UNIVERSITI PUTRA MALAYSIA

DIGITAL FORENSICS FRAMEWORK FOR INVESTIGATING CLIENT CLOUD STORAGE APPLICATIONS ON SMARTPHONES

FARID DARYABAR

FSKTM 2015 4

DIGITAL FORENSICS FRAMEWORK FOR INVESTIGATING CLIENT CLOUD STORAGE APPLICATIONS ON SMARTPHONES

By

FARID DARYABAR

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

May 2015

This thesis is dedicated to my parents

For their endless love, support, patience and encouragement

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

DIGITAL FORENSICS FRAMEWORK FOR INVESTIGATING CLIENT CLOUD STORAGE APPLICATIONS ON SMARTPHONES

By

FARID DARYABAR

May 2015

Chair: Ali Dehghantanha, PhD
Faculty: Computer Science and Information Technology

In today's modern world, the growing use of smartphones with the Internet access supported increasing deployment of cloud storage applications to access data anywhere, anytime. It provides a sharp increase of the possibility of malicious activities to abuse the cloud storages. One of the emerging challenges regarding digital forensic research investigations is cloud storage, as well as increasing use of cloud storage applications on mobile devices. The overlap of these two growing technologies further cyber criminals opportunities to conduct malicious activities such as identity theft, piracy, illegal trading, sexual harassment, cyber stalking and cyber terrorism. This has made mobile devices as an important source of evidence in digital investigation.

Not knowing where the data may reside can impede the investigators, as it could take considerable time to contact all potential service providers to determine if the data is stored within their cloud service. Current mobile forensic analyzer tools, procedures and methods are able to extract valuable information from VoIP, Social Networking, Mail Applications on smartphones; however, the mobile forensic analyzer tools cannot acquire enough valuable information from cloud applications on smartphones. Therefore, there is a forensically sound need for a digital forensic framework focusing on analysis phase of smartphones to identify potential data on cloud storages. In this thesis, a framework for investigating client cloud storage applications on smartphones is proposed.

Using the framework, we seek to analyze and determine the data remnants from the use of five popular cloud client Apps of OneDrive, Box, Mega, GoogleDrive, and Dropbox on the popular smartphones that use operating systems of Android and iOS. A variety of circumstances have been considered, including methods to upload, download, delete and share files in the cloud storage clients to determine residue data on client devices. Moreover, in terms of evidence preservation, possible modifications in files content and metadata that may affect preservation of evidence from these platforms are examined.

A variety of artifacts were detected from different users' activities such as login, upload, download, delete, and sharing files. Moreover, the cloud client applications in the Android device did not cause any alteration to the content of the files. However, the

files' timestamps were changed from the original sample files, and this needs to be considered when forming conclusions in relation to examination of times and dates of the files within the cloud client applications. The findings may assist forensic examiners and practitioners in real world examination of cloud client applications on Android and iOS platforms.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia Sebagai memenuhi keperluan untuk ijazah master sains

DIGITAL FORENSIK RANGKA KERJA UNTUK MENYIASAT PELANGGAN CLOUD PERMOHONAN PENYIMPANAN PADA TELEFON PINTAR

Oleh

FARID DARYABAR

May 2015

Pengerusi: Ali Dehghantanha, PhD
Fakulti: Sains Komputer dan Teknologi Maklumat

Dalam dunia moden hari ini, perkembangan penggunaan telefon pintar yang disokong oleh akses internet, telah meningkatkan penggunaan aplikasi storan awan bagi mengakses data di mana sahaja tempat dan pada bila-bila masa. Ia mungkin menyebabkan penyiasatan potensi mendadak dalam aktiviti berniat jahat untuk menyalahgunakan storan awan. Salah satu cabaran yang baru muncul berkaitan dengan kajian penyelidikan forensik digital adalah storan awan, serta peningkatan penggunaan aplikasi storon awan pada telefon pintar. Perkembangan kedua-dua teknologi dalam satu masa yang sama, telah menyebabkan penjenayah siber berpeluang untuk menjalankan aktiviti berniat jahat seperti pencurian identiti, cetak rompak, perdagangan haram, gangguan seksual, ugutan siber dan keganasan siber. Ini telah membuatkan telefon bimbit sebagai sumber penting bagi bukti-bukti dalam siasatan digital.

Tanpa mengetahui di mana data tersebut disimpan, ia akan menghalang penyiasat, ianya akan mengambil masa yang agak lama untuk menghubungi kesemua pusat servis yang berpotensi untuk memastikan sama ada data tersebut tersimpan di dalam storan awan mereka. Oleh itu, terdapat keperluan berbunyi forensik rangka kerja digital forensik yang boleh diterima di mahkameh berkaitan dengan telefon pintar bagi mengenalpasti data yang berpotensi di dalam storan awan. Di dalam tesis ini, satu rangka kerja telah di usul untuk melakukan siasatan ke atas aplikasi storan awan di telefon pintar pelanggan.

Dengan menggunakan rangka kerja ini, kami berusaha untuk memeriksa dan menentukan sisa data daripada penggunaan lima aplikasi popular pelanggan awan iaitu OneDrive, Box, Mega, GoogleDrive, dan Dropbox pada telefon pintar yang popular yang menggunakan sistem beroperasin Android dan iOS. Pelbagai keadaan telah dipertimbangkan, termasuklah pelbagai kaedah untuk memuat naik, memuat turun, memadam dan berkongsi fail dalam storan awan pelanggan bagi menentukan data sisa pada peranti pelanggan tersebut. Selain itu, dari segi pemeliharaan bukti, kemungkinan pengubahsuaian pada kandungan fail dan metadata yang mungkin memberi kesan pemeliharaan bukti dari platform ini akan diselidik.

Pelbagai artifak telah dikesan daripada aktiviti pengguna yang berbeza seperti login, memuat naik, memuat turun, memadam, dan perkongsian fail. Selain itu, aplikasi pelanggn awan dalam peranti Android tidak menyebabkan apa-apa perubahan kepada kandungan fail. Walau bagaimanapun, cap waktu fail yang telah diubahsuai dari fail sampel asal, dan ini perlu dipertimbangkan apabila membuat kesimpulan berhubung dengan pemeriksaan tarikh dan masa fail dalam aplikasi pelanggan awan. Hasil kajian boleh membantu pemeriksa dan pengamal forensik dalam penyiasatan dunia sebenar untuk aplikasi pelanggan awan pada platform Android dan iOS.

AKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my research supervisor Dr. Ali Dehghantanha for the continuous support of my study and research, for his patience, motivation, and immense knowledge. I would also like to show gratitude to my supervisory committee, including Assoc. Prof. Dr. Nur Izura Udzir, Assoc. Prof. Dr. Nor Fazlida Mohd Sani, and Dr. Solahuddin bin Shamsuddin. Without their assistance and dedicated involvement in every step throughout the process, this thesis would have never been accomplished.

I would like to thank faculty of computer science and information technology for its supporting guidance and materials.

Getting through my thesis required more than academic support. To all my friends, thank you for your understanding and encouragement.

Last but not least, I am immensely grateful to my parents for their unlimited love and support throughout my life.

APPROVAL

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science.

The members of the Supervisory Committee were as follows:

Ali Dehghantanha, PhD.
Senior lecturer
Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Nur Izura Udzir, PhD.
Associate. Professor
Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Nor Fazlida Mohd Sani, PhD.
Associate. Professor
Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Solahuddin Bin Shamsuddin, PhD.
Chief Technology Officer
Cyber Security Malaysia
(External Member)

BUJANG KIM HUAT, Ph.D.
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by the graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: _____

Name and Matric No.: Farid Daryabar / GS33313

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature:	Signature:
Name of Chairman of Supervisory Committee: -	Name of Member of Supervisory Committee: -
Signature:	Signature:
Name of Member of Supervisory Committee: -	Name of Member of Supervisory Committee: -

TABLE OF CONTENTS

		Page
ABSTRACT		**i**
ABSTRAK		**iii**
AKNOWLEDGEMENTS		**v**
APPROVAL		**vi**
DECLARATION		**viii**
LIST OF TABLES		**xii**
LIST OF FIGURES		**xiii**
LIST OF ABBREVIATIONS		**xvii**
CHAPTER		
1	**INTRODUCTION**	**1**
	1.1 Background	1
	1.2 Motivation	2
	1.3 Problem Statement	3
	1.4 Research Objectives	4
	1.5 Research Questions	4
	1.5.1 Research Question 1	4
	1.5.2 Research Question 2	5
	1.6 Research Contributions	6
	1.7 Research Scope	6
	1.8 Thesis Structure	6
2	**LITERATURE REVIEW**	**8**
	2.1 Cloud Computing	8
	2.2 Digital Forensics Investigation	8
	2.2.1 Cloud Computing Impacts on Digital Forensics	9
	2.2.2 Smartphone Cloud Computing Digital Forensics	10
	2.2.3 Current Related Researches	11
	2.3 Summary	14
3	**RESEARCH METHODOLOGY**	**16**
	3.1 Introduction	16
	3.1.1 Research Process	16
	3.2 Experiment Design	17
	3.2.1 Research Data Set	18
	3.2.2 Research Question 1 Experiment Process	18
	3.2.3 Research Question 2 Experiment Process	26
	3.3 Research Equipment	30
	3.4 Summary	31
4	**DESIGN AND IMPLEMENTATION**	**32**
	4.1 Introduction	32
	4.2 Proposed Digital Forensic Framework	32
	4.2.1 Commencement	33
	4.2.2 Identification and Preparation	33
	4.2.3 Acquisition	34

4.2.4 Preservation 34
4.2.5 Analysis 35
4.2.6 Reconstruction 36
4.2.7 Reporting 36
4.3 Analogy of the SCFF 37
4.4 Summary 37

5 RESULTS AND FINDINGS 39
5.1 Introduction 39
5.2 Android Forensic 39
5.2.1 Android Forensic Commencement 39
5.2.2 Android Forensic Identification and Preparation 40
5.2.3 Android Forensic Acquisition 41
5.2.4 Android Forensic Preservation 44
5.2.5 Android Forensic Analysis 44
5.2.6 Android Forensic Reconstruction 75
5.2.7 Android Forensic Reporting 78
5.3 iOS Forensic 78
5.3.1 iOS Forensic Commencement 78
5.3.2 iOS Forensic Identification and Preparation 79
5.3.3 iOS forensic Acquisition 80
5.3.4 iOS Forensic Preservation 84
5.3.5 iOS Forensic Analysis 84
5.3.6 iOS Forensic Reconstruction 120
5.3.7 iOS Forensic Reporting 124
5.4 File Metadata Preservation 124
5.4.1 Android and iOS Acquisition 125
5.4.2 Android and iOS Analysis 126
5.5 Summary of Findings 138
5.5.1 Data Remnants analysis and comparison 138
5.5.2 Preservation 140

6 CONCLUSION AND FUTURE WORK 143
6.1 Conclusion 143
6.2 Contributions of the Research 147
6.3 Future Work 148

REFERENCES 149
BIODATA OF STUDENT 154
LIST OF PUBLICATIONS 155

LIST OF TABLES

Table	Page
1.1. Popularity of client cloud storage applications on smartphones (Garcia-Arenas et al., 2011)	2
3.1. Performed activities in cloud client applications on the Android device.	21
3.2. Performed activities in cloud client applications on the iOS forensic of the backup stage.	22
3.3 Performed activities in cloud client applications on the iOS forensic of the internal storage and network traffic stages.	22
3.4. Upload and Download Files on the Android device	27
3.5. Upload and Download Files on the iOS device	27
3.6. List of software used in the research	30
3.7. List of hardware used in the research	31
5.1. Summary of the analysis findings in Android internal memory	76
5.2. Summary Of the analysis findings in Android internal storage	77
5.3. Summary Of the analysis findings in Android network traffic	78
5.4. Description and information of the readable backup files	85
5.5 General information of OneDrive Application	87
5.6 General information about the Box Application	91
5.7 General information about the Mega Application	93
5.8. General information about GoogleDrive Application	96
5.9. GoogleDrive users login information	97
5.10 General information about Dropbox Application	103
5.11. Summary of the analysis findings of iOS backup	121
5.12. Summary of the analysis findings of iOS internal storage	123
5.13. Summary of the analysis findings of iOS network traffic	124
5.14. Summary of detectable user activities remnants on Android and iOS platforms	138
5.15. Hash value and timestamps of the original and the downloaded files in Android	141
5.16. Hash value and timestamps of the original and the downloaded files in iOS	142
6.1. Findings of common terms in the Android internal memory	143
6.2. Cloud client applications network traffic findings in Android device	144
6.3. Cloud client applications network traffic findings in iOS device	146

LIST OF FIGURES

Figure	Page
2.1. Procedure for investigation of a cloud storage service (Chung et al., 2012)	13
3.1. The research process	17
3.2. Research experimental design 1	19
3.3. Block Diagram of Research Scope for Android	20
3.4. Block Diagram of Research Scope for iOS	20
3.5 Flowchart diagram of the experimentation setup for the analysis phase	25
3.6. Android and iOS actions scenario	26
3.7 Research experimental design 2	27
3.8 Android and iOS actions scenario for metadata preservation	28
3.9 Flowchart diagram of the experimental setup for the metadata preservation	29
4.1. SCFF the Proposed Digital Forensic investigation Framework	33
4.2. Flowchart diagram of the generalized framework.	36
4.3. Digital forensic framework comparison (Martini & Choo, 2012)	37
5.1. A bit-by-bit image of the Android device's internal memory of AB1 activity	41
5.2. A bit-by-bit image of the Android device's internal memory of AD3 activity	42
5.3. TCPDUMP installation process on the Android device	43
5.4. Network traffic capturing procedures of AB1 to AB5.	44
5.5. OneDrive username and password	45
5.6. Box username and password	46
5.7. Mega username in the RAM dump	46
5.8. Mega authenticator server	46
5.9. The password string	46
5.10. GoogleDrive username and password	47
5.11. Dropbox username and password	47
5.12. OneDrive path and its running service on the Android Device	48
5.13. OneDrive login analysis	49
5.14. File uploading operation	50
5.15. Header and Footer of the uploaded file	50
5.16. The uploaded file that was extracted from the image	50
5.17. SkyDrive Download ID	51
5.18. Downloaded file using the SkyDrive ID	51
5.19. Header and footer of the downloaded file	51
5.20. The downloaded file that was extracted from the image	52
5.21. File deleting operation	52
5.22. Deleted file that was extracted from the image	52
5.23. Attaching the shared file by the OneDrive user	53
5.24. Sharing the file using the email service	53
5.25. Box location on the Android device	53
5.26. Last login information of the Box application	54
5.27. Uploading Action using the Box application	54
5.28. Creation of uploaded file in Box application	55
5.29. The metadata of the uploaded file	55
5.30. The Uploaded file that was extracted from AB2 activity	55
5.31. Box application download operation	56
5.32. Assigned file ID in Box application	56
5.33. Hex header and footer of the uploaded file	56
5.34. The uploaded file that was extracted from AB3 activity	57
5.35. Location of the uploaded file on the Android device	57

5.36. Delete operation in the Box application 57
5.37. Hex header and footer of the uploaded file 58
5.38. The deleted file that was extracted from AB4 activity 58
5.39. Shared file in Box application 58
5.40. The shared file timestamp and user id of the Box application 59
5.41. Mega install operation on the Android device 59
5.42. Mega installation location 60
5.43. Downloaded file location 60
5.44. Hex header and footer of the downloaded file 61
5.45. Downloaded file that was extracted from AG3 activity image file 61
5.46. A shared link created by the Mega client application 61
5.47. GoogleDrive application's location 62
5.48. GoogleDrive Account and its sync period 62
5.49. Google Drive last user information 63
5.50. Locations of the downloaded file 64
5.51. GoogleDrive user's account and the downloaded file 64
5.52. Hex header and footer of the downloaded file 64
5.53. Downloaded file that was extracted from AG3 activity image file 64
5.54. Deleted MS Word file by the user account 65
5.55. Hex header and footer of the deleted file 65
5.56. The deleted file that was recovered from the AG4 activity image 66
5.57. Shared file in GoogleDrive application 66
5.58. Dropbox client application location on the Android device 67
5.59. Dropbox user's account 67
5.60. Dropbox uploading task 68
5.61. The uploaded file's location 68
5.62. Uploaded file hex header and footer 68
5.63. Uploaded file that was extracted from AD2 activity 69
5.64. Dropbox download task 69
5.65. Downloaded file location 69
5.66. Downloaded file hex header and footer 70
5.67. Downloaded file that was extracted from AD2 activity 70
5.68. Thumbnail of the deleted file 71
5.69. Dropbox shared link 71
5.70. OneDrive application network traffic 72
5.71. Box application network traffic 73
5.72. Mega application network traffic 73
5.73. GoogleDrive client application's network traffic 74
5.74. Dropbox client application's network traffic 74
5.75. iOS backup acquisition of BIO4 activity 81
5.76. Backup image of BIO4 activity on iOS device 81
5.77. Acquired internal storage bit-by-bit image of SID3 activity 82
5.78. network creation and Internet sharing on the forensic workstation 83
5.79. Network traffic capturing procedures of SIO1. 84
5.80. OneDrive information extracted from the "info.plist" and "manifest.plist" files 87
5.81. OneDrive login analysis of iOS device 88
5.82. File uploading operation 88
5.83. The uploaded file that was extracted from the image 88
5.84. OneDrive Downloaded file operation. 89
5.85. The downloaded file that was extracted from the image 89

5.86. Deleted fragments from “onedrive.db” 90
5.87. The deleted file’s ID 90
5.88. Attaching the shared file by OneDrive under the user ID 90
5.89. The shared file that was extracted from the image 91
5.90. Box information extracted from the “info.plist” and “manifest.plist” files 92
5.91. Mega information extracted from the “info.plist” and “manifest.plist” files 94
5.92. Mega cloud client application user’s ID 95
5.93. Downloaded file’s location 95
5.94. Downloaded file that was extracted from the BIM3 activity image file 96
5.95. GoogleDrive information extracted from the “info.plist” and “manifest.plist” files 97
5.96. Google Drive user’s login information 98
5.97. Upload operation of the GoogleDrive cloud client application 98
5.98. The uploaded file that was extracted from BIG2 activity 99
5.99. File download operation by the GoogleDrive application 100
5.100. Downloaded file that was extracted from BIG3 activity image file 100
5.101. File Deleting by the user account in GoogleDrive application 101
5.102. The deleted file that was extracted from BIG4 activity 101
5.103. Shared file in GoogleDrive application 102
5.104. The shared file that was extracted from BIG5 activity 102
5.105. the user account in the list of share accounts 102
5.106. Dropbox information extracted from the “info.plist” and “manifest.plist” files 103
5.107. Dropbox cloud client application user’s ID 104
5.108. Dropbox uploading Progress 105
5.109. The uploaded file’s name and ID 106
5.110. Uploaded file that was extracted from BID2 activity 106
5.111. Dropbox download task 107
5.112. Downloaded file name and its ID 107
5.113. Downloaded file that is extracted from BID3 activity 107
5.114. Dropbox delete progress 108
5.115. Dropbox shared progress 108
5.116. The xbm file that was extracted from BID5 activity 108
5.117. OneDrive installation on the iOS Device 109
5.118. OneDrive user ID on the iOS device 110
5.119. File uploading operation of OneDrive application on the iOS device 110
5.120. Uploaded file’s name of OneDrive application on the iOS device 110
5.121. Deleted file’s name of OneDrive application on the iOS device 111
5.122. Box installation on the iOS Device 111
5.123. Uploaded file’s name of Box application on the iOS device 112
5.124. Mega installation on the iOS Device 113
5.125. Uploaded file’s name of the Mega application on the iOS device 113
5.126. Downloaded file location of the Mega application on the iOS device 113
5.127. Downloaded file’s name of the Mega application on the iOS device 114
5.128. GoogleDrive installation on the iOS Device 114
5.129. Dropbox installation on the iOS Device 115
5.130. Dropbox user ID on the iOS device 116
5.131. Uploaded file’s name of the Dropbox application on the iOS device 116
5.132. OneDrive application network traffic 117
5.133. Box application network traffic 118
5.134. Mega application network traffic 118

5.135. GoogleDrive client application's network traffic 119
5.136. Dropbox client application's network traffic 120
5.137. Header and footer of the downloaded file 127
5.138. MD5 hash value of the original and the downloaded files 127
5.139. Timestamps comparison 127
5.140. Header and footer of the downloaded file 128
5.141. MD5 hash value of the original and the downloaded files 128
5.142. Timestamps comparison 129
5.143. Header and footer of the downloaded file 129
5.144. hash value of the original and the downloaded files 130
5.145. Timestamps comparison 130
5.146. Header and footer of the downloaded file 131
5.147. MD5 hash value of the original and the downloaded files 131
5.148. Timestamps comparison 131
5.149. Header and footer of the downloaded file 132
5.150. MD5 hash value of the original and the downloaded files 132
5.151. Timestamps comparison 133
5.152. MD5 hash value of the original and the downloaded files 134
5.153. Timestamps comparison 134
5.154. hash value of the original and the downloaded files 135
5.155. Timestamps comparison 135
5.156. MD5 hash value of the original and the downloaded files 136
5.157. Timestamps comparison 136
5.158. MD5 hash value of the original and the downloaded files 137
5.159. Timestamps comparison 137
5.160. Comparison of the data remnants of the cloud client application on the smartphones 140

LIST OF ABBREVIATIONS

API	Application Programming Interface
ADB	Android Debug Bridge
DD	Disk Dump
DFRWS	Digital Forensics Research Workshop
FTK	Forensic Tool Kit
GSM	Global System for Mobile Communications
IaaS	Infrastructure as a Service
ID	Identifier
IM	Internal Memory
IS	Internal Storage
iOS	Apple Operating System
IT	Information Technology
LAN	Local Area Network
MD5	Message Digest
NaaS	Network as a Service
NIST	National Institute of Standards and Technology
OS	Operating System
NT	Network Traffic
PaaS	Platform as a Service
PC	Personal Computer
PCAP	Network traffic capture file
PIN	Personal Identification Number
PLIST	Property List
URL	Uniform Resource Locator
RAM	Random Access Memory
SaaS	Software as a Service
SHA1	Secure Hash Algorithms
SQL	Structured Query Language
SSH	Secure Shell
TCP	Transmission Control Protocol
UDID	Unique Device Identifier
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VM	Virtual Machine
VMDK	Virtual Machine Disk
VMEM	Virtual Memory

CHAPTER 1

INTRODUCTION

1.1 Background

There are vast varieties of factors that have a great influence on our daily life, but just like the two sides of a coin they offer both benefits and drawbacks, and cloud computing is not an exception. In today's modern world, digital storage associated with computer resources is increasingly shifting toward cloud computing, which provides digital data storages using a set of infrastructure over the Internet or internally over a private corporation network. National Institute of Standards and Technology (NIST) introduced the definition of cloud computing as a model intended for empowering ubiquitous, easy and on demand access over a network to a shared pool of digital resources which can be quickly launched with minimum management attempts (Hogan et al., 2011). Although, Mason and George (2011) stated that the significances regarding acquiring and preserving evidence in digital format for the resolution of civil disputes along with the criminal activities prosecution might be considerably influenced in the future with cloud computing. Furthermore, Martini and Choo (2012) indicated that the increased use of cloud storage services brings an easier way for criminals to store their incriminating files such as child exploitation, illicit drug, and terrorism materials, however, it might be extremely challenging for investigators to seize these files.

On the other hand, Barmpatsalou et al. (2013) mentioned that the technology regarding mobile devices has shown revolutionary development over the past few years. Al-Hadadi and AlShidhani (2013) highlighted that the availability of high speed Internet connections by using 3rd Generation (3G) and 4th generation (4G) technologies made the smartphones essential in our lives everyday. In contrast, smartphones grew to become subjects to the same or even greater vulnerabilities as computers. According to Samet et al. (2014), from year 2009 to 2014 there is a dramatic increase in the rate of mobile cloud computing usage, approximately 88% per year. However, the growing use of smartphones with the Internet access makes the easy accessibility of the cloud storage services by the users. Moreover, it provides a sharp increase of the possibility of malicious activities to abuse the cloud storages. As Barmpatsalou et al. (2013) stated, criminal activities on smartphone is vital in crime prevention and more scientific research and methodologies are required to assist digital forensic investigators to manage the collected data from the smartphones. Additionally, there are various types of cloud storage providers such as OneDrive®, Box Inc., Mega Ltd., GoogleDrive™, and Dropbox™, which provide free cloud storage services on popular smartphones such as Android and iOS devices (Garcia-Arenas et al., 2011). Table 1.1 shows the popularity of the cloud storage clients.

Therefore, one of the emerging challenges in digital forensics is investigation of cloud storages. Further increase in the size of these storages amplified the problem. Muda et al. (2014) defined digital forensic as the science of collecting, preserving, analyzing and presenting evidence from computers for criminal investigations or civil disputes that are sufficiently trusted in order to operate in court in a convincing way. On the other hand, Taylor et al. (2011) stated that based on the difficulties in defining what data stored on what specific devices, digital forensic investigation on cloud storages is potentially more difficult for the digital forensic examiners to acquire and analyze

evidence compare to the same standards for traditional digital forensic investigation on computers. In this connection, Zhu (2011) maintained that in terms of data acquisition and preservation, smartphone forensic is dealing with many challenges to obtain data without altering in forensically sound methods. While, Quick and Choo (2013a) indicated that one of the most significant issues that digital forensic investigators are facing is the identification of cloud storage providers and accounts that examination and analysis of smartphones can solve the problem. Quick and Choo (2014) indicated that it is of high importance to find out the type of data remnants left behind by users in cloud storages on the devices. In terms of data integrity and data preservation, it is very critical for digital forensic investigators to find out the file contents and timestamps have not been altered using the different cloud services during uploading and downloading the files (Oestreicher, 2014a). As a result, it is necessary to have a set of procedures and methodology for performing digital forensic examination to be likewise flexible and adaptable enough to assist investigators with existing and future cloud storages on smartphones.

Table 1.1. Popularity of client cloud storage applications on smartphones (Garcia-Arenas et al., 2011)

Cloud Storage Clients	Popularity	Space for Free	Mobile OS Support
OneDrive	More than 250 millions users	7GB	Android and iOS
Box	More than 70 millions users	10GB	Android and iOS
MEGA	More than 70 millions users	50GB	Android and iOS
Google Drive	More than 400 millions users	15GB	Android and iOS
Dropbox	More than 100 millions users	2GB	Android and iOS

1.2 Motivation

The motivation for conducting research into client cloud storage forensics preservation and analysis can be summarized in the following points. Cloud storage is increasingly being used by consumers, businesses, and government users to store growing amounts of data. While, cloud client applications is increasingly being accessed with mobile electronic devices. Criminals are embracing the opportunity to store illicit data in cloud file hosting services, which contributes to difficulties in proving ownership and interaction.

The use of cloud computing by criminals or their victims means that data of interest may be virtualized, geographically distributed, and transient. This presents technical and jurisdictional challenges for identification and seizure by law enforcement and national security agencies, which can impede digital forensic investigators and potentially prevent agencies from acquiring digital evidence and forensically analyzing digital content in a timely fashion (Quick & Choo, 2014).

Taylor et al. (2011) explained that in legal terms, cloud computing systems will make it potentially more difficult for the computer forensic analyst to acquire and analyse digital evidence to the same standards as that currently expected for traditional server-based systems, due to the difficulty in establishing what data was stored or processed by what software on what specific computing device.

According to (Quick & Choo, 2014; Samet et al., 2014), from year 2009 to 2014 there is a dramatic increase in the rate of mobile cloud computing usage, approximately 88%

per year and smartphones are becoming widely use to access cloud storage and it is subject to store and distributes criminal data such as child abuse materials and terrorism-related materials by cyber criminals. Furthermore, Sameera Almulla (2013) indicated that there are already several cases of attacks conducted on information stored in cloud computing. For instance, Google announced that its cloud single sign on was being attacked. One issue facing forensic investigators is the identification of service providers, accounts and data remnants, including usernames and passwords. Therefore, the analysis of user mobile devices such as an Apple iPhone or Android mobile phone may provide this information.

1.3 Problem Statement

In the recent researches, Zhu (2011) investigated a cloud client application of Dropbox on Android version 2 and iOS version 4. Using XRY and Oxygen forensic tools, the researcher found and extracted usernames and filenames on the devices, but the content of the files could not be retrieved. Chung et al. (2012) proposed a process model for digital forensic investigation of cloud storage applications such as Amazon S3, Dropbox, Evernote and Google Docs on personal computers (PCs) and smartphones including Android version 2.2.2 and iOS version 4.3.5. The proposed model was designed only for the investigation from the backup files of the devices' internal storages in the steps of collection, analysis and reporting. Hale (2013) discussed the digital artifacts that left behind from using Amazon cloud drive on personal computers with Windows XP and Windows 7 operating systems. It was stated that there is a need for detection of artifacts that left from different types of cloud storage applications. Otherwise, the forensic investigators might overlook critical data during their examinations. Quick and Choo (2014) proposed a digital forensic analysis cycle for GoogleDrive cloud application on a virtual computer running Windows 7 and an iPhone 3G with iOS version 4.2.1. In the case of iOS, XRY application was used to extract a logical image of the iOS device, and the inbuilt browser (Safari) was used to access the GoogleDrive's contents for the research's experiments and analysis. In addition, the authors have done the same analysis using the proposed analysis cycle for SkyDrive application (Quick & Choo, 2013a) and Dropbox application (Quick & Choo, 2013b) on a virtual computer running Windows 7.

To identify the gap of the research, due to the relatively recent prevalence of the cloud storage services for the smartphones, the researches of Hale (2013) did not provide a digital forensic framework for the investigation. Chung et al. (2012) have proposed a framework, however, the framework did not include the collection and analysis of the internal memory and network traffic. Additionally, the preservation of the evidence was not considered in that research. The proposed framework of (Quick & Choo, 2013a, 2013b, 2014) was developed as a cyclic framework. However, making a cyclic framework shows only one round of the investigation. When the examiners need to start a new investigation and continue the previous investigations at the same time, the proposed framework should be iterative.

In terms of data remnants and artifacts, the content of the files in the research of Zhu (2011) could not be retrieved through using the forensics tools. Chung et al. (2012) indicated that the smartphones' internal memory could possibly consist of important information about users, such as IDs and passwords of the cloud storage services. In this connection, Hale (2013) stated that a knowledge of the artifacts that left behind using cloud storage applications prevents missing critical data during an investigation.

The researches' experiments were done using the old version of Android and iOS operating systems (OSs). The research of (Quick & Choo, 2014) was tied to certainly not having the ability to install the GoogleDrive cloud client application on the iPhone 3G with iOS version 4.2.1.

In spite of the researches of (Zhu, 2011; Chung et al., 2012; Hale, 2013; Quick and Choo, 2013a, 2013b, 2014), current mobile forensic analyzer tools, procedures and methods are able to extract valuable information from VoIP, Social Networking, and Mail Applications on smartphones. However, the mobile forensic analyzer tools may not acquire enough and valuable information from cloud client applications on smartphones (Zhu 2011; Quick and choo, 2013a). Consequently, in this research, the objective 1 was defined to fill such gaps.

In terms of evidence integrity and preservation, Oestreicher (2014) mentioned that the evidence might be altered during uploading and downloading actions, thus it is needed to prove the originality of the evidence or the evidence are sufficiently similar to satisfy the courts. The objective 2 of the research fills the gap regarding the evidence integrity and preservation by analyzing the files hash values and timestamps comparison to identify whether the downloaded files are sufficiently similar to the original files or not.

1.4 Research Objectives

The research proposes a digital forensic investigation framework for smartphones where forensics artifacts of cloud client storages would be detected. The objectives of the research are provided as follows.

1. To develop a digital forensic framework focusing on the analysis phase for smartphones namely Android and iOS platforms to assist the examiners and investigators in conducting digital forensic investigations into cloud client applications of OneDrive, Box, Mega, GoogleDrive and Dropbox.

2. To propose a method in preservation phase to examine and verify the integrity and the originality of the acquired data and evidence during downloading the files from the cloud client applications within Android and iOS platforms.

1.5 Research Questions

This section introduces the research questions and hypotheses to achieve the planned objectives of the research. For the purposes, a suitable methodology is pursued to form the research, upon which the experiments are based. The research questions are defined as follows.

1.5.1 Research Question 1

The first primary research question is:

Q1. What are the data remnants of using cloud client applications of OneDrive, Box, Mega, GoogleDrive and Dropbox within Android and iOS platforms?

The question 1 leads to the following hypotheses:

H0. There are no data remnants using the cloud client applications within Android and iOS platforms to determine the cloud service provider, username and password, or uploaded, downloaded, deleted, and shared files details.
H1. There are data remnants of using the cloud client applications within Android and iOS platforms to determine the cloud service provider, username and password, or uploaded, downloaded, deleted, and shared files details.

The first primary question leads to the sub-questions given below.

Q1a. What data artifacts remain in the Android device' internal memory of using the cloud client applications?
Q1b. What data artifacts remain in the Android device' internal storage of using the cloud client applications?
Q1c. What data artifacts remain in the Android device' network traffic of using the cloud client applications?
Q1d. What data artifacts remain in the iOS device' Backup files of using the cloud client applications?
Q1e. What data artifacts remain in the iOS device' internal storage of using the cloud client applications?
Q1f. What data artifacts remain in the iOS device' network traffic of using the cloud client applications?

1.5.2 Research Question 2

The second primary research question is defined as follows:

Q2. Is there any forensically sound method available to preserve the data remnants by using cloud client applications of OneDrive, Box, Mega, GoogleDrive and Dropbox within Android and iOS platforms?

The question 2 leads to the following hypotheses:

H0. File downloading activities of the cloud client applications do not alter the internal file data and the associated file metadata.
H1. File downloading activities of the cloud client applications alter the internal file data and the associated file metadata.
H2. File downloading activities of the cloud client applications alter the internal file data, but do not alter the associated file metadata.
H3. File downloading activities of the cloud client applications do not alter the internal file data, but alter the associated file metadata.

The first primary question also leads to the sub-questions below.

Q2a. Are the downloaded files during the downloading action using the cloud client applications on Android platform are identical to the original files?
Q2b. Are the downloaded files during the downloading action using the cloud client applications on iOS platform are identical to the original files?

1.6 Research Contributions

1. A digital forensic framework for smartphones of Android and iOS platforms which focuses on an analysis method to assist the examiners and investigators in conducting digital forensic investigations into cloud client applications of OneDrive, Box, Mega, GoogleDrive and Dropbox. To verify the framework, the data remnants of the most popular cloud client applications of OneDrive, Box, Mega, GoogleDrive and Dropbox within Android and iOS platforms are investigated.

2. Preservation method for the files contents and metadata during downloading the files from OneDrive, Box, Mega, GoogleDrive and Dropbox within Android and iOS platforms. Possible modifications in files content or metadata that may affect preservation of evidence from these platforms are examined.

1.7 Research Scope

The research was undertaken using Android version 4.2 and iOS version 7.1.2 for smartphones. Alternative operating systems and their versions may all have different outcomes and data remnants. Additionally, the research was limited to the most popular cloud client applications of OneDrive, Box, Mega, GoogleDrive and Dropbox at the time of undertaking this study. However, any other application may have different results and findings. Additionally, the research was undertaken using the proposed forensics analysis method on the smartphones components of internal memory and the internal storage. However, the network traffic of the devices was analyzed using the existing forensics tools.

This research was limited to rooted Samsung Galaxy Tab II, 16 GB, and a jailbroken iPad 4th generation (Wi-Fi + Cellular) with 32GB internal storage. However, non-jailbroken devices may provide different outcomes and information. Android and iOS devices normally do not allow access to the system files. This means that the file system is restricted and cannot be seen by the user. Therefore acquiring a physical bit-by-bit image from the internal memory and internal storage of the devices is not possible. Thus, to obtain these, it was necessary to root or jailbreak the devices first in order to get access to the file systems. For the Android device in hand for this research, the CF-Root method was used. The reason for choosing this method is that CF-Root keeps the device's firmware as close to stock as possible (Akmal, 2014). This means that this method applies the least amount of modification to the device's firmware and file system. For the iOS device in hand for this research, the Pangu freeware was used. The reason for choosing Pangu is that aside from Cydia, it does not install any other third party application on the iOS device (Esposito, 2014).

1.8 Thesis Structure

The thesis consists of an introduction and follows the chapters which describe the research in detail, and finally summarize the findings. The thesis also includes an overall summary, acknowledgements, table of contents, list of figures, tables, and a glossary of technical terms.

Chapter 1 introduces the overall topic, including background information regarding cloud storage, Smartphones, digital forensic investigation, and the issues faced by investigators. The problem statement of the research is discussed, and the objectives are listed. To conduct the objectives, the two main research questions and associated

hypotheses are discussed. Then, the limitation of this research is explained. In the end, the structure of the research is outlined.

Chapter 2 examines current literature focusing on cloud and smartphone forensic. The first section outlines cloud computing, digital forensic analysis, smartphone digital forensic and cloud storage implications. Issues relating to identification, preservation, analysis, and presentation are outlined. Additional issues are generally described, and a summary concludes the chapter.

Chapter 3 aims to clarify the research methodology applied to the thesis. The research methodology for each research question is detailed and answered. Finally, a summary concludes this chapter.

Chapter 4 outlines the proposed Digital Forensic investigation framework and the way this can be applied to the forensic analysis of the cloud storage on the smartphones. Each step of the framework has been explained (Commencement, Identification & Preparation, Acquisition, Preservation, Analysis, Reconstruction, and Reporting).

Chapter 5 describes the procedures of the framework for the analysis of five popular cloud storage services of OneDrive, Box, Mega, GoogleDrive and Dropbox. In each case, the data remnants on the Android device are first examined using the proposed framework. Next, the iOS device is examined to further assess the framework and to determine the data remnants. The data remnants regarding the cloud client applications are then explained and listed at the end of each smartphone examination. Then, the preservation of the data remnants is explained.

Chapter 6 concludes the overall research. In the first section, the research is outlined and the questions and hypotheses are listed, detailing the manner in which the questions are answered and how the objectives and contributions achieved. Next, a summery of the research and the areas for future research are then provided.

REFERENCES

Akmal, T. (2014). Root XXU1AOCV Android 5.0.2 Lollipop on Galaxy S6 G920F Official Firmware - Tutorial / Guide. Retrieved from http://www.teamandroid.com/2015/04/27/root-xxu1aocv-android-502-lollipop-galaxy-s6-g920f-official-firmware/

Al-Hadadi, M., & AlShidhani, A. (2013). Smartphone Forensics Analysis: A Case Study. *International Journal of Computer and Electrical Engineering*, 576–580. http://doi.org/10.7763/IJCEE.2013.V5.776

Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*, *9*, S24–S33. http://doi.org/10.1016/j.diin.2012.05.007

Ayers, R., Brothers, S., & Jansen, W. (2014, May). Guidelines on Mobile Device Forensics. NIST Special Publication 800-101 Revision 1.

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013). A critical review of 7 years of Mobile Device Forensics. *Digital Investigation*, *10*(4), 323–349. http://doi.org/10.1016/j.diin.2013.10.003

Birk, D., & Wegener, C. (2011). Technical Issues of Forensic Investigations in Cloud Computing Environments. In *2011 IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)* (pp. 1–10). http://doi.org/10.1109/SADFE.2011.17

Carrier, B., Spafford, E. H., & others. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, *2*(2), 1–20.

Chung, H., Park, J., Lee, S., & Kang, C. (2012). Digital forensic investigation of cloud storage services. *Digital Investigation*, *9*(2), 81–95. http://doi.org/10.1016/j.diin.2012.05.015

Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, *9*(SUPPL.), S90–S98. http://doi.org/10.1016/j.diin.2012.05.001

Esposito, D. (2014). How to jailbreak iOS 7.1 and 7.1.x with Pangu (Video). Retrieved from http://9to5mac.com/2014/06/23/how-to-jailbreak-ios-7-1-and-7-1-1-with-pangu-video/

García-Arenas, M., Merelo Guervós, J. J., Castillo, P., Laredo, J. L. J., Romero, G., & Mora, A. M. (2011). Using free cloud storage services for distributed evolutionary algorithms. In *Proceedings of the 13th annual conference on Genetic and evolutionary computation* (pp. 1603–1610). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2001792

Gupta, P., & Kumar, S. (2014). A Comparative Analysis of SHA and MD5 Algorithm. *Architecture*, *1*, 5.

Gu, Q., & Guirguis, M. (2014). Secure Mobile Cloud Computing and Security Issues. In *High Performance Cloud Auditing and Applications* (pp. 65–90). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4614-3296-8_3

Hale, J. S. (2013). Amazon Cloud Drive forensic analysis. *Digital Investigation*, *10*(3), 259–265.

Hogan, M., Liu, F., Sokol, A., & Tong, J. (2011). Nist cloud computing standards roadmap. *NIST Special Publication*, *35*. Retrieved from http://selil.com/CLOUD/thoughtData/1/NIST_CCSRWG_092_NIST_SP_500-291_Jul5.pdf

Houston, D. (2011, March). 6 Lessons from Dropbox - One Million Files Saved Every 15 minutes - High Scalability. Retrieved August 13, 2014, from http://highscalability.com/blog/2011/3/14/6-lessons-from-dropbox-one-million-files-saved-every-15-minu.html

Induruwa, A. (2011). Hidden in the clouds: The impact on data security and forensic investigation. In *Advances in ICT for Emerging Regions (ICTer), 2011 International Conference on* (pp. 77–77). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6075014

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006, August). Guide to Integrating Forensic Techniquws into Incident Response-SP800-86. omputer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg.

Li, J., Gu, D., & Luo, Y. (2012). Android Malware Forensics: Reconstruction of Malicious Events (pp. 552–558). IEEE. http://doi.org/10.1109/ICDCSW.2012.33

Ludwig, A., Fraser, J., & Williams, R. (2012). Crime scene examiners and volume crime investigations: an empirical study of perception and practice. *Forensic Science Policy & Management: An International Journal*, *3*(2), 53–61.

Martini, B., & Choo, K.-K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, *9*(2), 71–80.

Marturana, F., Me, G., & Tacconi, S. (2012). A Case Study on Digital Forensics in the Cloud. In *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)* (pp. 111–116). http://doi.org/10.1109/CyberC.2012.26

Mason, S., & George, E. (2011). Digital evidence and "cloud"computing. *Computer Law & Security Review*, *27*(5), 524–528.

McKemmish, R. (1999). *What is forensic computing?*. Australian Institute of Criminology. Retrieved from http://aic.gov.au/documents/9/C/A/%7B9CA41AE8-EADB-4BBF-9894-64E0DF87BDF7%7Dti118.pdf

McKinley, H. L. (2003). SSL and TLS: A Beginners' Guide. *SANS Institute*. Retrieved from http://scholar.google.com/scholar?cluster=15972673858310736913&hl=en&oi=scholarr

Mossberg, W. S. (2012, April 25). Google Stores, Syncs, Edits in the Cloud. *Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424052702303459004577362111867730108?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702303459004577362111867730108.html

Muda, A. K., Choo, Y.-H., Abraham, A., & N. Srihari, S. (Eds.). (2014). *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications* (Vol. 555). Cham: Springer International Publishing. Retrieved from http://ezproxy.upm.edu.my:2135/book/10.1007/978-3-319-05885-6

Nelson, B., Phillips, A., & Steuart, C. (2010). Lab Manual for Nelson/Phillips/Steuart's Guide to Computer Forensics and Investigations. Retrieved from http://dl.acm.org/citation.cfm?id=1965161

Oestreicher, K. (2014a). A forensically robust method for acquisition of iCloud data. *Digital Investigation*, *11*, S106–S113.

Oestreicher, K. (2014b). A forensically robust method for acquisition of iCloud data. *Digital Investigation*, *11*, S106–S113. http://doi.org/10.1016/j.diin.2014.05.006

Palmer, G. (2001). A road map for digital forensic research. *Proceedings of the 2001 Digital Forensic Research Workshop*.

Quick, D., & Choo, K.-K. R. (2013a). Digital droplets: Microsoft SkyDrive forensic data remnants. *Future Generation Computer Systems*, *29*(6), 1378–1394. http://doi.org/10.1016/j.future.2013.02.001

Quick, D., & Choo, K.-K. R. (2013b). Dropbox analysis: Data remnants on user machines. *Digital Investigation*, *10*(1), 3–18.

Quick, D., & Choo, K.-K. R. (2013c). Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? *Digital Investigation*, *10*(3), 266–277.

Quick, D., & Choo, K.-K. R. (2014). Google Drive: Forensic analysis of data remnants. *Journal of Network and Computer Applications*, *40*, 179–193. http://doi.org/10.1016/j.jnca.2013.09.016

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, *1*(3).

Sameera Almulla, Y. I. (2013). Cloud forensics: A research perspective. http://doi.org/10.1109/Innovations.2013.6544395

Samet, N., Ben Letaifa, A., Hamdi, M., & Tabbane, S. (2014). Forensic investigation in Mobile Cloud environment (pp. 1–5). IEEE. http://doi.org/10.1109/SNCC.2014.6866510

SeungHwan, J., Gelogo, Y. E., & Park, B. (2012). Next Generation Cloud Computing Issues and Solutions. *International Journal of Control & Automation*, *5*(1). Retrieved from http://scholar.google.com/scholar?cluster=15056064319856074108&hl=en&oi=scholarr

Slusky, L., Partow-Navid, P., & Doshi, M. (2012). Cloud computing and computer forensics for business applications, 43–53.

Socha, S., & Gelbmann, T. (2005). EDRM File Format Data Set 1.0.1. Retrieved January 17, 2015, from http://www.edrm.net/resources/data-sets/edrm-file-format-data-set

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. *Computer Law & Security Review*, *26*(3), 304–308.

Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). Forensic investigation of cloud computing systems. *Network Security*, *2011*(3), 4–10. http://doi.org/10.1016/S1353-4858(11)70024-1

Taylor, M., Hughes, G., Haggerty, J., Gresty, D., & Almond, P. (2012). Digital evidence from mobile telephone applications. *Computer Law & Security Review*, *28*(3), 335–339.

Wen, Y., Man, X., Le, K., & Shi, W. (2013). Forensics-as-a-Service (FaaS): Computer Forensic Workflow Management and Processing Using Cloud (pp. 208–214). Presented at the CLOUD COMPUTING 2013, The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization. Retrieved from http://www.thinkmind.org/index.php?view=article&articleid=cloud_computing_2013_8_40_20185

Wolthusen, S. D. (2009). Overcast: Forensic discovery in cloud environments. In *IT Security Incident Management and IT Forensics, 2009. IMF'09. Fifth International Conference on* (pp. 3–9). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5277835

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). COMMON PHASES OF COMPUTER FORENSICS INVESTIGATION MODELS. *International Journal of Computer Science & Information Technology (IJCSIT)*, *3*(3).

Zainudin, N. M., Merabti, M., & Llewellyn-Jones, D. (2010). A digital forensic investigation model for online social networking. *Proceedings of the 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting, Liverpool*, 21–22.

Zawoad, S., Dutta, A. K., & Hasan, R. (2013). SecLaaS: Secure Logging-as-a-Service for Cloud Forensics. *arXiv:1302.6267 [cs]*. Retrieved from http://arxiv.org/abs/1302.6267

Zhu, M. (2011). *Mobile Cloud Computing: implications to smartphone forensic procedures and methodologies* (Thesis). Auckland University of Technology. Retrieved from http://aut.researchgateway.ac.nz/handle/10292/2660