Forensic Analysis of Data Transience Applications in iOS and Android

September 19, 2013

Cindy Wu

Overview

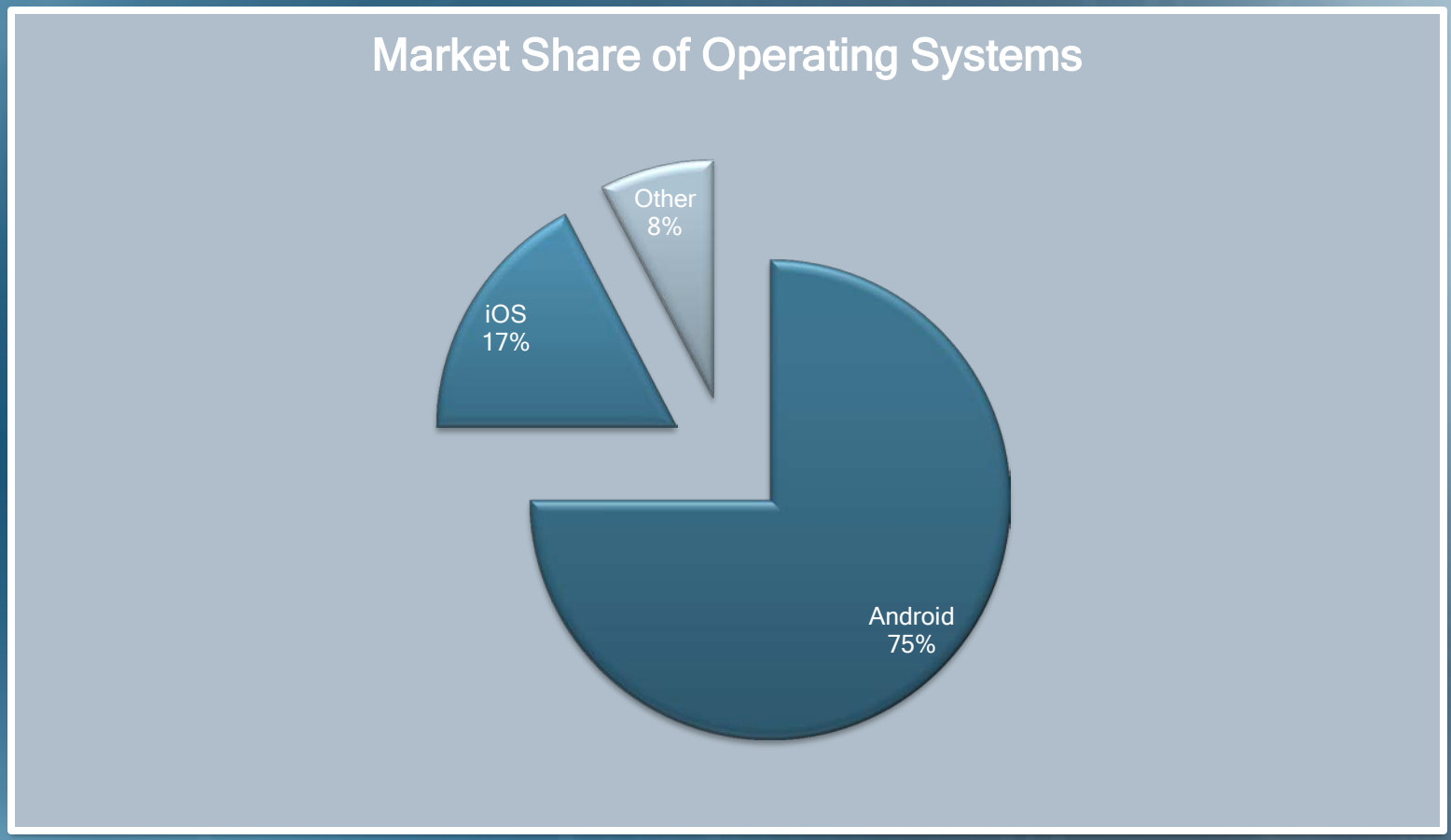
- Background
- Materials and Methods
- Snapchat Results/Discussion
- Burner Results/Discussion
- Conclusion
- Future Considerations

Background

What is Digital Forensics?

- The process of uncovering and interpreting electronic data for use in a court of law.
- New versions of operating systems, software applications, and hardware platforms are constantly being released in addition to new generations of mobile devices
  - Practices are constantly being updated
- Mobile forensics

Statistics



Mobile Phone Capabilities




Mobile Phone Capabilities

NOMOPHOBIA

Applications - Snapchat

"Snapchat is a new way to share moments with friends. Snap an ugly selfie or a video, add a caption, and send it to a friend (or maybe a few). They'll receive it, laugh, and then the snap disappears."

- Team Snapchat

May 9, 2013

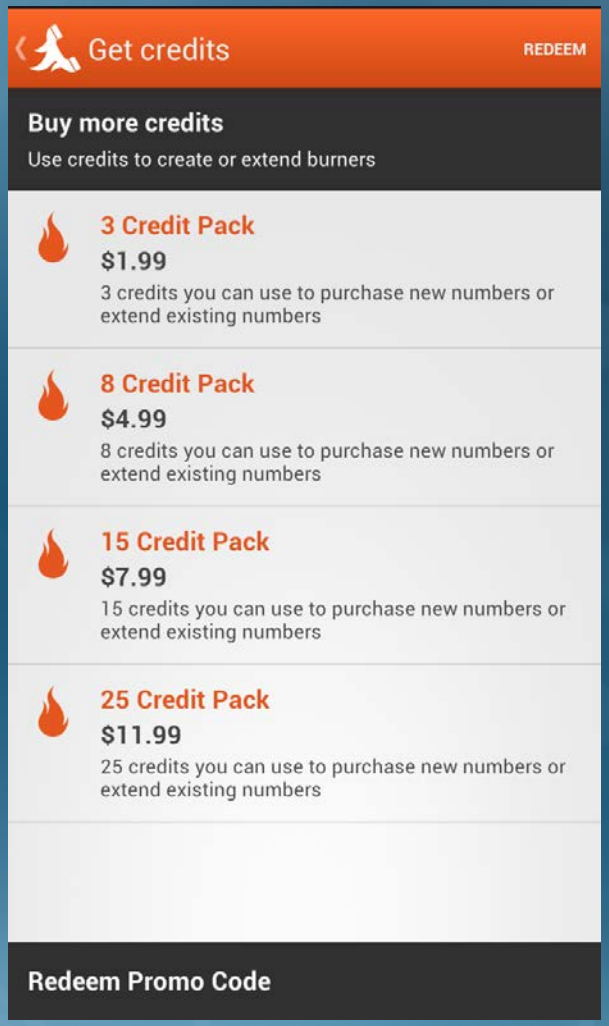
- “Also, if you’ve ever tried to recover lost data after accidentally deleting a drive or maybe watched an episode of CSI, you might know that with the right forensic tools, it’s sometimes possible to retrieve data after it has been deleted. So… you know… keep that in mind before putting any state secrets in your selfies :)” – Team Snapchat

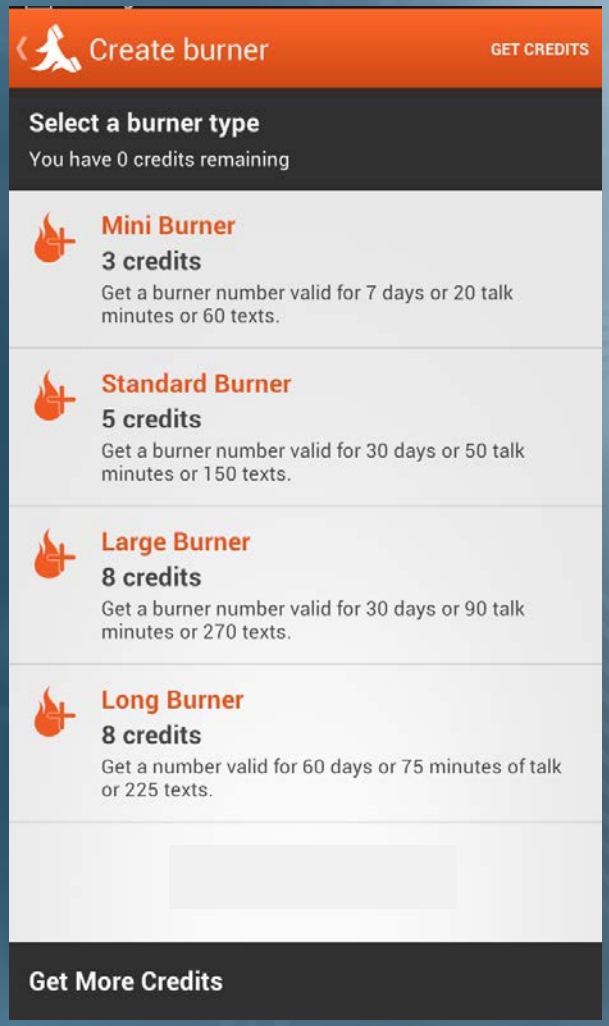
Applications - Burner App

“Burner is an mobile application and service that enables users to obtain temporary, disposable numbers for voice and SMS communication. Fast, safe, and private, Burner lets you get as many numbers as you want, use each as a private line within your iPhone or Android, and "burn" a number whenever you're done with it.”

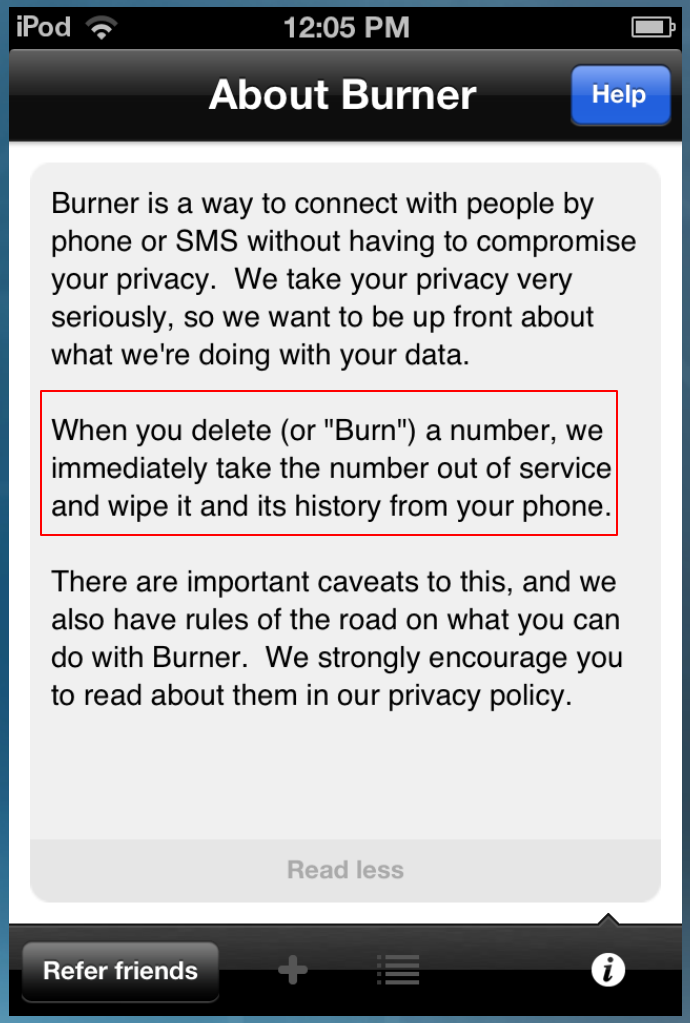
- Ad Hoc Labs, Inc.

Burner - Purchase Required





About Burner



How are these Apps relevant to Digital Forensics?

- Snapchat has over 10 million Google Play downloads
- Burner has over 50,000 Google Play downloads

- Users who believe in the transience of the data will seek security in these third party applications
- Some may be criminals

- Revealing any recovery of artifacts or metadata can prove communication, association, and the presence of any questionable content.

Hypotheses

If Snapchat is used by Android and iOS users, some transferred data will be recoverable within a certain time frame

AND

If Burner is used by Android and iOS users, some transferred data will be recoverable within a certain time frame

Materials and Methods

Testing Devices

LG Nexus 4 E960
Android 4.2.2 Jelly Bean

iPod Touch 3G
iOS v6.1.3

Other Devices Used for Data Exchange

- BlueStacks App Player (Snapchat Only)

- Personal Smartphone Devices

Application Criteria

- Known to be data transient
- Popular
- Available in both markets

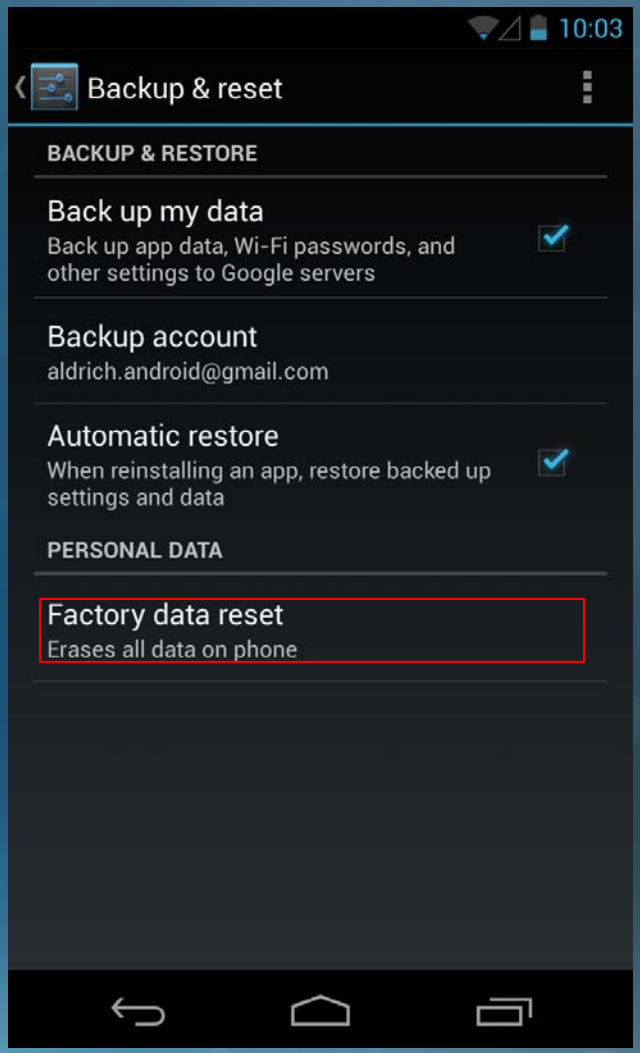
Analysis Tools

Cellebrite® UFED Touch v1.9.0.130
with Physical Analyzer 3.7.2

AccessData® Forensic Toolkit v4.0

Android and iOS Device Setup

Restore to Factory Settings



Data Exchange for Snapchat

Data (videos and snaps) was exchanged with the two devices

- Opened
- Delivered
- Read
- Unread

A manual log in MS Excel

- Contact
- Content
- Date
- Status

Data Exchange for Burner

Data was exchanged with the two testing devices

A manual log of the contacts, content, and approximate timestamps was stored in Microsoft Excel for comparison to any recovered data

Two trials to determine:

- Whether recovery of data was possible
- Whether time elapsed played a factor
- Whether automatic expiration (Trial 1) or manual deletion (Trial 2) affected recovery of data

Image Acquisition

Android

Cellebrite UFED Touch

- Physical extraction
- File system dump

iOS

Cellebrite Physical Analyzer

- File system extraction
- Acquired both system and data partitions

Forensic Toolkit v4.0 Analysis

Analysis in FTK

- Used AccessData Forensic Toolkit v4.0.0
- All iPod images were added to FTK
  - TAR / ZIP files
- All Android images were added to FTK
  - ZIP files

Analysis in FTK for Snapchat

All data was carved for graphics

Index searches

- MISDEWu
- WuMISDE
- Experidigi
- EmmyMISDE

Overview Tab Search

- File Extensions

Analysis in FTK for Burner

Live Search

- U.S. phone numbers

Index Search

- Keywords from Manual Log

Snapchat Results/Discussion

iOS Significant Snapchat Plists

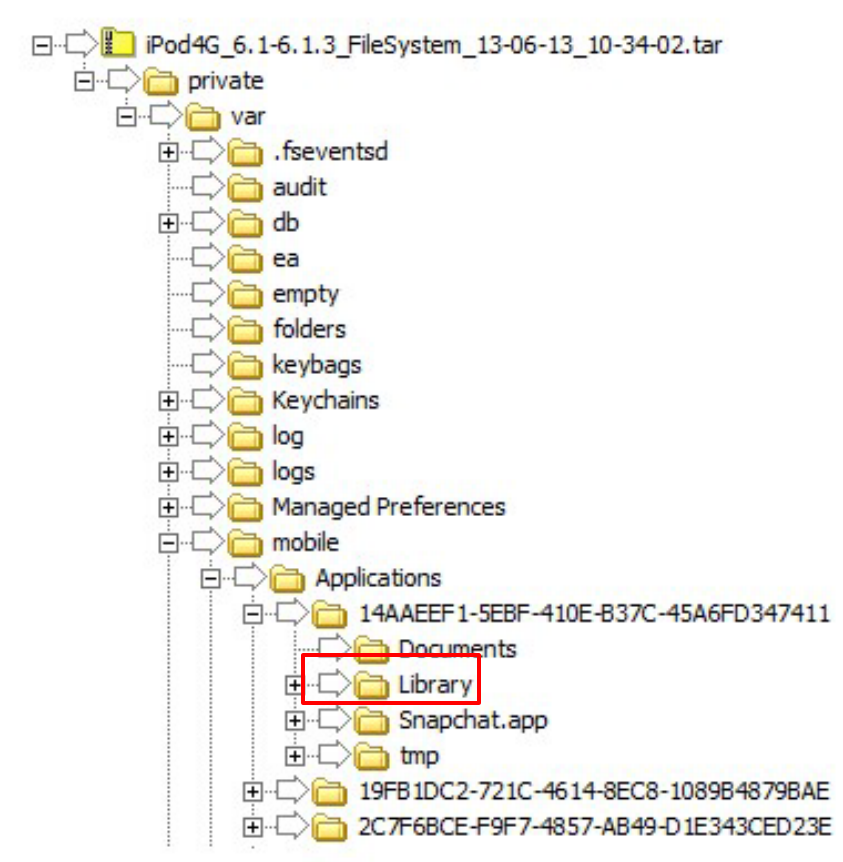
com.topoya.picaboo.plist

- private\var\mobile\Library\Preferences

user.plist

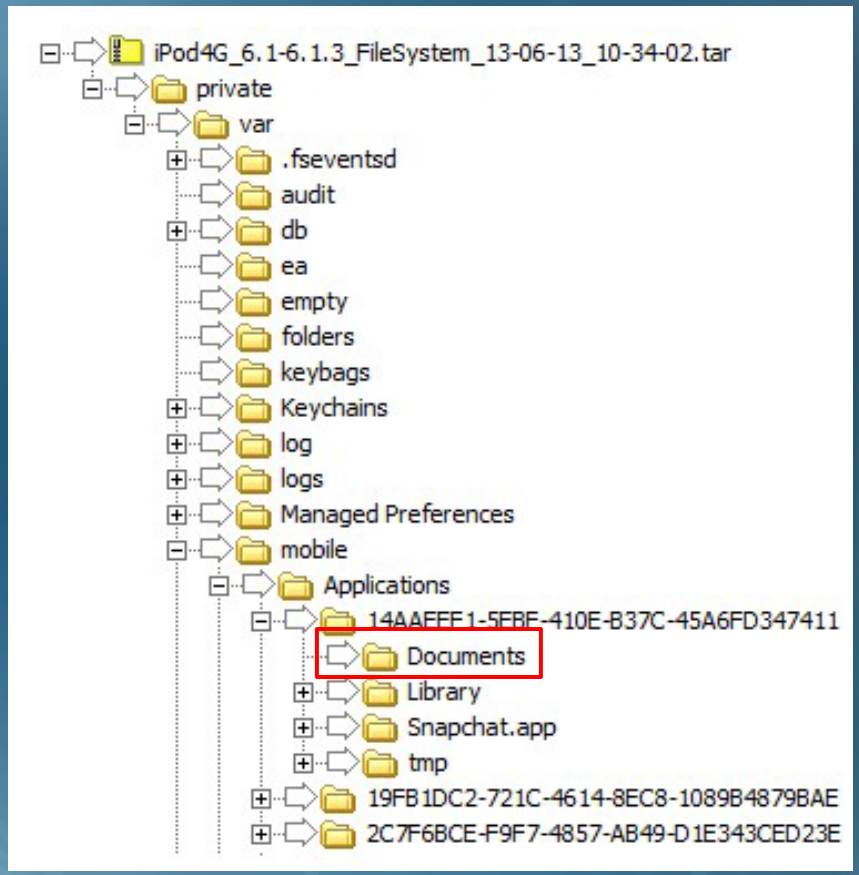
- private\var\mobile\Applications\14AAEEF1-5EBF-410E-B37C-45A6FD347411\Documents

com.topoya.picaboo.plist

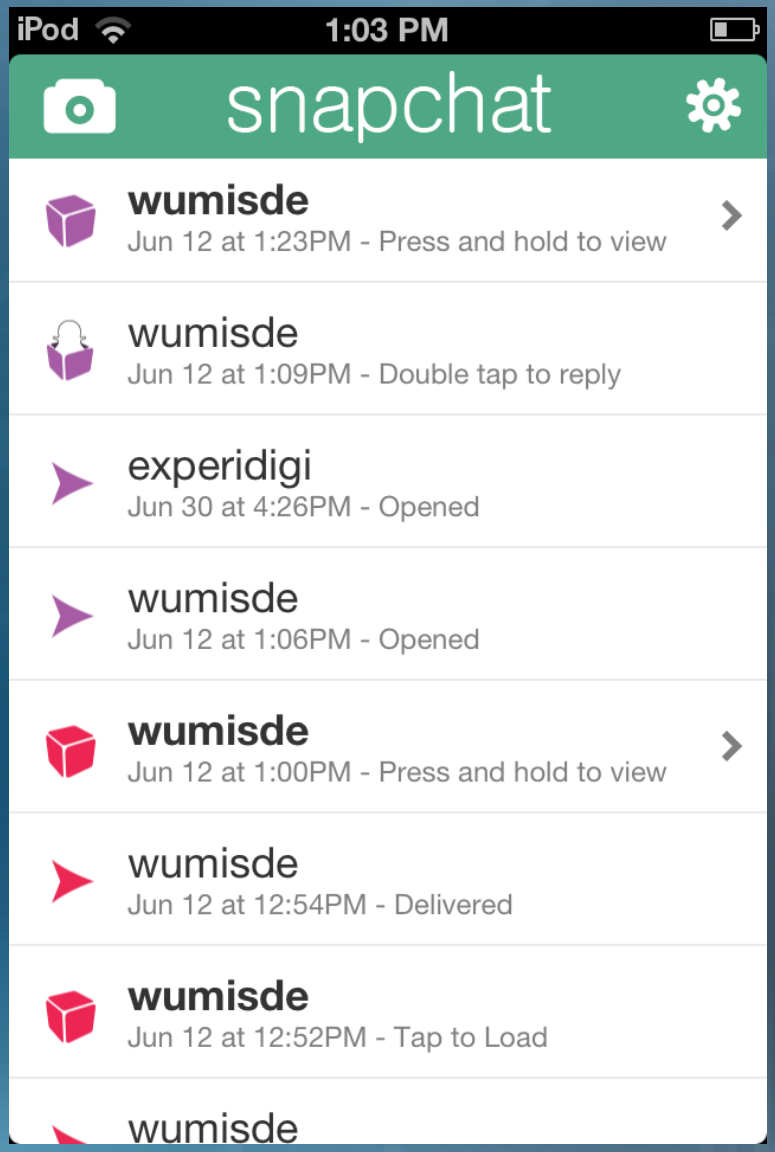


Key	Value Type	Value
Property list	*Dictionary*	*(4 values)*
misdewuSentSnap	*String*	YES
crittercism_51146f388cb83152d300001e	*Dictionary*	*(3 values)*
Critterability	*Dictionary*	*(3 values)*
wifi	*Number*	1
host	*Number*	0
internet	*Number*	0
current_device	*Dictionary*	*(9 values)*
model	*String*	iPod touch
system_version	*String*	6.1.3
carrier	*String*	unknown
system_name	*String*	iPhone OS
status_bar_orientation	*Number*	1
locale	*String*	en
platform	*String*	iPod4,1
orientation	*Number*	1
enabled_remote_notification_types	*String*	0
user_metadata	*Dictionary*	*(1 values)*
username	*String*	misdewu

user.plist



[47]	*String*	28955437105694568 4r
[48]	*String*	wumisde
[49]	*Dictionary*	*(2 values)*
NS.time	*Number*	392749745.68400002
[50]	*Dictionary*	*(2 values)*
NS.time	*Number*	392749745.68400002
[51]	*Dictionary*	*(2 values)*
NS.time	*Number*	392749808.75404102
[52]	*Dictionary*	*(13 values)*
[53]	*String*	145419371056744413s
[54]	*String*	experidigi
[55]	*Dictionary*	*(2 values)*
NS.time	*Number*	392749544.41300011
[56]	*Dictionary*	*(2 values)*
NS.time	*Number*	392749544.41300011
[57]	*String*	MISDEWU1371056724EXPERIDIGI
[58]	*Dictionary*	*(13 values)*
[59]	*String*	783196371056744413s
[60]	*Dictionary*	*(2 values)*
NS.time	*Number*	392749607
[61]	*Dictionary*	*(2 values)*
NS.time	*Number*	392749544.41300011
[62]	*String*	MISDEWU1371056724WUMISDE
[63]	*Dictionary*	*(13 values)*
[64]	*String*	367186371056437634r
[65]	*String*	wumisde
[66]	*Dictionary*	*(2 values)*
NS.time	*Number*	392749237.63400006
[67]	*Dictionary*	*(2 values)*
NS.time	*Number*	392749237.63400006
[68]	*Dictionary*	*(13 values)*
[69]	*String*	974653371056091333s
[70]	*Dictionary*	*(2 values)*
NS.time	*Number*	392748891.33299994
[71]	*Dictionary*	*(2 values)*
NS.time	*Number*	392748891.33299994
[72]	*String*	MISDEWU1371056086WUMISDE
[73]	*Dictionary*	*(13 values)*


iPod
1:03 PM
snapchat
wumisde
Jun 12 at 1:23PM - Press and hold to view
wumisde
Jun 12 at 1:09PM - Double tap to reply
experidigi
Jun 30 at 4:26PM - Opened
wumisde
Jun 12 at 1:06PM - Opened
wumisde
Jun 12 at 1:00PM - Press and hold to view
wumisde
Jun 12 at 12:54PM - Delivered
wumisde
Jun 12 at 12:52PM - Tap to Load
wumisde

Android Significant Snapchat Folders and Files

com.snapchat.android_preferences.xml

- Root\data\com.snapchat.android\shared_prefs\

received_image_snaps folder

- Root\data\com.snapchat.android\cache\

images folder

- Root\data\com.android.vending\cache\

com.android.chrome folder

- Root\data\com.android.chrome\databases\files

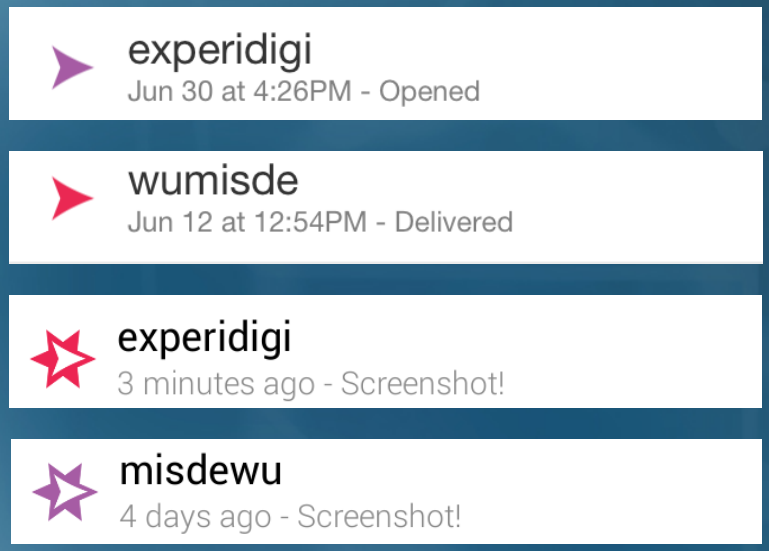
com.snapchat.android_preferences.xml

```
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
<map>
<int name="snapsSinceLastOpened" value="0" />
<string name="sendersSinceLastOpened" />
<string name="user">{"mAddressBook":{"mContactsNotUnSnapchat":[],"mContactsUnSnapchat":[],"mContactsUnSnapchatAlreadyInvited":[],"mEmailsToNames":{},"mPhoneNumbersToNames":{}},"mAuthToken":"82fe227b-1223-4f3c-953f-bf840fabf1a3","mBests":["misdewu","emmymside","experidigi"],"mEmail":"wumisde@gmail.com","mFriends":
[{"mBottomPanelDisplayName":"emmymside","mDisplayName":"","mUsername":"emmymside.","mUrl":"http://www.snapchat.com/emmymside","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"experidigi","mDisplayName":"","mUsername":"experidigi","mUrl":"http://www.snapchat.com/experidigi","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"misdewu","mDisplayName":"","mUsername":"misdewu","mUrl":"http://www.snapchat.com/misdewu","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},{"mBottomPanelDisplayName":"teamsnapchat","mDisplayName":"Team
Snapchat","mUsername":"teamsnapchat","mUrl":"http://www.snapchat.com/teamsnapchat","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"wumiside","mDisplayName":"","mUsername":"wumiside","mUrl":"http://www.snapchat.com/wumiside","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false}],"mFriendsWithoutRequestsOrPendingOrBlocked":[],"snapsUpdatedSinceLastServerChange":[],"snaps":
[{"type":"ReceivedSnap","mSender":"misdewu","mWasViewed":false,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":false,"mWasScreenshotted":false,"mDisplayTime":2,"mStatusMessage":"Press and hold to view","mId":"5355712710624115722","mTimestamp":1371062411572,"mStatus":1,"mIcon":2130837851,"mMediaType":0},
{"type":"SentSnap","mCaptionParameters":{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"experidigi","mFailed":false,"mTimeOfLastSendAttempt":1371065281941,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Opened","mId":"12446437106177918 3s","mTimestamp":1371061971000,"mStatus":2,"mIcon":2130837849,"mMediaType":0},{"type":"SentSnap","mCaptionParameters":
{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"misdewu","mFailed":false,"mTimeOfLastSendAttempt":13710652819 41,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Opened","mId":"88738853100108110 3s","mTimestamp":13710019230 00,"mStatus":2,"mIcon":2130837849,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"experidigi","mWasViewed":false,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":false,"mWasScreenshotted":false,"mDisplayTime":10,"mStatusMessage":"Press and hold to view","mId":"976678371058936119r","mTimestamp":1371058936119,"mStatus":1,"mIcon":2130837851,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"misdewu","mWasViewed":false,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":false,"mWasScreenshotted":false,"mDisplayTime":3,"mStatusMessage":"Press and hold to view","mId":"4764893710579562 83r","mTimestamp":1371057956283,"mStatus":1,"mIcon":2130837851,"mMediaType":0},
{"type":"SentSnap","mCaptionParameters":{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"misdewu","mFailed":false,"mTimeOfLastSendAttempt":1371065281941,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Delivered","mId":"9446243710577936 37s","mTimestamp":1371057793637,"mStatus":1,"mIcon":2130837850,"mMediaType":1},{"type":"SentSnap","mCaptionParameters":
{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"misdewu","mFailed":false,"mTimeOfLastSendAttempt":1371065281941,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Opened","mId":"2895543710569456 84s","mTimestamp":1371057008000,"mStatus":2,"mIcon":2130837850,"mMediaType":1},
{"type":"ReceivedSnap","mSender":"misdewu","mWasViewed":true,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":true,"mWasScreenshotted":false,"mDisplayTime":0,"mId":"7831963710567444 13r","mTimestamp":1371056744413,"mStatus":2,"mIcon":2130837843,"mMediaType":1},{"type":"SentSnap","mCaptionParameters":
{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"misdewu","mFailed":false,"mTimeOfLastSendAttempt":1371065281941,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Delivered","mId":"3671863710564376 34r","mTimestamp":1371056437634,"mStatus":1,"mIcon":2130837840,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"misdewu","mWasViewed":false,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":false,"mWasScreenshotted":false,"mDisplayTime":3,"mStatusMessage":"Press and hold to view","mId":"9746533710560911333r","mTimestamp":1371056091333,"mStatus":1,"mIcon":2130837851,"mMediaType":0},
{"type":"SentSnap","mCaptionParameters":{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"misdewu","mFailed":false,"mTimeOfLastSendAttempt":13710652819 41,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Delivered","mId":"4489133710539580 03s","mTimestamp":13710539800 03s","mStatus":1,"mIcon":2130837849,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"misdewu","mWasViewed":true,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":true,"mWasScreenshotted":false,"mDisplayTime":0,"mId":"1664113710575753153r","mTimestamp":1371055753153,"mStatus":2,"mIcon":2130837842,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"emmymside","mWasViewed":true,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":true,"mWasScreenshotted":false,"mDisplayTime":0,"mId":"6365583710529485 49r","mTimestamp":1371052948549,"mStatus":2,"mIcon":2130837842,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"experidigi","mWasViewed":true,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":true,"mWasScreenshotted":false,"mDisplayTime":0,"mId":"5331133710517951519r","mTimestamp":1371051795139,"mStatus":2,"mIcon":2130837842,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"emmymside","mWasViewed":false,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":false,"mWasScreenshotted":false,"mDisplayTime":3,"mStatusMessage":"Press and hold to view","mId":"7664063710465223 36r","mTimestamp":1371046522336,"mStatus":1,"mIcon":2130837851,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"experidigi","mWasViewed":false,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":false,"mWasScreenshotted":false,"mDisplayTime":10,"mStatusMessage":"Press and hold to view","mId":"5144237104644700 7r","mTimestamp":1371046447007,"mStatus":1,"mIcon":2130837851,"mMediaType":0},
{"type":"SentSnap","mCaptionParameters":{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"misdewu","mFailed":false,"mTimeOfLastSendAttempt":1371065281942,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Delivered","mId":"3490613710430976 67r","mTimestamp":1371043097667,"mStatus":1,"mIcon":2130837840,"mMediaType":0},{"type":"SentSnap","mCaptionParameters":
{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"emmymside","mFailed":false,"mTimeOfLastSendAttempt":1371065281942,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Opened","mId":"4234033710439876 67r","mTimestamp":1371051418000,"mStatus":2,"mIcon":2130837849,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"misdewu","mWasViewed":false,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":false,"mWasScreenshotted":false,"mDisplayTime":3,"mStatusMessage":"Press and hold to view","mId":"9955213710438095 47r","mTimestamp":13710438095 47,"mStatus":1,"mIcon":2130837851,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"misdewu","mWasViewed":true,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":true,"mWasScreenshotted":false,"mDisplayTime":0,"mId":"5174073710437350 95r","mTimestamp":1371043735095,"mStatus":2,"mIcon":2130837842,"mMediaType":0},{"type":"SentSnap","mCaptionParameters":
{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"experidigi","mFailed":false,"mTimeOfLastSendAttempt":1371065281943,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Opened","mId":"9489253710435835975","mTimestamp":1371043851000,"mStatus":2,"mIcon":2130837849,"mMediaType":0},{"type":"SentSnap","mCaptionParameters":
{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"misdewu","mFailed":false,"mTimeOfLastSendAttempt":1371065281943,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Delivered","mId":"4526743710435835975","mTimestamp":1371043583597,"mStatus":1,"mIcon":2130837849,"mMediaType":0},{"type":"SentSnap","mCaptionParameters":
{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"emmymside","mFailed":false,"mTimeOfLastSendAttempt":1371065281943,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Delivered","mId":"4850793710435835975","mTimestamp":1371043583597,"mStatus":1,"mIcon":2130837849,"mMediaType":0},{"type":"FriendRequest","mSender":"experidigi","mIsAddFriendButtonPressed":false,"mStatusMessage":"Added
you","mId":"9073823710425533262r","mTimestamp":1371042553262,"mStatus":1,"mIcon":2130837841,"mMediaType":3},{"type":"SentSnap","mCaptionParameters":
{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"emmymside","mFailed":false,"mTimeOfLastSendAttempt":1371065281943,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Opened","mId":"0451283700811220083s","mTimestamp":1370081802000,"mStatus":2,"mIcon":2130837840,"mMediaType":0},{"type":"SentSnap","mCaptionParameters":
{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"misdewu","mFailed":false,"mTimeOfLastSendAttempt":1371065281943,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Opened","mId":"3611473709812200 83s","mTimestamp":1371042346000,"mStatus":2,"mIcon":2130837849,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"emmymside","mWasViewed":true,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":true,"mWasScreenshotted":false,"mDisplayTime":0,"mId":"410/8/3/09///210////","mTimestamp":13709///210///,"mStatus":2,"mIcon":2130837842,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"misdewu","mWasViewed":true,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":true,"mWasScreenshotted":false,"mDisplayTime":0,"mId":"8322730977031880r","mTimestamp":1370977031880,"mStatus":2,"mIcon":2130837842,"mMediaType":0},{"type":"SentSnap","mCaptionParameters":
{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"misdewu","mFailed":false,"mTimeOfLastSendAttempt":1371065281943,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Opened","mId":"3804683709769764 22s","mTimestamp":1370977500000,"mStatus":2,"mIcon":2130837849,"mMediaType":0},{"type":"SentSnap","mCaptionParameters":
{"mPosition":0.0,"mOrientation":0},"mDisplayTime":0,"mRecipient":"emmymside","mFailed":false,"mTimeOfLastSendAttempt":1371065281943,"mUploaded":false,"mWasScreenshotted":false,"mStatusMessage":"Opened","mId":"3933453709769764 22s","mTimestamp":1370977219000,"mStatus":2,"mIcon":2130837849,"mMediaType":0},
{"type":"ReceivedSnap","mSender":"misdewu","mWasViewed":true,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":true,"mWasScreenshotted":false,"mDisplayTime":0,"mId":"5611013709768465 35r","mTimestamp":1370976846535,"mStatus":2,"mIcon":2130837842,"mMediaType":0},
{"type":"FriendRequest","mSender":"emmymside","mIsAddFriendButtonPressed":false,"mStatusMessage":"Added you","mId":"2188923709768218914r","mTimestamp":1370976218914,"mStatus":1,"mIcon":2130837841,"mMediaType":3},{"type":"FriendRequest","mSender":"misdewu","mIsAddFriendButtonPressed":false,"mStatusMessage":"Added
you","mId":"4056643709833072907r","mTimestamp":1370833072907,"mStatus":1,"mIcon":2130837841,"mMediaType":3},{"type":"FriendRequest","mSender":"misdewu","mIsAddFriendButtonPressed":false,"mStatusMessage":"Added you","mId":"1055013708830728 54r","mTimestamp":1370833072854,"mStatus":1,"mIcon":2130837841,"mMediaType":3},
{"type":"ReceivedSnap","mSender":"teamsnapchat","mWasViewed":true,"mCaptionPosition":0.0,"mCaptionOrientation":0,"mIsLoading":false,"mIsTimerRunning":false,"mIsBeingViewed":false,"mWasOpened":true,"mWasScreenshotted":false,"mDisplayTime":0,"mId":"1286637087856931 0r","mTimestamp":1370878569310,"mStatus":2,"mIcon":2130837842,"mMediaType":0}],"mMobileVerificationKey":"MTQ3NDp3dW1pc2Rl","mMyFriendsFriends":
[{"mBottomPanelDisplayName":"misdewu","mDisplayName":"","mUsername":"misdewu","mUrl":"http://www.snapchat.com/misdewu","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"emmymside","mDisplayName":"","mUsername":"emmymside","mUrl":"http://www.snapchat.com/emmymside","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"experidigi","mDisplayName":"","mUsername":"experidigi","mUrl":"http://www.snapchat.com/experidigi","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},{"mBottomPanelDisplayName":"teamsnapchat","mDisplayName":"Team
Snapchat","mUsername":"teamsnapchat","mUrl":"http://www.snapchat.com/teamsnapchat","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"emmymside","mDisplayName":"","mUsername":"emmymside","mUrl":"http://www.snapchat.com/emmymside","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"experidigi","mDisplayName":"","mUsername":"experidigi","mUrl":"http://www.snapchat.com/experidigi","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"misdewu","mDisplayName":"","mUsername":"misdewu","mUrl":"http://www.snapchat.com/misdewu","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},{"mBottomPanelDisplayName":"teamsnapchat","mDisplayName":"Team
Snapchat","mUsername":"teamsnapchat","mUrl":"http://www.snapchat.com/teamsnapchat","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"wumiside","mDisplayName":"","mUsername":"wumiside","mUrl":"http://www.snapchat.com/wumiside","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false}],"mNotificationId":"APA91bF1VKxwLzBqn1UcnaidWlUkXx3tx9s1ynKeg-LhrKxKmuj_UkLe35fpwz-sL/tZh9nKccd_W1eK1x4pv4KfouJkp-
EbE6Ny9v12uRuqZ7baou8d0uYjZ7OO3-B8BXUseOdPetUOjmMlrJjq6TOkRRX8UDnw","mUsername":"wumiside","mSendToFriends":[{"mBottomPanelDisplayName":"misdewu","mDisplayName":"","mUsername":"misdewu","mUrl":"http://www.snapchat.com/misdewu","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"emmymside","mDisplayName":"","mUsername":"emmymside","mUrl":"http://www.snapchat.com/emmymside","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"experidigi","mDisplayName":"","mUsername":"experidigi","mUrl":"http://www.snapchat.com/experidigi","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},{"mBottomPanelDisplayName":"teamsnapchat","mDisplayName":"Team
Snapchat","mUsername":"teamsnapchat","mUrl":"http://www.snapchat.com/teamsnapchat","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"emmymside","mDisplayName":"","mUsername":"emmymside","mUrl":"http://www.snapchat.com/emmymside","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"experidigi","mDisplayName":"","mUsername":"experidigi","mUrl":"http://www.snapchat.com/experidigi","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"misdewu","mDisplayName":"","mUsername":"misdewu","mUrl":"http://www.snapchat.com/misdewu","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},{"mBottomPanelDisplayName":"teamsnapchat","mDisplayName":"Team
Snapchat","mUsername":"teamsnapchat","mUrl":"http://www.snapchat.com/teamsnapchat","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false},
{"mBottomPanelDisplayName":"wumiside","mDisplayName":"","mUsername":"wumiside","mUrl":"http://www.snapchat.com/wumiside","mPhoneNumber":"","mIsChecked":false,"mIsPending":false,"mIsRecent":false,"mIsBlocked":false,"mIsBestFriend":false,"mDuplicateDisplayName":false}],"mPhoneNumber":"","mScreenshotDetector":{"mViewingSessions":
[],"mSender":"","mStoppedViewingTime":0,"mStartedViewingTime":0,"mNumImages":6,"mDatabaseColumnIndex":0},"mRecents":["teamsnapchat"],"mRequests":[],"mPrivacySetting":1,"mNumSnapsSent":7,"mNumSnapsReceived":9,"mLogged":true,"mHasDisplayedContactListWarning":true,"syncOnFeedOpen":false}</string>
<string name="currentUser">wumiside</string>
<boolean name="snapchatUserIsLoggedIn" value="true" />
<int name="snapchatCameraPreference" value="0" />
<int name="version" value="26" />
</map>
```

Microsoft Excel Log

Snaps																		
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	misdewu	FALSE	"0.0"	0	FALSE	FALSE	FALSE	FALSE	FALSE	3	"Press and hold to view"	5355713706241157	2r	1371062411572	1	2130837851		0
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 12, 2013 / 2:32:51 PM					
SentSnap	"0.0"	0	0	experidigi	FALSE		1371065281941	FALSE		FALSE		Opened	12446437061779183s		1371061971000	2	2130837849		0
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 12, 2013 / 2:32:03 PM					
SentSnap	"0.0"	0	0	misdewu	FALSE		1371065281941	FALSE		FALSE		Opened	887380371061681030s		1371061923000	2	2130837849		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	experidigi	FALSE	"0.0"	0	FALSE	FALSE	FALSE	FALSE	FALSE	10	"Press and hold to view"	97667837105893611	9r	1371058936119	1	2130837851		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	misdewu	FALSE	"0.0"	0	FALSE	FALSE	FALSE	FALSE	FALSE	3	"Press and hold to view"	4764893705795628	3r	1371057956283	1	2130837851		0
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 12, 2013 / 1:23:13 PM					
SentSnap	"0.0"	0	0	misdewu	FALSE		1371065281941	FALSE	FALSE			Delivered	9446243710577936375		1371057793637	2	2130837850		1
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 12, 2013 / 1:10:08 PM					
SentSnap	"0.0"	0	0	misdewu	FALSE		1371065281941	FALSE	FALSE			Opened	2895543710569456845	84s	1371057008000	2	2130837850		1
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	misdewu	TRUE	"0.0"	0	FALSE	FALSE	FALSE	TRUE	FALSE	0	N/A	7831963710567444133r		1371056744413	2	2130837843		1
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 12, 2013 / 1:00:37 PM					
SentSnap	"0.0"	0	0	misdewu	FALSE		1371065281941	FALSE	FALSE			Delivered	367186371056437634s		1371056437634	1	2130837849		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	misdewu	FALSE	"0.0"	0	FALSE	FALSE	FALSE	FALSE	FALSE	3	"Press and hold to view"	9746533710566091333r		1371056091333	1	2130837851		0
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 12, 2013 / 12:52:18 PM					
SentSnap	"0.0"	0	0	misdewu	FALSE		1371065281941	FALSE	FALSE			Delivered	448913371055938065s		1371055938065	1	2130837849		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	misdewu	TRUE	"0.0"	0	FALSE	FALSE	FALSE	TRUE	FALSE	0	N/A	1664113710557531533r		1371055753153	2	2130837842		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	emmymside	TRUE	"0.0"	0	FALSE	FALSE	FALSE	TRUE	FALSE	0	N/A	6365583710529485495r		1371052948549	2	2130837842		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	experidigi	TRUE	"0.0"	0	FALSE	FALSE	FALSE	TRUE	FALSE	0	N/A	5531133710517951595r		1371051795159	2	2130837842		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	emmymside	FALSE	"0.0"	0	FALSE	FALSE	FALSE	FALSE	FALSE	3	"Press and hold to view"	7664063710465223361	6r	1371046223361	1	2130837851		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	experidigi	FALSE	"0.0"	0	FALSE	FALSE	FALSE	FALSE	FALSE	10	"Press and hold to view"	5144237104644700	7r	1371046447007	1	2130837851		0
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 12, 2013 / 9:33:07 AM					
SentSnap	"0.0"	0	0	misdewu	FALSE		1371065281942	FALSE	FALSE			Delivered	348061371043987667s		1371043987667	1	2130837849		0
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 12, 2013 / 11:36:58 AM					
SentSnap	"0.0"	0	0	emmymside	FALSE		1371065281942	FALSE	FALSE			Opened	423403371043987667s		1371051418000	2	2130837849		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	misdewu	FALSE	"0.0"	0	FALSE	FALSE	FALSE	FALSE	FALSE	3	"Press and hold to view"	9933213710438095473	r	1371043809547	1	2130837851		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	misdewu	TRUE	"0.0"	0	FALSE	FALSE	FALSE	TRUE	FALSE	0		5174073710437350953r		1371043735095	2	2130837842		0
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 12, 2013 / 9:30:51 AM					
SentSnap	"0.0"	0	0	experidigi	FALSE		1371065281943	FALSE	FALSE			Opened	948925371043583597s		1371043851000	2	2130837849		0
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 12, 2013 / 9:26:23 AM					
SentSnap	"0.0"	0	0	misdewu	FALSE		1371065281943	FALSE	FALSE			Delivered	452674371043583597s		1371043583597	1	2130837849		0
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 12, 2013 / 9:26:23 AM					
SentSnap	"0.0"	0	0	emmymside	FALSE		1371065281943	FALSE	FALSE			Delivered	485079371043583597s		1371043583597	1	2130837849		0
Type	mSender	mIsAddFriendButtonPressed									mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
FriendRequest	experidigi	FALSE									"Added you"	9073823710425532623r		1371042553262	1	2130837841		3
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 11, 2013 / 4:18:12 PM					
SentSnap	"0.0"	0	0	emmymside	FALSE		1371065281943	FALSE	FALSE			Opened	945128370981220083s		1370981892000	2	2130837849		0
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 12, 2013 / 9:05:46 AM					
SentSnap	"0.0"	0	0	misdewu	FALSE		1371065281943	FALSE	FALSE			Opened	361147370981220083s		1371042346000	2	2130837849		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	emmymside	TRUE	"0.0"	0	FALSE	FALSE	FALSE	TRUE	FALSE	0	N/A	4167873709772107773r		1370977210777	2	2130837842		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	misdewu	TRUE	"0.0"	0	FALSE	FALSE	FALSE	TRUE	FALSE	0	N/A	8322737097703188	0r	1370977031880	2	2130837842		0
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 11, 2013 / 3:05:00 PM					
SentSnap	"0.0"	0	0	misdewu	FALSE		1371065281943	FALSE	FALSE			Opened	380468370976976422s		1370977500000	2	2130837849		0
Type	mCaptionParameters		mDisplayTime	mRecipient	mFailed	mTimeofLastSendAttempt	mUploaded		mWasScreenshotted		mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
	mPosition	mOrientation				June 12, 2013 / 3:28:01 PM							June 11, 2013 / 3:00:19 PM					
SentSnap	"0.0"	0	0	emmymside	FALSE		1371065281943	FALSE	FALSE			Opened	3933453709769764225		1370977219000	2	2130837849		0
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	misdewu	TRUE	"0.0"	0	FALSE	FALSE	FALSE	TRUE	FALSE	0	N/A	5611013709768465353r		1370976846535	2	2130837842		0
Type	mSender	mIsAddFriendButtonPressed									mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
FriendRequest	emmymside	FALSE									"Added you"	2188923709762189143r		1370976218914	1	2130837841		3
Type	mSender	mIsAddFriendButtonPressed									mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
FriendRequest	misdewu	FALSE									"Added you"	4956664370883072897r		1370883072897	1	2130837841		3
Type	mSender	mIsAddFriendButtonPressed									mStatusMessage	mId	mTimeStamp	mStatus	mIcon	mMediaType		
FriendRequest	misdewu	FALSE									"Added you"	1055013708830728547r		1370883072854	1	2130837841		3
Type	mSender	mWasViewed	mCaptionPosition	mCaptionOrientation	mIsLoading	mIsTimerRunning	mIsBeingViewed	mWasOpened	mWasScreenshotted	mDisplayTime	mStatus Message	mId	mTimestamp	mStatus	mIcon	mMediaType		
ReceivedSnap	teamsnapchat	TRUE	"0.0"	0	FALSE	FALSE	FALSE	TRUE	FALSE	0	N/A	1286637087856931	0r	1370878569310	2	2130837842		0

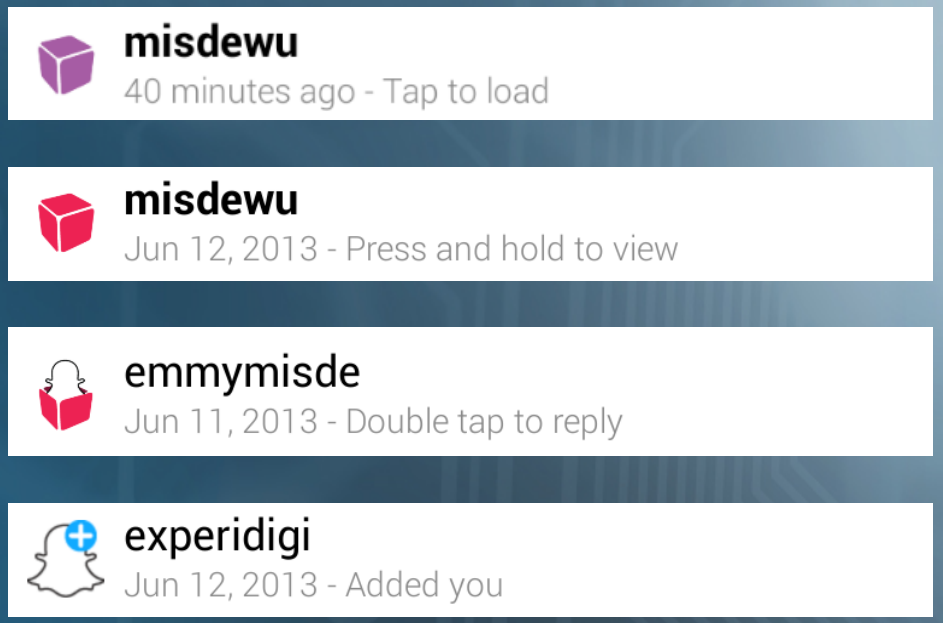
Sent Snaps



- Display Time
- Message ID

Received Snaps

- Display Time
- Message ID
- Screenshot



mlcon

2130837542 

2130837543 

2130837544 

2130837545 

2130837546 

2130837547 

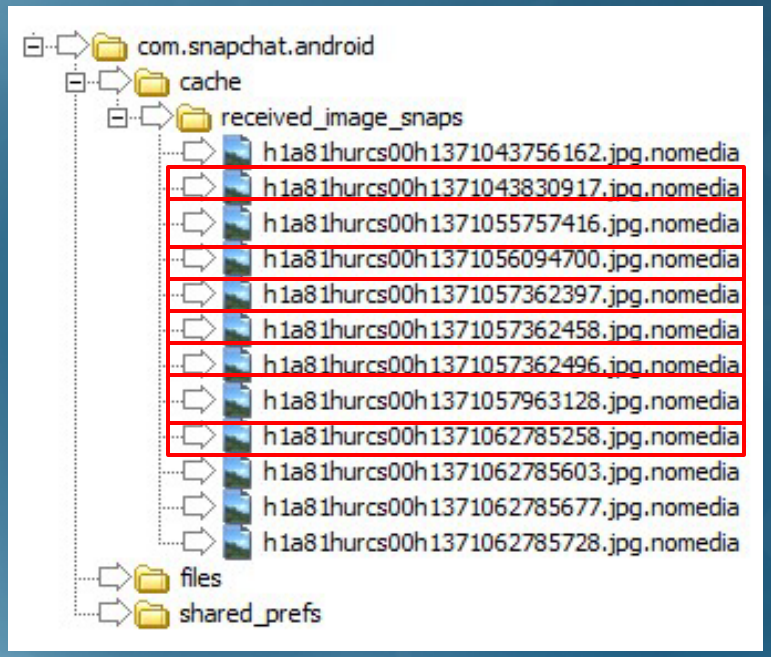
2130837548 

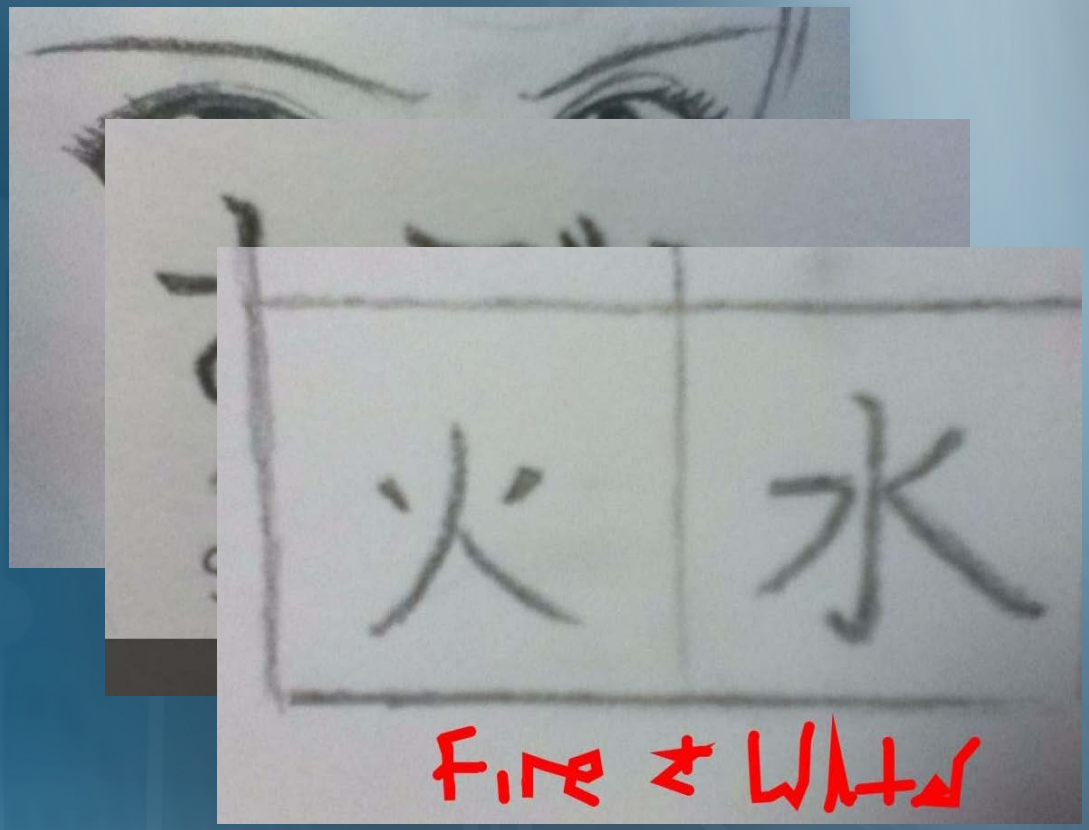
2130837549 

2130837894 

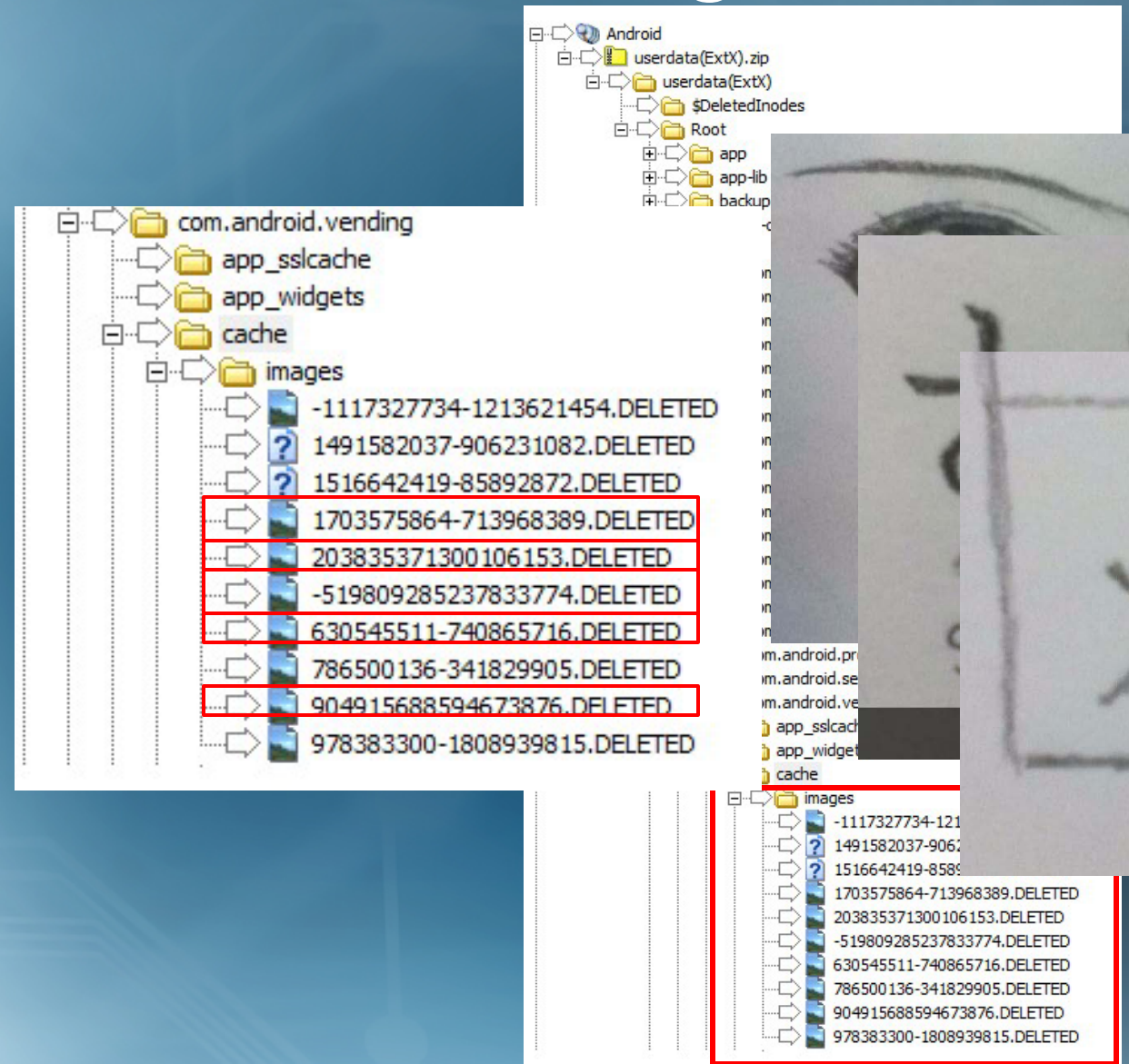
Clear Feed

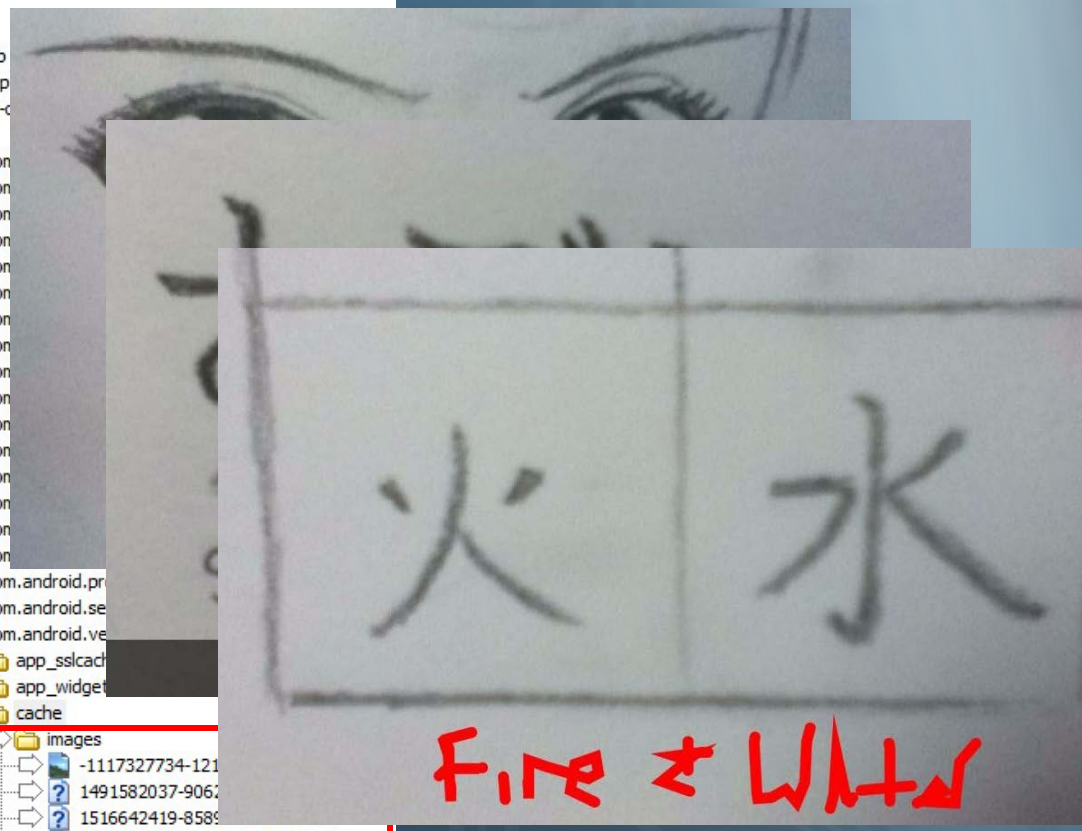
received_image_snaps folder



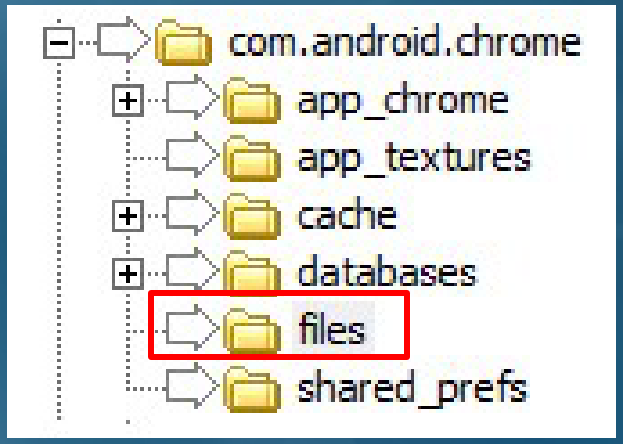


images folder





com.android.chrome



Tab5.DELETED

Discussion - Snapchat

Android device

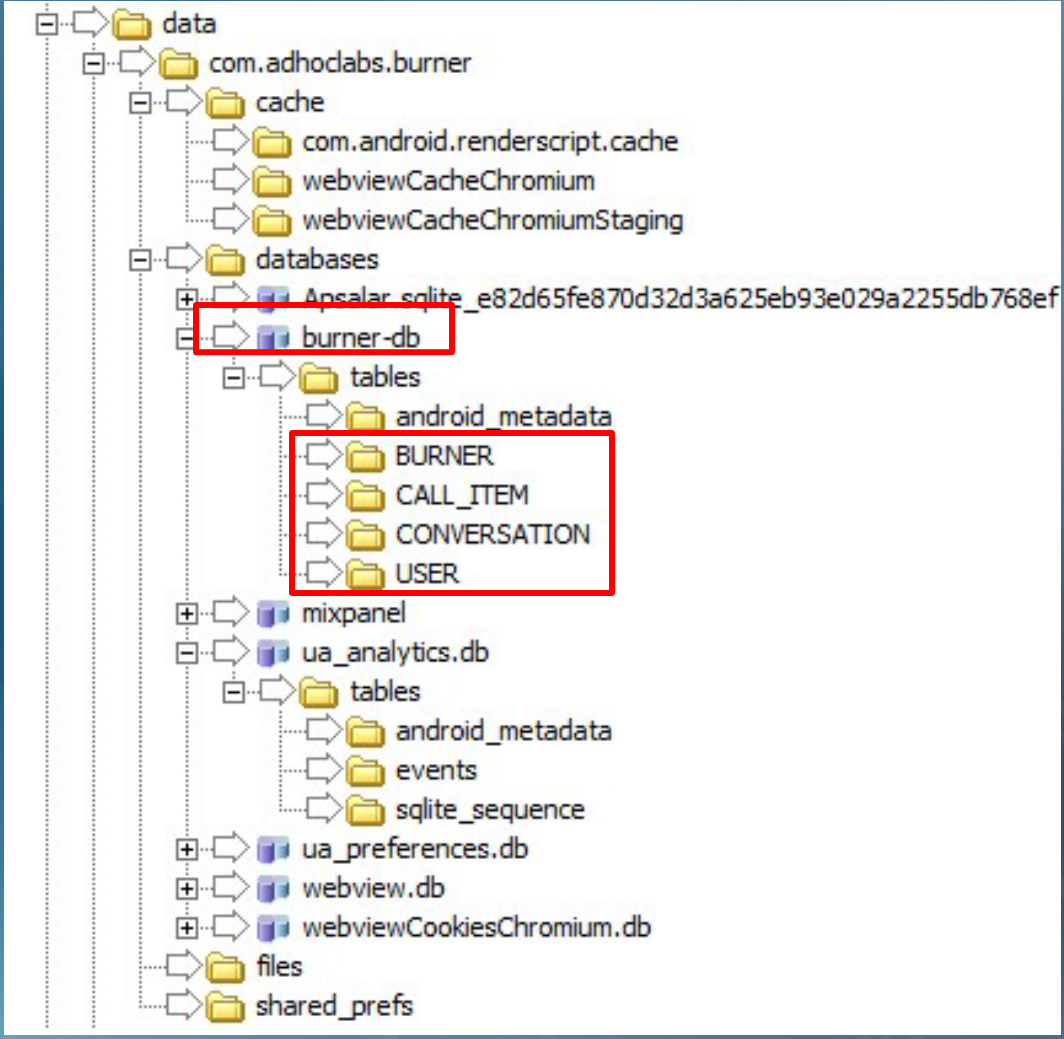
- Log is recoverable
  - Received/Sent
  - Contact
  - Was Viewed
  - Timestamp
  - Status Message
  - mID
  - Etc.
- ‘Clear Feed’ causes log to be unrecoverable
- Some received images recoverable

iOS device

- Log is recoverable
  - Received/Sent
  - Contact
  - mID
  - Timestamp
- ‘Clear Feed’ causes log to be unrecoverable

Burner Results/Discussion

Android Burner Data Location



Burner and Conversations

BURNER

rows 0-0

rowid	BURNER_ID	USER_ID	SID	ABOUT	SECRET	NUMBER	REMAINING_MINUTES	TOTAL_MINUTES	NOTIFICATIONS	RING	CREATED	EXPIRES	UPDATED_AT
1	d97756c50895f0017449f7315566262c	0250040ba35ea379817daad26fcbcdf3	[NULL]	Aldrich Android	c0x1YrEFzKy1NXhl8e_eUr0ha2tpqYYe	+12084490827	0	15	1	1	1373981033000	1374067433000	2013-07-16T17:50:35Z

CONVERSATION

rows 0-5

rowid	_id	BURNER_ID	NUMBER	NOTE	LAST_ITEM_TYPE	LAST_ITEM_DATE
1	1	d97756c50895f0017449f7315566262c	+15189669836	[NULL]	0	1373987275000
2	2	d97756c50895f0017449f7315566262c	[redacted]14043	[NULL]	0	1373987173000
3	3	d97756c50895f0017449f7315566262c	+[redacted]14043	[NULL]	0	1373987173508
4	4	d97756c50895f0017449f7315566262c	[redacted]47023	[NULL]	0	1373989377000
5	5	d97756c50895f0017449f7315566262c	[redacted]01852	[NULL]	0	1373993744000
6	6	d97756c50895f0017449f7315566262c	[redacted]17416	[NULL]	0	1373996991000

Call_Item

CALL_ITEM

rows 0-16

rowid	ID	CONVERSATION_ID	TYPE	DATE	BODY	VOICEMAIL_URI
1	SM1dadcac33e6bf886da992415f13ff538	1	1	1373981268000	Hey Aldrich! When can we meet?	[NULL]
3	SMe74a10c443f5b3fc7857c145f021d478	1	0	1373981436000	Ritter Park. 8pm.	[NULL]
4	SM29456f992cdf69a08f1c1375ecf561cc	2	1	1373981900000	Did you get in touch with Izze?	[NULL]
5	CA2dac5ed545eaecfef8e67992f8dace32	2	3	1373986313000	[NULL]	[NULL]
6	SMeaa728f7a07b8a37ff1339be2455efc0	1	1	1373987017000	Where are you?	[NULL]
9	SM3979010a5b07540642d6227bb6f89ef0	2	0	1373987173000	Yes.	[NULL]
10	SMe9fcb10026f5e39275bf8e0c0fa3ea91	1	0	1373987275000	By the tennis courts.	[NULL]
11	SMdadf514bdc853ec6d26d64fc2823826d	4	1	1373987799000	Hey, I'm interested in buying some...things...you have posted on craigslist.	[NULL]
13	SM78796ba04d8b62bc5b52fb687c78f31f	4	0	1373988510000	What's your offer? I have a huge selection.	[NULL]
14	SM187238fb09ec87a1614d69a6eb7a7bc6	4	1	1373988693000	Do you do bundle deals? I was thinking of shelling out $100 for five, rather than $30 each.	[NULL]
16	SM17d234d56d6253267be738cd5e86a8d9	4	0	1373989128000	$125 for 5 and you got yourself a deal.	[NULL]
17	SMa4c32215985dc8a52d65f6d75c9af744	4	1	1373989230000	Alright. Sounds like a plan, my friend.	[NULL]
19	SMb7d493da57ba40e1b9e3a902dc7d4097	4	0	1373989377000	Meet me at the park at midnight.	[NULL]
20	SMd5380594cf95c6ec2437719b40aa0291	5	1	1373993545000	Korean Zombies!!!! watch out now	[NULL]
22	SM4de258ffc825857f17213c0ee60e4be6	5	0	1373993744000	Oh no! Not the zombies!!!	[NULL]
23	SM0802baecad2f1594bbb344f1aa5bd288	6	1	1373996761000	Meet me in the woods at 10. Bring a shovel.	[NULL]
25	SMb5e3fac8ac3e50c0f4d4293efd3056cf	6	0	1373996991000	Who is it this time?	[NULL]

Android User

USER

rows 0-0

rowid	USER_ID	PHONE	CREDITS	SECRET	SHARE_URL	REFERRAL_CODE
1	0250040ba35ea379817daad26fcbcdf3	16313460845	2	cDx1YrEFzKy1NXhl8e_eUr0ha2tpqYYe	http://brnr.me/h4cO	KAMDLIZP

SQLite Table Summary

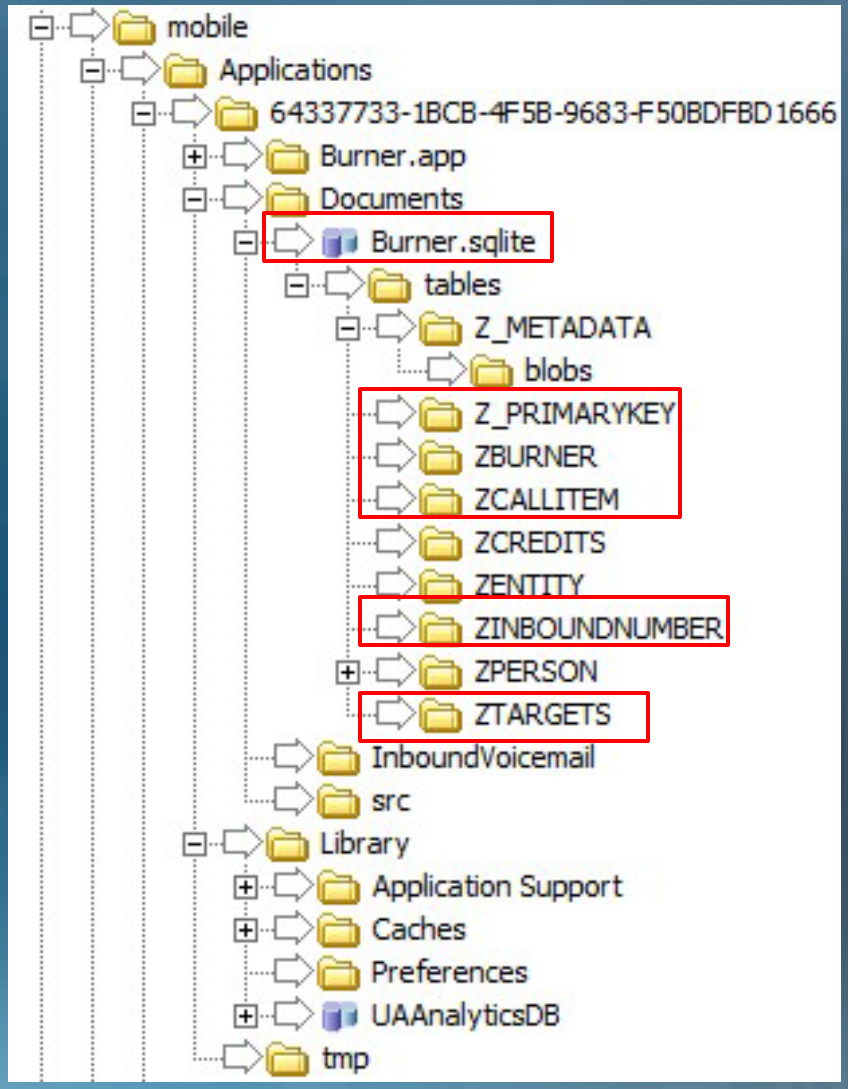
Table	Row Count
android_metadata	1
USER	1
BURNER	1
CONVERSATION	6
CALL_ITEM	17

Before Trial 1

Table	Row Count
android_metadata	1
USER	1
BURNER	0
CONVERSATION	0
CALL_ITEM	0

After Trial 1 & 2

iOS Burner Location



ZBurner

ZBURNER

rows 0-0

rowid	Z_PK	Z_ENT	Z_OPT	ZAUTO_DIAL	ZMAXLENGTH	ZNOTIFICATIONS	ZREMAINING	ZRING	ZSOUNDCLOUD	ZSTART_OFFSET	ZTOTALMINUTES	ZUNSYNCED_MINUTES
1	1	1	203	[NULL]	1440	1	1	1	0	0	15	0

ZVOICE_NOTIFICATIONS	ZBURNERTOPERSON	ZCREATED	ZEXPIRES	ZUPDATED	ZABOUT	ZCALLS	ZDISABLED	ZFRIENDLYNUMBER	ZICON
[NULL]	1	395673887	395760287	395690302	Izze IPod	[NULL]	[NULL]	(518) 966-9836	

ZID_	ZINBOUND_CALLS	ZINBOUND_TEXTS	ZNUMBER	ZSECRET
de705e474e45ed099f32368103a94ca5	[NULL]	[NULL]	+15189669836	_7HSpjgxTPpVdPSfcaJpQRBVR2gu6ULq

ZSID_	ZSKU	ZSMS_URL	ZSTATUS	ZUNAVAILABLE_MESSAGE	ZURI	ZVOICE_URL	ZVOICEMAIL_URL
PN1a06179008e475d35512d7e4f2f14ca8	com.adhoclabs.burner.sample	[NULL]	available	[NULL]	[NULL]	[NULL]	[NULL]

Inbound Number

ZINBOUNDNUMBER

rows 0-5

rowid	Z_PK	Z_ENT	Z_OPT	ZFAVORITE	ZREAD	ZSTARRED	ZUNREAD_ITEMS	ZINBOUNDTOBURNER	ZUPDATED	ZNOTE	ZNUMBER	ZTAGS	ZUPDATEDSTRING
1	1	5	48	[NULL]	0	[NULL]	[NULL]	[NULL]	395680076.091352	[NULL]	+12084490827	[NULL]	2013-07-16 15:07:56 +0000
2	2	5	42	[NULL]	0	[NULL]	[NULL]	[NULL]	395682944.772112	[NULL]	+[redacted]4043	[NULL]	2013-07-16 15:55:44 +0000
3	3	5	36	[NULL]	[NULL]	[NULL]	[NULL]	[NULL]	395682588.239858	[NULL]	[redacted]7023	[NULL]	2013-07-16 15:49:48 +0000
4	4	5	20	[NULL]	[NULL]	[NULL]	[NULL]	[NULL]	395686649.887916	[NULL]	[redacted]1852	[NULL]	2013-07-16 16:57:29 +0000
5	5	5	9	[NULL]	0	[NULL]	[NULL]	[NULL]	395690126.872656	[NULL]	[redacted]5257	[NULL]	2013-07-16 17:55:26 +0000
6	6	5	10	[NULL]	[NULL]	[NULL]	[NULL]	[NULL]	395690281.25198	[NULL]	[redacted]7416	[NULL]	2013-07-16 17:58:01 +0000

ZCall_Item

ZCALLITEM

rows 0-18

rowid	Z_PK	Z_ENT	Z_OPT	ZCONNECTED	ZFAVORITE	ZREAD	ZCALLITEMTOBURNER	ZCALLITEMTOINBOUNDNUMBER	ZDATE	ZLASTPLAYED	ZBODY	ZCALL_SHARE_URL	ZRECORDING_URL	ZSID	ZTYPE_	ZVOICEMAIL_SHARE_URL
1	1	2	2	1	[NULL]	[NULL]	[NULL]	1	395674068.81853	[NULL]	Hey Aldrich! When can we meet?	[NULL]	[NULL]	SM10868ac23f0209da1d471a9dd070422d	outbound_sms	[NULL]
2	2	2	3	1	[NULL]	[NULL]	[NULL]	1	395674235.56178	[NULL]	Ritter Park. 8pm.	[NULL]	[NULL]	SM53398698aacb9ace22c98fcc6297e6b8	sms	[NULL]
3	3	2	2	1	[NULL]	[NULL]	[NULL]	2	395675064.915883	[NULL]	Do you have a job for me?	[NULL]	[NULL]	SM66268121b7108c77423bcceed8588021	outbound_sms	[NULL]
4	4	2	4	0	[NULL]	[NULL]	[NULL]	2	395679329.169469	[NULL]	[NULL]	[NULL]	[NULL]	CA435495468823a8161cbc943d37700d7b	call	[NULL]
5	5	2	2	1	[NULL]	[NULL]	[NULL]	2	395679560.122605	[NULL]	I'm at the drop location. Keep watch.	[NULL]	[NULL]	SM73fe90df8f292adbdacaf8c859c98657	outbound_sms	[NULL]
6	6	2	2	1	[NULL]	[NULL]	[NULL]	1	395679816.710187	[NULL]	Where are you?	[NULL]	[NULL]	SMce61491d4985719d919f481c4624b50c	outbound_sms	[NULL]
7	7	2	5	1	[NULL]	[NULL]	[NULL]	1	395680076.091352	[NULL]	By the tennis courts.	[NULL]	[NULL]	SM7a95d93bbec5e3e59e94bb62993c337a	sms	[NULL]
8	8	2	6	1	[NULL]	[NULL]	[NULL]	3	395680706.642532	[NULL]	Arrrrrr! I be a pirate and I noticed some booty you have for sale on craigslist! I want to add this booty to me collection. Arrrrr!	[NULL]	[NULL]	SM6945da9e4f784eedcd7deb25b15a86ba	sms	[NULL]
9	9	2	2	1	[NULL]	[NULL]	[NULL]	3	395681839.87538	[NULL]	Ahoy, matey! What be this booty ye speak of?	[NULL]	[NULL]	SM4872d6dcf74817046ede2824f1e8f2b0	outbound_sms	[NULL]
10	10	2	7	1	[NULL]	[NULL]	[NULL]	3	395682185.864312	[NULL]	Well, ye landlubber, I was hoping I could garner some of your delicious spiced island rum. Arrrr.	[NULL]	[NULL]	SM98120f5d3ef7dde64639ea01858cd870	sms	[NULL]
11	11	2	2	1	[NULL]	[NULL]	[NULL]	3	395682588.239858	[NULL]	Arrr! Bring 3 gold doubloons to the forsaken island at dusk.	[NULL]	[NULL]	SM0b0a95ec70593370f4acaadac2a6bafe	outbound_sms	[NULL]
12	12	2	2	1	[NULL]	[NULL]	[NULL]	2	395682944.772112	[NULL]	Will do. I'm out of sight but nice shirt.	[NULL]	[NULL]	SM0a0fe3646ac7a79f9e818ccf45d3b065	sms	[NULL]
13	13	2	9	1	[NULL]	[NULL]	[NULL]	4	395686361.963057	[NULL]	polish sausages are disgusting!	[NULL]	[NULL]	SM333d94ca07ca129485002ed3faea8810	sms	[NULL]
14	14	2	2	1	[NULL]	[NULL]	[NULL]	4	395686649.887916	[NULL]	Gross.	[NULL]	[NULL]	SMf0032fd5e5f2c501d6216ecc19e9d980	outbound_sms	[NULL]
15	15	2	2	1	[NULL]	[NULL]	[NULL]	6	395690128.754344	[NULL]	El lagarto está llorando	[NULL]	[NULL]	SM6aac13dfd1d31c2bc2ce868bfc9eb3ce	sms	[NULL]
16	16	2	2	1	[NULL]	[NULL]	[NULL]	5	395690126.872656	[NULL]	Hello how are you?	[NULL]	[NULL]	SM3127f50cdf84305efab2c5f7ecc7d873	sms	[NULL]
17	17	2	2	1	[NULL]	[NULL]	[NULL]	5	395690118.943882	[NULL]	Fuzzy meatballs.	[NULL]	[NULL]	SMf8ade9811894ac9f40f01761fb127153	sms	[NULL]
18	18	2	2	1	[NULL]	[NULL]	[NULL]	6	395690258.623727	[NULL]	No hablo español	[NULL]	[NULL]	SM1fcd56b3dfd27f22c702de58a0d27072	outbound_sms	[NULL]
19	19	2	2	1	[NULL]	[NULL]	[NULL]	6	395690281.25198	[NULL]	Tá an laghairt caoineadh	[NULL]	[NULL]	SM7e6a9ff132268808ab54436ea333abfc	sms	[NULL]

ZTarget

ZTARGETS

rows 0-0

rowid	Z_PK	Z_ENT	Z_OPT	ZTARGETTOPERSON	ZNUMBER
1	1	7	1	1	13044496771

SQLite Table Summary

Table	Row Count
ZBURNER	0
ZCALLITEM	19
ZCREDITS	1
ZENTITY	0
ZINBOUNDNUMBER	6
ZPERSON	1
ZTARGETS	1
Z_PRIMARYKEY	7
Z_METADATA	1

Before/After Trial 1

=

Table	Row Count
ZBURNER	0
ZCALLITEM	19
ZCREDITS	1
ZENTITY	0
ZINBOUNDNUMBER	6
ZPERSON	1
ZTARGETS	1
Z_PRIMARYKEY	7
Z_METADATA	1

After Trial 2

Z_PRIMARYKEY

rowid	Z_ENT	Z_NAME	Z_SUPER	Z_MAX
1	1	Burner	0	1
2	2	CallItem	0	19
3	3	Credits	0	1
4	4	Entity	0	0
5	5	InboundNumber	0	6
6	6	Person	0	1
7	7	Targets	0	1

After Trial 1

rowid	Z_ENT	Z_NAME	Z_SUPER	Z_MAX
1	1	Burner	0	2
2	2	CallItem	0	31
3	3	Credits	0	1
4	4	Entity	0	0
5	5	InboundNumber	0	10
6	6	Person	0	1
7	7	Targets	0	1

After Trial 2

Discussion - Burner

Android device

- Log is unrecoverable after burner number expires

iOS device

- Log is recoverable only if number automatically expired
  - Received/Sent
  - Contact Numbers
  - Timestamp
  - Type
  - Message ID
  - Message Content

Conclusions

Android device

Snapchat data was recoverable

- ‘Clear Feed’ removes log

Received Snapchat images were recoverable based on time elapsed

No data was recoverable from Burner app regardless of how it was removed from the device

iOS device

Minimal Snapchat data was recoverable

- ‘Clear Feed’ removes log

No Snapchat images were recovered

All data from Burner app was recoverable for burner numbers that were not manually deleted

Future Considerations

Snapchat

- Determine estimated time before server completely removes a snap/video

Burner

- Test mobile network capabilities involving calls and voicemails

Similar Third-Party Applications

Acknowledgments

- Dr. Terry Fenger
- Christopher Vance
- Cpl. Robert Boggs
- Marshall University
- Samantha Kochmann
- Jamie Sternlicht
- Jenny Sulcebarger
- Harry Wu

References

[1] Android and iOS Combine for 92.3% of All Smartphone Operating System Shipments in the First Quarter While Windows Phone Leapfrogs BlackBerry, According to IDC. *ICD Analyze the Future.* 31 July 2013. <http://www.idc.com/getdoc.jsp?containerId=prUS24108913>

[2] Edmondson, M. Forensic Artifact Analysis of the Burner App for the iPhone. *Digital Forensic Tips*. 23 July 2013. <http://digitalforensicstips.com/2013/07/forensic-artifact-analysis-of-the-burner-app-for-the-iphone/>.

[3] Guynn, J. Privacy watchdog EPIC files complaint against Snapchat with FTC. *Los Angeles Times.* 28 May 2013. <http://articles.latimes.com/2013/may/17/business/la-fi-tn-privacy-watchdog-epic-files-complaint-against-Snapchat-with-ftc-20130517>.

[4] Hickman, R. Snapchat Unveiled: An Examination of Snapchat on Android Devices. *Decipher Forensics.* 28 May 2013. <http://decipherforensics.com/publications>.

[5] Hoog, Andrew and Strzempka, Katie. *iPhone and iOS Forensics: Investigation, Analysis, and Mobile Security for Apple iPhone, iPad, and iOS Devices.* Syngress: Amsterdam. 2011.

[6] Hoog, Andrew. *Android Forensics: Investigation, Analysis, and Mobile Security for Google Android.* Syngress: Amsterdam. 2011.

[7] Mobile Majority: U.S. Smartphone Ownership Tops 60%. *Neilsen*. June 6, 2013.

Picture References

- www.snapchat.com
- www.burnerapp.com
- http://greggornation.files.wordpress.com/2012/12/snapchat-icon.png?w=587
- http://www.cellebrite.com/mobile-forensic-products/ufed-touch-ultimate.html
- http://developer.android.com/distribute/googleplay/promote/brand.html
- http://forensictools.pl/pl/oprogramowanie/10-forensic-toolkit-3.html
- http://www.lg.com/uk/images/lg-mobile-phones/e960/gallery/medium02.jpg
- http://www.apple.com/ipod-touch/
- http://www.glasbergen.com/cartoons-about-mobile-phones/
- http://themyndset.com/wp-content/uploads/2011/09/chase-app-icon.jpg
- http://us.123rf.com/400wm/400/400/alexwhite/alexwhite1209/alexwhite120900032/15308285-shopping-cart-icon.jpg
- http://ecx.images-amazon.com/images/I/81UpVH8B49L._SL500_AA300_.png
- http://www.thenewipadblog.net/wp-content/uploads/2012/12/Google-Maps-icon.jpg
- http://www.pastbook.com/txt/assets/Facebook-Icon.png
- http://www.apkdad.com/wp-content/uploads/2013/05/ExDialer-Contacts-Icon.png
- http://icons.iconarchive.com/icons/marcus-roberto/google-play/512/Gmail-icon.png
- http://www.software.fashel.net/wp-content/uploads/2013/07/Skype-icon.png
- http://www.mysmartphonetutor.com/wp-content/uploads/2013/06/SMS-Icon.png
- http://fs02.androidpit.info/ali/x03/8171403-1374702400804-144x144.png

Questions?


© Randy Glasbergen
www.glasbergen.com
GLASBERGEN
"Your smartphone is overqualified."