Forensic Science International: Digital Investigation 44 (2023) 301478

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

Family locating sharing app forensics: Life360 as a case study

Posie Aagaard, Bijan Dinyarian, Omar Abduljabbar, Kim-Kwang Raymond Choo*

Department of Information Systems and Cyber Security the University of Texas at San Antonio, San Antonio, TX, 78249-0631, USA

ARTICLE INFO

Article history:
Received 6 December 2021
Received in revised form
20 October 2022
Accepted 24 October 2022
Available online xxx

Keywords:
Family locating sharing
Life360 app forensics
Mobile device forensics
Mobile app forensics

ABSTRACT

Smartphones and mobile applications (apps) are ubiquitous in societies worldwide, and one popular app category is family locating service (also referred to as family locator) apps. Such apps allow users to continuously share their location with others for reassurance that their immediate family, friends, or loved ones are safe, creating a virtual safety net. Some family locator apps support invitation-only family circles, which creates the expectation that users' personal data is shared only with trusted individuals. Focusing on Life360 (version 21.9.0), a popular family locator app, we demonstrate the extent and types of forensic artifacts and sensitive data that could be acquired using both commercial and open source tools from the use of the app on iOS and Android devices (iPhone 6S – iOS 13.1.3 and iOS 14.4.2, iPhone 7 – iOS 14.8, iPhone 12 Mini – iOS 14.8, TCL 10L – Android 11, and two Samsung Galaxy S7s – Android 8.0.0). For example, we demonstrate how one can readily acquire user personal data generated by Life360 through device logical file and network traffic forensics, and only one device would need to be compromised for all Circle users' personal data to be compromised.

1. Introduction

Family locator service applications (apps), including apps individuals use to track themselves or to track others ("other-tracking apps") (Gabriels, 2016), advertise a variety of "family safety" purposes. These apps are often paired with related services such as identity theft protection, SOS help alert, and proximity-based crime reporting. Family locator apps make use of the Global Positioning System (GPS), Wi-Fi networks, and local Bluetooth connections to precisely track user locations in a variety of connectivity scenarios (Alkhattabi et al., 2020). Each app offers a suite of related features, such as iSharing's two-way radio and Life360's ability to monitor and report driving data, including hard braking, phone usage, high speed, rapid acceleration, and the distances driven. Some family locator apps offer a geofencing option to notify app members when others in the family Circle enter or leave a common geographic area or have a low device battery (McFarland, 2019).

Family safety apps are marketed as tools for improved personal safety combined with "increased freedom to roam" (Simpson, 2014), yet there have been only a few studies on the effects of family safety apps on reducing violent crime (Maxwell et al., 2020). Caution about the security of personal data leakage is warranted: Two studies of family location-sharing applications recovered artifacts of personally identifiable information, such as profile photos and live and recorded personal GPS coordinates, as well as presumed-private messages between members and other sensitive data (Alkhattabi et al., 2020; Bays and Karabiyik, 2019).

Life360 is reportedly the "#1 family safety membership" with "25 million members and counting", which shares private location data only with designated trusted individuals in a unique "Circle." The app was created in the wake of Hurricane Katrina to locate and help loved ones in need. Life360 offers free user accounts with basic location tracking services or premium paid accounts with additional services and extended available data tracking. Life360 account setup only requires a phone number, email address, and first and last name. A user can create a custom Circle and invite specific individuals or join one or more existing Circles. The user who sets up the Circle is considered to be the administrator who designates which data points are tracked (e.g., location tracking, speed monitoring, or other features).[1] Hasinoff (2017) is critical of Life 360, asserting that it "collects, repackages, and commodifies [users'] personal information." Life360's privacy policy stipulates that the company is free to share and sell its users' data, with few

* Corresponding author.
E-mail addresses: posie.aagaard@utsa.edu (P. Aagaard), bijan.dinyarian@my.utsa.edu (B. Dinyarian), omar.abduljabbar@my.utsa.edu (O. Abduljabbar), raymond.choo@fulbrightmail.org (K.-K.R. Choo).

[1] Life360b. Family safety membership. September 10, 2021. www.life360.com

https://doi.org/10.1016/j.fsidi.2022.301478
2666-2817/

exceptions or opportunities to opt out.[2] Data analytics company Arity, which buys Life360 data, sells its analyses to insurance companies that use the data to calculate insurance prices[2] (Burmeister et al., 2021).

We chose to investigate Life360 because of its growing popularity and reputation in a category of applications marketed as tools to improve personal or family safety (Maxwell et al., 2020). Family locator apps' functionality to distribute data to trusted Circle members may place unwitting users at risk for breached personal or sensitive information confidentiality. A literature review on family locating apps reveals a shortage of forensic analysis studies on the topic. Other related non-forensic research articles describe privacy concerns for family locator apps, particularly given the personal and sensitive data "trusted" and shared in group circles (Gabriels, 2016; Harkin et al., 2020; Hasinoff, 2017; Maxwell et al., 2020).

In this paper, we conduct a forensic analysis of Life360's activities on both Android and iOS devices using paid, trial-version, or free forensic tools (i.e., MOBILedit Forensics Express, Fiddler Everywhere, OSForensics, 010 HexEditor, FTK Imager, Android Studio, and Realm Browser). Our findings describe the types and extent of sensitive data artifacts from all Life360 Circle members' devices that can be recovered from a single Circle member's device.

In the next section, we will briefly review the extant literature on mobile application forensics, and more specifically family locator application forensics.

2. Extant literature

Smartphones generate and store a multitude of data points about individuals.[3] Alkhattabi et al. (2020) reported that some Android apps that store sensitive information could potentially leak data, including location-sharing apps. Yellanki (2020) found that Android apps with access to sensitive data may remain unprotected by standard Android permissions. Geo-location data derived from the Global Positioning System (GPS) on a smart device may offer forensic value in judicial processes (Sansurooah and Keane, 2015). Concerns that law enforcement can access Life360 data and use it against individuals without their knowledge became real in 2020 when police officers convinced a child to use his father's location history data to arrest the father on charges of arson.[4]

2.1. Family locator app psychology

Technology extension theories posit that technologies are objects that magnify or extend humans' physical or mental abilities (Brey, 2000; McGuire 2012). Technologies can provide humans with the capability to cause harm against others that they would otherwise be incapable of perpetrating (Wood, 2021). Safety apps often market to women as feared victims of public stranger violence (PSV), advertising an alternative for restricting their lifestyles or developing avoidance behaviors because of fear of crime (FOC). Some locator apps are marketed exclusively to women. Apps like India-based Whatsapp aim to provide women with emergency tools to report potential crimes to police using simple, unobtrusive smart device gestures (Chand et al., 2015). However, Hasinoff (2017) argued that location-based zones of safety in apps like Life360 can create a questionable impression that known spaces are "safe" and unknown spaces are "unsafe." Hasinoff (2017) quips, "Life360 might be better understood as an app that continuously creates and resolves anxiety" and like Sansurooah and Keane (2015) pointed out that constant surveillance can be especially damaging in situations that involve an imbalance of power, such as domestic violence. User reports of inaccurate or lagging location data have included complaints that the app's inaccuracies can exacerbate interpersonal dynamics involving jealous spouses or overprotective parents (Hasinoff, 2017).

2.2. Child safety using family locator apps

Safety apps also advertise the ability to track young children as part of a family safety membership. Such apps have been touted as a positive solution for parents to maintain constant surveillance of their children and are no longer viewed as a tool used only by abusive or strict parents (Marciano et al., 2021). However, (Gabriels, n.d.) questions whether constant parental tracking creates a false sense of security or creates an environment in which parents are too involved in their children's decisions. This is labeled as "over-proximity," or "over-involvement that might thwart [children's] self-development" by parents who "might mistake control for care" (Gabriels, n.d.). Another critique is that children could over-rely on apps and fail to learn self-responsibility and safety coping skills (Simpson, 2014). Additionally, parents' use of apps to track their children could reinforce existing negative parenting styles (Gabriels, 2016).

Apple devices now push real-time notifications to users that apps are using their location data, which can result in multiple Life360 user notifications that their location data is being shared.[5] Minors have expressed frustration with and disapproval of personal tracking apps. Through memes, teens have vocalized their concerns on social media giant TikTok that parents who use Life360 do not trust their children. The teens also share a multitude of tips for evading Life360's location tracking features (Meisenzahl, 2019; Marciano et al., 2021). While Life360 acknowledges federal protections afforded to children under the age of 13 by the Child Online Privacy Protection Act (COPPA) of 2000, the app does not require a child's age to be entered upon account activation, thereby undermining the age limit. Life360 lacks some basic account security safety features, such as alerts when a new parent account is being used on a new device or when parental account passwords are changed (Mannan et al., 2020).

Digital databases of registered sex offenders and related crimes have been commonly used to produce publicly available online maps and apps over the last two decades. Life360 integrates sex offender and criminal activity data into the app, allowing users to examine any crime reports that occurred in the last 30 days near each member within the Circle. Hasinoff (2017) argues that crimes that occur in the past do not constitute a present threat, and most sex offenders do not reoffend. Further, she notes that most sex offender crimes are perpetrated by family members or close acquaintances — potentially the same individuals with unrestricted access to children's detailed location data (Hasinoff, 2017).

2.3. One step removed? Spy apps

There seems to be no shortage of illicit apps designed to spy on

[2] Life360a. Life360 Privacy Policy. 2021. https://support.life360.com/hc/en-us/articles/360043228154-Full-Privacy-Policy

[3] Brewster, T. Life360 Comes at You Fast—Cops Convince Arson Suspect's Kid to Give Up Dad's Location on Family Tracking App. Forbes, February 12, 2020. forbes.com/sites/thomasbrewster/2020/02/12/life360-comes-at-you-fast–cops-use-family-surveillance-app-to-trace-arson-suspect

[4] Anonymous. Phone Update Reminds Users – Again and Again – of Being Tracked, Dow Jones Institutional News, 2019. https://www-proquest-com/wire-feeds/iphone-update-reminds-users-again-being-tracked/docview/2331548355/se-2?accountid=7122

[5] Life360 app version 21.9.0

others. Some locating applications offer tracking capabilities similar to Life360 but are designed for deceptive purposes and are hence classified as “spy apps.” Spy apps enable an unauthorized individual to capture sensitive information from or about another person. Such apps can be difficult to detect because they rely on standard services to stash the data they steal, avoid alarming actions such as privilege escalation typically associated with malware, and are designed to act like a legitimate app. Government entities and law enforcement have historically been consumers of malware designed to spy on citizens, but there is growing commercial availability of spy apps packaged as security apps (Harkin et al., 2020).

HelloSpy is an app surreptitiously installed by an individual to secretly and illegally monitor another user's text messages, GPS location, call details, photos, and social media activity on a user's device. Many intimate details of a person's life can potentially be gleaned from this data. No app icon appears on the user's mobile device, leaving the user unwittingly vulnerable for uninvited guest access to the user's personal life (Sansurooah and Keane, 2015). HelloSpy's marketing includes a photo of a male physically assaulting a female with a caption urging the importance of tracking a spouse (Chatterjee et al., 2018). 1TopSpy goes a step further, collecting a user's contacts and photo, web, and app usage history. The app also reports all live and recorded GPS locations to unauthorized individuals (Gabriels, n.d.).

Spy app SpyIC claims to be the most downloaded surreptitious location app in the world, yet there have been no forensic analyses of SpyIC reported in the scientific literature. Even legitimate apps can serve as nefarious “dual-use apps” when repurposed for use as “intimate partner surveillance” (IPS). Some of these apps which are self-labeled as legitimate deliberately masquerade as benevolent products while simultaneously displaying advertisements for IPS (Chatterjee et al., 2018). A thorough literature search did not reveal any forensic studies of specific spy apps. This may be because Google and Apple both proactively identify and remove obvious spy apps from their app stores. A spy app may be available one day and no longer available the next day (Chatterjee et al., 2018).

2.4. Relevant family locator app studies

Although several family locator apps have been studied in the context of crime prevention for subscribing individuals (Maxwell et al., 2020), results of only two forensic studies on family locator apps have been published. Bays and Karabiyik (2019) conducted a high-level forensic analysis and comparison of two family locator apps: iSharing and Life360. The study used a limited number of devices (two iOS devices and one Android device). One of the iOS devices was jailbroken, and the Android device was rooted and unrooted to analyze the different results of artifacts recovered. The study analyzed only the applications' free services and did not include forensic analysis of network traffic. Its purpose was to discover forensic artifacts from Life360 and iSharing on connected iOS and Android devices that tracked location data for 72 hours.

Table 1 lists artifacts recovered from Bays and Karabiyik (2019)'s Life360/iSharing forensic analysis for each device by locator application. Bays and Karabiyik (2019) followed the NIST Guidelines on Mobile Device Forensics (*Special Publication* 800−101) (Ayers et al., 2018) and restored all devices to factory settings prior to conducting the forensic analysis. Next, they installed the latest version of each third-party tracking locator application (iSharing and Life360) and performed a baseline forensic analysis on each of the three devices. Thereafter, they collected data including tracking location and internal messages on each device for 72 hours. Then, utilizing the tools Cellebrite UFED 4PC 7.5.0.845 and Magnet AXIOM 2.6.0.11689, they ran another forensic analysis to examine the results, which revealed multiple recovered artifacts. The authors assert that the recovered artifacts, including location data of individuals and the contacts in their sharing “Circles,” could help law enforcement during investigations (Bays and Karabiyik, 2019).

The Bays and Karabiyik (2019)'s study shows that the Life360 app on an Android (unrooted) device appears to be somehow safeguarded from forensic analysis, yielding only the user's profile image, whereas the artifacts recovered on the Android (rooted) device include messages exchanged and associated coordinates within the user's Circle. Artifacts recovered for the non-jailbroken iOS devices using Life360 included contact lists, user GPS coordinates, and remembered locations. iSharing, on the other hand, yielded artifacts such as contact list and contact GPS coordinates. The jailbroken iOS device contained iSharing artifacts like user password, user phone number, and user home address. The Android (unrooted) device included artifacts containing iSharing user email, contact lists, contact GPS coordinates, and user GPS coordinates.

Alkhattabi et al. (2020) conducted a forensic investigation of 41 different Android family locator apps from the Google Play store to evaluate the apps from security and privacy perspectives. The study focused exclusively on Android apps and used only two Android mobile devices running Oreo to conduct the investigation. Apps were chosen based on the highest number of Google Play store downloads. While some of the apps had only 100 downloads, most had more than 100,000 downloads, and five apps had more than 1,000,000. Life360 was the most downloaded family locator app, with 50, 000, 000 downloads. The study's findings are presented as percentages, with no details to identify which family locator app has specific security and privacy weaknesses through data leakage. Additionally, the study only analyzed free family locator app services.

Most family locator apps request access to the user's location, storage, and contact information. Alkhattabi et al. (2020) conducted an app permission extraction to identify the most sensitive permissions requested by each family locator app, which would determine what kind of information, if any, had been leaked. Network traffic analysis was performed to capture all traffic on each device to identify if any sensitive information was leaked through the user-server Hypertext Transfer Protocol (HTTP) request. Local storage analysis was used to collect all data entered by users, as well as the permissions that they acknowledged, to determine what kind of data was being saved and whether there were any security privacy concerns.

Alkhattabi et al. (2020) granted all required permissions, created an account for each family locator app, created a private Circle, invited other users to the Circle, and sent text messages within the app. Each family locator app ran for 20 minutes on the smartphone before being deleted and replaced with the next family locator app, and so on. After the initial setup was completed, Alkhattabi et al. (2020) utilized a stress-testing tool called Exerciser Monkey to send about 500 random action events on each family locator app. They used the *tcpdump* tool and the reverse engineering tool *apktool* to extract all URLs from each family locator app to capture all traffic that should be encrypted. Alkhattabi et al. (2020) suspected that some information might not be encrypted, resulting in red flags for those specific family locator apps.

Alkhattabi et al. (2020) found that 33 (80.4%) of the 41 family locator apps did not safeguard users' sensitive information via network traffic or in local storage. 24 of the 33 susceptible apps (72.7%) exposed users' location data via HTTP requests and local storage. 9 apps (27.3%) disclosed family group codes through network traffic and in local storage, which could be recovered by malicious actors and exploited for unintended purposes. 3 apps (9.0%) were discovered to use the SD card to store voice chats and

Table 1
Artifacts Recovered from Bays and Karabiyik (2019) iSharing and Life360 Forensic Analysis.

iSharing		Life360		
iOS	Android	iOS	(rooted) Android	(unrooted) Android
Contact lists	Contact lists	Contact lists	Messages, associated coordinates	User's profile pictures (SD card)
User information (password, phone number, address)	User information (email address)	User GPS coordinates	Users' profile pictures	–
Contact GPS coordinates	User and contact GPS coordinates	Remembered locations	–	–

Table 2
Test devices.

Device	Model	OS Version
iPhone 7	NN9G2LL/A	iOS 14.8
TCL 10L	T770B	Android 11
iPhone 6S	MKRR2LL/A	iOS 13.1.3
iPhone 6S	MKRP2LL/A	iOS 14.4.2
iPhone 12 Mini	MG8B3LL/A	iOS 14.8
Samsung Galaxy S7	SM-G930P	Android 8.0.0
Samsung Galaxy S7 (rooted)	SM-G930F	Android 8.0.0

group members' information, allowing other apps that use the SD card for storage to access that information as well. 4 apps (12.1%) disclosed user credential information such as username and password. 14 apps (42.4%) leaked text messages exchanged between group members. 13 apps (39.4%) leaked group members' email address, phone number, full name, and location data. In addition to these results, 5 (15.1%) family locator apps exposed sensitive information from their servers due to the lack of authentication or authorization.

Fig. 1 shows the most commonly recovered types of artifacts from the Alkhattabi et al. (2020)'s forensic analysis.

Aside from the small number of devices used in the study of Alkhattabi et al. (2020) and its exclusive focus on Android apps, the study is also limited by its analysis only of family locator apps' free services. Alkhattabi et al. (2020) expressed concern that if family locator apps' premium services were forensically analyzed, they would locate additional forensic artifacts created by access to dangerous Android permissions.

Because only two forensic analyses of family locator apps have been published (Bays and Karabiyik (2019); Alkhattabi et al. (2020)), we reviewed other similar categories of mobile apps that have been studied for the potential to leak sensitive data. Keegan and Ng (2021) conducted a forensic analysis of dating app *Happn* using four Android and four iOS mobile devices with their respective phone numbers to create eight profiles that were then split into four pairs of two. The groups interacted with different activities with multiple sessions by sending messages and rejecting profiles. The study targeted network traffic between devices and the *Happn* server using several tools that determined compatibility with the device's OS they were targeting. They used *Fiddler* as a proxy to target iOS devices and Android packet sniffer app (*Packet Capture*). The network traffic was encrypted; therefore, several steps were taken to decrypt it.

Table 3
Outlines our research workflow.

Research Workflow
Wiped and restored devices to factory settings
Configured devices using empty iCloud and Gmail accounts
Installed latest version of Life360 (21.9.0)
Created 7 Life360 personas and Life360 Circle groups
Purchased Gold (premium) membership of Life360
Interacted with Life360 to populate devices with data
Allowed each device to track locations for 168 hours (1 week)
Performed a logical acquisition with MOBILedit
Captured network traffic using Fiddler

The study also targeted logical data. Knox et al. (2020) used MOBILedit Forensic Express to acquire data from iOS and Android devices. They also used iTunes backups after each session to analyze the application's property lists (plist) and SQL databases. For Android, they used images from the MEmu emulator, and they used Autopsy and FTK Imager to analyze the images. Similar to the studies of Alkhattabi et al. (2020) and Bays and Karabiyik (2019), forensic artifacts discovered include a sizable list of data points, including detailed information about the user's device, presumed-private messages, and map location data.

Several artifacts were located from the Android devices in the captured traffic, including text-based messages, profile information, audio messages, and profile pictures. To discover physical image artifacts, the study utilized MiXplorer to analyze the root file directory accessed. Information was pulled out from both *Happn* and Packet Capture, including age, profile biography, gender, whether the user sent a like, and URLs that link to pictures of the user. All this data would allow someone to easily build a profile on a user or track them down.

On iOS devices, network traffic was roved during the sign-up process, and two packets were found as a result of that process. The more alarming was the captured packet containing the access token for the user and his/her associated user ID, all in plain text. The access token value never changed for each session. As it is used to authorize access and then as a credential for Auth0, an attacker could exploit the token to access the target's account.

Once the iPhone was jailbroken, some additional artifacts were found. An interesting one relates to Hdata.db. After the last session, the account was "paused" to see if artifacts could still be retrieved. Afterward, the database appeared empty and only began storing data when the account was logged back on and activity was conducted.

Knox et al. (2020) study's limitations were related to changes made after the *Happn* app version was updated. The iOS devices could only associate a phone number with one account. If the number was previously in use, *Happn* used it for the newly created account. It was not an issue prior to the update. The second limitation was that when the profiles were paused, *Happn* did not store the data in its database. Regarding Android devices, one limitation is that the same phone number can be used for multiple *Happn* accounts, which may be considered an authentication hole. In addition, MOBILedit did not add any new findings to those discovered using other tools on both Android and iOS devices.

3. Experiment setup and findings

Limitations of the studies of Bays and Karabiyik (2019) and

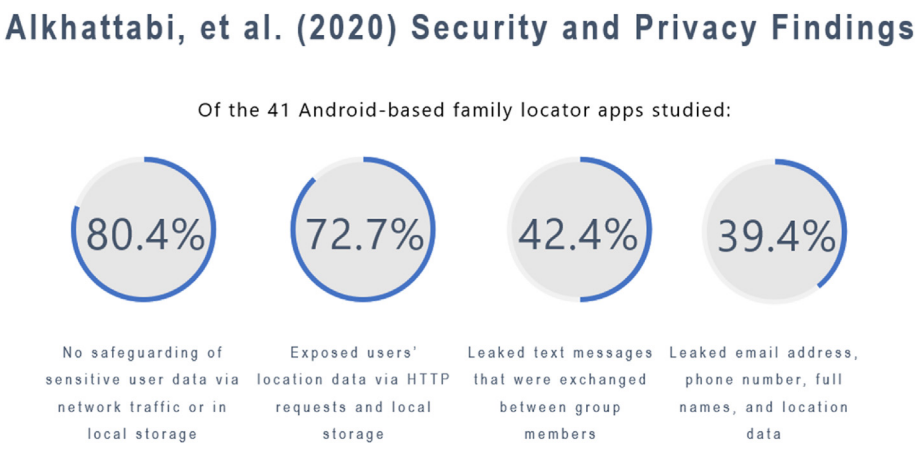


Fig. 1. Android family locator app weaknesses: top percentages.

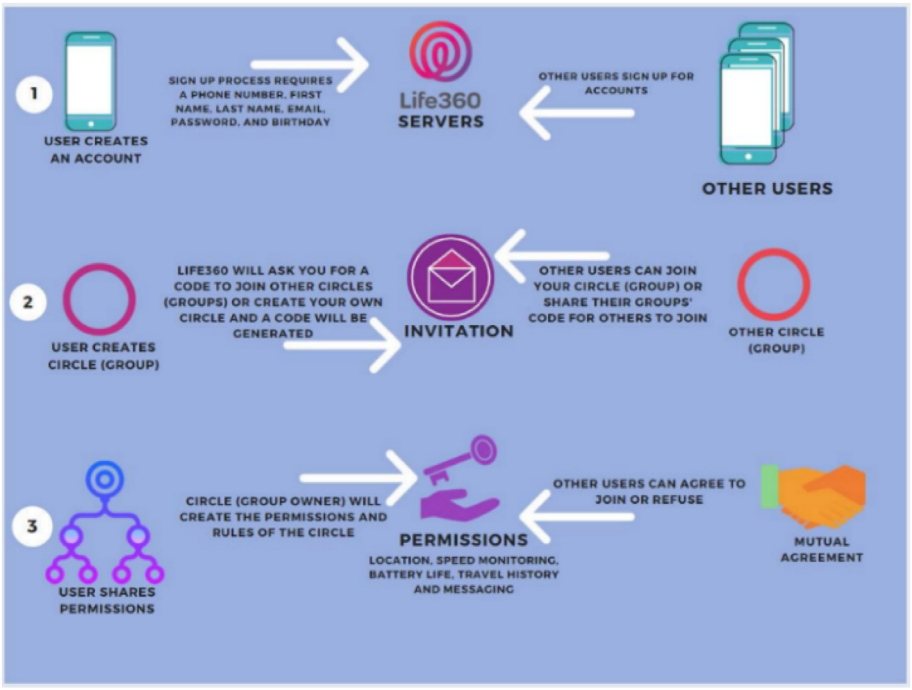


Fig. 2. Life360 Account Setup (information sourced from Life360.com).

Alkhattabi et al. (2020) provide a springboard for a new family locator app forensic analysis. Rather than limit forensic analysis to only two or three devices as these studies did, our study is expanded to include both Android and iOS devices with older and newer device OSes. We designed our experiment with multiple iOS devices on a variety of iOS versions to confirm or refute any differences in the amount of data that can be forensically recovered or captured based on differences in phone model or iOS version. We included two different Android models, as well as a pair of Android devices with the same base model running the same Android OS, one of which was rooted and the other which was not rooted, to identify any variations in forensic findings. Our study also investigates Life360's premium features.

Following NIST's Guidelines on Mobile Device Forensics (*Special Publication 800–101, Revision 1*) (Ayers et al., 2014), we identify and analyze data generated from a premium Life360 membership, including extended-history personal location data sharing and individual driving data. The study's goal is to collect all forensic artifacts from Life360 to determine whether certain information users do not want publicly disclosed could be unknowingly and intentionally or unintentionally forensically discovered.

Although the study of Bays and Karabiyik (2019) did not include analysis of network traffic, Alkhattabi et al. (2020)'s study of Android locator apps' security and privacy stresses the crucial role of network traffic for family locator apps, as data must be transmitted in a constant stream between client devices and remote servers. Transmissions must be encrypted as one step toward protecting the integrity and confidentiality of the data. Following in the footsteps of Alkhattabi et al. (2020), our study includes network traffic analysis. Rather than creating a surface-level analysis comparing only a few features of two family locator apps or restricting the forensic analysis only to two devices on the Android platform, we took a closer forensic look specifically at Life360's basic and premium features on both iOS and Android devices.

In late 2021, Life360 defended its user data selling practices and declined to identify how many or which privacy data partners the company uses. As one of Life360's "approximately a dozen data partners," data broker Cuebiq denies selling user location and other private data to law enforcement agencies (Keegan and Ng, 2021; Priest, 2021). Life360 offers an Emergency Data Access option authorizing the company to provide law enforcement with "information that could help locate [a] missing person."[6] A secondary goal of our study is to consider how forensic artifacts from Life360 may be advantageous from a criminal justice perspective. For example, in a child kidnapping case, how useful would Circle-shared data from a single device be for law enforcement? Our study shows that data for multiple users could be forensically recovered from a single device, or captured traffic from one device could reveal the location history of each identified user in each Circle with which a device has interacted.

3.1. Device and Life360 account setup

Our study's seven devices include two iPhone 6Ses on iOS 13.1.3 and 14.4.2, respectively, an iPhone 7 on iOS 14.8, an iPhone 12 mini on iOS 14.8, an unrooted Samsung Galaxy S7 on Android 8.0.0, a rooted Samsung Galaxy S7 on Android 8.0.0, and a TCL 10L on Android 11 (see Table 2), which were wiped and restored to factory settings as specified in NIST 800−101 (Ayers et al., 2014).

Table 4 outlines our research workflow. We created a total of seven new iCloud or Google email accounts configured for each device, installed Life360 version 21.9.0, and created seven fictitious personas. We followed these steps to create individual Life360 accounts (see Fig. 2): 1) Provided name and phone number, email address, password, and date of birth. 2) Added a profile picture. 3) Created four Life360 Circles and set identical permissions to allow precise location sharing, speed monitoring, and access to battery life, travel history ("Drive Detection"), Emergency Data Access, and messaging access. 4) Sent a Circle join code (valid for two days) to two other devices in the test group. 5) Accepted Circle invitation. 6) Created check-in locations.

To confirm which data from the app would generate artifacts, the study design required accounts to allow *least restrictive* device permissions. Unlike other applications which are not in the family locator category, Life360's core locating and alerting service functionality is wholly dependent upon those permissions. Based on Andriotis and Takasu (2020)'s research on user preferences and behaviors related to device permissions, the permissions used in our study would be categorized as user Profile number 2 or 5, which are "generally permissive." Life360 does allow individuals to opt out of individual permission sharing (e.g., precise location tracking) but requires users to allow location tracking for the application to function. If a user chooses not to authorize Life360 to use a particular device permission, the app displays contextual messages to prompt the user to allow access. For certain types of accounts, other users in a Circle are notified when a user disables permissions.

Life360 account setup does not require email verification or any form of two-factor authentication. No verification was required to create an account for a 14-year-old. Creating an account for a 13-year-old would have required submitting a parent's driver's license. However, it is unclear how Life360 might verify a parent's and child's identity based on a driver's license photo. Because of potential ethical and legal issues, we did not create a 13-year-old account and submit a "parent's" driver's license.

We purchased a Life360 Gold (premium) membership for each group Circle and began generating data for each device while allowing location tracking for 168 hours, or one week. After that, we used MOBILedit for logical acquisition and *Fiddler Everywhere* to capture Life360 network traffic. Table 3 lists tools used in the study.

The three workstations used to extract forensic artifacts were: 1) Cyber Power running Windows 10 Pro 64-bit build with 32GB of RAM with an Intel Core i7-6850 CPU; 2) HP 360 Spectre Windows 10 64-bit 16GB Intel Core i7-7500 CPU; and 3) Dell OptiPlex 5040 Windows 10 Pro 64-bit Intel Core 8GB i5-6500 CPU.

3.2. Logical file analysis: methodology

We used the commercial mobile forensics acquisition and analysis tool MOBILedit Forensic Express PRO v. 7.4.1.21502 to extract logical images from the three Android and four iOS mobile devices. For the initial file acquisition, all devices were unlocked using the device passcode and connected to Windows machines as "trusted devices." None of the iOS devices were jailbroken. We rooted one Samsung Galaxy S7 (Android) device. We chose MOBILedit's Application Analysis option[7] and selected Life360 as the application to analyze.

We created MOBILedit backups and iTunes backups for iPhone devices, which provided access to proprietary-format property list (.plist) files (Hoog and Strzempka, 2011). MOBILedit created a temporary iTunes backup password during the data retrieval process. The Android devices had to be placed into Debug mode prior to connecting to MOBILedit and then had to allow access to MOBILedit's Forensic Connector. For the unrooted Android devices, MOBILedit flashed a warning that unrooted devices would only provide limited forensic results. We selected MOBILedit's option to create an Android backup file (.ab) in the hopes of locating additional artifacts. We inserted an SD card into the rooted Android device to determine whether the app created artifacts on the device's external storage.

3.3. Logical file analysis: summary findings

3.3.1. iOS devices: logical file analysis artifact locations

As detailed in Tables 5 and 6a, the MOBILedit analysis revealed several informative data artifact sources for iPhone devices. The *com.life360.safetymap.plist* file includes plaintext information about the individual user, including name, phone number, email address, timestamps, and detailed address and GPS location data. The *messaging.sqlite* database from MOBILedit's iTunes backup provided the most information, with detailed personal information not only for the individual whose phone was analyzed, but also for each other member of the Life360 Circle. Data points in *messaging.sqlite* include first and last name; phone number; email address; detailed GPS location data, including alphanumeric physical addresses, place names, and latitude/longitude GPS coordinates of location "check-ins" and Life360 auto-recorded locations. In addition to the plaintext messages between Circle members the study of Bays and Karabiyik (2019) discovered, we also found message receipt/read/deletion statuses; Circle creation date, ID, and name(s); member ID; member Circle admin status; device battery % charged; in-transit status and time spent in transit; Wi-Fi connection status; and avatar (profile photo) URL.

Examples of iPhone findings are shown in Figs. 3−6 below (see Fig. 7).

[6] MOBILedit Forensic Express user guide, 2021. https://forensic.manuals.mobiledit.com/MM/index.html

[7] Kamen Velikov. How To: Capture iOS Traffic with Fiddler. January 21, 2019. https://www.telerik.com/blogs/how-to-capture-ios-traffic-with-fiddler

Table 4
Lists the tools used in the study.

Tools Used		
Tool	Version	Purpose
MOBILedit Forensics Express	7.4.1.21502	Logical acquisition and analysis
Fiddler Everywhere	2.2.0	Network traffic capture and analysis for iOS/Android devices
Charles Proxy	4.6.3	Network traffic capture and analysis for Android devices
Packet Capture	1.7.2	Network traffic capture and analysis for Android devices
OSForensics	9.0.1002	Plist viewer and SQLite DB Browser
010 HexEditor	12.0.1	File viewer (no extensions)
FTK Imager	4.5.0.3	File viewer
Android Studio	2020.3.1	File viewer (.apk and.xml)
Realm Browser	3.0.1	Realm file viewer

Table 5
Details artifacts extracted from each iOS or Android device using MOBILedit.

Summary of Findings						
Logical Analysis Using MOBILedit						
Artifact Type	iPhone 6S, iOS 13.1.3 iPhone 6S, iOS 14.4.2	iPhone 7, iOS 8	iPhone 12 mini, iOS 14.8	TCL 10L, Android 11 (*unrooted*)	SSG S7, Android 8.0.0 (*unrooted*)	SSG S7, Android 8.0.0 (*rooted*)
Name	☑	☑	☑			☑
Phone number	☑	☑	☑			☑
Email address	☑	☑	☑			☑
Timestamps	☑	☑	☑	☑	☑	☑
Avatar (profile photo) URL/image	☑	☑	☑			☑
User GPS coordinates & amount of time spent in location	☑	☑	☑			☑
Contact GPS coordinates & time spent in location	☑	☑	☑			☑
Plaintext messages with read, receipt, and deletion status	☑	☑	☑			☑
User images	☑	☑	☑			☑
Circle names, creation dates, and IDs	☑	☑	☑			☑
Full info of other users in Circle	☑	☑	☑			☑
Check-in location name, GPS coordinates, and address	☑	☑	☑			☑
Recorded location, name, GPS coordinates, & address	☑	☑	☑			☑
Driving data (Arity descriptors)	☑	☑	☑			☑
User in-transit status; transit start/end times, speed	☑	☑	☑			
Device permissions requested by app/ granted				☑	☑	☑
Device metadata	☑	☑	☑			☑
Application usage information				☑	☑	☑
Wi-Fi connectivity indicator	☑	☑	☑			☑
Battery status indicator	☑	☑	☑			☑
Names of app's privacy partners (128)						☑

3.3.2. *Android Devices: logical file analysis findings*

Consistent with the study of Bays and Karabiyik (2019), Android data artifacts from the MOBILedit logical file analysis were less plentiful for the unrooted devices and included Life360 application download and last application date timestamps, a listing of device permissions enabled in Life360 (e.g., location sharing and physical movement detection), and encrypted or encoded driving logs. Upon connecting the unrooted Android devices to a laptop or PC, we could view partial file the |*data* folder structure for Life360. Consistent with Lwin et al. (2020), we could not view any files in the |*data* folder of the unrooted devices. As evidenced in the Life360 v. 21.9.0 APK's *Manifest.xml* file, the app does not allow backups to be created.

As detailed in Table 6b and Figs. 8–12 below, the rooted Samsung Galaxy S7 included artifacts very similar to artifacts discovered on the iPhone devices. Compared to the studies of Bays and Karabiyik (2019) and Alkhattabi et al. (2020), our study's results from the rooted Android device are much expanded. Our results also confirm Bays and Karabiyik (2019)'s concern that artifacts from Life360's premium features can be recovered from a rooted Android device.

The L*360LocalStoreRoomDatabase* file contains name; phone number; email address; avatar photo; Circle ID; Member ID; Circle admin status; emergency contact's name, email, phone number, avatar, Circle ID, and URL; precise GPS coordinates, physical address, check-in location name, Wi-Fi connection state, location sharing status (binary on or off), reason for lost Wi-Fi connection, battery charge status, in-transit status, and start/end time of travel. This file also includes what Life360 labels as user privacy settings for premium services, including Dark Web protection status (binary on or off), detailed breach indicator, identity protection status, Emergency Data Access, personalized ads, driving services, and

ZEMAIL	ZFIRSTNAME	ZLASTNAME	ZMEMBERID	ZPHONE
juhan.dough@gmail.com	Juhan	Dough	a46c667a-75f0-...	+18304611753
ElizTundry@protonmail.com	Elizabeth	Tundry	967062d7-44ce-...	+16292500935
osimkindf@gmail.com	Oscar	Simkindf	e62cab33-857e-...	+13362234721
juhan.dough@gmail.com	Juhan	Dough	a46c667a-75f0-...	+18304611753
osimkindf@gmail.com	Oscar	Simkindf	e62cab33-857e-...	+13362234721
omar.s.aj@protonmail.com	iOS	AJ	fc056af7-9a0e-4...	+12109935680

Fig. 3. Logical File iOS Findings Sample: **Messaging.sqlite**

Z_PK	Z_ENT	Z_OPT	ZCREATEDAT	ZCIRCLEID	ZNAME
2	1	875	653877565	ae40443d-17cb-...	DF Proj
3	1	819	656278248	062a2e4b-36cf-...	SimkinDF Family
4	1	808	656298687	2cb4bf4b-a6d8-...	Mandatory Fun

Fig. 4. Logical File iOS Findings Sample: **Messaging.sqlite**

ZDIRECTOBJECT	ZMESSAGEID	ZMESSAGETEXT
Starbucks	6d6af4e7-98d9-...	Checked in @ Starbucks
Starbucks	68acbc52-daf1-...	Checked in @ Starbucks
Starbucks	6b7f31b3-df54-4...	Checked in @ Starbucks
	26141d29-da88-...	Elizabeth, did you stick to your no-caffeine diet at Starbucks??
	45c3c14e-5faf-4...	Sadly no, I couldnât resist the caffeine ð¬
H-E-B plus!	79c58ccc-4edc-...	Checked in @ H-E-B plus!
H-E-B plus!	be57d8c6-113b-...	Checked in @ H-E-B plus!
H-E-B plus!	6b4f1682-a15b-...	Checked in @ H-E-B plus!
	48e38298-2c88-...	I am at the grocery store too!
	d1b179b5-989f-...	HEB - here everything is better

Fig. 5. Logical File iOS Findings Sample: Check-In Locations and Plaintext Messages in **Messaging.sqlite**

kL360UserDefaultsStorememberInfo	Dictionary	(7 items)
emailID	String	juhan.dough@gmail.com
is_optimus_prime	String	true
member_count	Number (Integer)	18
circle_count	Number (Integer)	3
is_admin	String	true
place_count	Number (Integer)	7
first_name	String	Juhan

Fig. 6. Logical File iOS Findings Sample: Email Address, Member Count of All Circles Associated with User, Count of User Membership in Circles, Circle Admin Status, Location Count, First Name in **safetymap.plist**

```
<application
    android:theme="@ref/0x7f130009"
    android:label="@ref/0x7f120630"
    android:icon="@ref/0x7f0f0000"
    android:name="com.life360.android.shared.Life360BaseApplication"
    android:process="@ref/0x7f120823"
    android:description="@ref/0x7f120630"
    android:allowBackup="false"
```

Fig. 7. *Life360 v. 20.9.1's* ***Manifest.xml*** *file from the APK: no backup.*

digital safety statuses (binary on or off).

Consistent with the iPhones' findings, the *Messaging.db* file included all users' messages (including timestamp, send/fail, read, received, or deleted status), detailed location and check-in GPS coordinates and addresses, photos sent by users, and participant first name. The *|data* directory included images of user GPS locations on a map. The *com.life360.android.safetymapd_preferences.xml* file includes an AES key. *Usagestats.log* and *meminfo.log* include individual device in-memory daily stats (all apps/packages, last date and duration used, app events log, total elapsed time and total device screen time) and individual device applications' memory usage.

We inserted an SD card into the rooted Android device but did not discover Life360 user profile photos in the SD card's *|data|com.life360.android.safetymapd* folder for the Life360 app version 21.9.0, as the study of Bays and Karabiyik (2019) did for the "latest version" (unidentified) Life360 app version in their 2019 study.

3.4. Network traffic analysis: methodology (iOS and Android Devices)

To observe and examine network traffic between a mobile device and Life360 servers, we simulated a Man-in-the-Middle (MITM) attack to intercept traffic. We analyzed network traffic generated by Life360 to understand what types of information can be extracted from the traffic. The tool utilized to capture that traffic was *Fiddler Everywhere*, a powerful tool that can be configured to decrypt traffic as it is being captured. However, to capture the traffic, three steps of configuration needed to be executed:

1. Downloading and installing a paid subscription to *Fiddler Everywhere* on a workstation and configuring it to decrypt HTTPS traffic.

Table 6a
Artifact Locations: iOS Devices iPhone 6S, iOS 13.1.3; iPhone 6S; iOS 14.4.2, iPhone 7, iOS 14.8; iPhone 12 Mini, iOS 14.8.

Artifact Type	Directory Location: \iPhone\Apple iPhone [6s][7][12]\ phone_files\phone\applications0\com.life360.safetymap\backup\Library\
Messages, all users' information	\Application Support\Messaging.sqlite
User information, location information, images	\Preferences\com.life360.safetymap.plist
User GPS coordinates, driving durations, Arity descriptors, Circle contact GPS coordinates, recorded locations, device battery % charged, Wi-Fi connection status, user in-transit status/ start-end times, Circle name, profile photo	\Application Support\LocationReader.sqlite

2. Configuring the device on the workstation IP address (as the workstation will act as the MITM during the traffic exchange) and installing and trusting a Fiddler root certificate to allow the traffic to be decrypted by *Fiddler*.
3. Connecting both the victim device and the workstation that hosts the proxy to the same network and configuring the victim device's network connection to manually proxy through the workstation.
4. Pinging the victim device from the workstation to confirm that the two can communicate.

The process of downloading and installing the certificate depended on the listening port assigned in *Fiddler*. The port used for this study was 8866. Therefore, the only accessible link was http://ipv4.fiddler:8866. This link contains the certificate to be downloaded, installed, and trusted to decrypt the traffic. *Fiddler* is a robust tool; however, for the tool to work correctly, we performed some trial and error in setting up the tool to intercept and decrypt the traffic. The study specified both iOS and Android devices to be configured for network traffic capture.

We opened two other ports and configured them to capture traffic to replicate the experiment and its results. In each instance, the port and certificate were changed. The Wi-Fi router was also configured to allow these ports to forward traffic to the *Fiddler* proxy. All three ports were blocked by default on the routers, so we initially used tethered phone network connections as hotspots to capture Life360 network traffic on the proxy. However, once the router was configured to allow traffic on these ports, the iOS traffic capture packets started flowing,[8] including unencrypted traffic and traffic decrypted by *Fiddler*.

3.5. Network traffic analysis: findings summary

Tables 7 and 8 show the results of traffic intercepted by *Fiddler* on the iOS and Android devices, as detailed in Sections 3.5.1 and 3.5.2.

3.5.1. iOS device network traffic findings for the MITM attack via proxy

We successfully conducted a MITM attack on Life360 network traffic on all four of the iOS devices, as *Fiddler Everywhere* displayed a rich variety of decrypted Life360 iOS-sourced traffic. The iOS traffic revealed all user information that the app had generated and stored since it was installed: e.g., locations, phone numbers, profile pictures, and email addresses for all Circle members. Any messages exchanged by members in the Circle were captured and decrypted to cleartext. Our testing also involved capturing network traffic generated by live user-initiated actions, including changed email addresses, phone numbers, and passwords. *Fiddler Everywhere* captured and decrypted traffic in transit, including both old and new passwords, email addresses, and phone numbers in cleartext. This revealed information that can be used to constitute a full background on a human subject being followed. Figs. 13–15 are examples of iOS network artifacts captured and decrypted by *Fiddler*.

Fig. 15 shows that driving behavior data and addresses the members shared were also captured. In addition, when a user sent a message, a user location check-in, or any other transmission to another Circle member, the packet of the device sending the message shows information of that device such as the device name, number, and battery status.

Packets carrying coded driving data were also captured and labeled with names such as "dvbArityP3." The company Arity purchases data from Life360 to provide auto insurance offers to users. The Life360 privacy policy states that the user can opt out of this feature; however, the user would lose some tracking features. The traffic capture for iOS devices gave massive access to user information; because of the capture of live user-initiated events, the findings exceeded findings from logical file acquisition using MOBILedit.

Fig. 16 shows that some of the traffic captured as we tried to spoof live URLs in a browser displayed HTTPS links presenting ERROR MESSAGE 403 – Forbidden and the message "nothing to see here, move along." This demonstrates that at least a basic element of security is implemented on Life360's servers. There was some Life360 encrypted traffic (location data) that *Fiddler* could not decrypt.

The Life360 app sends an HTTPS-tunneled HTTP request with the CONNECT and the target hostname and port number to the proxy. The third-party certificate installed and trusted on an iOS device enables *Fiddler* to decrypt the traffic and present it in cleartext. Most of the personal Life360 data was sent as.JSON files. Life360 uses TLS 1.2, a weaker cipher suite known for its vulnerabilities, including any that do not support Perfect Forward Secrecy (PFS). Life 360 should use the latest version (TLS 1.3), which is not known to have the same vulnerabilities. We were successful in decrypting the intercepted iOS traffic because Life360 does not use certificate pinning for iOS in the version of the app that we used in the study (v. 21.9.0). Other iOS apps such as iTunes use certificate pinning and reject the *Fiddler* third-party certificate, preventing HTTPS traffic from that domain from being captured and leading to service connectivity failure.[9]

3.5.2. Android Devices: network traffic findings for the MITM attack via proxy

The three proxy applications configured to capture traffic from

[8] https://docs.telerik.com/fiddler-everywhere/traffic/configure-ios

[9] Srinivas. Root Detection and Evasion. *InfoSec: Application Security*. July 2, 2014. https://resources.infosecinstitute.com/topic/android-hacking-security-part-8-root-detection-evasion

Table 6b
Artifact locations: Android devices rooted device: SSG7, android 8.0.0 unrooted devices: SSG S7, android 8.0.0 and TCEL 10L, android 11.

Artifact Type	Directory Location	Rooted Device	Unrooted Devices
Encrypted or encoded driving logs	\phone_files\phone\applications0\com.life360.android.safetymapd	\live_external\files\CoreEngine_Life360\Release\Production\DrivingEngineLog	\live_external\files\CoreEngine_Life360\Release\Production\DrivingEngineLog
Application usage, timestamps	\phone_files\phone\applications0\com.life360.android.safetymapd	\description.info.xml	\description.info.xml
Device Permissions	\phone_files\phone\applications0\com.life360.android.safetymapd	\com.life360.android.safetymapd.apk	\com.life360.android.safetymapd.apk
All Circle users' contact and location information; device and network connectivity information	\phone_files\phone\applications0\com.life360.android.safetymapd\live_data\databases	L360LocalStoreRoomDatabase	–
Privacy settings	\phone_files\phone\applications0\com.life360.android.safetymapd\live_data\databases	L360LocalStoreRoomDatabase	–
128 of Life360's privacy data partners	\phone_files\phone\applications0\com.life360.android.safetymapd\live_data\databases	L360LocalStoreRoomDatabase	–
Message and location data	\phone_files\phone\applications0\com.life360.android.safetymapd\live_data\databases	Messaging.db	–
Images of user GPS locations on a map	\mobiledit_export_files\phone\misc\analyzers\com.life360.android.safetymapd_webkit_cached_media_files\volley_cache\data	\analyzers\com.life360.android.safetymapd_webkit_cached_media_files\volley_cache\data	–
AES key	\phone_files\phone\applications0\com.life360.android.safetymapd\live_data\shared_prefs	com.life360.android.safetymapd_preferences.xml	–
Individual device applications/ processes memory usage	phone_files\phone\applications1\Dumpsys	meminfo.log	–
Individual device in-memory daily stats	phone_files\phone\applications1\Dumpsys	usagestats.log	–
All users' images (profile, check-in locations)	pdf_files\phone	\misc\thumbs	–
User email account name and password field (encoded)	\phone_files\phone\raw0\data\system_ce\0	accounts_ce.db	

the Android devices failed to capture traffic worth exploring. The only traffic captured on the unrooted Android devices was tunneled through HTTPS. As such, base URLs for captured Life360 packets had identical port 443 (:443) appended, with no additional server directory structure apparent. We had speculated that to capture traffic, root access to the Android system files was needed to add an exception rule for Life360 traffic to be captured by *Fiddler*. However, this did not prove to be true, as we captured the same limited HTTPS-tunneled traffic for the rooted Android device.

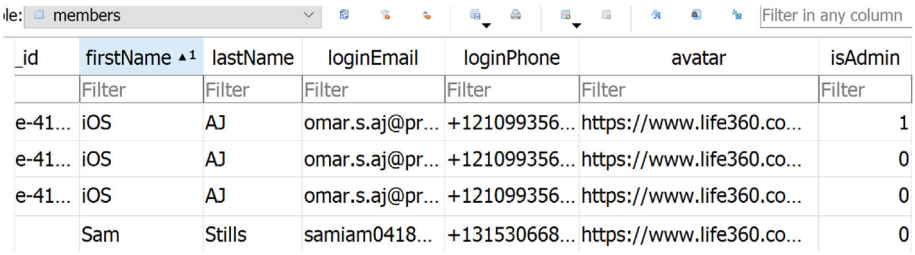
Captured traffic from *Charles Proxy* and *Packet Capture App* in our study did not reveal any unencrypted traffic or successfully decrypted traffic. After only a few packets using *Packet Capture App*, traffic stopped being captured. The app was the only tool that captured Android traffic, but there was no data in the packets. The app also required a certificate to be installed on the device, but it was not available on the Google Play Store.

To investigate why Life360 traffic on the Android devices could neither be captured nor decrypted, we extracted the Life360 21.9.0 APK (application package kit) from the rooted Android device. Upon inspection of the APK's.java files using Android Studio, we discovered that this version of the app uses certificate pinning to mitigate MITM attacks by preventing proxies like *Fiddler* from being able to capture or decrypt app traffic. Certificate pinning limits which certificates a server will accept for authentication of client-server connections. This eliminates the notion of trust in entities such as Domain Name Server (DNS) and Certificate Authority (CA) and reduces the likelihood that a server's certificate can be spoofed (such as in a MITM attack). In addition to certificate pinning, the app also uses root detection.

3.6. Logical analysis and network traffic analysis summary findings

We studied seven mobile devices, whereas the two other related studies only conducted a forensic analysis of the Life360 app on two or three devices, respectively. We designed our experiment with multiple iOS devices on a variety of iOS versions to confirm or refute any differences in the amount of data that can be forensically recovered or captured based on differences in phone model or iOS version. We confirmed that all four of the iOS devices in the study – even the later iPhone 12 mini running on a modern iOS version – had identical forensic findings for both the logical analysis and the network traffic analysis. There was no security feature in the newer model or iOS preventing access to forensic artifacts.

Similarly, we included two different brands of Android devices, as well as a pair of devices with the same base model running the same Android 8.0.0, one of which was rooted and the other which was not rooted. Our study found significantly different results for the rooted Android device based on a logical forensic analysis versus the same analysis for the unrooted Android devices. The data recovered from the rooted Android device by logical analysis was similar to the data recovered from the iOS devices using the same method. However, rooting the Android device did not lead to a successful MITM attack to intercept and decrypt live Life360 user traffic. Life360's SSL certificate pinning in the Android app prevented traffic from being captured or decrypted. Additionally, our analysis of the Life360 APK revealed evidence that the app checks



ble: members — Filter in any column

_id	firstName	lastName	loginEmail	loginPhone	avatar	isAdmin
	Filter	Filter	Filter	Filter	Filter	Filter
e-41...	iOS	AJ	omar.s.aj@pr...	+121099356...	https://www.life360.co...	1
e-41...	iOS	AJ	omar.s.aj@pr...	+121099356...	https://www.life360.co...	0
e-41...	iOS	AJ	omar.s.aj@pr...	+121099356...	https://www.life360.co...	0
	Sam	Stills	samiam0418...	+131530668...	https://www.life360.co...	0

Fig. 8. User information from ***L360LocalStoreRoomDatabase***.

content	created_at	failed_to_send	sent	dismissed	read	deleted
Filter	Filter	Filter	Filter	Filter	Filter	Filter
Hey yall	1658535806	0	1	0	1	0
Checked in @ study	1658535855	0	1	0	1	0
Checked in @ Study	1658535876	0	1	0	1	0
Checked in @ The...	1658535984	0	1	0	1	0
Hi	1658537402	0	1	0	1	0

Fig. 9. *Plaintext Messages and related info from* ***Messaging.db***.

```
Applications Memory Usage (in Kilobytes):
Uptime: 67245332 Realtime: 501273807

Total PSS by process:
   Total  (   PSS   SwapPss ) kB
    180,073K: system (pid 3629)
    169,286K: com.google.android.googlequicksearchbox:search (pid 20480)
    159,048K: com.android.systemui (pid 4063 / activities)
    155,073K: com.sec.android.app.launcher (pid 5028 / activities)
    136,451K: com.android.chrome (pid 19101)
    113,434K: com.google.android.apps.maps (pid 18752)
```

Fig. 10. *Android Device: Memory Usage of All Apps/Processes on the Device from* ***meminfo.log***.

for device root access. Although root detection is a common app security measure[10], it is unclear what effect it may have on Life360 app functionality on the device.

4. Research limitations and future research

Due to project scope and time constraints, the research project had certain limitations. We only used one mobile device forensics tool, MOBILedit. Because of such a wide variety of available Android devices, other resources and studies like Skulkin et al. (2019) recommend using more than one forensic acquisition tool.

A future study could delve more deeply into potential connections between the logical or physical file analysis and network traffic analysis. Artifacts from one forensics source might inform those from the other. For example, Life360 assigns user, message, and several other types of IDs that appear in various files. It may be possible to cross-check and correlate logical and network traffic data for a more complete view of Life360-generated data.

Future research could investigate potential options for bypassing certificate pinning to successfully decrypt Life360 traffic captured from Android devices in a MITM attack. Some possible options include: 1) installing and trusting the 3rd-party *Fiddler* proxy certificate as a system certificate in the Android device. As more recent versions of Android OSes reject user certificates even if installed as a system certificate, this method may not be successful in all settings. Another option would be: 2) using an SSL certificate

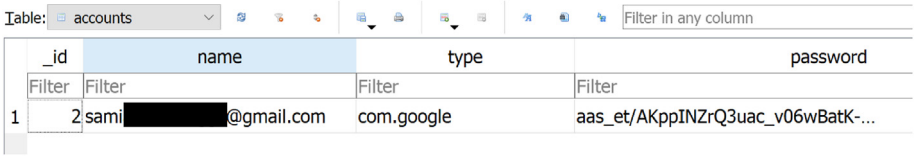


Table: accounts — Filter in any column

	_id	name	type	password
	Filter	Filter	Filter	Filter
1	2	sami[redacted]@gmail.com	com.google	aas_et/AKppINZrQ3uac_v06wBatK-...

Fig. 11. *Email Account and Encrypted or Encoded Password Information from* ***accounts_ce.db***.

life360-prod	CustomerId
{"gpsTrailFrequency":15,"nextKVMDownload":8640,"arityBaseUrl":"https://api.arity.com/drivingbeha	InternalConfigurationProd
{"collection":{"gps":true,"ttlDays":30,"maxTripSizeMins":120},"transmission":{"maxPayloadSizeMB":0.	HFDConfigurationProd
life360	AppId
{"gpsIntervalSecs":15,"uploadIntervalSecs":45,"uploadUrl":"https://api.arity.com/drivingbehavior/gps/	RealtimeGPSConfigurationProd
	LatestUnProcessTrip
GB	deviceLocale
hwpPv91Z9Mz3TlbcuVAYvcR3PJps9XLOFJfjPnHoFPE+DglWR76eEclxPTzonYDu	DeviceId
	notifi_priority_at_detection
{"A":1.0,"A0":4.08,"B":1,"B0":1.718,"C":0.79,"C0":4.41,"D":0.4,"D0":6.125,"E":0.4,"E0":38.72,"F":-0.1	CollisionConfigurationProd
hwpPv91Z9Mz3TlbcuVAYvcR3PJps9XLOFJfjPnHoFPE+DglWR76eEclxPTzonYDu	UserId
TPOabJkk1UUvVN26MCqj3YiXYcFxP5We	aes_key
{"accelerationThreshold":3.57632,"airPlaneModeDuration":60,"angleChangeThresholdCustomer":0.6,	SdkConfiguration

Fig. 12. *AES key in* ***com.life360.android.safetymapd_preferences.xml***.

Table 7
Network traffic findings summary.

Artifact Types	iPhone 6S, iOS 13.1.3 iPhone 6S, iOS 14.4.2	iPhone 7, iOS 14.8	iPhone 12 mini, iOS 14.8	TCL 10L (*unrooted*), Android 11	SSG S7, Android 8.0.0 (*unrooted*)	SSG S7, Android 8.0.0 (*rooted*)
Name	☑	☑	☑			
Phone number	☑	☑	☑			
Email	☑	☑	☑			
User password (old and new)	☑	☑	☑			
Timestamps	☑	☑	☑	☑	☑	☑
Profile picture	☑	☑	☑			
Authentication token	☑	☑	☑			
User GPS coordinates	☑	☑	☑			
Contact GPS coordinates	☑	☑	☑			
Plaintext messages with read/receipt status	☑	☑	☑			
Images	☑	☑	☑			
Circle names	☑	☑	☑			
Other contacts in Circles	☑	☑	☑			
Check-in locations (GPS & address)	☑	☑	☑			
Recorded locations (GPS & address)	☑	☑	☑			
Driving data (speed, Arity score and descriptors)	☑	☑	☑			
Device metadata	☑	☑	☑			
Transit status	☑	☑	☑			
Number of unread messages/alerts	☑	☑	☑			
Bluetooth connectivity status	☑	☑	☑			
Message deletion status	☑	☑	☑			
Device battery charge % & whether charging	☑	☑	☑			
Life360 device ID and device fingerprint ID	☑	☑	☑			

Table 8
Network Traffic Artifact Sources iOS devices (iPhone 6S, iOS 13.1.3; iPhone 6S, iOS 14.4.2, iPhone 7, iOS 14.8, iPhone 12 mini, iOS 14.8).

Artifacts	Source URL
User GPS coordinates, username, name, app version	https://sdk.iad-01.braze.com/api/v3/data
Plaintext messages, User IDs, Circle IDs, locations, message read/deleted status, receiver IDs	https://api-cloudfront.life360.com/v3/Circles/062 … 41140c/threads/message
Device name, device (OS) version, app version, device type (e.g., iOS), carrier, device model	https://api-cloudfront.life360.com/v3/users/devices
Circle IDs, Circle leave/join event (Circle IDs)	https://api-cloudfront.life360.com/v3/users/premium?CircleId = ae40443 … c7b
Device fingerprint ID	https://api2.branch.io/v1/open
Driving data (in code but not encoded or encrypted)	https://api-cloudfront.life360.com/v3/experiments
Binary value indicating whether member uses crash alerts	https://api-cloudfront.life360.com/v3/driverbehavior/crashenabledstatus
Data transmitted: User ID, name, address, email, phone number, profile photo, account creation date/time, user's old and new passwords in plaintext, phone number change, email change, user ID, name, profile photo	https://api-cloudfront.life360.com/v3/users
User GPS and physical address location auto-record, timestamp start/end at location, User ID, account creation date/time, device battery status, user in-transit status/start-end times, location duration, binary Wi-Fi connection indicator, speed (MPH), number of read or unread messages	https://api-cloudfront.life360.com/v3/Circles/ae40443d … 0cc7b/members/history

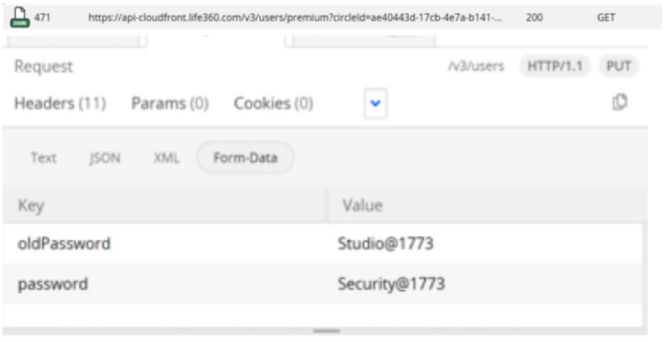


Fig. 13. Network traffic findings sample: Password change in cleartext.

"killer" app to bypass the Life360 app's protective SSL certificate pinning. An experiment could test whether a firewall block of QUIC (HTTP/3) UDP traffic could bypass SSL certificate pinning by forcing a downgrade to HTTP/2 traffic that could be decrypted by a proxy like *Fiddler*.

5. Conclusion

Our research discovered multiple forensic artifacts that comprised significant amounts of personal data generated by Life360 and stored on mobile devices. Artifacts can be captured using a logical analysis or a network traffic analysis on a variety of iOS devices that do have not have been jailbroken, including those running more recent versions of iOS. In addition to user contact

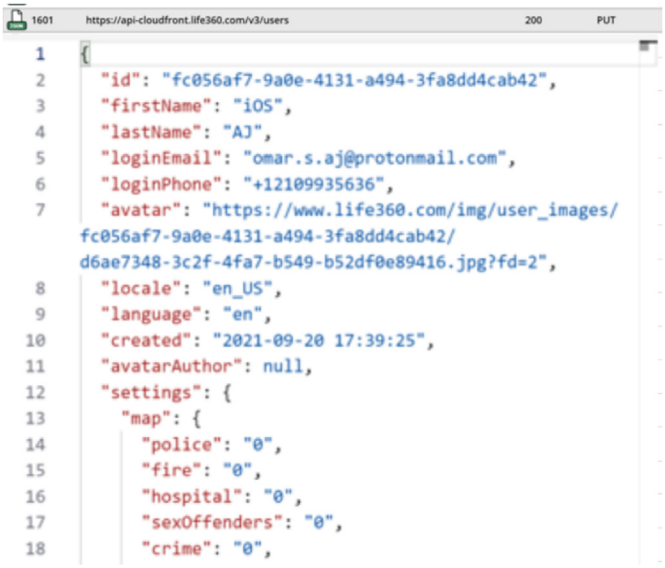


Fig. 14. Network traffic findings sample: User data.

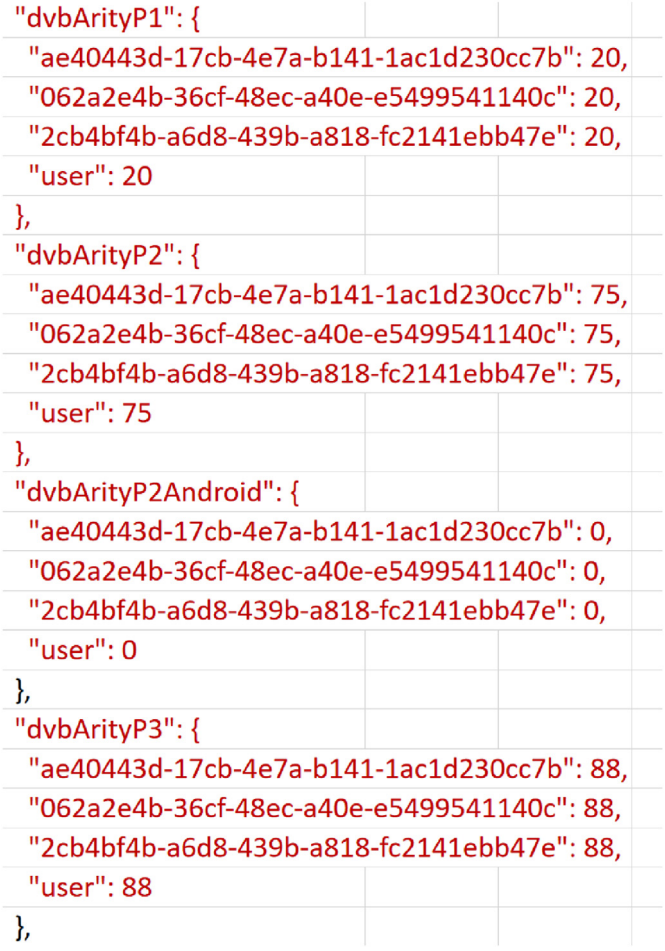


Fig. 15. Network traffic findings sample: Driving data.

information reported by the study of Bays and Karabiyik (2019), we also discovered artifacts generated by Life360's "premium features" (for example, driving data and device battery status), as well as

Fig. 16. Network Traffic Findings Sample: HTTP 403 forbidden error.

other additional artifacts. Our study also highlights another vector for forensic artifacts generated by Life360: network traffic. In addition to discovering the same type of personal data in the iOS network traffic as in the logical file analysis, we simulated a MITM attack to capture and decrypt sensitive data resulting from live user-initiated actions such as changing an account password. Notably, it is possible that only one device would need to be compromised for all Life360 Circle users' personal data to be compromised.

Our study echoes the study of Bays and Karabiyik (2019), showing that only limited Life360 data could be retrieved from a logical analysis of an unrooted Android device. However, our study additionally establishes that many Life360 artifacts can be extracted from a *rooted* Android device via a logical analysis, which is a new finding for Life360. Unlike existing Life360 forensic studies, we determined conclusively that the Life360 app for Android uses SSL certificate pinning, which thwarts MITM traffic interception and decryption. The Life360 app for Android also uses root detection. We confirmed the regardless whether rooted or unrooted, MITM attack using a proxy was not successful for recovering forensic artifacts because of SSL certificate pinning.

Declaration of competing interest

The authors declared that there is no conflict of interest in this study.

Data availability

Data will be made available on request.

Acknowledgement

We would like to express our gratitude to Compelson Labs for their support and for making MobilEdit available for our research. This work was partially supported by National Science Foundation (NSF) CREST under Grant HRD-1736209.

References

Alkhattabi, Khalid, Alshehri, Ahmed, Yue, Chuan, 2020. Security and privacy analysis of android family locator apps. In proceedings of the 25th ACM symposium on access control models and technologies, 47–58. https://dl.acm.org/doi/pdf/10.1145/3381991.3395612.

Andriotis, P., Takasu, A., 2020. To allow, or deny? That is the question. In: Moallem, A. (Ed.), HCI for Cybersecurity, Privacy and Trust. HCII 2020, Lecture Notes in Computer Science, 12210, pp. 287–304. https://doi.org/10.1007/978-3-030-50309-3_20.

Ayers, R., Livelsberger, B., Guttman, B., 2018. Quick-start guide for populating mobile

test devices. NIST special publication (SP) 800–202 (draft). Natl. Inst.Stand.-Technol. nist.gov/system/files/documents/2017/05/09/mobile_device_data_population_setup_guide.pdf.
Ayers, R., Brothers, S., Jansen, W., 2014. Guidelines on Mobile Device Forensics (NIST Special Publication 800–101. U.S. Department of Commerce, Washington, DC. nist.gov/publications/guidelines-mobile-device-forensics?pub_id=915021.
Bays, J., Karabiyik, U., 2019. Forensic Analysis of Third-Party Location Applications in Android and iOS. IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1–6. https://ieeexplore.ieee.org/document/9093781.
Brey, P., 2000. Technology as extension of human faculties. In: Mitcham, C. (Ed.), Metaphysics, Epistemology, and Technology, Research in Philosophy and Technology, 19, pp. 59–78.
Burmeister, F., Drews, P., Schirmer, I., 2021. Modeling the C(o)urse of privacy-critical location-based services–exposing Dark side archetypes of location tracking. In: in proceedings of the 54th Hawaii international conference on system sciences, p. 6651. https://scholarspace.manoa.hawaii.edu/bitstream/10125/71419/0650.pdf.
Chand, D., Nayak, S., Bhat, K.S., Parikh, S., Singh, Y., Kamath, A.A., 2015. A Mobile Application for Women's Safety: WoSApp, TENCON 2015 - 2015 IEEE Region 10 Conference, pp. 1–5. https://doi.org/10.1109/TENCON.2015.7373171.
Chatterjee, R., Doerfler, H.O., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., Ristenpart, T., 2018. The Spyware Used in Intimate Partner Violence. IEEE Symposium on Security and Privacy (SP), pp. 441–458. https://doi.org/10.1109/SP.2018.00061, 2018.
Gabriels, K., 2016. 'I keep a close watch on this child of mine': a moral critique of other-tracking apps. Ethics Inf. Technol. 18, 175–184. https://doi.org/10.1007/s10676-016-9405-1.
Gabriels, K.. 'Quantified otherness': does continuous technical connectivity destabilize our moral connectedness? n.d. https://www.theinternetofthings.eu/sites/default/files/docs/EU%20Internet%20of%20Things.pdf.
Harkin, D., Molnar, A., Vowles, E., 2020. The commodification of mobile phone surveillance: an analysis of the consumer spyware industry. Crime Media Cult. 16 (1), 33–60. https://doi.org/10.1177/1741659018820562.
Hasinoff, A.A., 2017. Where are you? Location tracking and the promise of child safety. Televis. N. Media 18, no 6, 496–512. https://doi.org/10.1177/1527476416680450.
Hoog, A., Strzempka, K., 2011. iPhone and iOS Forensics. Syngress learning, .oreilly.com/library/view/iphone-and-ios/9781597496605/.
Keegan, Jon, Ng, Alfred, 2021. The popular family safety app Life360 is selling precise location data on its tens of millions of users. The Markup, December 6. https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user.
Knox, S., Mogdaham, S., Patrick, K., Phan, A., Choo, K.-K.R., 2020. What's really 'happning'? A forensic analysis of android and iOS *Happn* dating apps. Comput. Secur. 94. https://doi.org/10.1016/j.cose.2020.101833.
Lwin, H.H., Aung, W.P., Lin, K.K., 2020. Comparative Analysis of Android Mobile Forensics Tools. IEEE Conference on Computer Applications (ICCA), pp. 1–6. https://doi.org/10.1109/ICCA49400.2020.9022838.
Mannan, M., Youssef, A., Ali, S., Elgharabawy, M., Duchaussoy, Q., 2020. Privacy Report Card for Parental Control Solutions. https://madiba.encs.concordia.ca/reports/OPC-2019/OPC-2019-Full-Report.pdf.
Marciano, Parental Surveillance, Avi, Styles, Parenting, 2021. Toward a model of familial surveillance climates. Mobile Media Commun. https://doi.org/10.1177/20501579211012436.
Maxwell, L., Sanders, A., Skues, J., Wise, L., 2020. A content analysis of personal safety apps: are they keeping us safe or making us more vulnerable? Violence Against Women 26 (2), 233–248. https://doi.org/10.1177/1077801219832124.
McFarland, Scholle, 2019. Take control of catalina. Take Control Books. learning.oreilly.com/library/view/take-control-of/9781098123208/.
McGuire, M., 2012. Technology, Crime and Justice: The Question Concerning Technomia, first ed. Willan. https://doi.org/10.4324/9780203127681.
Meisenzahl, M., 2019. Teens are finding sneaky and clever ways to outsmart their parents' location-tracking apps, and it's turning into a meme on TikTok. Business Insider. businessinsider.com/life360-location-tracker-teens-tiktok-memes-tips-2019-11.
Priest, David, 2021. Life360 app is selling data from millions of families, report says. CNET. https://www.cnet.com/home/security/life360-app-is-selling-data-from-millions-of-families-report-says.
Sansurooah, K., Keane, B., 2015. The Spy in Your Pocket: Smartphones and Geo-Location Data. Australian Digital Forensics Conference. https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1153&context=adf.
Simpson, B., 2014. Tracking children, constructing fear: GPS and the manufacture of family safety. Inf. Commun. Technol. Law 23 (3), 273–285. https://doi.org/10.1080/13600834.2014.970377.
Skulkin, O., Tindall, D., Tamma, R., 2019. Learning Android Forensics, second ed. Packt Publishing learning.oreilly.com/library/view/learning-android-forensics/9781789131017/.
Wood, M.A., 2021. Rethinking how technologies harm. Br. J. Criminol. 61 (3), 627–647. https://advance-lexis-com/api/document/collection/analytical-materials/id/62TH-MXM1-K054-G2KF-00000-00?cite=Br%20J%20Criminol%20(2021)%2061(3)%3A%20627-647&context=1516831.
Yellanki, S.K.A., 2020. Survey on potential privacy leaks of GPS information in android applications. https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=3450&context=thesesdissertations.