Acta Scientific COMPUTER SCIENCES

Volume 2 Issue 10 October 2020

Research Article

Catch Me if You Can: Analyzing Geolocation Artifacts Left by the Tile Application on iPhones

Valentin Gazeau* and Qingzhong Liu

Sam Houston State University, Department of Digital Forensics Huntsville, Texas, USA

***Corresponding Author:** Valentin Gazeau, Sam Houston State University, Department of Digital Forensics Huntsville, Texas, USA.

Received: August 12, 2020

Published: September 30, 2020

Abstract

Mobile Forensics is a branch of Cyber Forensic that gathers and analyses mobile devices such as smartphones, tablets and third party applications to collect digital data of forensic value. Mobile forensic software tools mainly investigate ”typical” cell phone data such as contact information, text messages and voicemail. Most of the time, these methods ignore the data stored in third party applications. Most third-party applications mounted on Apple iOS mobile devices leave a trace with items of forensic significance. This includes records of user identity, such as passwords, timestamps, geographic locations, contact information, native data, and various media archives. One such application called Tile could potentially hold very valuable information which can be used in a digital forensics investigation such as geolocation of specific items at a given time.

Keywords: Mobile Forensics; Cyber Forensic; iPhone

Introduction

People everywhere in the world carry cell phones and/or other mobile devices with them. Forensic examiners have discovered that knowledge from these devices can be indispensable during an investigation [1]. The data collected by the user can include crucial information such as who they connect with and where they traveled which is all connected to the network clock of the cellular provider. The range of information stored by the user’s smart device consists of email history, geo-location information, usernames, passwords, wireless access points and timestamps which is a goldmine of information from an investigative point of view [1].

With the launch of the iPhone, the Apple company has created a mobile handheld platform that allows users to install and configure a wide range of applications through their app store [2]. With the app store, users can select and install applications of their choice and the software is downloaded and installed from the Apple servers [2]. The user can now start the app which immediately starts collecting data about the user for their customized use and store information about how and when they interact with the application.

Anyone who has enough programming expertise can write applications once they agree to the conditions set out in the Apple Developers License. Apple’s Software SDK includes many programming lessons for a developer to locally store data on the smart device [2]. Third-party application information are typically maintained in plain text format according to the programming specifications established by Apple [2]. When people communicate with their applications the data provided by the user would be preserved locally on the smartphone and rendered accessible to a forensic investigator.

Tile is a company that produces devices to help users find their belongings, such as keys, wallets and backpacks [3]. The devices work with a companion Android and iOS mobile app that allows users to locate lost items through Bluetooth or where they were last seen. When an object is attached to a keychain or other element by a Tile hardware unit, a consumer may use the Tile app to find the component if the object is missing [3]. The Tile application uses radio technology from the Bluetooth low-energy 4.0 technology to locate any tile in a range of 150-foot to 300-foot. The application will detect Tile outside the Bluetooth range of 100 feet with ”crowd

GPS": when an object with a Tile tracker is recorded missing beyond the reach of another user's Tile program, the program of the next user can submit an anonymous alert of the item's position to the owner of the product [3]. Alternatively, a user can share his or her tile with a user so that both users can find the tile.

The device is a tiny, high-tech gadget that one can attach or put inside things like keys, phones, and wallets to keep them from being lost with the help of the application which showcases all tile devices within a map [3]. While Tile was designed primarily to help people keep track of their belongings. As Tile has grown in popularity, crimes that have in some way involved the application, have also increased, particularly crimes that involve stalking and abuse, in fact it was reported multiple times that they have been used maliciously to stalk other people by hiding a Tile device in a purse, car consoles and such [3].

The situation prompts this study to identify, recover and analyze artifacts related to Tile's use. The first detailed forensic analysis of the Tile third party application is presented in this report on Apple iOS devices. The precondition to accessing such objects are that the iOS device is password unlocked and the researcher has access to unencrypted backup data. The assumption here is that the Tile application can store very valuable data during an investigation in the form of geolocation coordinates with their corresponding time stamps of specific items. The Tiles could also be used by users preemptively to prove the location of an item of interest at a specific time in court.

This study focuses on the following suggested questions, common to forensic examinations:

- What items are being tracked by the user.
- A list of geolocations for each of the tracked items.
- A list of timestamps related to each geolocation of each item.

The remainder of this paper is structured as follows. Section two covers the literature review. Section three describes the research methodology. Section four presents the experimental results and an analysis of the data. Section five draws conclusions and presents future work.

Literacy Review

Most of the research relating to third party application analysis on smartphone devices relates mostly to messaging applications such as Messenger, Viber, Kik, Whatsapp and such [4]. While some of those applications include geolocation data, those research focused mainly on questions such as: Who has the user been communicating with and when? What was the content of the communications? What attachments were exchanged? etc...

McMillan., *et al.* conducted a study that showed that calls and data from messaging application were provided the most evidential data during digital investigations, but application data such as geolocation were also deemed of considerable importance [4]. Most of the research in the field of mobile forensics has concentrated on finding data of these types on specific operating systems.

Early instant messaging work centered on the common apps of the time on mobile devices. Artifacts from three systems were analyzed by Husain and Sridhar, those applications are: AIM, Yahoo! and Google Talk. The authors managed to find artifacts, even with a small data set, that may have been of interest to investigators. It was obtained by examining the archive files of an iPhone 3G version 2.2.1. Apple's mobile device management program, iTunes, provided the backup files [5].

Al Mutawa., *et al*. conducted a similar stud focusing on applications for social networking which also provide instant messaging apps such as Facebook and MySpace. The smartphone devices being tested included an iPhone 4 version 4.3.3, an Android and a BlackBerry. The methodology used for the research included downloading the software for social networking on the computers, conducting typical usage operations, and imaging each device to perform manual analysis [6]. Similarly to the previous researchers, the authors used the iTunes software to provide a copy of the backup of the user files for the iOS system from which they managed to find objects linked to social networking apps.

A. Mahajan., *et al*. conducted a forensic analysis on five Android smartphones of two of the most used instant messaging application: WhatsApp and Viber. The authors used Cellebrite UFED Classic Ultimate to image the smartphone devices' hard drives. They carried out the forensic analysis using Cellebrite's UFED physical analyser and a manual examination. The UFED Interactive Analyzer provided user chat sessions and timestamps for each conversation performed through the WhatsApp application [7]. It did not show any artifacts pertaining to Viber, however. On the other hand, manual analysis revealed that WhatsApp stores its operations in two databases: one stores the chat logs, and the other stores contact list.

Akarawita., *et al*. created ANDROPHSY, which is known as the first open-source mobile forensic platform, it facilitated the whole process of mobile forensic practice. Its performance and functionality compete with other common market-based commercial devices [8]. One of the steps reviews Android device files gathered by logical acquisition. It included an embedded SQLite decoder to make third party application anaylsis easier to conduct. It also featured a time line of each operation, a file explorer, a hexviewer tool and an Android MD5 hash server.

Carmen and Choo researched the Tinder app and showed that the geolocation of a user can be tracked as well as their linked Facebook profile. They also demonstrated that their user pictures can be collected [9].

Hoang, Asano, and Yoshikawa have demonstrated that one can approximate precisely the location of a Grinder user even though the user decides not to reveal his/her position to other users. In fact, they were able to discern the secret geolocation of a user by manipulating the way Grinder arranges certain profiles from the application [10]. Users are sorted by distance in an ascending order, meaning that if a profile is seen before and after a target profile we can use that profile's geolocation to estimate the upper and lower limits of the target distance from the opponent and thus discern the user's approximate geolocation [10].

Shetty, Grispos and Choo managed to use an exploit to perform man-in-the-middle attacks on popular dating apps showing that they are also vulnerable to network-based attacks.They forged a certificate which was installed once mobile devices were connected to the rogue network, this way, the authors managed to decrypt traffic between the user's device and the dating app server [11].

Mata., *et al*. also managed to find the geolocation of users of the Feeld application with the use of GPS trilateration. By changing locations with fake GPS, then extracting the database, and refreshing the application multiple times, they managed to gather enough information to locate the distance to other users [12]. By creating circles at the user's location with radius of the distance on a map at each of the GPS coordinates, one can easily locate that user's approximate location.

Device	Version	
Iphone X	IOS 13.5.1	
Tile mate	2.68.0	
Tile slim	2.68.0	

Table 1: Devices used.

Tools Used	Purpose
Paraben's E3	Logical extraction and analysis of data
MOBILEdit	Logical extraction and analysis of data
Autopsy	View and analyze extracted data
SQLite Viewer	View database contents
Hex Editor	View and parse memory processes
Google Earth	View and locate geo-coordinates

Table 2: Tools used.

Methodology

In this experiment, an Iphone X with IOS 13.5.1 was set up with the Tile app installed. Two Tile mates were used, one to track a bag and the other to track keys. The Tile mate has a 200 ft. Bluetooth range and user replaceable battery. One Tile slim was also used to keep track of a wallet. Those items have moved multiple times between the area of the Woodlands Texas and Hunstville Texas at multiple locations for a couple months.

Paraben's E3 Universal Electronic Evidence Examiner and MOBILEdit Forensic express were used to perform a logical acquisition of application data on the smartphone device. This software can perform logical, physical, chip bypass, cloud acquisition, and rooting as well as analysis capabilities for data parsing of Apps.

Once the application data has been extracted Autopsy was used to manually traverse and examine the found data. Multiple tools were used in order to view the data such as SQLite viewer to analyze the databases, Hex Editor to parse memory processes for the plaintext data and Google Earth to locate the found geolocations.

Results and Discussion

As previously mentioned, the iOS device used for this experiment is password unlocked and the investigator has to the password to access the unencrypted backup data. Unfortunately, the logical extraction performed with MOBILedit did not yield any interesting data such as geolocations, timestamps and/or item identifications, rather they collected information about the application itself rather than the data created and used by the application.

Paraben's E3 Electronic Evidence Examiner logical extraction did not collect a lot of files from the application either which we suspect Tile to store most of its data in a remote server rather than the device's disk. While the Tile application did not have a lot of information stored on disk, it does keep logs which are located inside the application data, more precisely it is located under the library folder and the log folder of the application data. The logs were compressed with gzip and could not be viewed directly from Paraben's software though. Once the compressed logs were extracted from Paraben's image, we could easily extract them with the used of 7zip. The contents looked to be disorganized and contained incomprehensible IDs, but the logs do harbor a lot of useful information such as timestamps and geolocations. While there aren't any information about what item is being tracked it could still give investigators a strong overview of where all the tracked items were and at what time which could prove very valuable in an investigation.

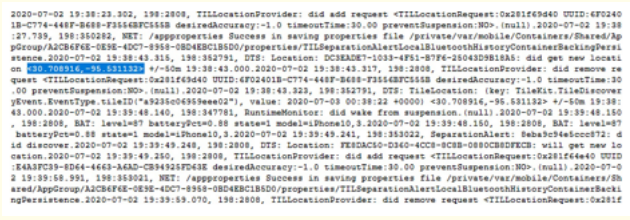

Figure 1: com.thetileapp.tile.log.

From here, Python3, with the help of regular expressions, was used to create a small snippet of code to parse all the geolocations found in the log files as well as their corresponding timestamps and write them to a file:

```
import re

pat = re.compile(r"(<\d*\.?\d*,-\d*\.?\d*>)")
out = open("coordinate", "w")

coordinates = []
with open('tile.log') as my_file:

  for line in my file:
    testre = pat.search(line)

  if(testre != None):
    date = line[0:23]
    coordinate = testre.group(1)
    longi = coordinate.split(",")[0][1:]
    lati = coordinate.split(",")[1][:-1]

    out.write(longi+", "+lati+", "+date+"\n")

out.close()
```

Listing 1: Coordinate parser.py.

The file is then parsed by another Python3 program which uses plotly and a Mapbox access token to view the results on a world base map. The resulted to plot all of the geolocations to create an html file of an interactive map which showcases the coordinates and timestamps (Listing 2).

The resulted html file can be opened on any web browser to view all of the geolocations on an interactive map with their corresponding timestamps. Figure 2 shows the results [13-21].

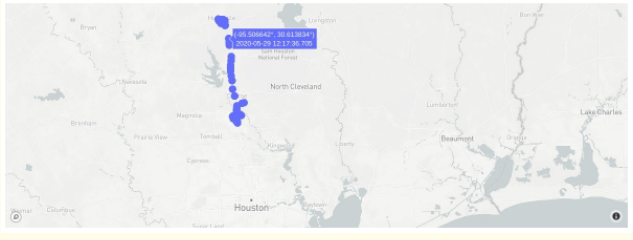

Figure 2: Tile location history.html.

```
import plotly
import chart studio.plotly as py
import plotly.tools as tls
import plotly.graph objects as go

coordinates = []
with open('coordinate') as my file:
     for line in my file:
        coordinates.append(line[:-1].split(','))

latitudes = []
 longitudes = []
 timestamps = []
for i in coordinates:


   longitudes.append(i[1])
   timestamps.append(i[2])

data = [

   go.Scattermapbox(
     lat=latitudes,
     lon=longitudes,
     mode='markers',
     marker=dict(size=15),
     text=timestamps,
   )
]


layout = go.Layout(
   autosize=True,
   hovermode='closest',
   mapbox=dict(
     accesstoken='****',
     center=dict(lat=38.92,lon=-94),
   ),
)

fname='LocationHistory.html'
fig = dict(data=data, layout=layout)
plotly.offline.plot(fig, filename=fname)
```

Listing 2: Location history.py.

Conclusion

Third-party software on the Apple Mobile platform provide large quantities of data that can provide a forensic analyst useful information. Users interacting with the app stores a lot of valuable data, usually in plain text which can be obtained from the User Data partition of the mobile device. Some applications still store data when not being used as they run background services such as Tile. The methods of obtaining the information are quick and straightforward but integrating them into different forensic systems for mobile devices will provide substantial benefits for both the forensic community and law enforcement.

We found that even if the Tile company stores most of its data in a cloud or server, there are still very valuable information that can be found within the logs. Data includes time-stamps and Geolocational references which can help to locate an item at a particular time in a region. Even if the data doesn't look organized, with the help of python we can easily clean the data and display it in a more readable format which can greatly help digital investigations.

Since the iOS device has to be unlocked and the investigator needs access to the unencrypted data, it may be a challenge for investigators, but nowadays, plenty of software offer the ability bypass the locking mechanism with the use of lockfiles, jailbreaking and/or performing different kinds of attacks on the back up encryption password.

Because the identification of each item is missing, it may present a problem for digital investigations as they can't be used to prove the location of a specific item at a specific time (unless the user only uses one tile). Furthermore, even if the user only has one tile that he/she is tracking, it still doesn't prove the location and time of the specific item, only the tile itself, which could have been moved purposely in order to fake an item's location. Even though, this research is not enough to prove the location and time of a specific item, it still provides a lot of information concerning the overall locations and times of all tiles (not tracked items). Which can be used to prove the overall location of the user. Another thing to take in account is the fact that Tile can also track the device (smartphone) used to track all tiles, meaning that among all these geolocations, the phone's location is included.

Bibliography

1. Levinson A., *et al.* "Third Party Application Forensics on Apple Mobile Devices". 44th Hawaii International Conference on System Sciences (2011).
2. Apple. (n.d.).
3. Find Your Keys, Wallet amp; Phone with Tile's App and Bluetooth Tracker Device (n.d.).
4. Mcmillan D., *et al.* "A hybrid mass participation approach to mobile software trials". Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems - CHI '12 (2012).
5. Husain MI., *et al.* "IForensics: Forensic Analysis of Instant Messaging on Smart Phones". *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Digital Forensics and Cyber Crime* (2010): 9-18.
6. N Al Mutawa., *et al.* "Forensic analysis of social networking applications on mobile devices". *Digital Investigation* 9 (2012): S24-S33.
7. A Mahajan., *et al.* "Forensic Analysis of Instant Messenger Applications on Android Devices". *International Journal of Computer Applications* 68.8 (2013): 0975-8887.
8. IU Akarawita., *et al.* "ANDROPHSY - forensic framework for Android". 2015 Fifteenth International Conference on Advances in ICT for Emerging Regions (ICTer), Colombo (2015): 250-258.
9. M Carmen and KK R Choo. "Tinder me softly – How safe are you really on Tinder?". in 12th EAI International Conference on Security and Privacy in Communication Networks (2016): 271-286.
10. NP Hoang., *et al.* "Your Neighbors Are My Spies: Location and other Privacy Concerns in Dating Apps". in The 18th IEEE International Conference on Advanced Communication Technology, Pyeongchang (2016).
11. R Shetty., *et al.* "Are You Dating Danger? An Interdisciplinary Approach to Evaluating the (In)Security of Android Dating Apps". *IEEE Transactions on Sustainable Computing* 99 (2017): 1-1.
12. Mata N., *et al.* "Are Your Neighbors Swingers or Kinksters? Feeld App Forensic Analysis". 2018 17th IEEE International Conference on trust, security and privacy in computing and Communications/12th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE) (2018).
13. H Chu., *et al.* "Digital evidence discovery of networked multimedia smart devices based on social networking activities". *Multimedia Tools and Applications* 71.1 (2014): 219-234.
14. "An Analysis of Smartphones Using Open Source Tools versus the". Marsheall University. Forensic Science Center, Huntington.
15. Husain MI., *et al.* "A simple cost-effective framework for iPhone forensic analysis". *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* 53 (2011): 27e37.
16. Anglano C. "Forensic analysis of whatsapp messenger on android smartphones". *Digital Investigation* (2014).
17. Digital forensic tools. (n.d.).
18. MOBILedit. (n.d.).
19. P Andriotis., *et al.* "Multilevel Visualization Using Enhanced Social Network Analysis with Smartphone Data". *International Journal of Digital Crime and Forensics* 5.4 (2013): 34-54.
20. Toyama K., *et al.* "Geographic location tags on digital images". In Proceedings of the Eleventh ACM international Conference on Multimedia (2003).

21. Ayers Richard. "Mobile Device Forensics - Tool Testing". *National Institute of Standards and Technology* (2009): 1-23.