



UNIVERSITI PUTRA MALAYSIA

***AN ANALYSIS METHOD OF FORENSIC INVESTIGATION FOR
PLATFORM-AS-A-SERVICE CLOUD STORAGE SERVICES***

KAVEH SHAERPOUR

FSKTM 2016 41



**AN ANALYSIS METHOD OF FORENSIC INVESTIGATION FOR
PLATFORM-AS-A-SERVICE CLOUD STORAGE SERVICES**

By

KAVEH SHAERPOUR

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

December 2016

COPYRIGHT

All material contained within the thesis, including without limitation text, logos, icons, photographs and all other artwork, is copyright material of Universiti Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial use of material may only be made with the express, prior, written permission of Universiti Putra Malaysia.

Copyright © Universiti Putra Malaysia



Abstract of thesis presented to the Senate of University Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

AN ANALYSIS METHOD OF FORENSIC INVESTIGATION FOR PLATFORM-AS-A-SERVICE CLOUD STORAGE SERVICES

By

KAVEH SHAERPOUR

December 2016

Chair: Ramlan Mahmod, PhD

Faculty: Computer Science and Information Technology

Cloud computing has changed most of the ways users interact with computers and mobile devices. Every user, power-users or normal users, can take advantage of Cloud storage and in such a way that they can develop or store their data in cloud and access them anytime they want. There are three types of cloud Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) but our focus is PaaS. Though, PaaS has made it easier to code and develop new application for developers, it has helped criminals to write their malicious application with minimum trace as well. PaaS cloud client applications could be a very useful for forensics investigators as they contain much information about the user. Although, there have been many digital forensics researches done on SaaS and IaaS, there have been close to none such research on PaaS. Therefore, the problem here is first there is not enough research in PaaS and second criminals use this service to create malicious applications.

Previous researches on forensic analysis of PaaS cloud applications on Windows machines and smartphones used present forensic analyser tools and failed to detect all the data remnants such as file contents, email addresses, activity trails of users and many more. Also, majority of works were done on SaaS and IaaS cloud applications.

In this research, to address the problems of lack of work on PaaS and lack of enough forensic data after analysis we propose a new analysis method for PaaS cloud applications to maximise the amount forensic that can be extracted in process of analysis. The proposed analysis method is valid for examining the internal storage, internal memory and network traffic of PC and smartphones. In the proposed analysis method of this project, the raw data of collected images is analysed. This analysis is done based on predefined keywords to detect login information. Upon identification of user's data and pattern, the keywords which are common among PaaS applications are defined and then the raw data of images are analysed once again to find any remaining

data remnants on the system. After the evidences are found and extracted then the researcher proceeds to presenting the findings in a report form. The new analysis method is tested on popular PaaS client applications namely Openshift and Heroku on Windows PC and mobile platforms iOS and Android.

The outcome of this research establishes the use of the mentioned PaaS applications on the investigated computers and smartphones and results in identification of artefacts such as usernames, passwords, login information, application source code and application information. The result of this research assists forensic examiners and practitioners in understanding the types of artefacts that are likely to remain on Windows machines and iOS and Android smartphones after using PaaS applications and also it helps these applications' developers to make the applications more secure and users to know the security issues of these applications.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia Sebagai memenuhi keperluan untuk ijazah Master Sains

**KAEDAH ANALITIK UNTUK PENYIASATAN FORENSIK BAGI
PERKHIDMATAN STORAN AWAN PLATFORM-SEBAGAI-PERKHIDMATAN**

Oleh

KAVEH SHAERPOUR

Disember 2016

Chair: Ramlan Mahmod, PhD

Fakulti: Sains Komputer Dan Teknologi Maklumat

Pengkomputeran cloud telah mengubah kebanyakan cara berinteraksi antara komputer dan peranti mudah alih. Setiap pengguna, samada power users atau pengguna biasa, boleh memanfaatkan penyimpanan cloud di dalam apa-apa cara dimana mereka boleh membangunkan atau menyimpan data mereka di dalam cloud dan mengaksesnya bila-bila saja mereka mahu. Terdapat tiga jenis cloud, Platform as a Service (PaaS), Software as a Service (SaaS) dan Infrastructure as a Service (IaaS) tetapi tumpuan utama kita adalah PaaS. Walaupun PaaS telah memudahkan kod dan membangunkan aplikasi baru untuk pemaju, ia juga telah membantu penjenayah untuk menulis aplikasi tidak baik mereka sendiri dengan kesan yang minima. Klien aplikasi PaaS cloud boleh menjadi sangat berguna untuk penyiasat forensik kerana ia mengandungi banyak informasi tentang pengguna. Walaupun terdapat banyak kajian forensik digital yang telah dilakukan pada SaaS dan IaaS, tiada kajian berkenaan PaaS. Oleh itu, masalah di sini adalah pertama, tiada kajian yang mencukupi keatas PaaS dan kedua, penjenayah menggunakan servis ini untuk mencipta aplikasi yang tidak baik.

Kajian sebelum ini terhadap analisi forensik aplikasi PaaS cloud pada mesin Windows dan telefon pintar menggunakan alatan analisis forensik masa kini dan gagal untuk mengesan kesemua sisa data seperti kandungan fail, alamat email, jejak aktiviti pengguna dan banyak lagi. Juga, majoriti kerja dilakukan pada SaaS dan aplikasi cloud IaaS.

Dalam kajian ini, bagi menangani masalah kekurangan kerja ke atas PaaS dan kekurangan data forensik selepas analisis, kami mencadangkan satu kaedah analisis baru untuk aplikasi cloud PaaS supaya dapat memaksimumkan jumlah forensik yang boleh diekstrak dalam proses analisis. Kaedah analisis yang dicadangkan sah untuk memeriksa penyimpanan dalaman, memori dalaman dan rangkaian trafik PC dan telefon pintar. Dalam cadangan kaedah analisis projek ini, data mentah imej yang terkumpul dianalisis. Analisis ini dilakukan berdasarkan kata kunci yang telah

ditetapkan untuk mengesan maklumat log masuk. Melalui pengenalpastian data dan corak pengguna, kata kunci yang biasa dikalangan aplikasi PaaS ditakrifkan dan kemudian imej data mentah dianalisis sekali lagi untuk mencari mana-mana baki sisa data di dalam sistem. Selepas menjumpai bukti-bukti dan diekstrak, penyelidik kemudiannya membentangkan hasil kajian dalam bentuk laporan. Kaedah analisis baru ini telah diuji terhadap klien aplikasi PaaS yang popular iaitu Openshift dan Heroku pada Windows PC dan platform mudah alih iOS dan Android.

Hasil kajian ini menetapkan penggunaan aplikasi PaaS yang disebut pada komputer dan telefon pintar yang disiasat dan hasil identifikasi dari artifak seperti nama pengguna, kata laluan, maklumat log masuk, aplikasi kod sumber dan aplikasi maklumat. Hasil kajian ini membantu pengamal dan pemeriksa forensik dalam memahami jenis artifak yang berkemungkinan kekal pada mesin Windows dan telefon mudah alih iOS dan Android selepas menggunakan aplikasi PaaS dan juga membantu pemaju-pemaju aplikasi ini untuk membuat aplikasi yang lebih selamat dan pengguna tahu tentang isu keselamatan aplikasi ini.

ACKNOWLEDGEMENT

I appreciate my supervisor committee Prof. Dr. Ramlan Mahmod and Assoc. Prof. Dr. Nur Izura for their guidance and help without which I would not be able to finish this project. I must thank all my friends and classmates who helped and supported me for every aspect of this thesis.

I thank my parents and my brother who supported me in every way possible and kept their patience with me during my master's studies.



This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Ramlan Mahmod, PhD

Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Chairman)

Nur Izura binti Udzir, PhD

Associate Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Member)

ROBIAH YUNUS, PhD

Professor and Dean

School of Graduate Studies

Universiti Putra Malaysia

Date:

Declaration by 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.: Kaveh Shaerpour, GS34380

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: _____
Name of Chairman of
Supervisory
Committee: _____

Signature: _____
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	xv
CHAPTER	
1 INTRODUCTION	1
1.1 Background	1
1.2 Problem Statement	1
1.3 Research Objectives	2
1.4 Research Questions	3
1.4.1 Research Question 1	3
1.5 Research Scope	3
1.5.1 Version Dependent	3
1.5.2 Platform Dependent	4
1.5.3 Hardware Dependent	4
1.6 Thesis Organisation	4
2 LITERATURE REVIEW	6
2.1 Introduction	6
2.2 Cloud computing and cloud storage	6
2.3 Digital Forensic Investigations	7
2.4 Cloud Storage and Digital Investigations	9
2.4.1 Mobile devices analysis	10
2.5 Current Related Researches	11
2.6 Summary	12
3 METHODOLOGY	14
3.1 Introduction	14
3.2 Design	14
3.3 Implementation	15
3.3.1 Data Set	16
3.3.2 Data Remnant Implementation	16
3.3.3 Research Equipment	22
3.4 Experimentation Design	22
3.4.1 Data Remnant Experiment Design	22
3.5 Analysis	26
3.6 Summary	27

4	THE DESIGN OF ANALYSIS METHOD	28
4.1	Introduction	28
4.2	Analysis Method	28
4.3	PaaS Analysis Method (PAM)	28
4.4	Summary	32
5	RESULTS AND DISCUSSIONS	33
5.1	Introduction	33
5.2	Experiment 1	33
	5.2.1 Windows Results	33
	5.2.2 iOS Results	58
	5.2.3 Android Client App-Based	64
5.3	Summary	68
6	CONCLUSION	71
6.1	Introduction	71
6.2	Conclusion	71
6.3	Future Works	72
	REFERENCES	73
	BIODATA OF STUDENT	76
	LIST OF PUBLICATIONS	77

LIST OF TABLES

Table	Page
2.1. Cloud Overview	7
3.1. Login IDs used for experiments	16
3.2. Details of Created Virtual Machines for Openshift (OS) and Heroku (H)	20
3.3. Research Equipment	22
3.4. List of Keywords Used	26
5.1. Forensics artefacts found in Windows and web-based analysis	68
5.2. Forensics artefacts found in iOS and Android analysis	69



LIST OF FIGURES

Figure	Page
3.1. Research Steps	15
3.2. Bloc Diagram for Windows Native App	17
3.3. Bloc Diagram for Windows Browsers	18
3.4. Bloc Diagram for Android	18
3.5. Bloc Diagram for iOS	19
3.6. Diagram of created VMs	21
3.7. Experiments Process	24
4.1. Digital Forensic Analysis Cycle	29
4.2. Analysis method comparison between this project and past projects	30
4.3. PaaS Analysis Method (PAM)	31
5.1. Prefetch Files Location	34
5.2. Location of authorization token	34
5.3. Private Key	35
5.4. Sample of RegRipper Output	36
5.5. The occurrences of username within memory	36
5.6. The Openshift Credential	37
5.7. Name of the application created found in memory	37
5.8. Source Code Found	38
5.9. Application content found	38
5.10. Deleted application found	39
5.11. Capture files when user signed in	40
5.12. Prefetch Files Location	41
5.13. Private Key	42
5.14. Sample of RegRipper Output	43
5.15. The occurrences of username within memory	43
5.16. The Heroku Credential	44
5.17. Name of the application created found in memory	44
5.18. Source Code Found	45
5.19. Application content found	45
5.20. Deleted application found	46
5.21. Uninstallation of Client Software	47
5.22. Capture files when user signed in	47
5.23. The occurrences of username within memory	48
5.24. The Openshift Credential	48
5.25. Name of the application created found in memory	49
5.26. Source Code Found	50
5.27. Application content found	50
5.28. Deleted application found	51
5.29. Openshift History Files	51
5.30. Openshift Cache File	52
5.31. Openshift Cookies Files	52
5.32. DNS Tab Results	53
5.33. The occurrences of username within memory	53
5.34. The Heroku Credential	54

5.35. Name of the application created found in memory	54
5.36. Source Code Found	55
5.37. Application content found	55
5.38. Deleted application found	56
5.39. Heroku History Files	56
5.40. Heroku Cache File	57
5.41. Heroku Cookies Files	57
5.42. DNS Tab Results	58
5.43. Hex Display of directory of Openshift	59
5.44. The occurrences of username within memory	59
5.45. The Openshift Mobile Credential	60
5.46. Cache display of Openshift	60
5.47. Capture files when user signed in	61
5.48. Hex Display of directory of Heroku (Manoku)	62
5.49. The occurrences of username within memory	62
5.50. The Heroku (Manoku) Credential	63
5.51. Cache display of Heroku (Manoku)	63
5.52. Capture files when user signed in	64
5.53. The occurrences of username within memory	65
5.54. The Openshift Credential	65
5.55. Capture files when user signed in	66
5.56. The occurrences of username within memory	67
5.57. The Heroku Credential	67
5.58. Capture files when user signed in	68

LIST OF ABBREVIATIONS

ACPO	Association of Chief Police Officers
DD	Disk Dump
DFRWS	Digital Forensic Research Workshop
FTK	Forensic Tool Kit
iOS	Apple iPhone Operating System
IP	Internet Protocol
MD5	Message Digest 5
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
OS	Operating System
PCAP	Network Traffic Capture File
SHA1	Secure Hash Algorithm 1
SWGDE	Scientific Working Group on Digital Evidence
USB	Universal Serial Bus

CHAPTER 1

INTRODUCTION

1.1 Background

Cloud storage is relatively a new field in Information Technology although it has its roots in 1960's ARPA projects (Watson, 2009). Cloud storage is the network of servers that are accessible from anywhere any time. NIST have defined cloud as "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011). Baun, et al. (2011) have explained NIST model more in depth and they stated that NIST model consists of five crucial characteristics, three kind of service model and four deployment models. The five characteristics of NIST cloud model are on demand self-service, ubiquitous (broad) network access, resource pooling, rapid elasticity or expansion and measured service. Yang & Jia (2014) have explained the service models and deployment models of cloud storage services. The deployment models of cloud storage services are private cloud, community cloud, public cloud and hybrid cloud. Daryabar et al. (2013) have identified three service models of cloud based on NIST model as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Since the rate of growth and popularity of cloud between users has increased in past few years each company has started to offer a cloud storage service such as Dropbox, Amazon and Evernote (Chung, et al. 2012) and Google Drive, Microsoft OneDrive (Quick & Choo, 2013b, 2013c) and Apple iCloud (Oestreicher, 2014). All these attentions given to cloud has attracted different kind of clients, some just upload their personal or corporate data and some commit criminal activities in the cloud.

Criminals have started to use cloud to either target other cloud storage systems or to store their criminal data. They use cloud to store materials such as child pornography videos or pictures, data about their illegal operation or they use cloud storage services (Martini & Choo, 2013) to attack other services which happened to Sony PlayStation store which was attack from an Amazon server (Wagenseil, 2011) or they attack the cloud storage services and leak users' personal data as happened in iCloud incident (Griffiths, 2014). The issue facing forensic investigators is to identify the data remnant such as login information. Therefore, analysis of devices such computers or smartphones may provide helpful information for investigators.

1.2 Problem Statement

In recent researches on cloud forensics, Zhu (2011) investigated cloud client application of Dropbox on Android and iOS. In that research by using tools such as XRY and Oxygen forensic tools, the researcher found and retrieved information such

usernames and filenames but not contents of the files. Chung et al. (2012) proposed a process model for forensic investigation of SaaS applications such as Amazon S3, Dropbox, Evernote and Google Docs on Windows and Android and iOS. The proposed model was designed to investigate back up files of internal storages. Hale (2013) discussed the data remnants of Amazon cloud drive on Windows XP and 7. Mahajan, et al. (2013) performed digital forensic investigation on Viber and WhatsApp client applications on Android devices. Ruan & Carthy (2013) have experimented a forensics model for cloud storage services such as PaaS. The model is Cloud Forensic Maturity Model (CFMM) which composes of two inter-related parts, the Cloud Forensic Investigative Architecture (CFIA) and the Cloud Forensic Capability Matrix (CFCM). In their research, the researchers aimed to create a unified framework for cloud forensics on computers. Quick and Choo (2013c) proposed a forensic analysis cycle for Google Drive on Windows 7 and iPhone 3G. They used XRY application to perform iOS device investigation. Furthermore, the authors have performed same analysis by using their proposed framework on SkyDrive (2013a) and Dropbox (2013b) on a virtual machine running Microsoft Windows 7. Alqahtany et al. (2016) proposed A forensic acquisition and analysis system for IaaS which consists of multiple agents to gather data from different parts of cloud to perform analysis on it.

Regarding data remnants findings in the mentioned researches, Zhu (2011) could not retrieve the content of files by using forensic tools. Chung et al (2012) showed that internal memory of smartphones could potentially contain valuable information such as login data. Ruan & Carthy (2013) only provided their model that was proposed for PaaS and the rest of cloud types but they did not show any analysis done using the model. Alqahtany et al. (2016) did not provide any findings of experiment in their research.

Even though the researches done by Zhu (2011), Chung et al. (2012), Hale (2013) Quick and Choo (2013a, 2013b, 2013c) and Alqahtany et al. (2016) have existed and many current analysis tools and methods are able to retrieve very important information from VoIP, Social networking and SaaS cloud applications on smartphones and computers but the methods used in these researches and tools may not retrieve enough valuable information from cloud client applications on both computers and smartphone (Simou et al, 2014). As it is shown the most of these analysis methods are focused on SaaS type of cloud and there is close to none models on PaaS cloud and they do not help investigator to retrieve majority of forensic data. To fill this gap and create an analysis method to maximise the extraction of valuable forensic data which is developed for PaaS cloud type, the objective 1 was defined.

1.3 Research Objectives

This research proposes an analysis method to investigate both computers and smartphones to retrieve valuable forensic artefacts stored on them after using PaaS cloud storage client applications. The objective of this research is as follow

- 1) To develop an analysis method to help examiners, researchers and investigators to follow a forensically sound standard process when analysing PaaS cloud storage applications.

The discovery of data remnants provides a more in-depth understanding of the kind of artefacts that are most likely to remain and help the examiners in different stage of their examinations.

1.4 Research Questions

The following research questions are defined to achieve the research objectives in more organised manner.

1.4.1 Research Question 1

Question 1. What data remnants remains on hard disk using PaaS cloud storage services within Microsoft Windows, iOS and Android?

Question 1 leads to hypothesis 1 and 2;

Hypothesis 1. There are data remnants when using the PaaS cloud storage applications on Microsoft Windows, iOS and Android which can be used to identify login information, application storage data and application modification data.

Hypothesis 2. There are no data remnants when using the PaaS cloud storage applications on Microsoft Windows, iOS and Android which can be used to identify login information, application storage data and application modification data.

1.5 Research Scope

In this research, it is assume that the person who investigate the victim's machine has a real-time access to it. This scenario is applied when the victim's machine is connected to a network and its administrator has complete access to it or investigators have gotten real-time access with rootkits. This assumption is critical because some of the remnants are found in the internal memory.

The proposed framework of this research can be used on most of the PaaS cloud clients on computers and smartphones, however, different types of data remnants could be recovered when different platforms, versions and hardware are investigated, therefore, limitations of this research are only relevant to the data remnants and recovered artefacts not to the proposed framework.

1.5.1 Version Dependent

Since this research is quasi-experimental in nature, obtained results are applicable to the software versions available at the time of conducting the research. Previous

software versions may result in different findings and future software versions may have different outcomes from the ones obtained in this research.

1.5.2 Platform Dependent

This research focused on identifying the data remnants residing on Windows, Android and iOS platforms from the use of Heroku, and Openshift applications. Alternative platforms such as OS X and Windows Phone may produce different data remnants. Furthermore, other such applications such as Bluemix, Azure and AWS Elastic Beanstalk may result in different data remnants. Therefore, different outcomes may be achieved in relation to research questions when different platforms and applications are involved.

1.5.3 Hardware Dependent

This research was conducted using a Windows 8.1 PC, a jailbroken Apple iPhone running iOS 8.1 and a rooted Samsung Galaxy S4 running Android 4.4.2. Thus, other OS versions and other phones may present different results. In addition, a non-jailbroken or not rooted devices may provide less information since acquiring a physical image and obtaining the slack spaces from the internal storage is not possible.

1.6 Thesis Organisation

This thesis begins with an abstract which provides a summary of the research and continues with acknowledgments, approval, and declaration, list of figures, list of tables and list of abbreviations used in the thesis.

Chapter 1- Introduction begins with background which provides information about PaaS Cloud storage and digital forensic investigation to introduce the topic of the research to reader. Background is followed by problem statement where the gap of research and the reason for conducting this research is described. Then, the objectives of the research are outlined. Finally, research scopes are highlighted and structure of the thesis is explained.

Chapter 2- Literature Review provides a review of current literature relevant to this research. This chapter provides an outline on PaaS cloud, digital forensic analysis and mobile forensics analysis. Existing issues in forensic analysis of PaaS cloud storage services applications are highlighted and a summary concludes the chapter.

Chapter 3- Methodology explains the nature of the research and outlines the research steps. Research methodology for each research objective and experiments process are described in detail along with the dataset used for experiments. Finally, equipment and software used for research experiments are listed and the chapter is concluded.

Chapter 4- The Design of Analysis Method presents the analysis method proposed for this research and explains each step of the analysis method and listing all the necessary keywords to perform the analysis on the machines.

Chapter 5- Results and Discussions presents analysis results of Heroku and Openshift PaaS cloud storage services applications within Windows, Android and iOS devices utilizing the proposed analysis method. Analysis is undertaken to determine the data remnants of each application. Afterwards, integrity and validity of file data and metadata of PaaS cloud storage services files on each application within Windows, Android and iOS platforms are discussed. Results and findings of the analysis are presented and discussed and the chapter is concluded with the summary.

Chapter 6- Conclusion provides a summary of the research and thesis. First, a summary of what has been done throughout the thesis is provided and then the results and outcomes of the research are presented. Finally, validity, implications of the research and future research opportunities are discussed.

REFERENCES

- ACPO. (2007). Good Practice Guide for Computer-Based Electronic Evidence Official release version 4.0. 7safe. Retrieved on 30 October 2014, Retrieved from http://www.7safe.com/electronic_evidence/
- Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, 5(1), 118–131.
- Alqahtany, S., Clarke, N., Furnell, S., & Reich, C. (2016). A forensic acquisition and analysis system for IaaS. *Cluster Computing*, 19(1), 439–453. <https://doi.org/10.1007/s10586-015-0509-x>
- Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on mobile device forensics* (No. NIST SP 800-101r1). National Institute of Standards and Technology. Retrieved from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>
- Baun, C., Kunze, M., Nimis, J., & Tai, S. (2011). *Cloud Computing*. Berlin, Heidelberg: Springer Berlin Heidelberg.
- Brezinski, D., & Killalea, T. (2002). Guidelines for Evidence Collection and Archiving. The Internet Society. Retrieved from <https://www.ietf.org/rfc/rfc3227.txt>
- 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>
- Cybercrime Lab. (2007). Digital Forensic Analysis Methodology. Department of Justice (DOJ). Retrieved from http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/forensics_chart.pdf
- CyberSecurity Malaysia. (2014). Corporate Overview. Accessed on 20 October 2014, Retrieved from http://www.cybersecurity.my/en/about_us/corporate_overview/main/detail/2065/index.html
- Daryabar, F., Dehghantanha, A., Udzir, N. I., Mohd Sani, N. F. binti, bin Shamsuddin, S., & Norouzizadeh Dezfoli, F. (2013). A Review on Impacts of Cloud Computing on Digital Forensics. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 2(2), 77–94.
- 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>
- Government of Malaysia. (1997). Act 563: Computer Crimes Act 1997. The Commissioner of Law Revision, Malaysia.
- Griffiths, S. (2014). Are iCloud leaks making retro tech more popular? [Magazine]. Retrieved 15 November 2014, from <http://www.dailymail.co.uk/sciencetech/article-2828641/Are-iCloud-leaks-making-retro-tech-popular-Polaroid-camera-sales-soar-people-seek-pictures-private.html>
- Guo, H., Jin, B., & Shang, T. (2012). Forensic investigations in Cloud environments. In *2012 International Conference on Computer Science and Information Processing (CSIP)* (pp. 248–251). <http://doi.org/10.1109/CSIP.2012.6308841>

- Hale, J. S. (2013). Amazon Cloud Drive forensic analysis. *Digital Investigation*, 10(3), 259–265.
- Kirk, J. (2012). If Megaupload users want their data, they're going to have to pay. Retrieved 30 October 2014, from http://www.techworld.com.au/article/427341/megaupload_users_want_their_data_they_re_going_pay/
- Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. (2013). Forensic Analysis of Instant Messenger Applications on Android Devices. *arXiv Preprint arXiv:1304.4915*. Retrieved from <http://arxiv.org/abs/1304.4915>
- Martini, B., & Choo, K.-K. R. (2013). Cloud storage forensics: ownCloud as a case study. *Digital Investigation*, 10(4), 287–299. <http://doi.org/10.1016/j.diin.2013.08.005>
- Maturana, 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>
- McKemmish, R. (1999). *What is forensic computing?* Canberra: Australian Institute of Criminology.
- Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. Retrieved from <http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf>
- Nelson, B., Phillips, A., & Steuart, C. (2010). *Guide to computer forensics and investigations* (3rd ed.). Boston, MA: Course Technology Cengage Learning.
- NIJ. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (Special Report No. NCJ 199408). US Department of Justice, Office of Justice Program, National Institute of Justice. Retrieved from <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>
- NIJ. (2008). *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition* (Special Report No. NCJ 219941). Retrieved from <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>
- Oestreicher, K. (2014). A forensically robust method for acquisition of iCloud data. *Digital Investigation*, 11, S106–S113. <http://doi.org/10.1016/j.diin.2014.05.006>
- Poisel, R., & Tjoa, S. (2012). Discussion on the Challenges and Opportunities of Cloud Forensics. In G. Quirchmayr, J. Basl, I. You, L. Xu, & E. Weippl (Eds.), *Multidisciplinary Research and Practice for Information Systems* (Vol. 7465, pp. 593–608). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Ponemon Institute. (2011). Security of Cloud Computing Providers Study. Sponsored by CA Technologies. Retrieved from <http://www.ca.com/~media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf>
- Quick, D. (2012). *Forensic Analysis of Cloud Storage Client Data* (Master's Thesis). University of South Australia, Adelaide, South Australia.
- 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. <http://doi.org/10.1016/j.diin.2013.02.003>
- Quick, D., & Choo, K.-K. R. (2013c). 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>

- Reilly, D., Wren, C., & Berry, T. (2011). Cloud Computing: Pros and Cons for Computer Forensic Investigations. *International Journal Multimedia and Image Processing*, 1(1), 1–7.
- Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, 1(3), 1–12.
- Ruan, K., & Carthy, J. (2013). Cloud Forensic Maturity Model. In M. Rogers & K. C. Seigfried-Spellar (Eds.), *Digital Forensics and Cyber Crime* (Vol. 114, pp. 22–41). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud Forensics. In G. Peterson & S. Sheno (Eds.), *Advances in Digital Forensics VII* (Vol. 361, pp. 35–46). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud Forensics Solutions: A Review. In L. Iliadis, M. Papazoglou, & K. Pohl (Eds.), *Advanced Information Systems Engineering Workshops* (Vol. 178, pp. 299–309). Thessaloniki, Greece: Springer International Publishing.
- 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. <http://doi.org/10.1016/j.clsr.2012.03.006>
- Wagenseil, P. (2011). Amazon's Cloud Servers Possibly Used in Sony Attack. Retrieved 23 February 2017, from http://www.nbcnews.com/id/43054841/ns/technology_and_science-security/t/amazons-cloud-servers-possibly-used-sony-attack/#.WLWUjn-K9-Z
- Watson, D. L. (2009). Hey – Get Off My Cloud! In H. Jahankhani, A. G. Hessami, & F. Hsu (Eds.), *Global Security, Safety, and Sustainability* (Vol. 45, pp. 224–232). Berlin, Heidelberg: Springer Berlin Heidelberg.
- 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.
- Williams, J. (2012). ACPO Good Practice Guide for Digital Evidence, Version 5. Metropolitan Police Service.
- Yang, K., & Jia, X. (2014). *Security for Cloud Storage Systems*. New York, NY: Springer New York.
- Zawoad, S., Dutta, A. K., & Hasan, R. (2013). SecLaaS: Secure Logging-as-a-Service for Cloud Forensics. arXiv:1302.6267. Retrieved from <http://arxiv.org/abs/1302.6267>
- , M. (2011). Mobile Cloud Computing: implications to smartphone forensic procedures and methodologies (Thesis). Auckland University of Technology.