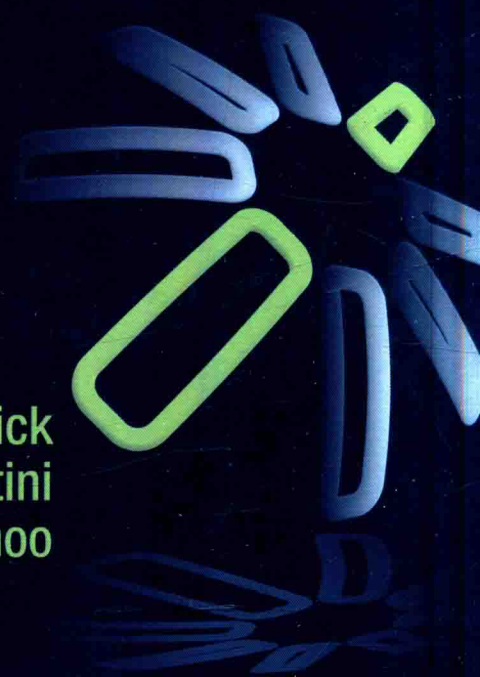
SYNGRESS

Cloud Storage Forensics



Darren Quick
Ben Martini
Kim-Kwang Raymond Choo

Cloud Storage Forensics

Darren Quick

Ben Martini

Kim-Kwang Raymond Choo

Brett Shavers, Technical Editor

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Syngress is an imprint of Elsevier

SYNGRESS

Acquiring Editor: *Chris Katsaropoulos*
Editorial Project Manager: *Benjamin Rearick*
Project Manager: *Punithavathy Govindaradjane*
Designer: *Mark Rogers*

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Quick, Darren.
Cloud storage forensics/Darren Quick, Ben Martini, Kim-Kwang Raymond Choo.
pages cm
ISBN 978-0-12-419970-5
1. Computer crimes–Investigation. 2. Forensic sciences–Data processing. 3. Cloud computing. 4. Information storage and retrieval systems. I. Martini, Ben, 1990- II. Choo, Kim-Kwang Raymond. III. Title.
HV8079.C65Q53 2014
363.250285'46782--dc23
2013037978

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-419970-5

Printed and bound in the United States of America
14 15 16 17 18 10 9 8 7 6 5 4 3 2 1

Cloud Storage Forensics

This book is dedicated to our families for their tireless support and understanding throughout all the time we spent on this research.

Acknowledgments

We would like to acknowledge the support provided by the University of South Australia and South Australia Police, and in particular the first author's supervisor, Detective Senior Sergeant Barry Blundell. The second author is supported by funding from the University of South Australia and the Defence Systems Innovation Centre (DSIC).

We are also grateful to Chris Katsaropoulos, Senior Acquisitions Editor, and Ben Rearick, Editorial Project Manager at Syngress, and the technical reviewer for their support in this project. It is not easy to keep on schedule, but they were relentless ... in a good way.

The views and opinions expressed in this book are those of the authors alone and not the organizations with whom the authors have been associated or supported. This book was hosted, and some parts written, using cloud storage.

Darren Quick
Ben Martini
Kim-Kwang Raymond Choo

About the Authors

Darren Quick is an Electronic Evidence Specialist with the South Australia Police and a PhD Scholar at the Information Assurance Research Group, Advanced Computing Research Centre at the University of South Australia. He has undertaken over 550 forensic investigations involving thousands of digital evidence items including computers, hard drives, mobile telephones, servers, and portable storage devices. He holds a master of science degree in Cyber Security and Forensic Computing, and has undertaken formal training in a range of forensic software and analysis techniques. In 2012, Darren was awarded membership of the Golden Key International Honour Society. Darren has coauthored a number of publications in relation to digital forensic analysis and cloud storage, and is a member of the Board of Referees for Digital Investigation—The International Journal of Digital Forensics and Incident Response. He still has his first computer, a VIC20, in the original box.

Ben Martini is the Digital Forensics Research Administrator, a Course Coordinator, and a PhD Scholar at the Information Assurance Research Group, Advanced Computing Research Centre at the University of South Australia. His PhD research focus is in the field of Digital Forensics looking at the implications of cloud computing. He has a broad range of research interests in the information technology sector with a focus on computer security and digital forensics issues. Ben has worked actively in the South Australian IT industry in sectors including government departments, education, and electronics across various organizations and continues to deliver occasional invited presentations to industry organizations in his area of expertise. He holds a master's degree in Business Information Systems and a bachelor degree in Information Technology (Networking and Security). He is supported by scholarships from both the University of South Australia and the Defence Systems Innovation Centre.

Dr Kim-Kwang Raymond Choo is a Fulbright Scholar and Senior Lecturer at the University of South Australia. He has (co)authored a number of publications in the areas of anti-money laundering, cyber and information security, and digital forensics including a book published in Springer's *Advances in Information Security* book series and six Australian Government Australian Institute of Criminology refereed monographs. He has been an invited speaker for a number of events (e.g., 2011 UNODC-ITU Asia-Pacific Regional Workshop on Fighting Cybercrime and 2011 KANZ Broadband Summit 2011) and delivered Keynote/Plenary Speeches at ECPAT Taiwan 2008 Conference on Criminal Problems and Intervention Strategy, 2010 International Conference on Applied Linguistics and 2011 Economic Crime Asia Conference, and 2014 International Conference on Applied Linguistics & Language Teaching, and Invited Lecture at the Bangladesh Institute of International and Strategic Studies. He was one of over 20

international (and one of two Australian) experts consulted by the research team preparing McAfee's commissioned report entitled "Virtual Criminology Report 2009: Virtually Here: The Age of Cyber Warfare"; and his opinions on cyber crime and cyber security are regularly published in the media. In 2009, he was named one of 10 Emerging Leaders in the Innovation category of The Weekend Australian Magazine/Microsoft's Next 100 series. He is also the recipient of several awards including the 2010 Australian Capital Territory (ACT) Pearcey Award for "Taking a risk and making a difference in the development of the Australian ICT industry," 2008 Australia Day Achievement Medallion in recognition of his dedication and contribution to the Australian Institute of Criminology, and through it to the public service of the nation, British Computer Society's Wilkes Award for the best paper published in the 2007 volume of The Computer Journal, and the Best Student Paper Award by the 2005 Australasian Conference on Information Security and Privacy.

Forewords

Cloud computing is widely regarded as the next transformational wave of information and communications technology (ICT) for business, governments, and individual consumers. The elastic supply of ICT storage and computing capabilities at low cost is likely to open up numerous game changing opportunities. Apart from reducing operational costs, cloud computing is driving business innovation with radical new business models and step change improvements in the effectiveness of ICT for all users.

The Australian Government has recognized the potential of this new technology through its Cloud Computing Strategic Direction Paper of April 2011. Today, Australian Government agencies can choose to use cloud computing services where they provide value for money and adequate security.

New technology advancements such as cloud computing can create disruptive outcomes and new risks. Cloud computing not only aggregates computing power, but it also amasses information. Users, providers, and government policy makers are quite rightly concerned about privacy and security risks. Will the benefits of cloud computing outweigh the risks for governments, industry, and society?

This book is concerned with the risks associated with the criminal exploitation of cloud computing.

Due to the virtual, dynamic, and borderless nature of cloud computing services, government and law enforcement investigations into malicious cyber activities will require cooperation between government agencies from multiple countries.

Government and law enforcement investigators face difficulty in accessing the physical hardware to locate evidential data. The data may also be spread across multiple data centers in different countries. To reduce the risk of digital (forensic) evidence being called into question in judicial proceedings, it is important to have a rigorous methodology and set of procedures for conducting digital forensic investigations and examinations.

This book presents the first published framework on cloud forensics. The framework is used to examine three popular public and one private cloud storage services. The reported findings will contribute to a better understanding of the types of artifacts that are likely to remain for digital forensics practitioners. It is an essential companion for digital forensic practitioners and researchers who wish to understand cloud (storage) forensics and how to collect digital evidence from cloud storage services.

The book's publication is timely as it provides new insights in managing risk in cloud computing and addresses the growing challenge associated with cyber security.

Dr. Alexander Zelinsky
Chief Defence Scientist
Defence Science and Technology Organisation (DSTO) Canberra, Australiax

In just a few short years, forensic computing has gone from a new field of forensic opportunity to an area with complex technical challenges that are constantly evolving. With constant change comes enormous technical challenge for forensic computing practitioners to keep up with those intent on using electronic devices to aid them in their criminal activities or help them avoid detection.

Previously, access to computing devices was easy and access to information held on the devices was relatively straightforward. With the proliferation of smart mobile devices and the data sharing and storage opportunities, the challenges around accessing and securing data for forensic examination is considerable.

With the advent and now ubiquitous access to "*cloud storage*" combined with the shear volume of data that is recorded, stored, and shared, research such as this is critical in guiding practitioners in how best to secure and examine off-site data. While cloud storage and cloud computing offer real benefits to the legitimate computer or smart device user, it also creates enormous opportunity for those with intent to commit any sort of criminal offending, whether it be child exploitation or financial crime, to stay one step ahead of investigators.

The challenge is to assess whether cloud storage may have been used, identify key indicators that confirm cloud use, determine where the cloud storage service actually is, and attempt to secure the data for forensic examination. Through a number of case studies, the authors have demonstrated that it is possible to lay robust frameworks to enable practitioners to identify, locate, and secure key evidence from cloud based services.

This book draws on the authors' considerable operational and research experiences and will become a key reference manual enabling practitioners in forensic computing to keep up with cloud storage developments in this rapidly evolving area.

Mike Whitaker
Senior Sergeant
Chair, Electronic Evidence Specialist Advisory Group (EESAG)
Senior Managers of Australian and New Zealand
Forensic Laboratories (SMANZFL), Australia

Contents

CHAPTER

Introduction 1

INFORMATION IN THIS CHAPTER[1]

- Introduction to cloud computing
- Cybercrime and cloud computing

INTRODUCTION

It is not clear when the term cloud computing was first coined. For example, Bartholomew (2009), Bogatin (2006), and several others suggested that "cloud computing" terminology was, perhaps, first coined by Google™ Chief Executive Eric Schmidt in 2006. Kaufman (2009) suggests that cloud computing terminology "originates from the telecommunications world of the 1990s, when providers began using virtual private network (VPN) services for data communication." Desisto, Plummer, and Smith (2008) state that "[t]he first SaaS [Software as a Service] offerings were delivered in the late 1990s...[a]lthough these offerings weren't called cloud computing." In this paper, we adopt the definition introduced by the National Institute of Standards and Technology (NIST): "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011).

In recent years, there has been a marked increase in the adoption of cloud computing. Gartner's 2011 Hype Cycle for Cloud Computing report, for example, referred to cloud computing as the "most hyped concept in IT" (Smith, 2011: 3). "Cloud computing" has been a trending search on Google since 2009 with continued interest (Google, 2013). Another Gartner report suggested that cloud computing could be a US$149 billion market by 2014 and by 2016 could have 100% penetration in Forbes list of the Global 2000 companies (McGee, 2011). It can be reasonably assumed that many of those top 2000 companies will provide some

[1]Material in this chapter has been adapted from Hooper, Martini and Choo (2013) and other publications of the authors.

level of online access via cloud computing to both their internal users and their customers.

The availability of cloud storage services is becoming a popular option for consumers to store data that is accessible via a range of devices, such as personal computers, tablets, and mobile phones. There are a range of cloud storage hosting providers, and many offer free cloud storage services, such as Dropbox™, Microsoft® SkyDrive®[2], and Google Drive™. Due to the large number of these services available, many commentators have used the phrase Storage as a Service (StaaS) to describe this type of service (Kovar, 2009; Meky & Ali, 2011; Waters, 2011; Wipperfeld 2009). This is an addition to the traditional cloud computing architectures documented by Mell and Grance (2011) of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Consumers have adopted the cloud storage paradigm in huge numbers with Gartner forecasting massive growth in the area stating that users will be storing a third of their data in the cloud by 2016 (Gartner, 2012). However, many enterprises have remained cautious in moving their data into the public cloud storage environment due to issues such as data sovereignty and security, and complying with regulatory obligations. For example, enterprises who fail to comply with data protection legislation may lead to administrative, civil, and criminal sanctions.

A number of open and closed source cloud software products have been developed and/or are in development to address the needs of the enterprises and even individuals who want to leverage the features of cloud computing while continuing to store data on-site or otherwise under the control of the data custodian. Storing data on-site and/or having the data centers physically in the jurisdiction are increasingly seen as ways to reduce some of the location risks that cloud (storage) service clients currently face. For example, it was suggested at one of the hearings of the Australian Government Parliamentary Joint Committee on Intelligence and Security that "the default position should be that governments, agencies and departments ought to keep their information onshore but use cloud for providers, because there are great cost savings to government by using cloud, using digital storage and accessing the digital economy, being a model user of things like the NBN, data cente[r]s and cloud computing. We think there is a real leadership role for government, but it needs to be done within something of a risk minimi[z]ation strategy, which means that you keep the data onshore and you do not look to send it offshore to a jurisdiction that you do not know about" (Australian Government Parliamentary Joint Committee on Intelligence and Security, 2012: 16). More recently in 2013, the Australian Government has also released the National Cloud Computing Strategy (Australian Government Department of Broadband, 2013) and the policy and risk management guidelines for the storage and processing of Australian Government information in

[2]It has been reported in the media that "Microsoft confirms it will change SkyDrive name after trademark suit" (see Ludwig, 2013; British Sky Broadcasting Group Plc & Ors v Microsoft Corporation Microsoft & Anor [2013] EWHC 1826 (Ch) (28 June 2013)).