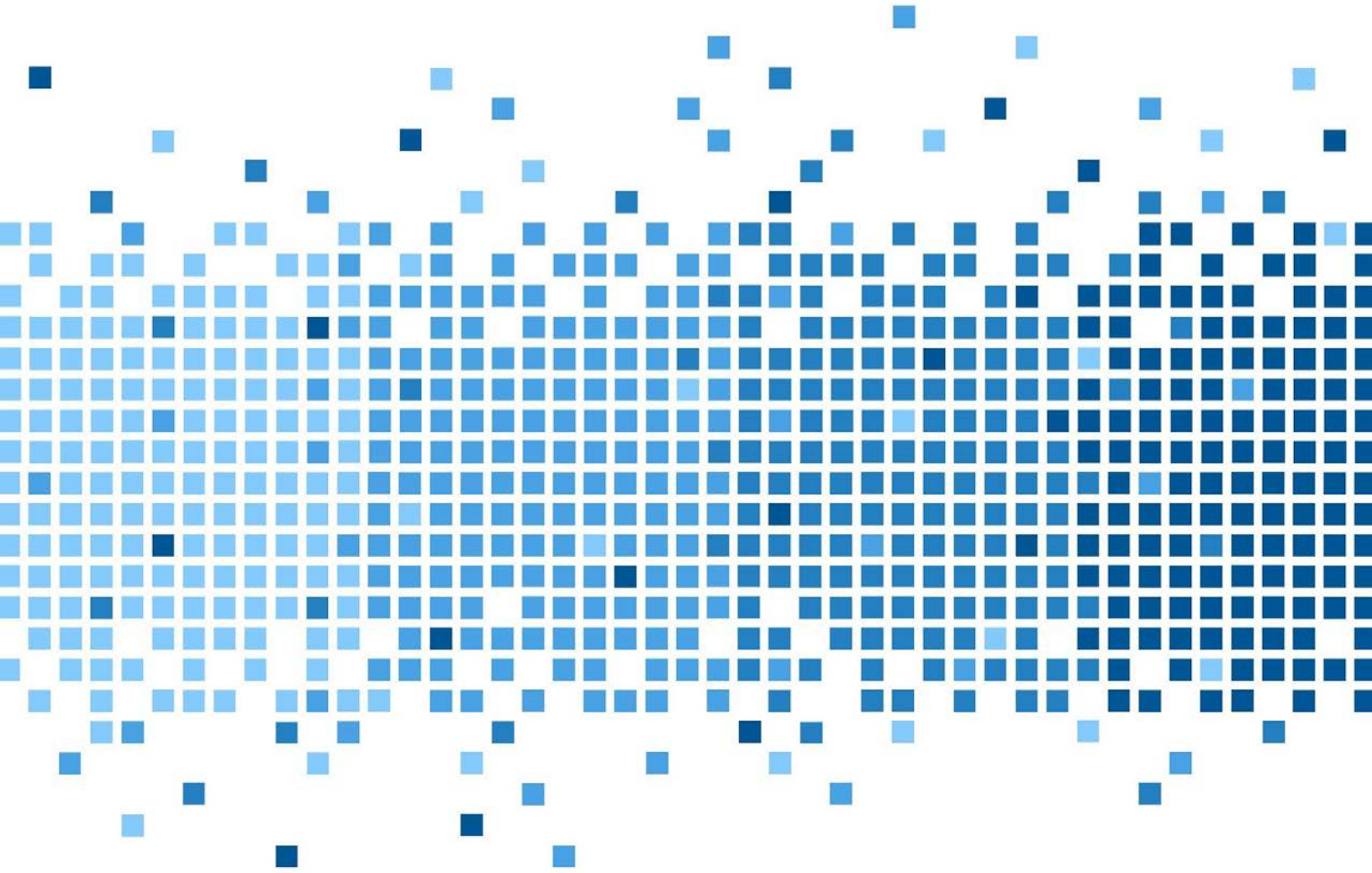
CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation

2018



175 Lakeside Ave, Room 300A
Burlington, Vermont 05401
Phone: (802) 865-5744
Fax: (802) 865-6446
http://www.lcdi.champlain.edu

4/13/2018

Mobile Forensics

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction

Applications are the backbone of every modern mobile operating system, continuing to increase in importance and relevance for both consumers and forensic investigators every day. With millions of applications available on leading mobile app stores, it has become virtually impossible to guarantee the safety and security of user data in a mobile environment. This project aims to ascertain the security of several leading applications available on the Apple App Store and Google Play Store by analyzing the artifacts that these apps leave on mobile devices.

Background

Previously, the LCDI has done Mobile Forensics projects similar to this one. These projects focused on popular applications including Signal, Facebook, Bumble, Tumblr, The Weather Channel, and more, utilizing both Apple and Android devices. In contrast, this current project will include the analysis of applications on a device with a Windows operating system, in addition to Apple and Android devices. This project will primarily focus on mobile applications that may not have a large user base, but should still offer sensible security protocols.

Addendum: After testing it with our first set of apps, it appears the Windows device cannot be properly assessed with the tools we are using. As such, it will be shelved for the remainder of the analyses.

Purpose and Scope

The purpose of our research is to find out what artifacts are stored by applications on mobile devices. We will be exploring six apps over the course of the project. These applications will be analysed on three devices: a Samsung Galaxy S3, a Nokia Lumia 600, and an iPhone 6. The Operating Systems for those devices will be listed in the Equipment Used portion of the report. In each instance, we will be searching for stored information on each device that could either be used in a forensic investigation or maliciously by a third party. That information could include, but is not limited to, financial data, personal information, and location data.

The applications to be analyzed are:

1. Telegram
2. Line
3. Viber
4. Rabbit
5. Twitch
6. Expedia

Research Questions

1. What information do popular applications use and store on iOS, Android, and Windows smartphones?
2. How well do applications hide location data, or other key information that users may not want third parties knowing?

Terminology

Android - A mobile operating system developed by Google, based on the Linux kernel.

Android Debug Bridge (ADB) - A command line tool used to communicate between Android based devices and a host machine.

Application (App) - Specifically designed software that is used for a specific task designated by its user. An application, or app for short, has a specific function. Applications can be downloaded by the user if not already loaded onto the system of use.

Artifacts - An object of digital archaeological interest, where digital archaeology roughly refers to computer forensics without the forensic (legal) context.

Autopsy - A graphical interface to The Sleuth Kit. Together, they can analyze Windows and UNIX disks and file systems.

Cookie - A small packet of data used by apps or websites to keep track of user activity.

Digital Evidence - Information or materials stored or transmitted in digital form that is to be tendered as an exhibit in a court of law.

Digital Forensics - A division of forensic science which focuses on the identification, examination, collection, preservation, and analysis of data from any device that can store electronic/digital information, such as computers and mobile phones. The science is applied in both criminal and civil investigations in a court of law, and in the private sector when investigating internal issues or intrusions.

EnCase - A suite of digital forensics tools created by Guidance Software. The software comes in several forms designed for forensic, cyber security, and e-discovery use.

Expedia - A company that assists people in creating trips to other locations by various means, sells travel tickets.

FTK - A forensic tool made by AccessData. FTK allows users to acquire, process, and verify evidence.

Google Assistant - A virtual assistant created by Google. Controllable by voice.

iOS - The mobile operating system developed by Apple for use on their iPhones, iPods, and iPads.

iPhone - A series of smartphones designed by Apple Inc. All models of the iPhones run on the iOS, a mobile operating system which is unique to Apple products such as the iPad and iPod Touch.

LINE - Messenger application that allows for video calls, and lets you share photos, contacts, and other information with friends.

Operating System (OS) - Software that communicates with the hardware and allows other programs to run. It is comprised of system software, or the fundamental files your computer needs to boot up and function.

Rabbit - Streaming application that allows users to stream online media synced up with their friends.

Smartphone - A mobile phone that includes functionality beyond making phone calls and sending text messages, such as installing third-party applications.

Telegram - Messenger app commonly used for security measures, such as an option for creating channels with self-deleting messages.

Twitch - Popular streaming application which caters to gamers and entertainment streamers.

UFED (Universal Forensic Extraction Device) - A high-end mobile forensics solution created by Cellebrite which extracts, decodes, and analyzes actionable data from legacy, smartphones, handheld tablets, and portable GPS devices.

Methodology and Methods

At the beginning of each two-week cycle, the devices will be restored to factory defaults, and applications for the new cycle will be installed. All three applications will be installed on each device, barring potential version/OS conflicts. The team members assigned to each device for that cycle will perform data generation for each app. The goal of the data generation is to use the app in the same way a normal user would, with the intent of generating artifacts that will be visible later during our analysis. For a messaging app, for example, this would include actions such as sending different types of messages, adding contacts, changing profile information, etc. When this step is completed, each device will be connected to a workstation and imaged using either *UFED Physical Analyzer* (for iOS) or *UFED 4PC* (for Android). The images (in .ufd format) will be analyzed using *UFED Physical Analyzer* and external tools such as *DB Browser for SQLite*. Our focus during the analysis stage will be on finding evidence of the actions performed during data generation, as well as any miscellaneous artifacts generated by the applications in question.

Cellebrite is a company which specializes in data extraction and analysis of mobile devices, and provides several different hardware and software tools. Our project will primarily be using their *UFED Physical Analyzer* tool for analysis and image acquisition for iOS devices. The tool allows users to explore a device's file system and export files of interest, as well as more advanced features such as image carving, timeline generation, and cookie extraction. *UFED Physical Analyzer* does not support the acquisition of Android devices, but these images can be created using our other Cellebrite product, *UFED 4PC*. Both imaging methods use specialized cables and adapters from a physical Cellebrite kit.

Equipment Used

Digital Tools	OS Version	Comments
Cellebrite Kit	N/A	Used cables and adapters to connect devices to UFED
UFED 4PC	6.5.0.702	Used for imaging Android device
UFED Physical Analyzer	7.1.0.106	Used for imaging iOS device and for image analysis
DB Browser for SQLLite	3.9.1	Used to read databases found in application files

Epoch Converter	N/A	Used to convert Unix timestamps
Android Studio	2.3.1	Used to run Android emulators for testing various tools, also for the ADB (Android Debug Bridge) command line tools.

Devices	OS Version	Comments
iPhone 6	iOS 11.2.5	The physical device used for data generation.
Samsung Galaxy S3	Android 4.4.2	The physical device used for data generation.

Data Collection

Analysis of the .ufd images was performed with *UFED Physical Analyzer*, which allowed us to explore the devices' file systems and find the artifacts we were looking for. Many of these artifacts were stored in database files, which required us to export them for analysis in an external database viewer. Others, such as cookies, images, or location data, were automatically parsed out by UFED. During our analysis we focused on collecting artifacts related to our data generation and which would be relevant during a potential forensic investigation, and compiled the artifacts and their locations in a separate document. They can be found **in the appendix.**

Analysis

The applications will go through two phases. First, the installation and data generation of each application on each device. Next, each phone will be analyzed along with any discovered artifacts created by each associated application. Ideally, the data generation will take advantage of as many features of the application, in order to create as much relevant data as possible. For instance, the Twitch application has a mobile livestreaming feature. From this, perhaps location data and even cached images of the livestream can be discovered during the imaging and analysis of the phone. For each application, we hope to discover different types of data. **The table, Possible Data Categories**, will layout the data the team may find during analysis. This data accounts for a worst case scenario where all data is stored on the device, and is easily findable and viewable.

Results

Within this section, we'll be going over all the artifacts that were found for each application in each phone. The artifacts for each application, and on each phone will be listed, along with an explanation, and accompanying images.

Viber

Viber is a free messaging and voice chat application available for iOS and Android. With over 900 million registered users, and 260 million monthly active users, the app has the potential to be part of any investigation. Although it advertises security, we were able to find a number of freely accessible artifacts in Viber's application folder including the full text of messages, location data, contact lists, and sent images.

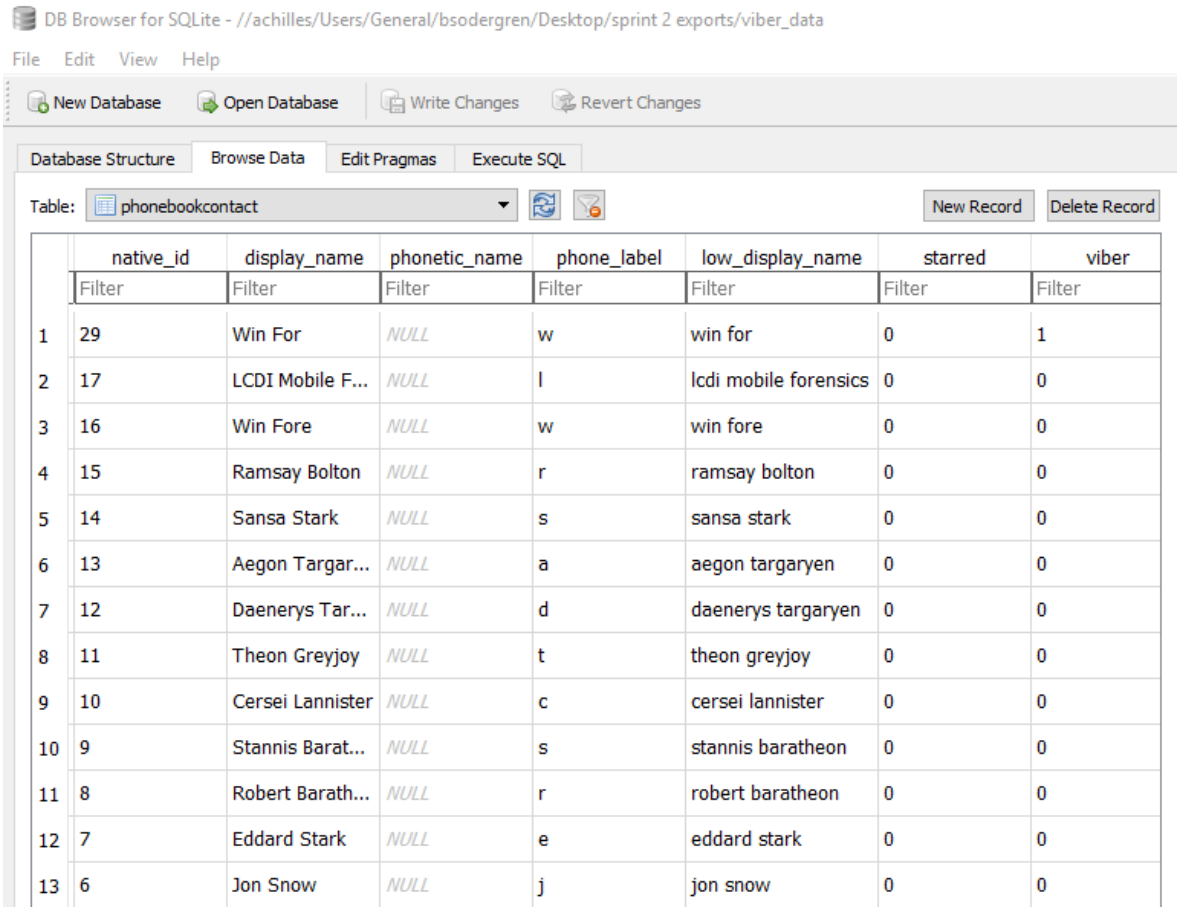
Android Artifacts

Location	Content
/data/data/com.viber.voip/databases/viber_data	Phonebookcontact table: contains full list of contacts on viber app as well as locally on device
/data/data/com.viber.voip/databases/viber_data	Phonebookdata table: contains list of contact phone numbers; can match to contacts in phonebookcontact table by their IDs
/data/data/com.viber.voip/databases/viber_messages	Adx table: logs certain events such as sending photos, messages, downloading sticker packs.
/data/data/com.viber.voip/databases/viber_messages	Messages table: Contains text of messages and metadata.
/data/data/com.viber.voip/databases/viber_messages	Participants_info table: Shows names, IDs, and phone numbers for everybody you've chatted with

List of artifacts recovered from Viber Android app

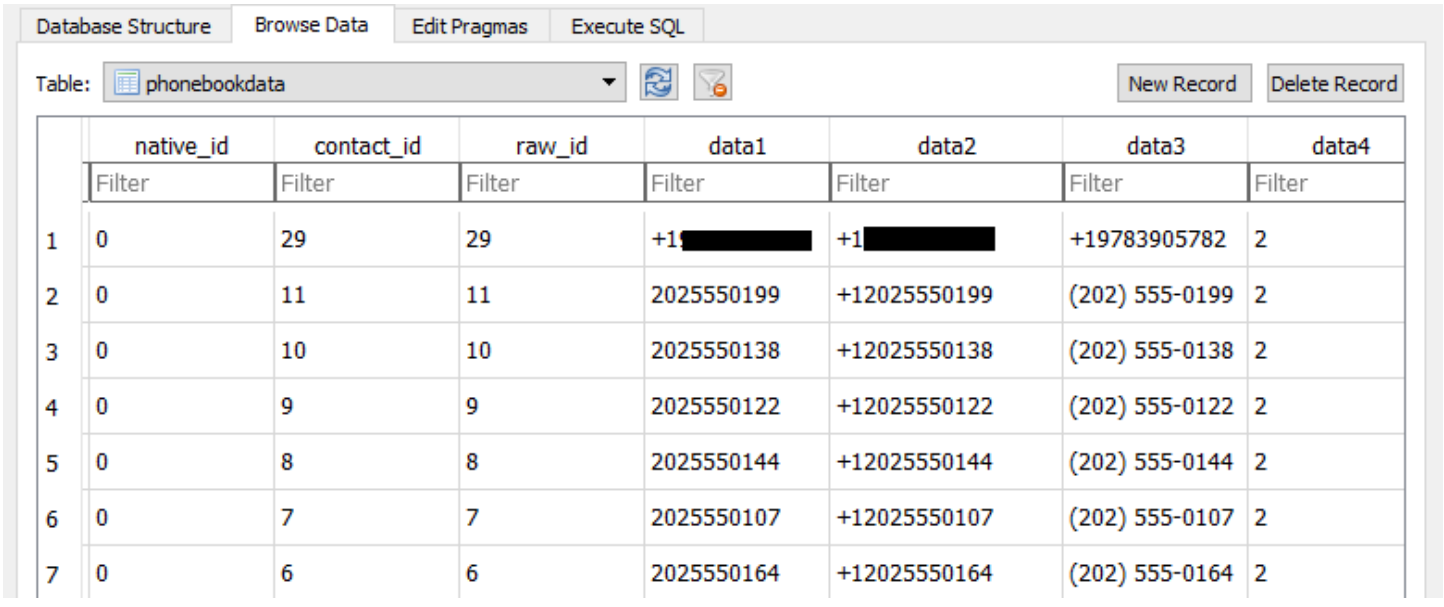
The viber_data database contains two tables of interest: **"Phonebookcontact"** and **"Phonebookdata"**. The table pictured below, "Phonebookcontact" (*figure 1)*, contains a full list of not only Viber contacts but also all of the contacts in the device's default contacts app. The "Phonebookdata" table (*figure 2*) contains the actual numbers for these contacts; while the names are not stored directly in the table, each contact's ID can be

matched against “Phonebookcontact” to find this information.



	native_id	display_name	phonetic_name	phone_label	low_display_name	starred	viber
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	29	Win For	NULL	w	win for	0	1
2	17	LCDI Mobile F...	NULL	l	lcdi mobile forensics	0	0
3	16	Win Fore	NULL	w	win fore	0	0
4	15	Ramsay Bolton	NULL	r	ramsay bolton	0	0
5	14	Sansa Stark	NULL	s	sansa stark	0	0
6	13	Aegon Targar...	NULL	a	aegon targaryen	0	0
7	12	Daenerys Tar...	NULL	d	daenerys targaryen	0	0
8	11	Theon Greyjoy	NULL	t	theon greyjoy	0	0
9	10	Cersei Lannister	NULL	c	cersei lannister	0	0
10	9	Stannis Barat...	NULL	s	stannis baratheon	0	0
11	8	Robert Barath...	NULL	r	robert baratheon	0	0
12	7	Eddard Stark	NULL	e	eddard stark	0	0
13	6	Jon Snow	NULL	j	jon snow	0	0

Figure 1



	native_id	contact_id	raw_id	data1	data2	data3	data4
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	0	29	29	+1[redacted]	+1[redacted]	+19783905782	2
2	0	11	11	2025550199	+12025550199	(202) 555-0199	2
3	0	10	10	2025550138	+12025550138	(202) 555-0138	2
4	0	9	9	2025550122	+12025550122	(202) 555-0122	2
5	0	8	8	2025550144	+12025550144	(202) 555-0144	2
6	0	7	7	2025550107	+12025550107	(202) 555-0107	2
7	0	6	6	2025550164	+12025550164	(202) 555-0164	2

Figure 2

The “**viber_messages**” database proved to have a wealth of information. The first table within that we documented, “**ADX**” (*figure 3*), logs certain events such as sending messages or photos. It doesn’t appear to be

comprehensive, but can be useful for establishing a general timeline. The timestamps under “last_tracked” can be converted by deleting the trailing three digits.

The “**messages**” table (*figure 4*) contains some of the most useful information for an investigator, with every message recorded and containing the full text of the message, links to locally-stored images, timestamps, and location data from where the message was sent. The locations can be viewed by taking the data from the latitude and longitude columns, adding a decimal point to make them valid coordinates, and pasting into Google Maps or any similar tool. Finally, the “**participants_info**” table (*figure 5*) contains a reference for every contact the user has interacted with, including their Viber usernames and phone numbers.

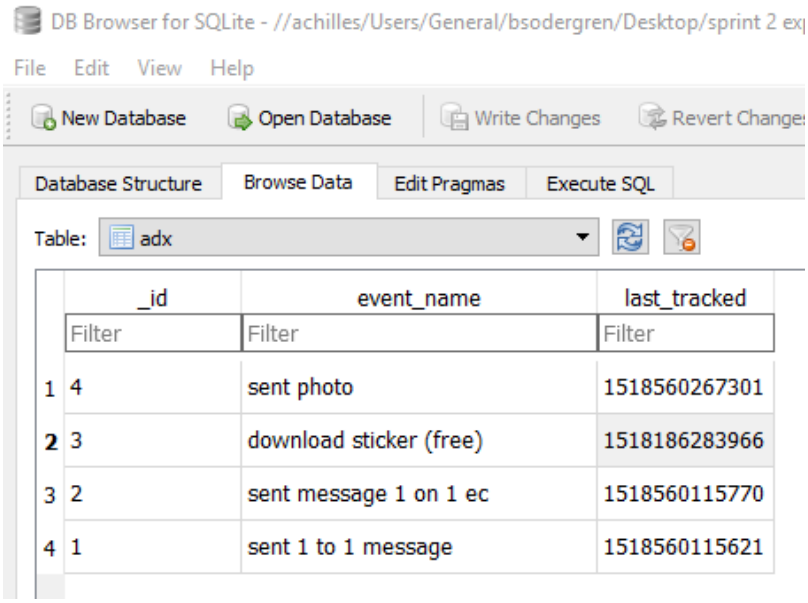


Figure 3

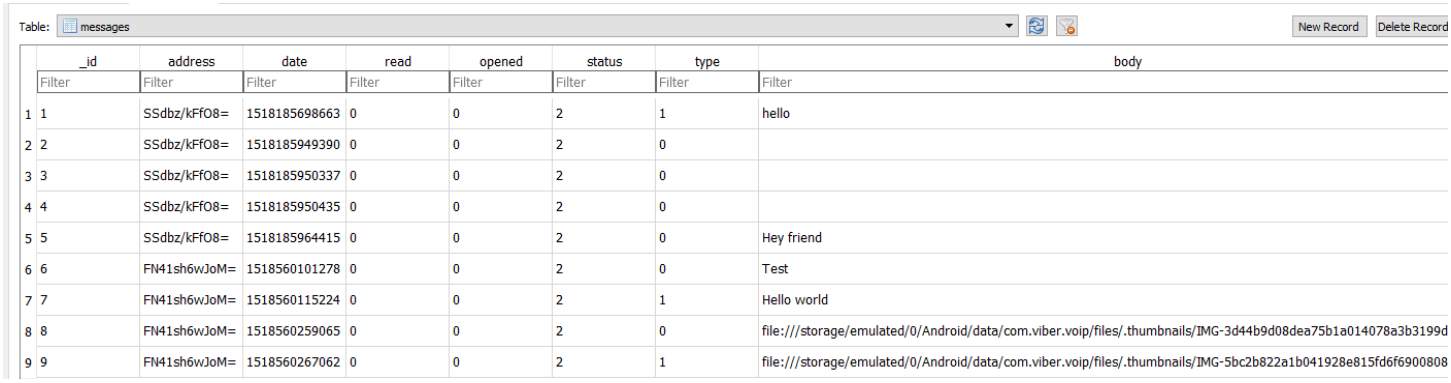


Figure 4

	_id	number	ncrypted_numbe	display_name	contact_name	contact_id	viber_id	viber_name
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	3	+1[redacted]		Win For	Win For	29	FN41sh6wJoM=	Win For
2	2	+1[redacted]		LCDI iOS	NULL	0	SSdbz/kFfO8=	LCDI iOS
3	1	+1[redacted]	wRJKReuhUyz...		NULL	0		

Figure 5

iOS Artifacts

Location	Content
LCDI's iPhone/Application/com.viber/Library/Cookies/Cookies.binarycookies	Viber installs cookies, seems to be for marketing purposes (As the name "market.viber.com" indicates).
Timeline function in UFED PA OR LCDI's iPhone/Applications/group.viber.share.container/com.viber/database/Contacts.data/ZVIBERMESSAGE	UFED's timeline/the recovered database file both show chat logs between users as well as in public chats accompanied with timestamps.
LCDI's iPhone/Applications/group.viber.share.container/avatar.jpg	Avatar image of the user.
LCDI's iPhone/Applications/group.viber.share.container/com.viber/database/contacts.data	Two tables in the database Contacts that would contain deleted private and public messages if there were any.

List of artifacts recovered from Viber iOS app

The artifacts found within the iOS version of Viber yielded similar results, with some minor differences.

One of the first artifacts we found had to do with cookies. According to our findings shown below, it appears that Viber uses cookies within the application (*figure 6*). This appears to be for marketing purposes, labeled with the tag "**market.viber.com**".

	mp_mixpanel__c	0	.viber.com	Viber
	mp_20625b657c285...	%7B%22distinct_id%22%3A%20...	market.viber.com	Viber
	B	49ikg3oupe1de	.yahoo.com	Viber

Figure 6

Using the tool *UFED Physical Analyzer*, we were able to utilize its timeline view to get a better visualization of chat logs between users of the app (*figure 7*), as well as public chats accompanied with their corresponding timestamps. This is similar to the data we were able to recover from the Android phone as well.

			Chats	2/9/2018 9:04:12 AM(UTC-5)	LCDI iOS	Viber
			Instant Messages	2/9/2018 9:04:12 AM(UTC-5)		Looks like we're all out of gifts for...
			Chats	2/9/2018 9:14:59 AM(UTC-5)	[redacted] John smith LCDI iOS	Viber
			Instant Messages	2/9/2018 9:14:59 AM(UTC-5)	From: [redacted] Joh...	hello
			Chats	2/9/2018 9:19:24 AM(UTC-5)	[redacted] John smith LCDI iOS	Viber
			Instant Messages	2/9/2018 9:19:24 AM(UTC-5)	From: LCDI iOS	Hey friend

Figure 7

Another artifact that we were able to recover from the iPhone was a thumbnail depicting the Avatar image of the user's account (*figure 8*). As shown below, a relatively high quality image of the keyboard that we set as our profile picture was able to be recovered, which could prove useful when a profile image would be of someone's face or other identifying features.

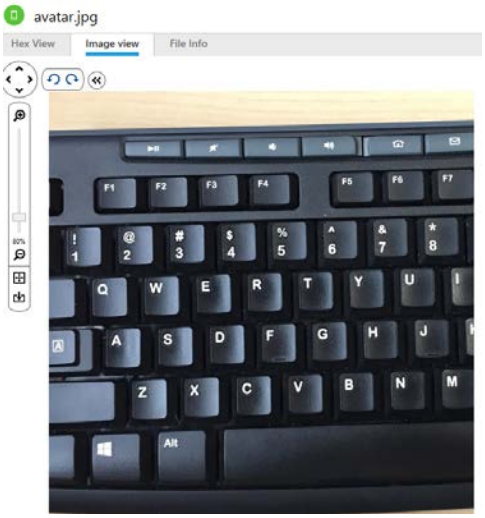


Figure 8

In addition to these artifacts, we also found two tables named "ZDELETEDVIBERMESSAGE" and "ZXPUBLICDELETEDMESSAGE", whose titles indicate it may be possible to retrieve any deleted messages from Viber. However, as we did not delete messages during data generation, we have no way of confirming the hypothesis.

Windows Artifacts

Location	Content
/Phone/Pictures/Viber/media-share-0-02-01-f21c2a3c0b52b6672f120afea3ac405dcab4e1fc3f7b5a9431dd81bd.jpg	Contains an image sent in a message.

List of artifacts recovered from Viber Windows app

Before we shelved the Windows phone for the rest of the project, we looked to see if the phone had any info that could potentially be carved out. Although using *UFED 4PC* and *UFED Physical Analyzer* led to little success, interestingly enough we were still able to carve out a photo that was sent from the contact "John Smith" to the user (*figure 9*).

To find this artifact, we had to manually look through the folder directories that *UFED 4PC* was able to provide for us. Within the "**/MTP Files/Phone/Pictures/Viber**" directory, the only file present was this photo. Although a clear explanation for why this was recovered was unclear in our analysis, a possible reason would be due to an unintentional download of the image file by the application before data extraction.

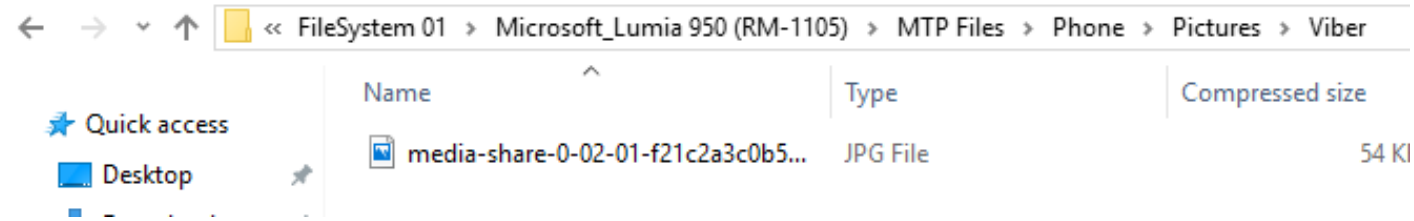


Figure 9

Telegram

Telegram is a messaging application that emphasizes speed and security. The app has roughly 180 million monthly users. It's cloud based, so relatively few artifacts were left accessible on the device.

Android Artifacts

Location	Content
/data/data/com.android.providers.contacts/databases/contacts2.db	Contains contacts added through Telegram.
Media/Phone/Telegram/Telegram Images/804722225_130699.jpg	Stock image used for Telegram profile pic.

/data/org.telegram.messenger/cache/0c2fb68f8 2f048a91b46d1c7d473116f.jpg	Contains image of location at Lakeside/LCDI.

List of artifacts recovered from Telegram Android app

While Telegram may be cloud based in how it stores most of its data, some things need to be left behind on the phone, generally things that would take too much space and bandwidth to constantly move to and from the cloud. These include images, location data, and contacts. All things that would be constantly updating, so it would be more efficient to store them on the phone.

The data table of the contacts 2 database, located within the device's native contacts app (*figure 10*), displays all contacts added through Telegram. This artifact just sits in the contacts folder of the phone. **Note that the black boxes represent actual phone numbers, blacked out for privacy**.

raw_contact_id	is_read_only	is_primary	s_super_primary	data_version	data1	data2	data3	data4
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
17	0	0	0	0	513528665	Telegram Profile	[redacted]	
17	0	0	0	0	LCDI Mobile F...	LCDI Mobile Forensics	NULL	NULL
16	0	0	0	0	457289434	Telegram Profile	[redacted]	
16	0	0	0	0	Win Fore	Win Fore	NULL	NULL

Figure 10

This artifact (*figure 11*) shows recovered location data, with Telegram picking up the coordinates of messages sent and received. It can be found in the cache of the application folder.

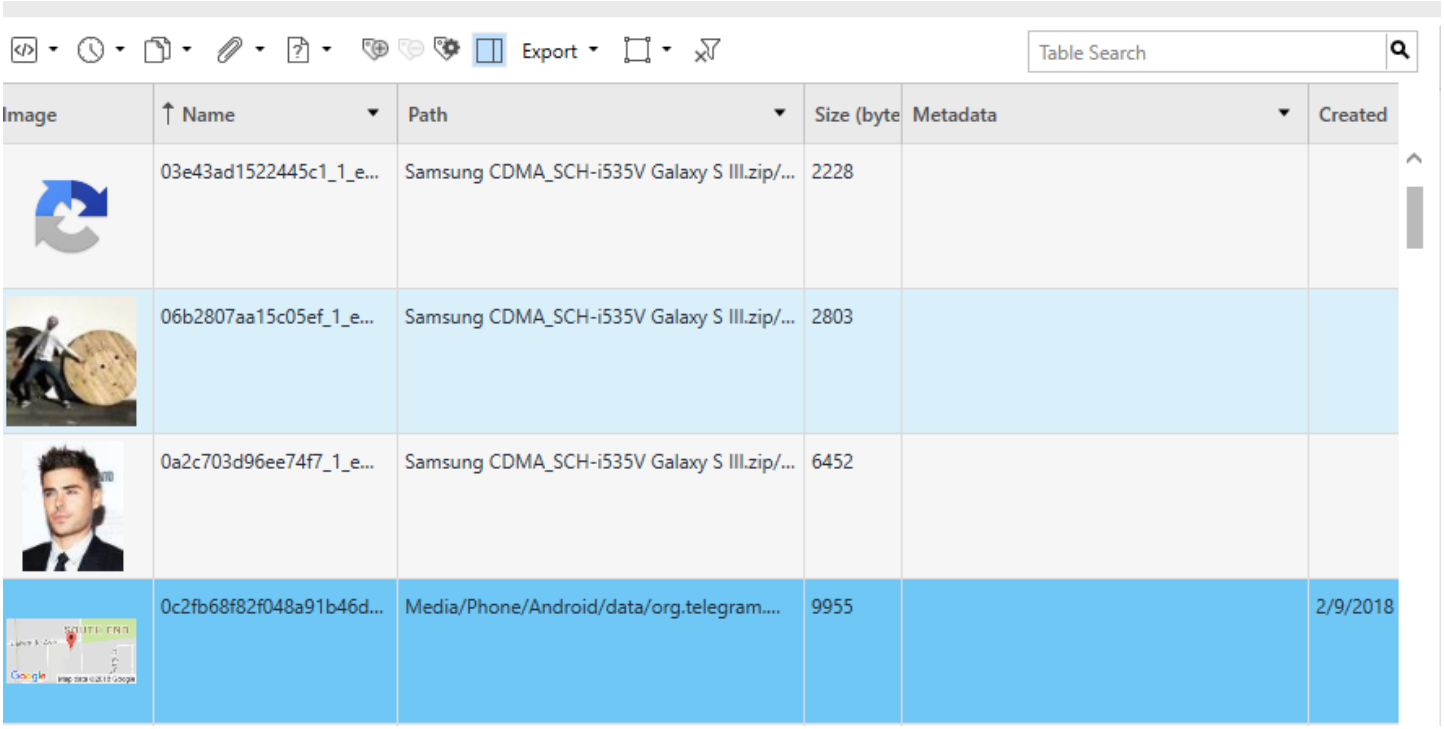


Figure 11

iOS Artifacts

Location	Content
N/A	N/A

Our analysis turned up no iPhone artifacts for Telegram. This is in part due to the realization that Telegram stores all of their information in the cloud, meaning that we would need access to cloud tools, such as *UFED Cloud Analyzer*, to look at this information.

LINE

LINE is yet another mobile messaging application. This one places a higher priority on communication, allowing for video chats and voice calls. The app boasts a monthly user base of 217 million.

Android Artifacts

Location	Content
N/A	N/A

There were no recovered Android artifacts for LINE.

iOS Artifacts

Location	Content
Applications/group.com.linecorp.line/Library/Application Support/PrivateStore/Pu7795a424dd937a50886ebd2917058288/Messages/Line.sqlite	Contains complete chat logs for both groups and individuals, including pictures and time stamps. Holds user info as well.
Applications/jp.naver.line/Library/Preferences/jp.naver.plist	Contains account information including name, username, and phone number.

List of artifacts recovered from Line iOS app

This list (*figure 12*) contains all the info on the user's LINE contacts. **Blacked out phone numbers are actual numbers hidden for privacy**. The first list, ZCREATEDAT, contains epoch timestamps, converted using an online Epoch Converter (*figure 13*).

ZCREATEDAT	ZKEY	ZLUID	ZMID	ZNAME	ZPHONENUMBER	NETIC	ZSORTABLENAME
Filter	Filter	Fi...		Filter	Filter		Filter
539879894.409437	[redacted]	11	u82...	Win Fore	[redacted]	NULL	win fore
539879894.427375	(202) 555-0162	5	NULL	Squidward Tentacles	2025550162	NULL	squidward tentacles
539879894.42952	(202) 555-0140	3	NULL	Sandy Cheeks	2025550140	NULL	sandy cheeks
539879894.431942	(202) 555-0185	1	NULL	Spongebob Squarepants	2025550185	NULL	spongebob squarepants
539879894.435377	[redacted]	12	NULL	Android Fore	[redacted]	NULL	android fore
539879894.436876	(202) 555-0126	6	NULL	Mrs. Puff	2025550126	NULL	mrs. puff
539879894.43889	(202) 555-0114	4	NULL	Eugene Krabs	2025550114	NULL	eugene krabs
539879894.440435	(202) 555-0143	2	NULL	Patrick Star	2025550143	NULL	patrick star

Figure 12

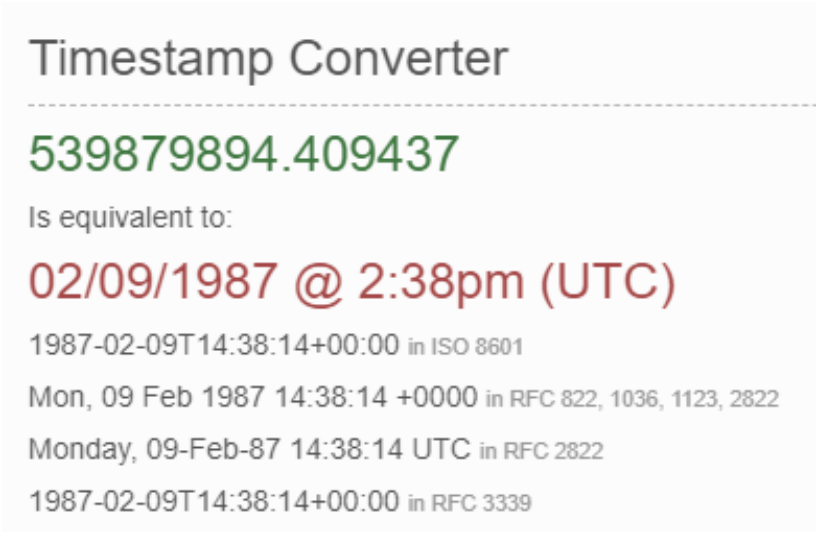


Figure 13

This database (*figure 14*) contains various messages recovered between users of the device.

u7795a424dd937a50886ebd29170582 ud534b54d0604e25a0c5d2d4a770a48	2/9/2018 9:49:09 AM(UTC-5)	2/9/2018 10:00:27 AM(UTC-5)	this is a group c490ad5...	Line: LCDI Mobile Fo
u7795a424dd937a50886ebd29170582 ud534b54d0604e25a0c5d2d4a770a48	2/9/2018 9:47:49 AM(UTC-5)	2/9/2018 9:48:34 AM(UTC-5)	kmullin7 ud534b54d06...	Line: LCDI Mobile Fo
1[redacted] John smith LCDI iOS (owner)	2/9/2018 9:14:59 AM(UTC-5)	2/9/2018 9:19:24 AM(UTC-5)		Viber
LCDI iOS (owner)	2/9/2018 9:04:12 AM(UTC-5)	2/9/2018 9:04:12 AM(UTC-5)		Viber
u7795a424dd937a50886ebd29170582 u82311c94e7071128f2530b9dc6d7b54	2/8/2018 8:40:32 AM(UTC-5)	2/8/2018 8:47:06 AM(UTC-5)	Win Fore u82311c94e7...	Line: LCDI Mobile Fo
u7795a424dd937a50886ebd29170582 uc353a971cb90ab899da27ca24746a31	2/6/2018 7:26:13 PM(UTC-5)	2/6/2018 8:50:01 PM(UTC-5)	LINE USA uc353a971cb...	Line: LCDI Mobile Fo
u7795a424dd937a50886ebd29170582 u085311ecd9e3e3d74ae4c9f5437cbcb	2/6/2018 7:26:09 PM(UTC-5)	2/6/2018 7:26:09 PM(UTC-5)	LINE u085311ecd9e3e3...	Line: LCDI Mobile Fo

Figure 14

Next is an artifact (*figure 15*), which contains the information of the user of the phone. It contains their user ID, phone number, and whatever they have as a status for their profile.

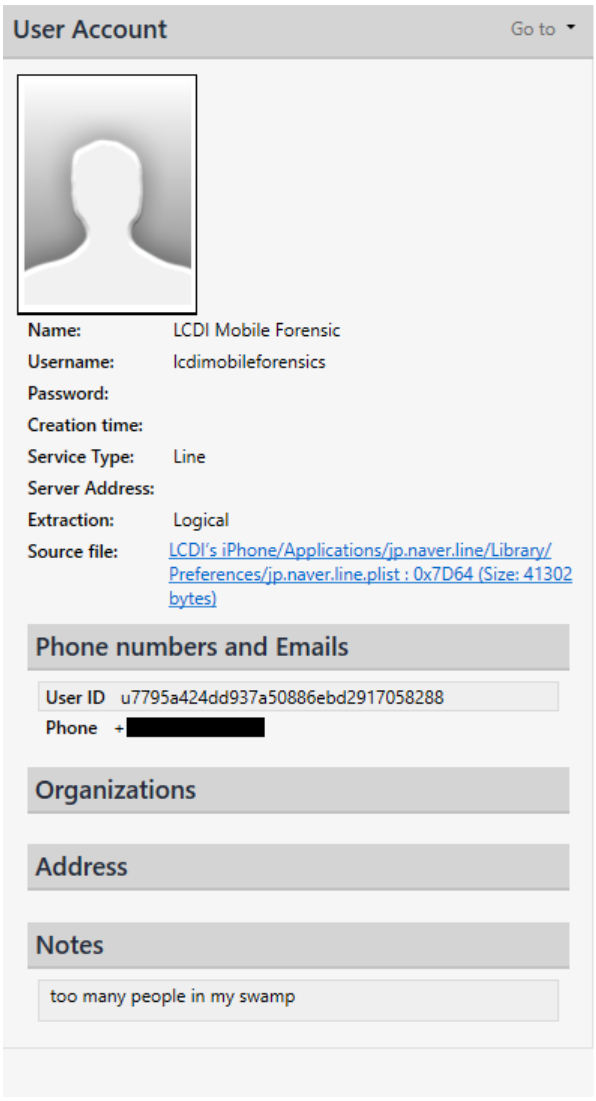


Figure 15

Rabbit

Rabbit is a social streaming application that lets you watch and listen to online media together with friends, synced up in real time. While the majority of users use the desktop version of the application, the mobile version has a growing user base of at least 100,000, based on Google Play downloads.

Android Artifacts

Location	Content
data/data/it.rabb.rabbitandroid/shared_prefs/com.google.android.gms.signin.xml	XML file contains email of user, as well as full name and display name (*figure 16*).

List of artifacts recovered from Rabbit Android app

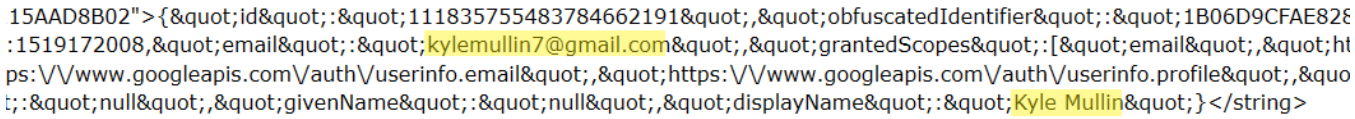


Figure 16 xml file showing user's email address and display name

iOS Artifacts

Location	Content
Applications/it.rabb.rabbitios/Documents/RCTAsyncLocalStorage_V1/3ae271cd7df2b4cd4b15d6ecab9db119	Contains timestamps for last connection, what device used the app, timezone, first name, last name, email, username, etc.
/Applications/it.rabb.rabbitios/Documents/RCTAsyncLocalStorage_V1/manifest.json	Contains friend information.

List of artifacts recovered from Rabbit iOS app

This screenshot below (*figure 17*) is essential as it shows timestamps such as last connection time for device, as well as the times in a room. Device types are also listed along with the IP address, and country.

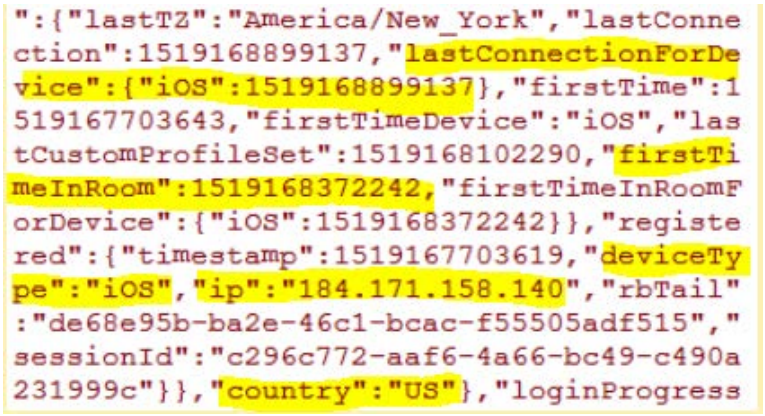


Figure 17

Another image of the same file mentioned below (*figure 18*) also contains the full name, username, and number of friends of the logged in user.

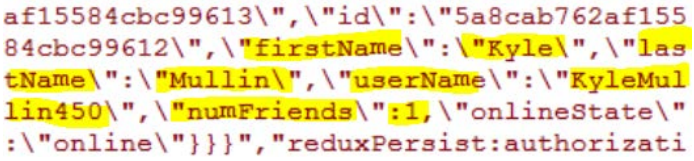


Figure 18

Twitch

Twitch is a streaming application which primarily caters to video gamers and e-sports participants, as well as artists and general purpose streamers. Its desktop counterpart is extremely popular, having been the largest video game streaming service for several years running. The mobile user base is also significant, with around 2.2 million monthly users of the Twitch app.

Android Artifacts

Location	Content
data/data/com.android.vending/databases/localappstate.db : 0x5EC6 (Table: appstate, Size: 94208 bytes)	Contains the plain text email used to sign in with the Twitch account, kylemullin7@gmail.com.

List of artifacts recovered from Twitch Android app

This artifact (*figure 19*) contains the login email used for the Twitch login which could be used in a phishing attempt or to identify a suspect's accounts and link information and clues together. Having this email in plain text is not a great security practice, but itis not crucial enough to be considered a breach in privacy.

```
77 36 36 43 63 38 39 59 5A 77 72 68 36 50 4B 48 6B 77 55 6D 35 42 51 33 4C 5F 33 42 | S6cTFQA-_IbR9w66Cc89YZwrh6PKHkwUm5BQ3L_3B
6B 35 35 46 69 30 54 5F 47 38 67 30 51 74 62 48 69 79 48 79 5F 77 52 42 30 39 6C 34 | LrTgof0cNt8r8k55Fi0T_G8g0QtbHiyHy_wRB09l4
47 7A 7A 55 73 30 77 4A 76 74 35 45 64 7A 56 4F 6D 34 46 63 4D 62 4A 45 36 51 56 58 | Mo_-BI__nxalQGzzUs0wJvt5EdzVOm4FcMbJE6QVX
4A 33 74 75 46 43 52 73 65 41 6A 77 54 43 36 64 41 68 37 35 5A 63 49 58 37 33 6A 76 | I323SxBUT_Ha6J3tuFCRseAjwTC6dAh75ZcIX73jv
74 49 5A 63 59 79 6E 2D 74 5F 4D 42 71 48 55 67 67 79 33 36 44 6B 48 42 59 4C 33 26 | kRf3p8Jueo9jotIZcYyn-t_MBqHUggy36DkHBYL3&
4E 65 4E 39 34 73 6E 9A 01 2B 68 64 6B 51 4E 6E 75 46 38 45 50 6B 35 48 51 61 6A 4F | cpn=5Tsn2po4rNeN94sn..+hdkQNnuF8EPk5HQajO
36 71 6A 73 4B 30 4E 4B 76 78 4C 63 01 61 B5 64 2F 67 01 61 B5 64 38 FF 6B 79 6C 65 | CicN6uo-b-9oF6qjsK0NKvxLc.a.d/g.a.d8.kyle
2E 63 6F 6D 54 77 69 74 63 68 01 47 05 8A 01 0F 08 00 10 C7 02 18 9A E6 E0 0B 28 EB | mullin7@gmail.comTwitch.G..............(.
1A 21 0A 16 63 6F 6D 2E 67 6F 6F 67 6C 65 2E 61 6E 64 72 6F 69 64 2E 67 6D 73 10 E0 | .....T........!..com.google.android.gms..
64 72 6F 69 64 2E 70 65 72 6D 69 73 73 69 6F 6E 2E 53 59 53 54 45 4D 5F 41 4C 45 52 | ... .(. .2&android.permission.SYSTEM_ALER
4E 9D 3E 01 61 B5 63 C7 71 73 69 6E 67 6C 65 5F 69 6E 73 74 61 6C 6C 0A 00 12 15 74 | T_WINDOW.N.(.N.>.a.c.qsingle_install....t
6F 69 64 2E 61 70 70 18 FF FF FF FF FF FF FF FF FF 01 3A 15 74 76 2E 74 77 69 74 63 | v.twitch.android.app...........:.tv.twitc
4A 54 08 00 10 9A E6 E0 0B 1A 21 0A 16 63 6F 6D 2E 67 6F 6F 67 6C 65 2E 61 6E 64 72 | h.android.appJT........!..com.google.andr
01 28 00 20 1A 32 26 61 6E 64 72 6F 69 64 2E 70 65 72 6D 69 73 73 69 6F 6E 2E 53 59 | oid.gms..... .(. .2&android.permission.SY
4E 44 4F 57 0D 00 00 00 01 05 D3 00 05 D3 08 91 0D 42 0D 87 00 00 00 00 00 00 00 00 | STEM_ALERT_WINDOW.............B.........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................................
```


Figure 19

iOS Artifacts

Location	Content
/Applications/tv.twitch/Library/Cookies/Cookies.binarycookies : 0x52A (Size: 2213 bytes)	Contains the login for this phone (lcdimobile01).
/Applications/tv.twitch/Library/Cookies/Cookies.binarycookies : 0x5E6 (Size: 2213 bytes)	Contains the API key for the Twitch account and/or the device.
/Applications/tv.twitch/Library/Cookies/Cookies.binarycookies	Contains last login date/time of account. 02-20-2018.

List of artifacts recovered from Twitch iOS app

The only information available for the iOS version of Twitch came from its binarycookies file, shown here as it was parsed automatically by UFED. Several pieces of information are visible here, notably the username (*figure 20*), API key (*figure 21*), and last login date (*figure 22*). **Some info blacked out for privacy.**

name	lcdimobile01	.twitch.tv	Twitch
login	lcdimobile01	.twitch.tv	Twitch

Figure 20

api_token	[redacted]	.twitch.tv	Twitch	/

Figure 21

last_login	2018-02-20T23:31:07Z	.twitch.tv	Twitch

Figure 22

The user account/login name may seem like an issue at first, but in the end it is somewhat irrelevant. The account username used by a user to login into their account can be publicly seen by anybody, and doesn't have any sort of personal identifiable information beyond that. That said, this could be used in a forensics investigation to prove that an account belonged to the devices owner, or that it was at least logged in on the device.

The API (Application Programming Interface) key has a variety of uses. Although Twitch doesn't specify what the API key is used for within their system, they're generally used for authentication and authorization of computer programs accessing or inputting into other programs or to identify a user. This could be considered a privacy concern, as the API key could be used to commit a malicious act.

The last login date can be definitely categorized into a key piece of forensic evidence. It can be used to prove a variety of scenarios such as unauthorized login or access, or proving that the application was in use during a specific window of time. The first piece of the cookie lists the date accessed, and then the time, in the 24-hour fashion. The "T" may indicate "Time", separating the date from the following timestamp. The "Z" at the end of the data may indicate "Zulu-time", another term for Greenwich Mean Time. This makes sense as GMT is about four hours ahead of Eastern Standard Time, and fits the window during which the team was using the application.

Expedia

Expedia is an application used to organize and pay for vacations and flights. It lets you search for and compare flights and hotel rooms, as well as showcasing attractions for different destinations. It has had at least 10 million unique downloads, according to the count on the Google Play store.

Android Artifacts

Location	Content
data/data/com.expedia.bookings/cache/okhttp/00866c5b41a4b20f9ad49bcdcc165082.1	Contains an image of a map, with the location of a researched hotel.
data/data/com.expedia.bookings/cache/okhttp/4127f4f84a051444173cbc0e65255c9b.1	Contains an image of a viewed hotel.
data/data/com.expedia.bookings/cache/okhttp/26c578b20c5cefd4d4bdbd0c5002f957.0	Contains an XML link, that leads to an Expedia webpage that contains details about a planned trip.

List of artifacts recovered from Expedia Android app

This location data (*figure 23*) was accessed through the location feature of UFED, and reflects several of the locations that were searched for hotels within the application. These locations are also available under UFED's Searched Items tab.

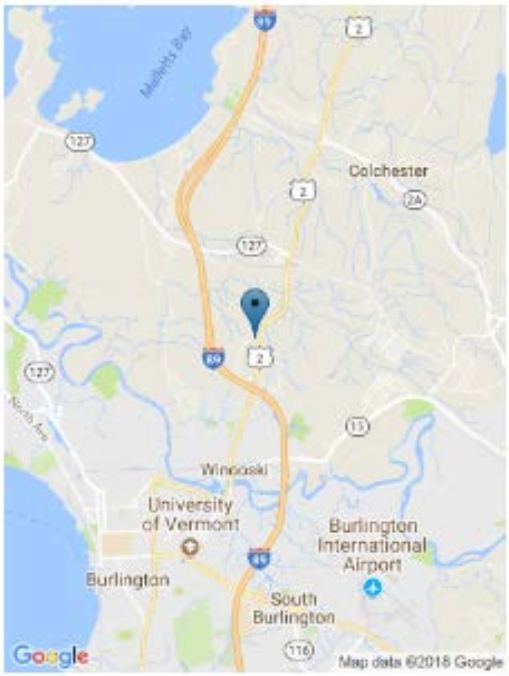


Figure 23

The below image (*figure 24*) was carved out from the application. This image shows the front of an "Anchorage Inn", which was one of the hotels viewed within the application.

Figure 24

iOS Artifacts

Location	Content
com.expedia.booking.plist	Contains the location info of researched locations.
/var/mobile/Library/Accounts/Accounts3.sqlite : 0x5E9F (Table: ZACCOUNT, SIZE: 188416 bytes)	Contains just Name/email account tied to Expedia account. The listed username is “1333960502”, which may be Expedia’s shorthand way of identifying users/customers.
com.expedia.booking/library/cookies/cookies.binarycookies	Contains 40 entries for Expedia’s cookies. Mostly illegible, but user’s selected currency is visible.

List of artifacts recovered from Expedia iOS app

The file com.expedia.booking.plist contained the location information for all of the hotels browsed within the app, shown below as carved out by UFED (*figure 25*). You can see all four locations of hotels searched for within the app; however, non-hotel location searches (such as our browsing events in Las Vegas) aren’t listed.

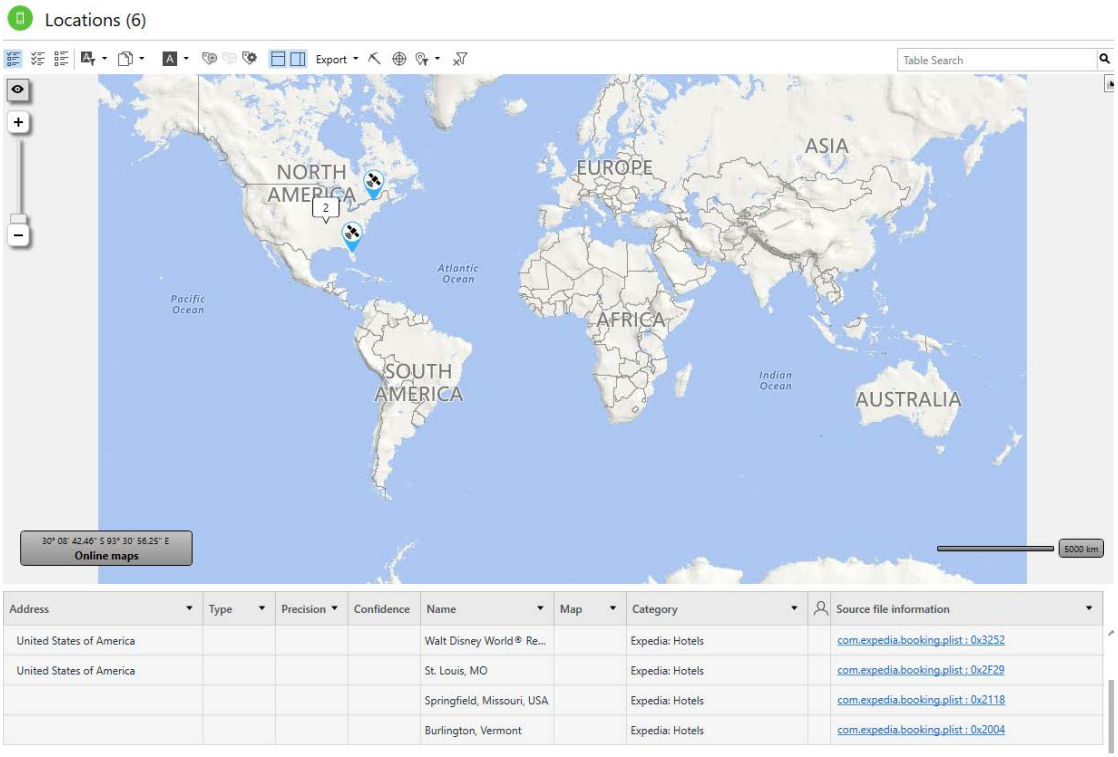


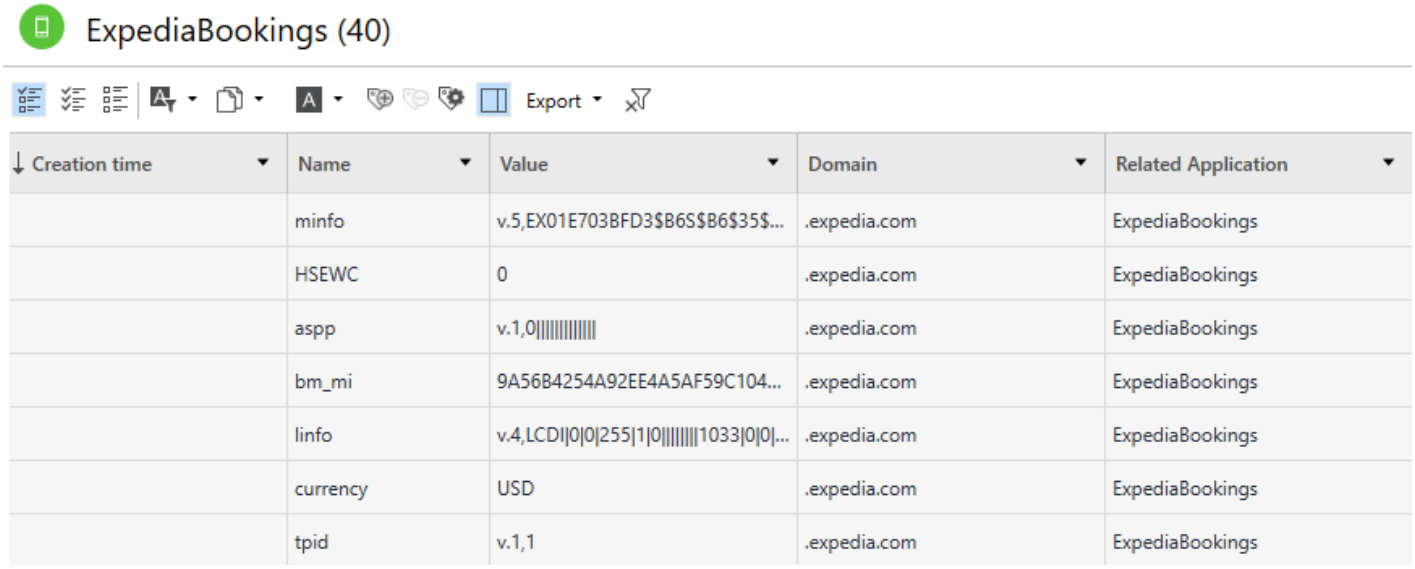
Figure 25

One of Expedia's databases (*figure 26*) contained a table named ZACCOUNT, which held the name and email address used to log in to the app.

LCDI Mobile	1333960502		Expedia		lcdimobileappios@gmail.com

Figure 26

Lastly, the below screenshot (*figure 27*) is of a table presented to us from *UFED Physical Analyzer*, in a tab labeled "**ExpediaBookings**". This appears to be specific information related to application settings. Since this information was found under the tab "ExpediaBookings", we believe that this information corresponds to the application settings being used at the time a booking was made or attempted.



Creation time	Name	Value	Domain	Related Application
	minfo	v.5,EX01E703BFD3$B6S$B6$35$...	.expedia.com	ExpediaBookings
	HSEWC	0	.expedia.com	ExpediaBookings
	aspp	v.1,0||||||||||||	.expedia.com	ExpediaBookings
	bm_mi	9A56B4254A92EE4A5AF59C104...	.expedia.com	ExpediaBookings
	linfo	v.4,LCDI|0|0|255|1|0|||||||1033|0|0|...	.expedia.com	ExpediaBookings
	currency	USD	.expedia.com	ExpediaBookings
	tpid	v.1,1	.expedia.com	ExpediaBookings

Figure 27

Conclusion

This section will be looking at the questions we asked, the expectations we had, and the results we found. While we by no means found all potential vulnerabilities, the ones we were able to identify have given us answers to our questions as listed below.

What information do popular applications use and store on iOS, Android, and Windows smartphones?

How well do applications hide location data or other key information that users may not want third parties knowing?

Our expectations for the first question were that we would find primarily personal data that the application would save for future use, location data, images, and information that would always need to be available, like texts. We were overall correct in our assumptions.

The goal of the second question is to determine how often a phone can determine the location of the user, as well as how and where this data can be located on the phone. It also needs to be determined how much of the personal information each application requests is actually saved on the phone. This data is prime material to be abused by questionable people, so its security is crucial.

To tackle this we went through the previously shown process of generating and analyzing data off of the devices in question. We pulled the data off the phones using *UFED 4PC*, which compiled it all into a readable and organized format. From there, we picked through the data from each phone, looking at info from each application. Ultimately, it all came together in the form of our **Results** section. There, data relevant to our research was gathered and explained. Overall, we found a few more artifacts than expected, especially regarding the messenger applications. Some data was easy to find, or left in plain text.

Further Work

While the team feels as if the best effort and a full application of our technical skills was put into every aspect of this project, our limited experience and knowledge could have caused us to unintentionally overlook a possible artifact or privacy concern. Unfortunately, it was not possible for the team to obtain the latest iPhone, Android, and Windows devices due to their software's compatibility with our imaging software. The project could have greater benefitted the digital forensics and cyber-security community had it been targeted towards more recent devices and application versions. The project was also restricted from the very beginning; our first analysis of the Windows device resulted in very limited information, lacking even basic artifacts such as contacts and messages. This caused the device to be dropped from the project shortly after starting. UFED PA also offers a cloud-forensics service that the team didn't have access to. Once providing the credentials to the program, an analyst can perform cloud forensics on supported services such as Facebook, Instagram, LinkedIn, iCloud Backup, Data, and Locations, along with several Google services. Additionally, this program allows for Telegram forensics, which would have been a great addition to the project.

Appendix

Possible Data Categories

Application	Possible Data Categories	Notes
Telegram	Personal/Account Information	Telegram is a cloud based service, so it is unlikely we will find any sort of data stored on the device.
Line	Personal Information, Chat Logs/History, Location History, Call History, Contacts, Contact Info	
Viber	Personal Information, Chat Logs/History, Location History, Call History, Contacts, Contact Info	
Rabbit	Connection History, Personal Account Information, Cached Images, Chat Logs	
Twitch	Stream History, Chat Logs, Cached Images, Location(s), Purchases, Account Connections	Twitch seems to be a server based streaming service; a client streams to a Twitch-owned server, and viewers connect to the server to view their stream.
Expedia	Locations, Search History, Purchases, Personal/Account Information	

Artifacts and Screenshots

Application	Link to Documented Artifacts
All Applications	https://drive.google.com/open?id=1RSUuv69DS6nejNv6HWZ45S2DarTMyQKw
Expedia	https://docs.google.com/document/d/1ZgNXMyrmHvmjO3pgPdNVp0Wt3fuK1QXF1XPt7SYZruU/edit?usp=sharing
LINE	https://docs.google.com/document/d/1putvT13V49UJtcPCW0z6NIkprTDrANm5N1QZRH8OJwM/edit?usp=sharing
Rabbit	https://docs.google.com/document/d/1Y7czFi7tVNp8y4-OKdXaxs3xiReqFHiGeiUPsWzKEQU/edit?usp=sharing

Telegram	https://docs.google.com/document/d/1yZM-FHe2lnrhKZWa4Z3cwsYL3gZUjfM-S08H4imWDW8/edit?usp=sharing
Twitch	https://docs.google.com/document/d/19pp5SwVstT0DumDLTUxRZnkQcHZSiRmFdSUif5VQU48/edit?usp=sharing
Viber	https://docs.google.com/document/d/104Tgk-TuleR8vpLL5yO-4E8Vdmik1j2w2dSNyXOnUwU/edit?usp=sharing

References

"Android Debug Bridge." https://developer.android.com/studio/command-line/adb.html. Android Developers, N/A. Web. 20 March 2018.

"Application (App)." https://techterms.com/definition/application. techopedia.com. Web. 22 March 2018.

"Artifacts." http://www.forensicswiki.org/wiki/Artifacts. Forensics Wiki. 31 October 2015. Web. 22 March 2018.

"Autopsy Forensic Browser." https://forensicswiki.org/wiki/Autopsy_Forensic_Browser. Forensics Wiki. 7 July 2014. Web. 22 March 2018.

"Digital Evidence." https://forensicswiki.org/wiki/Digital_evidence. Forensics Wiki. 21 March 2016. Web. 22 March 2018.

Christensson, Per. "Android Definition." TechTerms. Sharpened Productions, 16 May 2016. Web. 28 March 2018. https://techterms.com/definition/android

Christensson, Per. "Batch File Definition." TechTerms. Sharpened Productions, 21 October 2006. Web. 28 March 2018. https://techterms.com/definition/batchfile

Christensson, Per. "iOS Definition." TechTerms. Sharpened Productions, 22 October 2011. Web. 28 March 2018. https://techterms.com/definition/ios

Christensson, Per. "Operating System Definition." TechTerms. Sharpened Productions, 23 July 2016. Web. 28 March 2018. https://techterms.com/definition/operating_system

Christensson, Per. "Smartphone Definition." TechTerms. Sharpened Productions, 30 July 2010. Web. 28 March 2018. https://techterms.com/definition/smartphone

"Computer Forensics." https://forensicswiki.org/wiki/Computer_forensics. Forensics Wiki. Web. 13 February 2017. Web. 22 March 2018.

"EnCase® Forensic." Guidance Software, Web. 28 March 2018. www.guidancesoftware.com/encase-forensic#mobile.

"Free Calls & Messages." LINE, Web. 28 March 2018. line.me/en/.

"Forensic Toolkit." AccessData, Web. 28 March 2018. accessdata.com/products-services/forensic-toolkit-ftk

"Google", Google, Web. 28 March 2018. assistant.google.com

"iOS Definition." Tech Terms. Web. 29 March 2018. https://techterms.com/definition/ios

"iPhone." Apple, Web. 28 March 2018. www.apple.com/iphone/

"Pro Series" Cellebrite, Web. 28 March 2018. https://www.cellebrite.com/en/solutions/pro-series/

"Telegram – a New Era of Messaging." Telegram, Web. 28 March 2018. telegram.org/

"Twitch Desktop App." Twitch, Web. 28 March 2018. app.twitch.tv/

"Your Whole Trip, in One App." Expedia.com, Web. 28 March 2018. www.expedia.com/app.

"Watch Anything. With Anyone. Anytime." Rabbit, Web. 28 March 2018. www.rabb.it/