A Taxonomy of Cloud Endpoint Forensic Tools

Anand Kumar Mishra, Emmanuel Pilli, Mahesh Govil

▶ **To cite this version:**

Anand Kumar Mishra, Emmanuel Pilli, Mahesh Govil. A Taxonomy of Cloud Endpoint Forensic Tools. 14th IFIP International Conference on Digital Forensics (DigitalForensics), Jan 2018, New Delhi, India. pp.243-261, 10.1007/978-3-319-99277-8_14 . hal-01988833

HAL Id: hal-01988833

https://inria.hal.science/hal-01988833v1

Submitted on 22 Jan 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Chapter 14

A TAXONOMY OF CLOUD ENDPOINT FORENSIC TOOLS

Anand Kumar Mishra, Emmanuel Pilli and Mahesh Govil

Abstract Cloud computing services can be accessed via browsers or client applications on networked devices such as desktop computers, laptops, tablets and smartphones, which are generally referred to as endpoint devices. Data relevant to forensic investigations may be stored on endpoint devices and/or at cloud service providers. When cloud services are accessed from an endpoint device, several files and folders are created on the device; the data can be accessed by a digital forensic investigator using various tools. An investigator may also use an application programming interface made available by a cloud service provider to obtain forensic information from the cloud related to objects, events and file metadata associated with a cloud user. This chapter presents a taxonomy of the forensic tools used to extract data from endpoint devices and from cloud service providers. The tool taxonomy provides investigators with an easily searchable catalog of tools that can meet their technical requirements during cloud forensic investigations.

Keywords: Cloud computing, forensics, tool taxonomy

1. Introduction

In 1999, the U.S. National Institute of Standards and Technology (NIST) [33] initiated the Computer Forensic Tool Testing (CFTT) Program to develop specifications and test methods for digital forensic tools. The tool specifications, test procedures, test criteria, test sets and test hardware require descriptions of tool functionality. NIST subsequently developed a tool catalog based on the specifications targeted for tool developers and users. However, to enhance the use of the catalog by the digital forensics community, a taxonomy of cloud forensic tools is required that describes the tool attributes desired by users. The taxonomy should provide a searchable catalog of forensic tools, enabling

digital forensic investigators to find specific tools that can fulfill their technical requirements during cloud forensic investigations.

This chapter presents a taxonomy of cloud forensic tools. The taxonomy classifies tools into two broad categories. The first category comprises tools that are applied to local endpoint devices to collect artifacts that remain after cloud services have been used by web browsers or client applications. The second category comprises tools that leverage cloud application programming interfaces (APIs) and require user credentials to extract data and metadata from cloud user accounts. Several forensic tools claim to extract cloud-specific data from endpoint devices and cloud service providers. Therefore, this chapter also highlights the data that can be extracted from endpoint devices and via APIs from cloud service providers. Additionally, the chapter describes a case study involving data extraction from an endpoint device that used the OneDrive cloud service.

2. Cloud Forensics

Computer and mobile device forensic tools can be applied to extract and analyze cloud data artifacts residing on endpoint devices. Cloud service providers provide APIs for accessing cloud data; these APIs can also be used to collect data during forensic investigations.

Cloud forensics is the application of digital forensic science in cloud computing environments, and involves hybrid forensic approaches such as virtual, network and live forensics [44]. Cloud forensics is not possible without the involvement of the various cloud actors – service providers, consumers, brokers, carriers and auditors. Zawoad and Hasan [47] state that computer forensic principles and procedures can be applied in cloud computing environments. According to NIST [35], "[c]loud computing forensic science is the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through the identification, collection, preservation, examination, interpretation and reporting of digital evidence." Cloud forensics also faces novel legal issues arising from the multi-jurisdiction and multi-tenancy features of the cloud.

3. Taxonomy of Cloud Endpoint Forensic Tools

Cloud services are accessed via client software, a web browser or an app from a personal computer or mobile device. When cloud services are used, multiple files and folders (e.g., synchronized files and folders, prefetch files and cached files) may be created on the endpoint device. Digital forensic tools can be used to collect and analyze the artifacts from

storage devices and physical memory. When a web browser or mobile device app is used to connect to cloud services and perform upload, download and data access operations, logs and other useful information are generated that can identify the user and provide details about user activities.

Cloud APIs made available by cloud service providers may be used to access evidence in the cloud upon presenting user credentials. The APIs provide valuable cloud user information such as file and folder contents, metadata (file ID, size, name, version, date and time and file type) and details about file and folder operations. Figure 1 presents a taxonomy of cloud endpoint forensic tools.

3.1 Evidence in Endpoint Devices

This section discusses the potential sources of cloud-related digital evidence in cloud endpoint devices.

- **Client Software:** Cloud client software is installed on local devices to interact with cloud service provider resources. An investigator may check and verify the software using hash values. A shortcut may also be created when client software is installed. The shortcut may contain a link to locally-stored data.
- **Synchronized File Folder:** This folder is created on a local device when client software is installed. The folder may automatically synchronize with a cloud server when the endpoint device is connected to the Internet.
- **Recycle Bin:** The recycle bin folder is an important place to check for deleted data in a forensic investigation. Cloud-related data may be recoverable even after synchronized data has been deleted. Two files, `$I` and `$R`, are created when data is deleted from the recycle bin folder. These files are very important from the forensic point of view. `$I` contains file metadata such file size, path, date and time whereas `$R` enables the deleted data to be restored [22].
- **Directory:** A directory maintains information about the files and folders it holds, including file/folder names, sizes and creation dates and times. The directory listing of a cloud client folder provides useful information in a forensic investigation.
- **Dynamic Link Library Files:** Dynamic link library files contain code, data and resources that enable the execution of programs in a Windows environment [30]. These files are important in a

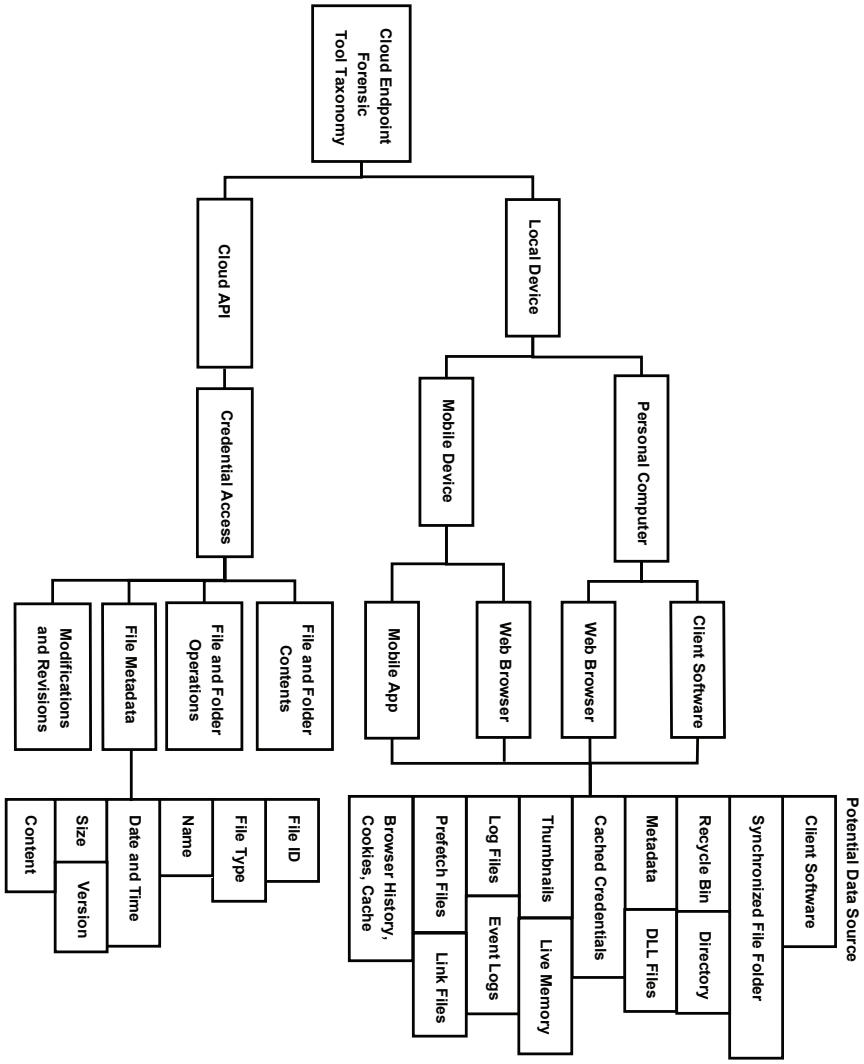

Figure 1. Endpoint forensic tool taxonomy.

forensic investigation. For example, an experimental installation of OneDrive on a Windows 10 system resulted in the creation of more than 122 dynamic link library files.

- **Cached Credentials:** Credentials may be stored in the system credential manager, which records the user name, password, system type and network address. The credentials, which are stored on the hard drive, may be protected by the Data Protection Application Programming Interface (DPAPI) [34].

- **Thumbnails:** Thumbnails are stored in a database when images are uploaded or downloaded from the cloud. The thumbnail database can be very useful in a forensic investigation [34].

- **Live Memory:** Information about running processes can be found in live memory (RAM). Live memory analysis using the Volatility tool during the execution of OneDrive yielded its `*.exe` file, process ID, date and time. The names of dynamic link library files related to the OneDrive application were also found in live memory.

- **Log Files:** Multiple files and folders are created on an endpoint device during client software installation. Moreover, a log file is maintained when user data is synchronized with a cloud service provider. These log files keep records of communicated data such as file size, file creation time and file edit time.

- **Event Logs:** Windows systems maintain various event logs. A forensic investigator may find useful information about application events, security events, system events and hardware events in these logs.

- **Prefetch Files:** A prefetch file is created whenever an application is started [28]. The prefetch files may contain valuable information pertaining to applications.

- **Link Files:** A link file is a shortcut file that is used to open an application in a Windows system. The file stores information about the file path, size, MAC time and address [27]. When a cloud client application is installed, a shortcut file is created to open the folder and synchronize the data.

- **Browser History:** The browser history records the websites visited, visit times and user profile information. Cloud services are often accessed via web browsers such as Internet Explorer, Mozilla

Firefox, Google Chrome, Safari, Opera and Microsoft Edge. When a website is visited, the browser history records key information unless the URL is visited in the unidentified (i.e., incognito or private) mode. Analysis of the URLs in the browser history provides useful information about the cloud services accessed and user IDs, along with icon files.

- **Browser Cookies:** When a website is visited, cookie files created by the web browser are stored on the endpoint device; these files contain personally-identifiable information and user preferences. A forensic investigator can extract user names, addresses, email, user IDs, etc. from browser cookies.
- **Browser Cache:** The browser cache holds temporary Internet files, including downloaded HTML files, style sheets, scripts and images from web servers for faster loading of web pages. The cache information is useful for browser fingerprinting.

3.2 Evidence Recoverable via Cloud APIs

Cloud service providers supply cloud APIs that support data collection from cloud services. A forensic investigator can obtain data directly from a cloud service provider using the appropriate API and credentials (if needed).

Cloud APIs also enable computer programs to interact with cloud data. Several cloud service providers supply APIs that enable third parties to build applications that can be integrated with their cloud services. While these APIs were not created for forensic purposes, they provide very useful information in forensic investigations. For example, the Google Drive API v3 [14] manages Google Drive files using operations such as file uploading, downloading, searching, detecting changes and updating file sharing permissions. The extractable information includes the list of files, file metadata (file name, file ID, file type, date and time, size, version, etc.), thumbnails and revision history. File and folder metadata include file and folder names, special notifications, and editing and deletion information.

The following data extracted using cloud APIs is valuable in forensic investigations:

- **File Content:** Cloud APIs can provide the contents of specified files. Google Drive provides this functionality via the DriveFile and DriveFolder interfaces [15].
- **Metadata:** Metadata is data about a file or folder. Google Drive provides more than ten operations (e.g., copy, create, delete, get,

list and update) that create file metadata. The metadata includes file name, size, ID, hash value, extension, edit times (creation, update and modification) and location. A forensic investigator would be very interested in knowing when files were viewed, modified and shared.

- **Operations Log:** Cloud storage services enable users to perform operations such as uploading, downloading, editing, sharing, deleting and moving files and folders. These operations generate logs with information such as the name of the downloaded file, user name, file ID, hash value, file size and download details.

- **Revision History:** Most of the time, when a user updates a file with a newer version, the file is directly modified in the cloud. The cloud service may maintain a revision history, which enables a user to revert to previous versions of a file. A cloud API may be used to obtain revision information for analyzing files and folders.

4. Cloud Endpoint Forensic Approaches

Tables 1 through 3 summarize the principal cloud endpoint forensic approaches. Each table has five columns. The first column identifies the researchers who presented or developed the approaches. The remaining columns identify the endpoint devices used by the researchers to access cloud services, the specific cloud services accessed during their experiments, and the cloud service access methods (web browser and desktop/mobile app).

Roussev et al. [42, 43] have presented a method for collecting data using cloud APIs from services such as Dropbox, Box, Google Drive, Microsoft OneDrive and Google Docs. They employed a dispatcher written in Python (`kumodd.py`) on top of the cloud APIs to collect and filter data from cloud services that require user credentials for access. The extracted information included the file download date, application version, username, file name, file ID, file size, remote path, download path, revisions and hash values, and timestamps.

5. Cloud Endpoint Device Forensic Tools

This section discusses the digital forensic tools that may be used to extract and analyze data residing in endpoint devices that have accessed cloud services via web browsers or client applications. The following information about forensic tools for cloud endpoint devices is based on vendor documentation:

Table 1. Cloud endpoint forensic approaches.

Researchers	**Endpoint Devices**	**Cloud Services Accessed**	**Cloud Service Access Method**	
			Web Browser	**Desktop/Mobile App**
Dykstra and Sherman [7]	Windows 2008 R2 Server	Amazon EC2	N/A	N/A
Chung et al. [4]	Windows PC, Mac, iPhone, Android	Amazon S3, Google Docs, Dropbox, Evernote	Internet Explorer, Mozilla Firefox	Dropbox Client, Evernote Client
Marturana et al. [26]	Windows PC	Google Docs, Flickr, PicasaWeb, Dropbox	Internet Explorer, Mozilla Firefox, Google Chrome	Dropbox Client
Koppen et al. [21]	Windows PC, iPad, Mobile Device	Google Docs, Dropbox, Windows Live Mesh	Internet Explorer	Dropbox Client, Windows Live Mesh
Hale [20]	Windows PC	Amazon Cloud Drive	Internet Explorer, Mozilla Firefox, Google Chrome	Amazon Cloud Drive Client
Epifani [11]	Windows 7 PC	Dropbox, Google Drive, SkyDrive, iCloud	Mozilla Firefox, Internet Explorer	Dropbox Client, Google Drive Client, SkyDrive Client
Martini and Choo [25]	Windows PC, Mobile Device	ownCloud	Internet Explorer, Mozilla Firefox, Google Chrome	ownCloud Sync Client, iOS ownCloud App

Table 2. Cloud endpoint forensic approaches (continued).

Researchers	Endpoint Devices	Cloud Services Accessed	Cloud Service Access Method	
			Web Browser	Desktop/Mobile App
Grispos et al. [16]	iOS Mobile Device, Android Mobile Device	Dropbox, Box, SugarSync	N/A	Cloud Service Mobile App
Quick and Choo [38]	Windows 7 PC, iPhone	SkyDrive	Mozilla Firefox, Internet Explorer, Google Chrome, Apple Safari	SkyDrive Client
Quick and Choo [39]	Windows 7 PC, iPhone	Dropbox	Mozilla Firefox, Internet Explorer, Google Chrome, Apple Safari	Dropbox Client
Quick et al. [40]	Windows 7 PC, iPhone	Google Drive	Mozilla Firefox, Internet Explorer, Google Chrome, Apple Safari	Google Drive Client
Federici [12]	Windows 7 PC	Dropbox, Google Drive, Microsoft Skydrive	Internet Explorer, Mozilla Firefox	Dropbox Client, Google Drive Client, SkyDrive Client
Oestreicher [36]	Mac OS System	iCloud	N/A	iCloud App
Grispos et al. [17]	iOS Mobile Device, Android Mobile Device	Dropbox, Box, SugarSync, Syncplicity	N/A	N/A

Table 3. Cloud endpoint forensic approaches (continued).

Researchers	Endpoint Devices	Cloud Services Accessed	Cloud Service Access Method	
			Web Browser	Desktop/Mobile App
Blakeley et al. [2]	Windows 8.1 PC	hubiC	Internet Explorer, Google Chrome, Mozilla Firefox	hubiC Client
Mehreen and Aslam [29]	Windows 8 PC	Dropbox	N/A	Dropbox Metro UI
Daryabar et al. [5]	iOS Mobile Device, Android Mobile Device	Mega	N/A	Mega v1 App
Daryabar et al. [6]	iOS Mobile Device, Android Mobile Device	OneDrive, Box, Google Drive, Dropbox	N/A	N/A
Rahman et al. [41]	Android Mobile Device	Google Drive, Dropbox, OneDrive	N/A	N/A
Thamburasa et al. [46]	Windows 7 PC	IDrive, Mega	Internet Explorer, Google Chrome, Mozilla Firefox	IDrive Client, Mega Cloud Drive
Easwaramoorthy et al. [8]	Windows 7 PC	OneDrive, Amazon Cloud Drive	Internet Explorer, Google Chrome, Mozilla Firefox	Client Software

- **Internet Evidence Finder:** Internet Evidence Finder [28] extracts and analyzes cloud artifacts from computers, smartphones and tablets. The digital artifacts include synced files/folders, file names, file sizes, dates/times, user IDs, URLs, file sharing settings and privacy settings.
- **Dropbox Decryptor:** Dropbox Decryptor [24] decrypts SQLite database files such as `filecache.dbx` and `config.dbx` that are created when a user accesses Dropbox.
- **UFED Cloud Analyzer:** The UFED Cloud Analyzer [3] is a mobile device data extractor that requires user credentials to retrieve information. It can extract data from more than 25 cloud data sources, including Facebook, WhatsApp, Google Services, iCloud Services, OneDrive and Dropbox.
- **EnCase eDiscovery:** EnCase eDiscovery [18, 19] may be used to collect electronically-stored information and preserve data from an onsite device or computer as well as from cloud-based data services.
- **Oxygen Forensic Detective:** The Oxygen Forensic Detective tool [37] extracts data from more than 35 cloud sources, including iCloud applications, Google services, cloud-based storage services and email services.
- **XRY Cloud:** XRY Cloud [32] is a forensic tool for mobile devices. With the appropriate user credentials, XRY Cloud provides data access to cloud services such as iCloud, Twitter, Google and Facebook.
- **Elcomsoft Cloud eXplorer:** Elcomsoft Cloud eXplorer [9] is a mobile device forensic tool that extracts data from Google services; it needs user credentials for data retrieval.
- **Elcomsoft Phone Breaker:** Elcomsoft Phone Breaker [10] is a mobile device forensic tool that extracts data from the Apple iCloud; it needs user credentials for data retrieval.
- **Belkasoft Acquisition Tool:** The Belkasoft Acquisition tool [1] acquires images of digital data from hard drives, removable drives, mobile devices and computer RAM, as well as cloud data from iCloud, Google Drive and Google Plus.
- **F-Response Now Cloud Services:** F-Response Now Cloud Services [13] provides read-only access to remote systems, including cloud services.

- **MailXaminer:** MailXaminer [45] is an email forensic tool for investigations involving iCloud, Office365, Rackspace, Gmail, Hotmail and Live Exchange Server.

6. OneDrive Forensics Case Study

This section describes a case study involving OneDrive forensics. In the case study, a OneDrive client application was installed on a computer running Windows 10. Files and folders were updated via the client application as well as using a web browser. The OneDrive application created multiple files and folders during the updates.

Data was extracted using WinPrefetchView v1.35, RAMMap v1.5, Volatility, RAM Capture and DumpIt. Due to space constraints, it is not possible to describe all the results. However, information is presented to enable readers to appreciate the amount of forensically-relevant data that can be found using a OneDrive Client API.

The following data was extracted and analyzed:

- **OneDrive Process Path:** The path (`C:\Users\UserName\AppData\Local\Microsoft\OneDrive\OneDrive.exe`) may be used to check if the client software was installed.
- **Application File:** The application file is located at `C:\Users\UserName\AppData\Local\Microsoft\OneDrive\17.3.6517.0809\OneDriveSetup`.
- **Synchronized File Folder:** OneDrive creates a local folder (`C:\Users\UserName\OneDrive`) in the client system to synchronize user data.
- **Hash Values:** MD5 hash values were checked before uploading the file `reference.txt` to OneDrive and after downloading the file from cloud storage. The MD5 hash value `C8E6450CBA8290B08C53A6EE5138DC89` was not changed during this process.

  Next, file `reference.txt` was edited and saved and the file was downloaded once again. The MD5 hash value of the file was observed to have changed to `867C329748FAF41223351331945F84ED`. As expected, the hash value of the edited file was different from the hash value of the previous version of the file.
- **Account Information:** The following account information was obtained:
  – *User Email ID:* `userid@hotmail.com`.
  – *Cloud Storage Used:* 10 MB of 5 GB.
  – *Microsoft OneDrive:* Version 2016 (Build 17.3.6517.0809).

- **Cached Credentials:** The cached credentials were stored on the hard drive and protected by the Data Protection Application Programming Interface.

- **OneDrive Log Data:** The following files were found at `C:\Users\UserName\AppData\Local\Microsoft\OneDrive\logs\Personal`:
  – `SyncEngine.odl:` This file was created after syncing a file to OneDrive; the file name and file hash were synced in the logs.
  – `TraceArchive.ETL` and `TraceCurrent.ETL:` These files hold the folder attributes.
  – `SyncDiagnostics.log:` This file keeps track of the current operations (e.g., files remaining to be synced).

- *Prefetch Files:* The file `ONEDRIVE.EXE-CA61B35B.pf` was found; it contained the following information:
  – *ClientPolicy:* This was located at `C:\Users\UserName\AppData\Local\Microsoft\OneDrive\settings\Personal\CLIENTPOLICY.INI`; the useful information included the share URL, file URL, etc.
  – *$MFT (Master File Table):* This table was located at `C:\Users\UserName\AppData\Local\Microsoft\OneDrive\logs\Personal\SyncEngine-2016-9-13.558.6736.7.aodl`.
  – *CollectOneDriveLogs (Windows Batch Files):* These files were found at `C:\Users\UserName\AppData\Local\Microsoft\OneDrive\17.3.6517.0809\CollectOneDriveLogs`.
  – *ApplicationSettings XML File:* This file was located at `C:\Users\UserName\AppData\Local\Microsoft\OneDrive\settings\Personal\ApplicationSettings`; the UserCIDwas found to be `6205 14542fa58fa4`.
  – `FileSync.LocalizedResources.dll:` This dynamic link library was found at `C:\Users\UserName\AppData\Local\Microsoft\OneDrive\17.3.6517.0809\FileSync.LocalizedResources.dll`.

- *Browser Password (Saved by User):* The following navigation was performed: Google Chrome → Settings → Show Advanced Settings → Passwords and Forms → Manage Passwords → Click on Saved Passwords → Show → (will ask for password) → (OneDrive password is displayed in a readable format).

- *Registry Files:* These files contained information about tuning parameters, device configuration and user preferences. Example registry files were:
  – `HKEY_CURRENT_USER\Software\Microsoft\OneDrive`.

– HKEY_CLASSES_ROOT\OneDrive.SyncFileInformationProvider.

- **Memory Inspection:** Memory was captured and stored in the ANAND-20160917-062356.raw file. A total of 122 dynamic link library files were found in raw memory. Example files were:
  – C:\Users\UserName\AppData\Local\Microsoft\OneDrive\17.3.6517.0809\LoggingPlatform.dll.
  – C:\Users\UserName\AppData\Local\Microsoft\OneDrive\17.3.6517.0809\qt5gui.dll.
  – C:\Users\UserName\AppData\Local\Microsoft\OneDrive\17.3.6517.0809\filesync.resources.dll.

- **Browser Information:** The following browser information was obtained:
  – *Local Storage:* The user ID was found at C:\Users\UserName\AppData\Local\Google\Chrome\UserData\Default\LocalStorage.
  – *Application Cache:* The cache was located at C:\Users\UserName\AppData\Local\Google\Chrome\UserData\Default\ApplicationCache.
  – *History:* The history information, which included login data, file uploaded, file downloaded, client ID, URL, date and time, was located at C:\Users\UserName\AppData\Local\Google\Chrome\UserData\Default\History.
  – *Cookies:* Cookies were located at C:\Users\UserName\AppData\Local\Google\Chrome\UserData\Default\Cookies.

- **Metadata Extraction via Cloud API:** The Microsoft Graph RESTful web API was used to access Microsoft cloud services [31]. The permissions were modified to access the OneDrive cloud service and the GET method was used to read data. The query graph.microsoft.com/v1.0/me/drive/root/children was used on "all the items on the drive."

  The query yielded metadata for all the files that had been uploaded to OneDrive. Table 4 shows the metadata obtained for one of the files, IMG_5202.jpg.

7. Conclusions

The taxonomy of cloud endpoint forensic tools presented in this chapter covers potential digital evidence sources in endpoint devices as well

Table 4. Metadata extracted using the cloud API.

Source	Contents
Drive Information	Last Modified Date and Time; Drive ID; App Display Name and ID; User Display Name and ID; File and Folder Path
File and Folder Information	Name; Size (Bytes); Hash Value; MIME Type; Creation Time; Image; cTag (Item Content); eTag (Metadata and Content)
Photograph Information	Camera Make; Camera Model; Focal Length; fNumber; ISO; Capture Date and Time; Exposure Numerator; Exposure Denominator
URL Information	Web URL; Download URL

as evidence residing in cloud service provider resources that can be accessed using cloud APIs. Thus, it provides a valuable framework for understanding cloud forensic tools and comparing their functionality. The taxonomy, which supports tool selection as well as requests for increased tool functionality, will be submitted for incorporation in the NIST Computer Forensics Tool Testing Project Tool Catalog. It is hoped that the taxonomy will help advance tool specification and development efforts by vendors, and also enable digital forensic professionals to describe their needs and find tools that meet their needs.

Acknowledgement

The authors wish to thank Barbara Guttman, Software Quality Group Leader at the NIST Information Technology Laboratory for her valuable advice on various aspects of this research.

References

[1] Belkasoft, Belkasoft Acquisition Tool, Menlo Park, California (`belkasoft.com/bat`), 2018.

[2] B. Blakeley, C. Cooney, A. Dehghantanha and R. Aspin, Cloud storage forensics: hubiC as a case-study, *Proceedings of the Seventh IEEE International Conference on Cloud Computing Technology and Science*, pp. 536–541, 2015.

[3] Cellebrite, UFED Cloud Extractor, Petah Tikva, Israel (`www.cellebrite.com/Mobile-Forensics/Products/ufed-cloud-analyzer`), 2018.

[4] H. Chung, J. Park, S. Lee and C. Kang, Digital forensic investigation of cloud storage services, *Digital Investigation*, vol. 9(2), pp. 81–95, 2012.

[5] F. Daryabar, A. Dehghantanha and K. Choo, Cloud storage forensics: Mega as a case study, *Australian Journal of Forensic Sciences*, vol. 49(3), pp. 344–357, 2017.

[6] F. Daryabar, A. Dehghantanha, B. Eterovic-Soric and K. Choo, Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices, *Australian Journal of Forensic Sciences*, vol. 48(6), pp. 615–642, 2016.

[7] J. Dykstra and A. Sherman, Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust and techniques, *Digital Investigation*, vol. 9(S), pp. S90–S98, 2012.

[8] S. Easwaramoorthy, S. Thamburasa, G. Samy, S. Bhushan and K. Aravind, Digital forensic evidence collection of cloud storage data for investigation, *Proceedings of the International Conference on Recent Trends in Information Technology*, 2016.

[9] Elcomsoft Proactive Software, Elcomsoft Cloud eXplorer, Moscow, Russia (`www.elcomsoft.com/ecx.html`), 2018.

[10] Elcomsoft Proactive Software, Elcomsoft Phone Breaker, Moscow, Russia (`www.elcomsoft.com/eppb.html`), 2018.

[11] M. Epifani, Cloud storage forensics, presented at the *SANS European Digital Forensics Summit*, 2013.

[12] C. Federici, Cloud Data Imager: A unified answer to remote acquisition of cloud storage areas, *Digital Investigation*, vol. 11(1), pp. 30–42, 2014.

[13] F-Response, F-Response Universal, Tampa, Florida (`www.f-response.com`), 2018.

[14] Google, Google Drive API v3, Mountain View, California (`developers.google.com/apis-explorer`), 2018.

[15] Google, Google Drive APIs, Mountain View, California (`developers.google.com/drive`), 2018.

[16] G. Grispos, W. Glisson and T. Storer, Using smartphones as a proxy for forensic evidence contained in cloud storage services, *Proceedings of the Forty-Sixth Hawaii International Conference on System Sciences*, pp. 4910–4919, 2013.

[17] G. Grispos, W. Glisson and T. Storer, Recovering residual forensic data from smartphone interactions with cloud storage providers, in *The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues*, R. Ko and K. Choo (Eds.), Syngress, Boston, Massachusetts, pp. 347–382, 2015.

[18] Guidance Software, EnCase eDiscovery, Pasadena, California (`www.guidancesoftware.com/encase-ediscovery?cmpid=nav_r`), 2018.

[19] Guidance Software, EnCase Forensic 8, Pasadena, California (`www.guidancesoftware.com/encase-forensic?cmpid=nav_r`), 2018.

[20] J. Hale, Amazon Cloud Drive forensic analysis, *Digital Investigation*, vol. 10(3), pp. 259–265, 2013.

[21] J. Koppen, G. Gent, K. Bryan, L. DiPippo, J. Kramer, M. Moreland and V. Fay-Wolfe, Identifying remnants of evidence in the cloud, in *Digital Forensics and Cyber Crime*, M. Rogers and K. Seigfried-Spellar (Eds.), Springer, Heidelberg, Germany, pp. 42–57, 2012.

[22] T. Leschke, Cyber dumpster-diving: $Recycle.Bin forensics for Windows 7 and Windows Vista, presented at the *Department of Defense Cyber Crime Conference*, 2010.

[23] Magnet Forensics, Artifacts, Herndon, Virginia (`www.magnetforensics.com/artifacts`), 2018.

[24] Magnet Forensics, Dropbox Decryptor Version 1.3, Herndon, Virginia (`www.magnetforensics.com/free-tool-dropbox-decryptor`), 2018.

[25] B. Martini and K. Choo, Cloud storage forensics: ownCloud as a case study, *Digital Investigation*, vol. 10(4), pp. 287–299, 2013.

[26] F. Marturana, G. Me and S. Tacconi, A case study on digital forensics in the cloud, *Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 111–116, 2012.

[27] J. McQuaid, Forensic Analysis of LNK Files, Magnet Forensics, Herndon, Virginia (`www.magnetforensics.com/computer-forensics/forensic-analysis-of-lnk-files`), August 6, 2014.

[28] J. McQuaid, Forensic Analysis of Prefetch files in Windows, Magnet Forensics, Herndon, Virginia (www.magnetforensics.com/computer-forensics/forensic-analysis-of-prefetch-files-in-windows) August 6, 2014.

[29] S. Mehreen and B. Aslam, Windows 8 cloud storage analysis: Dropbox forensics, *Proceedings of the Twelfth International Bhurban Conference on Applied Sciences and Technology*, pp. 312–317, 2015.

[30] Microsoft, Dynamic-Link Libraries, Redmond, Washington (msdn.microsoft.com/en-us/library/windows/desktop/ms682589(v=vs.85).aspx), 2018.

[31] Microsoft, Use the Microsoft Graph API, Redmond, Washington (developer.microsoft.com/en-us/graph/docs/concepts/use_the_api), 2018.

[32] MSAB, XRY – Extract, Stockholm, Sweden (www.msab.com/products/xry/#cloud), 2018.

[33] National Institute of Standards and Technology, Computer Forensics Tool Testing (CFTT) Program, Gaithersburg, Maryland (www.cftt.nist.gov), 2018.

[34] Network Associates, Windows Data Protection, Microsoft, Redmond, Washington (msdn.microsoft.com/en-us/library/ms995355.aspx), 2001.

[35] NIST Cloud Computing Forensic Science Working Group, NIST Cloud Computing Forensic Science Challenges, Draft NISTIR 8006, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, Maryland, 2014.

[36] K. Oestreicher, A forensically-robust method for acquisition of iCloud data, *Digital Investigation*, vol. 11(S2), pp. S106–S113, 2014.

[37] Oxygen Forensics, Oxygen Forensic Detective, Alexandria, Virginia (www.oxygen-forensic.com/en/products/oxygen-forensic-detective), 2018.

[38] D. Quick and K. Choo, Digital droplets: Microsoft SkyDrive forensic data remnants, *Future Generation Computer Systems*, vol. 29(6), pp. 1378–1394, 2013.

[39] D. Quick and K. Choo, Dropbox analysis: Data remnants on user machines, *Digital Investigation*, vol. 10(1), pp. 3–18, 2013.

[40] D. Quick, B. Martini and K. Choo, *Cloud Storage Forensics*, Syngress, Boston, Massachusetts, 2014.

[41] N. Rahman, N. Cahyani and K. Choo, Cloud incident handling and forensics-by-design: Cloud storage as a case study, *Concurrency and Computation: Practice and Experience*, vol. 29(14), 2016.

[42] V. Roussev, I. Ahmed, A. Barreto, S. McCulley and V. Shanmughan, Cloud forensics – Tool development studies and future outlook, *Digital Investigation*, vol. 18, pp. 79–95, 2016.

[43] V. Roussev, A. Barreto and I. Ahmed, API-based forensic acquisition of cloud drives, in *Advances in Digital Forensics XII*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 213–235, 2016.

[44] K. Ruan, J. Carthy, T. Kechadi and I. Baggili, Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results, *Digital Investigation*, vol. 10(1), pp. 34–43, 2013.

[45] SysTools Software, MailXaminer, Pune, India (`www.mailxaminer.com/product`), 2018.

[46] S. Thamburasa, S. Easwaramoorthy, K. Aravind, S. Bhushan and U. Moorthy, Digital forensic analysis of cloud storage data in IDrive and Mega cloud drive, *Proceedings of the International Conference on Inventive Computation Technologies*, 2016.

[47] S. Zawoad and R. Hasan, Cloud Forensics: A Meta-Study of Challenges, Approaches and Open Problems, Technical Report, Department of Computer Science, University of Alabama at Birmingham, Birmingham, Alabama, 2013.