THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 17 Article 1

January 2022

Forensic Discoverability of iOS Vault Applications

Alissa Gilbert
Purdue University, gilbera@purdue.edu

Kathryn C. Seigfried-Spellar
Purdue University, kspellar@purdue.edu

Recommended Citation

Gilbert, Alissa and Seigfried-Spellar, Kathryn C. (2022) "Forensic Discoverability of iOS Vault Applications," *Journal of Digital Forensics, Security and Law*: Vol. 17 , Article 1.
DOI: https://doi.org/10.15394/jdfsl.2022.1773
Available at: https://commons.erau.edu/jdfsl/vol17/iss1/1

Forensic Discoverability of iOS Vault Applications

Cover Page Footnote

The abstract for this paper was presented at the 72nd Annual Scientific Meeting of the American Academy of Forensic Sciences, AAFS, Anaheim, CA.

FORENSIC DISCOVERABILITY OF IOS VAULT APPLICATIONS

Alissa Gilbert, Kathryn Seigfried-Spellar
Purdue University, gilbera@purdue.edu, kspellar@purdue.edu

ABSTRACT

Vault Applications store potentially sensitive information on a smartphone; and are available on Android and iOS. Using these applications could be used to hide potential evidence or illicit photos. After comparing five iOS photo vaults, each vault left evidence and photos behind. However, of the three forensic toolkits used, each produced different results in their scans of the phone. The media left behind was due to the photo vaults not protecting their information as claimed and using basic obfuscation techniques in place of security controls. Future research will look at how newer security controls are implemented and if they are easily discoverable.

Keywords: vault apps, sexting, privacy, digital forensics, iOS forensics

1. INTRODUCTION

Sexting has become more commonplace in mobile communications, which led to many vault apps appearing on mobile phone application stores, such as the App Store for iPhones. Vault applications have gained media attention stating these vault apps help keep your private photos safe. Previous research suggests that 40% of Android vault applications stored passwords in cleartext, and one third did not encrypt photos (Zhang, et al., 2017). These findings suggest that iOS applications may also not live up to their standards. If vault applications securely conceal private photos, they should not be easily found when imaged forensically. The following study describes the use of vault applications and their effectiveness in hiding and securing the user's private photos.

2. LITERATURE REVIEW

2.1 Vault Applications

The world has become dependent on digital sources of information, and the use of computer-based systems has been common intoring, processing, and transmitting data (Palmer, 2001). A drive for the progress of technology is correlated to an increase in public dependency on it and has led to the further integration of technology into daily life (Oriwoh, et al., 2013). As the number of solutions provided by technology increases, the amount of information stored about an individual subsequently increases (Palmer, 2002). This has raised concerns for security and privacy for the vast amount of generated user data. While ways to secure and hide data are consistently being developed (Garfinkel, 2010), one such implementation is "vault applications."

These vault applications store information privately on laptops, personal computers, mobile phones, and tablets (Newton, 2018). The most common use of vault applications for photo vault storage of sensitive or sexual uses (Lovejoy, 2017). There are multiple photo vault applications available to users on all mobile devices. These applications allow the user to securely store personal data, which makes it difficult for anyone except the device's owner to view the files even if they have access to the device (Zhang, et al., 2017). These mobile vault applications often disguise themselves by pretending to look like other applications or only displaying information when they enter a valid password (Newton, 2018).

These images need to be kept securely for personal privacy and to avoid any unwanted malicious activity towards the sender. Similarly, due to the frequent use of phones, users may also possess pictures of sensitive or personally identifiable information (such as social security numbers, passports, health-related information, and others). An additional layer of security and privacy is added to a person's device (Newton, 2018).

On the contrary, it is also possible for malicious actors to use these applications to hide pictures that may be illegal or show illegal activity. For example, a criminal may store sexually explicit images of children or pictures relating to an illegal sale of drugs on these vault applications. In such cases, vault applications may serve as a hindrance to law enforcement. Vaults are developed to safeguard a user's privacy and hide personal data but can also be misused to hide any incrimination files in case of a crime. This means the implications of such applications need to be viewed from a user security perspective and investigative anti-forensics standpoint (Zhang, et al., 2017).

In previous research on Android devices, vault applications were easily discovered by digital forensic toolkits. In a study by Michaila Duncan and Umit Karabiyik, all 64 of their investigated vault apps were detected during forensic analysis. While the researchers expected to find all unencrypted data, more advanced tools were able to decrypt images and locate them, leading to a 100% success rate on recovery (2018). Android has more options for jailbreaking, apps available, removable media, and other opportunities that make it easier to investigate many applications versus a more limited phone with limited storage.

2.2 Relevance to Investigations

During investigations, law enforcement is much more likely to encounter a suspect with a mobile device than a computer (Marturana, et al., 2011). Mobile forensics can reveal a significant amount of data ranging from an individual's communication to their travel habits (Tassone, et al., 2013). Mobile devices contain the most relevant evidence per gigabyte (SANS, 2019). This has caused an increasing demand for the analysis of forensic artifacts of interest on mobile phones (Palmer, 2001). In addition, forensic artifacts extracted from mobile devices could serve as evidence in both civil and criminal court cases (Adams, et al., 2008).

For mobile devices acquired during an investigation, vault applications may be present on the suspect's phone, which may be used to hide any incrimination files in case of a crime. Zhang (Zhang, et al., 2017) describes a case in which around half of the students from a Colorado high school used "calculator-like vault applications to distribute and hide hundreds of nude photos of themselves." In such cases, while traditional digital forensic tools may be able to recover photos directly stored on the phone, they may not be able to find those secured by photo vaults (Zhang, et al., 2017). Due to these vault applications, it is necessary to assess what kinds of information can still be recovered forensically and find new ways to extract actionable information despite these anti-forensic measures.

2.3 iOS Application Testing Methods

2.3.1 Forensics of mobile devices.

Mobile phones contain gigabytes of information about the user's behavior, location, contacts, interests, and beliefs (Abdulla Alghafli, et al., 2012). In the case of vault applications, information the user wants to keep private. Al-Zarouni (Al-Zarouni, 2006) stated the main issues with extracting and analyzing information from mobile technology: it requires specialized interfaces, storage media, and hardware. Similarly, the file system resides in volatile memory, requiring the phones to be powered on for analyses; each phone contains different operating systems based on the type and file system in place (Al-Zarouni, 2006).

Based on methods used to acquire data from mobile phones, acquisition methods can be classified into four basic categories: manual, logical, physical, and chip-off (Abdulla Alghafli, et al., 2012). The manual acquisition is the simplest method to gather data off the phone, as it involves using buttons and keypads to browse through the phone's contents manually. This method will be ineffective, as all vault applications require some password or authentication mechanism, which the investigator would not be aware of (Newton, 2018). Most existing tools in digital forensics use logical extraction, which involves retrieving information in the logical partitions of the mobile phone's memory (Abdulla Alghafli, et al., 2012). This research study utilized logical acquisition as it was the only available method. The physical acquisition of phones is based on "copying the entire physical memory locations of the phone memory chip." A chip-off involves reading data from the chip to acquire the internal non-volatile memory. The success of these methods is dependent on the file and operating system, as well as if the device requires successful authentication for the user to gain access (Jansen Ayers, 2007).

2.3.2 iPhone forensics

Since iPhones make up a large portion of the phone market, multiple studies have been conducted on iPhones and data extraction. Based on logical extractions of iPhones, Mutawa and colleagues (Mutawa, et al., 2012) as well as (Awan, 2015) could recover multiple forensics artifacts of value from common social media platforms such as user and friend data, profile pictures, timestamps, comments and posts, and in some cases, chats and cookies. Yang, Dehghantanha, Choo, and Muda (Yang, et al., 2016) as well as Husain and Sridhar (Husain Sridhar, 2009), were able to extract information from instant messaging applications such as AIM, Yahoo Messenger, and Google Talk on iPhones and extract information such as login credentials, login metadata, and conversation history. Third-party applications from devices, such as the iPhone, contain a significant amount of data, and proper analysis can prove beneficial to an investigation (Levinson, et al., 2011). A forensic analysis of an iPhone can also uncover deleted files. Like a computer, deleting the file will only delete the link to the file or the data (Zdziarski, 2008).

While the extraction of such information was possible with older iPhones, Apple has made it harder to gain access to a user's iPhone (Norouzizadeh Dezfouli, et al., 2016). When acquiring images from iPhones, the logical method is always possible, but the overall data acquired is limited; full physical acquisition is not possible on most iPhones (Jansen Ayers, 2007). However, the physical method always works on iPhones that have been jailbroken by the user (Abdulla

Alghafli, et al., 2012). Physical acquisition is still possible on iPhones below iPhone 5s, and a significant amount of data can be found on file system dumps of iPhones containing iOS version 9 and below. Beginning with iOS version 10.3, it is harder for current tools to extract several information files successfully unless the iPhone is jailbroken (Hoog Strzempka, 2015). The iPhone in this study was past iOS 9 and could not be analyzed physically, only logically.

Some newly updated tools can extract relevant information from iPhones, but cannot link them to an application; manually parsing through the files could still provide investigators with valuable data (Yang, et al., 2016). Since the filesystem was completely changed in iOS 11 to Apple's own creation and limited literature exists on iOS 11, it is difficult to say how it will affect the extraction and analysis of iPhones. As an additional complication, users are now required to enter the phone passcode or backup password each time an iPhone with iOS 10.3 or above is plugged into a computer (Newton, 2018). This makes it more difficult for investigators, as they would need to obtain the password from the suspect to access the phone. However, researchers such as Iqbal, Iqbal, and Al Obaidli (Iqbal, et al., 2012) are developing tools to acquire and analyze Apple devices without jailbreaking the device.

In terms of this study, these struggles with iPhone forensics might impact the study's photos acquisition. Without the phone being jailbroken, the results and accuracy of the acquisition might be skewed in that some of the evidence was left behind (i.e., not recovered).

2.3.3 iPhone Vault testing

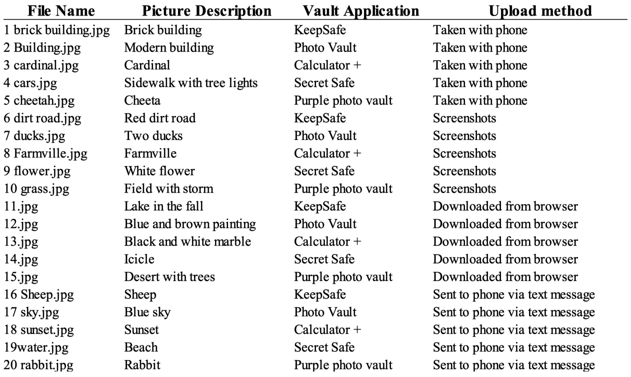
Generally, information about third-party applications can be found in the User Data partition of the iPhone device, which should be similar in the case of the vault-based applications (Levinson, et al., 2011). While limited literature exists on vault applications, a recent study by Zhang (Zhang, et al., 2017) analyzed vault applications on Android devices. Their results showed that around 67% obfuscated the vault code, and around 28% used native libraries, which negatively affected reverse-engineering the code for breaking into the applications. Zhang, however, was still able to find and view hidden data on the device without having any privileged access on the phone. Approximately a third of the vaults did not encrypt photos, while nearly 44% did not encrypt videos; ∼40% also stored the password in cleartext. It was also possible to break into some of the vault applications by swapping the password file with a custom one (Zhang, et al., 2017). Since no such testing is performed on the iPhone and iOS ecosystem, we conducted a similar study for commonly used vault applications on iPhone devices.

3. METHODS

To test the privacy and effectiveness of the vault apps, a mix of photos were assigned to multiple vault apps, then analyzed forensically to see what artifacts would be left by the application. If the vault apps were to maintain security and privacy for the images, there should not be a readable copy of the picture on the phone. This would also be successful if a photo is found but encrypted. The vault application failed when we found the "hidden" photos as readable objects where a basic imaging processor determined the image content. Ideally, the file name should not be discovered as well.

3.1 Photos

Nature photos were obtained from Creative Commons under the Attribution (cc-by). Different file name structures were also changed to observe any modification from the vault applications. See Figure 1 for the variations



File Name	Picture Description	Vault Application	Upload method
1 brick building.jpg	Brick building	KeepSafe	Taken with phone
2 Building.jpg	Modern building	Photo Vault	Taken with phone
3 cardinal.jpg	Cardinal	Calculator +	Taken with phone
4 cars.jpg	Sidewalk with tree lights	Secret Safe	Taken with phone
5 cheetah.jpg	Cheeta	Purple photo vault	Taken with phone
6 dirt road.jpg	Red dirt road	KeepSafe	Screenshots
7 ducks.jpg	Two ducks	Photo Vault	Screenshots
8 Farmville.jpg	Farmville	Calculator +	Screenshots
9 flower.jpg	White flower	Secret Safe	Screenshots
10 grass.jpg	Field with storm	Purple photo vault	Screenshots
11.jpg	Lake in the fall	KeepSafe	Downloaded from browser
12.jpg	Blue and brown painting	Photo Vault	Downloaded from browser
13.jpg	Black and white marble	Calculator +	Downloaded from browser
14.jpg	Icicle	Secret Safe	Downloaded from browser
15.jpg	Desert with trees	Purple photo vault	Downloaded from browser
16 Sheep.jpg	Sheep	KeepSafe	Sent to phone via text message
17 sky.jpg	Blue sky	Photo Vault	Sent to phone via text message
18 sunset.jpg	Sunset	Calculator +	Sent to phone via text message
19water.jpg	Beach	Secret Safe	Sent to phone via text message
20 rabbit.jpg	Rabbit	Purple photo vault	Sent to phone via text message

Figure 1. Photo Vault Apps and Evidence Acquisition

of photo names. Nature images that did not include pictures of people were used as benign test images. These images were under the cc-by license, which allowed for convenience. These photos were then added to the iPhone without additional image artifacts, such as thumbnails or copies. Any copies found were at the creation of the vault applications.

3.2 Experiment Design

An iPhone SE (A1662) on iOS 11.3 was used to test popular vault apps from the App Store. Five popular applications were installed; KeepSafe, Photo Vault, Calculator +, Secret Safe, and Purple photo vault. In Fall 2019, these vault applications were selected as they were the top results in the Apple App Store and were most downloaded by Apple users. These names are the application name from the App Store, but they have different names for folder names inside iOS. KeepSafe keeps its respective name, Photo Vault is also called enchanted cloud, Calculator + is also secret Calculator, Secret Safe is loveyouchenapp, and Purple photo vault is also referred to as galaxy studio. Each application received four similar jpegs and received the jpeg image, respectively.

In order to assess the applications, three forensic software packages were used; UFED Cellebrite (v. 7.23), Magnet Axiom (v. 3.8.0), and Black Bag Mobilyze 2019 R1. While this study did not compare the tools, it should be noted that not all tools produced the same results. The twenty images were added to the phone and then imaged through the three respective forensic applications. In order to access any cross interactions from the other applications, 20 different images were used and assigned to the specific vault application to store the image. This would make it easier to see if the application modified the images or if a thumbnail is created. If the forensic application finds all artifacts, five dedicated images should be found per application.

Cellebrite, Axiom, and Mobilyze have different features that may discover artifacts from the applications, such as pin codes, thumbnails, preview videos, or file names. Thus, more than one acquisition method was used.

4. RESULTS

Each app's key indicators of success or failure were given an abbreviated letter and character between the five vault applications and the three different forensic software. This summary can be seen below in Figure 2. The scope of this research is not to determine if any of the forensic software packages are more effective than others in finding mobile forensic artifacts. Cellebrite, Axiom, and Mobilyze shared similar results. In order to minimize redundancy, an entire breakdown of Cellebrite will be included to give further context to the summary in Figure 2. Cellebrite Physical Analyzer displayed the results from the extraction.

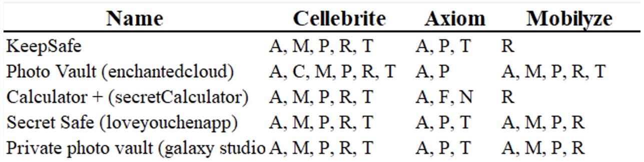
4.1 Summary

To compare the different types of evidence between each vault and forensic tool, the discovery indicators were described between them. The following letters indicate each item in the key for Figure 2:

A = Application discovered by forensic software
C = Passcode found
E = Photos were found encrypted
F = Facebook tracker found in-app
L = Live video preview image found
M = Multiple copies of the same photo were found
N = No photos found
P = All four photos were discovered
R = Original photos still found in the camera roll
T = Thumbnails/Preview Found

While Cellebrite and Axiom had all twenty photos in the iOS default photo gallery, Mobilyze did not recognize photos assigned to KeepSafe and Calculator + and did not find these applications on the phone. It is assumed that these eight missing pictures are in the default photo gallery, as suggested by the two other software packages. Overall, Mobilyze found the least amount of information from the vault applications, suggesting that using more than one forensic application to analyze the same image of the iPhone provides the most correct and whole picture of what evidence is on the phone.

Axiom did not find the 20 images in the camera roll for the vault applications. Cellebrite found all of them, and Mobilyze could only find three out of the five apps, with these three apps having their twelve respective pictures found during analysis. At first glance, Cellebrite found the most results between the three applications and was the only application to find one of the passcodes from the photo vault app Photo Vault (enchanted cloud). As Cellebrite found the most forensic artifacts, Table 3 describes what evidence was found for each application, the file name (to show any modifications), the description of the photo-matching to Figure 1, and the location in Cellebrite where the evidence was found.



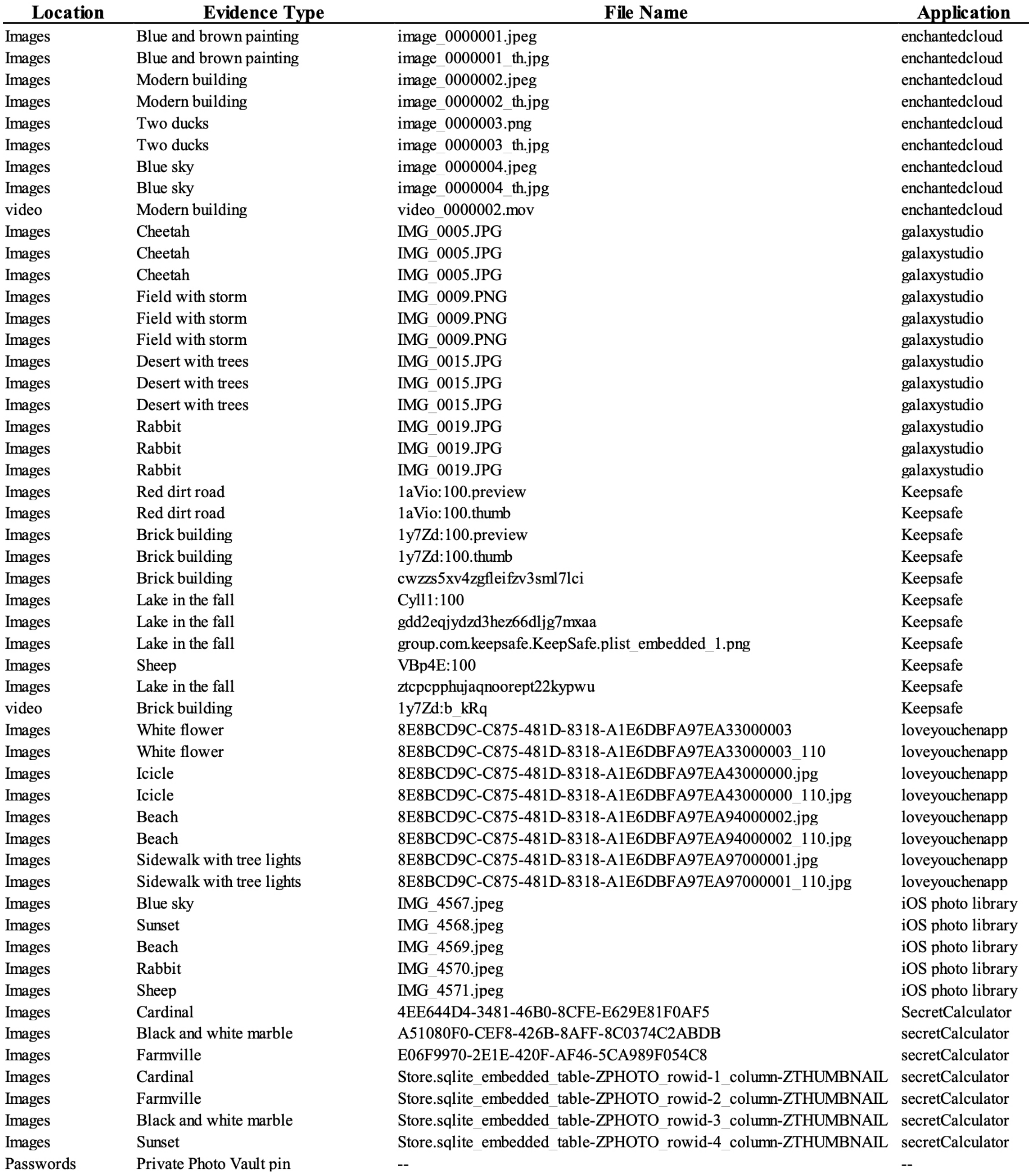
Name	Cellebrite	Axiom	Mobilyze
KeepSafe	A, M, P, R, T	A, P, T	R
Photo Vault (enchantedcloud)	A, C, M, P, R, T	A, P	A, M, P, R, T
Calculator + (secretCalculator)	A, M, P, R, T	A, F, N	R
Secret Safe (loveyouchenapp)	A, M, P, R, T	A, P, T	A, M, P, R
Private photo vault (galaxy studio	A, M, P, R, T	A, P, T	A, M, P, R

Figure 2. Evidence Found per Vault App and Forensic Tool

The package names of applications vary from their names as displayed in the app store. This created difficulty in analyzing matching different applications as the Cellebrite, Axiom, and Mobilyze found them versus how they display to users.

4.2 Thumbnails

The modification of the file names lends some information about how each vault application is storing each photo. For example, Calculator + stored each private photo as an entry in an SQL database and makes a custom file named . . . ZTHUMBNAIL instead of creating a thumbnail file with the designated thumbnail file extension .thumb such as KeepSafe. This may provide some forensic protection as using the common file extension will cause other forensic software tools not to find the thumbnail, where the thumbnails with the designated file extension were found. For example, KeepSafe used the .thumbs file extension found in Cellebrite and saw that Axiom also discovered it. While Cellebrite found the custom thumbnail file for secret Calculator, both Axiom and Mobilyze did not find these thumbnails, displaying that this type of obfuscation that the vault app provides is effective against some forensics software packages, but not all of them. Photo Vault (enchantedcloud) created a photo for a thumbnail to be viewed in the app, but it did not create a thumbnail file nor did it create a filename without a file extension. It created another image file, a jpeg like the original picture, but changed the file's name to designate to the application that is it a thumbnail picture.



Location	Evidence Type	File Name	Application
Images	Blue and brown painting	image_0000001.jpeg	enchantedcloud
Images	Blue and brown painting	image_0000001_th.jpg	enchantedcloud
Images	Modern building	image_0000002.jpeg	enchantedcloud
Images	Modern building	image_0000002_th.jpg	enchantedcloud
Images	Two ducks	image_0000003.png	enchantedcloud
Images	Two ducks	image_0000003_th.jpg	enchantedcloud
Images	Blue sky	image_0000004.jpeg	enchantedcloud
Images	Blue sky	image_0000004_th.jpg	enchantedcloud
video	Modern building	video_0000002.mov	enchantedcloud
Images	Cheetah	IMG_0005.JPG	galaxystudio
Images	Cheetah	IMG_0005.JPG	galaxystudio
Images	Cheetah	IMG_0005.JPG	galaxystudio
Images	Field with storm	IMG_0009.PNG	galaxystudio
Images	Field with storm	IMG_0009.PNG	galaxystudio
Images	Field with storm	IMG_0009.PNG	galaxystudio
Images	Desert with trees	IMG_0015.JPG	galaxystudio
Images	Desert with trees	IMG_0015.JPG	galaxystudio
Images	Desert with trees	IMG_0015.JPG	galaxystudio
Images	Rabbit	IMG_0019.JPG	galaxystudio
Images	Rabbit	IMG_0019.JPG	galaxystudio
Images	Rabbit	IMG_0019.JPG	galaxystudio
Images	Red dirt road	1aVio:100.preview	Keepsafe
Images	Red dirt road	1aVio:100.thumb	Keepsafe
Images	Brick building	1y7Zd:100.preview	Keepsafe
Images	Brick building	1y7Zd:100.thumb	Keepsafe
Images	Brick building	cwzzs5xv4zgfleifzv3sml7lci	Keepsafe
Images	Lake in the fall	Cyll1:100	Keepsafe
Images	Lake in the fall	gdd2eqjydzd3hez66dljg7mxaa	Keepsafe
Images	Lake in the fall	group.com.keepsafe.KeepSafe.plist_embedded_1.png	Keepsafe
Images	Sheep	VBp4E:100	Keepsafe
Images	Lake in the fall	ztcpcpphujaqnoorept22kypwu	Keepsafe
video	Brick building	1y7Zd:b_kRq	Keepsafe
Images	White flower	8E8BCD9C-C875-481D-8318-A1E6DBFA97EA33000003	loveyouchenapp
Images	White flower	8E8BCD9C-C875-481D-8318-A1E6DBFA97EA33000003_110	loveyouchenapp
Images	Icicle	8E8BCD9C-C875-481D-8318-A1E6DBFA97EA43000000.jpg	loveyouchenapp
Images	Icicle	8E8BCD9C-C875-481D-8318-A1E6DBFA97EA43000000_110.jpg	loveyouchenapp
Images	Beach	8E8BCD9C-C875-481D-8318-A1E6DBFA97EA94000002.jpg	loveyouchenapp
Images	Beach	8E8BCD9C-C875-481D-8318-A1E6DBFA97EA94000002_110.jpg	loveyouchenapp
Images	Sidewalk with tree lights	8E8BCD9C-C875-481D-8318-A1E6DBFA97EA97000001.jpg	loveyouchenapp
Images	Sidewalk with tree lights	8E8BCD9C-C875-481D-8318-A1E6DBFA97EA97000001_110.jpg	loveyouchenapp
Images	Blue sky	IMG_4567.jpeg	iOS photo library
Images	Sunset	IMG_4568.jpeg	iOS photo library
Images	Beach	IMG_4569.jpeg	iOS photo library
Images	Rabbit	IMG_4570.jpeg	iOS photo library
Images	Sheep	IMG_4571.jpeg	iOS photo library
Images	Cardinal	4EE644D4-3481-46B0-8CFE-E629E81F0AF5	SecretCalculator
Images	Black and white marble	A51080F0-CEF8-426B-8AFF-8C0374C2ABDB	secretCalculator
Images	Farmville	E06F9970-2E1E-420F-AF46-5CA989F054C8	secretCalculator
Images	Cardinal	Store.sqlite_embedded_table-ZPHOTO_rowid-1_column-ZTHUMBNAIL	secretCalculator
Images	Farmville	Store.sqlite_embedded_table-ZPHOTO_rowid-2_column-ZTHUMBNAIL	secretCalculator
Images	Black and white marble	Store.sqlite_embedded_table-ZPHOTO_rowid-3_column-ZTHUMBNAIL	secretCalculator
Images	Sunset	Store.sqlite_embedded_table-ZPHOTO_rowid-4_column-ZTHUMBNAIL	secretCalculator
Passwords	Private Photo Vault pin	--	--

Figure 3. Forensic Artifacts found by Cellebrite

4.3 Other Artifacts

Referencing Figure 2 shows one of the features examined if multiple copies of the same photo were found. Copying the sensitive photo to be viewed by the vault application caused more evidence to be found forensically. The .mov files were found from images taken on the iPhone with its built-in camera, which created a live preview of the images as a short video.

Private Photo Vault's pin number was found in plaintext by Cellebrite but was not found by the other forensic applications. This code was verified as the correct pin to unlock the phone. Other applications, such as KeepSafe, also had four-digit pin codes to unlock the vaults, but they were not found during the investigation. Additional copies of some private photos were created as .png files, another image type, and stored on the phone, creating more evidence to be found by the forensic tool. Frequently, these applications create more evidence and do little to obscure or secure private images.

5. CONCLUSION

Based on the current study, vault apps provide minimum protection from forensic analysis. Their primary usage should be to obscure sensitive photos from other users of the mobile device, not to provide important additional security or privacy for these private photos. While some techniques were effective at hiding evidence from some forensic software packages, the forensic applications themselves were the greatest contributing factor as to whether evidence was located on each phone. The software packages that found the most evidence was Cellebrite, while the app that provided the greatest protection was Calculator + (secretCalculator). However, Cellebrite was able to find all of the photos and metadata for the photos from Calculator + and all five applications and the twenty pictures were discovered. Future research should investigate more effective methods of hiding and securing photos, including a cloud-only solution for vault applications that do not store the image locally, but instead, they are stored off of the device via the cloud. Finally, reviewing the literature on other vault applications, these results are similar to previous research which also found 100% of the artifacts from Android vault applications (Duncan Karabiyik, 2018).

5.1 Future Work

In response to the proliferation of sexual messages and images, vault applications are becoming popular. Future research should examine other platforms, which claim to protect sensitive images, as well as the ability of other forensic tools to identify probable data. These newer apps should be compared singularly on Android and iOS similarly to these vault applications, while adding an additional phase to test new vault application features that these applications claim to use, such as AI image detection. Ultimately, continued research in this area will address not only the security and privacy of vault applications but their potential role in digital forensic investigations.

REFERENCES

[1] Abdulla Alghafli, K., Jones, A. Martin, T. A., 2012. Forensics data acquisition methods for mobile phones. Proceedings of International Conference for Internet Technology and Secured Transactions, December.pp. 265-269.

[2] Adams, C., Whitledge, A. Shenoi, S., 2008. Legal issues pertaining to the use of cell phone data. Advances in Digital Forensics, Volume IV, pp. 231-243.

[3] Al-Zarouni, M., 2006. Mobile Handset Forensic Evidence: a challenge for Law Enforcement. Australian Digital Forensics Conference.

[4] Awan, F. A., 2015. Forensic examination of social networking applications on smartphones. Proceedings of the 2015 Conference on Information Assurance and Cyber Security , December.Issue 36-43.

[5] Duncan, M., Karabiyik, U., 2018. Detection and Recovery of Anti-Forensic (VAULT) Applications on Android Devices. Proceedings of the 2018 Annual ADFSL Conference on Digital Forensics, Security and Law

[6] Garfinkel, S. L., 2010. Digital forensics research: The next 10 years. Digital Investigation, Volume 7, pp. S64-S73.

[7] Hoog, A. Strzempka, K., 2015. iPhone and iOS forensics: Investigation, analysis and mobile security for Apple iPhone, iPad and iOS devices.

[8] Husain, M. I. Sridhar, R., 2009. iForensics: forensic analysis of instant messaging on smart phones. International Conference on Digital Forensics and Cyber Crime, September.pp. 9-18.

[9] Iqbal, B., Iqbal, A. Al Obaidli, H., 2012. A novel method of iDevice (iPhone, iPad, iPod) forensics without jailbreaking. 2012 International Conference on Innovations in Information Technology, March.pp. 238-243.

[10] Jansen, W. Ayers, R., 2007. Guidelines on cell phone forensics. National Institute of Science and Technology Special Publication, Volume 800, pp. 101-110.

[11] Levinson, A., Stackpole, B. Johnson, D., 2011. Third party application forensics on apple mobile devices. 44th Hawaii International Conference on System Sciences, January.pp. 1-9.

[12] Lovejoy, B., 2017. 'Nude' app uses CoreML to automatically detect protect intimate photos on an iPhone. [Online] Available at: https://www.9to5mac.com/ [Accessed March 2018].

[13] Marturana, F., Me, G., Berte, R. Tacconi, S., 2011. A quantitative approach to triaging in mobile forensics. Proceedings of the 2011 IEEE 10th International Conference Trust, Security and Privacy in Computing and Communications , November.pp. 582-588.

[14] Mutawa, N. A., Baggili, I. Marrington, A., 2012. Forensic analysis of social networking applications on mobile devices. Digital Investigation, pp. S24-S33.

[15] Newton, C., 2018. Nude is a next-generation photo vault that uses AI to hide your sensitive photos. [Online] Available at: https://www.theverge.com/

[16] Norouzizadeh Dezfouli, F., Dehghantanha, A., Eterovic-Soric, B. Choo, K. K., 2016. Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. Australian journal of forensic sciences, 48(4), pp. 469-488.

[17] Oriwoh, E., Jazani, D., Epiphaniou, G. Sant, P., 2013. Internet of things forensics: Challenges and approaches. Proceedings of the 9th International Conference on Collaborative Computing: Networking, Applications and Worksharing, October.pp. 608-615.

[18] Palmer, G., 2001. A road map for digital forensic research.. Proceedings of the

2001 Digital Forensic Research Conference, August.

[19] Palmer, G. L., 2002. Forensic analysis in the digital world. International Journal of Digital Evidence, Volume 1, pp. 1-6.

[20] SANS, 2019. FOR585: Advanced smartphone forensics. [Online] Available at: https://digital-forensics.sans.org/ [Accessed 05 December 2017].

[21] Tassone, C., Martini, B., Choo, K. K. R. Slay, J., 2013. Mobile device forensics: A snapshot. Trends and Issues in Crime and Criminal Justice, Issue 460, pp. 1-7.

[22] Yang, T. Y., Dehghantanha, A., Choo, K. K. R. Muda, Z., 2016. Windows instant messaging app forensics: Facebook and Skype as case studies. PloS one, 11(3).

[23] Zdziarski, J. A., 2008. iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets.

[24] Zhang, X., Baggili, I. Breitinger, F., 2017. Breaking into the vault: Privacy, securiy and forensic analysis of Android vault applications. Computers Security, Volume 70, pp. 516-531.