Cloud Storage Forensic Analysis

Darren Quick
quidp003@mymail.unisa.edu.au
Supervisor: Dr Kim–Kwang Raymond Choo
Outline

1 – Introduction
2 – Literature Review
3 – Research Method
4 – Digital Forensic Analysis Cycle
5 – Dropbox
6 – Skydrive
7 – Google Drive
8 – Preservation
9 – Summary
Introduction

- Cloud computing
- Cloud storage
- Gartner Report (Kleynhans 2012)
- Personal cloud will replace PC’s as the main storage by 2014
- Dropbox, Microsoft SkyDrive, and Google Drive
- PC; client software or browser
- Portable devices; browser or apps
Introduction

- Criminals and victims data of interest
- Virtualised, geographically disbursed and transient
- Technical and legal issues for investigators;
  - Identification of data; i.e. service provider
  - Username,
  - Data in the account
  - Difficult to prove ownership
  - Data may be moved or erased before it can be preserved
Research Objectives

- **Objective 1**: To examine current research published in literature relating to cloud storage and identified cloud storage analysis methodologies.

- **Objective 2**: To develop a digital forensic analysis framework that will assist practitioners, examiners, and researchers follow a standard process when undertaking forensic analysis of cloud storage services.

- **Objective 3**: To conduct research using popular cloud storage services; Dropbox, Microsoft SkyDrive, and Google Drive, and determine whether there are any data remnants which assist digital forensic analysis and investigations.

- **Objective 4**: To examine the forensic implications of accessing and downloading cloud stored data from popular cloud storage services; Dropbox, Microsoft SkyDrive, and Google Drive.
Literature Review

- NIST (2011) definition of cloud computing
- IaaS – Infrastructure as a Service – user control
- PaaS – Platform as a Service – OS provided
- SaaS – Software as a Service – User has limited control
- Criminal use
- Security of cloud services is well addressed
- Mobile devices
Digital forensic analysis process
Common procedures for investigation
McClain (2011) Dropbox analysis
Chung et al. (2012) Dropbox, Google Docs, Amazon S3 and Evernote
Zhu (2011) examines Skype, Viber, Mail, Dropbox
Reese (2010) examines Amazon EBS
Clark (2011) examines Exif metadata in pictures
Research Method

- Objectives not answered in literature
- Need to conduct primary research

Q₁ What data remnants result from the use of cloud storage to identify its use?

H₀ – There are no data remnants from cloud storage use

H₁ – There are remnants from cloud storage use
Research Question 1

a) What data remains on a Windows 7 computer hard drive after cloud storage client software is installed and used to upload and store data with each hosting provider.

b) What data remains on a Windows 7 computer hard drive after cloud storage services are accessed via a web browser with each hosting provider?

c) What data is observed in network traffic when client software or browser access is undertaken?

d) What data remains in memory when client software or browser access is undertaken?

e) What data remains on an Apple iPhone 3G after cloud storage services are accessed via a web browser with each hosting provider?

f) What data remains on an Apple iPhone 3G after cloud storage services are accessed via an installed application from each hosting provider?
Q₂ What forensically sound methods are available to preserve data stored in a cloud storage account?

- $H_0$ the process of downloading files from cloud storage does not alter the internal data or the associated file metadata.
- $H_1$ the process of downloading files from cloud storage alters the internal file data and the associated file metadata.
- $H_2$ the process of downloading files from cloud storage does not alter the internal data, but does alter the file metadata.
- $H_3$ the process of downloading files from cloud storage alters the internal data, but not the associated file metadata.
Research Question 2a

Q₂a) What data can be acquired and preserved from a cloud storage account using existing forensic tools, methodologies, and procedures when applied to cloud storage investigations?
Research Method

- Research experiment undertaken using Virtual PC’s to create various circumstances of accessing cloud storage services.
- VM’s forensically preserved and analysed for data remnants
Experiment Process

- Prepare Virtual PC’s with Windows 7
- Base (control) clean installation
- Install Browser (Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari)
- Install Client Software and upload test files
- Use browser to access account and view files
- Use browser to access and download files
- Use Eraser to erase files
- Use CCleaner to remove browsing history
- Use DBAN to erase virtual hard drive
Digital Forensic Analysis Cycle

- Commence (Scope)
- Prepare and Respond
- Identify and Collect
- Preserve (Forensic Copy)
- Analyse
- Present
- Feedback
- Complete
Using the Framework to guide the process
Analysis of the VM images
In the Control VM’s; ‘Dropbox’ references
Client Software 1.2.52; encrypted, sample files
System Tray link to ‘launch Dropbox website’
Browser remnants
OS remnants; Prefetch information, Link Files, $MFT, Registry, Thumbcache, Event logs
Network traffic; IP’s, URL client/web
RAM; password in cleartext
Eraser/CCleaner; left remnants
DBAN; all erased
Dropbox

- iPhone 3G iOS 4.2.1 (using the framework)
  - Base (control); nil located
  - Browser; filenames in History.plist + URL
  - Dropbox App; username in keychain.plist

- Case study (used to illustrate findings)
  - ‘Botnet’ hypothetical example describing finding information on PC and iPhone re Dropbox use
Conclusion;
- dbx files are now encrypted, earlier versions;
  - Filecache.db and config.db
- Password in cleartext in memory
- Process of booting a forensic image in a virtual PC will synchronise and provide access to the account without requiring a username or password

Current Police investigation; located illicit data being stored in a Dropbox account (real world application of the research)
Using the Framework to guide the process
Analysis of the VM images
In the Control VM’s; ‘skydrive’ references
Client Software; SyncDiagnostics.log, OwnerID.dat
OS remnants; Prefetch information, Link Files, $MFT, Registry, Thumbcache, Event logs
Network traffic; IP’s, filenames
RAM; password in cleartext
Eraser/CCleaner; left remnants
DBAN; all erased
Microsoft SkyDrive

- iPhone 3G iOS 4.2.1 (using the framework)
  - Base (control); nil located
  - Browser; OwnerID in URL, filenames in History.plist
  - SkyDrive App; username in keychain.plist

- Case study (used to illustrate findings)
  - ‘IP Theft’ hypothetical example describing finding information on PC and iPhone re SkyDrive use
Microsoft SkyDrive

Conclusion;
- SyncDiagnostics.log and OwnerID.dat files
- Password in cleartext in memory
- Process of booting a forensic image in a virtual PC may synchronise the files in an account. Access to the account requires a password.
Using the Framework to guide the process
Analysis of the VM images
In the Control VM’s; ‘drive google’ references
Client Software; Sync_config.db and snapshot.db
Password in cleartext stored on Hard Drive
System Tray link to ‘visit Google Drive on the web’
OS remnants; Prefetch information, Link Files, $MFT, Registry, Thumbcache, Event logs
Network traffic; IP’s, username
Eraser/CCleaner; left remnants
DBAN; all erased
Google Drive

- iPhone 3G iOS 4.2.1 (using the framework)
  - Base (control); nil located
  - Browser; username in cookies, filenames in History.plist
  - Google Drive App; unable to install, need iOS 5

- Case study (used to illustrate findings)
  - ‘Steroid importation’ hypothetical example describing finding information on PC and iPhone re Google Drive use
Google Drive

Conclusion;

- `sync_config.db` and `snapshot.db` files
- **Password in cleartext** in RAM and on Hard Drive
- System Tray link to ‘visit Google Drive on the web’
- Process of booting a forensic image in a virtual PC will give full access to an account without requiring a username or password
Forensic Preservation

- No documented process to collect data once identified
- Some jurisdictions have legal power to secure data accessible at the time of serving a warrant, such as 3LA *Crimes Act 1914*
- Tested in VM with Dropbox, Microsoft SkyDrive, and Google Drive
- Access via Browser and Client Software
- **No change to files** (Hash values same after downloading when compared with original)
### Times and Dates change;

<table>
<thead>
<tr>
<th></th>
<th>Last Accessed</th>
<th>File Created</th>
<th>Last Written</th>
<th>Entry Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropbox</td>
<td>browser</td>
<td>Last Written (UTC)</td>
<td>Last Written (UTC)</td>
<td>unZIP time</td>
</tr>
<tr>
<td></td>
<td>client</td>
<td>download time</td>
<td>download time</td>
<td>same</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>download time</td>
</tr>
<tr>
<td>Google</td>
<td>browser</td>
<td>1/01/1980</td>
<td>1/01/1980</td>
<td>unZIP time</td>
</tr>
<tr>
<td>Drive</td>
<td></td>
<td>last written</td>
<td>download time</td>
<td>same</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>download time</td>
</tr>
<tr>
<td>SkyDrive</td>
<td>browser</td>
<td>upload date/time</td>
<td>upload date/time</td>
<td>unZIP time</td>
</tr>
<tr>
<td></td>
<td>client</td>
<td>download time</td>
<td>download time</td>
<td>same</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>download time</td>
</tr>
</tbody>
</table>
Results

- $Q_1 = H_1$
  There are remnants from cloud storage use which enable the identification of the service, a username, or file details.

- $Q_2 = H_2$
  The process of downloading files from cloud storage does not alter the internal data, but does alter the file metadata.
Contributions

- Identified software files for each service, e.g.
  - SyncDiagnostics.log – SkyDrive
  - Snapshot.db – Google Drive
  - Filecache.db – Dropbox

- Identified OS remnants;
  - Prefetch
  - Link files
  - Registry

- Identified Browser History remnants

- No change to access and download files

- Difference in timestamps for downloaded files

- Process to boot PC in a VM
Other cloud storage services;
- Amazon S3, iCloud, and UbuntuOne

Physical iPhone extract compared to logical extract

Android, Windows Mobile devices

Apple iOS 5 devices

Further test the framework


References

- Kleynhans, S (2012), *The New Pc Era– the Personal Cloud*, Gartner Inc,
- Reese, G (2010), *Cloud Forensics Using Ebs Boot Volumes*, Oreilly.com