Xournals

Academic Journal of Forensic Science

ISSN: 2581-4273 | Volume 06 | Issue 01 | April-2023

Cyber-Forensic Processes for Cloud Based Applications

Shrinjoy Goswami[1], Ankit Tripathi[2]

Available online at: www.xournals.com

Received 07th February 2023 | Revised 10th March 2023 | Accepted 25th March 2023

Abstract:

The field of digital forensics known as computer forensics deals with crimes performed on networks, computers, and digital storage media from companies like Apple (iCloud), Amazon (Amazon Web Service), Dropbox, Google, etc. It refers to a collection of methodical steps and techniques used to locate, collect, preserve, extract, interpret, document, and present evidence from computing equipment in a way that makes it admissible during a court case or other legal or administrative activity. Cybercrimes are occurring as a result of the increased use of technology in daily life. In the business world, fraud involving cloud computing is on the rise (gaining access to someone's storage systems, stealing log files, data sheets, account theft, data breach, data loss, etc.). When it comes to cloud-based mobile applications, the activities that are conducted are not only kept on the device, but also in a distant cloud. So, using forensically sound methodology is crucial to obtaining all of the evidence from the Cloud and the smart phone. The vast majority of people are unaware of how to protect their digital storage. This paper discusses importance of cloud forensics, collection and examination of the cloud data through UFED Cloud Analyzer.

Keywords: *Computer forensics, Dropbox, Digital storage media, Cybercrime, Data breach.*

Authors:

1. *B.Sc, Forensic Science, Garden City University, INDIA*
2. *Senior Scientific Officer, Sherlock Institute of Forensic Science, INDIA*

Introduction

The use of Google Drives or cloud storage (for the storing of huge files, data, log files, etc.) has also grown over time. Social networking has evolved primarily over the years into a new type of online communication. In order to provide quicker innovation, adaptable resources, and scale economies, cloud computing, in its simplest form, is the supply of computing services via the Internet ("the cloud"), encompassing servers, storage, databases, networking, software, analytics, and intelligence **(www.azure.microsoft.com).**

Apple (iCloud), Amazon (Amazon Web Service), Dropbox, and Google are some of the most well-known providers of cloud storage. Data breaches caused by inadequate security procedures are a major cloud security issue. Companies must ensure that the online storage service they choose ensures total protection against data leaks and unauthorized access **(www.scaler.com).**

Investigations that are concentrated on crimes that primarily involve the cloud are referred to as cloud forensics. This can involve identity theft or data breaches **(www.appdirect.com).**To protect personal data, smart phones save forensic evidence on cloud storage services. The virtual memory-stored information for the application used to access a cloud computing system will be lost if a user leaves the cloud environment. In the cloud context, it makes the evidence extraction process more difficult.

To obtain the evidence, the forensic investigator looks at a number of potential cloud sites, including the hardware, network, hypervisor, virtual machines, and hosts OS. Three pieces of information, including log purpose in terms of justification, log technique in terms of use, and log time in terms of session ID and timestamp information, are the focus of gathering log information from the cloud **(Sharma *et al.*, 2020).**

A developed cloud forensic process paradigm called Forensic Process as a Service (FPaaS) is built on the cloud-based Business Process Execution Language (BPEL). To help the dynamics and reconstruction of the evidence, the systematic digital forensic investigation model focuses on the investigation of computer fraud and cybercrime **(Eleyan and Eleyan, 2015).**

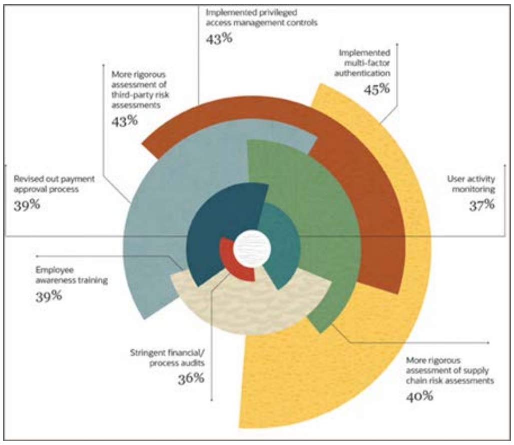


Figure No. 1: Prevention steps against cloud computing threats (www.oracle.com)

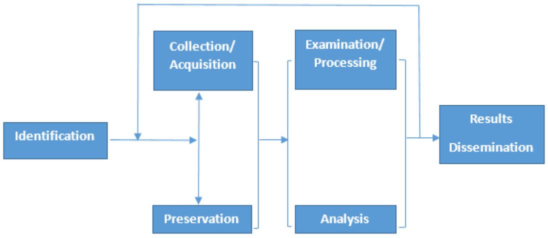


Figure No. 2: Cloud Forensic Process

UFED Cloud Analyzer for Cloud Data Extraction

An advanced tool for cloud data extraction is the UFED Cloud Analyzer. Instantaneous extraction, preservation, and analysis of stored files, other content, and private social media profiles are all made possible by the device. The UFED Cloud Analyzer's greatest advantage is that it not only gathers data from the cloud but also organizes and categorizes it in the most understandable manner for forensic investigations **(www.detective-store.com).** The features of UFED Cloud Analyzer:

- Mobile-based extraction
- Username-based extraction
- Forensic Data Preservation
- Visualize data in a unified format
- Extensive cloud-based data sources

The steps, which need to be taken during UFED Cloud Analyzer investigations:

- Extract
- Access
- Analyze
- Share

Objective

- To extract the data from iCloud Storage.
- To analyze the cloud storage using UFED Cloud Analyzer.
- To examine the accessibility of extracted cloud storage data.

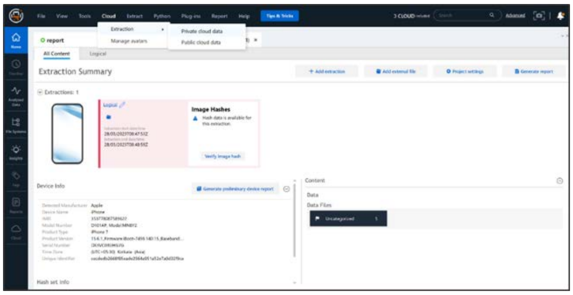
Methodology

In this study, iPhone7 was taken as an exhibit. The objective is to extract and recover data from the iCloud storage through UFED Cloud Analyzer and to examine and analyze the data which was recovered. The below process depicts what all steps are done.

<u>Details of Exhibit:</u>

Device name : iPhone
Model name : iPhone7

- The phone was connected through UFED to the system and then a full-content backup is extracted in UFDR format. After the extraction process is completed, the UFDR report is transferred to Cloud Analyzer. To extract iCloud data "Private cloud data" has to be selected because, iCloud comes under a private digital storage platform. Some examples of private digital storage platforms are AWS, Cisco, IBM, etc.

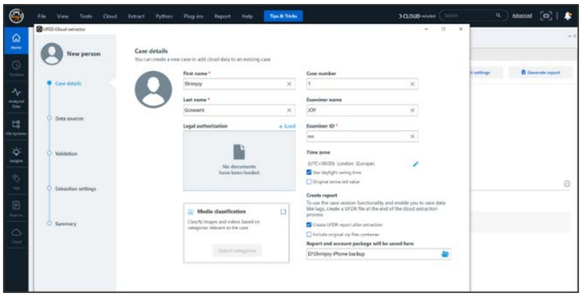


28/03/2023T08:47:53Z
28/03/2023T08:48:59Z

Detected Manufacturer: Apple
Device Name: iPhone
IMEI: 355778087589622
Model Number: D101AP, Model:MN8J2
Product Type: iPhone 7
Product Version: 15.6.1_Firmware:iBoot-7459.140.15_Baseband...
Serial Number: DKWC89SHG7G
Time Zone: (UTC+05:30) Kolkata (Asia)
Unique Identifier: cacdedb2668f85eade2564a051a52a7a0d32f9ca

Figure No. 3: Showing selection of Private Cloud Data

- The necessary details are needed to be filled, path has to be given in which folder the report will get stored and mainly the date time stand has to be selected; like from which particular date the data or applications accessed by the suspect.



Case details
You can create a new case or add cloud data to an existing case

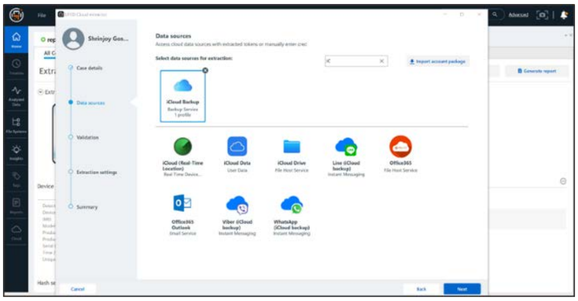
First name *: Shrinjoy
Last name *: Goswami
Legal authorization
Case number: 1
Examiner name: JOY
Examiner ID *: 00
Time zone: (UTC+00:00) London (Europe)
☑ Use daylight saving time
☐ Original extracted value

Media classification ☐
Classify images and videos based on categories relevant to the case.

Create report
To use the save session functionality and enable you to save data like tags, create a UFDR file at the end of the cloud extraction process.
☑ Create UFDR report after extraction
☐ Include original zip files container
Report and account package will be saved here: D:\Shrinjoy iPhone backup

Figure No. 4: Filling the Case Details

- After selection of all the important details the application has to validate the process after which the extraction will start.

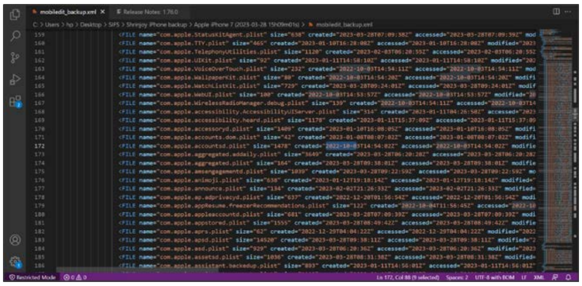


Data sources
Access cloud data sources with extracted tokens or manually enter cred

Select data sources for extraction:

Figure No. 5: The above process shows the Cloud Data Extraction process

- After the data is recovered and extracted, the next step is to analyze and examine the data obtained, sometimes, the cloud backup file might not be in a readable form, so in that case, the backup file has to be converted into readable form via FTK Imager.



C: > Users > hp > Desktop > SIFS > Shrinjoy iPhone backup > Apple iPhone 7 (2023-03-28 15h09m01s) > mobiledit_backup.xml

```
<FILE name="com.apple.StatusKitAgent.plist" size="638" created="2023-03-28T07:09:38Z" accessed="2023-03-28T07:09:39Z" mod
<FILE name="com.apple.TTY.plist" size="465" created="2023-01-10T16:28:08Z" accessed="2023-01-10T16:28:08Z" modified="2023
<FILE name="com.apple.TelephonyUtilities.plist" size="1120" created="2023-02-03T06:20:55Z" accessed="2023-02-03T06:20:55Z
<FILE name="com.apple.UIKit.plist" size="92" created="2023-01-11T14:58:10Z" accessed="2023-01-11T14:58:10Z" modified="202
<FILE name="com.apple.VoiceOverTouch.plist" size="232" created="2022-10-03T14:54:11Z" accessed="2022-10-03T14:54:11Z" mod
<FILE name="com.apple.WallpaperKit.plist" size="80" created="2022-10-03T14:54:20Z" accessed="2022-10-03T14:54:20Z" modifi
<FILE name="com.apple.WatchListKit.plist" size="729" created="2023-03-28T09:24:01Z" accessed="2023-03-28T09:24:01Z" modif
<FILE name="com.apple.WebUI.plist" size="100" created="2022-10-03T14:53:57Z" accessed="2022-10-03T14:53:57Z" modified="20
<FILE name="com.apple.WirelessRadioManager.debug.plist" size="139" created="2022-10-03T14:54:11Z" accessed="2022-10-03T14
<FILE name="com.apple.accessibility.AccessibilityUIServer.plist" size="314" created="2023-01-11T04:26:58Z" accessed="2023
<FILE name="com.apple.accessibility.heard.plist" size="1178" created="2023-01-11T15:37:09Z" accessed="2023-01-11T15:37:09
<FILE name="com.apple.accessoryd.plist" size="1409" created="2023-01-10T16:08:05Z" accessed="2023-01-10T16:08:05Z" modifi
<FILE name="com.apple.accounts.dom.plist" size="42" created="2023-01-08T08:07:02Z" accessed="2023-01-08T08:07:02Z" modifi
<FILE name="com.apple.accountsd.plist" size="1478" created="2022-10-03T14:54:02Z" accessed="2022-10-03T14:54:02Z" modifie
<FILE name="com.apple.aggregated.addaily.plist" size="3649" created="2023-03-28T06:20:28Z" accessed="2023-03-28T06:20:28Z
<FILE name="com.apple.aggregated.plist" size="164" created="2023-03-28T09:38:01Z" accessed="2023-03-28T09:38:01Z" modifie
<FILE name="com.apple.amsengagementd.plist" size="1039" created="2023-03-28T09:22:59Z" accessed="2023-03-28T09:22:59Z" mo
<FILE name="com.apple.animoji.plist" size="638" created="2023-01-12T19:18:14Z" accessed="2023-01-12T19:18:14Z" modified="
<FILE name="com.apple.announce.plist" size="134" created="2023-02-02T21:26:33Z" accessed="2023-02-02T21:26:33Z" modified=
<FILE name="com.apple.ap.adprivacyd.plist" size="637" created="2022-12-20T01:56:54Z" accessed="2022-12-20T01:56:54Z" modi
<FILE name="com.apple.appResume.freezerRecommendations.plist" size="122" created="2022-10-04T11:56:45Z" accessed="2022-10
<FILE name="com.apple.appleaccountd.plist" size="681" created="2023-03-28T07:09:39Z" accessed="2023-03-28T07:09:39Z" modi
<FILE name="com.apple.appstored.plist" size="1555" created="2023-03-28T08:49:42Z" accessed="2023-03-28T08:49:42Z" modifie
<FILE name="com.apple.aprs.plist" size="62" created="2022-12-29T04:04:22Z" accessed="2022-12-29T04:04:22Z" modified="2022
<FILE name="com.apple.apsd.plist" size="14520" created="2023-03-28T09:38:11Z" accessed="2023-03-28T09:38:11Z" modified="2
<FILE name="com.apple.asd.plist" size="929" created="2023-03-28T06:20:36Z" accessed="2023-03-28T06:20:36Z" modified="2023
<FILE name="com.apple.assetsd.plist" size="1036" created="2023-03-28T08:31:38Z" accessed="2023-03-28T08:31:38Z" modified=
<FILE name="com.apple.assistant.backedup.plist" size="893" created="2023-01-11T14:56:01Z" accessed="2023-01-11T14:56:01Z"
```

Figure No. 6: Shows the create date of a specific application

Results and Discussion

The cloud data was obtained and examined. The accessed, modified and created dates were studied in order to check the step wise accessibility of the data stored on the iCloud. Once the iCloud data was analyzed and segregated by the cloud analyzer, its login activity was studied. The date at which it was first installed was obtained similarly, the frequency at which it is being accessed could be determined. The complete logs of the iCloud data are crucial to for the security of a user. Along with the login information, the network details at which the cloud application has been connected to at different time periods can also be examined through the obtained report. Each information obtained in the report is crucial to be studied as can provide complete details of the storage application. Other than the above method, there can be an alternative way of doing the cloud data recover which is through Mobiledit Forensic Express if the report exported in UFDR format.

Such type of data which comprises of the entire information regarding the accessibility of the cloud storage applications could be highly beneficial in the forensic investigations, as it can easily determine the login activity at the time of data breach. However, the cost and time involved in extracting data, as well as the accuracy of the data, are major obstacles. The correctness of the data depends on the quality of the data source, which can be an expensive and time-consuming procedure. Along with the extraction, the process of gathering evidence is challenging in the cloud environment due to the transitory nature of cloud computing and the physical inaccessibility of evidentiary artefacts.

Conclusion

Cloud computing is a hands on technology that has been serving all kinds of businesses and day to day life processes, which is a shared platform of different resources such as data storage, user applications, etc. However, with increasing demand and activity of cloud computing, its limitations have also been projecting in our lives such as data breach and unknown user activity. This paper resolves such problems where information regarding the user activity on the cloud application and its data accessibility can be obtained. UFED analyzer is vital tool which helps in recovering and extracting the cloud data which can be further analyzed and the obtained data can final be examined to study the logs provided. But this also comes along with the challenges which needs to be kept in mind before performing such processes. This research carries a lot of information in the cyber forensics as it can reveal information with respect to the entire user activity.

References:

“Everything You Need to Know about Cloud Forensics.” https://www.appdirect.com/blog/cloud-forensics-and-the-digital-crime-scene#:~:text=What%20Is%20Cloud%20Forensics%20and,and%20can%20better%20preserve%20evidence.

“What Is Cloud Computing? A Beginner's Guide: Microsoft Azure.” | Microsoft Azure, https://azure.microsoft.com/en-in/resources/cloud-computing-dictionary/whatiscloudcomputing#:~:text=Simply%20put%2C%20cloud%20computing%20is,resources%2C%20and%20economies%20of%20scale.

Cloud Threat and Security Report: Addressing Cyber Risk and Fraud in ... https://www.oracle.com/a/ocom/docs/cloud/oracle-ctr-2020-addressing-cyber-risk-and-fraud-in-clud.pdf?source=%3Aow%3Ao%3Ah%3Amt%3A%3A%3ARC_WWMK210122P00009C0007%3AJC21_OCI_Q3_C14_M3401_S031YZ18_DS153_T11&lb-mode=overlay.

References:

Eleyan, Amna, and Derar Eleyan. “Forensic Process as a Service (FPaaS) for Cloud Computing.” European Intelligence and Security Informatics Conference, Sept. 2015, https://doi.org/10.1109/eisic.2015.14.

Scaler Topics - Technopedia for Your Mastermind, https://www.scaler.com/topics/cloud-computing/riskmanagementincloudcomputing/#:~:text=Risk%20management%20in%20cloud%20computing%20follows%20a%20process%20that%20involves,data%20breaches%2C%20availability%20and%20cyberattacks.

Sharma, Puneet, et al. “Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications.” Procedia Computer Science, vol. 167, Elsevier BV, Jan. 2020, pp. 907–17. https://doi.org/10.1016/j.procs.2020.03.390.

Shop, Spy. “Cloud Data Extraction - UFED Cloud Analyzer.” Detective Store - Spy Equipment and Surveillance Gear, https://www.detective-store.com/ufed-cloud-analyzer-for-cloud-data-extraction-1284.html.