Retrieving E-Dating Application Artifacts from iPhone Backups

Ranul Thantilage, Nhien-An Le-Khac

Chapter 12

RETRIEVING E-DATING APPLICATION ARTIFACTS FROM iPHONE BACKUPS

Ranul Thantilage and Nhien-An Le-Khac

Abstract Criminal activities are widely facilitated by online means; so are sex crimes. Online dating, also referred to as e-dating, enables people to get in touch with potential romantic partners through digital means. Unfortunately, sex criminals also exploit online dating platforms to find victims.

Several e-dating applications have been developed for computers and mobile phones, but few, if any, efforts have focused on retrieving evidence from e-dating applications. This chapter describes forensic methods for retrieving evidence from two popular e-dating applications – Tinder and Coffee Meets Bagel – by examining iPhone backups created via iTunes on Windows and Macintosh personal computers.

Keywords: iPhone forensics, evidence retrieval, e-dating applications

1. Introduction

Many crimes, including sex crimes, are facilitated by online activities. Online dating applications, also referred to as e-dating applications, enable people to interact with potential romantic partners via digital means. Unfortunately, sex criminals also exploit online dating applications to find victims.

One such application is Tinder, which is widely used by young individuals. Tinder's terms of use forbid users below the age of 18 from using the application [21]. However, it is common for young teens to register with the application by faking their ages. This makes them vulnerable to sexual predators.

According to a 2016 report by the National Crime Agency of the United Kingdom [15], online-dating-related rape increased 450% during the previous six years. Meanwhile, the number of e-dating application

users has increased significantly. According to 2020 usage statistics [13], Tinder has more than 57 million registered users and processes approximately 1.6 billion swipes every day.

Another e-dating application, Coffee Meets Bagel, has more than seven million installs [19]. The app received international coverage on Valentine's Day 2019 after it suffered a data breach affecting around six million users [6]. The stolen data was offered on the dark web for $20,000 in Bitcoin [17].

Millennials and post-millennials use smart devices more than any other population age group, with iPhones being the most popular devices. Therefore, this research focuses on iPhone-based usage of Tinder and Coffee Meets Bagel. iPhone forensics is a well-established area of digital forensics, but little work has concentrated on extracting evidence from iPhone backups. This is a key gap because investigators may not have access to the smart devices of criminals and/or victims; in fact, they may only know the names of the individuals.

Since it is common to backup iPhone data on Windows and Macintosh computers, investigators could access these computers at the criminals' and/or victims' homes, and proceed to examine the backups to find evidence of criminal activity. Indeed, iPhone backups on personal computers contain considerable amounts of data related to e-dating application usage.

This research concentrates on evidence retrieval from iPhone backups created by iTunes. The main contributions are forensic acquisition and analysis of artifacts from Tinder and Coffee Meets Bagel apps in iPhone backups on personal computers.

2. Related Work

As Internet usage increases around the globe, so does online dating. A 2002 research study reported that 1,458 of 1,836 (79.4%) of surveyed Internet users in Sweden used the Internet for sexual purposes [5]. A factor analysis study in 2010 revealed that online dating application users were primarily interested in seeking partners and accessing erotica [4].

Van Voorst et al. [22] have discussed the risks associated with using mobile apps to meet potential partners. They also described the forensic acquisition and analysis of evidence from an Instant Messaging within a Virtual Universe (IMVU) 3D application, which has been exploited by criminal entities to commit a variety of offenses.

Newett et al. [16] researched the intimate lives of Australians aged 18 to 30 years. They also studied how the Tinder platform contributed to intimate outcomes. Full 91.92% of the respondents were frequent Tinder

users. While sex was the least motivating factor for female respondents, it was the third most important factor for male respondents. Ranzini and Lutz [18] noted that women use Tinder more for friendship and self-validation whereas men use it hooking up/sex, traveling and forming relationships.

Feltz [11] researched the security of Tinder and demonstrated that it has significant vulnerabilities as a geosocial mobile app. In particular, attackers can use methods such as trilateration to pinpoint the exact physical locations of users. Other security researchers have found vulnerabilities in Tinder; many of the vulnerabilities have been addressed, but some persist.

Farnden et al. [10] have conducted a study of geosocial apps. They analyzed popular proximity-based dating applications to determine the types of data that can be recovered. An important result was that 50% of the apps supported the forensic recovery of chat messages.

Heffernen [12] has described a forensic analysis of an early version of the Tinder app (version 2.1.0) on an iPhone 4S running iOS 6.1.3. The iPhone Analyzer tool was used to extract Tinder's SQLite database file. Analysis of the database tables revealed that very few artifacts were present.

Several researchers have focused on mobile device forensics and its important role in investigations [1, 9]. However, the vast majority of work has concentrated on extracting data from devices. For example, Cheema et al. [3] have analyzed the iOS filesystem to identify directories and files that could be relevant to traditional criminal investigations. Likewise, the iOS forensics work by Drish [7] deals mainly with data acquisition from devices. Epifani and Stirparo [8] discuss forensic analyses of iOS messaging apps; they showed how application data is separated from its bundles, and also investigated the directory structure and deleted data.

Baggili et al. [2] have developed a tool named LiFE that conducts forensic analyses of iOS backups. The tool analyzes device information, call history, voice messages, GPS locations, conversations, notes, images, address books, calendar entries, SMS messages, Facebook data and email.

A review of the literature reveals that research has largely concentrated on independent platforms and applications. Very little research has focused on iPhone backup forensics and what has been done involves general applications, not e-dating applications. Moreover, research on e-dating applications has studied vulnerabilities and usage statistics. In contrast, the research described in this chapter concentrates on the retrieval of Tinder and Coffee Meets Bagel artifacts from iPhone backups created by iTunes on Windows and Macintosh personal computers. This

is important because investigators often do not have access to the physical iPhones, but they could access personal computers at the criminals' and/or victims' homes, and conduct forensic analyses of iTunes backups to find evidence of criminal activity.

3. Challenges

Mobile devices are routinely encountered in criminal investigations. Lutes and Mislan [14] identify several challenges related to mobile device forensics. These include diverse carriers and manufacturers, data preservation, power and data connectors, operating systems, communications protocols and security mechanisms.

Compared with other mobile device platforms, iOS device forensics is more challenging because iOS devices employ full drive encryption as well as protections such as per-file keys and backup encryption (if enabled). Furthermore, iOS is a proprietary encrypted operating system.

4. Evidence Extraction Methods

This section presents the methods used to extract e-dating application artifacts from iPhone backups on Windows and Macintosh personal computers.

iTunes is used to create iPhone backups on personal computers. Backups are stored at different locations depending on the operating systems on the personal computers. For example, the Windows 10 operating system stores the backup at:

```
%systempartition%\Users\%username%\AppData\Roaming\
    AppleComputer\Mobilesync\Backup\
```

In the case of a Macintosh operating system, the backup is stored as:

```
Users/%username%/Library/applicationsupport/
    MobileSync/backup
```

The backup folder is identified by a 40-digit SHA-1 hash value that is created from the unique device identifier (UID) of the iPhone. The file name is also encoded using a SHA-1 hash of the file path and file name.

The key to analyzing an iPhone backup is to identify the hash value of the required file. This requires the forensic practitioner to know the file name and file path (domain). Note that AppDomain is used for applications that are downloaded from the Apple App Store.

21	fa148e80e46580784ed1907d71b4cedfe5071a21	AppDomain-com.cardify.tinder	Libr
22	bd881d082294367de00a97791cbf3741481c3466	AppDomain-com.cardify.tinder	Libr
23	b50ed9ebfae9076641965008111c90ea5bfc56c0	AppDomain-com.cardify.tinder	Libr

(a) SHA-1 hash value in the `Manifest.db` file.

Original text	AppDomain-com.cardify.tinder-Library/Application
Original bytes	417070446f6d61696e2d636f6d2e63617264696679
SHA-1	bd881d082294367de00a97791cbf3741481c3466

(b) Computed SHA-1 hash value.

Figure 1. Verification of Tinder database SHA-1 hash values.

4.1 Tinder

Evidence related to Tinder is stored in an SQLite database. The database file is located at:

```
AppDomain-com.cardify.tinder-Library/
    ApplicationSupport/Tinder/Tinder2.sqlite
```

The hash value of the SQLite database file can be obtained by going through the `Manifest.db` file available in the root of the backup or by computing it using a SHA-1 hash generator.

Figures 1(a) and 1(b) confirm that the hash value for the file is:

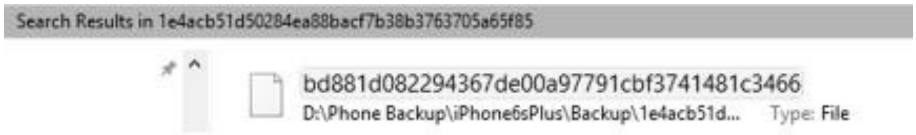
```
bd881d082294367de00a97791cbf3741481c3466
```

Searching for the hash value in the backup folder enables a forensic practitioner to identify and extract the SQLite file. Note that, at first glance, the file does not show an extension. However, the file type can be checked using `file tool/command` in Linux.

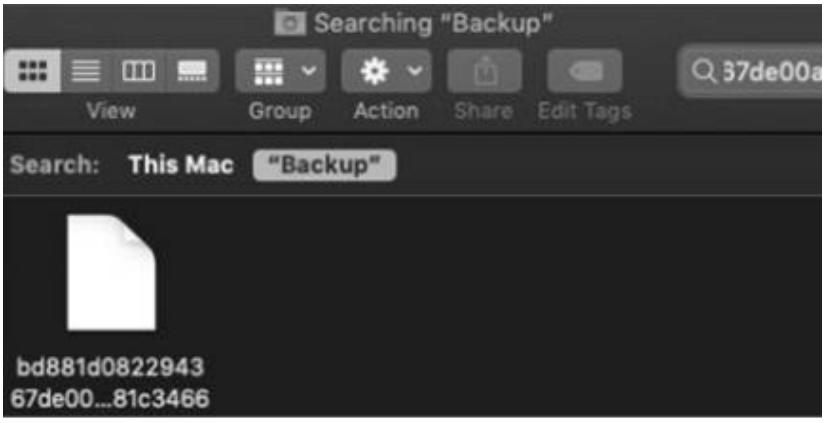
Figures 2(a) and 2(b) show the SQLite files retrieved using the hash values from Windows and Macintosh iTunes backups, respectively.

The hash values of the files are the same for each application. Therefore, a forensic practitioner should record the file hash values needed in investigations to save time by not repeating the steps.

The Tinder database contains more than 30 tables, many of which could provide important evidence in an investigation. The tables of spe-



(a) Windows iTunes backup.



(b) Macintosh iTunes backup.

Figure 2. Searching for the Tinder `SQLite.db` using the hash value.

cial interest are: ZMATCH, ZMESSAGE, ZPHOTO, ZPROCESSEDPHOTO, ZPROCESSEDVIDEO and ZUSER. Each table is linked using a database key (i.e., primary key). By writing appropriate queries, a forensic practitioner can link the tables to each other and gather a vast amount of data.

Table 1 shows the evidentiary data that can be retrieved from the Tinder SQLite database.

4.2 Coffee Meets Bagel

The method for retrieving evidentiary data from Coffee Meets Bagel (CMB) is similar to that used for Tinder. Coffee Meets Bagel also stores data in a SQLite database.

The database file is located at:

```
AppDomainGroup-group.com.coffeemeetsbagel.mainapp-
    CMBMobile.sqlite
```

The hash value of the SQLite database file can be obtained by going through the `Manifest.db` file available in the root of the backup or by computing it using a SHA-1 hash generator.

Table 1. Evidentiary data in the Tinder SQLite database.

Table	**Evidence**
ZMATCH	Match Timestamp Last Activity Timestamp User ID Match ID
ZMESSAGE	Match ID Timestamps From User ID Message ID Message Text
ZPHOTO	User ID Photo ID Image URL
ZPROCESSEDPHOTO	Photo ID Image URL
ZVIDEO	Photo ID Video URL
ZUSER	Match ID Birthdate Distance in Miles Tinder Bio First Name User ID Liked

Figures 3(a) and 3(b) confirm that the hash value of the database file is:

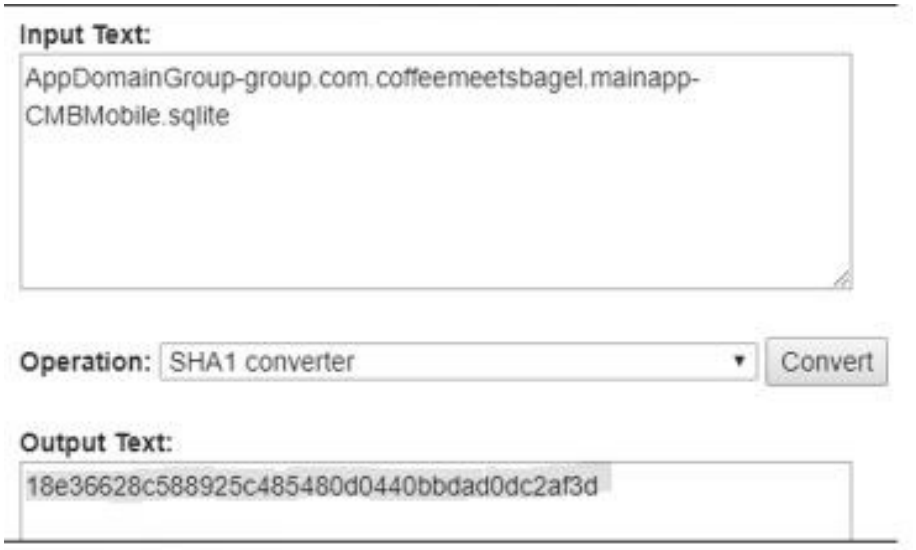
```
18e36628c588925c485480d0440bbdad0dc2af3d
```

Figure 4 shows that the hash value can be searched in the backup folder in Windows to retrieve the `SQLite.db` file.

The Coffee Meets Bagel database contains more than 10 tables, many of which could provide important evidence in an investigation. The tables of special interest are: ZBAGEL, ZCHATMESSAGECACHE and ZPROFILE. Each table is linked using a database key (i.e., primary key). By writing appropriate queries, a forensic practitioner can link the tables to each other and gather a vast amount of data.

Table 2 shows the evidentiary data that can be retrieved from the Coffee Meets Bagel SQLite database.

(a) SHA-1 hash value in the `Manifest.db` file.



(b) Computed SHA-1 hash value.

Figure 3. Verification of Coffee Meets Bagel database SHA-1 hash values.

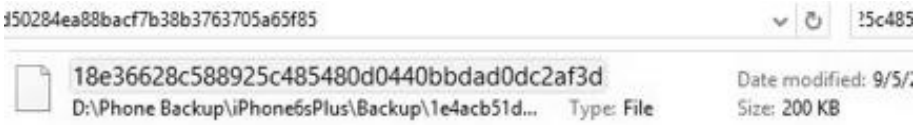


Figure 4. Searching for the Coffee Meets Bagel `SQLite.db` using the hash value.

Tables 1 and 2 demonstrate that timestamps and dates are retrieved in several instances. The timestamps are stored in the Apple Cocoa Core Data timestamp format, which corresponds to the number of seconds elapsed since `00:00, January 1, 2001 GMT`. These timestamps should be converted to a local time format.

Table 2. Evidentiary data in the Coffee Meets Bagel SQLite database.

Table	Evidence
ZBAGEL	Profile ID Created Timestamp Last Updated Timestamp
ZCHATMESSAGECACHE	Timestamp ID XMPP Message
ZPROFILE	User Age Personal Details (e.g., height) User Birthdate Last Updated Timestamp User Geolocation User City User Country User Bio User Employment Details User Ethnicity User Religion User First Name

5. Experimental Evaluation

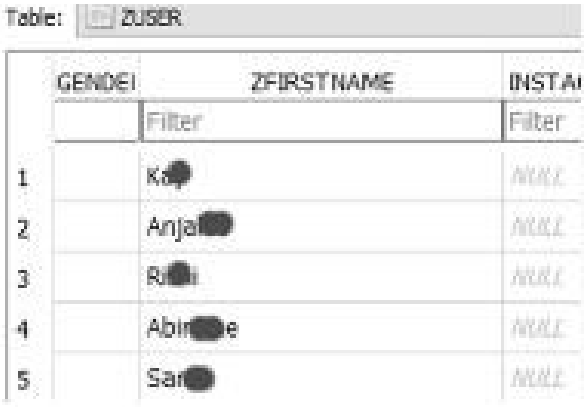
The proposed methods were tested using several iPhone models and iOS versions to create Windows and Macintosh backup files. The following are the specifications of the iPhones used in the experimental evaluation:

- **Device 1:** iPhone 6S Plus, iOS 11.4, 64 GB capacity.
- **Device 2:** iPhone 6, iOS 11.4, 16 GB capacity.
- **Device 3:** iPhone XS Max, iOS 12.3, 64 GB capacity.

The following iTunes software versions were employed:

- **iTunes Version 1 (Windows):** Version 12.6.1.25.
- **iTunes Version 2 (Windows):** Version 12.9.2.6.
- **iTunes Version 3 (Macintosh):** Version 12.9.2.5.

(a) User birthdate and bio information.



(b) User first name information.

Figure 5. User information extracted from the ZUSER table.

5.1 Tinder Evidence

Table 1 shows that considerable data pertaining to the Tinder application is stored in an iPhone backup. Therefore, a forensic practitioner can examine the personal computer of a suspect or victim to obtain evidence about online dating activities. This section discusses the evidentiary data that can be retrieved from the Tinder application.

Figure 5 shows the user birthdates, bios and first names that were extracted from the ZUSER table.

Figure 6 shows the message IDs and texts associated with matched users that were extracted from the ZMESSAGE table.

Figure 6. Message IDs and texts extracted from the ZMESSAGE table.

Figure 7 shows how the URLs of photographs can be retrieved from the ZPROCESSEDPHOTO table, along with a sample photograph. Note that portions of the images are covered or pixelated to preserve privacy.

5.2 Coffee Meets Bagel Evidence

Table 2 shows that considerable data pertaining to the Coffee Meets Bagel application is stored in an iPhone backup. An important feature of Coffee Meets Bagel is that geolocation information pertaining to users of the application can be extracted easily.

Figure 8 shows the personal information of users, including name, birthday, ethnicity, religion and geolocation data, that was extracted from the Coffee Meets Bagel backup file.

Figure 9 shows the exact location of a user obtained from geolocation data in the ZPROFILE table. Once again, portions of the screenshots are obfuscated for privacy reasons.

6. Conclusions

iPhone forensics is a well-established area of digital forensics, but little work has concentrated on extracting evidence from iPhone backups. This chapter has described forensic methods for retrieving evidence related to two popular e-dating applications – Tinder and Coffee Meets Bagel – by examining iPhone backups created via iTunes on Windows and Macintosh personal computers. Since it is common to backup iPhone data on Windows and Macintosh computers, investigators who

Table: ZPROCESSEDPHOTO

	H	ZIMAGEURL
		Filter
7		https://images-ssl.gotinder.com/5a0a6f1[redacted]/320x400_66d991cf-bf65-49b6-
8		https://images-ssl.gotinder.com/5ba2c09c5[redacted]320x400_17a6d344-9378-467
9		https://images-ssl.gotinder.com/564f8da[redacted]x172_f7ef0239-f7a2-42fd-8
10		https://images-ssl.gotinder.com/5b53de00[redacted]320x400_262343d5-02f2-4e8
11		https://images-ssl.gotinder.com/5b176975[redacted]0x800_e163a438-38e6-487

(a) Photograph URLs in the ZPROCESSEDPHOTO table.

(b) Photograph retrieved using a URL.

Figure 7. Photograph extracted using data in the ZPROCESSEDPHOTO table.

do not have access to user's iPhones could examine the backups to find evidence of criminal activity.

The experiments demonstrate that iPhone backups on personal computers contain considerable amounts of data related to e-dating application usage. By carefully analyzing the SQLite database of the backup folder, a digital forensic practitioner can obtain valuable information about interpersonal interactions conducted via the e-dating application. The recoverable evidence includes personal information, photographs, timestamps and conversation history from the Tinder and Coffee Meets Bagel apps, and, in the case of Coffee Meets Bagel, valuable geolocation data about app users as well.

ZCITY	ZCOUNTRY	'A__E'	ERIA__GE	IA__R	ZEMPLOYER	ZETHNICITY
Filter	Filter		Filter	...	Filter	Filter
Pannipitiya	LK		f			
Sri Jayawarde...	LK	NULL	m	NULL	Firm	Asian
Sri Jayawarde...	LK	NULL	m	NULL		South Asian
Colombo	LK	NULL	m	NULL	Bund Wien	White/Caucas...
Colombo	LK	NULL	m	NULL	Government	South Asian
Colombo	LK	NULL	m	NULL	Apcco Dairy	Asian

(a) User city, country, employer and ethnicity information.

ZPROFILE

GIVETAK	ZBIRTHDAY	ZLAST_UPDATED	ZLATITUDE	ZLONGITUDE
	Filter	Filter	Filter	Filter
	-3261	589374603	6.870887	79.94830
	-3156	589372286	6.869999	79.91000
	-3472	587562831	6.869999	79.940002
	-3786	491766908	6.909999	79.860000

(b) User birthday and geolocation information.

Buddhist	NULL	Western Province	NULL	NULL	Charm
	NULL	Western Province	NULL	NULL	Dilmini
Christian	NULL	Western Province	NULL	NULL	Julia
Buddhist	NULL	Western Province	NULL	NULL	Madhu
Catholic	NULL	Western Province	NULL	NULL	Sashika
Hindu	NULL	Western Province	NULL	NULL	Shakthi
Christian	NULL	Western Province	NULL	NULL	Jeuel

(c) User first name and religion information.

Figure 8. User information obtained from the ZPROFILE table.

Although they are very popular, Tinder and Coffee Meets Bagel are by no means the only e-dating applications encountered in investigations. Future research will employ a new framework [20] to support evidence retrieval from other e-dating platforms on iPhones and Android devices.

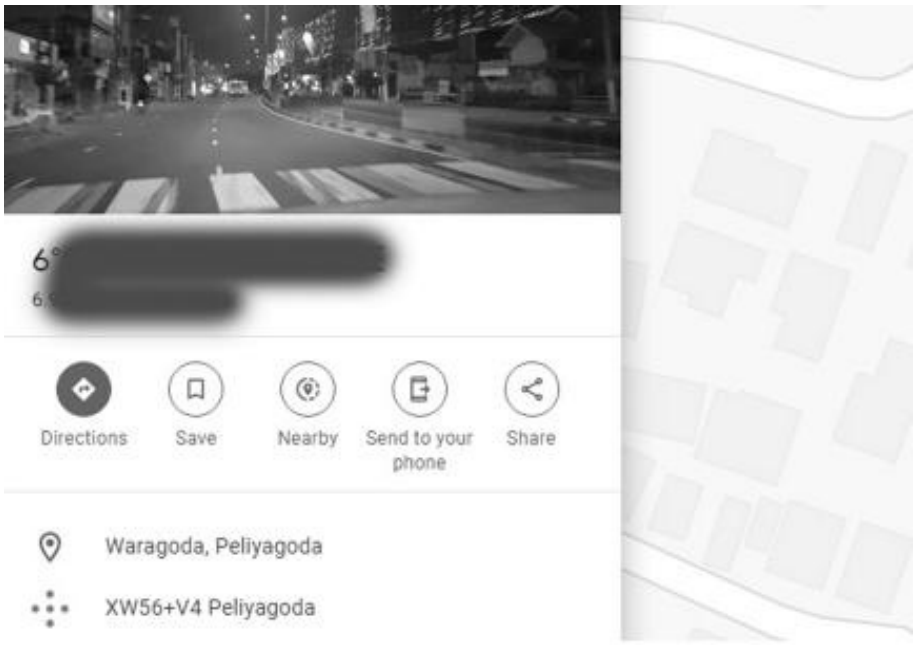


Figure 9. Screenshot of user location obtained from data in the ZPROFILE table.

References

[1] L. Aouad, T. Kechadi, J. Trentesaux and N. Le-Khac, An open framework for smartphone evidence acquisition, in *Advances in Digital Forensics VIII*, G. Peterson and S. Shenoi (Eds.), Springer, Berlin Heidelberg, Germany, pp. 159–166, 2012.

[2] I. Baggili, S. Al Awawdeh and J. Moore, LiFE (Logical iOS Forensics Examiner): An open source iOS backup forensic examination tool, *Proceedings of the Conference on Digital Forensics, Security and Law*, pp. 41–52, 2014.

[3] A. Cheema, M. Iqbal and W. Ali, An open source toolkit for iOS filesystem forensics, in *Advances in Digital Forensics X*, G. Peterson and S. Shenoi (Eds.), Springer, Berlin Heidelberg, Germany, pp. 227–235, 2014.

[4] A. Cooper, S. Mansson, K. Daneback, R. Tikkanen and M. Ross, Predicting the future of Internet sex: Online sexual activities in Sweden, *Sexual and Relationship Therapy*, vol. 18(3), pp. 277–291, 2003.

[5] K. Daneback, S. Mansson and M. Ross, Using the Internet to find offline sex partners, *CyberPsychology and Behavior*, vol. 10(1), pp. 100–107, 2007.

[6] C. de Looper, Happy Valentine's Day! Coffee Meets Bagel dating app may have been breached, *Digital Trends*, Portland, Oregon, February 14, 2019.

[7] L. Drish, iOS Device Forensics, Graduate Project, Department of Computer Science, Governors State University, University Park, Illinois, 2014.

[8] M. Epifani and P. Stirparo, *Learning iOS Forensics*, Packt Publishing, Birmingham, United Kingdom, 2015.

[9] F. Faheem, N. Le-Khac and T. Kechadi, Smartphone forensic analysis: A case study of obtaining root access of an Android Samsung S3 device and analyzing the image without an expensive commercial tool, *Journal of Information Security*, vol. 5(3), pp. 83–90, 2014.

[10] J. Farnden, B. Martini and K. Choo, Privacy risks in mobile dating apps, *Proceedings of the Twenty-First Americas Conference on Information Systems*, 2015.

[11] M. Feltz, The Security of Tinder: A mobile app that may be more intimate than we thought, Report, Department of Computer Science, Tufts University, Medford, Massachusetts (`www.cs.tufts.edu/comp/116/archive/fall2015/mfeltz.pdf`), 2015.

[12] N. Heffernen, Analysis of Forensically Significant Artifacts of Tinder App on iPhones, M.Sc. Dissertation, School of Computer Science and Informatics, University College Dublin, Dublin, Ireland, 2013.

[13] M. Iqbal, Tinder revenue and usage statistics (2020), *Business of Apps*, Staines-upon-Thames, United Kingdom, April 24, 2020.

[14] K. Lutes and R. Mislan, Challenges in mobile phone forensics, *Proceedings of the Fifth International Conference on Cybernetics and Information Technologies, Systems and Applications*, pp. 348–352, 2008.

[15] National Crime Agency, Online first date rapes increase, London, United Kingdom, February 8, 2016.

[16] L. Newett, B. Churchill and B. Robards, Forming connections in the digital era: Tinder, a new tool in young Australian intimate life, *Journal of Sociology*, vol. 54(3), pp. 346–361, 2017.

[17] P. Paganini, Coffee Meets Bagel dating app confirms data breach, *Security Affairs*, February 15, 2019.

[18] G. Ranzini and C. Lutz, Love at first swipe? Explaining Tinder self-presentation and motives, *Mobile Media and Communication*, vol. 5(1), pp. 80–101, 2017.

[19] K. Seal, Coffee Meets Bagel users get hacked on Valentine's Day, *Dating Sites Reviews* (`www.datingsitesreviews.com/article.php?story=coffee-meets-bagel-users-get-hacked-on-valentine-s-day`), March 4, 2019.

[20] R. Thantilage and N. Le-Khac, Framework for the retrieval of social media and instant messaging evidence from volatile memory, *Proceedings of the Eighteenth IEEE International Conference on Trust, Security and Privacy in Computing and Communications and Thirteenth IEEE International Conference on Big Data Science and Engineering*, pp. 476–482, 2019.

[21] Tinder, Terms of Use, Match Group, Dallas, Texas (`policies.tinder.com/terms/us/en`), 2020.

[22] R van Voorst, T. Kechadi and N. Le-Khac, Forensic acquisition of IMVU: A case study, *Journal of Digital Forensics, Security and Law*, vol. 10(4), pp. 69–78, 2015.