Recovering Digital Evidence in a Cloud Computing Paradigm

Jad Saliba
Founder and CTO
Background

• Teenage geek - IT/Software industry

• Police officer for 7 years

• Worked in Tech Crimes Unit

• Started JADsoftware as a part-time home project – now a team of developers
Overview

• The Cloud Computing Trend in Digital Forensics
• What You Can Do
• The Who, What, Where, and How of popular Cloud services
Trends in Digital Forensics
Cloud Computing

• More people trusting the cloud

  – A recent report from Apple stated that about 85 million users have registered and signed up for the iCloud services.
  – Microsoft also reports uprising signups from at least 17 million users a month from their DropBox and SkyDrive services.
Trends in Digital Forensics

Cloud Computing

• Less data left on the hard drive by applications
  – Examples: Yahoo! Messenger v11
              GoogleTalk
Trends in Digital Forensics
Cloud Computing

• Increased web browser usage
  – “Internet browsing will evolve from a browser as component of a higher level OS, to a browser as the primary function of the device.”
  – 2011 Technology Trends report from J.Gold Associates, LLC.
  – As more data goes to the cloud and more applications are cloud-based, the browser becomes the focus
What You Can Do

• Focus more on data within RAM and browser artifacts

• With less data being left on hard drives/unallocated space, RAM and files like the pagefile.sys/hiberfil.sys and resident MFT files become more important

• Increased RAM sizes = more data to be found in RAM
Where To Find The Evidence

• Live RAM captures
  – Best source for volatile artifacts
  – Many artifacts that are not logged anywhere can be found in RAM
  – Examples: World of Warcraft chat (eventually can be found elsewhere – pagefile, etc)
  – Use utilities like FTK Imager, dumpit, IEF Triage
Where To Find The Evidence

- Pagefile.sys
  - Used as “virtual memory” – data is paged in and out of the pagefile as needed
  - Even on systems with a large amount of RAM, Microsoft recommends to keep the pagefile enabled
  - Also a great source for volatile artifacts
  - Many artifacts that are found in RAM only can also make their way into the pagefile
Where To Find The Evidence

- **Hiberfil.sys**
  - Contains complete image of RAM and system state to be used to restore system from hibernation
  - Artifacts from a historic point in time (the last time the system was hibernated)
  - Similar to the user making a RAM capture for you
  - Compressed data in “Xpress” blocks
  - Tools to decompress: hibr2dmp from Matthiu Suiche, Simon Key’s Enscript, Internet Evidence Finder (decompresses on the fly)
Where To Find The Evidence

• Unallocated space
  – A great deal of deleted data can be found here – including browser cache data
  – With SSD drives, less data will be found, depending on when the “garbage collection” last occurred
  – In our testing, data remained in unallocated days after it was deleted (with high use and also some idle time)
WHO

• Dropbox
WHAT

• Dropbox
  – Cloud based file backup/sharing/syncing service
  – 5 years “old”
  – Went from 5 million to 25 million users last year
  – 300 million files saved each day and 1 million files every five minutes
  – Total of 100 billion files saved as of last year
WHERE

- Dropbox – Desktop Application
HOW

• Dropbox – Desktop Application
HOW

• Dropbox – Desktop Application
  – Older version is not encrypted
  – SQLite databases
  – Automatically updates to the latest version as soon as you connect to the network – files get encrypted immediately
HOW

- Dropbox – Desktop Application
HOW

• Dropbox – Desktop Application
  – Older version easy to parse, Python scripts available from ATC-NY or via IEF v5.5.
  – Newer version encrypted – nothing available to decrypt the files...yet. 😊
  – Need to rely on artifacts left behind from desktop application or web access if newer version was used
WHERE

• Dropbox – Web Based Access
  – Temporary Internet Files
  – RAM dumps
  – pagefile.sys/hiberfil.sys
HOW

• Dropbox – Web Based Access
  – Example URL when file viewed:
HOW

• Dropbox – Web Based Access
HOW

• Dropbox – Web Based Access
HOW

• Dropbox – Web Based Access
HOW

• Dropbox – Web Based Access

HOW

• Dropbox – Web Based Access


JADsoftware
Digital Forensics Solutions
HOW

• Dropbox – Web Based Access
HOW

• Dropbox – Web Based Access
WHO

• Flickr
WHAT

• Flickr
  – Image and video hosting website
  – Created by Ludicorp in 2004 and acquired by Yahoo! in 2005
  – Total of 51 million registered members (June 2011)
  – Hosting more than 6 billion images (Aug 2011)
WHERE

• Flickr
  – Temporary Internet Files
  – RAM dumps
  – pagefile.sys/hiberfil.sys
WHERE

• Flickr
• Flickr
• **Flickr**

```
{"id":"7231020308","title":"P1010287 (Small)","license":"0","safety_level":1,"owner":"78930610@N02","ownername":"MrTest1","pathalias":null,"url":"/photos/78930610@N02/7231020308/","media":"photo","date_posted":"1337484434","date_taken":"2011-10-22 14:32:13","fave_count":"0","comment_count":"0","is_fave":false,"secret":"192376b8a3","sizes":{"sq":{"label":"Square","file":"_192376b8a3_s.jpg","url":"http:\/\/farm6.staticflickr.com\/5339\/7231020308_192376b8a3_s.jpg","width":75,"height":75},"q":{"label":"Large Square","file":"_192376b8a3_q.jpg","url":"http:\/\/farm6.staticflickr.com\/5339\/7231020308_192376b8a3_q.jpg","width":150,"height":150},"t":{"label":"Thumbnail","file":"_192376b8a3_t.jpg","url":"http:\/\/farm6.staticflickr.com\/5339\/7231020308_192376b8a3_t.jpg","width":100,"height":75},"s":{"label":"Small","file":"_192376b8a3_m.jpg","url":"http:\/\/farm6.staticflickr.com\/5339\/7231020308_192376b8a3_m.jpg","width":240,"height":180},"n":{"label":"Small 320","file":"_192376b8a3_n.jpg","url":"http:\/\/farm6.staticflickr.com\/5339\/7231020308_192376b8a3_n.jpg","width":320,"height":240},"m":{"label":"Medium","file":"_192376b8a3.jpg","url":"http:\/\/farm6.staticflickr.com\/5339\/7231020308_192376b8a3.jpg","width":500,"height":375},"z":{"label":"Medium 640","file":"_192376b8a3_z.jpg","url":"http:\/\/farm6.staticflickr.com\/5339\/7231020308_192376b8a3_z.jpg","width":640,"height":480}}
```

---

![JADsoftware logo](https://example.com/jadsoftware.png)

**JADsoftware**

Digital Forensics Solutions
WHO

• Google Docs
WHAT

• Google Docs
  – Web-based office suite and data storage service offered by Google
  – Create and edit documents online, upload documents
  – Now blended with Google Drive – launched April 24th, 2012
WHERE

• Google Docs
  – Temporary Internet Files
  – RAM dumps
  – pagefile.sys/hiberfil.sys
WHERE

- Google Docs
HOW

• Google Docs

{minimumRole:20,url:https://\docs.google.com\file\d\0B7qA7G94h0r9Sm1PaV9lbmRoR1k\edit},attributes:{blob_versionable:true,collaboratorsCanInvite:true,convertible:true,downloadable:true,mine:true,shareable:true,subscribed:true},cosmoType:DoclistBlob,fileExtension:pdf,filters:[items,documents,pdf],id:\\0420B7qA7G94h0r9Sm1PaV9lbmRoR1k,importance:0.55,lastCollaborator:{email:gmluser@gmail.com,id:\\04204292055178555970217,me:true,name:Jad Saliba},lastEditedText:\\04210:30 pm,lastEditedUtc:1337221843211,lastModByMeText:\\04210:30 pm,lastModByMeUtc:1337221843184,mav:0,mimeType:application\pdf,myRole:40,name:testdoc (2).pdf,

...
WHO

• Google Drive


Access everywhere.
Google Drive is everywhere you are—on the web, in your home, at the office and on the go. So wherever you are, your stuff is just...there. Ready to go, ready to share. Get started with 5 GB free.

Google Drive is available for:
• PC and Mac
• Chrome OS
• iPhone and iPad (coming soon)
• Android devices
WHAT

• Google Drive
  - File storage and sync service by Google
  - An extension of Google Docs, allowing users to store all types of files
  - Will eventually replace Google Docs
  - Now has an optional client-side application
WHERE

- Google Drive – Desktop Application
HOW

- Google Drive – Desktop Application

**OPEN TABLE 'cloud_entry'**

<table>
<thead>
<tr>
<th>resource_id</th>
<th>filename</th>
<th>modified</th>
<th>created</th>
<th>a</th>
<th>doc_type</th>
<th>removed</th>
<th>url</th>
<th>size</th>
<th>checksum</th>
<th>shared</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 folder:root</td>
<td>root</td>
<td>0</td>
<td>0</td>
<td>a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2 fileB7qA7G94h09VG1kVdURmZhiZjA</td>
<td>ICQ.7z</td>
<td>0</td>
<td>0</td>
<td>a</td>
<td></td>
<td></td>
<td><a href="https://docs.g">https://docs.g</a>...</td>
<td>f0134bed23b1...</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>3 fileB7qA7G94h09VDRaeEZGNUhqdWs</td>
<td>testfb.txt.htm</td>
<td>0</td>
<td>0</td>
<td>a</td>
<td></td>
<td></td>
<td><a href="https://docs.g">https://docs.g</a>...</td>
<td>993d03dc3a45...</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>4 fileB7qA7G94h09QUISSWpaRTcMrk0</td>
<td>AnandTech.com - Understanding SSDs.zip</td>
<td>0</td>
<td>0</td>
<td>a</td>
<td></td>
<td></td>
<td><a href="https://docs.g">https://docs.g</a>...</td>
<td>424549</td>
<td>eee69f173404...</td>
<td>0</td>
</tr>
<tr>
<td>5 pdfB7qA7G94h09RV9mMmJENUpJT8W</td>
<td>AnandTech.com - Understanding SSDs.pdf</td>
<td>0</td>
<td>0</td>
<td>a</td>
<td></td>
<td></td>
<td><a href="https://docs.g">https://docs.g</a>...</td>
<td>693099</td>
<td>c63918c3f7cb...</td>
<td>0</td>
</tr>
</tbody>
</table>

**OPEN TABLE 'local_entry'**

<table>
<thead>
<tr>
<th>inode_number</th>
<th>filename</th>
<th>modified</th>
<th>checksum</th>
<th>size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 1688849860322157</td>
<td>ICQ.7z</td>
<td>1332270900</td>
<td>f0134bed23b1...</td>
<td>6062</td>
</tr>
<tr>
<td>2 4503599627428710</td>
<td>C:\Users\jad\Google Drive</td>
<td>1339163477</td>
<td>eee69f173404...</td>
<td>424549</td>
</tr>
<tr>
<td>3 675539941331275</td>
<td>AnandTech.com - Understanding SSDs.zip</td>
<td>1339163477</td>
<td>eee69f173404...</td>
<td>424549</td>
</tr>
<tr>
<td>4 7881299347930028</td>
<td>testfb.txt.htm</td>
<td>1339012930</td>
<td>993d03dc3a45...</td>
<td>24799</td>
</tr>
<tr>
<td>5 2617717283466524</td>
<td>AnandTech.com - Understanding SSDs.pdf</td>
<td>1339163460</td>
<td>c63918c3f7cb...</td>
<td>693099</td>
</tr>
</tbody>
</table>

**OPEN TABLE 'mapping'**

<table>
<thead>
<tr>
<th>inode_number</th>
<th>resource_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 4503599627428710</td>
<td>folder:root</td>
</tr>
<tr>
<td>2 1688849860322157</td>
<td>fileB7qA7G94h09VG1KvdURmZhiZjA</td>
</tr>
<tr>
<td>3 7881299347930028</td>
<td>fileB7qA7G94h09VDRaeEZGNUhqdWs</td>
</tr>
<tr>
<td>4 675539941331275</td>
<td>fileB7qA7G94h09QUISSWpaRTcMrk0</td>
</tr>
<tr>
<td>5 2617717283466524</td>
<td>pdfB7qA7G94h09RV9mMmJENUpJT8W</td>
</tr>
</tbody>
</table>
**HOW**

- **Google Drive** – Desktop Application

---

<table>
<thead>
<tr>
<th>resource_id</th>
<th>filename</th>
<th>modified</th>
<th>created</th>
<th>doc_type</th>
<th>removed</th>
<th>url</th>
<th>size</th>
<th>checksum</th>
<th>shared</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>root</td>
<td></td>
<td></td>
<td>a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>file0B7qA7G94h09VGrikdURmZlhiZJa</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>file0B7qA7G94h09VDRaeEZGNUhqdlWs</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>file0B7qA7G94h09QUISSWpaRTcXMi0</td>
<td>1339163477</td>
<td>1339163477</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>pdf0B7qA7G94h09RV9mMmJENUpJT8</td>
<td>1339163460</td>
<td>1339163460</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>inode_number</th>
<th>filename</th>
<th>modified</th>
<th>checksum</th>
<th>size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ICQ.7z</td>
<td>1332270900</td>
<td>f0134bed23b1...</td>
<td>6062</td>
</tr>
<tr>
<td>2</td>
<td>C:\Users\jad\Google Drive</td>
<td>1339163477</td>
<td>eee969f173404...</td>
<td>424549</td>
</tr>
<tr>
<td>3</td>
<td>AnandTech.com - Understanding SSDs.zip</td>
<td>1339163477</td>
<td>eee969f173404...</td>
<td>424549</td>
</tr>
<tr>
<td>4</td>
<td>testfb.txt.hml</td>
<td>1339012930</td>
<td>993d03dc3a45...</td>
<td>24799</td>
</tr>
<tr>
<td>5</td>
<td>AnandTech.com - Understanding SSDs.pdf</td>
<td>1339163460</td>
<td>c63918c3f7cb...</td>
<td>693099</td>
</tr>
</tbody>
</table>

---

**mapping**

<table>
<thead>
<tr>
<th>inode_number</th>
<th>resource_id</th>
<th>modified</th>
<th>checksum</th>
<th>size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>folder:root</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>file0B7qA7G94h09VGrikdURmZlhiZJa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>file0B7qA7G94h09VDRaeEZGNUhqdlWs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>file0B7qA7G94h09QUISSWpaRTcXMi0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>pdf0B7qA7G94h09RV9mMmJENUpJT8</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
WHERE

• Google Drive – Web Based Access

  – RAM dumps

  – pagefile.sys/hiberfil.sys
HOW

• Google Drive – Web Based Access
WHO

• SkyDrive
WHAT

• SkyDrive
  – File hosting service that allows users to upload and sync files to a cloud storage
  – Files can be accessed from a web browser or the local device
  – Part of the Windows Live online services and allows users to keep the files private, share them with contacts, or make the files public
  – 7GB of free storage
WHERE

• SkyDrive – Web Based Access
  – Temporary Internet Files
  – RAM dumps
  – pagefile.sys/hiberfil.sys
WHERE

- **SkyDrive** – Web Based Access
  - Data saved in browser cache containing details of files in the user’s SkyDrive
  - If using Internet Explorer, file can be found in the Temporary Internet Files with this filename:

![GetItems[1].htm]
HOW

• SkyDrive – Web Based Access

"creationDate":634727984909230000,"creatorCid":"BBFD2567E3ED65CA","creatorName":"Jad","displayCreationDate":"16/05/2012","displayModifiedDate":"16/05/2012","displaySize":"1,029 KB","eTag":"BBFD2567E3ED65CA!138.0","extension":".pdf","group":0,"iconType":"Pdf","id":"BBFD2567E3ED65CA!138","isPdf":true,"itemType":1,"lastModifierCid":"BBFD2567E3ED65CA","lastModifierName":"Jad","modifiedDate":634727984909230000,"name":"TheMeaningofLife","ownerCid":"BBFD2567E3ED65CA","ownerDcid":"4900719691373386294","ownerName":"Jad","parentId":"root","sharingLevel":"Just me","sharingLevelValue": 4, "size": "1055706","urls": {"download":"https://\dtilpw.bay.livefilestore.com\y1p4hLjLjqVkEVxO2zq8qe9oknt20HC4m1Ywr8FSUGB5eav5XTjP_HrvtAekFQpCPIU4TqPX1ti0u5OeBehWufJCvemPzaScjh_\TheMeaningofLIFE.pdf?download&psid=1","viewInBrowser":"https://skydrive.live.com\redir.aspx?cid=bbfd2567e3ed65ca&page=view&resid=BBFD2567E3ED65CA!138&parid=BBFD2567E3ED65CA!134
HOW • SkyDrive – Web Based Access

"creationDate":634727984909230000,"creatorCid":"BBFD2567E3ED65CA","creatorName":"Jad","displayCreationDate":"16\05\2012","displayModifiedDate":"16\05\2012","displaySize":"1,029 KB","eTag":"BBFD2567E3ED65CA!138.0","extension":".pdf","group":0,"iconType":"Pdf","id":"BBFD2567E3ED65CA!138","isPdf":true,"itemType":1,"lastModifierCid":"BBFD2567E3ED65CA","lastModifierName":"Jad","modifiedDate":634727984909230000,"name":"TheMeaningofLife","ownerCid":"BBFD2567E3ED65CA","ownerDCid":"4900719691373386294","ownerName":"Jad","parentId":"root","sharingLevel":"Just me","sharingLevelValue":4,"size":"1055706","urls": {"download":"https:\/\/dtlilpw.bay.livefilestore.com\/y1p4hLJJqVkJEVx02zq8qe9oknt20HC4m1Ywr8FSUGB5eav5XTjp_HrvtAekFQpCPIU4TqPX1ti0u5OeBehWufJCvemPzaScjh_\/_TheMeaningofLIFE.pdf?download&psid=1","viewInBrowser":"https:\/\/skydrive.live.com\/redir.aspx?cid=bbfd2567e3ed65ca&page=view&resid=BBFD2567E3ED65CA!138&parid=BBFD2567E3ED65CA!134

100-nanosecond intervals that have elapsed since 12:00:00 midnight, January 1, 0001
WHERE

• SkyDrive – Desktop Application
WHERE

- SkyDrive – Desktop Application
WHERE

• SkyDrive – Desktop Application
WHERE

- SkyDrive – Desktop Application
WHERE

• SkyDrive – Desktop Application

User/Drive ID
WHERE

- SkyDrive – Desktop Application
WHERE

- SkyDrive – Desktop Application
WHERE

• SkyDrive – Desktop Application
WHERE

• SkyDrive – Desktop Application
Conclusion

• A great deal of Cloud activity can be found on hard drives and in live RAM

• Can be used to:
  – obtain search warrants/subpoena’s
  – show misuse or exfiltration of company files
  – provide info on files synced from mobile devices

• Internet Evidence Finder v5.5 now supports Cloud Artifacts
Questions?

http://www.jadsoftware.com

Email: jad@jadsoftware.com