A Unified Forensic Framework for Data Identification and Collection in Mobile Cloud Social Network Applications

Muhammad Faheem
School of Computer Science and informatics
University College Dublin
Dublin, Ireland

Dr Tahar Kechadi
School of Computer Science and informatics
University College Dublin
Dublin, Ireland

Dr An Le Khac
School of Computer Science and informatics
University College Dublin
Dublin, Ireland

***Abstract*—Mobile Cloud Computing (MCC) is the emerging and well accepted concept that significantly removes the constraints of mobile devices in terms of storage and computing capabilities and improves productivity, enhances performance, saves energy, and elevates user experience. The consolidation of cloud computing, wireless communication infrastructure, portable computing devices, location- based services, and mobile web has led to the inauguration of novel computing model. The Mobile social networks and cloud computing technology have gained rapid and intensive attention in recent years because of its numerous available benefits. Despite being an advanced technology to communicate and socialize with friends, the diverse and anonymous nature of mobile cloud social networking applications makes them very vulnerable to crimes and illegal activities. On considering the point of mobile cloud computing benefits, the forensic assistance based mobile cloud computing could offer a solution to the problem of social networking applications. Therefore, this work proposes a Mobile Cloud Forensic Framework (MCFF) to facilitate forensic investigation in social networking applications. The MCFF comprises of two components such as the forensic logging module and the forensic investigation process. The forensic logging module is a readiness component that is installed both the device and on the cloud. The ClouDroid Inspector (CDI) tool uses of the record traced by forensic logging module and conduct the investigation in both the mobile and the cloud. The MCFF identifies and collects the automated synchronized copies of data on both the mobile and cloud environment to prove and establish the use of cloud service via Smartphones.**

Keywords*—Mobile cloud computing; forensics; mobile cloud forensics; social networking applications

I. INTRODUCTION

The skyrocketed explosion of mobile applications and the support of cloud computing for a variety of services for the mobile users has motivated to integrate the cloud computing into the mobile environment. The Mobile Cloud computing introduces new types of high scalability and low-cost on-demand services and benefits for the mobile users to experience the full advantage of cloud computing [1] [2].

The benefits of MCC are the extended battery lifetime, improved data storage capacity and processing power, and more reliability. Several business organizations have invested in the applications of MCC, specifically in social networking applications [3].

The Social networks allow its users to access the networks soon after publishing their personal data such as name, age, gender, interests, whereabouts and habits. The cyber criminals take advantage of these abundant personal information that are uploaded to the social networking websites to manipulate and exploit at their hire and commit illegal activities. The common illegal activities that are being committed on these websites include uploading illegal material, defaming and stalking [4]. The vulnerability of the social networking applications to commit the numerous criminal activities has increased the importance of digital forensics in this domain. The digital evidences collected from social networking applications on a suspect's smartphone have great significance in investigating a crime scenario to prove the suspect's innocence.

The mobile users also communicate through the cloud storage services to store the data and access storage through a variety of Inter- connected devices [5]. The toughest aspect of investigating a cloud storage service is that it is hard to find out the user's activity till the end of their use of service [6]. Several free and paid cloud storage services are available such as Dropbox [7], Microsoft SkyDrive [8], and Google Drive [9]. These remote cloud storage services store the data of mobile social networking applications such as Twitter, Facebook, Skype, Google plus, and WhatsApp. Therefore, the information collected from the mobile cloud storage has a high forensic value. A Mobile cloud forensics is an interdisciplinary of cloud computing and digital forensics. There are no forensic capabilities between the cloud service providers and customers that could assist investigations of illegal activities in the cloud [10]. There is an urgent need to frame a well-established cloud with forensic capabilities, including a set of toolkits and advanced procedures for cloud investigations [11]. The forensic cloud in [12] suggests the investigators to concentrate more on enhancing the investigation process rather than concentrating on technology used in the investigation process. The mounting demand of mobile device and cloud platform, throws a poses several threats perpetually while there are only limited security features. A review conducted by Ruder Finn (PR agency) estimated that 91% of smartphone users stay in online to access social networks [13]. The number of active

social network users in 2014 was around 1.79 billion. In 2018, it is estimated that the number of active social network users will be around 2.44 billion [14]. Cyber criminals and illegal activities exploit the advantage of the mobile cloud environment to commit crimes in social networking applications. The criminals can broadcast terrorist ideology, share information, and manipulate other's personal information manipulating the social networking applications. The innocent-seeming social network user profiles are susceptible to the danger of secrecy of Android devices [15]. Therefore, incorporating forensic investigation in social networking applications has a high scope and significance to prove the suspect's innocence.

This work attempts to conduct forensic investigation in mobile cloud social networking application by developing a mobile cloud forensic framework. The framework comprises of two components such as a forensic logging module and an investigation process. The investigation process exploits the forensic logging module to conduct investigation process. The framework deploys a CDI tool to perform investigation in mobile cloud based social networking application. The main idea of the MCFF is to identify and collect the synchronized data copies of mobile and cloud environment.

The next section defines Aim and Objective followed by problem statement, contributions and related work in the area of mobile cloud application forensics. The section 3 is an overview of Mobile cloud forensics frame work and two case studies. In section 4 we explain experimentation and results of the case studies followed by conclusion and future work

A. Aim and Objectives

It is a challenging task to identify and collect the evidential artifacts from the mobile cloud environment. The primary goal of this work is to develop a forensic framework to identify and collect the evidence from the social networking applications to ensure the device's use of cloud service by correlating the evidences collected from mobile and cloud. The core aim and objectives of this work include:

a) To develop a mobile cloud forensic framework to identify the use of the cloud-based application and to collect the evidential artifacts on the cloud with the assistance of data identified and collected from the mobile device.

b) To develop a unified forensic framework for data identification and collection in mobile cloud social network applications. This framework is designed to support various applications that run on different mobile devices and flexible enough to work with various cloud service providers. It validates and ensures a forensically sound approach.

c) To solve the multi-jurisdiction and multi-tenancy issues in collecting the evidential data from the cloud environment and establish and maintain a chain of custody for evidence.

B. Problem Statement

The Mobile devices are not pre-installed with security software to protect from malicious applications. In the absence of security software, the cyber criminals could use malicious application with ease to get an access to the user's private information. There is no unified framework for assisting the forensic investigation. It is still a challenging task to conduct forensics in a mobile cloud environment. The activities performed through social networking applications can be stored both in the mobile and cloud environment. However, several earlier works are limited to the retrieval of very basic information related to the use of social networking applications. There are possibilities to determine whether the activities performed through social networking applications and collect them. The current forensic investigation procedure lacks the recovery of data from both the mobile device and the cloud. The identification of the real suspects is a major issue in the mobile cloud environment. There is no unified mobile cloud forensic architecture to support several applications running on diverse Smartphones with different cloud service providers. For any mobile cloud social network application, there is some possible provenance to prove the ownership or the connection from the seized device, but it is absent while examining the cloud. Therefore, there is a requirement for identifying and collecting the residual artifacts of mobile applications left behind the device and a cloud.

C. Contributions

The key contribution is the development of a forensic framework for the mobile cloud environment, especially for social network applications. The main contributions of this work include:

1) This work extends the social networking applications with a forensic readiness component called forensic logging module. The Mobile Cloud Forensic Framework exploits forensic logging module for identifying and collecting the forensic rich data in mobile and cloud side. The proposed unified framework supports a variety of social network applications running on diverse mobile devices, and it is a standard framework flexible enough to work with different cloud service providers.

2) The proposed framework facilitates the forensic capabilities that collect the automated synchronized copies of data on both the mobile and cloud server to prove the evidence of cloud usage using CDI tool. The add-on component (forensic logging module) enhances the traceability of events performed by the user with respect to local mobile device and a remote server.

3) This work identifies the evidence of using a cloud service by correlating the artifacts recovered from a mobile device with the cloud artifacts. It validates and ensures collected evidence in a forensically sound condition. It establishes and maintains a chain of custody for evidence.

4) This work solves multi- jurisdiction and multi- tenancy using information traced in the Forensic logging module.

II. Related Work

A forensic examination of an Android phone's logical image reveals that basic Facebook friend information is stored in the contacts database as the device synchronizes all contact's Facebook status updates with the device's contact [16]. It also reveals that the device stores Twitter passwords and updates performed through the Twitter application in the plain text.

However, forensic research works on Blackberry and Windows Smartphones do not state on the recovery of any artifacts associated with the use of social networking applications.

Most of the third-party applications on the Apple Mobile platform contain a significant amount of forensic-rich data [17]. The user's information during the interaction with applications is stored in plain text format and can be recovered from the user data partition of the device. Artifacts such as authentication credentials, timestamps, and Geo-locational references locate a device at a particular time. The data related to third party applications can be retrieved from a forensic image of the device. These data may also be available as backups stored on the machine with which the device has been synced.

The forensic analysis of social networking applications of Facebook, Twitter, and MySpace on three popular smartphones such as BlackBerry Torch 9800, iPhone 4, and the Android-based Samsung Galaxy S was conducted to determine whether activities performed through these applications were stored in the internal memory of the device [18]. Moreover, it extends to estimate the amount and locations of data if stored in the device's memory. The results revealed that the activities could not be recovered from BlackBerry devices, whereas activities performed through these three applications left a significant amount of valuable data that could be recovered and used by forensic investigators in the iPhones and Android phones.

The data of WeChat provides evidential artifacts that may be of considerable value in an investigation [19]. The data that could be retrieved from WeChat identifies the suspect's contacts and affiliations, habits and interests, ideas and beliefs in the iPhone. Though the forensic investigation of WeChat application extracts the evidence in the iPhone, it fails to extract those evidences in the cloud environment.

The forensic investigation of Skype calls and chats on the Android devices revealed that evidence can be extracted from the device. It analyzed both the RAM and NAND flash memories in different scenarios and time. The results of the analysis revealed that the Skype call patterns and chat messages get sticked in the RAM, and NAND flash memories even after deleting calls, chat histories and signing out of the Skype [20].

There are several gaps in the forensic investigation of the mobile cloud environment. There are only a few works in the literature investigating the social networking applications in the mobile cloud environment. Most of the works recovers forensic rich data only from the mobile device. There are no add-on components specifically deployed for the forensic purpose. Moreover, there is no valid solution to multi- tenancy, and multi- jurisdictional issue on the cloud side. There are no efforts made to probe the activities performed through social networking applications by the user in the mobile and cloud environment. This paper mainly focuses on the forensic investigation of cloud-based mobile social networking applications.

III. Mobile Cloud Forensic Framework

The methodology proposes a forensic framework for the mobile cloud environment consisting of two major modules such as a forensic logging module and an investigation module using a tool called ClouDroid Inspector (CDI).

A. Basic Overview of Mobile cloud forensic framework

This work introduces a novel Mobile Cloud Forensic Framework (MCFF) that supports forensic investigation in social network applications. Any of the social networking applications can extend the forensic logging module to help the forensic investigation. An investigator starts the investigation initially with the mobile device after the investigation process has been triggered internally or externally. With the evidence collected from the device, the investigation process is continued on the cloud side. The forensic investigator extracts the potential evidence traced in readiness component and other sources in the mobile and cloud environment using the CDI forensic tool. The main objective of the proposed MCFF is to ascertain the right direction related to a particular investigation scenario.

The MCFF attempts to prove the cloud usage via Smartphone. Therefore, in MCFF, the investigator conducts an investigation in the mobile device and uses the data collected from the mobile device to access the cloud account. The proposed forensic model uses the potential evidence collected from the mobile device to search for similar correlating evidence in the cloud to prove the cloud usage accessed by the Smartphone. It facilitates to handle a large volume of data efficiently so that an investigator has a clear view of the investigation process.

The proposed framework utilizes the advantage of synchronized copies of data on both the device and the cloud server to prove the usage of cloud services. This work attempts to solve the multi-jurisdiction issues to some extent. This work also deals with the Multi-tenancy property of the cloud that introduces difficulties in identifying the real suspect among several cloud users.

Figure 3 demonstrates the architecture of MCFF to identify and collect the synced data of cloud usage through mobile devices. The mobile device acts as a concept of interface for both accessing the social networking application and for forensic analysis.

a) The forensic logging module represents the pre-investigative readiness components with its components of identity management and event management. The Identity management is the ability of a cloud entity/ mobile entity to deal with individual user identities such as authentication and authorization. The functions of identity management enabler are mainly concerned with authorization and authentication. It includes a policy discourse to define with attributes (roles, and identity), and the request for credentials to grant permission to access the resources.

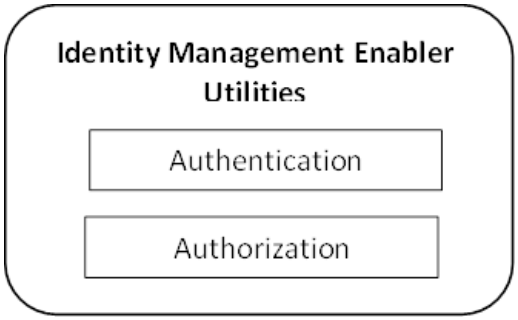


Fig. 1. Identity Management Enabler

The Event Management conceptually constructs the unit of an "event" and technically implement the corresponding concept so that it can be constructed, traced, reconstructed whenever required. Event management is a range of high-level of interoperability among different cloud users. The Event construction defines the event in the cloud environment and mobile environment that answers the questions of "who", "what", "when", "where" and "how". The Event freezing freezes the event at the immediate state in case of a criminal misdeed or an investigation. The Event traceability traces the event's current state of the cloud system and mobile system or back to its original state. The Time sequence capability records a definite and synchronized time series in the mobile and cloud system. The Event reconstruction capability reconstructs the past state of the event with a level of acceptable accuracy so that the reconstructed information can be declared as the digital evidence.

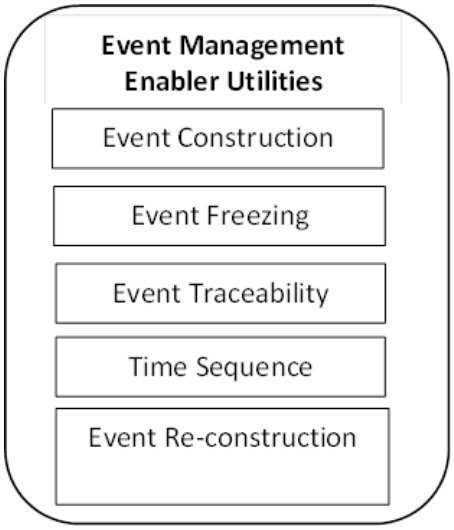


Fig. 2. Event Management Enabler

b) The investigation module in the mobile and cloud indicates the core forensic procedures. This work is designed an investigation tool called CDI that exploits the data traced by the forensic logging module to perform a forensic investigation initially on the mobile device followed by the cloud shield. Finally, the forensic investigation can prove the mobile device's use of cloud service through correlating the evidence extracted from mobile and cloud environment. The existing identification and data collection methodologies in forensics do not design a separate logging module. Moreover, the existing forensic data collection methods do not use data reduction techniques. The proposed data collection technique uses reduced data collection technique to collect only the potential evidence that is relevant to the crime scenario. These potential evidences are enough to prove the cloud usage via Smartphone.

B. Forensic readiness - Forensic Logging Module

The proposed approach designs a separate logging module to act as a forensic readiness component and traces the log related to only social network applications despite system log. This is because, the device stores the log files in circular buffer and the storage capacity of those buffers is relatively small. The new information of log file overwrites the oldest information if the list is full. The time factor becomes an obstacle for the forensic investigator. It is not possible in all the cases for the investigator to seize the device right after a crime has been committed. Critical information regarding the crime can be overwritten by any other new information in the log file. Therefore, this work intentionally designs a logging module to assist forensic investigation.

The forensic logging module comprises of a log generator, a log transport, and a log harmonizer. The log generator enables the logging of component from which the logs are to be collected. The status of an application has to be logged with respect to the authorization, whether it is a success or a failure. Some of the essential activities to be traced regarding social networking applications are the login and logout in both local and remote access, password and authorization changes, denied authorization and all the events performed by a privileged account. The log transport module of the logging module transfers the collected records to the device's local storage (location of the forensic SD card). This store is not accessible to mobile users. The log harmonizer is a centralized component that tunes different log type to appropriate or common log type.

The log fields of forensic logging module are selected based on two functionalities such as identity and event of a user. The identity functionality provides the answers to who committed the crime. The event functionality provides the answers of what, why, and when. Therefore, the forensic logging module covers the logging fields in every log such that it provides answers for who, what, why and when in social networking applications. The log fields relating to the identity of a user include User_Unique_ID, and Geo-location while the log fields relating to events performed by the user include Time_stamp, Application, Event_Performed, Session_ID, Status, Severity, and reason.

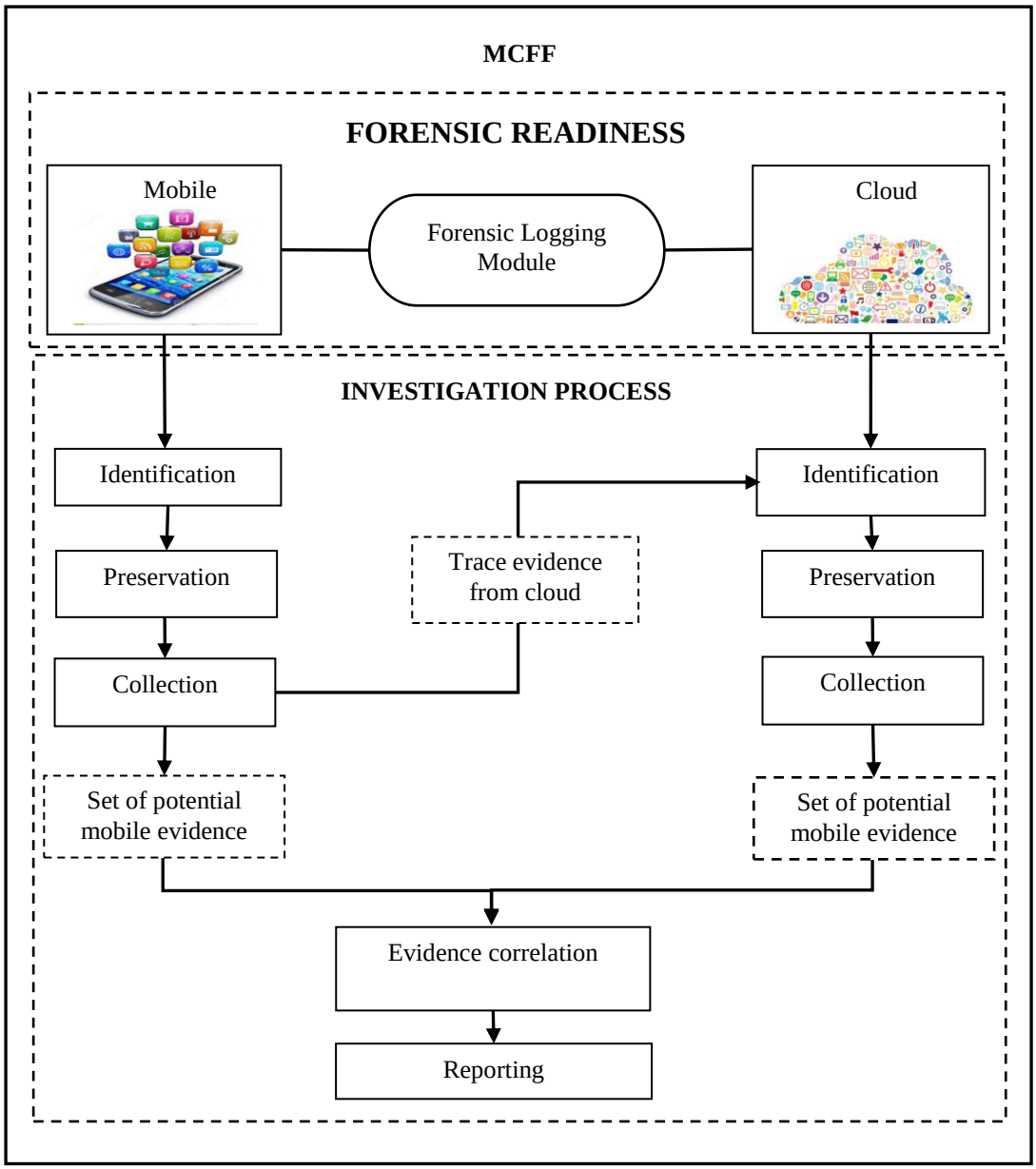


Fig. 3. Architecture of Mobile Cloud Forensic Framework

{ User_Unique_ID, Time_stamp, Application, Event_Performed,Session_ID, Geo_location, Status, Severity, reason }

The User_Unique_ID log field reveals the unique ID of the particular mobile user accessing the cloud service (social network application). The unique ID considered in this work is International Mobile Equipment Identity (IMEI) number of a device. Time_stamp indicates the time of the traced event happened. The Application field indicates the social networking application that generated the log entry. A Session_ID represents a single request from the mobile to cloud service. The Geo_location represents the latitude and longitude of the device. The status represents whether the login request for accessing the social network is success or failure. A Severity categorizes the type of log such as debug, info, warn, or error identifies the reason why something has happened. For instance, the reason explains why the access was denied. The investigator can even apply data reduction techniques in the logging module to filter the log records in terms of any of the logging fields to obtain most relevant evidence to the crime scenario.

C. Forensic Evidence

The android OS offers an open development platform. This facilitates developers the control to develop applications that gain full advantage of some functionalities such as location information, the ability to set alarms, add notification services to the status bar, and several other features. The files and meta-data extraction process involves 3 steps: initially, obtains the image of the disk, extracts the files from the image and analyzes the evidences. This process is implemented initially

on the mobile side and followed by the cloud. Finally, correlates the evidence collected from mobile and cloud side. Two scenarios are created to conduct a forensic investigation using the proposed ClouDroid Inspector tool to prove the use of social networking applications installed in Smartphones by running Android operating system. The CDI tool is responsible to conduct investigation in mobile and cloud environment. The CDI tool is capable of locating the log records traced by the forensic logging module in cloud and mobile. The CDI tool initiates the forensic investigation in mobile side followed by the cloud side. This work develops a sample social network application called Model Social Network Application (MSNApp) and SocialApp. The functionality of the MSNApp and SocialApp are similar to other social network application that allows registered users to a create account, upload images, audios, and photos, send texts, and keep in touch with friends, family and colleagues.

Scenario 1: An employee (suspect) is believed to be transferring the stolen confidential documents to another company using his cloud account through Smartphone. This scenario is considered to illustrate the capability of the proposed work to prove the data possession of the suspect.

- Step 1: Identification in mobile device

The investigator identifies the sources of evidence in the suspect's mobile device. The Identification and collection of evidence in mobile devices are not formally conducted as the real identification would proceed with law enforcement identifying mobile devices. The mobile device is kept in a controlled virtual machine environment. Enable the USB debugging tool called Android Debugging Bridge (ADB) present in the SDK to get connected to the device and access the command shell with rooting privileges and make a copy of the system partitions stored in the internal memory. The most common technique to identify the source of evidence in mobile devices is "Imaging". This virtual image collection would be equivalent to the physical disk image file. There are several system partitions in the Android OS such as boot, system, recovery, data, cache, and misc. The MTD (Memory Technology Device) based devices have "/proc/mtd" populated with the partition layout, by the linux kernel. Thus, no specific partition layout file is required by Online Nandroid, on MTD based devices. This work is interested in collecting data from the system and data partitions. The identified files are preserved using a software Write-blocker.

- Step 2: Collection in mobile device:

The CDI tool initially collects the log files traced by the readiness component. The logging module stores the log files (social network application logs) in the system reserved area so that it can be accessed only by the CDI. The CDI not only collects the log files but also other files such as sync and file meta-data. The sync and file meta-data artifacts in mobile device have high forensic importance that reflect the use of cloud computing. These artifacts not only provides log data, but also determines the cloud instances that assist to link the user actions with the data stored in the cloud environment through the file meta-data such as authorization and timestamps.

With the rooted Android mobile device, the CDI tool access the protected directories on the system related to social network application's data (/data/data directory) and a backup of all the files in this directory in the suspect's Smartphone. Install a new forensic SD card in the device and the location of this SD card is selected as the location to write the collected data to the forensic memory card. The files copied in the forensic memory card are then analyzed individually. The "dd" / "cp" command is used to collect the files from the mobile and copy to the forensic SD card. The CDI collects the details of the logging module as shown below.

{ 358472042445412, Fri Apr 24 09:54:37 GMT+05:30 2015,
MSNApp, upload, 07GdftrGGRjYYHFS3KIYHGR, 121.47856
46.52379 4362, success, Info, does not exist }

The CDI exploits SQLite database browser to collect data from the SQLite database. The SQLite database contains numerous significant data required for the current investigation process. The CDI retrieves the username and password from the tables of SQLite database and uses this information to access the social networking application.

The sync metadata is stored on the client in SQLite database (DB.sqlite). The DB sqlite file contains a wide range of information of forensic importance. The database comprises of a table called "metadata". It stores the cached files in synchronized directories on the local disk. The file metadata configurations/ databases can locate the files/directories synced to the local client. The data related to the cloud service and authentication is collected from "cloud.cfg" which is a configuration file located in the path directory of the corresponding application. The configuration file comprises of a list of "url", "user"', and "passwords". This information is enough for the investigator to prove the usage of cloud services through mobile device. The mobile device offers cloud details and credentials for the user and cache files accessed and a list of files stored on the Cloud instance during the last sync.

The android device does not facilitate a unified backup solution. Several organizations have developed backup tools to facilitate the user for backing up the device using SD card or organization's server. To recover the deleted data on the mobile device, the configuration files have to be synced with the "Backup" directory using the extension of ".cfg". This allows the CDI to recover the cloud instance, username, and password used on the mobile device even after the suspect has deleted the content on the mobile device. Some application stores the username and password in the SQLite database in the encrypted form. It is difficult to retrieve the original password from encrypted form. The possible solution is to use the source code of the installed application. If the password is stored in encrypted format, it can be decrypted using the decompiled Java code for decryption from apk. The encrypted password is passed as an argument to the decryption method that returns the original password.

- Step 3: Identification and collection in cloud:

The CDI precedes the investigation in the cloud side with the data collected from the device. The simplest method of

identification of cloud artifacts is the installation of the forensic logging module. This module is deployed in the cloud purposely for forensic investigation in a special storage. The username and password retrieved from mobile (SQLite database) is used to access the cloud account. In a cloud environment, the data uploaded by the suspect are more important evidence. Data generated by a cloud instance corresponding to a particular user is valuable evidence that links the user to the data located in the cloud environment such as log data or encryption keys. The evidences are extracted using "dd"/ "cp" command. CDI facilitates the investigator to use data reduction techniques to collect a data subset from remote cloud result in time and storage size savings and also makes the consequent investigative steps easier. For instance, the investigator can use the Time_stamp detail (Fri Apr 24 09:54:37 GMT+05:30) to search the data relevant to the given time_Stamp.

- Step 4: Correlation of evidences:

The investigator currently has the data collected from the cloud and the device. The CDI collects log files from the forensic logging module installed both in the mobile and cloud and other critical information. The sync and file metadata, cloud authentication and service data collected from the device supports the investigation.

The file MSNApp.db (collected from SQLite database) holds a set of forensic-rich activities performed by MSNApp user includes chat messages, list of friends, mailbox, and uploaded files, photos and videos. The records include critical information such as the user's ID, contents exchanged, URL of uploaded materials, and timestamps of performed activities. The investigator checks for the same details in the log files collected from the mobile device and from the cloud to prove the suspect's data possession. The same set of details of a user is recorded in logs of both cloud and mobile, and hence, the cloud usage by the user can be proved by timeline analysis. The proposed framework solves the multi-jurisdiction issues and multi-tenancy issues by using user_unique_ID and Geolocation information in the logging module.

The forensic investigator correlates this evidence to reconstruct the digital crime scene after collecting the evidences. Moreover, the cloud system tracks every change occurring in the client data and keeps different versions of them using a versioning technique. This technique helps to retain the original data at different times. This work has chosen the versioning technique to reconstruct the evidence in a short time between the cloud and the mobile. The information collected from logging module, SQLite database, synced and file metadata proves the data ownership of the suspect. The investigation process is then documented for reporting.

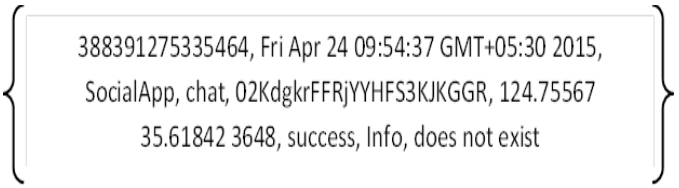
Scenario 2: A Person 'X' uses the victim's cloud account to spread (upload) inappropriate material via MSNApp on Fri Apr 24 09:54:37 GMT+05:30 2015. This scenario is considered to prove the innocence of the victim using MCFF (CDI tool). In this scenario, the person 'X' is a real suspect. Moreover, this scenario highlights the importance of considering the cloud evidential artifacts to deal with the scenario in addition to mobile evidential artifacts.

The investigator keeps the time at which the inappropriate material has been spread as the reference time. In this scenario, the investigator has to check whether the activity logged at the reference time in both the mobile and cloud is the same or different. The victim may or may not be accessing the social network application at the suspected time of inappropriate material sharing. In case, if the victim is accessing the social networking application at the reference time, the activity performed will be different from that of the victim's friend. If the victim is not accessing the social network application, the event will not be traced in the logging module as the module traces only the logs related to social networking application.

- Step 1: Identification and collection in mobile side:

The device and the cloud traces and stores the log files in the forensic logging module. The CDI tool gains the root access and identifies the system partition. The CDI tool initially images the possible sources of evidence on the mobile side. The "data" partition consists of data related to third party application. The CDI tool identifies the logging module and other critical location holding files of interest. The use of software write-blocker preserves the identified files. The SQLite database in the device contains more critical information. The Data regarding the use of cloud service and authentication is identified and collected from "cloud.cfg" which is a configuration file located in the path directory of the corresponding application.

The configuration file comprises of a list of "url", "user"', and "passwords". The "dd"/ "cp" command is used to collect the evidences. The information is collected from the device to the installed forensic SD card as explained in the scenario 1. The information collected from the logging module of the mobile device is listed below. According to this scenario, the information in the logging module is enough to prove the victim's innocence.



The log files reveal that the victim's device has used a social network application called Social App (a sample social network application) on Fri Apr 24 09:54:37 GMT+05:30 2015 and performed a chat activity.

With this evidence, the investigator cannot arrive at a conclusion because there is a chance for the victim to alter the log details. Therefore, the investigator has to investigate the cloud side to decide on victim's compliance.

- Step 2: Identification and collection on cloud side:

The CDI is capable of identifying the location of files stored in the forensic logging module in the cloud. The investigator then makes a decision for selecting the method of collection based on the quantum of the instance. The information collected by the logging module of the cloud are listed below.

388391275335464, Fri Apr 24 09:54:37 IST 2015, SocialApp, chat, 02KdgkrFFRjYYHFS3KJKGGR, 124.75567 35.61842 3648, success, Info, does not exist

- Step 3: Correlation of evidences:

The investigator can prove the cloud usage using the collected artifacts only after the correlation of evidences. The investigator can correlate the log files (in this scenario) collected from the mobile and cloud side to link the victim with an activity. Cross referencing these artifacts in the aspect of timeline analysis determines the distributed user activity. There are several challenges in correlating the cloud and mobile evidential artifacts. The time_stamp of an activity differs from server to server. Therefore, time_stamp from the local file system of every server in the cloud does not represent the same time. This work suggests setting up a reference time in the cloud and to use the time synchronization protocol. The log records have revealed the same details on cross referencing the evidence collected from the device and cloud. It confirms that some other person has used the victim's MSNApp cloud account to spread illegal material on Fri Apr 24 09:54:37 GMT+05:30 2015. This set of evidences proves the victim's innocence. The investigation procedure is finally documented for reporting. The detection of real suspect is not the focus of this scenario but to prove the innocence of the victim using MCFF.

IV. EXPERIMENTATION

This work uses the Java language to conduct mobile cloud forensic investigation on the Android platform.

A. Development tools

The Eclipse is an integrated development environment which ensures a complete functional and commercial quality industrial platform. It contains a base workspace and an extensible plug-in system for customizing the environment. The Eclipse is an open source software comprising of the Eclipse platform, Java Development Tools (JDT), C/ C++ Development Tools (CDT) and Plugin Development Environment (PDE). The Eclipse platform is an open extensible IDE providing a common development platform. The JDT supports Java development, CDT supports C/ C++ development, PDE supports plug-in development.

An Eclipse SDK is a combination of all tools and components produced by Eclipse platform, JDT, and PDE. These components together offer a feature-rich and complete development environment to allow developers to develop tools that can be efficiently integrated with ease into Eclipse. The cloud uses Netbeans integrated development environment.

B. Android SDK and virtual device controller

An Android SDK offers the development components which are used to develop Android applications on Windows/ Linux/ Mac. The Android OS supports all platforms with a tool set for Android mobile application development. This tool set comprises of Android emulator, plug-in tools for Android development used in Eclipse (ADT), and tools for debugging, packaging and installing applications in the Android emulator. The Android SDK supports the Java language to develop applications on the Android platform. The developers could use the tools provided by SDK to introduce the program into .apk file as a package and use the Emulator to simulate and test the Android application.

The actual device has been designed in a virtual environment using Android Virtual Device (AVD). Each AVD defines the hardware and the software options and configures several projects. The virtual device controller offers a graphical user interface in which the developer can create and manage Android Virtual Devices (AVDs).

C. Dalvik Debug Monitor Server (DDMS)

A DDMS is a debugging tool that provides port-forwarding services, screen capture on the device, logcat, current progress, and ratio state information and location data spoofing. Delete the author and affiliation lines for the second affiliation.

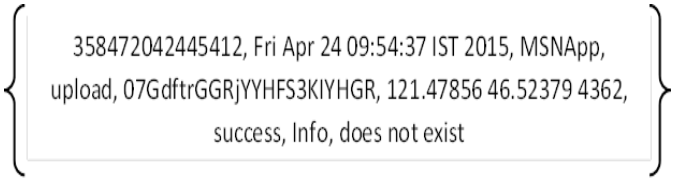
D. Resutls

This section explains the correlation phase of the forensic process. It is this phase that analyses and compares the evidences obtained from the device and the cloud.

Scenario 1:

The CDI tool initially identifies the location of the log records traced by the forensic logging module in the device. The investigator obtains the entire log file and filters out specific details. These specific details correspond to the data relevant to the crime scenario. The files stored in the forensic logging module are recovered from the application package directory /data/data/com.example.ModelSocialNetworkApp. This directory contains four folders such as Log, cache, databases, and lib. The log files are obtained from the directory /data/data/com.example. ModelSocialNetworkApp/Log.The Log file consists of the information such as IMEI number, Time Stamp, Application, Event, Session ID, Geolocation (Latitude, Longitude), Status, Severity, Reason. The important source of evidence in device is SQLite database. The records in the database of the MSNApp can be obtained from /data/data/com.example.ModelSocialNetworkApp/databases.
The database of MSNApp comprises of three tables such as UserDetail, android_metadata, sample_table. The actual username and password are recovered from the table called UserDetail. The username and password for accessing the MSNApp are "user1@gmail.com" and "user1@123" respectively.

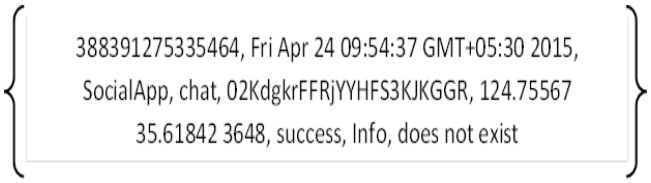
The files in the database contain several other significant information such as the chat messages and the URL links of uploaded pictures. The uploaded files from the MSNApp have names preceded with the word "upload". The SD- card is installed in the directory /mkdir/sdcard/Forensics/ for forensic purpose. The evidential artifacts are written into the SD card. The password and the username extracted from the device are given as input to access the MSNApp. The CDI tool recovers the log files from the cloud directory /home/eucalyptus/Forensic/log/LogFile1.log. This log file is also written into the SD card.



The log in the cloud revealed that the file has been uploaded using MSNApp on Fri Apr 24 09:54:37 IST 2015. The log in the mobile also has revealed the same. Therefore, the uploading of the file via MSNApp from the device has been proved using the CDI tool.

Scenario 2:

There are two social networking applications on the victim's device called MSNApp and SocialApp. The victim's friend has used the victim's MSN account to upload inappropriate material on Fri Apr 24 09:54:37 GMT+05:30 2015. To prove the victim's innocence, it is enough to collect and correlate the log files in mobile and cloud side. The CDI tool collects the log file from both the social networking application installed on the victim's device. There is no log information gathered from the MSNApp at the reference time from the victim's device. Instead, a log file is obtained from the SocialApp at the reference time from the directory /data/data/com.example.SocialApp/Log.



The log collected from the victim's device reveals, that the victim was chatting on Social App at the reference time and no log was recovered from the MSNApp. The CDI tool progresses the investigation to the cloud side as there is a chance for the victim to delete the log details. The CDI tool collects the log records from the directory /home/eucalyptus/Forensic/log/LogFile1.log and filters the record for the entries related to the reference time. The log file collected from the cloud appears as the same as the log file obtained from the device. This confirms that victim has accessed the Social App at the reference time. Therefore, the correlation results conclude that someone has used the victim's MSNApp account to upload the inappropriate material.

V. Conclusion & Future Work

This work proposes a Mobile Cloud Forensic Framework to support forensic investigation in mobile cloud environment. The two major parts of the framework are the forensic logging module and the forensic investigation process. The forensic investigation process employs the forensic logging module to conduct investigation. This work has proved that the proposed MCFF has secured a number of significant evidences from both the mobile and the cloud. In futre any social networking application can extend the forensic logging module. Two scenarios are created to validate the effectiveness of the proposed MCFF. The CDI tool, locates the files of the logging module in the device and the cloud. It initially collects the sensitive information from the device and then proceeds to the cloud. The CDI successfully conducts the forensic investigation in two scenarios. The MCFF is able to trace the cloud instance, even if an evidential data is securely deleted on the mobile. The correlation of potential evidences of mobile and cloud alone considerably restricts the time spent on the investigation.

References

[1] Dinh, Hoang T., Chonho Lee, Dusit Niyato, and Ping Wang, "A survey of mobile cloud computing: architecture, applications, and approaches" Wireless communications and mobile computing, Vol. 13, No. 18, pp. 1587-1611,

[2] Qi, Han, and Abdullah Gani "Research on mobile cloud computing: Review, trend and perspectives" Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP), 2012.

[3] W. Zhenyu, Z. Chunhong, J. Yang, and W. Hao, "Towards Cloud and Terminal Collaborative Mobile Social Network Service," in Proceedings of the 2nd IEEE International Conference on Social Computing (SocialCom), pp. 623, 2010.R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[4] De Paula AMG "Security aspects and future trends of social networks" Proceedings of the 4th International Conference of Forensic Computer Science, pp. 66 –77, 2009

[5] George Grispos, William Bradley Glisson, and Tim Storer, "Using Smartphones as a Proxy for Forensic Evidence contained in Cloud Storage Services" 46th Hawaii International Conference on System Sciences, pp. 1-10, 2013

[6] M. Taylor, J. Haggerty, D. Gresty, R. Hegarty "Digital evidence in cloud computing systems", Digital Investigation, computer law and security review, Vol. 26, pp.304- 308, 2010

[7] https://www.dropbox.com/

[8] https://www.dropbox.com/help

[9] https://drive.google.com/drive/

[10] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: An overview," in proceedings of the 7th IFIP International Conference on Digital Forensics, pp. 35- 46, 2011.

[11] Keyun Ruan, Joe Carthy, Tahar Kechadi, Ibrahim Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results", Elsevier journal on Digital Investigation, Vol. 10, No. 1, pp. 34- 43, 2013

[12] Jooyoung Lee and Dowon Hong, "Pervasive Forensic Analysis based on Mobile Cloud Computing" IEEE computer society, 3rd International Conference on Multimedia Information Networking and Security, pp. 572- 576, 2011

[13] Finn Ruder. "New study shows 'intent' behind mobile Internet use" Retrieved on 18 February 2012 from: http://www.prnewswire.com/news-releases/new-study-shows-intent-behind-mobile-interetuse-84016487.html, 2012.

[14] http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

[15] Andrew Hoog, "Android Forensics: Investigation, Analysis, and Mobile Security for Google Android" Elsevier, 2011

[16] Lessard J, Kessler GC. "Android forensics: simplifying cell phone examinations" Small Scale Digital Device Forensics Journal, Vol. 4, No. 1, 2010;

[17] Levinson, A., Stackpole, B., Johnson, D. "Third Party Application Forensics on Apple Mobile Devices" 44th Hawaii International Conference on System Sciences, pp. 1-9, 2011

[18] Noora Al Mutawa, Ibrahim Baggili, Andrew Marrington, "Forensic analysis of social networking applications on mobile devices" Elsevier transaction on Digital Investigation, Vol. 9, pp. S24–S33, 2012

[19] Feng Gao, and Ying Zhang, "Analysis of WeChat on IPhone" 2nd International Symposium on Computer, Communication, Control, and Automation (3CA), pp. 278- 281, 2013

[20] Mohammed I. Al-Saleh, and Yahya A. Forihat, "Skype Forensics in Android Devices" International Journal of Computer Applications, Vol. 78, No.7, pp. 38- 44, 2013.