The Evidence Self-Destructing Message Apps Leave Behind

STROZ FRIEDBERG

Presented by:
Andrea London, Forensic Examiner
Kyle O'Meara, Forensic Examiner

8/4/2013

Presentation Synopsis

DEFCON

This presentation will self-destruct in 45 minutes: A forensic deep dive into self-destructing message apps

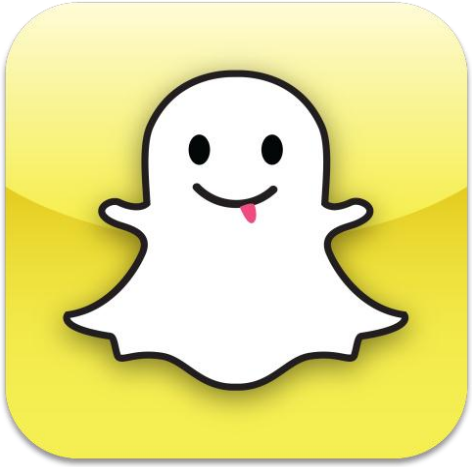
Prior to 2013, the phrase 'Self Destructing Message' was most commonly associated with Inspector Gadget, Maxwell Smart, and the occasional Tom Cruise movie. With the advent of smartphone apps like Snapchat, Wickr, and Facebook Poke, the self-destructing message has left the world of 'International Men of Mystery' and arrived to the civilian world by way of smart phone applications. These apps, and others, claim to provide ephemeral or private messaging to assure senders that their messages are burnt after reading.

A message can be encrypted, but that does not make it clandestine or deniable. Through the use of forensic images, packet captures, and API review - we have recovered a wide range of artifacts from messages before, after, and during transmission. We are neutral, fact finding, forensic examiners on a mission. A mission to seek truth and provide you with the results of our deep dive forensic review of self-destructing messaging smartphone apps.

Overview

- What is Self Destructing Messaging?
- Smartphone Forensics
- iOS Forensic Artifacts
- Android Forensic Artifacts
- Network Traffic Analysis

Self-Destructing Messaging Apps

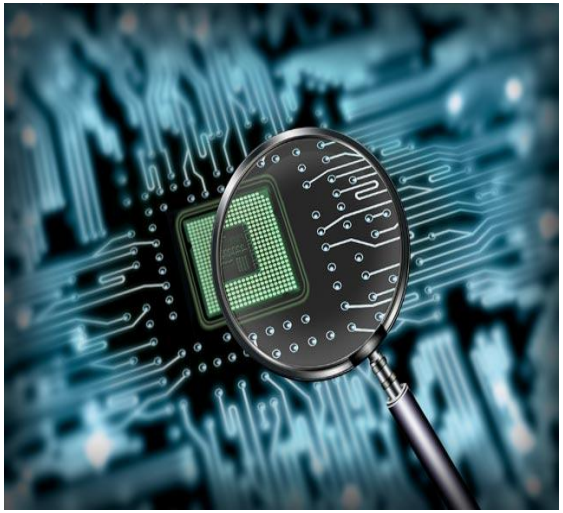


SNAPCHAT

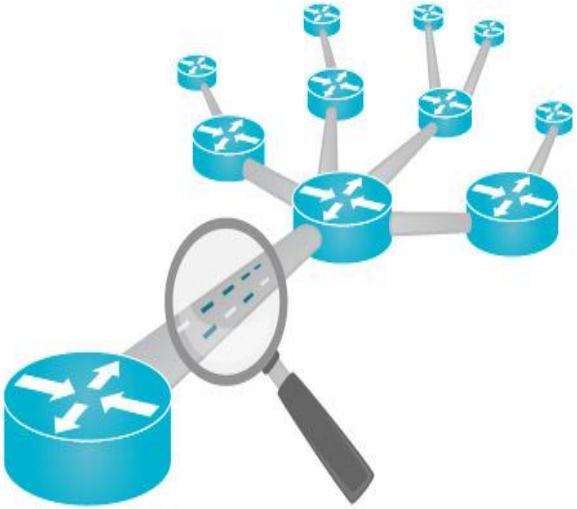
FACEBOOK
POKE

WICKR

Testing Protocol



Device Analysis



Network Traffic Analysis

Application Program Interface Review

Testing Protocol

- Devices
  - iPhone 4 running iOS 5 & 6
  - Samsung Galaxy S3 running 4.1.2 (Jelly Bean)
  - Samsung Galaxy S3 mini (rooted) running 4.1.2 (Jelly Bean)
- Software
  - Cellebrite Physical Analyzer v3.7
  - AccessData MPE+

Device Review and Analysis of Apps

Where do the apps store data?

Is supporting evidence present?

Is data cached in multiple places?

Is the message recoverable ?

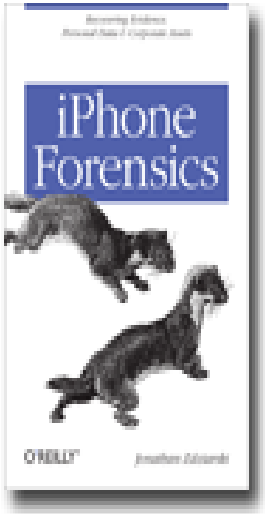
Is data encrypted on the device?

The Forensic Process – Then and Now

Analyzing phone contents directly from the screen and photographing important content

Able to recover phone memory with minimal disruption and analyze it separately.

iOS Forensics

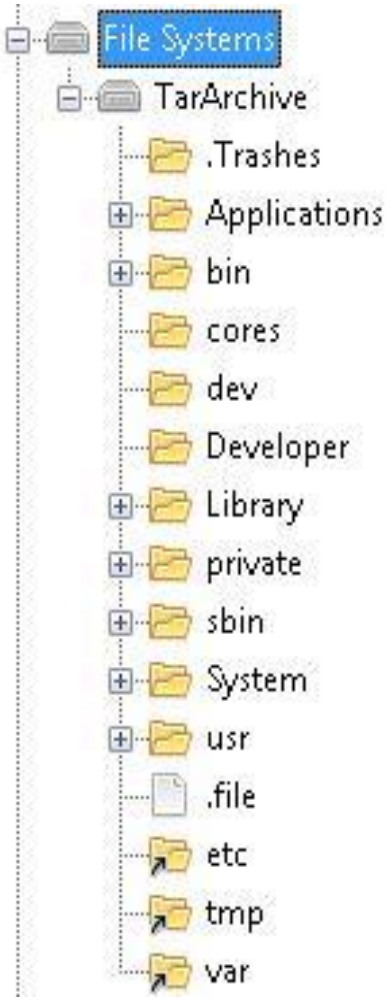


Physical Preservation

- Full copy of flash memory
- Requires custom images / jailbreaking for acquisition
- Possibly getting an encrypted file system
- iPhone, iPhone 3G, iPhone 3GS, iPhone 4

File System Preservation

- Full copy of file system
- Requires custom images / jailbreaking for acquisition
- Unencrypted copy of the file system.
- iPhone, iPhone 3G, iPhone 3GS, iPhone 4



iTunes/API Preservation

Whatever iTunes / API Can Access

- Photos
- Contacts
- SMS Database
- Application Data

All iOS Devices

Android Preservation

Physical

- Temporarily roots phone
- Bootloader for some Samsung and Nokia phones

Logical Extraction

- File system / Application Data
- SMS Database /Email Database
- Multimedia

Abuse

METRO News Sport Guilty Pleasures Ents & Tech Life & Style
TV Film Music Gaming Tech

Half of Snapchat users have received inappropriate pictures

Thursday 6 Jun 2013 11:29 am

Mashable SOCIAL MEDIA TECH BUSINESS ENTERTAINMENT US & WORLD LIFESTYLE WATERCOOLER VIDEO

Lifestyle FOLLOW MASHABLE

Teens' Nude Photos From Snapchat Lead to Investigation

1.5k SHARES 507 Share 808 Tweet 9 Share 31 128 2

NEWS Channel 5 ON YOUR SIDE newsnet5.com abc

Site GO>>

Sunday, June 16, 2013

HOME NEWS WEATHER TRAFFIC ENTERTAINMENT LIFESTYLE SPORTS MONEY MARKETPLACE VIDEO ABOUT

Snapchat - the 'now you see it, now you don't' app causes concern among Internet crime investigators

Local students learn about sexting penalties

Video Photo

Posted: 05/03/2013

By: Lee Jordan, newsnet5.com

Cleveland, OH

74° Cloudy Power of 5 Weather

• Forecast: Tracking a few showers Sunday

Cleveland Headlines

Man found shot at gas station dies

Cleveland Police are investigating the

MEMBER CENTER: Create Account | Log In SITE SEARCH WEB SEARCH BY Google Go

13 wthr.com INDIANA'S NEWS LEADER EYEWITNESS NEWS

Home News Video Weather Traffic Sports Entertainment Health Community Lifestyle Hot Topics

Snapchat App used to lure young girls

By Richard Essex - bio | email

LEBANON - Parents we have all had this conversation with our children about cell phones.

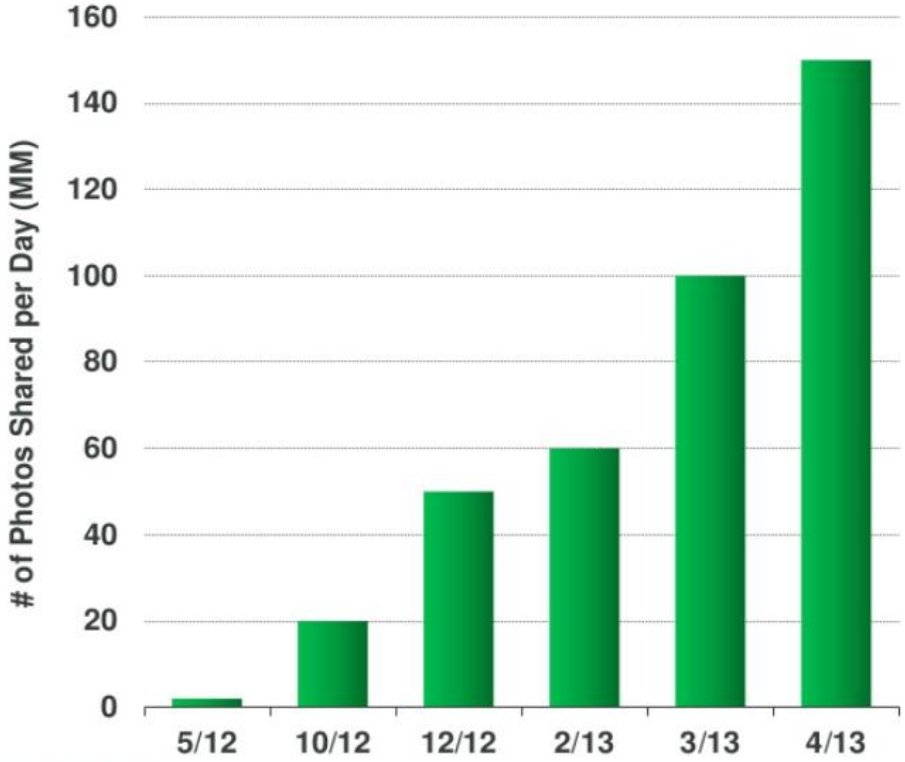
If you are like many parents a cell phone for your child is for their safety, then the phone becomes a problem, they send too much texting or too much time on the phone. Now you are going to want to check their phone for an app called Snapchat.

Most Popular Stories

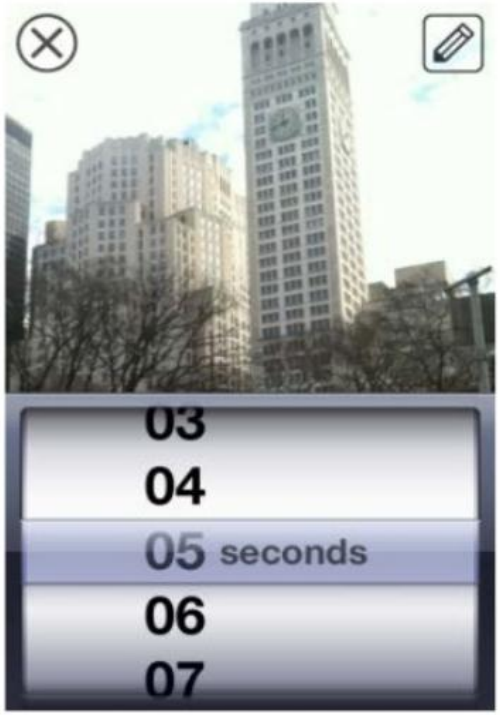
- Recycling center fire still smoldering, but under control VIDEO INCLUDED
- Fire evacuations lifted: Residents can return to their homes
- Two airlifted from Gas City I-69 roll over crash
- Warren County man dies in dirt bike crash
- Boy, 5, nearly drowns at Noble County park
- Shock lingers after Nazi unit leader found in US

Short-Term Sharing Exploding – Snapchat Growth From Content That Disappears, Up >2x in 2 Months

Snapchat Daily Number of 'Snaps' 5/12 – 4/13



Choose How Long Your 'Snap' Lives



KPCB

Source: Snapchat. 15

SnapChat + Law Enforcement

CONTACTING LAW ENFORCEMENT AND ASSISITING IN INVESTIGATIONS

If you believe that you or your child have been the victim of a crime that involved the use of Snapchat, please contact your local law enforcement for assistance.

With the right legal process from law enforcement, Snapchat is often able to preserve evidence, provide identifying information and cooperate with investigations.

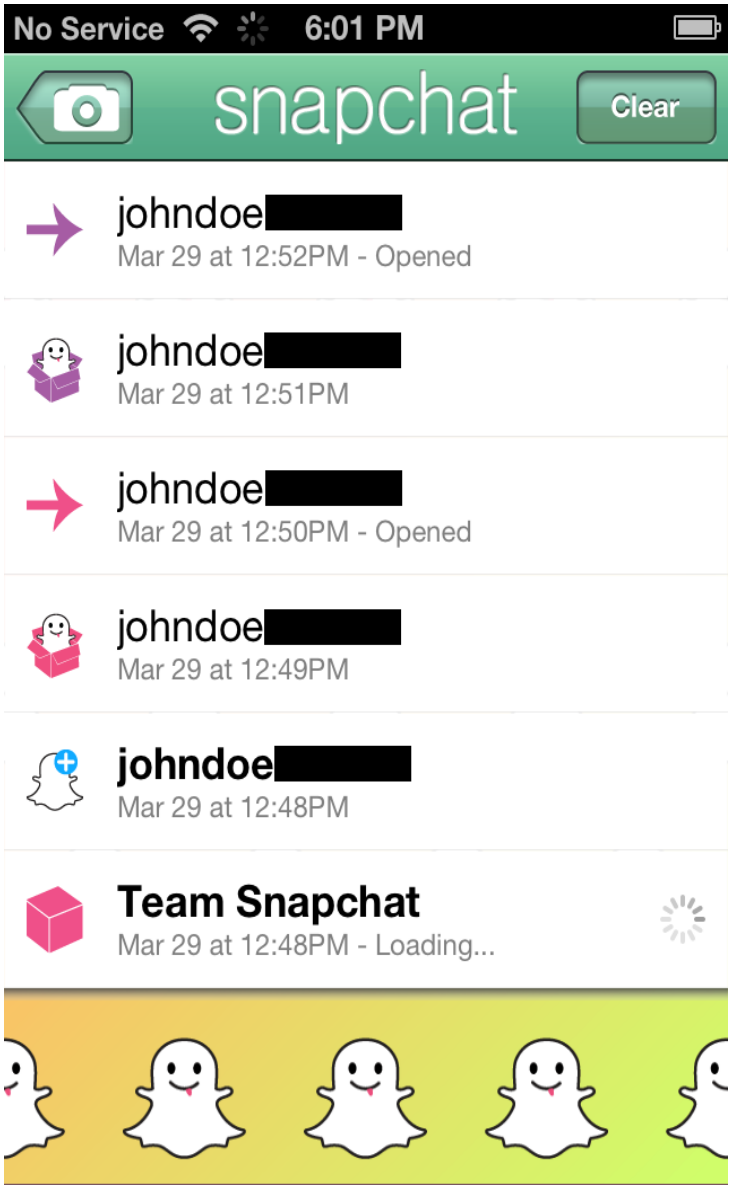
It is important to note that once a message has been viewed, it is usually impossible for Snapchat to retrieve a copy of its contents, even for law enforcement. If you wish to preserve evidence of the on-going receipt of illicit messages, leave the messages unopened and contact law enforcement. Unopened messages will expire after 30 days, but prior to that, they can typically be retrieved by law enforcement.

Please let the investigating officer know that they can contact Snapchat via email at lawenforcement@snapchat.com. We also offer a Law Enforcement Guide with further information, including a sample preservation letter and a release form for users wishing to authorize the release of their data to law enforcement without the need for a subpoena or search warrant.

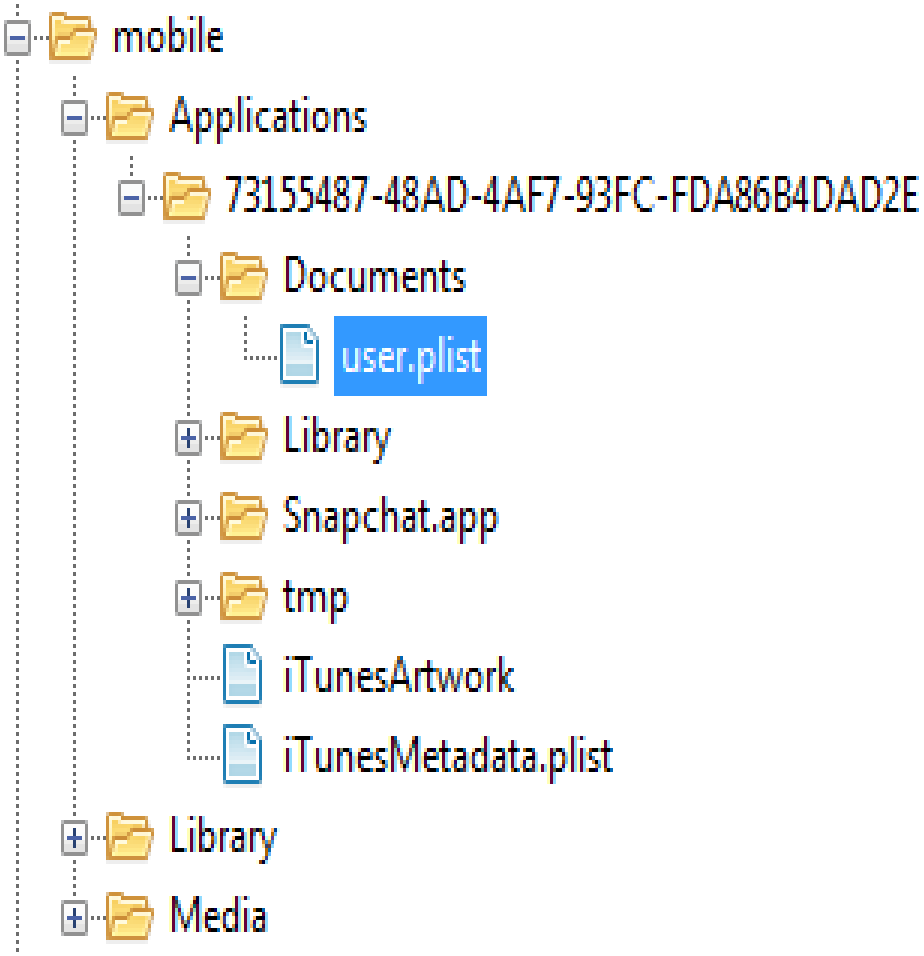
SnapChat + Law Enforcement

It is important to note that once a message has been viewed, it is usually impossible for Snapchat to retrieve a copy of its contents, even for law enforcement. If you wish to preserve evidence of the on-going receipt of illicit messages, leave the messages unopened and contact law enforcement. Unopened messages will expire after 30 days, but prior to that, they can typically be retrieved by law enforcement.

iOS Artifacts



iOS Artifacts



IOS Artifacts

user.plist

user.plist 〉 No Selection

Key	Type	Value
Root	Dictionary	(4 items)
$version	Number	100,000
$objects	Array	(53 items)
Item 0	String	$null
Item 1	Dictionary	(0 items)
Item 2	String	janesmith[redacted]
Item 3	[illegible]	[redacted]
Item 4	[illegible]	[redacted]
Item 5	[illegible]	(1 item)
NS.objects	Array	(0 items)
Item 6	Dictionary	(0 items)
Item 7	[illegible]	53846836457953839[illegible]
Item 8	[illegible]	johndoe[redacted]
Item 9	[illegible]	(1 item)
NS.time	Number	386,272,350
Item 10	Dictionary	(2 items)
$classes	Array	(2 items)
$classname	String	NSDate
Item 11	Number	2
Item 12	Number	1
Item 13	String	JANESMITH[redacted]1364579530JOHNDOE[redacted]
Item 14	Dictionary	(2 items)
$classes	Array	(2 items)
Item 0	String	Snap
Item 1	String	NSObject
$classname	String	Snap
Item 15	Dictionary	(0 items)
Item 16	String	35007364579470930r
Item 17	Dictionary	(1 item)
Item 18	Dictionary	(0 items)
Item 19	String	551644364579426331s

Timestamp

User Names

Message IDs

User.Plist Decoded

Object Name	Description
username	The user's Snapchat user name
snaps	A list of snap objects, with each snap object containing one message's metadata
friends	A list of Snapchat users on the user's friend list
time	The default timer value
email	The user's email address

User.Plist Decoded – Snaps

Snap Element	Description of Contents
client_id	Null for messages received by the user; Populated with an id comprised of the sender's user name, Unix time stamp, and recipient's user name for messages sent by the user
id	ID of Message
recipient	Null for messages received by the user; Populated with the recipient's user name for messages sent by the user
sender	Populated with the sender's user name for messages received by the user; Null for messages sent by the user
status	Message Read Status -- 1 indicates unread and 2 indicates read
time	Value of the self-destruct timer – empty for read messages
timestamp	Time when the message was sent to Snapchat's servers
type	Numeric value indicating type of message: 0 indicates picture message; 1 indicates video message; 3 indicates friend add request

User.Plist Decoded – Snaps Decoded

user.plist

user.plist 〉 No Selection

Key	Type	Value
Root	Dictionary	(4 items)
$version	Number	100,000
$objects	Array	(53 items)
Item 0	String	$null
Item 1	Dictionary	(0 items)
Item 2	String	janesmith[redacted]
Item 3	String	[redacted]
Item 4	String	[redacted]
Item 5	Dictionary	(1 item)
NS.objects	Array	(0 items)
Item 6	Dictionary	(0 items)
Item 7	String	538468364579538399s
Item 8	String	johndoe[redacted]
Item 9	Dictionary	(1 item)
NS.time	Number	386,272,350
Item 10	Dictionary	(2 items)
$classes	Array	(2 items)
$classname	String	NSDate
Item 11	Number	2
Item 12	Number	1
Item 13	String	JANESMITH[redacted]1364579530JOHNDOE[redacted]
Item 14	Dictionary	(2 items)
$classes	Array	(2 items)
Item 0	String	Snap
Item 1	String	NSObject
$classname	String	Snap
Item 15	Dictionary	(0 items)
Item 16	String	35007364579470930r
Item 17	Dictionary	(1 item)
Item 18	Dictionary	(0 items)
Item 19	String	551644364579426331s

User.Plist Decoded – Snaps Decoded

Id	Recipient	Sender	Time	Status	Type	Timestamp
538468364579538399s	johndoe[redacted]	janesmith[redacted]		2	1	3/29/2013 12:52
35007364579470930r	janesmith[redacted]	johndoe[redacted]		2	1	3/29/2013 12:51
551644364579426331s	johndoe[redacted]	janesmith[redacted]		2	0	3/29/2013 12:50
348326364579398983r	janesmith[redacted]	johndoe[redacted]		2	0	3/29/2013 12:49
545573364579338614r	janesmith[redacted]	johndoe[redacted]		1	3	3/29/2013 12:48
166456364579290377r	janesmith[redacted]	teamsnapchat	10	1	0	3/29/2013 12:48

Photos

- Snaps downloaded to the phone when Snapchat is opened.
- Snaps can still be accessed if phone loses Internet connectivity while Snapchat is open.
- Snaps are not accessible if phone loses Internet connectivity and Snapchat is closed.
- Stored in memory?

Videos

- Unopened videos can be recovered from the device.
- File names match IDs on user.plist
- Last sent video stored on device?

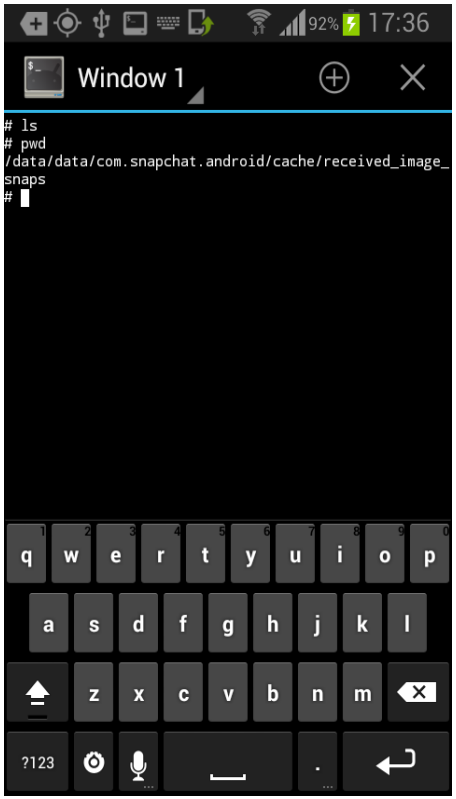
Metadata

- Data stored as XML files in data/data/com.snapchat.android
- com.snapchat.android_preferences.xml Closest Equivalent to iOS user.plist file
- Contains type, mSender, mWasViewed, mCaptionPosition, mCaptionOrientation, mIsLoading, mIsTimerRunning, mIsBeingViewed, MWasOpened, mWasScreenshotted, mDisplayTime, mId, mTimestamp, mStatus, mIcon, and mMediaType

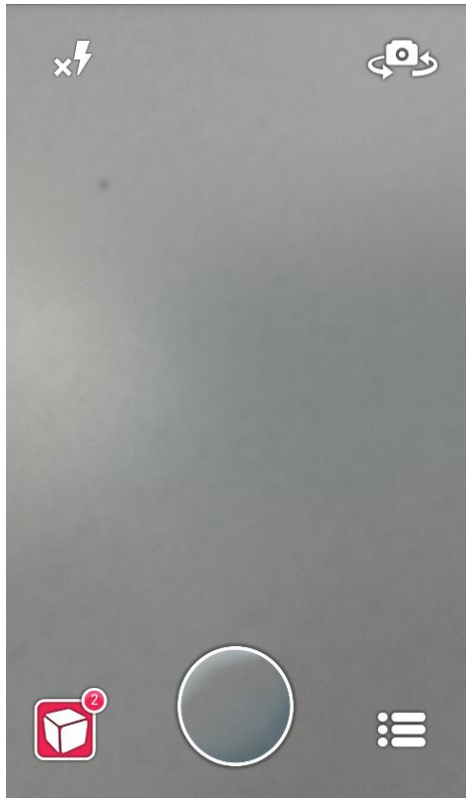
Snaps

- Stored as unencrypted files in data/data/com.snapchat.android/cache/received_image_snaps
- Snapchat deletes all snaps after last unviewed snap is viewed.
- This is not a secret – Snapgrab Android app has leveraged this knowledge since April 2013
- If the user does save the snap that was sent it will be located in /media/Snapchat

Snapchat on Root Android Device



Empty directory before receiving Snapchats



Two Snapchats have been received

Directory showing two images

Snapchat on Root Android Device

Viewed one Snapchat

Directory still shows two images present

All Snapchats have been viewed

Snapchat on Root Android Device

Directory is now empty

Network Traffic Analysis

```
2013-06-08 17:26:29 POST https://feelinsonice-hrd.appspot.com/bq/login
                        ←200 text/html 1.44kB
Request                                                    Response
Date:            Sat, 08 Jun 2013 22:26:31 GMT
Content-Type:    text/html
Server:          Google Frontend
Content-Length:  1475
Couldn't parse: falling back to Raw
{"added_friends_timestamp":0,"bests":[],"snapchat_phone_number":"+1310[redacted]","image_caption":f
alse,"auth_token":"0[redacted]70","received":0,"logged":true,"added_frien
ds":[],"requests":[],"username":"jason[redacted]","sent":3,"snaps":[{"id":"139369016027902r","sn":"
jason[redacted]","ts":1369016027902,"sts":1369016027902,"m":1,"st":1},{"id":"139369016027902s","rp"
:"jason[redacted]","ts":1369016027902,"sts":1369016027902,"c_id":"JASON[redacted]1369016025JASON[redacted]
","m":1,"st":1},{"id":"891606368923770781r","sn":"jason[redacted]","t":3,"ts":1368923770781,"sts":
1368923770781,"m":0,"st":1},{"id":"891606368923770781s","rp":"jason[redacted]","ts":1368923770781,"
sts":1368923770781,"c_id":"JASON[redacted]1368923767JASON[redacted]","m":0,"st":1},{"id":"651129368920
295880r","sn":"jason[redacted]","t":3,"ts":1368920295880,"sts":1368920295880,"m":0,"st":1},{"id":"6
51129368920295880s","rp":"jason[redacted]","ts":1368920295880,"sts":1368920295880,"c_id":"JASON[redacted]
[redacted]1368920291JASON[redacted]","m":0,"st":1},{"id":"755808368920283590r","sn":"teamsnapchat","t":10,
"ts":1368920283590,"sts":1368920283590,"m":0,"st":1}],"friends":[{"name":"jason[redacted]","display
":"","type":0},{"name":"teamsnapchat","display":"Team Snapchat","type":0}],"device_token":"24AA3
51387[redacted]9128EA447","email":"jason[redacted]@[redacted].com","
[2/27]                                                     ?:help q:back
```

Decrypting Snaps

Snaps appear to be encrypted / obfuscated

Multiple people reverse engineered the Snapchat Android APK

- Arlen Cuss's Snapchat: not for state secrets
- Thomas Lackner's Snaphax PHP Library
- Neil Hanlon

Findings:

- Data is encrypted using AES in ECB mode
- Media is decrypted when it is downloaded (e.g. not immediately before access)
- Encryption key is: "M02cnQ51Ji97vwT4"
  - http://adamcaudill.com/2012/12/31/revisiting-snapchat-api-and-security/

Decrypting Snaps

Snaphax / PHP

```
function decrypt($data) {
        return mcrypt_decrypt('rijndael-128', $this->options['blob_enc_key'], $data, 'ecb');
}
```

Arlen Cuss / Ruby

```
> data = File.open('x', 'r:ASCII-8BIT').read; nil
=> nil
> c = OpenSSL::Cipher.new('AES-128-ECB')
=> #<OpenSSL::Cipher:0x007f8182658618>
> c.decrypt
=> #<OpenSSL::Cipher:0x007f8182658618>
> c.key = 'M02cnQ51Ji97vwT4'
=> "M02cnQ51Ji97vwT4"
> o = ''.force_encoding('ASCII-8BIT')
=> ""
> data.bytes.each_slice(16) {|s| o += c.update(s.map(&:chr).join)}
=> nil
> o += c.final; nil
=> nil
> o[0...60]
=> "\xFF\xD8\xFF\xE0\0\x10JFIF\0\x01\x01\0\0\x01\0\x01\0\0\xFF\xDB\0C\0\x14\x0E\
x0F\x12\x0F\r\x14\x12\x10\x12\x17\x15\x14\x18\x1E2!\x1E\x1C\x1C\x1E=,.$2I@LKG@FE
PZ"
>
```

Facebook Poke

- The Poke App
  - Branded as a 'simple and fun way to say hello to your friends' app
  - Runs on iOS devices running iOS5.1 or later.
  - iPhone3GS and above, iPod Touch (4th and 5th Gen), and iPad
  - Can send messages, photos, and videos
  - Sender chooses how long, up to 10 seconds, their friends can view the message
  - 'After that, they disappear from the app.'
- Our analysis
  - iPhone 4 running iOS 6.1
  - Physical acquisition, file system analysis, network capture anaylsis
  - Used Cellebrite Phyiscal Analyzer to do the physical and file system
  - mitmproxy and Wireshark configured on a MacBook to network capture analysis

iOS Artifacts

Directories of interest

- 3021DF18-B5A6-41CF-BACD-8BEA55B4ACCC/Library/Caches/com.facebook.Poke
  - Cache.sqlite - contains information related to profile pictures associate with app users Facebook friends
- 3021DF18-B5A6-41CF-BACD-8BEA55B4ACCC/Library/Caches/FBStore/315_14_/FBDiskCache
  - Contains thumbnail pictures size profile pictures of Poke app user and Friends they communicated with through the app
- 3021DF18-B5A6-41CF-BACD-8BEA55B4ACCC/Library/Caches/FBStore/315_14_/
  - Store.sqlite
    - This is the gold mine of artifacts
    - ZPOKEMESSAGES table
      - Recipients – appears to be a counter
      - Sender - 2 represents device
      - Time Limit - time message was sent
      - Creation Time - in absolute Mac time
      - Media Type - null or MediaType
      - Message Text - the specific text that was sent

Part of the ZPOKEMESSAGES Table

ZLOCATION	ZRECIPIENTS	ZSENDER	ZTIMELIMIT	ZCREATIONTIME	ZTEXTYPOSITION	ZGRAPHQLID	ZMEDIATYPE	ZMESSAGETEXT
NUL	104	2	3	389711562	0.99	608835746809	image/jpeg	NUL
NUL	95	2	3	389711592	0.99	608835776749	image/jpeg	NUL
NUL	98	2	3	389711631	0.492	608835796709	image/jpeg	NUL
NUL	100	2	3	389711688	NUL	608835986329	NUL	NUL
NUL	101	2	3	389712024	0.492	608836495309	image/jpeg	NUL
NUL	97	2	3	389712086	0.492	608836649999	image/jpeg	NUL
NUL	102	2	3	389712104	0.99	608836689919	image/jpeg	NUL
NUL	99	2	3	389712144	NUL	608836749799	NUL	NUL
NUL	110	2	5	390246930	0.492	609388893299	image/jpeg	This is a Mac mini.
NUL	109	2	5	390246391	0.492	609388109869	image/jpeg	NUL
NUL	196	1	3	393862642	NUL	137067846497520	NUL	
NUL	199	1	3	393862736	NUL	137068226497482	NUL	
NUL	201	1	3	393863052	NUL	137069539830684	NUL	
NUL	200	1	3	393864008	NUL	137073716496933	NUL	
NUL	198	2	5	393864049	NUL	614325704889	NUL	NUL
NUL	197	1	3	393886482	NUL	137196519817986	NUL	
NUL	171	1	3	393888017.53038	0.00	NUL	NUL	
NUL	195	1	3	393889715	NUL	137206849816953	NUL	
NUL	370	1	3	393953328	NUL	137409913129980	NUL	Defcon rio Las Vegas
NUL	372	1	3	393953374	NUL	137410019796636	NUL	Stroz Friedberg digital forensic
NUL	381	1	3	393953401	0.99	137410496463255	image/jpeg	NUL
NUL	380	1	3	393953426	0.99	137410539796584	image/jpeg	NUL
NUL	377	1	3	393953480	0.5853	137410646463240	image/jpeg	Two forensic books
NUL	371	1	3	393953507	0.5721	137410746463230	image/jpeg	Basketball hoop

- ZPOKEMESSAGEFEEDEDGE
  - Time Updated – in absolute Mac format
  - Viewer State – can see if the message was viewed and screen captured
- Other tables in Store.sqlite that related to the associated Facebook account not necessarily specific to the Poke app
  - ZAVATAR – rows of interest: Alias, FBID, Name

iOS Analysis

- 3021DF18-B5A6-41CF-BACD-8BEA55B4ACCC/Library/Caches/Snapshots/com.facebook.com/
  - contained a photo that was taken of the main page inside the app. If the user doesn't clear their recipients, it may be possible to see recent communications
- 3021DF18-B5A6-41CF-BACD-8BEA55B4ACCC/Library/Preferences/
  - 6********9.plist - related to FB user of Poke ap
  - 1**********4.plist – related to FB user of Poke app
  - com.facebook.Poke.plist – plist that contains general information (see picture)
    - user agent
    - Login UUID
    - Last Facebook register time (Unix format)
    - Database locations – we already looked at these locations

com.facebook.Poke.plist 〉 No Selection

Key	Type	Value
▼ Root	Dictionary	(16 items)
DeviceInsightsAttributionIDKey	String	1[redacted]1
WebKitDiskImageCacheSavedCacheDire	String	
APNSPushRegistrationAttemptTakenPla	Boolean	YES
DeviceInsightsAttributionExpiryKey	Date	Jun 27, 2013 11:22:22 AM
APNSRemoteNotificationType	Number	7
timer	Number	3
WebDatabaseDirectory	String	/var/mobile/Applications/3021DF18-B5A6-41CF-BACD-8BEA55B4ACCC/Library/Caches
WebKitShrinksStandaloneImagesToFit	Boolean	YES
APNSLastFBRegistrationTime	Number	1,372,260,481.2266
WebKitOfflineWebApplicationCacheEna	Boolean	YES
com.facebook.analytics.deviceInfoExpir	Date	Jun 27, 2013 11:27:09 AM
APNSDeviceToken	Data	<f1[redacted]f>
FBLoginUUID	String	EE[redacted]5
WebKitLocalStorageDatabasePathPrefer	String	/var/mobile/Applications/3021DF18-B5A6-41CF-BACD-8BEA55B4ACCC/Library/Caches
FBUserAgentSystemUserAgent	String	Mozilla/5.0 (iPhone; CPU iPhone OS 6_1 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Mobile/10B141
FBUserAgentSystemVersion	String	10B141

Network Analysis Poke App

- Used mitmproxy setup to capture traffic between iPhone devices
- Messages
  - Sending messages
    - POST to _https://graph.facebook.com/me/pokemessages when sending messages
  - Receiving messages
    - GET _https://attachment.fbsbx.com/poke_media.php?id=*******&access_token=******** when receiving messages
    - POST https://graph.facebook.com/graphql/
  - Under SSL payload is just gzip encoded – no further encryption
  - Can easily save payload decode and extract any picture
  - If text was just sent, 'media_type' field in the payload is 'null'
  - If only picture was sent, the 'media_type' field in the payload is image/jpeg
  - If a picture message with text was sent - the payload will include a 'message' field that also contains the text sent with the picture
  - Can verify Facebook IDs and there associated accounts that are seen in communications using _http://developers.facebook.com/tools/explorer/

Network Analysis Poke App

MITMPROXY payload of picture message

```
2013-06-26 11:33:25 GET https://attachment.fbsbx.com/poke_media.php?id=[redacted]&access_token=[redacted]
                        [redacted]
                        [redacted]
                        ← 200 image/jpeg 28.1kB
Request                                                    Response
Content-Transfer-Encoding:  binary
Content-Type:               image/jpeg
Content-Encoding:           gzip
X-FB-Debug:                 J1xF5Ygk+VIrWWN/ljBHrWYGNgjMKw9VqUobeU1nkl0=
Date:                       Wed, 26 Jun 2013 15:33:24 GMT
Connection:                 keep-alive
Content-Length:             28770
[decoded gzip] JPEG image
Format        JPEG (ISO 10918)
Size          360 x 480 px
Mode          RGB
icc_profile   ....lcms....mntrRGB XYZ
              .........).9acspAPPL.................................-lcms.............................................
              desc.......^cprt...\....wtpt...h....bkpt...|....rXYZ........gXYZ........bXYZ........rTRC.......@gTRC.......@bTRC.......
              @desc........c2.......................................................................................text....FB..XYZ
              ...............-XYZ ...........3....XYZ ......o...8.....XYZ ......b.........XYZ
              ......$.........curv...............c...k...?.Q.4!.).2.;.F.Qw].kpz....|.i.}...0..
jfif          258
jfif_density  (1, 1)
jfif_unit     0
jfif_version  (1, 2)
progression   1
progressive   1
```

MITMPROXY payload of picture message with text

```
locale:           en_US
text_y_position:  0.5721154
access_token:     [redacted]

sdk_version:      3
time_limit:       3
sdk:              ios
message:          Basketball hoop
recipients:       ["68800659"]
pretty:           0
app_version:      93694
format:           json
media:            ......JFIF............XExif..MM.*..................i.........&..............................h...................C.
                  ..........................................................?..........C.............................................
                  ............................h.."....................................?
                  ....................}........!1A..Qa."q.2....#B...R..$3br.?
                  .....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.............................................................
                  ....................................?
                  ....................w.......!1..AQ.aq."2...B....?#3R..br.
```

Wickr

LEAVE NO TRACE™

Wickr App

- Wickr app
  - Free app that allows for encrypted messages to be sent from user to user
  - 'Leave No Trace'
  - Compliant with FIPS 140-2, HIPAA, NSA Suite B Compliancy
  - Used AES 256 to encrypt data
- Our analysis
  - iPhone 4 running iOS 6.1
  - Physical acquisition, file system analysis, network capture anaylsis
  - Used Cellebrite Phyiscal Analyzer to do the physical and file system
  - mitmproxy and Wireshark configured on a MacBook to network capture analysis

iOS Artifacts

Directories of interest

- 624E929C-1990-4A46-9ADA-4D6D682DD0FB/Library/Caches/com.mywickr.wickr
  - Cache.db
    - Contained no data
- 624E929C-1990-4A46-9ADA-4D6D682DD0FB/Library/Caches/Snapshots/com.mywickr.wickr
  - Snapshot picture but the photo is black i.e. nothing duplicated
- 624E929C-1990-4A46-9ADA-4D6D682DD0FB/Library/Cookies
  - Cookie.binarycookies – no content of interest
- 624E929C-1990-4A46-9ADA-4D6D682DD0FB/Library/Preferences
  - com.apple.mobileslideshow.plist
  - com.mywickr.wickr.plist
    - Included database locations
- 624E929C-1990-4A46-9ADA-4D6D682DD0FB/tmp/aforensics
  - 3 files random.af0, random.af1, random.af2 – contents of each file is all zeros

Network Traffic Analysis

- Used mitmproxy setup to capture traffic between iPhone devices
  - Sent messages
    - _https://secex.info/service/103/src/postMessage.php
  - Received messages
    - _https://secex.info/service/103/src/downloadMessage.ph p
  - Payload size provides possible indictator of what type of message maybe have been sent.
    - Text or picture or video
      - In test case each payload was significantly longer
  - Payloads appear to be encrpyted under SSL
    - First 5 bytes are similar in each payload –
      - 0x313336342B or 1365+ (ASCII)
  - Messages in memory that may be captured on the phone could be capture and kept 'forever'....BUT cryptographically protected

Network Traffic Analysis

Sent message sample payload


```
--Boundary+0xAbCdEfGbOuNdArY
Content-Disposition: form-data; name="json_id"

7505b440d12f8822e8d3e314b6ff92977eb1c45b91162d50b7457b14ee3d9535
--Boundary+0xAbCdEfGbOuNdArY
Content-Disposition: form-data; name="json_secure"

uthic6gner8oZ4vXW1JJCYJQFS5aKP2SVkKanaNl/qsPWkLH08KfU6kAR3p3vpFW0kGprN2BksTiAd9mjpt4lndymROOWnYr1Y/2iSbMLNQ1vg2Fqf1YowuL1xAaHe1a0vBBu
m7TMa0zP8f0OQnn0E286FLcjNdr/5iW8jgDd64k3DPV9uT2xfiBJ0ciQ/ykFx66dpAdNJm/0NmX1D5JOACFKfYMAPKXiDuDE0s4G6AqIE1BXkcOrGWu7WbdJZncvZrWwc6BNO
60C/TGuxKNgflXdUz6dsI2N+LFqHvn/8W7DZc0AgnlZg3PqHLHrQ0zsnW8gB8GE3OTipc0Hj191RBQe2dxCTR4vGQl3bUvb4JYqxmO+U3qlJqTtmpc1yM4WKCxr/Ru9/bsd3o
v8OyD4TpCFZupgLDt1TmC76KrwDE4wnh9SOpLGhZA5LTGmcjAd6RXnug2/V6yibftGm/VLsXiiU3b/M2iWeyQAeCYlqZpimgleQKtChEHIzIhQnJVjVlzqBOF6DpcxSvmJNkM
B4gL4OxLTUOHOi8dzc/xxaI+nYTACBayWBdrl+lKP9ISgEyOKmYne0dBN6mK+g==
--Boundary+0xAbCdEfGbOuNdArY
Content-Disposition: form-data; name="blob"; filename="blob.msg"
Content-Type: sec/blob

1364+^X*"<84>^Q7<EE><A5>I<DC><E9><9C>+L{U<C8>t<BB>^C<95><A6><B7><A3><D8>M<B9>ESC^\g<F8><99>^^?<FE><88>"-<B5><80>^F^L<D5>.<FF><B4>^?
<BC><E1>^G<8B>^G<D3>C<F8>^Z<F1>y<DD>-<AE><9E>5<B7><BF>n^T<BA>z^V<FB>G<91><D6><E0>7<85>Ig<F0><DE>-<92><EE>3<D1>P<F2><F3>^\A-f<A2>0p
<BA><DA>bhW<92>Y<FE>1A<D3>x<A5><A4><9D>I<AF><D2>1bz<98><CB>#^XESC<AD>^ObrV<CB><DB>O<F8><98><B5><F8>+<CC>%<95><95><AA><FC><83><82>~\(
<91><E2>^H.<A7>x^F^OF^U\^Z%:J<BB><81><D5>iYl7<F2>ei<DE>^S<81>:8<EB>^@<EF>rU~p<DA><F7><A6>P0
Qg8b <ED> <80>^ <E2>^E<CB><C5> <FD>>s`(^O) <8A>w <AF>^G<D5> <BD>/. <B5> <91> <E8><B8> <B1> <C5>W <U+077A>^ <97><FD><E4> <AD>^ :
<C1><E7><FF>=Q^N<F0>y<FB><8D><84>^D<FE>i<87>^C<nlX<E2><A6><94><BE><97><F7>.?<D5><U+D8C0><88>NgA^\wp6gT<90><C2> <B9>^V90>J>^RXJMY<BA>fP
<C0><B6>cZ4<CC>~\^G<C8> <BF>n^C||<86>X<E2>^K<EB><D1>_^G<GB>]P t<C3>f<C7>D<93>^Z<F7>^S^@U<D2>Z^R<8A><FF>h<9D><FA>^MQ<81><BC>><E9>E^?
<F1>e^^><97>QU1}<96>c<EE><8E>m<9C><A2>8<F8><DF><F9>^DT<C1>l<ED>V<B4>Лх^<95><F3>I~<8A>x<E7>L<C7>a^@<DE><F9>/_^U<A3><C7>uC>#3
^Wrn<F2><ED><88>^W<B0><C1>~LuDw<A3>^B2_*<ED><84><E3><AA>8/<B7>:Ed<A6><D6><C8>^@<B9>^Z<DA S#z <86>^ 7 <9A 1 ^\<B2
<A7><87>é<F8><A8>+Gb^V3<C4>^US^F^_<D1><96><8C><EC>J<B6>Hi<8F> }<8C>&<8C><B3>-<B2><A4><C5>l<BC>x<AB>L!k^?^Vd^X<F1><97>fV{&e<C8>^Z<EC>
<EB>N<BD>7<CF>z<D9>a<CB>^N<9B>2tESC<E0><8F>FY<8A><BE>:<AB>H<DB>l<98><93><84>8>FA>^E^]<B3>Qy<86><A4>u<81>!<C1>p<D4><C6><E1><C5>O<F2>ᄅ
`K<9C><D7>T~<FB>i<AE><E1>^]7<EA><82><C6>^Y^M<8F><BA>h1 ^Y<9C>;^D<92>{^Q/t<9A>c<E7>\<88>F<88>H<CC>D<BA>S<F1>X<9F><A4>ESC
<U+0082> <8D>jL^U<C6>#f<C9>h@a<CE>+<83>@<D4>,=<E8><FD><BF><E7>3!<D2><FF>qXŸ<AF>p<AA>\<FD>X<81>h#^C<88>^Y ^T!<A1>uNU`9<E3><F7>A
<E7>SS<DA><F5><A9>PIP<EC>^F^X^Jy<F9><E0><E7><9A>M><8A><C1><D2>B=e<AC>_U^QR<A0><CB>s<E7><B5><F7><B2>7<BF>j<F3><C1><DD>G^U<9A>^K<F0>
<FC>^W<9F><A3>M<A3><B8>?J<B9>\<85><B0>MU<CD>*`~><EC>ib<E5>(^U#9<C0><8B><F4><F4>H<A1><ui1`]^U~<86><CE>C<80><93>/.<FD>kx +^?[<A6>x~0
<81><A4>i(>{^Y<EB>L:<A1>E<U+D6322><86><C2>>Qh<8F><F5><95><8E>
^F<A1>mZ<CD><D5>^Ajw^Dsp<D1> ^MS<9C>Ms<CE><E2><BB>^T^V^S\<9B>B3<91><8B><AB>[<8A>^N@<F3><85><CE>B<A8><8B><90><D4>^Kvy<BC>7b><DA><D4><r
<C3>dESC<9B><93><B8>R_<C2>@<A4><93><A2>W<B3><E5><99>"_2<D9>l;^C<DA>5KъCΛ<A8><CF>c&"<97><AF><C3>8 <F3>x<FC>B<D6>(G<85><DC>^?'<CD>+
<AE>9<C8>=^G<98><97><DF>^D<E2><FC><9E>c(<8C><8A><D7>WH'<B2>&[<]<92>5<C3>t<AA><EB><89>N!<D7>^R<DE><E6>4^U~<E0><DB><D7>^R<CE>"<C0><F6>#
3<B0>(ÅWi<D1>_<C6><E1><8F>^Gb<E5><A1>g^D<95>^Sq^D <E6><95><E2>[<DE>eD^U j<CF><F6><C6>&^C<96>,1<9D><AE><BC><C0>m <DB> ]]ESC<88><F0>
<A0>^V<98>Söq<BF><99>^T<BD><D8>64<90>!<C5>]d^K<97><BB><A3>&<BD>E<9B>&D8<8B>ESC<B6>_<C3>a<FB>V(<A3>*<C6><DE>^Gc<CF>GG%<B0><DB>^_^F<9E>
<B5><D5> X<CD>H<E7><F5><83>W8m<F1>U<8C>A^C<99>k<DE>J<F0><A2>U_<9A><A5><95><D0>^_<95>Zqcp^B<83><AC>,<E9><F0><C9> q^WP<B1><85>U<C7>"^B
```

Network Traffic Analysis

Received message sample payload


```
1364+<EB>^P^W<C5>^M<96><BA>H<8C>I<E8>E^DQ`<F7><BC>!<91><D6><EE><C0>     <8B><8C>^_<U+0382><C9><D5>5<C8>{<C0><8B><F0><B3>/<F3>N<9A>7
<C9><EA>^O<CC>T<A6><AB><BB>t<AB><F9><AE>^X^@<DD>^R7<E2>^X<85>^E<AA><D3>O<95>h
^A?<A7><C9>/t^C^_S<E8>^U<F2>/<B5><FD><DA><CB>^T<87><AD>u<95>^\<F8>rT<FB><BE>^[E<AB><BA><8F><B3>^A<CE>^_uz<A8>2^F<A8>^ Y7 <A7> <B6
<87>^Put{<B4><D7><D0><DF>UY<F3>1^D^L<E2><F8>]T<AB>\,^\<E9><BD>4<9F><B9>hhS<FF>*<E4>[<88>1^Z<C5>^X<E3>&^X<AA>;.<93><90>V{<EA><83><A
<A3><B8>_k<EA>8BX2<BC><E0>c<F0><AA><FE><AB>^K<AC>re<D7>+<94>^Q^Pk<A2><E3>o<86>6c<8C><DA>{ue<DA>4+nXu^^L^D<9D>*     <9E><C4>;<FB>^GC^R
<E2>V<AB><BC><96>     ^Fe<8F>M<C5>Y^^U<EC><85><EC><E7>fm<A4><A7>g<E6> M<9E>^$<<89>;<F7>0C^B^ZHh;8D<AA>V<95>A^F<CE>N=^R<CB>\<FC>J(<E7>
<DF>^K4<AF><B2><AC>i^C<U+A749>d^C<95><A7>D<A6><98>tI^Nke<AC><B0><DF>     <91><BC>5I#i+.<93><E3>z<98><93><E2>^M;<FE><E0><CB>@3Kl<C1>^X
)<BD>`h<8B>^Xy{xk<96><ED>]^CM^E<F9><A6>^K^AxHR<E6>s0<80>K<A6>XZ<99><F8>lxB<A5>^K5<81>^Co^Z^X<F2>^]<83><82>`<DF>)<BA>[redacted]#łG.5<EC><F3>
<FE><C9><DD>n<BF><BE>.<91><F7><B2><AD>f+ESCpE<F4>^X<8E>2+<EB><C3>z<E6>@<93><D2>(<ED>^_^A<F2>Ψ{<9E>1<BE><DF>^]<D8>\7<F8><91><FF><E1>J&
<94>q_<B6><B7><90>]<EE>D<DF>#<90><F4>5N<D3>(6^F<93>M<99><CD><EE><D8>l<U+07FB.0d <DF !( <90><92 Gn <A7 <BD <D4 yU <AB <81 q
<95>C^L<86>^HJ<EE><D6>^N<81 <EE><EC ^W<85 <A2>^E<D1>^R<A5><ED>^ à ^\<C4 pV <F5 <F2 <EA><A7><F5><A0><FA +;*`f ^K<B7><F3 <D3 B
)<97><C8>2<CA><C3><C5><D8>a8,<F3>Y06]H<A8>^U^\<A8>^YzX<BF>GKs<B4><BB>,$?1i<D1><D2>T<96>\{`^^R<82>^H6P<F3><C2>r<CA><FC>7<F5><DE>p<FF>
<B5>3<E7>^F<9C>gj^D<D6>!<FF>
<A6>n<D9>x<CE>J<8A><B1>&<84>Z_<AB><E2>[<CA>
<EE><DF>I^TI^0<9C><A3>z:<BE>n:<C6>1<F6>^R^U<C3><EA>^^<A1><8F>^@^Mw<9C>4<F6>wes#0KL^<98>^A<B4><F4>W<F8>[<EF>M8$<B4>Vl#z<FF><F3><8C>
<EB>!,USK<E6>uk^R<E3>Tl2<81><A3><BB><BF>[<D1>P<BF>ED<81>^Q.^O'<CD>g<B3>^W^V^K<8C><87>/<A3>?<EE>?<F3><E1><B8>W<^M5<9C><D1><E8>><8A>P\
<9D><F6><A7>xth<AF>%pQ<84>@;<EB><C2>^^?<E2><CB>a%<82>A^?=<E0><BB>^H<D4><BA><F7><E8>[<B0>?<81>3<D3><FA><A5><B6><BA>Z[<C9>rx<B6>^Cc
<83><88><FA><B1><AF>A^U^^<F4><A7><F4>UU<B7>^P^X<D7>j<A4><EF>V<F6><F6><E8>Y^M<FC>J<B4><E9><89>,Xddyc<B7>`ý^]<F5>ESCr<FE>^C<99><E8>=W
<C0>ZpL<F9>=m<F5>+I<9B>^Og<97><D1><F4><9B><B3>G<B6><E5>z<8A>Ut<88>ē<DD><FA><EE>`Z}a5<AB>e?<BB>B<8F>T^B<AD>p^W#<EB><B6>^P<CE>
<F5><98><DA><D7>l"X,<AC><EE><CA>V<E3>z"<D3>Aq^^#<F8>&<90>v<F4>r<BC>D<D9>4<87>!<CD><DF>^]^S^H<C1><B6>=<DB>^G^U^D^P^<97> A=^L o<DB><F7>
&<AD>h0B2<88><DE><C6>:_<DB>8<BD><B5>F<U+E7D7><D1>$e<96><DA><FE><9A>?<D0><D7><FA><A9><98>?<9B>q<U+05ED>ESC<E0>'<8F>f<FE>^]<FE><99><A6>
s<8C><8F>^V<E1><9D>/^X<CC><E7>J^S-}^U<DE>tt^B<84><A9>,>^T^G<AE><E6>#<9A>W^SV<AE>^F^N<D6>^S5ESC<E3><F5>1^S<F3>-p<B8>r^W<81>^?ESCr@<D3>
sdE<B8>^G<E4>^^*<B4>x<AF>TM<B2>w!ESC9hC<AA><DB><EB><D4>[^_<81><90><BD><CA><E0><A5><DE>aad^W<FE><B0><89>]^G<B8>G<C8><F6>=^U^B[redacted]<A3>
<E8>^E<BB><88>^Eg
}<D1>a^<AA><8F><BF>h`Yt<B3><A5>EX<83><BF>@<F1>!<D7>8<D3>r!<8F><91><DF>^A<DE>P[:^X<B7><93>z<8B>^N<EC>`^]<F9><E5><89>^PE<92>%<8D>9<CC>
<C9>.<C9>H <AC>^NBF?+<EB>|<F1><B9><BB>Q4<9E>\U<8D><FD><9F>v_Z3K<88><80>]<9F><F7>h<D8>^B)^X<E7>^M^X<E2>^G<DA><ED><C9>T<B1><U+0609>
<E8><E8>N<F9>[w<D7>I^G<E1><FB>^C[Zz<B7>Z+$B<AF><84><B5>^U?`<EE>1<CF>%^_<B0>7<9B><96><F4>^F<C5><E7><C0><93>P<BB>m<8E><C0><D5><CB>o<A3>
<E9><AD>^Z<DB><DB>3[<84>+N<EE><F3><94>yH^W%*<85><A4>2<BB><A3>^L^S<91>[^G<D7>^S<9C><F8>.193+4<D9><D9>^Nrr^U^S^XVjQ<C2>P<8A>^L/<E8>
<88>t<EB>:(^CG<F6>D<AC>;<ED><F7><8D><E2>;#<88>^YQ<A5><81>U<A2>     <F9>#.<E8>!<B4>^E<83><96><F1><E9>Mv`.<E1>.<83>^D<DB><E6>4#<BB>0<BC>
_ŪfycωW<A7><BA>FQs^?.Y^K<C9>5S28s<E5><89><FA><AA><F3>öx!<FA>n\<D9><CC><F4><A2>~<8E><B3>^<EF><E3>^_<8D><B0>^S<B8>^M<E6><87><EE>L6<AE>
<95><BE>{7o<ED><DD><C7>U<92>6sc<CE>,<E0><93>GJqN^\%^F<B0>'<8A><9A>\<F3><D0>l<D9>;<F0><C3>©<BA>z<B3>^P<E2><D0>Bc<D3>~.<8F><B7><EA>γΠ
<9D>^K^Y^^<94><A7>     106+<FD><82>^WŪ<A1>}<F2>8<D1><E7><BD><E7><F9><BC><C3><F3><8D><93>ℳ ^M<8B>dQ;<^\?<98>;<EC><B2>,<D9>^Q^Fe<FF>^\
<A7>l<87>#^Gě菴_<A2><D1>|<F4><E4><9B>@{<C5>0[r^@@Lld<B0>|?<93><8F>G<B4>^W<90><FC><E1><96>i*<D2>^DPS<87>5<C6>p^K<CF><CD>F}<B3><FF><D3>Ï
_<91>^_:00+
```

Summary

Our findings

- iOS Devices
  - User.plist
  - Wickr – nothing significant
- Android Devices
  - com.snapchat.android_preferences.xml
  - Cached images

Future Research

- Unallocated string searching
- Memory extraction of Android devices using LiME

Sources & Tools Used

- Binary plist Parser / NSKeyedArchiver
- http://digitalinvestigation.wordpress.com/tag/nskeyedarchiver/
- http://code.google.com/p/ccl-bplist/
- Snapchat on Android
- http://www.decipherforensics.com/publications
- http://tryingtoreason.wordpress.com/2013/05/13/actually-snapchat-does-delete-your-photos-just-not-straight-away/
- http://ryanburke.co.uk/portfolio-item/snapgrab/
- Snapchat Encryption
- https://github.com/tlack/snaphax
- https://kivikakk.ee/2013/05/10/snapchat.htm

SEEK TRUTH

THANK YOU

STROZ FRIEDBERG

strozfriedberg.com

Andrea London
T: 214.377.4566
alondon@strozfriedberg.com

Kyle O'Meara
T: 202.464.5819
komeara@strozfriedberg.com