Identify Users on Dating Applications: A Forensic Perspective

Paul Stenzel and Nhien-An Le-Khac(✉)

University College Dublin, Dublin, Ireland
paul.stenzel@ucdconnect.ie, an.lekhac@ucd.ie

Abstract. Online dating has grown in popularity since the introduction of the World Wide Web and within the last decade the widespread use of smartphones and dating applications, or 'apps'. Associated with this popularity is the increased scrutiny around these apps and what companies are doing to protect users' private information. Dating apps are one of the riskiest, considering the users of these apps outline their innermost thoughts and desires, along with sharing intimate images and, in most cases, their location that can potentially identify their home, work, and other locations users may not intend to share. Associated with the privacy risks is the use of dating apps for criminal purposes including; stalking, sexual violence, drug dealing, and other violent crimes. These crimes present a challenge to law enforcement as the offenders may not be known to the victim(s) at all which may mean the lines of inquiry for investigators are limited in identifying the offender's real identity. There has been no study in literature into what investigators could obtain from these apps to identify another user if you only had one account, such as an account from a victim of a crime. Therefore, in this paper, we examine six of the 'top' dating applications and outline a process to analyze data obtained from their use to determine whether there is sufficient information that can be obtained to identify another user profile and their real-world identities.

Keywords: Dating application investigation · user identification · OSINT · network traffic analysis · mobile device forensics · iOS forensics

1 Introduction

Online dating has become one of the most popular ways for people to meet around the world. The widespread use of smartphones, along with dating applications, or apps, has enabled people to match with others with similar interests easily [1–3]. This is especially true for the LGBT community where, in the United States, the use of dating apps, is roughly twice as common as straight adults [4].

Dating applications also allow predatory or opportunistic criminals to use the applications for malicious purposes. Sexual assaults are unfortunately common and are widely publicized in an attempt to highlight the dangers of meeting people online [5, 6]. Associated with this increased use of technology is the fact that incredibly personal information

S. Goel and P. R. Nunes de Souza (Eds.): ICDF2C 2023, LNICST 570, pp. 58–77, 2024.
https://doi.org/10.1007/978-3-031-56580-9_4

was being stored and shared on these applications and, in several cases, was not being transmitted or stored securely [7].

The most common way investigators access social media data is via access to the device or by using some form of legal process [8]. The borderless nature of Cybercrime is used to describe the challenges Law Enforcement investigators face when investigating crime on the internet due to legal challenges, and limitations on cross-border investigations [9]. While the legal process is generally straightforward to obtain within the country an investigator is in (noting evidential requirements) this is not always the case internationally. Companies may be based overseas from where the investigator is located requiring, in some cases, Mutual Legal Assistance requests to be made, which can be time-consuming and cumbersome [10].

Due to the fragile nature of digital evidence, ensuring relevant data is preserved and obtained quickly is crucial in identifying additional items of interest and holding offenders to account for their crimes. Dating applications hold a large amount of personal information which can be crucial to identify persons of interest and, in some cases, other victims. Identifying information that is on those apps that could be used by investigators to identify real-life identities quickly, and may lessen the danger to other dating application users, and other members of the public when a crime has been committed.

Previous research into dating applications has generally focused on the psychology of how and why people use the applications and from the technical approach, the privacy and security risks of what people may be able to find out about users that they did not intend to intentionally share [11, 12]. While other research has attempted to inform investigators about what may be available in different dating apps, this has generally focused on one dating app, and what may be recovered, or one aspect of where information may be stored [13]. Users of dating apps are more than likely to utilize more than one dating app at a time [14]. This increases the opportunities for investigators as a much larger data set can be reviewed for relevant information rather than focusing on only one app.

As dating apps are the most common way for people to meet, and criminals utilize these apps to commit crimes, research into how investigators can utilize these apps to help solve those crimes is needed and is the gap that will be addressed in this paper. The main question therefore is 'How can you identify another user on a dating application only from the interaction between the two profiles?'.

In this paper, we address this challenge by studying all aspects of how the data is transmitted and stored within various dating apps. This includes data packet capture of data being sent to/from a user's device, extractions of data off the phone after an interaction has taken place, backups of users' accounts, as well as how Open-Source Intelligence (OSINT) methods and trilateration techniques could be employed to identify users as well.

Through our approaches, the identity of other users of dating apps can be identified. This process fundamentally depends on what apps are being used along with what investigators have access to as part of their investigation i.e., what tools and legislation allow them to access this type of data, and what policies their agencies have in conducting this type of work. While some app developers have utilized technology in better ways to protect users' privacy, this is not the case for all apps and this may allow information

about the user to be identified including, name, age, profile information, and even their location. The main contribution of this paper can be listed as follows:

- A wider literature review on dating apps and how the law enforcement and investigative community can utilize information from these apps to protect members of the public.
- Providing an investigative process on what can be used to identify another user on a dating app which will enable investigators to identify artifacts of interest that, when combined, will assist in identifying a victim, witness, or suspect, who is using a dating app. This process will be able to be utilized across any mobile operating system and is agnostic to the dating app as an assessment of what can, and has been obtained, provides investigative opportunities on who the other user of the dating app may be.
- An intensive experiment was used to demonstrate the efficiency, usability, portability, and flexibility of the proposed process.
- Investigators working on specific cases can refer to this process to determine what sections of this research apply to their case and then assess what information they may be able to obtain to advance their case.

2 Literature Review

Due to the prevalence of encryption on the Internet, law enforcement's ability to identify suspects is becoming increasingly challenging. The most common approaches to this problem are to: work with the companies on an ad-hoc basis, provide them legal process directly, seek law enforcement cooperation, or for companies overseas who are unwilling to accept foreign legal process, to use letters rogatory or Mutual Legal Assistance. Due to how technology has evolved, the above legal processes have resulted in a system that is confusing, uncertain and does not meet the needs of the users [17].

Online dating applications (or apps) have been identified as a specific area where being able to obtain data as quickly as possible may prevent further victimization as people who use dating apps may not be well known to the victims or, in some cases, the companies running the apps may remove or block users before law enforcement can obtain vital data for an investigation [18, 19]. Data that may be available to law enforcement from dating apps is wide, due to the amount of personal information a user provides when setting up an account, along with the use of location-based services obtained from the phone's GPS, GSM, LTE, Wi-Fi, and Bluetooth radios [20].

Privacy and security concerns relating to online dating have been a concern for security researchers for over a decade with the Electronic Frontier Foundation (EFF) highlighting their concerns in 2012 [21]. Several of the concerns raised by the EFF still exist today with the use of dating apps and this highlights the slow uptake of application security by companies.

While no specific research has been conducted relating to identifying a user from dating app data, there is literature that is relevant in several different areas, including data that is being transmitted (Packet Capture) [7, 22–24], OSINT and trilateration of users [25–29], along with forensic analysis of mobile phones [30–33], and backups of those devices.

There were estimated to be over 6 billion smartphones in use around the world in 2021 with half of those being Samsung or Apple devices [34]. In 2012, Boyles et al. found that 59% of American smartphone owners were likely to back up their devices, however only roughly a third of those that did, did so frequently [35]. Both Android and Apple devices can back up a large variety of information including phone settings, pictures and videos, and app data, and are therefore relevant to investigators, even if the phone associated with the account is located [36, 37].

iTunes backups were obtained in [24] as part of their research into the happn dating app with the authors focusing on the SQL databases and plist (Property List) files for user data. User information was found in the database hdata.db and included several tables of data useful for investigators, this included the user's location at the time of app use, email address, profile picture URLs for the user and matched users, messages, and a table connecting a username to their photos. The researchers also referenced information obtained in plists with the hdata.db file to show how investigators could infer whether dating app accounts may be fake if the device name (contained in the plist file) was different from the app user name.

Thantilage et al. (2020) proposed a method of examining iOS backups generated by iTunes focusing on two dating apps Tinder, and Coffee Meets Bagel [10]. The authors were able to show that once the backup folder is identified (through the 40-digit Unique Device Identifier), investigators may be able to locate the file name of interest by converting that file path to a SHA-1 hash value or locating it in the Manifest.db file available in the root of the backup. In the Tinder database, they were able to identify a large amount of PII that would be relevant to an investigator including personal information about the user, and information about matches in Tinder including names, birthdates, bio, and profile pictures. In comparison, the Coffee Meets Bagel app listed the personal information of the user, as well as information on other users, including geo data of the users' exact location.

Previous research into dating apps has evolved significantly from identifying privacy and security concerns in Patsakis et al. and Choo et al. [7, 12] where app developers allowed significant personal information to be disclosed without the use of encryption, through to what artifacts may be useful for investigators analyzing specific dating apps. Methods, Frameworks, and Taxonomies have also been created to assist investigators in how to approach dating apps, identify the most important artifacts, and present them in a way that is easy to comprehend. The use of different approaches to the same challenges has helped this field of research, and this includes the novel approach of 'colluding trilateration' in [29] and utilizing backups to mobile phones when the device may not be available in [10].

The main research gaps identified in the previous literature are around the suspect, or a person of interest, and how dating apps could be used to assist in identifying that person, or those people. Most of the current research focuses on either, the risk to the user of the dating app i.e., privacy and security risks, or what information you could obtain from an app, or data from an app e.g., backups or packet capture, which is generally after a suspect or person of interest has been identified.

3 Problem Statement and Forensic Approach

3.1 Research Objectives

While there has been previous research into dating apps, most of the research has focused on privacy and security concerns or taxonomies that have been created to assist law enforcement in explaining what can be extracted from devices, or their backups, as opposed to identifying criminals or their victims. This ultimately means that law enforcement will need to engage with the companies that develop/run the apps or, if the companies are overseas and won't respond to the legal process of that country, a Mutual Legal Assistance request, or similar.

The broad range of data potentially available to investigators needs to be considered when determining what may assist in an investigation. This can include the mobile device itself and the databases on the phone used to store user information, any backups made of the phone, data sent/received while the app is being used [41], and analysis of any open-source information that may identify the user or their location.

This research aims to determine whether there is sufficient data sent, received, or stored during the use of a dating app to identify another user profile on a dating app. A specific scenario relating to this question is whether certain combinations of data from apps can be combined to enable the identification of a user. The process used in this research is agnostic to apps and operating systems and could therefore be used in any other platform. The most significant artifacts to assist in this answer will be collected and then presented in terms of what combinations of this data may assist investigators in identifying users of these applications. Due to the ever-changing nature of technology, the applications used and their versions, are provided as an indicator of what may be able to be obtained. Two main research questions that we aim to address in this paper are as follows: (i) What information can be sought, or obtained, to identify a user from a user profile (one in your control) of an e-dating application? This would include all facets of the app being used e.g., data extracted from the application installed on a phone, backups of the same data, network traffic when an app is being used, and OSINT/Trilateration of the user profile; (ii) What information could be used to match a user profile with a real person? This would include exploring how to attribute OSINT e.g., reverse image searching of a user's profile image, or reviewing artifacts obtained from a device.

3.2 Forensic Methodology

To determine what artifacts can be used to identify a user profile, and subsequently, a real-life person, a process has been created to obtain the most amount of data from dating apps. This data can then be presented to show what may be the most useful information across the variety of apps tested.

Six different dating apps were chosen as this would provide a broad range of artifacts that could be obtained and would enable the same testing methodology to be employed across all of the apps tested. An iOS platform was selected to obtain data for this research due to the prevalence of these devices in Western countries, however, the same process could also be applied to Android devices. Testing was conducted using both Android and iOS devices due to the ability to leverage the strengths of how the different devices

can be used and what software can be installed on them. Two profiles were created, one male and one female, with each profile being associated with one of the mobile devices.

This approach was only considered from a 'black-box' perspective i.e., APKs were not reverse-engineered and all testing was considered from a position where, although you may get physical access to a device, there would not be sufficient time or expertise available to reverse engineer the app to obtain data that is not available through the 'normal' use of the app. The source code of the apps, documentation related to them, or assistance of the developers was not obtained in this research.

Briefly, our approach has four main phases: (i) Packet capture; (ii) OSINT and Trilateration; (iii) Analysis of the mobile device, and finally (iv) The analysis of a backup of the device.

4 Experiments

4.1 Platforms and Datasets

Dating Apps. Testing was done primarily on the Apple iOS operating system due to their prevalence in Western countries however the same process can be utilized on Android operating systems. The six apps chosen for this research aim to represent the broad range of dating apps that are available in the Apple Store. This selection also attempts to take into consideration any improvements in the app developers' security and privacy processes due to the wide media coverage, and research on this issue [15, 16]. All of the apps were installed and tested on the same test device using generated (fake) profiles which are explained further below. None of the apps were updated during testing and were connected to a segregated wireless network, along with software filtering of traffic, which ensured that traffic generated from the test device and/or app server was passing through that network.

Table 1 outlines the app name, company, and version number of the app tested, as well as the category and position the app had on the Apple App Store at the time this research was completed.

The setup was very sterile in that only network traffic from the specific app in question, along with some Apple/iCloud traffic, will be captured. This will not likely identify any third-party interactions with the apps, as other services i.e., Facebook, have not been used. If the app developers have implemented any security features that detect MITM attacks, other than certificate pinning, and change how the servers respond to requests then this may not be able to be identified through this testing. In relation to the use of OSINT, as both the profiles that were set up are not real, the application of these techniques will not locate, or provide information to identify a user - as there is no real-life person to be found.

Table 1. Dating Apps used in the experiments

App	Company	Version	Category
Bumble	Bumble Holding Limited	5.272.0	Lifestyle (No. 6)
Happn	French FTW & Co	9.41.0.0	Lifestyle
Hinge	Hinge Inc	9.1.0	Lifestyle (No. 8)
OkCupid	Humor Rainbow Inc	66.2.0	Lifestyle (No. 72)
Plenty Of Fish	Plenty Of Fish Media	18.50	Social Networking (No. 23)
Tinder	Tinder Inc	13.10.1	Lifestyle (No. 3)

Investigation Tools. Tools used in the analysis of data acquired from the various collection methods explained above are listed in Table 2 below.

Table 2. Tools used in the experiments

Tool	Version	Required Use
DB Browser for SQLite	3.12.2	Analysis of iPhone Backup
Fake GPS	5.4.1	Trilateration of profiles
Fiddler Everywhere Pro	3.3.1	Analysis of packet capture
iBackup Viewer	4.27.5	Analysis of.plist files
IrfanView	4.60	Examining images for metadata
iTunes	12.12.4.1	Creating iTunes backup of iPhone
Notepad++	8.2.1	Opening.txt and other files
UFED 4PC	7.56.2.282	Forensic Acquisition of iPhone
VLC Media Player	3.0.7.1	Playing media files

Experimental Devices. The following test devices were used for all apps tested:

- Primary Test Phone - Used for analysis: Phone - iPhone 7, Model Number - MNAC2LL/A, Operating System - iOS 15.5
- Secondary Test Phone - Used to simulate interactions: Phone - Galaxy S9+, Model Number - SM-G965U1, Operating System - Android Version 8.0.0

Test devices were reset (wiped) before use with only profile information relating to the generated user installed on the app, no other data was added i.e., contact lists, additional media, etc. The apps were installed on the device as a standard user would do so, which was accessing the Apple App Store and installing the app once selected.

User Data. User profile data was generated for use in the test devices from online resources which generate names, photos of faces, etc. to ensure that no information from

a real-life individual was used in the testing. For OSINT testing, one profile image for each profile was selected from a publicly available website to be used in the dating apps. Profile data required for each dating app is not recorded due to the large variety of questions asked upon sign-up, however, this was answered similarly across all apps using generic answers e.g., drink - socially, smoke - never, etc. to ensure profiles could be activated successfully. Table 3 outlines information about the test profiles that were used.

Table 3. User Profiles used in experiments

	Profile 1	**Profile 2**
Mobile Phone	iPhone	Samsung
Name	Docbob Hayfarmer	Lynette Birdie
Age	30	24
Gender	Male	Female
Sexual Orientation	Straight	Straight
Phone No.	+15714784269	+15712901787
Profile Image		

4.2 Packet Capture

One of the core approaches to collecting data on these dating apps is through packet capture and the analysis of the traffic on completion. To capture the network traffic between the apps and the app servers, a debugging proxy was used to route the traffic through a computer running the software 'Fiddler Everywhere Pro', on a desktop running Windows 11 Pro. All of the apps tested utilize TLS/1.2 for encryption and a trusted root certificate was installed on the iOS device to intercept the traffic and decrypt the TLS connections.

Traffic from each of the apps was collected by using each app separately from one another and then saving the related session to an appropriate file name for analysis at a later stage. While advertising information and Apple data were collected, this was not analyzed as was out of scope for this research. Figure 1 outlines the device setup for the packet capture of network traffic.

4.3 OSINT and Trilateration

OSINT techniques can be employed on dating sites just like any other social media site although it is noted that privacy settings are available to restrict the amount of information a user displays. Depending on the information a user provides, this can be used to form searches on other sites, for example, a username or profile picture may be

used in other places on the internet providing additional information about the subject. In this research, a process is outlined of what can be searched for, however, the testing of this is in no way comprehensive as the user data is generated to ensure it does not link to a real-life person. This means that this method cannot be tested accurately unless it is used against another profile, noting that in some cases investigators may be attempting to determine whether a profile is fake, and OSINT techniques may assist in supporting this belief. Various tools are available to investigators when conducting OSINT and these may be commercial or free and may be user-friendly e.g., entering a name on a website, or reasonably technical e.g., utilizing an API to conduct a query. In this research, the use of OSINT will be used to complement the other types of data that can be collected through the other methods employed in this testing [38, 39].

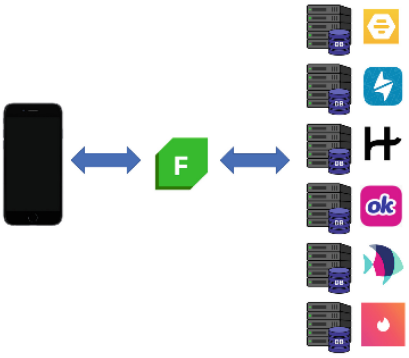

Fig. 1. Packet Capture topology.

Trilateration, in use with Dating Apps, has been around for several years with one of the first applications of this coming from a security researcher in 2014 [40]. The method is based on the premise that if you can obtain three distances (ideally 120 degrees apart from one another) from a location, then by measuring the distances to the location and plotting this information, you would be able to determine their location down to a small area.

Figure 2 is an example of trilateration in use. A point is identified in the vicinity of Tyrone, Ireland and three locations are selected around that location with their latitude and longitude positions recorded and their distances (radius of the circle) measured to that point, in this example these are:

Lat 54.5884163, Long -7.1608755 - radius 3716.81m.

Lat 54.5825294, Long -7.0652196 - radius 3232.85m.

Lat 54.6136177, Long -7.1034742 - radius 1671.31m.

The points on this map can be represented in various ways e.g., Attacker 1, 2, 3, and corresponding Distance 1, 2, 3 with the Victim at the intersection of these points being referred to as V [29]. In this case, multiple locations can be selected changing from trilateration to multilateration.

Fig. 2. An example of trilateration in use.

4.4 Forensic Analysis of Mobile Phone

Once all testing of the iPhone was complete, the phone was forensically acquired using a Cellebrite 4PC (Version 7.56.0.282). Databases for each of the apps were obtained or manually parsed out for analysis following the extraction.

4.5 Backups of Mobile Phone

For the iOS device, data was obtained using an iTunes backup using a method similar to the one proposed in [10], however, several changes in how and where the data was stored were noted.

In Windows 10, the iTunes backup was stored in the following path:

```
"%systempartition%\Users\%username%\Apple\MobileSync\Backup\"
```

The backup folder for the device is created using the device's Unique Device Identifier, or UDID, and is either a 40-character alphanumeric string on iPhone X model phones and below, or a 25-character string on models released after the Model X e.g., Model XS, etc. [41].

Within the backup folder is a series of folders labeled `00` through to `ff` which contain data backed up from the phone in a series of formats including, plist*,.sqlite,* and*.db*. These files are not provided extensions in the backup folders but are referenced from the *'Manifest.db'* database in the root of the directory.

The *Manifest.db* file references one main table *'Files'* and within that are three main columns of interest which are: *fileID, domain,* and *relativePath.* There are several domains contained within the backup including *AppDomain* (used for applications), *CameraRollDomain* (used for media files), *HomeDomain* (used for phone preferences, notifications, etc.) which all the files/folders 'belong'. The *relativePath* is the path to the file.

The *fileID* contains a SHA-1 hash of the domain and *relativePath* with the first two alphanumeric characters referencing which folder the file will be located in, for example, an image labeled 'IMG_0001.JPG' would be listed in

the Camera Roll Domain and, in this case, has the path: `CameraRollDomain-Media/DCIM/100APPLE/IMG_0001.JPG` and, as shown in Fig. 3, has a SHA-1 hash of *343e26971dfe9c395c425c0ccf799df63ae6261e*. This file will then be located in the folder `'34'` and can be opened with any type of picture viewer.

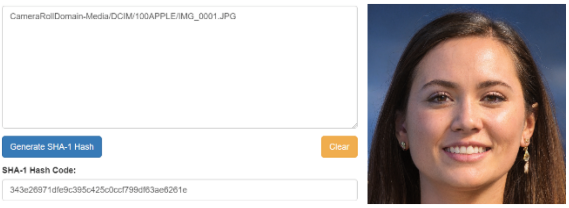

Fig. 3. IMG_0001.JPG and its SHA-1 hash.

Table 4 identifies the SQLite databases for the different dating apps being examined including the SHA-1 hashes of each of these path names. Table 5 describes more details on tables and the potential evidence of relevant databases.

Table 4. SQLite databases for the different dating apps

Apps	Databases/.plist files with SHA-1 hash
Bumble	AppDomain-com.moxco.bumble-Library/Preferences/com.moxco.bumble.plist SHA-1: d1387f814159b7030604610a7d02db295be3c244
happn	AppDomain-fr.ftw-and-co.whoozer- Documents/hdata.db SHA-1: 086ad83172abb9c7121862ced1a34748cb168166
Hinge	AppDomainGroup-group.co.hinge.mobile.ios.notification-extensions-Library/Preferences/group.co.hinge.mobile.ios.notification-extensions.plist SHA-1: 1bc170a7d2ee2fdc871d8982894b5c967f298c4a
OkCupid	AppDomain-com.okcupid.app-Documents/persistenceFolder/Converstions SHA-1: 2ad036b058851630675c252579df11e8b83e2112
Plenty Of Fish	AppDomain-com.pof.mobileapp.iphone-Library/Preferences/com.pof.mobileapp.iphone.plist SHA-1: 8e07086fcdbf37c1121b49c08fd10e1bf5dc3b8c AppDomainGroup-group.com.pof.mobileapp-POFNotifications.sqlite SHA-1: 0c3b8ca9b9c754361bbee4f7834ef40a1ef15fbd
Tinder	AppDomain-com.cardify.tinder-Library/Application Support/Tinder/Tinder2.sqlite SHA-1: bd881d082294367de00a97791cbf3741481c3466

5 Description of Results

From the capture of network traffic, examination of backups, and forensic acquisition of the mobile device, a large number of artifacts were obtained that could be used to identify another user using a dating app. The same process was completed on the six dating apps and showed that, although the individual apps may collect and store information differently, significant information could still be obtained. Table 6 provides a summary of some of the information that can be collected from utilizing the process above with various results obtained depending on the app and how the developers implemented security and privacy controls.

Table 5. Databases and tables with potential evidence for the different dating apps

Apps	Databases/.Plist files	Tables	**Potential Evidence**
Bumble	AppDomaincom moxco.bumble-Library/Preferences/com.moxco.bumble.plist	AppsFlyerFirstInstallDate AppsFlyerUserId Com.badoo.store_review_events.cold.launch	Install date of app User ID of the app Last 10 launches of the app including appVersion and date
happn	AppDomain-fr.ftw-and-co.whoozer- Documents/hdata.db AppDomain-fr.ftw-and-co.whoozer- Documents/Voice Messages	ZFLHPConversation ZFLHPDevice ZLHPProfileItem Audio Files with hexadecimal file name	Creation timestamp, Identifier No.s Lat/Long, Altitude, Location Accuracy Current Distance from me, Profile About Audio Files sent/received between users
Hinge	AppDomain-co.hinge.mobile.ios- Library/Application Support/HingeChat.sqlite AppDomainGroup-group-co.hinge.mobile.ios.notifications-extensions-Library/Preferences/co.hinge.mobile.ios.notification-extensions.plist	ZChatDBO ZChatMessageDBO X-App-Version X-Device-Model X-Device-Region	Participant ID's Identifier for Users, message text, sender/receiver The version of the App used Model of the phone used Region of the world device was used

(*continued*)

Table 5. (*continued*)

Apps	Databases/.Plist files	Tables	**Potential Evidence**
OkCupid	AppDomaincom okcupid.app-Library/Preferences/com.okcupid.app.plist AppDomain-com.okcupid.app-Documents/persistenceFolder/conversations AppDomain-com.okcupid.app-Documents/persistenceFolder/conversationThread3189043646602928958-V3	AppsFlyerInstallDate AppsFlyerUserId Id Age, Location Username, primaryImage lastMessageDate, isOnline Text	Install date of app User ID of the app Identification number of matched user Age of matched user, Location of matched user Username of the match, Primary linked image Last message date, Whether the user is online Message text sent/received from the user
Plenty Of Fish	AppDomainGroupgroup com.pof.mobileapp-POFNotifications.sqlite AppDomain-com.pof.mobileapp.iphone-Library/Preferences/com.pof.mobileapp.iphone.plist	ZGroupHash ZMessageID AppsFlyerUserId kPOFThumbnailCacheMeetMeKey	Hash of group Message Identification User ID of the app Thumbnails of recent views and matches
Tinder	AppDomain-com.cardify.tinder-Library/Application Support/Tinder/Tinder2.sqlite AppDomain-com.cardify.tinder-Library/Preferences/com.com.cardify.tinder.plist AppDomain-com.cardify.tinder-Documents/Idonotlikegreeneggsandham.txt	ZContactCard, ZUser, ZMatch, ZMessage, ZPhoto, ZUser Profile Email, Install Date, UserID Item 369, 946, 949	Phone Number of User, Location Proximity, User accounts interacted with, message IDs, Message Text, Type of message, ImageURL, reference for user images Email, Install Date, and UserID Job Title, Lat/Long of User, Email Address

Bumble and Plenty of Fish provided the least amount of information with device information, and information on the user being captured, however, there was little information obtained about the other user, except for some messaging gifs (Bumble), profile images, and the Encryption Key (Plenty Of Fish). Messaging was able to be collected from Hinge, OkCupid, and Tinder in at least one of the three methods (packet capture, forensic acquisition, or backup) as well as device information and various other user locations, however, no trilateration attacks could be used against these apps.

The most information was able to be obtained from happn, mainly due to how 'matches' are made with the app which requires both users to pass each other in the same location, this enables trilateration to be used effectively against other users. An extensive amount of profile data was also able to be obtained, and this included the capture of profiles that the user did not interact with.

While OSINT collection was limited by the use of fake profiles in this research, and not tested on real-life profiles, all of the apps tested provided opportunities to use OSINT techniques to obtain further information about the user. Most apps provided methods to obtain profile information that could then be used to geographically locate a person.

Updates to the various apps to include certificate pinning, and server-side rounding of the lat/long sent to the users' device effectively prevented the capture of sensitive content (e.g., messaging), or trilateration of users, however, this was not implemented consistently across all apps allowing a large amount of information to be obtained.

6 Evaluation and Discussion of Results

After the analysis of the six dating apps selected was completed, several observations were noted, including that app developers/providers have been slow to implement security and privacy measures although some have made improvements when comparing previous research. There were a large number of artifacts that could be recovered through the various methods employed above. Utilizing the other users' photos, location, and in some cases, profile information, and messaging, would enable investigators to potentially identify a real-life user utilizing these dating apps. Due to the variety of crimes that can be facilitated through the use of these apps, it is important for those tasked with protecting the community and investigating crimes to have all the tools at their disposal.

This research ultimately showed that through the combined use of different types of data that can be obtained while a user is using a dating app, a person's identity could, in some cases, be quickly identified with the use of law enforcement databases and other resources. Due to the evolving state of the Internet, the artifacts that have been obtained in this research are likely to change in a short space of time. The process used to obtain the various pieces of data that could assist investigators will not be substantially affected by this evolution however, and could be used in the future to identify victims, witnesses, and offenders committing crimes facilitated by the use of dating apps.

Analysis of mobile devices in the field of forensics has long been established as an important phase of investigations, especially when it comes to any offending that has an online component.

Traditionally, a mobile device will be seized as evidence and extraction completed whilst the device is disconnected from any available network, typically at a law enforcement building. While this approach has been shown to provide an extensive number of

results when it comes to dating applications, these devices may not always be accessible at certain stages of an investigation and other methods may need to be employed to gain data. In this paper, information such as location, usernames, and user images, can be obtained from a network traffic capture and is a useful tool to consider, if it could be used. It is important to be aware of these opportunities, as a focus of evidential law enforcement investigations is often to obtain the most amount of relevant data possible. It is clear from the results found throughout this paper that as technology evolves, so does the public's interest in the growing desire for privacy. The companies that own these dating applications appear to be constantly developing further features and privacy functions. This can be determined by comparing the results found in this paper to prior work, such as [22] where it was found that Tinder provided a larger amount of data than it does today, such as geolocation data and full usernames.

This paper focused on combining approaches across multiple different applications, comparing them against each other, as well as methodically gathering data from mobile device extractions, backups, OSINT and network packet captures. This rounded approach also provides a process to approach investigations where dating apps have been, or are being used, as compared to previous literature that focused primarily on one specific application, or one technique. This assists both the law enforcement community and the digital forensics community.

Mobile devices can store a significant amount of information due to their ever-increasing storage capacity, with some now out-performing computers. This means that users store so much personal data, that there is a need for it to be backed up, should it be lost, destroyed, or accidentally erased. Due to this, further forensic opportunities are made available for dating apps including artifacts that can be located in a user's mobile device backup on their computer, that are no longer present on a mobile device.

The results outlined in this paper around the mobile device backups vary between each dating application, however, each found valuable insight and provided another avenue to locate data throughout the process of attempting to identify another user using the dating apps.

Further to the backup data proving to be a useful source of information, these findings demonstrate that the network packet capture can provide incredibly useful information too. Through the packet capture of the application 'OkCupid', the chat history between test user accounts was obtained. This data was not available in the forensic analysis of the mobile device itself, however, was available in the backup of the mobile device. It should also be noted that when considering the findings of this research and applying them to investigations in the future, it can be dependent on the level of extraction obtained from specific mobile devices which can have a direct result on how much data can be obtained. For example, a significant amount of the findings analyzed from the dating applications came from a mobile device extraction that was able to obtain database files. In comparison, this may not be possible with a lower level of extraction, particularly when it comes to application data.

The network packet capture was made possible by having direct access to the testing mobile device, although this was not necessary, and being able to install a root certificate which enabled decryption of the HTTPS traffic through the software Fiddler. This approach was appropriate for this setting and showed proof-of-concept however, as

Table 6. Summary of findings for the different dating apps

Apps	Packet Capture	OSINT and Trilateration	Forensic Analysis of Mobile Phone	Backup of Mobile Phone
Bumble	User information including device details, phone number, authentication codes, country, gender, and age were captured however little on other users. GIFs were captured but no messaging	Trilateration has been widely publicized and has been prevented by implementing rounding users' distance on the server, this meant location was not accurate. OSINT is only related to profile images and settings	A large amount of user data was able to be obtained including username, location ID, LastLocation, and profile information. No messaging data or user profile information of other users was able to be obtained	Backup of the Bumble app recovered the Install Date, UserID, and last 10 launches of the App (including app version)
happn	A large amount of information was captured including users that were only viewed, this included: user-agent string, country, gender, date of birth, email, rejected/ accepted profiles, lat/long, text, GIFs, and audio files	As happn uses locations where people have crossed paths the location is known. Further trilateration can be done on a user who has selected 'always on' for location services in the app. Various OSINT techniques could be used to identify a user	Similar to the packet capture, a large amount of information was able to be accessed including voice messages, URL links to all images (viewed or interacted with), and profile traits e.g., smoker, non-smoker. No messages or profile information could be accessed via this method	The iTunes backup contained the same information as the phone extraction however included messages sent/received as well as user device information including lat/long etc.
Hinge	A moderate amount of data was obtained however little information on other users, this included device details, user-agent string, country, gender, first name, email, and age	Trilateration of users was not possible due to only the selected city of other users was presented preventing any form of attribution from being made. OSINT is only related to profile images and settings	A large amount of user data was able to be obtained including the install date of the app, OS version, Country, model of phone, and session end date/time. Location ID, LastLocation, and profile information	The Hinge database contains information about chat messages sent/received, message and sender identifiers, timestamps, voice calls, language, region, device platform, and model as well as likes
OkCupid	Other users' details were provided to the user without any interaction, this included: ID, username, display name, location, all profile images, and information. Full chat history could also be obtained via packet capture	The same location information is provided as Hinge which would prevent trilateration attacks. A 'nearby' feature is provided showing profiles of users within a certain distance of the user. This could be used to identify a small area of where a user may be	Extraction of the OkCupid app identified a small amount of user data including app install time, language, and region. No chat history or images were obtained	The conversation folder contains a 'Comma Separated Value' view of previous matches recorded by the app. Relevant information for an investigator includes: the ID of the profile, age, first (display) name, username, primary profile image, and last online time

(*continued*)

Table 6. (*continued*)

Apps	Packet Capture	OSINT and Trilateration	Forensic Analysis of Mobile Phone	Backup of Mobile Phone
Plenty Of Fish (POF)	A small amount of data was obtained on the use of the application however little information on other users. The information included data about the user's device and email address	POF rounded their location to one decimal place meaning that the approximate location of the other user is within 10 km of the location. This radius is typically greater than the location presented in the app	A large amount of user data was obtained, similar to Hinge, and included: the install date of the app, User ID, User agent string, and URL links to cached images. The Encryption Key along with the iTunes backup file name was also obtained	The POF files contain information including UserIDs of both parties, sender/receiver identifier, creation date, message identifier, type of notification, and thumbnails of recently viewed profiles
Tinder	Tinder provided a moderate amount of data on both profiles including profile details, pictures, all messaging content, phone number, and Lat/Long of the user (within 1 km approx.)	Trilateration within Tinder is no longer possible because many articles highlight the privacy risks of providing location data. No location information was obtained on the other profile thereby preventing trilateration	User information including Install timestamp, latest 'ping' with lat/long down to 13 decimal places, Interests, location information (Country and City, email address, full message history, as well as extensive user profile information	Tinder backup information contains a large amount of data useful for investigators, this includes user profile information, distance from the user, bio of the user, first name, and other profile information

mentioned within this paper consideration should be given to an individual's legislation, and policy constraints, if this were to be applied in a real-world scenario.

7 Conclusion and Future Direction

A comprehensive study of six dating apps was conducted to develop a process that investigators can use to obtain information that will assist their cases if an offender is unknown, but has used dating apps. The process was developed using a device running iOS device however this process does not rely on a particular type of hardware or Operating System and could easily be transitioned to another model of Apple or Android device as the focus is on the app data rather than the platform.

Due to the types of information that can be obtained through phone extractions, packet capture, and examination of backups, an investigator can select what may be available to them in their current circumstances and how that data may identify persons of interest and suspects.

The additional use of OSINT [38, 39] and trilateration to pinpoint where someone may be, provides investigators with the ability to use that information, along with their law enforcement data, to identify those people more easily. Although one app by itself may not provide sufficient information, it has been outlined in this paper that users typically use more than one app at a time which enables investigators to combine data from several apps, along with other information they have access to, to identify, or assist in identifying other users of the apps they need to speak to in relation to a crime.

Future research into this area could be conducted on methods to identify the same user across multiple different social media and dating apps, whether through data fingerprinting, facial recognition, or another method. As authentication tokens were able to either be captured through packet capture, or accessed through a phone extraction, research could be done on the feasibility of decrypting traffic without using a trusted root certificate [42].

References

1. Rosenfeld, M.J., Thomas, R.J., Hausen, S.: Disintermediating your friends: how online dating in the United States displaces other ways of meeting. Proc. Natl. Acad. Sci. **116**(36), 17753–17758 (2019). https://doi.org/10.1016/j.chb.2004.11.013
2. Potarca, G.: The demography of swiping right. An overview of couples who met through dating apps in Switzerland. PloS One **15**(12), e0243733 (2020). https://doi.org/10.1177/2056305116641976
3. Zhu, C.: Using dating apps: the change in dating practices and attitudes toward monogamous serious relationships among Chinese young adults (2021). https://www.researchgate.net/publication/355378118
4. Brown, A.: Lesbian, gay and bisexual online daters report positive experiences – but also harassment. Pew Res. Center (2020). https://www.pewresearch.org/fact-tank/2020/04/09/lesbian-gay-and-bisexual-online-daters-report-positive-experiences-but-also-harassment/. Accessed 04 Dec 2022
5. Picciani, E.: He sexually assaulted her after they met on bumble. Then she saw him on tinder. Then hinge. Colombia Journalism Investigations (2020). https://www.propublica.org/article/he-sexually-assaulted-her-after-they-met-on-bumble-then-she-saw-him-on-tinder-then-hinge. Accessed 15 Dec 2022
6. Hurley, S., Leask, A.: Grace Millane murder: tinder messages with her killer revealed. NZ Herald (2019). https://www.nzherald.co.nz/nz/grace-millane-murder-tinder-messages-with-her-killer-revealed/Y67WCAJFSIOLKBXZEY3244NLXI/. Accessed 11 Dec 2022
7. Patsakis, C., Zigomitros, A., Solanas, A.: Analysis of privacy and security exposure in mobile dating applications. In: Boumerdassi, S., Bouzefrane, S., Renault, É. (eds.) MSPN 2015. LNCS, vol. 9395, pp. 151–162. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-25744-0_13
8. Finklea, K.: Law enforcement and technology: using social media. Congressional Research Service (2022). https://sgp.fas.org/crs/misc/R47008.pdf. Accessed 14 Dec 2022
9. Interpol: National Cybercrime Strategy Guidebook (2021). https://www.interpol.int/content/download/16455/file/Cyber%20Strategy%20Guidebook.pdf. Accessed 13 Dec 2022
10. De Busser, E.: The digital unfitness of mutual legal assistance. Secur. Hum. Rights **28**(1–4), 161–179 (2018). https://doi.org/10.1163/18750230-02801008
11. Barrada, J.R., Castro, A.: Tinder users: sociodemographic, psychological, and psychosexual characteristics. Int. J. Environ. Res. Public Health **17**(21), 8047 (2020). https://doi.org/10.3390/ijerph17218047
12. Farnden, J., Martini, B., Choo, K.-K.R.: Privacy risks in mobile dating apps. arXiv preprint arXiv:1505.02906 (2015). https://doi.org/10.48550/arXiv.1505.02906
13. Thantilage, R., Le-Khac, NA.: Retrieving E-dating application artifacts from iPhone backups. In: Peterson, G., Shenoi, S. (eds.) Advances in Digital Forensics XVI. DigitalForensics 2020. IFIP Advances in Information and Communication Technology, vol. 589, pp. 215–230. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-56223-6_12

14. Lee, J.: Online dating app usage data study. Healthy Framework (2022). https://healthyframework.com/dating/online-dating-app-usage-data-study/. Accessed 14 Dec 2022
15. O'Flaherty, K.: Five dating app dilemmas answered by experts. The Guardian (2022). https://www.theguardian.com/lifeandstyle/2022/jul/10/five-dating-app-dilemmas-answered-by-experts. Accessed 13 Aug 2022
16. Stoicescu, M.-V., Matei, S., Rughinis, R.: Sharing and privacy in dating apps. In: 2019 22nd International Conference on Control Systems and Computer Science (CSCS), pp. 432–437. IEEE (2019). https://doi.org/10.1109/CSCS.2019.00079
17. James, J.I., Gladyshev, P.: A survey of mutual legal assistance involving digital evidence. Digit. Investig. **18**, 23–32 (2016). https://doi.org/10.1016/j.diin.2016.06.004
18. Price, H.: Dating apps accused of ignoring sexual assault. BBC Three (2022). https://www.bbc.co.uk/bbcthree/article/aeadcc6c-3d3a-4c75-9316-079c1d70b2d3. Accessed 05-Dec 2022
19. Gregory, K.: A predator kept targeting victims on Tinder for years. Why wasn't he stopped sooner? ABC News (2020). https://www.abc.net.au/news/2020-02-07/dating-app-sexual-assault-predator-was-using-dating-profiles/11931586. Accessed 16 Dec 2022
20. Sansurooah, K., Keane, B.: The spy in your pocket: smartphones and geo-location data (2015). https://doi.org/10.4225/75/57b3fb68fb88e
21. Reitman, R.: Six heartbreaking truths about online dating privacy. Electronic Frontier Foundation (2012). https://www.eff.org/deeplinks/2012/02/six-heartbreaking-truths-about-online-dating-privacy. Accessed 05 Dec 2022
22. Kim, K., Kim, T., Lee, S., Kim, S., Kim, H.: When harry met tinder: security analysis of dating apps on android. In: Gruschka, N. (ed.) NordSec 2018. LNCS, vol. 11252, pp. 454–467. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03638-6_28
23. Mata, N., Beebe, N., Choo, K.-K.R.: Are your neighbors swingers or kinksters? feeld app forensic analysis. In: 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), pp. 1433–1439. IEEE (2018). https://doi.org/10.1109/TrustCom/BigDataSE.2018.00199
24. Knox, S., Moghadam, S., Patrick, K., Phan, A., Choo, K.-K.R.: What's really 'Happning'? A forensic analysis of Android and iOS Happn dating apps. Comput. Secur. **94**, 101833 (2020). https://doi.org/10.1016/j.cose.2020.101833
25. Department of Defense: DOD Open Source Software FAQ. Office of the DoD CIO (2021). https://dodcio.defense.gov/open-source-software-faq/. Accessed 16 Dec 2022
26. Phang, J.: Cybersecurity for noobs (Part 2) — staying safe with online dating using OSINT (2021). https://medium.com/geekculture/cybersecurity-for-noobs-part-2-staying-safe-with-online-dating-using-osint-fa9ef7a7cbff. Accessed 16 Dec 2022
27. Ninovic, V.: It's a Match! Dating Apps and SOCMINT (2022). https://intel-inquirer.medium.com/its-a-match-dating-apps-and-socmint-2c05c44e9590. Accessed 15 Dec 2022
28. Huang, H., Gartner, G., Krisp, J.M., Raubal, M., Van de Weghe, N.: Location based services: ongoing evolution and research agenda. J. Location Based Serv. **12**(2), 63–93 (2018). https://doi.org/10.1080/17489725.2018.1508763
29. Hoang, N.P., Asano, Y., Yoshikawa, M.: Your neighbors are my spies: location and other privacy concerns in GLBT-focused location-based dating applications. In: 2017 19th International Conference on Advanced Communication Technology (ICACT), pp. 851–860. IEEE (2017). https://doi.org/10.48550/arXiv.1604.08235
30. Nelson, B., Phillips, A., Steuart, C.: Guide to Computer Forensics and Investigations: Processing Digital Evidence. 6th edn. Cengage Learning, Boston (2018)
31. Sharma, B.K., Yadav, V., Purba, M.K., Sharma, Y., Kumar, V.: Challenges, tools, and future of mobile phone forensics. J. Positive Sch. Psychol. 4463–4474 (2022). https://www.researchgate.net/publication/360355132_Challenges_Tools_and_Future_of_Mobile_Phone_Forensics

32. Hutchinson, S., Shantaram, N., Karabiyik, U.: Forensic analysis of dating applications on android and iOS devices. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 836–847. IEEE (2020). https://doi.org/10.1109/TrustCom50675.2020.00113
33. Cahyani, N.D.W., Choo, K.K.R., Ab Rahman, N.H., Ashman, H.: An evidence-based forensic taxonomy of Windows phone dating apps. J. Forensic Sci. **64**(1), 243–253 (2019). https://doi-org.ucd.idm.oclc.org/10.1111/1556-4029.13820
34. O'Dea, S.: Number of smartphone subscriptions worldwide from 2016 to 2027. Statista (2022). https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. Accessed 07 Dec 2022
35. Boyles, J., Smith, A., Madden, M.: Privacy and data management on mobile devices. Pew Res. Center **4**, 1–19 (2012). https://www.pewresearch.org/internet/2012/09/05/privacy-and-data-management-on-mobile-devices/. Accessed 07 Dec 2022
36. Google: back up or restore data on your Android device (2022). https://support.google.com/android/answer/2819582. Accessed 07 Dec 2022
37. Apple: Backup methods for iPhone, iPad, and iPod touch (2022). https://support.apple.com/en-us/HT204136. Accessed 16 Dec 2022)
38. Bielska, A., Kurz, N., Baumgartner, Y., Benetis, V.: Open Source Intelligence Tools and Resources Handbook. i-intelligence, Winterthur (2020). https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf. Accessed 11 Aug 2022
39. Larsen, O.H., Ngo, H.Q., Le-Khac, N.A.: A quantitative study of the law enforcement in using open source intelligence techniques through undergraduate practical training. Forensic Sci. Int. Digit. Invest. **47**, 301622 (2023). https://doi.org/10.1016/j.fsidi.2023.301622
40. Veytsman, M.: How I was able to track the location of any Tinder user (2014). https://blog.includesecurity.com/2014/02/how-i-was-able-to-track-the-location-of-any-tinder-user/. Accessed 11 Aug 2022
41. Le-Khac, N-A., Choo, KK.R.: Database forensics. In: A Practical Hands-on Approach to Database Forensics. Studies in Big Data, vol. 116, pp. 3–26. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-16127-8_2
42. Schipper, G.C., Seelt, R., Le-Khac, N.-A.: Forensic analysis of Matrix protocol and Riot.im application. Forensic Sci. Int. Digit. Invest. **36**, 301118 (2021). https://doi.org/10.1016/j.fsidi.2021.301118