Digital Forensics Evidence Acquisition In Cloud Storage Service: Examining and evaluating tools and techniques
Student: Gilchan Park / Advisor: Simuel Liles

Project overview
The purpose of this research is to provide an evaluation of proposed forensic acquisition methodologies and tools in cloud storage services and discuss the limits of those existing tools. As the number of users of cloud storage services such as Dropbox, Google Drive, Microsoft SkyDrive, etc rapidly increases, cloud storage has been identified as an emerging challenge to digital forensic researchers and practitioners. With the analysis of current forensic methodologies of cloud storage, it is expected that cloud storage should be enhanced at the aspect of security.

Techniques and Methods

1) INVESTIGATION INTO ARTIFACTS OF CLOUD STORAGE SERVICES [1]

Concept
- The collection and analysis of the artifacts of all accessible devices which are log files and database files left by cloud storage applications.
- Examination of the artifacts that contain traces of use of a cloud storage service.

Limitations
- Heavily dependent on third party applications. E.g., If cloud service providers refuse providing the decryption key for encrypted artifacts, the forensic examiners cannot gather potential evidence on them.
- Malicious users can simply avoid leaving a trace by manipulating log files.

Artifacts of Cloud Storage Service (Windows)

<table>
<thead>
<tr>
<th>Service</th>
<th>File system path</th>
<th>File name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon S3</td>
<td>~\AppData\Amazon</td>
<td>userdata</td>
<td>E-mail address for login</td>
</tr>
<tr>
<td>Dropbox</td>
<td>~\Dropbox</td>
<td>userdata</td>
<td>E-mail address for login</td>
</tr>
<tr>
<td>Evernote</td>
<td>~\Evernote</td>
<td>userdata</td>
<td>E-mail address for login</td>
</tr>
</tbody>
</table>

2) DIGITAL FORENSIC SOFTWARE AS A SERVICE (DFSaaS) [2]

Concept
- The cloud based forensic tool.
- All forensic examiners can analyze collected evidence at the same time provided network connection.
- Fast performance by massive and distributed data processing in cloud computing.

Limitations
- A user authentication has a potential threat to be hacked.
- Uncertainties arising in chain of custody of evidence by allowing multiple analysts to simultaneously access to log files.

References