)	4Q07 Sales	Market Share 4Q07 (%)	4Q07-4Q08 Growth (%)
Nokia	15,561.7	40.8	18,703.3	50.9	-16.8
Research In Motion	7,442.6	19.5	4,024.7	10.9	84.9
Apple	4,079.4	10.7	1,928.3	5.2	111.6
HTC	1,631.7	4.3	1,361.1	3.7	19.9
Samsung	1,598.2	4.2	671.5	1.8	138.0
Others	7,829.7	20.5	10,077.3	27.4	-22.3
<b>Total</b>	<b>38,143.3</b>	<b>100.0</b>	<b>36,766.1</b>	<b>100.0</b>	<b>3.7</b>

**Table 3.2 Smartphone Sales to End Users by Vendor, 4Q 2008 (Gartner, 2009)**

Each new release of iPhone brought a new set of features, upgraded iOS and potential exploits for discovery by hackers. Nowadays, iPhone as well as smart phones manufactured by Samsung, HTC, LG or Sony that operate on Android OS are in the centre of hackers' interest as they both combined have majority of smart phone operating systems market share. IDC report for 2013 (IDC, 2014) shows that total market share of iOS and Android OS devices in 2013 was at 93.8% as depicted in table 3.3.

**Top Five Smartphone Operating Systems, Shipments, and Market Share, 2013 (Units in Millions)**

Operating System	2013 Shipment Volumes	2013 Market Share	2012 Shipment Volumes	2012 Market Share	Year-Over-Year Change
Android	793.6	78.6%	500.1	69.0%	58.7%
iOS	153.4	15.2%	135.9	18.7%	12.9%
Windows Phone	33.4	3.3%	17.5	2.4%	90.9%
BlackBerry	19.2	1.9%	32.5	4.5%	-40.9%
Others	10.0	1.0%	39.3	5.4%	-74.6%
<b>Total</b>	<b>1009.6</b>	<b>100.0%</b>	<b>725.3</b>	<b>100.0%</b>	<b>39.2%</b>

**Table 3.3 Top Five Smartphone Operating Systems, Shipments and Market Share, 2013 (IDC, 2014)**

The focus of this chapter is Android and Apple operating systems for smart phones and their security.

## **3.2 *Apple's iOS***

### **3.2.1 *History of iPhone Operating System***

The first iPhone was released in 2007 was supplied with OS X operating system (Web Archive, 2014). It has a few applications; some of them were standard to any mobile as follows (Morrissey and Campbell, 2010).

- SMS.
- Calendar.
- Photos.
- Camera.
- Notes.
- Clock.
- Calculator.
- Settings.

- Phone
- Mail.

Some of the applications were not standard ones.

- YouTube
- Stocks.
- Weather.
- Maps.
- iTunes.
- iPod.
- Safari.

Initially application were web based applications that could be downloaded from Apple or set up as bookmarks for Safari web browser.

On 11 July 2008 Apple released iPhone 3G along with iPhone 2.0 software 2 (Apple, 2008). This OS upgrade brought new features. There were two major additions to operating system. The first one was App Store that allowed users to download applications for iPhone. The second one was GPS functionality which allowed numerous applications to use GPS API to geo-tag files such as photos. Apart from these two applications there were few more that are worth listing.

- Microsoft Exchange support.
- Push email.
- The capability to view Microsoft Word documents.
- Exif data which is held when images are emailed from the device.

On 8 June 2009 Apple released iPhone 3GS with the new iPhone OS 3.0 (Apple, 2009). It was another major update with a number of extra features.

- Cut, copy and paste.
- YouTube account owners were able to sign in.
- Call history with detailed logs.
- Video capture (iPhone 3GS only).
- Addition of thumbnails of the original photos.
- Autofocus function in the camera (iPhone 3GS only).

- Use of MobileMe to enable Find My iPhone option. This allowed users to remotely send a message to the device, add a passcode or wipe it.
- CalDAV support.
  - Standard for accessing, managing and sharing calendar and schedule data based on iCalendar format (tools.ietf.org, 2007).
- LDAP support.
  - Lightweight Directory Access Protocol provides access to distributed directory services compliant with X.500 data and service models (tools.ietf.org, 2006).
- Spotlight search.
- Tethering.
- Voice memos.
- Encrypted backups.
- Hardware encryption (iPhone 3GS only).
- Voice control.
- Fraud protection in Safari web browser.
- Improved Exchange support.
- Push notifications.

On 8 April 2010 Apple released new iPhone OS 4. Later that year Apple released iPhone 4 and “iPhone OS” was rebranded to “iOS” (Apple, 2010). This OS upgrade was the most significant so far. The following are the features.

- VoIP.
- Switching between applications.
- Multitasking.
- Folders.
- Personalisation of home and lock screen wallpapers.
- Improved email support.
  - Multiple Exchange accounts.
  - A unified mailbox.
  - Switching between mailboxes was quick.
  - Multiple applications were supporting attachments.
- iBooks – Apple’s .pdf reader.

- Enterprise support.
  - PIN set email encryption.
  - Mobile device management.
  - Wireless applications distribution.
  - SSL VPN feature.
- Spell checking.
- Wireless Bluetooth keyboard support.

On 4 October 2011 Apple launched iPhone 4S powered by iOS 5 (Apple, 2011). This OS upgrade came with the following notable features.

- Siri, multiple application voice assistant.
- iCloud, free up to 5GB Apple cloud storage service.
- Notification Centre, centralised manager for applications notifications.
- iMessage, service for sending messages, photos and videos between iOS 5 users.
- Newsstand, magazine and newspaper subscription centre.
- Built-on Twitter integration.
- HD camera.
- Over-the-air activation of the device and software updates.

On 12 September 2012 Apple announced iPhone 5 with iOS 6 (Apple, 2012). Handset has been redesigned; it was thinner, lighter and was supplied with bigger screen. Operating system traditionally came with a set of new features.

- New maps application, google maps application was removed from the operating system.
- Enhanced Siri features that include applications like Facebook, Twitter or ability to launch an application.
- Built-in Facebook integration.
- Passbook application for boarding passes, tickets, coupons, loyalty cards.
- Guided Access, allows users to limit what applications and even further what parts of display a user can access.
- FaceTime calls support over mobile networks.
- VIP mailbox that stores emails from user preferred contacts.

- Do Not Disturb option.
- Quick message when declining an incoming call and call back reminder.

On 20 September 2013 Apple released iPhone 5S and iPhone 5C models with completely redesigned iOS 7 (Apple, 2013). The latest operating system for Apple mobile devices family introduced utilisation of 64-bit kernel, libraries and drivers. Native applications have been re-engineered for 64-bit in order to take full advantage of this architecture. New OS brought the following new features.

- Control Centre, quick access to Wi-Fi, Bluetooth, Airplane and Do Not Disturb switches as well as music player, clock, calculator and native flashlight applications.
- Notification Centre available at lock screen with Today feature, quick access daily agenda, weather and traffic.
- Enhanced Multitasking.
- AirDrop, content sharing feature with people nearby.
- Redesigned Photo and Safari applications.
- Twitter search integration.
- Wikipedia integration.
- Within an application Bing web search.
- iTunes Radio, a free internet radio facility.
- Activation Lock via Find my iPhone. Activation Lock requires Apple ID and password when turning off Find My iPhone, erasing data or re-activating a device once it was wiped.
- All new users are able to download iLife and iWork suites for free. These suites consist of creativity and productivity applications such as:
  - iPhoto – photo editor.
  - iMovie – video editor.
  - GarageBand – music editor.
  - Pages – Microsoft Word like application.
  - Numbers – Microsoft Excel like application.
  - Keynote – Microsoft Powerpoint like application.

### **3.2.2 Operating System**

iPhone operating system is based on OS X and it utilises modified kernel of the Mac OS X. Development is based on XCode and Cocoa Touch (Apple Developer, 2014). There are four layers to run applications in iOS (Hoog and Strzempka, 2011).

- Core OS.  
This layer is responsible for access to external accessories, low-level networking, management of memory and file system processing. At this layer dynamic library creates and manages certificates and is required by Keychain services to provide encryption/decryption role for Keychain files.
- Core services.  
This layer along with Core OS provides the essentials for applications use. Low-level data types and file access operations take place at this level through C-based interfaces. Security services for data storage and cryptographic purposes are used within keychain databases. Core Foundation, CFNetwork and SQLite functions are this layer.
- Media.  
Graphics, audio and video technologies are located at this layer.
- Cocoa Touch.  
This is the location of technologies mostly using Objective-C which are responsible for implementation of the visual interface for applications.

The latest version of iPhone's operating system is 7.0.4 and was released on 14 November 2013 (Apple, 2013).

### **3.2.3 File System and memory**

iOS utilises two memory types (Hoog and Strzempka, 2011). There are RAM (Random Access Memory) which is a volatile memory and NAND (Iwata et al., 1987) chip, a Solid-State Drive which a non-volatile memory. From forensic perspective chip-off data extraction has been very difficult due to the hardware-based encryption

present on the iPhone (Zdziarski, 2012). NAND has a high density, no mechanical moving parts which enhance durability.

The file system used in iOS device was initially Hierarchical File System (Morrissey and Campbell, 2010). However, it was enhanced to include Unicode file name encoding, bigger block size from 512-byte blocks to 4KB blocks (Hoog and Strzempka, 2011). This file system was named HFS Plus. Currently all iOS devices use HFSX file system which differs from HFS Plus that it is case sensitive so that two file that have the same name but different case can be stored in the memory.

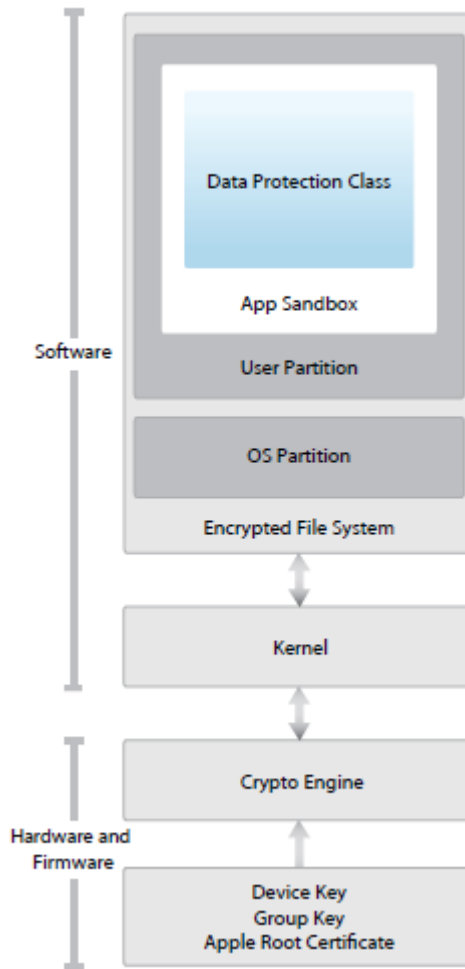
#### ***3.2.4 Security of iOS***

Apple, as detailed in the iOS security whitepaper, introduced a number of features to secure their operating system (Apple, 2014). These features start to operate as soon as user powers on the device and are listed below.

- System Security.
- Encryption and data protection.
- Application security.
- Network security.
- Internet services.
- Device controls.

Figure 3.1 depicts various levels of security architecture of iOS platform. Each level has its specific role thus its security requirement and security framework for each has been individually designed and implemented. Focus of this chapter is on services and components that are in use during regular smart phone use along with accompanying cloud storage applications.





**Figure 3.1 Security architecture of iOS (Apple, 2014)**

### ***3.2.4.1 System Security***

System security consists of the following components.

- Secure Boot chain.  
Start-up is a staged process of which each stage has its components (Apple, 2014). These are bootloaders, kernel, kernel extensions and baseband firmware. All of these are cryptographically signed by Apple to guarantee integrity and processed only when the chain of trust is successfully verified. This component is responsible for validation of iOS and which is designed to run only on Apple devices as well as if the lowest level of software has not been compromised.
- System Software Authorisation.

New features and identified security flaws are being dealt with in each software upgrade for the device. Furthermore, this component prevents installation of older version of iOS so that previous iOS' vulnerabilities cannot be exploited.

#### ***3.2.4.2 Encryption and Data Protection***

After ensuring that only trusted code and applications run on an iOS device additional encryption and data protection supplements secure storage of user data. This feature is operational even if other parts of the device were tampered with.

- **Hardware security features.**  
A dedicated 256-bit AES crypto engine is built into Direct Memory Access path. The encryption takes place between NAND memory and main system memory which does not decrease device's performance. In an addition to AES encryption, SHA-1 is applied in hardware which reduces cryptographic burden even more.
- **File data protection.**  
Protection is ensured by creation and management of keys. This takes place on top of the hardware encryption. Data protection generates a new 256-bit key for each file. Subsequently each key is wrapped using NIST AES key wrapping standard, RFC 3394 and stored in file's metadata.
- **Passcode.**  
When passcode is set up, iOS enables Data Protection. Passcode relates to device Unique Identifier. This means that any brute-force attacks must be performed on the device. The encryption keys are iterated many times in order to slow down the attacker. A user can set up the device to wipe after up to ten incorrect passcode entries attempts. It also applies time delays when invalid password is used.
- **Data protection classes.**  
Application that creates a file assigns a class to it. Classes have different policies that specify when data is accessible. The following are basic classes.

- Complete protection.
- Protected unless open.
- Protected until first user authentication.
- No Protection.
- Keychain data protection.
 

This component secures storage of keys and login tokens and other sensitive data that applications require. SQLite database is implementation of keychain.
- Keybags.
 

Both classes', file protection and data protection, keys are stored and handled by keybags. There are four of keybags present in iOS.

  - System keybag for normal operation of the iOS device. This is the only keybag stored on the device.
  - Backup keybag for creation and encryption of the devices' backups. Keybag is set in iTunes and stored on a PC.
  - Escrow keybag that is used for iTunes synchronisation as well as Mobile Device Management (MDM). This keybag is stored on a PC used for iTunes synchronisation or the MDM server.
  - iCloud backup keybag works on a similar basis as backup keybag.
- FIPS 140-2.
 

The cryptography present in iOS 7 is compliant with United States Federal Information Processing Standard (FIPS) 140-2 level 1. All cryptographic processes in Apple applications and third party applications that adhere and utilise iOS cryptography modules are validated and considered integral. Bluetooth services are outside of this scope.

### ***3.2.4.3 Application Security***

Applications are essential to the iOS ecosystem thus they are signed and verified, ensured that they cannot run malicious code and are sandboxed to protect user data. All of these measures are implemented to provide stability and security of the platform. The following components are responsible for application security compliance.

- Application code signing.  
All user processes and applications are controlled by iOS kernel. Applications must have an Apple-issued certificate signature in order to execute code. Apple and third party applications must comply with this. It also is part of chain of trust from operating system to applications.
- Runtime process security.  
Application cannot compromise other applications or the system itself. Restriction is in place for all third party applications from accessing files stored by other applications or applying changes to the device. This prevention mechanism is called sandboxing.
- Data protection in applications.  
Software development kit for iOS provides a suite of API's for developers to implement data protection. It is available for file and database API's such as CoreData or SQLite.
- Accessories.  
All accessories made for iOS devices have to be authorised by Apple. When connecting to the device they need to respond with an Apple-provided certificate which is verified by the device.

#### ***3.2.4.4 Network Security***

Ability to network is essential and iOS support a number of network security protocols to enable users to utilise their devices at the highest level. Below is a list of supported network mechanism and protocols.

- SSL, TLS protocols.  
Support for Secure Socket Layer (SSL v3) and Transport Layer Security (TLS v1.0, TLS v1.1, TLS v1.2) as well as Datagram TLS is essential in iOS. All applications that utilise internet connection automatically use these protocols to encrypt communication.
- VPN.

Minimal set up and configuration of iOS device is required for virtual private networking. iOS support VPN servers that use variety of protocols and authentication mechanisms.

- **Wi-Fi.**  
Industry standard Wi-Fi protocols including WPA2 Enterprise are supported by iOS.
- **Bluetooth.**  
Encryption Mode 3, Security Mode 4 and Service Level 1 Bluetooth type connections are supported within iOS.
- **Single Sign-On.**  
SSO with Kerberos-based networks is support on iOS devices. This allows corporate users to authenticate with enterprise environment. SSO is supported by Safari and networking API's allow developers to utilise this mechanism by whitelisting these API's.
- **AirDrop security.**  
AirDrop uses Bluetooth Low-Energy (BTLE) and Apple-created peer-to-peer Wi-Fi technology to exchange files and data with devices in vicinity. While enabling AirDrop, a 2048-bit RSA identity is stored on the device. Also AirDrop identity hash based on the user's Apple ID is created. When sharing via AirDrop is used the device sends signal to other devices that have AirDrop turned on and are powered on. These devices respond with shortened owner's identity hash. Devices use TLS encrypted connection for sharing data.

#### ***3.2.4.5 Internet Services***

Internet services like iMessage, FaceTime, Siri, iCloud, iCloud Backup and iCloud Keychain have been designed to empower users. They were built with the same aim as all other services and components which high security and usability. Secure handling of data at rest or in transit, safeguarding of users' data and protection against malware or unauthorised access were in mind of developers of these services.

### **3.2.4.6 Device Controls**

Device controls is set of tools that empower businesses who want to use iOS devices or have an active Bring Your Own Device (BYOD) policy in place. By using Exchange ActiveSync and MDM, IT security officers can implement set of policies that allow to control, monitor and restrict use of certain applications or other services. Below is a list of the device controls.

- Passcode protection.
- Configuration enforcement.
  - Passcode policies.
  - Device features restrictions such as Siri, iCloud, camera.
  - Wi-Fi settings.
  - VPN settings.
  - Email server profile.
  - Exchange profile.
  - LDAP directory service settings.
  - CalDAV calendar service settings.
  - Web clips.
  - Credentials and keys.
  - Advanced mobile network settings.
- Mobile Device Management.
- Apple configurator (available only on OS X device).
- Device Restrictions.
- Supervised Only Restrictions (implemented via OS X device)
- Remote Wipe.

### **3.3 Conclusion**

This chapter focused on one of the most popular mobile operating systems. Its history, development throughout the years as well as technical details and security features were discussed. Although iOS is not so widely used as it used to be, this operating

system started the smart phone revolution and its developments and features are still used as a blueprint by other mobile operating system providers.

Next chapter discusses forensic software tools classification as well as tools that were made available to the researcher.

## 4 FORENSIC SOFTWARE

### 4.1 Introduction

In Chapter 3, operating systems for mobile device of two market leaders were discussed. This chapter will focus on forensic methods and forensic software utilised in this research. The reason for use of the forensic software listed in this chapter was that these software products were made available to the researcher.

### 4.2 Classification of Forensic Tools

Sam Brothers came up with a forensic tool classification system (Brothers, 2007) that is based on the depth of the level examiner and/or forensic software acquires data of the device. Although, author relates his levelling system to iPhone, this system can be used for any mobile phone, tablet or GPS device. Software developers of forensic tools refer to this classification.



Figure 4.1 Forensic analysis tools classification (Brothers, 2007)



### **4.2.1 Manual Extraction**

Manual extraction of data is performed through interaction with a device. Direct examination of the device is based on manual, hand investigation of it. Examiner, as long as the device is in a operational condition, can browse through available files on the device built-in memory or memory card as well as contacts, calendar, notes, voice memos, photographs, videos and files stored by applications. Examination is limited to the ecosystem of the device that is available to the owner of the device.

Software that operates at this level is available from the following sources:

- ERT available at <http://www.fernico.com/ert.htm>
- Project-A-Phone available at <http://www.projectaphone.com/>

### **4.2.2 Logical Extraction**

Logical extraction requires a connection between a device and a computer running forensic software to acquire data. Connection is usually established with use of data cable (USB or serial), Bluetooth or Infrared. Protocols to establish the communication vary and a few of them are briefly discussed below.

- Wireless.  
BREW Binary Runtime Environment for Wireless protocol (Brewmp Developer, 2014). BREW has been developed by Qualcomm and is used by software programmers to develop portable applications that run on Code Division Multiple Access-based handsets (CDMA).
- Hayes AT Commands (Nemesis Lonestar, 2000).  
This protocol originated as a transmission protocol used to ensure data integrity or provide compression between modems. Since then it has been developed and expanded and found its use in GSM area. This protocol is used for the following actions (Sonymobile, 2010).
  - Develop new communication software.
  - Work with SMS and Contacts.
  - Amend settings on mobile phones.
  - Add a mobile device to a list of supported modems in an application.

- F-Bus (Fast bus)

This is another communication protocol for transferring data. It was widely used in low-tier Nokia handsets.

Communication is based on client-server framework. Data is acquired in the following manner:

- Software initiates a command that is sent to a device using established connection.
- Device's processor receives the command and processes it.
- Response to the command is compiled.
- Software receives the response from the device.

Software that acquires data at the logical level:

- XRY Logical available at <http://www.msab.com>
- BlackLight available at <http://www.blackbagtech.com>
- CellXTract available at <http://www.logicube.com>
- MOBILedit Forensic available at <http://www.mobiledit.com>
- Oxygen Forensic available at <http://www.oxygen-forensic.com>
- Mobile Phone Examiner available at <http://www.accessdata.com>
- Lantern available at <http://katanaforensics.com>
- UFED Analyzer available at <http://www.cellebrite.com>
- Secure View available at <http://mobileforensics.susteen.com>
- EnCase Forensics available at <http://www.guidancesoftware.com/>

### ***4.2.3 Physical Extraction***

Connection means are the same as in logical extraction level. The difference is that boot loader or unsigned code is uploaded into the memory of the phone which results in all or almost all data duplicated on to computer hosting the forensic software. Replicated data is stored in a raw HEX (binary) format. This method establishes link to the diagnostic connection such as JTAG (Corelis, 2013) on the device to acquire data.

JTAG stands for Joint Test Access Group. This group developed a technique for printed circuit boards (PCBs) and integrated circuits (chips or microchips) debugging in 1980s. In 1990 JTAG testing was standardised as the IEEE 1149.1-1990 standard for reduced-pin and enhanced-functionality test access port and boundary-scan architecture (IEEE Standard, 2014). This standard defines built-in circuitry that allows test, maintenance and support of PCBs. Its standard interface makes possible for instructions and test data communication as well as response from tested object.

The following software operates at the above level:

- The Zdziarski Method (iOS only) available at <http://www.iosresearch.org/>
- XRY Physical available at <http://www.msab.com>
- iXAM (iOS limited to older device models) available at [http://www.ixam-forensics.com/ip\\_forensics.asp](http://www.ixam-forensics.com/ip_forensics.asp)
- EnCase Forensics (Android OS only) available at <http://www.guidancesoftware.com/>

#### ***4.2.4 Chip-Off Extraction***

This technique is based on physical removal and analysis of memory chip also called NAND flash. A chip reader connected to the computer is used to read all data stored on the chip. Like in the physical extraction duplicated data is in a raw format. The data may be encrypted as some devices store data at rest encrypted.

Flash Doctor developed by Salvation Data Technology available at <http://www.salvationdata.com/> allows examiner for chip-off extraction.

#### ***4.2.5 Microread***

This methodology is the most time-consuming, the most expensive and requires enormous knowledge. Microread is uses an optical character recognition or relies on manual read of individual bits from device's memory. The status of physical gates

needs to manually read then translated to binary code which translates to ASCII characters. This technique is used only when prior attempts fail or examiner knows that chip is faulty.

There is no software for this type of data acquisition commercially available.

### ***4.3 BlackLight***

BlackLight® forensic software has been developed by BlackBag™ Technologies, Inc. (Blackbagtech, 2014). BlackBag offers software for forensic acquisition and analysis; training and certification; eDiscovery, native Mac OS X data processing. It can be used a quick triage tool or sophisticated examination tool.

#### ***4.3.1 BlackLight features***

BlackLight is comprehensive analysis software (Blackbagtech, 2014). It allows the examiner to extract and analyse data from Mac OS X, Windows computers including registry and iPhone, iPad and iPod devices.

The following is a list of data that BlackLight software can acquire during examination process including search and filter options.

- Snapshot of user's device.
  - Device type.
  - iOS/OS version.
  - Serial number.
  - UDID (Unique Device Identifier).
  - IMEI (International Mobile station Equipment Identity).
  - Artefacts summary statistics for documents, emails, videos, calls, voicemails and more.
  - User's device account information and common internet account data for social media applications or iCloud.

- Recent usage history including list of last running applications, most recent web-based location searches and dialled phone numbers with associated contact information.
- Examination of large data sets using file filter option. User can define filter settings as follows:
  - File name, kind, size or extension.
  - Date when file was created, modified and accessed.
  - Picture metadata attributes including GPS location and camera type (iOS device).
  - Positive and negative hash set.
- Media filter. Support for media files commonly used along with following features:
  - Built-in GPS mapping for files containing geolocation stamp.
  - Proprietary skin tone analysis mechanism.
  - Video frame analysis.
- Social media activity.
  - Ability to track transaction on the following social media applications; Facebook, Twitter, LinkedIn, Foursquare.
- Messaging filter.
  - Support and view of messaging history in its native form for SMS, MMS, Skype, iMessage, iChat, Kik, TextPlus, TextFree.
- Data analysis. Apart from data listed above, BlackLight has ability to demonstrate data from the following areas of iOS device.
  - Phone; all data explicit to iPhone such as recent calls, voicemails, voice memos, favourites.
  - Application data; user explicit application files stored within the application.
  - Contacts.
  - Locations; chronological list of all GPS data from Google Maps, Apple Maps, Foursquare, Kik, Whatsapp applications as well as data from Location Services.
- Reporting tool. A customisable report that can be saved as .pdf, .html, .docx or .txt.

- All acquired data can be exported.

#### ***4.4 EnCase Forensic***

EnCase® Forensic has been developed by Guidance® Software (Guidancesoftware, 2014). Organisation provides tools for computer investigations including intellectual property theft, compliance auditing, incident response and responding to eDiscovery requests.

##### ***4.4.1 EnCase Forensic features***

EnCase Forensic supports a broad array of platforms (Guidancesoftware, 2014); Apple iOS (logical acquisition only), RIM BlackBerry, Google Android (logical and physical acquisition), Windows Mobile Operating Systems, SIM cards, iTunes and backup files. EnCase performs precise binary image of the original media.

EnCase allows examiner to analyse the following:

- Origins of the data.
- Type of user actions that created the data.
- Time the data was last accessed.

Also it enables examiner to:

- Recover files and partitions.
- Identify deleted files.
- Analyse file signature.
- Analyse hash.
- Examine most common files in their native format.
- View registry.
- Search using different techniques.
  - Conditional search.
  - Word search.
  - Boolean search.

- GREP search (Globally search a Regular Expression and Print) (Kernighan and Pike, 1984).
- Search across various types of information such as email, system, user-generated files using three principal methods of search through raw data:
  - Index searches.
  - Tag searches.
  - Keyword searches.

The searches results are thorough across the three search methods.

- Acquire user-specific activity including internet use history, cookies, logon details and more.
- Acquire device information, contacts, call history, SMS, MMS, other messages, organiser, notes, file system.
- Create reports that are highly customisable in .rtf, .pdf or .html formats.

## ***4.5 Oxygen Forensic Suite***

Oxygen Forensic® has been developed by Oxygen Software (Oxygen-forensic, 2014). This company delivers advanced forensic data examination tools for mobile devices. Oxygen forensic acquires data from mobile devices operating on Android, iOS, BlackBerry, Windows Phone and Symbian platforms and other operating systems such as Bada and Chinese Mediatek (MTK) devices.

### ***4.5.1 Oxygen Forensic Suite Standard Edition features***

The following data can be acquired and examined with use of Oxygen Forensic Suite Standard Edition (Oxygen-forensic, 2014).

- Device information.
  - Full technical description of a device.
    - Manufacturer.
    - Retail model name.
    - Platform and its revision.

- IMEI.
  - MAC addresses.
  - IMSI.
  - Serial Number.
  - Phone number and any other model specific data.
- Summary of user's accounts.
- Contact details from Contacts, Call Logs, Messages, Skype, chat and other applications.
- Call logs, SMS, MMS, iMessage and other messages specific to device type. Also recovery of messages from iOS, Android OS and Symbian OS devices.
- Calendar and tasks entries.
- File System.

The investigator can browse through a device's file system to access and examine user's photographs, videos, documents, device databases and any other files stored on the mobile device's memory. Oxygen Forensic comes with built-in text, hex, multimedia, SQLite, Plist viewers, geo-location and Exif extractors.

- Exif is Exchangeable image file format (JEITA, 2002), industry standard introduced by Japan Electronics and Information Technology Industries Association. This standard is for file formats used in images, sounds and tags including geo-location tags in digital cameras and other hardware processing image and audio files recorded by digital equipment.
- Reporting tool.  
Highly customisable report can be availed of and generated in .pdf, .xlsx, .html, .rtf and .xml file formats.

#### ***4.5.2 Oxygen Forensic Suite Analyst Edition features***

Oxygen Forensic Suite Analyst Edition provides all features that investigator can avail while using Standard Edition extended with features below (Oxygen-forensic, 2014).



- Contact details from Contacts, Call Logs, Messages, Skype, chat and other messaging, social media and call-feature applications such as Facebook, WhatsApp and Viber can be aggregated.
- Applications.
 

Ability to retrieve and list user data and files from pre-installed and user applications along with files created by these applications. Investigator may:

  - Retrieve logins and passwords to the application.
  - Find geo-location of the last run.
  - Inspect all used and created application files.
  - Know exactly when the application was used.
  - Access system and user applications.
- Dictionaries.
 

This feature allows the examiner to access all words that were ever inputted in device messages, notes and calendar. This is user's dictionary created during use of the device by its owner.

  - View of all words inputted by the user.
  - Reveal passwords.
  - Simulate possible phrases.
  - Change language if required.
  - Estimate frequency of word usage.
  - Reveal words order.
- Global search.
 

It is highly customisable search engine that allow investigator look for text, phone numbers, emails, geo coordinates, IP addresses, MAC addresses, Credit Card numbers. This feature enables to search data in a single device, all devices allocated to the case or all acquired devices. Also search can be applied by:

  - Query.
  - Boolean term.
  - Any predefined pattern.
  - Keyword list manager, custom list of terms for which search is performed simultaneously.

- **Link and stats.**  
This feature allows examining social interactions and connections between mobile devices of users under investigation.
- **Passwords.**  
Section demonstrates user details acquired from default secure storage such as keychain database or applications files. This feature is available for iOS and Android devices.
- **Chinese phones support based on Mediatek chipset.**
- **Guide to automate Android device rooting for access to all data set. Rooting android device gives the following advantages:**
  - Access to full file system stored on both built-in memory and memory card.
  - Access to application data including logins, passwords, history, cache.
  - Information on past geo-location information.
  - Access to removed data in database tables.

Supported Android operating systems are 1.6-2.3.4 and 3.0-4.2.2.
- **Timeline.**  
Investigator can view acquired data in a chronological way. This feature works on a single device or multiple devices allocated to a case.
- **Data Viewers is an extension of feature available in Standard Edition. It allows exploring actual and removed data stored in databases and other files like property files (iOS).**
- **Web Connections & Locations.**
- **Feature combines data from Wi-Fi connections (SSID, BSSID), IP connections (Wi-Fi, GPRS, LTE including VPN, router, DNS data) and GPS data with Location services thus maps displaying visited places and routes can be created.**

## ***4.6 Conclusion***

This chapter discussed data acquisition methods classification as per “Guidelines on Mobile Device Forensics” drafted by Rick Ayers of National Institute of Technology of United States Department of Commerce, Sam Brothers of United States Customs and Border Protection and Wayne Jansen of Booz-Allen-Hamilton (Ayers et al., 2013). The majority of the chapter is focused on three forensic software products made available to the researcher. Detailed features of each of the tools were listed. All of these tools operate at logical level of extraction and all of them offer the same set of features in majority. Some of them have extra options like Oxygen’s Global Search, Password Recovery or Android Rooting guide. However, for purpose of this research the essential requirement for forensic software was acquisition of file system which all software products demonstrate.

The following chapter reviews research in this area of smart phone operating systems and use of cloud storage applications.

## **5 LITERATURE REVIEW**

### ***5.1 Introduction***

Chapter 2 detailed network and security architecture of cloud storage providers. Their compliance with the highest security standards and the top level of services they provide. In Chapter 3 mobile operating platforms were discussed. Both claim their systems to be secure and easy to use. This chapter will focus on concerns, advantages and previous researches of cloud storage technology and mobile operating systems.

### ***5.2 Mobile Cloud Computing***

There are a lot of concerns surrounding the use of mobile cloud computing. First of all, performance issues. Smart phones are getting bigger by the size and by the computational power. The trade-off for this is battery life expectation and operational memory (Alwan et al. 2013; Hu et al., 2013). Smart phones handle multiple applications and some of them or most of them depending on users' preferences are working in real time with high frequency utilising virtual memory or scanning all files. These processes affect other processes and users face delay times as a result of RAM deficiency or shorter battery life. Another concern is quality and mobile network coverage. Although, in urban areas this issue is not so common, there are black holes here and there. Or signal may be blocked by high buildings or thickness of the walls. In this scenario, users will see latency while accessing network as well as poor battery performance due to device increased power supply to aerial system to increase the levels of signal reception. To address some of these concerns network operators improve their network architecture, install additional signal boosters. On the other hand, cloud storage providers attempt to utilise partitioning and offloading techniques between client side and server side. The concept of partitioning is to divide the workload of applications between mobile device and cloud servers.

One of the key concerns is end user device handling. Industry can avail of mobile device management platforms but the end user does not have this option. MDMs allow enforcement of number of features including security policies such as discussed in Chapter 3. However, for end users security of their mobile devices is their own responsibility. There are number of security measures that mobile operating systems made available to end users and which they can implement (Cummins et al., 2012; Ahmad et al., 2013, Olivier and Pieterse, 2013). Depending OS provider features vary but there are essential ones that all platforms have in common. These features as well as recommendation are as follows.

- Password protection.
- Application of system updates which provide security updates.
- Turning off wireless features such as Wi-Fi, Bluetooth or portable hotspot when not in use.
- Enable data wipe when incorrect password is entered multiple times.
- Minimise notifications that appear on the screen while it is locked.
- Do not root or jail-brake the mobile device.
- Do not enter and personal information on the mobile device.

Security of third party applications installed and used on mobile devices is another concern. This was discussed in detail in Chapter 3. Research in this area shows the importance of application sandboxing and issues with applications vetting process (Ahmad et al. 2013). While Apple make efforts to ensure security of their operating system and security of applications running on it in a number of ways, Android platform is an open source platform (Jeter and Mishra, 2013). Also due to its popularity it is more likely to be infiltrated via poorly vetted third party applications.

For the industry the key concern is commercialisation of IT. Bring your own device trend that emerged recently (Leavitt, 2013), brings a range of new risks. Android mobile device users can root their devices in order to gain administrator privileges and install applications from unknown sources. iPhone users can jail-brake theirs for mobile phones for the same purpose. Leavitt lists new approaches to security such as MDM platforms and Mobile Application Management (MAM) that these platforms

provide. MAM tool in other words is an equivalent of App Store or Google Play but the advantage for information security officers lies with the fact that it is managed internally within the business. This allows setting up corporate application store with applications that were evaluated internally. The other advantage of MDM is ability to whitelist and blacklist applications so that users will be prevented from using certain applications. This can protect the image of the company as some users may access applications with sexual or violent content or games. If the company handles highly sensitive data, administrators can blacklist applications that store content for their users. This addresses cloud computing storage concerns relating to location of the data stored, who can access it and in case of any legal disputes, jurisdictional issues.

### ***5.3 Conclusion***

This chapter discussed key concerns of mobile cloud computing as well as research performed so far. It also reviewed techniques and methods to protect corporate networks and resources. A list of recommendation for end user was revealed in order to promote and increase secure use of smart phones and applications that are installed on mobile devices.

## **6 EXPERIMENTATION & EVALUATION**

### ***6.1 Introduction***

The purpose of the experiment was to evaluate the security level of cloud storage applications for smart phone devices based on Apple and Android operating system. In order to perform the evaluation forensic software was obtained. The experiment was designed to capture a various scenarios that a device's state can be in to evaluate its impact on the date extracted. Also thorough analysis of extracted data was conducted in search of artefacts and any other relevant information that may be used to compromise user's cloud storage.

Nowadays, corporate users' devices are administered and monitored by Mobile Device Management platforms such as AirWatch, Mobile Iron or BlackBerry Enterprise Servers (Gartner, 2013). These platforms allow administrator forcing of a device password protection in order to secure data stored on devices if they are lost or stolen (AirWatch, 2014; MobileIron, 2014; BlackBerry 2013). Among a number of tools these platforms give to administrators, there are some that relate to secure handling and managing of enrolled mobile devices. The ones that are essential are GPS location services that give administrators the option to track devices and remote wipe options which are either erasure of the entire data on the device (restore to factory settings) or removal of enterprise data only.

There are number of scenarios that may lead to a device getting into the hands of malicious users or simply an individual unaware what data may be held on a device that they have found. In this research a possible scenario is one by which a malicious person wants to acquire data from a mobile device user in a way that will allow continuous access to user's data stored in the cloud.

## ***6.2 Forensic Software Installation***

### ***6.2.1 BlackLight forensic software installation***

BlackBag offers a 30-day trial of their BlackLight software. The demo gives the tester a full feature set to avail of during tests.

After application for a demo, an email was received with a URL to the software download site as well as license key. Once the software was downloaded and installed and started for first time there was an option to plug in a USB dongle or key in Demo license key. After demo license key was entered software was ready to use.

Forensic software version: BlackLight 2013 Release 3.

In this research BlackLight was found to be the most comprehensive software tool used. It was fast to acquire data off the smart phone and results were easily readable and interpreted. It displayed the file system in a hierarchical way that was easy to analyse. The data acquisition lasted a couple of minutes. Further data processing lasted around 45 minutes. For data processing the smart phone was not required.

### ***6.2.2 EnCase Forensic software installation***

Guidance Software does not offer trials or demos. Instead, they offer heavily discounted academic licenses.

Once the purchase was concluded, email with download and installation instruction as well as license key was received. The software was downloaded and installed. After initial start of the software, tester clicked on upper right dropdown menu and selected Activate Electronic License... An Activate Electronic License dialog window opened and the license key was inputted along with tester's email address. In next step a License Request file was generated and tester submitted it using link received in the email. Another email was sent including License Activation file and further



instructions. License Activation file was saved in to the same folder where License Request file resided. Then in the EnCase Activation Electronic License dialog window tester chose Finish to complete activation process and restarted software. EnCase Forensic can be installed on up to three machines.

Forensic software version: EnCase v7.09.03.

EnCase data acquisition was as fast as for BlackLight, Time to process acquired data was around 45 minutes as well. However, the analysis of the file structure and artefacts was cumbersome and not easy.

### ***6.2.3 Oxygen Forensic software Standard Edition installation***

Oxygen Software provides 180 days limited demo on their Oxygen Forensic software.

On application for Oxygen Forensic Suite 2014 (freeware) email with download and installation instruction as well as license key and customer ID for support purposes was received. Oxygen software was downloaded and installed. On the initial start of the software, tester selected Service then Enter Key from the menu. The registration form opened and license key was pasted and saved. Oxygen Forensic Suite was restarted to apply a new license key. Demo license allows installing software on two machines.

Forensic software version: Oxygen Forensic Suite 2014 Standard Edition 6.1.0.

Oxygen Forensic proved to be the least preferred software. It took much longer to acquire data so for the test case scenario it would not meet the expectation. Processing of acquired data was at the same level as BlackLight and EnCase. The results of processing of the evidence and the file structure presented to the researcher were similar to the ones provided by BlackLight.

### ***6.3 Experimentation***

This chapter discusses preparation of data set, test case scenarios including simulation of real life use of smart phones and cloud storage applications and files stored in the cloud. Test expectations are listed in this chapter and analysis of data acquired with use of forensic software tools.

#### ***6.3.1 Data Set***

A data set has been prepared for use with cloud storage. Data set consisted of twenty files.

- Four word files (.doc and .docx).
- Four picture files (.jpg).
- Four Adobe Reader files (.pdf).
- Four music files (mp3).
- Four video files, these files were different for Apple device and Android device due to compatibility issues i.e. Apple device does not support .3gp files and Android device does not support quick time (.mov) files.

Filename for each cloud storage application and smart phone tested were changed.

#### ***6.3.2 Transactions on files***

Cloud storage as a service is utilised in a number of ways. Users use it to back up their files, to access them anywhere they are and from any hardware they can use such as PC, laptop, smart phone or tablet. They upload, download, edit, share and remove files from their cloud storage. For the purpose of this research the following transactions were executed on files to simulate real life use of the cloud storage. The order and transactions on files acted upon are listed in the table 6.1. The table consist of files used for Dropbox cloud storage application installed on iPhone. The naming convention reflects cloud storage provider and operating system of a mobile device.

File name and type	Transaction
DB_iOS_01.doc	File viewed.
DB_iOS_02.docx	File viewed and deleted.
DB_iOS_03.docx	File viewed and saved for offline access.
DB_iOS_04.docx	No action.
DB_iOS_05.jpg	File viewed.
DB_iOS_06.jpg	File viewed and deleted.
DB_iOS_07.jpg	File viewed and saved for offline access.
DB_iOS_08.jpg	No action.
DB_iOS_09.pdf	File viewed.
DB_iOS_10.pdf	File viewed and deleted.
DB_iOS_11.pdf	File viewed and saved for offline access.
DB_iOS_12.pdf	No action.
DB_iOS_13.mp3	File viewed.
DB_iOS_14.mp3	File viewed and deleted.
DB_iOS_15.mp3	File viewed and saved for offline access.
DB_iOS_16.mp3	No action.
DB_iOS_17.mov	File viewed.
DB_iOS_18.mov	File viewed and deleted.
DB_iOS_19.mov	File viewed and saved for offline access.
DB_iOS_20.mov	No action.

**Table 6.1 File names and file transactions**

### ***6.3.3 Smart phone device state***

For each device and cloud storage application the following scenarios was determined.

- First device state.  
Data set has been synchronised with the device and device remains powered on.
- Second device state.  
Data set has been synchronised with the device and device has been powered off and on.
- Third device state.

Data set has been synchronised with the device and applications' cache has been cleared. For this test device was previously wiped.

- Fourth device state.

Data set has been synchronised with the device, applications' cache has been cleared and device has been powered off and on. For this test device was previously wiped.

Due to software limitations for all scenarios device passcode lock has been unlocked or not set up. The real life scenario would be when a user leaves their smart phone unlocked and unattended or passcode is known to potential malicious individual.

#### ***6.3.4 Tests expectations***

Each cloud storage application tested against various mobile devices states and transactions performed on files was expected to return as follows.

- Files viewed.
  - Files and thumbnails should be saved in cache of cloud storage application.
  - For device with cleared cache, there should be no records of files.
- Files viewed and deleted.
  - No records of files.
- Files viewed and saved for online access.
  - Files and thumbnails should be saved in cache of cloud storage application.
  - For device with cleared cache, there should be no records of files in cache.
  - Files should be saved in respective application in which each file was saved (iOS device) or smart phone memory (Android device).
- No action.
  - No records of files.

### ***6.3.5 Analysis of database files for individual cloud storage applications***

Thorough analysis of SQLite and database files will be performed in order to establish what details are stored within the application files by means of manual examination of files.

The expected outcome of the analysis is that no information that may be used to compromise user's cloud storage should be found. This includes user's email address, password or any other detail that directly may give malicious individual access to user's cloud storage.

### ***6.3.6 Hardware and software***

The following hardware and software was used to conduct the experiment.

Smart phone operating system was the key driver behind the choice of mobile devices. iOS and Android OS have the lion's share of the market. The researcher himself is iPhone user so the choice was to use iPhone 4S for experiments. Simplified technical specification of iPhone 4S is included in the table 6.2.

<b>Feature</b>	<b>iPhone 4S</b>
Operating system	iOS 7.0.4
Internal memory	16GB
Memory card	No

**Table 6.2 Smartphone features**

Cloud storage applications and their versions are listed in table 6.3.

Application	iPhone 4S	PC Client
Dropbox	3.0.2	2.4.7
Box	2.8.7	4.0 (Web based application client)
SugarSync	4.1.0.1	2.0.42.120603.20131120

**Table 6.3 Cloud storage mobile and PC client versions**

Forensic software tools used for the experimentation and their versions are listed in table 6.4.

Forensic Tool	Version
BlackLight 2013 (iOS only)	Release 3
EnCase Forensic	7.09.03
Oxygen Forensic Suite 2014 Standard Edition	6.1.0

**Table 6.4 Forensic software tools and versions**

Dell Latitude E4200 laptop with Windows 7 SP1 Enterprise Edition was used to install forensic software tools.

## **6.4 Test Outcomes**

The following are the test case results from the defined device.

### **6.4.1 iOS Applications**

All applications installed on the iPhone created their respective folders in */private/var/mobile/Applications*. Files and applications' metadata was stored in this location. This is stored in user's partition (Johnson, 2011).

### 6.4.1.1 Dropbox

Data set files saved for offline access were stored within different applications due to design of the application itself. The following applications were used in the test.

- iBooks application used to store .pdf file.
- Pages application used to store .docx file.
- iMovie application used to store .mov file.
- Library used to store .jpg file.
- iMovie application used to store .mp3 file.

Dropbox application created a folder in user's partition. Files from data set were recovered from */Library/Caches/Dropbox* folder and include:

- Viewed .doc file and viewed and saved for offline access .docx.
- Thumbnails images of viewed, viewed and saved for offline access and no actioned.jpg files. Also a .jpg image file stored for offline access.
- Viewed, viewed and stored for offline access .pdf files.
- Viewed (played), viewed and stored for offline access .mp3 file.

This file was saved in Apple iMovie application. File location was */iMovie/Library/Application Support/Documents/SharedMedia/AudioFile*.

- Thumbnail images of all .mov files, apart the one that was removed. Also a .mov file saved for offline access.

This file was saved in Apple iMovie application. File location was */iMovie/Library/Application Support/Documents/SharedMedia*.

Detailed analysis of Dropbox xml property list file *com.getdropbox.Dropbox.plist* stored in */Library/Preferences* folder revealed information on user account name and email address used to set the account. It also listed three .pdf file names that were viewed on the device. Clearing the cache or powering of the device did not change data stored in these files.

Dropbox SQLite metadata repository file *Dropbox.sqlite* located in */Documents* did not reveal any interesting findings presented in Appendix A.

### 6.4.1.2 Box

Data set files saved for offline access were stored within different applications due to design of the application itself. The following applications were used in the test.

- iBooks application used to store .pdf file.
- Pages application used to store .docx file.
- Library used to store .mov file.
- Library used to store .jpg.
- Box application used to store .mp3 file.

Box created a folder on user's partition when application was installed. Files from data set were recovered from */Library/Caches/TempFiles* folder and include:

- Viewed .doc file and viewed and saved for offline access .docx.
- Viewed, viewed and saved for offline access .jpg files.
- Viewed, viewed and stored for offline access .pdf files.
- Viewed (played) and stored for offline access .mov file.

This file was saved in Apple iMovie application. However, it could not be found in */iMovie* directory.

Music file saved for offline access was stored in */Documents/SavedFiles* folder.

A number of thumbnail images were found in */Library/Caches/Thumbnails* of Box folder application. They were:

- All .jpg files.
- All .mov files.
- One .pdf file (pdf icon).
- Two .docx files (word icons).
- One .mp3 file (icon only).

All files names were different form the ones originally uploaded. File names were all numbers i.e. 12266512488.mp3.



Further analysis of xml property list file *net.box.BoxNet.plist* located in */Library/Preferences* folder did not bring interesting findings which are presented in Appendix B.

Analysis of SQLite file *BoxCoreDataStore.sqlite* located in */Documents* folder brought findings. There was data stored in the table *ZBOXBASECOREDATA* that revealed as follows:

- Original file names.
- Box uniquely assigned file names i.e. 12266512488.
- File type.
- URLs to thumbnails images and preview files.
- Masterkey.
- File size.
- Local URL string which was Box unique file name and file type i.e. 12266512488.mp3
- Streaming URL.
- SHA-1.

All that information enabled a researcher to make follow up test described in paragraph 6.4.3.

#### **6.4.1.3 SugarSync**

Data set files saved for offline access were stored within different applications due to design of the application itself. The following applications were used in the test.

- iBooks application used to store .pdf file.
- Pages application used to store .docx file.
- iMovie application used to store .mov file.
- Library used to store .jpg file.
- iMovie application used to store .mp3 file.

SugarSync created folder on user's partition when application was installed. Files from data set were recovered from the following folders in */tmp* directory:

- */cache*
  - Viewed (played), viewed and removed and viewed and stored for offline access .mp3 files.
- */http\_cache*
  - Viewed, viewed and removed and viewed and stored for offline access .doc and .docx files.
  - All .jpg files.
  - Viewed, viewed and removed and viewed and stored for offline access .pdf files.
  - Thumbnails image of a viewed (played) and stored for offline access .mp3 file.
  - Thumbnails images of viewed (played), viewed and removed and viewed and stored for offline access .mov files.
- */links*
  - Viewed (played) and stored for offline access .mov file.

Analysis of SugarSync xml property file *com.sharpcast.sugarsync.plist* stored in */Library/Preferences* revealed user email address for the account which is presented in Appendix C.

Analysis of SQLite metadata repository file *Rigno.sqlite* stored in */Documents* folder didn't reveal any useful information.

#### **6.4.2 iOS Test Outcomes**

All tested cloud based storage applications provide the same services with some differences to what files can be stored within the application storage or with other applications like iBooks for .pdf files, Pages for Word documents, iPhone's library for music and picture files or iMovie for video clips. Due to these differences Dropbox,

Box and SugarSync execute operations using their own mechanism. Table 6.4 provides holistic view of recovered files from iPhone device.

Analysis of simulation of various states of the device brought following results.

- For all cloud storage applications whether device remained powered on (RPO) or was powered off (PO), the same data set was recovered in both states.
  - From Dropbox folder the least number of files was retrieved and they were all files saved for offline access and .doc and .pdf files viewed only as expected.
  - From Box folder all files that were saved for online access were retrieved as well as .doc, .jpg and .pdf files viewed only as expected.
  - From SugarSync folders all Word documents were retrieved bar the one that was not accessed. All .jpg. and .pdf files were recovered. Music files found were these that were played, played and removed and played and stored for offline access. The exception here was played .mp3 which has been removed from cache after the device was powered off. The expectation was to recover files that were viewed and viewed and saved for offline access..
- For all cloud storage applications whether the device had cache cleared (CC) or cache cleared and was powered off (CC-PO) the outcome was similar.
  - For Dropbox no files were recovered as expected.
  - For Box only .mp3 file as it was stored within the application as expected.
  - For SugarSync clearing cache had no effect. The same data set was retrieved as listed above. This means that application did not execute clearing the cache accurately. This was not expected.

File	Dropbox				Box				SugarSync			
	RPO	PO	CC	CC-PO	RPO	PO	CC	CC-PO	RPO	PO	CC	CC-PO
01.doc	√	√			√	√			√	√	√	√
02.docx									√	√	√	√
03.docx	√	√			√	√			√	√	√	√
04.docx												
05.jpg					√	√			√	√	√	√
06.jpg									√	√	√	√
07.jpg	√	√			√	√			√	√	√	√
08.jpg									√	√	√	√
09.pdf	√	√			√	√			√	√	√	√
10.pdf									√	√	√	√
11.pdf	√	√			√	√			√	√	√	√
12.pdf												
13.mp3									√		√	√
14.mp3									√	√	√	√
15.mp3	√	√			√	√	√	√	√	√	√	√
16.mp3												
17.mov												
18.mov												
19.mov	√	√			√	√			√	√	√	√
20.mov												

**Table 6.5 Results of file recovery for iPhone device**

**RPO = Remained powered on, PO = Powered off, CC = Cleared cache, CC-PO = Cleared Cache and powered off**

### **6.4.3 Box follow up tests on iPhone**

Upon discovery of data not expected further analysis was undertaken. The focus of the researcher was the URL that used on any PC allowed downloading of a file. Any of the URL tested gave positive result. URLs listed in SQLite table were for files that were

not removed from cloud storage provider servers. Below is the example of one if the URLs:

[https://mobile-api.box.com/api/1.0/download/fs39y40jon6tl94czuyeeegsargxpzv1/12266285894?device\\_id=2541F721-BEC9-4FD5-BA37-02231479C506&device\\_name=Test%20iPhone](https://mobile-api.box.com/api/1.0/download/fs39y40jon6tl94czuyeeegsargxpzv1/12266285894?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone)

Further investigation resulted in the following pattern in the URL.

[https://mobile-api.box.com/api/1.0/download/fs39y40jon6tl94czuyeeegsargxpzv1/12266285894?device\\_id=2541F721-BEC9-4FD5-BA37-02231479C506&device\\_name=Test%20iPhone](https://mobile-api.box.com/api/1.0/download/fs39y40jon6tl94czuyeeegsargxpzv1/12266285894?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone)

URL from another test case was:

[https://mobile-api.box.com/api/1.0/download/1aexr8i10ozx54anfyn40duy7yu0372f/12266285894?device\\_id=F3825526-F756-4102-A985-E3E6D618CD64&device\\_name=Test%20iPhone](https://mobile-api.box.com/api/1.0/download/1aexr8i10ozx54anfyn40duy7yu0372f/12266285894?device_id=F3825526-F756-4102-A985-E3E6D618CD64&device_name=Test%20iPhone)

Also another iPhone handset was used to with Box application and the result of forensic investigation brought out the following URL.

[https://mobile-api.box.com/api/1.0/download/xfeny61eeytrizwm3bfc4o8bmkuqj04m/12266285894?device\\_id=5C583178-A0F0-4D8D-BA78-3F7E07595647&device\\_name=Rad%27s%20iPhone](https://mobile-api.box.com/api/1.0/download/xfeny61eeytrizwm3bfc4o8bmkuqj04m/12266285894?device_id=5C583178-A0F0-4D8D-BA78-3F7E07595647&device_name=Rad%27s%20iPhone)

Examination of these URLs sought for a further decoupling of the URL and an attempt to name and source individual parts of the URL.

- Download part <https://mobile-api.box.com/api/1.0/download/>
- Some sort of token allocated to each instance of the application even if this application was installed on the same device or device was restored from the back. Each time that string had a different value. However, it always had the same number of alphanumeric characters, 32. Since this part of the URL changed with each new instance of the application installation it seems that it is generated when client connects to the server to download a

file. There was no URL for files that were removed from Box servers thus there was no need for this information on the client side.

- [xfeny61eeYtrizwm3bfc4o8bmkuqi04m.](#)
- [1aexr8i10ozx54anfyn40duy7yu0372f.](#)
- [fs39y40jon6tl94czuyeeegsargxpzv1.](#)
- File number which was actually the filename that is stored on Box servers. A study of all file numbers, and further tests within shorter or longer time intervals suggest that these number are generated whenever a Box user is uploading a file to a server. Once user uploads his or her files they get a bigger number in some sort of a sequence. It takes longer for bigger files to upload but this is not a factor in the numbering strategy that was investigated. The smallest file number that a file received was 12266285894 and the biggest was 12407061476. Further file uploads resulted in file numbers getting value of 14449398854 and later 14914355710.
- Device ID, similarly to token above is generated each time the application was installed or device was restored from the back up.
  - [?device\\_id=5C583178-A0F0-4D8D-BA78-3F7E07595647.](#)
  - [?device\\_id=F3825526-F756-4102-A985-E3E6D618CD64.](#)
  - [?device\\_id=2541F721-BEC9-4FD5-BA37-02231479C506.](#)

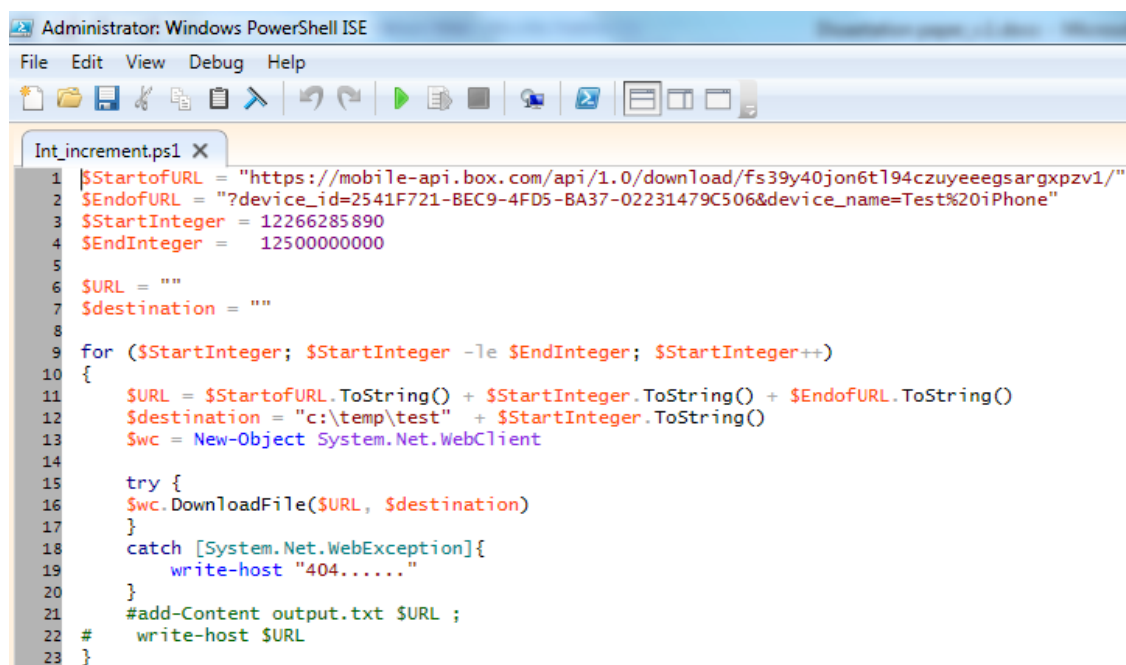
Study of another xml property file *com.apple.lsdidentifiers.plist* on user partition in folder */Isd* folder showed that device ID is generated at each instance of Box application installation. The below is the string extracted from plist file.

```
LSVendorIdentifier^LSApplications_$2541F721-BEC9-4FD5-BA37-02231479C506;^net.box.BoxNet0
```

- Device name was a device name given to the device by the researcher.

These findings lead to development of a simple script to see if user's data in the cloud could be compromised. The script was means to an automated download of all data stored by the user in the cloud during the script execution. The code depicted in figure 6.1 was written in .NET Framework and executed in Powershell Integrated Scripting Environment. The code split the URL between *download part/token* and *device ID&device name*. The integer was a file number, the lowest taken from SQLite table

and was incremented by 1 and attempted to download file and save it in chosen location. This exercise proved to be successful. The limitation was that files were saved in none-file type format as seen in Appendix D. This would add complexity for a malicious individual but another script could be developed to test a file against known file types or use file headers to ease this process. Another finding which was not unexpected was each of URLs created in SQLite file whether the device was wiped, restored from the backup or created in SQLite database on another iPhone worked. Another test was run to see if new files added to cloud storage can be downloaded executing script against URL that was not used by any device i.e. after device was wiped and a new instance of Box application was installed. This proved to be successful again. The reason for this is that one user may have two different devices i.e. business phone and private phone. This indicates that the URL is generated on the server side and remains there forever. Servers obtain device details initially (device ID and device name) and create a token for the URL. Files are saved during uploading to a server in a sequence and remain on the server in that format until they are removed. This concludes that once an individual obtains access without owner being aware of it they can access and download data from user's account.



```
Administrator: Windows PowerShell ISE
File Edit View Debug Help
Int_increment.ps1 X
1 $StartofURL = "https://mobile-api.box.com/api/1.0/download/fs39y40jon6t194czuyeeegsargxpzv1/"
2 $EndofURL = "?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone"
3 $StartInteger = 12266285890
4 $EndInteger = 12500000000
5
6 $URL = ""
7 $destination = ""
8
9 for ($StartInteger; $StartInteger -le $EndInteger; $StartInteger++)
10 {
11     $URL = $StartofURL.ToString() + $StartInteger.ToString() + $EndofURL.ToString()
12     $destination = "c:\temp\test" + $StartInteger.ToString()
13     $swc = New-Object System.Net.WebClient
14
15     try {
16         $swc.DownloadFile($URL, $destination)
17     }
18     catch [System.Net.WebException]{
19         write-host "404....."
20     }
21     #add-Content output.txt $URL ;
22     # write-host $URL
23 }
```

Figure 6.1 Script to download files from Box cloud storage

## **6.5 Conclusion**

This chapter described the approach to test cases scenarios, use of forensic tools, and analysis of acquired data and outcomes of the research. Data stored in the cloud synchronised with the device is well handled within Dropbox and Box applications and bar the fact that it is poorly handled within SugarSync application. The real problem was in underlying data for application to work efficiently and seamlessly for the users' advantage in Box application. As described in Box follow up tests there is a major security vulnerability that may affect one user that is targeted. However, this research leads to conclusion that there is a potential to infiltrate the whole data storage of all Box users. Malicious individual with an access to powerful machines and excellent scripting skills could develop a sophisticated script. This script could decouple the URL obtained from data acquired and execute the code that would generate tokens as well as device ID details and utilise dictionary tables for device names. This potentially may bring results in gaining access to data stored on Box servers for all users.



## **7 CONCLUSION**

### ***7.1 Introduction***

Smart phone devices using cloud storage applications should be trusted by the client. The ability to upload, download and share content on-the-go virtually anywhere poses a risk to users. Smart phones became inseparable devices in users' lives to a great extent. Safeguarding of them and securing data stored on them is an unnoticed and not addressed concern to many.

The purpose of this project was to uncover any potential security vulnerabilities when using cloud storage application on a mobile device. Upon findings of security flaws an attempt to exploit was the secondary goal of this research.

### ***7.2 Research Definition & Research Overview***

This research carried out an investigation of consequences of cloud storage mobile applications quality and reliability in the context of proliferation of smart phone devices and cloud storage services. Acquired data was subjected to thorough analysis of artefacts that cloud storage applications may have created on smart phone devices.

At the commencement of the project the following research objectives were identified.

- Uncover any potential security flaws when using cloud storage applications on a mobile device.
- Extraction of data using forensic software.
- Detailed analysis of cloud storage files structure and hierarchy.
- Preparation of data set consisting of a number files that will be uploaded to cloud storage.
- Simulation of real life transaction of data stored in the cloud.
- Development of number of test cases to simulate real life scenarios.
- Detailed review of the forensic software tools.

- Install of the forensic software products and familiarisation with them.
- Thorough literature review.
- Recommendation of a solution to avoid any security flaws.

### ***7.3 Contributions to the Body of Knowledge***

This project contributes to the body of knowledge related to security cloud storage applications on smart phone devices. Qualitative primary research being forensic acquisition of data off smart phone devices brings interesting findings. Dropbox and Box providers of cloud storage services stored files on the device in a secure manner while SugarSync was not proficient in providing the same level of security.

A second contribution proposed by this project is discovery of a security vulnerability of Box mobile cloud application that may lead to user's data being compromised. Unsecure storage of metadata should be addressed by the developers as it may lead to data leakage of all Box cloud storage users.

### ***7.4 Experimentation, Evaluation and Limitation***

This results of primary research at first glance indicated that mobile applications for two cloud storage vendors handled users' data on the devices as per best practises. Files that users download for offline access for Dropbox and Box are only files stored locally on users' devices when cache is cleared. SugarSync does not meet the expectations since regardless of the cache being cleared or not, application stores almost all data that users' access. This does not depend if files are viewed only or viewed and removed, they can be found in SugarSync folders.

Examination of findings that lead to secondary research for seemingly secure data handler that Box mobile application was considered uncovered major security flaw as discussed in Chapter 6. This research concludes as follows. The mobile device should

not store any information locally which will enable access to online content from unauthorised and unauthenticated user. The findings have shown that in certain circumstances a non-complex target address is stored locally which can be extracted using forensic tools. The address obtained can be used to gain access all files stored in user's cloud storage as well as files that the unaware user will upload in the future.

To avoid this situation recommendations are as follows.

- The target address should not be stored locally.
- The address should only be generated when the file is requested or uploaded. In this case the address should be removed afterwards.
- Alternatively, the target address could be encrypted if it required locally. Downside of this solution is increased computational overhead of encrypting data on the device. Also this method cannot utilise encryption techniques completely without affecting performance of the device.
- The target address should be non-trivial.
- Provider's servers have much more computational power and could generate more complex file structures, eliminate trivial target addresses or utilise cryptographic methods to their best.
- Any target addresses generated should always require authentication access to the stored data.

For end users the ultimate recommendation is not to use Box cloud storage services or if they wish to use it implement extra security measures.

- Users should keep their devices with them at all times.
- Set up password protection and keep their mobile devices locked when away from them.
- Use applications that work as containers for other applications which enforce additional layer of encryption. Example here can be a Boxcryptor.

## ***7.5 Future Work & Research***

The recommendation for future work is to investigate further and build on this research. Throughout this study, it was proved the use of cloud storage services on

mobile devices is insecure. The lack of proper controls of application data handling may result in cloud storage vendor data being compromised. Also a lot of data artefacts including details like Masterkeys or SHA-1 keys were uncovered during analysis of SQLite files acquired from Box application that should be further investigated.

## **7.6 Conclusion**

Smart phone security should be essential to any smart phone user. The security of smart phones in many cases relies on the way users handle their mobile devices themselves. Current environment and shift to cloud computing allowing users to store data within cloud storage and access it whenever they wish prompts for protection of the devices those users utilise for access to that data. Firstly more effort should put in choice based on research on security of the cloud storage vendors and the applications they provide. Additional security measures can be put in place by means of additional applications or utilisation of built-in extra encryption in the applications themselves if offered. However, there is not much more users themselves can do. Major responsibility lies with cloud storage vendors, their network architecture and security, and the expertise and the experience of application developers.

This study sought to discuss the concerns in the area of mobile cloud computing, research the subject of smart phones and mobile applications security with use of forensic tools. Subsequently analyse data and artefacts stored on the mobile devices to uncover any security vulnerabilities and make recommendations for future research.

## BIBLIOGRAPHY

ABI Rresearch. 2013. *Personal Cloud Storage Accounts Total One Billion in 2013, Generating 685 Petabytes*. [online] Available at: <https://www.abiresearch.com/press/personal-cloud-storage-accounts-total-one-billion-> [Accessed: 21 Mar 2014].

Agarwal, A. 2012. Security update & new features. *The Dropbox Blog*, [blog] 31 July 2012, Available at: <https://blog.dropbox.com/2012/07/security-update-new-features/> [Accessed: 21 Mar 2014].

Ahmad, M. S., Musa, N. E., Nadarajah, R., Hassan, R. and Othman, N. E. 2013. Comparison between android and iOS Operating System in terms of security. *Information Technology in Asia (CITA), 2013 8th International Conference on*, pp. 1-4. Available at: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6637558&queryText%3DComparison+Between+Android+and+iOS+Operating+System+in+terms+of+Security> [Accessed: 5 Jan 2014].

Airwatch. 2014. *Mobile Device Management*. [e-book] Available through: <http://www.air-watch.com/solutions/mobile-device-management> [http://www.air-watch.com/downloads/brochures/AirWatch\\_brochure\\_mobile\\_device\\_management.pdf](http://www.air-watch.com/downloads/brochures/AirWatch_brochure_mobile_device_management.pdf) [Accessed: 22 Mar 2014].

Akamai. 2014. *Cloud Services, Enterprise, Mobile, Security Solutions | Akamai*. [online] Available at: <http://www.akamai.com/> [Accessed: 21 Mar 2014].

Alwan, N., Lami, I. A. and Oriaku, C. 2012. The readiness of mobile operating systems for cloud computing services. *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on*, pp. 49-55. Available at: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6459717&queryText%3DThe+readiness+of+mobile+operating+systems+for+cloud+computing+services> [Accessed: 12 Nov 2013].

Amazon.com. 2014. *Global Infrastructure*. [online] Available at: <http://aws.amazon.com/about-aws/globalinfrastructure/> [Accessed: 21 Mar 2014].

Android Developer. 2014. *Distribute Apps | Android Developers*. [online] Available at: <http://developer.android.com/distribute/index.html> [Accessed: 22 Mar 2014].

Apple. 2008. *Apple - Press Info - iPhone 3G on Sale Tomorrow*. [online] Available at: <https://www.apple.com/pr/library/2008/07/10iPhone-3G-on-Sale-Tomorrow.html> [Accessed: 20 Mar 2014].

Apple. 2009. *Apple - Press Info - Apple Announces the New iPhone 3GS—The Fastest, Most Powerful iPhone Yet*. [online] Available at:

<https://www.apple.com/pr/library/2009/06/08Apple-Announces-the-New-iPhone-3GS-The-Fastest-Most-Powerful-iPhone-Yet.html> [Accessed: 20 Mar 2014].

Apple. 2010. *Apple - Press Info - Apple Previews iPhone OS 4*. [online] Available at: <https://www.apple.com/pr/library/2010/04/08Apple-Previews-iPhone-OS-4.html> [Accessed: 20 Mar 2014].

Apple. 2011. *Apple - Press Info - Apple Launches iPhone 4S, iOS 5 & iCloud*. [online] Available at: <https://www.apple.com/pr/library/2011/10/04Apple-Launches-iPhone-4S-iOS-5-iCloud.html> [Accessed: 21 Mar 2014].

Apple. 2013. *Apple - Press Info - iPhone 5s & iPhone 5c Arrive on Friday, September 20*. [online] Available at: <https://www.apple.com/pr/library/2013/09/16iPhone-5s-iPhone-5c-Arrive-on-Friday-September-20.html> [Accessed: 21 Mar 2014].

Apple. 2014. *Apple - iPhone in Business - IT Center - Security*. [online] Available at: <http://www.apple.com/iphone/business/it/security.html> [Accessed: 22 Mar 2014].

Apple Developer. 2014. *App Review - Apple Developer*. [online] Available at: <https://developer.apple.com/app-store/review/> [Accessed: 22 Mar 2014].

Apple Developer. 2014. *Cocoa Touch - iOS Technology Overview - Apple Developer*. [online] Available at: <https://developer.apple.com/technologies/ios/cocoa-touch.html> [Accessed: 20 Mar 2014].

Apple Support. 2014. *Apple security updates*. [online] Available at: <http://support.apple.com/kb/HT1222> [Accessed: 21 Mar 2014].

Ayers, R. Brothers, S. and Jansen, W. 2013. *Guidelines on Cell Phones Forensics*. [e-book] Available through: [http://csrc.nist.gov/groups/SNS/mobile\\_security/publications.html](http://csrc.nist.gov/groups/SNS/mobile_security/publications.html)  
<http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf> [Accessed: 21 Mar 2014].

Biswas, D. 2012. "Privacy policies change management for smartphones". *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 9<sup>th</sup> IEEE International Conference on*, pp. 70-75. URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6197606>

Blackbagtech. 2014. *About Us*. [online] Available at: <https://www.blackbagtech.com/about.html> [Accessed: 22 Mar 2014].

Blackbagtech. 2014. *Native Mac, iPad and iPhone Forensic Analysis Software, BlackLight by BlackBag Technologies*. [online] Available at: <https://www.blackbagtech.com/software-products/blacklight.html> [Accessed: 22 Mar 2014].

Blackberry. 2013. *Built to Keep Your Business Moving: Multi-OS Enterprise Mobility Management*. [e-book] Available through: <http://us.blackberry.com/business/software/bes/overview.html>

[http://us.blackberry.com/content/dam/blackBerry/pdf/business/english/bes10/BB\\_Ent\\_EMM%20brochure\\_US.pdf](http://us.blackberry.com/content/dam/blackBerry/pdf/business/english/bes10/BB_Ent_EMM%20brochure_US.pdf) [Accessed: 22 Mar 2014].

Box. 2014. *About Us / Box*. [online] Available at: <https://www.box.com/about-us/> [Accessed: 21 Mar 2014].

Box. 2014. *Box Security Overview*. [online] Available at: <https://www.box.com/resources/case-studies/security-whitepaper/> [Accessed: 21 Mar 2014].

Bracetti, A. 2012. *The 7 Best Smartphones Announced At Mobile World Congress 2012*. [online] Available at: <http://www.complex.com/tech/2012/02/the-7-best-smartphones-announced-at-mobile-world-congress-2012#2> [Accessed: 23 Mar 2014].

Brewmp Developer. 2014. *Reference / Brew MP Developer*. [online] Available at: [https://developer.brewmp.com/reference/api/brew\\_mp\\_1.0.2/telephony](https://developer.brewmp.com/reference/api/brew_mp_1.0.2/telephony) [Accessed: 21 Mar 2014].

Brothers, S. 2007. *iPhone Tool Classification*. [online] Available at: <http://www.appleexaminer.com/iPhoneiPad/ToolClassification/ToolClassification.html> [Accessed: 21 Mar 2014].

Buxton, B. 2014. *Detail*. [online] Available at: <http://research.microsoft.com/en-us/um/people/bibuxton/buxtoncollection/detail.aspx?id=40> [Accessed: 22 Mar 2014].

Cha, B. 2009. *All T-Mobile retail stores to carry G1*. [online] Available at: [http://news.cnet.com/8301-17938\\_105-10149502-1.html](http://news.cnet.com/8301-17938_105-10149502-1.html) [Accessed: 22 Mar 2014].

CompTIA. 2014. *Complimentary Research Reports*. [online] Available at: <http://www.comptia.org/research/complimentary-research-reports.aspx> [Accessed: 21 Mar 2014].

Corelis. 2013. *JTAG Tutorial*. [online] Available at: [http://www.corelis.com/education/JTAG\\_Tutorial.htm](http://www.corelis.com/education/JTAG_Tutorial.htm) [Accessed: 21 Mar 2014].

Cummins, E., Gonzalez, C., Lim, S., Oh, T., Ramachandran, R. and Stackpole, B. 2012. Best security practices for android, blackberry, and iOS. *Enabling Technologies for Smartphone and Internet of Things (ETSIoT), 2012 First IEEE Workshop on*, pp. 42-47. Available at: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6311252&queryText%3DBest+Security+Practices+for+Android%2C+BlackBerry%2C+and+iOS> [Accessed: 4 January 2014].

Dropbox for Business security: A Dropbox whitepaper. 2014. [e-book] Dropbox. Available through: <https://www.dropbox.com/business/features> Anonymous. 2014. [pdf] <https://www.dropbox.com/s/e9kk0cbiopxh2m4/Security%20Whitepaper.pdf> [Accessed: 21 Mar 2014]. [Accessed: 21 Mar 2014].

Dropbox. 2014. *Dropbox - About Dropbox*. [online] Available at: <https://www.dropbox.com/about> [Accessed: 21 Mar 2014].

- Dropbox. 2014. Dropbox - News. [online] Available at: <https://www.dropbox.com/news/company-info> [Accessed: 21 Mar 2014].
- Edgecast. 2014. *CDN - Content Delivery Network | EdgeCast*. [online] Available at: <http://www.edgecast.com> [Accessed: 21 Mar 2014].
- Ferdowsi, A. 2011. Yesterday's Authentication Bug. *The Dropbox Blog*, [blog] 20 June 2011, Available at: <https://blog.dropbox.com/2011/06/yesterdays-authentication-bug/> [Accessed: 21 Mar 2014].
- Gartner. 2009. *Gartner Says Worldwide Smartphone Sales Reached Its Lowest Growth Rate With 3.7 Per Cent Increase in Fourth Quarter of 2008*. [online] Available at: <http://www.gartner.com/newsroom/id/910112> [Accessed: 22 Mar 2014].
- Gartner. 2013. *Gartner Says Cloud Computing Will Become the Bulk of New IT Spend by 2016*. [online] Available at: <http://www.gartner.com/newsroom/id/2613015> [Accessed: 21 Mar 2014].
- Gartner. 2013. *Magic Quadrant for Mobile Device Management Software*. [online] Available at: <http://www.gartner.com/technology/reprints.do?id=1-1FRVS5W&ct=130524&st=sb> [Accessed: 22 Mar 2014].
- Google. 2014. Data center locations – Data Centers – Google. [online] Available at: <http://www.google.com/about/datacenters/inside/locations/index.html> [Accessed: 21 Mar 2014].
- Guidancesoftware. 2014. *About Guidance Software*. [online] Available at: <https://www.guidancesoftware.com/about/Pages/about-guidance-software.aspx?cmpid=nav> [Accessed: 22 Mar 2014].
- Haig, C. 2014. *Box OneCloud Reaches 1,000 App Milestone*. [online] Available at: <http://blog.box.com/2014/03/box-onecloud-reaches-1000-app-milestone/> [Accessed: 21 Mar 2014].
- Hoog, A. and Strzempka, K. 2011. *iPhone and iOS forensics*. Waltham, MA: Syngress/Elsevier.
- Hu, X., Leung, V., Shu, L., Yang, L. T. and Zhu, C. 2013. A Review of Key Issues That Concern the Feasibility of Mobile Cloud Computing. *Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, 2013 IEEE International Conference on*, pp. 769--776. Available at: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6682152>. [Accessed: 4 Feb 2014].
- IDC. 2014. *Android and iOS Continue to Dominate the Worldwide Smartphone Market with Android Shipments Just Shy of 800 Million in 2013, According to IDC - prUS24676414*. [online] Available at: <http://www.idc.com/getdoc.jsp?containerId=prUS24676414> [Accessed: 22 Mar 2014].



IEEE Standards. 2014. *IEEE SA - 1149.1-1990 - IEEE Standard Test Access Port and Boundary-Scan Architecture*. [online] Available at: <http://standards.ieee.org/findstds/standard/1149.1-1990.html> [Accessed: 21 Mar 2014].

IHS. 2014. *Cloud- Related Spending by Businesses to Triple from 2011 to 2017 - IHS Technology*. [online] Available at: <https://technology.ihs.com/490336/cloud-related-spending-by-businesses-to-triple-from-2011-to-2017> [Accessed: 21 Mar 2014].

Iwata, Y., Masuoka, F., Momodomi, M. and Shirota, R. 1987. New ultra high density EPROM and flash EEPROM with NAND structure cell. *Electron Devices Meeting, 1987 International*, vol.33 pp. 552-555. Available from: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1487443> doi: 10.1109/IEDM.1987.191485 [Accessed: 10 Nov 2013].

JEITA. 2002. *JEITA / JEITA Standards / AV&IT Technology Standardization / Digital Cameras*. [online] Available at: [http://www.jeita.or.jp/cgi-bin/standard\\_e/list.cgi?cateid=1&subcateid=4](http://www.jeita.or.jp/cgi-bin/standard_e/list.cgi?cateid=1&subcateid=4) [Accessed: 22 Mar 2014].

Jeter, L. and Mishra, S. 2013. Identifying and quantifying the android device users' security risk exposure. *Computing, Networking and Communications (ICNC), 2013 International Conference on*, pp. 11-17. Available at: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6504045&queryText%3DIdentifying+and+quantifying+the+android+device+users%27+security+risk+exposure> [Accessed: 30 November 2013].

Johnson, D., Levinson, A. and Stackpole, B. 2011. Third party application forensics on apple mobile devices. *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, pp. 1-9. Available from: [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=5719010](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5719010), doi: 10.1109/HICSS.2011.440 [Accessed: 20 Nov 2013].

Kandukuri, B.R, Paturi, V. R. and Rakshit, A. 2009; "Cloud security issues," *Services Computing, 2009.SCC'09. IEEE International Conference on*. pp. 517-520.

Keizer, G. 2007. *Jobs says Apple will fight iPhone unlocking hacks*. [online] Available at: [http://www.computerworld.com/s/article/9037398/Jobs\\_says\\_Apple\\_will\\_fight\\_iPhone\\_unlocking\\_hacks](http://www.computerworld.com/s/article/9037398/Jobs_says_Apple_will_fight_iPhone_unlocking_hacks) [Accessed: 22 Mar 2014].

Kernighan, B. W. and Pike, R. 1984. *The UNIX programming environment*. Englewood Cliffs, N.J.: Prentice-Hall.

Kholia, D. and Wegrzyn, P. 2014. *Looking Inside the (Drop) Box / USENIX*. [online] Available at: <https://www.usenix.org/conference/woot13/workshop-program/presentation/kholia> [Accessed: 21 Mar 2014].

Leavitt, N. 2013. Today's Mobile Security Requires a New Approach. *Computer*, 46 (11), pp. 16-19. Available at: [http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6673977&queryText%](http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6673977&queryText%3D)

3DToday%27s+Mobile+Security+Requires+a+New+Approach [Accessed: 22 Jan 2014].

Lee, E. 2007. *17-year-old hacker unlocks iPhone's secrets*. [online] Available at: <http://www.sfgate.com/news/article/17-year-old-hacker-unlocks-iphone-s-secrets-2545113.php> [Accessed: 22 Mar 2014].

MobileIron. 2014. *MobileIron Product Overview | MobileIron*. [online] Available at: <http://www.mobileiron.com/en/datasheet/mobileiron-product-overview> [Accessed: 22 Mar 2014].

Moffitt, J., Paterson, I., Saint-Andre, P. and Smith, D. 2010. *XEP-0124: Bidirectional-streams Over Synchronous HTTP (BOSH)*. [online] Available at: <http://xmpp.org/extensions/xep-0124.html#intro> [Accessed: 21 Mar 2014].

Morrissey, S. and Campbell, T. 2010. *IOS forensic analysis for iPhone, iPad, and iPod Touch*. [New York: Apress].

Nemesis Lonestar. 2000. *Data/FAX Modem Reference Index*. [online] Available at: <http://nemesis.lonestar.org/reference/telecom/modems/index.html> [Accessed: 21 Mar 2014].

Olivier, M. S. and Pieterse, H. 2013. Security steps for smartphone users. *Information Security for South Africa, 2013*, pp. 1-6. Available at: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6641036&queryText%3DSecurity+Steps+for+Smartphone+Users> [Accessed: 12 Feb 2014].

Oxygen-forensic. 2014. *Oxygen Forensic® Suite - Company*. [online] Available at: <http://www.oxygen-forensic.com/en/company> [Accessed: 22 Mar 2014].

Oxygen-forensic. 2014. *Oxygen Forensic® Suite - Features*. [online] Available at: <http://www.oxygen-forensic.com/en/features> [Accessed: 22 Mar 2014].

Regalado, A. 2011. *Who Coined 'Cloud Computing'?* | *MIT Technology Review*. [online] Available at: <http://www.technologyreview.com/news/425970/who-coined-cloud-computing/> [Accessed: 10 Jan 2014].

Ricker, T. 2008. *HTC Dream FCC approved, Android clear for launch?*. [online] Available at: <http://www.engadget.com/2008/08/18/htc-dream-fcc-approved-android-clear-for-launch/> [Accessed: 22 Mar 2014].

Safeharbor. 2009. *Safe Harbor - Organization Information*. [online] Available at: <http://safeharbor.export.gov/companyinfo.aspx?id=19515> [Accessed: 21 Mar 2014].

Salesforce. 2014. *About us - Salesforce.com*. [online] Available at: <http://www.salesforce.com/company/> [Accessed: 21 Mar 2014].

Shirk, G. 2013. *Going Global: Box Achieves ISO 27001 Certification*. [online] Available at: <http://blog.box.com/2013/05/going-global-box-achieves-iso-27001-certification/> [Accessed: 21 Mar 2014].

Sonymobile. 2010. *Developers Guidelines: AT Commands for Sony Ericsson phones*. [e-book] Lund: Sony Ericsson Mobile Communications AB. Available through: <http://developer.sonymobile.com/downloads/documentation/sony-ericsson-at-commands-online-reference/> [http://dl-developer.sonymobile.com/documentation/DW-65054-dg\\_at\\_2006--10\\_r17a.pdf](http://dl-developer.sonymobile.com/documentation/DW-65054-dg_at_2006--10_r17a.pdf) [Accessed: 21 Mar 2014].

Statista. 2014. *Smartphones sales, by operating system Q1 2009-Q3 2013* | Statistic. [online] Available at: <http://www.statista.com/statistics/266219/global-smartphone-sales-since-1st-quarter-2009-by-operating-system/> [Accessed: 22 Mar 2014].

Storagenewsletter. 2014. *StorageNewsletter » 500 Million Personal Cloud Storage Subscriptions in 2012*. [online] Available at: <http://www.storagenewsletter.com/rubriques/market-reportsresearch/ihc-cloud-storage-services/> [Accessed: 21 Mar 2014].

Sugarsync. 2014. *About Us - SugarSync*. [online] Available at: <http://www.sugarsync.com/company/> [Accessed: 21 Mar 2014].

Sugarsync. 2014. *SugarSync security*. [online] Available at: [https://sugarsync.custhelp.com/app/answers/detail/a\\_id/201/kw/security](https://sugarsync.custhelp.com/app/answers/detail/a_id/201/kw/security) [Accessed: 21 Mar 2014].

Sugarsync. 2013. *SugarSync Transitions to Paid-Only Service Model*. [online] Available at: [http://www.sugarsync.com/blog/20131210\\_sugarsync\\_press\\_release/](http://www.sugarsync.com/blog/20131210_sugarsync_press_release/) [Accessed: 21 Mar 2014].

Svajcer, V. 2012. *When Malware Goes Mobile: Causes, Outcomes and Cures*. [e-book] Sophos Ltd. p. 5-8. Available through: <http://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile/why-ios-is-safer-than-android.aspx> [Accessed: 22 Mar 2014].

Tools.ietf.org. 2007. *RFC 4791 - Calendaring Extensions to WebDAV (CalDAV)*. [online] Available at: <http://tools.ietf.org/html/rfc4791> [Accessed: 20 Mar 2014].

Tools.ietf.org. 2006. *RFC 4511 - Lightweight Directory Access Protocol (LDAP): The Protocol*. [online] Available at: <http://tools.ietf.org/html/rfc4511> [Accessed: 20 Mar 2014].

Venture Beat. 2009. *Sharpcast*. [online] Available at: <http://venturebeatprofiles.com/company/profile/sharpcast/overview/> [Accessed: 21 Mar 2014].

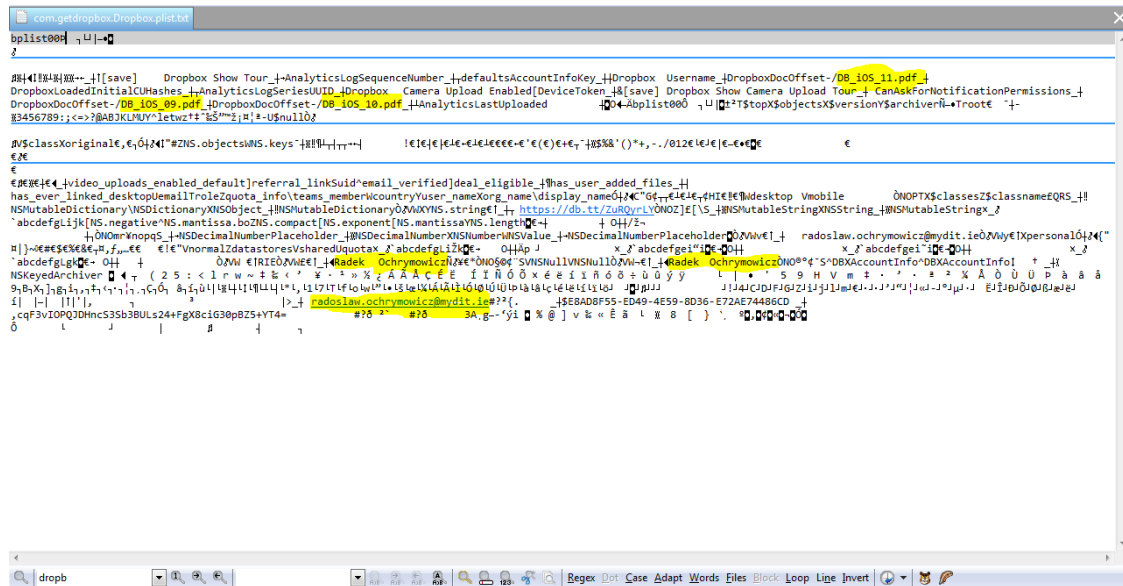
Web Archive. 2014. *Apple - iPhone - Tech Specs*. [online] Available at: <http://web.archive.org/web/20071006052144/http://www.apple.com/iphone/specs.html> [Accessed: 20 Mar 2014].

Whittaker, Z. 2013. *BlackBerry first to secure U.S. DOD device management approval* / *ZDNet*. [online] Available at: <http://www.zdnet.com/blackberry-first-to-secure-u-s-dod-device-management-approval-7000019156/> [Accessed: 22 Mar 2014].

Zdziarski, J. 2012. *Free Download: iOS Forensic Investigative Methods / Jonathan Zdziarski's Domain*. [online] Available at: <http://www.zdziarski.com/blog/?p=2287> [Accessed: 22 Mar 2014].

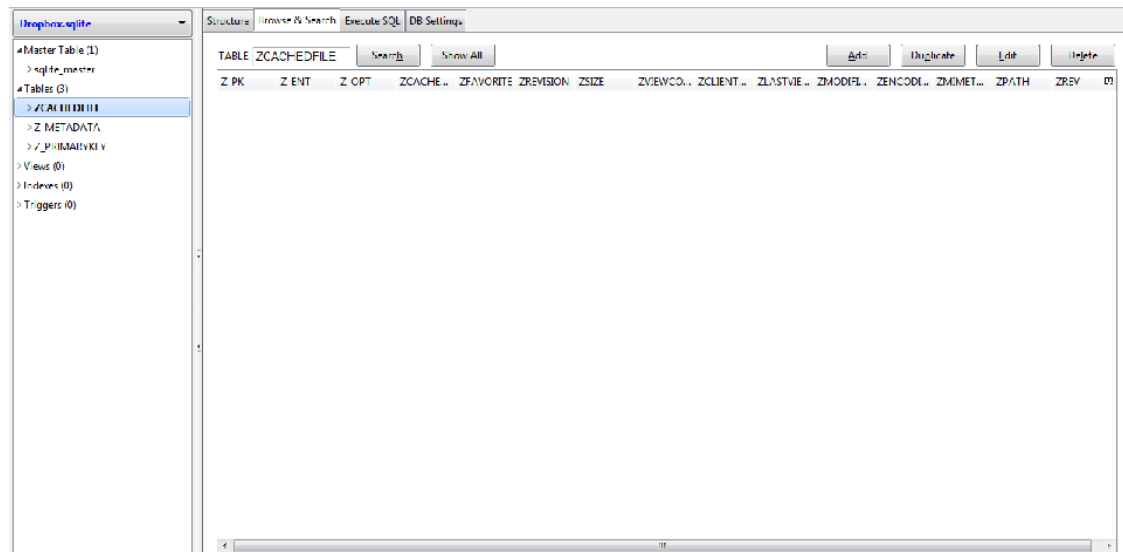
# APPENDIX A

## Dropbox xml property list file *com.getdropbox.dropbox.plist*



## Dropbox SQLite metadata file *Dropbox.sqlite*

### ZCACHEDFILE Table



## Z\_METADATA Table

The screenshot shows a database management interface for a SQLite database named 'Dropbox.sqlite'. The left sidebar displays a tree view of the database structure, including 'Master Table (1)', 'sqlite\_master', 'Tables (3)', 'Z\_CACHEDFILE', 'Z\_METADATA', 'Z\_PRIMARYKEY', 'Views (0)', 'Indexes (0)', and 'Triggers (0)'. The main window is titled 'TABLE Z\_METADATA' and contains a table with the following columns: Z\_VERSION, Z\_UUID, and Z\_PLIST. A single row of data is displayed with Z\_VERSION set to 1, Z\_UUID set to '032030DC-4A64-491D-9A76-53398311F832', and Z\_PLIST set to 'BLOB (Size: 296)'. The interface includes buttons for 'Add', 'Duplicate', 'Edit', and 'Delete' at the top right, and a status bar at the bottom showing '1 to 1 of 1'.

Z_VERSION	Z_UUID	Z_PLIST
1	032030DC-4A64-491D-9A76-53398311F832	BLOB (Size: 296)

## Z\_PRIMARYKEY Table

The screenshot shows the same database management interface, but now displaying the 'Z\_PRIMARYKEY' table. The table has four columns: Z\_ENT, Z\_NAME, Z\_SUPER, and Z\_MAX. A single row of data is shown with Z\_ENT set to 1, Z\_NAME set to 'CachedFile', Z\_SUPER set to 0, and Z\_MAX set to 0. The interface includes buttons for 'Add', 'Duplicate', 'Edit', and 'Delete' at the top right, and a status bar at the bottom showing '1 to 1 of 1'. The bottom status bar of the application also displays 'SQLite 3.8.0.2', 'Gecko 27.0.1', '0.8.1', 'Exclusive', 'Number of files in selected directory: 9', and 'ET: 1 ms'.

Z_ENT	Z_NAME	Z_SUPER	Z_MAX
1	CachedFile	0	0

# APPENDIX B

## BOX xml property list file *net.box.BoxNet.plist*



## BOX SQLite metadata file *BoxCoreDataStore.sqlite*

### ZBOXBASECOREDATA Tables

Z_PK	Z_ENT	Z_OPT	ZBOXID	ZMASTERKEY	ZCANR...	ZCOM...	ZOBJECT	Z4_OBL...	ZPARE...	ZCACH...	ZDISAB...	ZFORCE...	ZFORCE...	ZKEEPL...	ZLASTE...
1	3	17	207038356	207038356						1	0	0	0	1	1226631
2	5	7	124070522	207038356											
3	5	3	12266494538	207038356											
4	5	7	12407054224	207038356											
5	5	4	12266575660	207038356											
6	5	5	12407061476	207038356											
7	5	2	12266529232	207038356											
8	5	5	12407048612	207038356											
9	5	3	12266545622	207038356											
10	5	5	12266293310	207038356											
11	5	5	12266319894	207038356											
12	5	4	12266577570	207038356											
13	5	5	12266265894	207038356											
14	5	2	12266297866	207038356											
15	5	5	12266300412	207038356											
16	5	1	12266525356	207038356											
17	5	2	12266482548	207038356											
18	5	6	12266512408	207038356											
19	5	1	12266578252	207038356											
20	5	1	12266570698	207038356											
21	5	7	12407050074	207038356											
22	6	31	0	207038356											
23	9	11	207038356	207038356											

BoxCoreDataStore.sqlite

Structure Browse & Search Execute SQL DB Settings

Master Table (1)  
Tables (4)  
ZBOXBASECOREDATA  
Z\_4UPDATES  
Z\_METADATA  
Z\_PRIMARYKEY  
Views (0)  
Indexes (14)  
Triggers (0)

TABLE ZBOXBASECORE Search Show All Add Duplicate Edit Delete

ZLARGE...	ZLARGERHTHUMBNAILOCATION	ZNAME	ZPERML...	ZPREVIE...	ZSHA1	ZSHARE...	ZSMAL...	ZLOCALSHA1
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_10.pdf	dcgteop...	https://a...	a7759e2d089046ace8e592574fd2d6c7cc47e1			https://a...
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_13.mp3	dcgteop...	https://a...	46586997621758a3817c43cf682da0f1cae09f0d			https://a...
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_06.JPG	dcgteop...	https://a...	9627c23da4c6421aa7eb54cb718e61a4d7cf5af			https://a...
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_01.doc	dcgteop...	https://a...	bd2a002ef50070a95a1e92a55935ac9928604f11			https://a... bd2a002ef50070a
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_17.mov	dcgteop...	https://a...	fc79ccf6627e5bde4d89e34f233a657dca0a6f0			https://a...
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_18.MOV	dcgteop...	https://a...	a5b62f5875a6e5bc6b48a3f3fa773fd5dfdc02			https://a...
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_18.MOV	dcgteop...	https://a...	bee2f26d8066829d3eaea686bc7148cc589d7df			https://a...
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_18.MOV	dcgteop...	https://a...	a4e25c18501d94121a7b120a387c5650c5d2d146			https://a...
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_07.JPG	dcgteop...	https://a...	92f21b05cb717be69f65d7dd16ae4d3c49c9f85f			https://a... 92f21b05cb717be
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_11.pdf	dcgteop...	https://a...	e859de88571589e3eeb9b75c68c3432b636e4cb5			https://a... e859de88571589e
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_03.docx	dcgteop...	https://a...	0ef99fc4ec75dc89e6dc2521b82b059fe5855cd4			https://a... 0ef99fc4ec75dc8
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_05.jpg	dcgteop...	https://a...	e8e187a1798e6fa0d46e46d508ba64cae121d7c1			https://a... e8e187a1798e6
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_08.JPG	dcgteop...	https://a...	7043079cab6d3db624bf4cfee55e059c3f553a6			https://a...
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_09.pdf	dcgteop...	https://a...	4a5c6af421958d32b296da35f40fde7587a0f2d0			https://a... 4a5c6af421958d3
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_16.mp3	dcgteop...	https://a...	f972923af829ecc78e47562b6a917a53e5897f5a			https://a...
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_12.pdf	dcgteop...	https://a...	6f740606858198907d7653bfadb78271100fe8			https://a...
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_15.mp3	dcgteop...	https://a...	cab3aacc81b5ec64e434394624a86c5b26c0939			https://a... cab3aacc81b5ec
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_04.docx	dcgteop...	https://a...	99805c8edb4996b44144b7a017f033a614a6781			https://a...
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_20.MOV	dcgteop...	https://a...	899e89e383a81aa6167b542820ce0706a8960f5e			https://a...
https://a...	https://app.box.com/api/thumbs/4...	Box_iOS_02.docx	dcgteop...	https://a...	b55329bd3c6d32b09aee1c6e8d7880af05c34e10			https://a...
		All Files	douj					

SQLite 3.8.0.2 Gecko 27.0.1 0.8.1 Exclusive Number of files in selected directory: 9 ET: 10 ms

BoxCoreDataStore.sqlite

Structure Browse & Search Execute SQL DB Settings

Master Table (1)  
Tables (4)  
ZBOXBASECOREDATA  
Z\_4UPDATES  
Z\_METADATA  
Z\_PRIMARYKEY  
Views (0)  
Indexes (14)  
Triggers (0)

TABLE ZBOXBASECORE Search Show All Add Duplicate Edit Delete

ZPREVIE...	ZSHA1	ZSHARE...	ZSMAL...	ZLOCALSHA1	ZLOCALURLSTRING	ZMIME...	ZSTREA...
https://a...	a7759e2d089046ace8e592574fd2d6c7cc47e1			https://a...		applicati...	https://a...
https://a...	46586997621758a3817c43cf682da0f1cae09f0d			https://a...		applicati...	https://a...
https://a...	9627c23da4c6421aa7eb54cb718e61a4d7cf5af			https://a...		image/j...	https://a...
https://a...	bd2a002ef50070a95a1e92a55935ac9928604f11			https://a...	12266575660.doc	applicati...	https://a...
https://a...	fc79ccf6627e5bde4d89e34f233a657dca0a6f0			https://a...			https://a...
https://a...	a5b62f5875a6e5bc6b48a3f3fa773fd5dfdc02			https://a...			https://a...
https://a...	bee2f26d8066829d3eaea686bc7148cc589d7df			https://a...			https://a...
https://a...	a4e25c18501d94121a7b120a387c5650c5d2d146			https://a...			https://a...
https://a...	92f21b05cb717be69f65d7dd16ae4d3c49c9f85f			https://a...	12266293310.JPG	image/j...	https://a...
https://a...	e859de88571589e3eeb9b75c68c3432b636e4cb5			https://a...	12266319894.pdf	applicati...	https://a...
https://a...	0ef99fc4ec75dc89e6dc2521b82b059fe5855cd4			https://a...	1226657570.docx	applicati...	https://a...
https://a...	e8e187a1798e6fa0d46e46d508ba64cae121d7c1			https://a...	12266285894.jpg	image/j...	https://a...
https://a...	7043079cab6d3db624bf4cfee55e059c3f553a6			https://a...			https://a...
https://a...	4a5c6af421958d32b296da35f40fde7587a0f2d0			https://a...	12266300412.pdf	applicati...	https://a...
https://a...	f972923af829ecc78e47562b6a917a53e5897f5a			https://a...			https://a...
https://a...	6f740606858198907d7653bfadb78271100fe8			https://a...			https://a...
https://a...	cab3aacc81b5ec64e434394624a86c5b26c0939			https://a...	12266512488.mp3	audio/m...	https://a...
https://a...	99805c8edb4996b44144b7a017f033a614a6781			https://a...			https://a...
https://a...	899e89e383a81aa6167b542820ce0706a8960f5e			https://a...			https://a...
https://a...	b55329bd3c6d32b09aee1c6e8d7880af05c34e10			https://a...		applicati...	https://a...

SQLite 3.8.0.2 Gecko 27.0.1 0.8.1 Exclusive UFED Physical Analyzer 3 directory: 9 ET: 10 ms



BoxCoreDataStore.sqlite

Structure Browse & Search Execute SQL DB Settings

Master Table (1)  
Tables (4)  
ZBOXBASECOREDATA  
Z\_4\_UPDATES  
Z\_METADATA  
Z\_PRIMARYKEY  
Views (0)  
Indexes (14)  
Triggers (0)

TABLE ZBOXBASECORE Search Show All Add Duplicate Edit Delete

ZMINMETYPE	ZSTREAMINGURLSTRING
application/pdf	https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12407057522?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
image/jpeg	https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266494538?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
application/msword	https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266575660?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
image/jpeg	https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12407061476?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
application/pdf	https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266529232?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
image/jpeg	https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12407048612?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
application/pdf	https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266545622?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
application/vnd.openxmlformats-officedocument.wordprocessingml.document	https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266319894?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
image/jpeg	https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266577570?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
application/pdf	https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266300412?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
audio/mpeg	https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266512488?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
application/vnd.openxmlformats-officedocument.wordprocessingml.document	https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12407050074?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone

SQLite 3.8.0.2 Gecko 27.0.1 0.8.1 Exclusive Number of files in selected directory: 9 ET: 10 ms

BoxCoreDataStore.sqlite

Structure Browse & Search Execute SQL DB Settings

Master Table (1)  
Tables (4)  
ZBOXBASECOREDATA  
Z\_4\_UPDATES  
Z\_METADATA  
Z\_PRIMARYKEY  
Views (0)  
Indexes (14)  
Triggers (0)

TABLE ZBOXBASECORE Search Show All Add Duplicate Edit Delete

ZSTREAMINGURLSTRING
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12407057522?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266494538?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266575660?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12407061476?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266529232?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12407048612?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266545622?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266319894?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266577570?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266285894?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266300412?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12266512488?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone
https://mobile-api.box.com/api/1.0/download/fs39y40jon6t94czuyeeegsargpxz1/12407050074?device_id=2541F721-BEC9-4FD5-BA37-02231479C506&device_name=Test%20iPhone

SQLite 3.8.0.2 Gecko 27.0.1 0.8.1 Exclusive Number of files in selected directory: 9 ET: 10 ms



SQLite 3.8.0.2 Gecko 27.0.1 0.8.1 Exclusive Number of files in selected directory: 9 ET: 1 ms

Ringo.sqlite

- Master Table (1)
- Tables (5)
  - ZSYNCOBJECT
  - ZSYNCOBJECTEX**
  - ZUSERSETTINGS
  - Z\_METADATA
  - Z\_PRIMARYKEY
- Views (0)
- Indexes (3)
- Triggers (0)

Structure Browse & Search Execute SQL DB Settings

TABLE ZSYNCOBJECTEX Search Show All Add Duplicate Edit Delete

Z_PK	Z_ENT	Z_OPT	ZDELETED	ZUSERID	ZDISPLAYNAME	ZEXTRA	ZNAME	ZPARENTNAME
------	-------	-------	----------	---------	--------------	--------	-------	-------------

<< < 0 to 0 of 0 > >>

SQLite 3.8.0.2 Gecko 27.0.1 0.8.1 Exclusive Number of files in selected directory: 9 ET: 0 ms

Ringo.sqlite

- Master Table (1)
- Tables (5)
  - ZSYNCOBJECT
  - ZSYNCOBJECTEX
  - ZUSERSETTINGS**
  - Z\_METADATA
  - Z\_PRIMARYKEY
- Views (0)
- Indexes (3)
- Triggers (0)

Structure Browse & Search Execute SQL DB Settings

TABLE ZUSERSETTING Search Show All Add Duplicate Edit Delete

Z_PK	Z_ENT	Z_OPT	ZUSERID	ZKEY	ZVALUE
------	-------	-------	---------	------	--------

<< < 0 to 0 of 0 > >>

Ringo.sqlite

Structure Browse & Search Execute SQL DB Settings

TABLE Z\_METADATA Search Show All Add Duplicate Edit Delete

Z_VERSION	Z_UUID	Z_PLIST
1	F7368C04-C6FC-4050-BCTE-BF406A05BDE1	BLOB (Size: 420)

SQLite 3.8.0.2 Gecko 27.0.1 0.8.1 Exclusive Number of files in selected directory: 9 ET: 0 ms

Ringo.sqlite

Structure Browse & Search Execute SQL DB Settings

TABLE Z\_PRIMARYKEY Search Show All Add Duplicate Edit Delete

Z_ENT	Z_NAME	Z_SUPER	Z_MAX
1	SyncObject	0	0
2	SyncObjectEx	0	0
3	UserSettings	0	0

SQLite 3.8.0.2 Gecko 27.0.1 0.8.1 Exclusive Number of files in selected directory: 9 ET: 1 ms

# APPENDIX D

## Script test results

