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

Market Share of Operating Systems

- Android: 75%
- iOS: 17%
- Other: 8%
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
“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

Get credits

Buy more credits
Use credits to create or extend burners

- **3 Credit Pack**
  - $1.99
  - 3 credits you can use to purchase new numbers or extend existing numbers

- **8 Credit Pack**
  - $4.99
  - 8 credits you can use to purchase new numbers or extend existing numbers

- **15 Credit Pack**
  - $7.99
  - 15 credits you can use to purchase new numbers or extend existing numbers

- **25 Credit Pack**
  - $11.99
  - 25 credits you can use to purchase new numbers or extend existing numbers

Redeem Promo Code

Create burner

Select a burner type
You have 0 credits remaining

- **Mini Burner**
  - 3 credits
  - Get a burner number valid for 7 days or 20 talk minutes or 60 texts.

- **Standard Burner**
  - 5 credits
  - Get a burner number valid for 30 days or 50 talk minutes or 150 texts.

- **Large Burner**
  - 8 credits
  - Get a burner number valid for 30 days or 90 talk minutes or 270 texts.

- **Long Burner**
  - 8 credits
  - Get a number valid for 60 days or 75 minutes of talk or 225 texts.

Get More Credits
About Burner

Burner is a way to connect with people by phone or SMS without having to compromise your privacy. We take your privacy very seriously, so we want to be up front about what we’re doing with your data.

When you delete (or "Burn") a number, we immediately take the number out of service and wipe it and its history from your phone.

There are important caveats to this, and we also have rules of the road on what you can do with Burner. We strongly encourage you to read about them in our privacy policy.
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

Backup & reset

BACKUP & RESTORE

Back up my data
Back up app data, Wi-Fi passwords, and other settings to Google servers

Backup account
aldrich.android@gmail.com

Automatic restore
When reinstalling an app, restore backed up settings and data

PERSONAL DATA

Factory data reset
Erases all data on phone
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)
msdewuSentSnap | String | YES
crittercism_51145f388cb83152d300001e | 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 | msdewu
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
<table>
<thead>
<tr>
<th>Event Type</th>
<th>Date/Time</th>
<th>User ID</th>
<th>Status</th>
<th>Timestamp</th>
<th>Icon ID</th>
<th>MediaType</th>
<th>失败</th>
<th>已发送</th>
<th>已被查看</th>
<th>已被截屏</th>
<th>已被打开</th>
<th>聊天消息</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sent Snap</td>
<td>2013/06/12 9:26:23</td>
<td>83227370977031880r</td>
<td>2</td>
<td>1370981892000</td>
<td>2130837842</td>
<td>3</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>0</td>
</tr>
<tr>
<td>Sent Snap</td>
<td>2013/06/12 14:36:18</td>
<td>945128370981220083s</td>
<td>1</td>
<td>1371043851000</td>
<td>2130837849</td>
<td>0</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>0</td>
</tr>
<tr>
<td>Sent Snap</td>
<td>2013/06/12 17:32:30</td>
<td>166411371055753153r</td>
<td>2</td>
<td>1371051418000</td>
<td>2130837842</td>
<td>0</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>0</td>
</tr>
<tr>
<td>Sent Snap</td>
<td>2013/06/12 17:53:46</td>
<td>448913371055938065s</td>
<td>1</td>
<td>1371057008000</td>
<td>2130837851</td>
<td>0</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>0</td>
</tr>
<tr>
<td>Sent Snap</td>
<td>2013/06/12 17:57:47</td>
<td>124464371061779183s</td>
<td>2</td>
<td>1371068208000</td>
<td>2130837849</td>
<td>1</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>0</td>
</tr>
<tr>
<td>Friend Request</td>
<td>2013/06/12 17:00:00</td>
<td>553113371051795159r</td>
<td>1</td>
<td>1371056078000</td>
<td>2130837849</td>
<td>2</td>
<td>0</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>0</td>
</tr>
</tbody>
</table>
Sent Snaps

- Display Time
- Message ID

- **experidigi**
  Jun 30 at 4:26PM - Opened

- **wumisde**
  Jun 12 at 12:54PM - Delivered

- **experidigi**
  3 minutes ago - Screenshot!

- **misdewu**
  4 days ago - Screenshot!
Received Snaps

- Display Time
- Message ID
- Screenshot

- misdewu
  40 minutes ago - Tap to load

- misdewu
  Jun 12, 2013 - Press and hold to view

- emmymisde
  Jun 11, 2013 - Double tap to reply

- experidigi
  Jun 12, 2013 - Added you
mlcon

2130837542
2130837543
2130837544
2130837545
2130837546
2130837547
2130837548
2130837549
2130837894
You don't have any snaps :(
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

- Some received images recoverable
Burner Results/Discussion
Android Burner Data Location

[Diagram of data location with highlighted files:
- `data`
  - `com.adhoclabs.burner`
    - `cache`
      - `com.androidrenderscript.cache`
      - `webviewCacheChromium`
      - `webviewCacheChromiumStaging`
    - `databases`
      - `Apsalar.sqlite_e82d65fe870d32d3a625eb93e029a2255db768ef`
      - `burner-db`
        - `tables`
          - `android_metadata`
          - `BURNER`
          - `CALL_ITEM`
          - `CONVERSATION`
          - `USER`
          - `mixpanel`
          - `ua_analytics.db`
            - `tables`
              - `android_metadata`
              - `events`
              - `sqlite_sequence`
          - `ua_preferences.db`
          - `webview.db`
          - `webviewCookiesChromium.db`
          - `files`
          - `shared_prefs`]


### BURNER

**rows 0-0**

<table>
<thead>
<tr>
<th>rowid</th>
<th>BURNER_ID</th>
<th>USER_ID</th>
<th>STD</th>
<th>ABDIT</th>
<th>SECRET</th>
<th>NUMBER</th>
<th>REMAINING_MINUTES</th>
<th>TOTAL_MINUTES</th>
<th>NOTIFICATIONS</th>
<th>RING</th>
<th>CREATED</th>
<th>EXPIRES</th>
<th>UPDATED_AT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>d97755c50895f00174449f315566262c</td>
<td>0250040ba35ea379817daa26fcbcd5f</td>
<td>[NULL]</td>
<td>Android</td>
<td>Mel</td>
<td>1208448.083</td>
<td>15</td>
<td>1</td>
<td>1</td>
<td>137394013000</td>
<td>17406743000</td>
<td>2013-07-16T17:50:35Z</td>
<td></td>
</tr>
</tbody>
</table>

### CONVERSATION

**rows 0-5**

<table>
<thead>
<tr>
<th>rowid</th>
<th>_id</th>
<th>BURNER_ID</th>
<th>NUMBER</th>
<th>NOTE</th>
<th>LAST_ITEM_TYPE</th>
<th>LAST_ITEM_DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>d97755c50895f00174449f315566262c</td>
<td>+15189699836</td>
<td>[NULL]</td>
<td>0</td>
<td>1373987275000</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>d97755c50895f00174449f315566262c</td>
<td>14043</td>
<td>[NULL]</td>
<td>0</td>
<td>1373987173000</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>d97755c50895f00174449f315566262c</td>
<td>14043</td>
<td>[NULL]</td>
<td>0</td>
<td>1373987173508</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>d97755c50895f00174449f315566262c</td>
<td>17023</td>
<td>[NULL]</td>
<td>0</td>
<td>1373987937700</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>d97755c50895f00174449f315566262c</td>
<td>1852</td>
<td>[NULL]</td>
<td>0</td>
<td>1373993744000</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>d97755c50895f00174449f315566262c</td>
<td>17416</td>
<td>[NULL]</td>
<td>0</td>
<td>1373996991000</td>
</tr>
<tr>
<td>rowid</td>
<td>ID</td>
<td>CONVERSATION_ID</td>
<td>TYPE</td>
<td>DATE</td>
<td>BODY</td>
<td>VOICEMAIL_URI</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------------</td>
<td>------</td>
<td>-----------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>SM1d3c6bac3e6b8f854a92415f13f538</td>
<td>1</td>
<td>1</td>
<td>1373981268000</td>
<td>Hey Aldrich! When can we meet?</td>
<td>[NULL]</td>
</tr>
<tr>
<td>3</td>
<td>SMes4a10c443fb3c7687c745f021d478</td>
<td>1</td>
<td>0</td>
<td>1373981436000</td>
<td>Ritter Park. 6pm.</td>
<td>[NULL]</td>
</tr>
<tr>
<td>4</td>
<td>SM29456f992cd5f98a081c1375ecf561cc</td>
<td>2</td>
<td>1</td>
<td>1373981900000</td>
<td>Did you get in touch with Tizze?</td>
<td>[NULL]</td>
</tr>
<tr>
<td>5</td>
<td>CA24c854d545eae5e8e67992f82dace32</td>
<td>2</td>
<td>3</td>
<td>1373986313000</td>
<td>[NULL]</td>
<td>[NULL]</td>
</tr>
<tr>
<td>6</td>
<td>SMesaa728f7a078b837f1339be2455efc0</td>
<td>1</td>
<td>1</td>
<td>1373987017000</td>
<td>Where are you?</td>
<td>[NULL]</td>
</tr>
<tr>
<td>9</td>
<td>SM397901a5b07546062d6227bb6f89e6f0</td>
<td>2</td>
<td>0</td>
<td>1373987173000</td>
<td>Yes.</td>
<td>[NULL]</td>
</tr>
<tr>
<td>10</td>
<td>SMes9fcb10026f5e39275b9f6o0c0a3ea91</td>
<td>1</td>
<td>0</td>
<td>1373987275000</td>
<td>By the tennis courts.</td>
<td>[NULL]</td>
</tr>
<tr>
<td>11</td>
<td>SMd45f14bc853ac2d26d64fc2823826d</td>
<td>4</td>
<td>1</td>
<td>1373987799000</td>
<td>Hey, I'm interested in buying some things...you have posted on craigslist.</td>
<td>[NULL]</td>
</tr>
<tr>
<td>13</td>
<td>SM78790ba04db65b52b686787f83f1</td>
<td>4</td>
<td>0</td>
<td>1373988810000</td>
<td>What's your offer? I have a huge selection.</td>
<td>[NULL]</td>
</tr>
<tr>
<td>14</td>
<td>SM187238b09ac851a7164d9a6eb7a7bc6</td>
<td>4</td>
<td>1</td>
<td>1373988893000</td>
<td>Do you do bundle deals? I was thinking of shelling out $100 for five, rather than $30 each.</td>
<td>[NULL]</td>
</tr>
<tr>
<td>16</td>
<td>SM17d2034d56d6s23d627be738d2e06a8d9</td>
<td>4</td>
<td>0</td>
<td>1373989128000</td>
<td>$125 for 5 and you get yourself a deal.</td>
<td>[NULL]</td>
</tr>
<tr>
<td>17</td>
<td>SMes4c3221985c0a52d65b675c9af744</td>
<td>4</td>
<td>1</td>
<td>1373989230000</td>
<td>Alright. Sounds like a plan, my friend.</td>
<td>[NULL]</td>
</tr>
<tr>
<td>19</td>
<td>SMb7d493da57b4a0e1b9a3a02d7cd007f</td>
<td>4</td>
<td>0</td>
<td>1373989377000</td>
<td>Meet me at the park at midnight.</td>
<td>[NULL]</td>
</tr>
<tr>
<td>20</td>
<td>SMd58059f9c9f6c2437719b40a0291</td>
<td>5</td>
<td>1</td>
<td>1373993540000</td>
<td>Korean Zombies!!!! watch out now</td>
<td>[NULL]</td>
</tr>
<tr>
<td>22</td>
<td>SM4de258ffe825857f17213c00e650e4b6</td>
<td>5</td>
<td>0</td>
<td>1373993744000</td>
<td>Oh no! Not the zombies!!!</td>
<td>[NULL]</td>
</tr>
<tr>
<td>23</td>
<td>SM8802baec29f1594bb344f1aa5bbd288</td>
<td>6</td>
<td>1</td>
<td>1373996761000</td>
<td>Meet me in the woods at 10. Bring a shovel.</td>
<td>[NULL]</td>
</tr>
<tr>
<td>25</td>
<td>SMb5e3fac8ac3e50c0f4d293ef3056cf</td>
<td>6</td>
<td>0</td>
<td>1373996991000</td>
<td>Who is it this time?</td>
<td>[NULL]</td>
</tr>
</tbody>
</table>
# Android User

<table>
<thead>
<tr>
<th>rowid</th>
<th>USER_ID</th>
<th>PHONE</th>
<th>CREDITS</th>
<th>SECRET</th>
<th>SHARE_URL</th>
<th>REFERRAL_CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0250040ba35ea379817daad26fcbcdf3</td>
<td>16313460845 2</td>
<td></td>
<td>cDx1YrEFzKy1NXhl8e_eUr0ha2tpqYYe</td>
<td><a href="http://brnr.me/h4cO">http://brnr.me/h4cO</a></td>
<td>KAMDLIZP</td>
</tr>
</tbody>
</table>
SQLite Table Summary

### Before Trial 1

<table>
<thead>
<tr>
<th>Table</th>
<th>Row Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>android_metadata</td>
<td>1</td>
</tr>
<tr>
<td>USER</td>
<td>1</td>
</tr>
<tr>
<td>BURNER</td>
<td>1</td>
</tr>
<tr>
<td>CONVERSATION</td>
<td>6</td>
</tr>
<tr>
<td>CALL_ITEM</td>
<td>17</td>
</tr>
</tbody>
</table>

### After Trial 1 & 2

<table>
<thead>
<tr>
<th>Table</th>
<th>Row Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>android_metadata</td>
<td>1</td>
</tr>
<tr>
<td>USER</td>
<td>1</td>
</tr>
<tr>
<td>BURNER</td>
<td>0</td>
</tr>
<tr>
<td>CONVERSATION</td>
<td>0</td>
</tr>
<tr>
<td>CALL_ITEM</td>
<td>0</td>
</tr>
</tbody>
</table>
iOS Burner Location
### ZBURNER

<table>
<thead>
<tr>
<th>rowid</th>
<th>Z_PK</th>
<th>Z_ENT</th>
<th>Z_OPT</th>
<th>ZAUTO.Dial</th>
<th>ZMAXLENGTH</th>
<th>ZNOTIFICATIONS</th>
<th>ZREMAINING</th>
<th>ZRING</th>
<th>ZSOUNDCLOUD</th>
<th>ZSTART_OFFSET</th>
<th>ZTOTALMINUTES</th>
<th>ZUNSYNCE_MINUTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>203</td>
<td>[NULL]</td>
<td>1440</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ZVOICE_NOTIFICATIONS</th>
<th>ZBURNERTOPERSON</th>
<th>ZCREATED</th>
<th>ZEXPIRES</th>
<th>ZUPDATED</th>
<th>ZABOUT</th>
<th>ZCALLS</th>
<th>ZDISABLED</th>
<th>ZFRIENDLYNUMBER</th>
<th>ZICON</th>
</tr>
</thead>
<tbody>
<tr>
<td>[NULL]</td>
<td>1</td>
<td>395673887</td>
<td>395760287</td>
<td>395690303</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>(518) 966-9836</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ZID</th>
<th>ZINBOUND_CALLS</th>
<th>ZINBOUND_TEXTS</th>
<th>ZNUMBER</th>
<th>ZSECRET</th>
</tr>
</thead>
<tbody>
<tr>
<td>de705e474e45ed099f32368103a94ca5</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>+15189669836</td>
<td>_7HSpjgxTPpVdsfcaJpQRBVR2gu6ULq</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ZSID</th>
<th>ZSKU</th>
<th>ZSMS_URL</th>
<th>ZSTATUS</th>
<th>ZUNAVAIL_MESSAGE</th>
<th>ZURI</th>
<th>ZVOICE_URL</th>
<th>ZVOICEEMAIL_URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>PN1:a061790008e475d35512d7e4f2f14ca8</td>
<td>com.adhoclabs.burner.sample</td>
<td>[NULL]</td>
<td>available</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td></td>
</tr>
</tbody>
</table>
## ZINBOUNDNUMBER

### rows 0-5

<table>
<thead>
<tr>
<th>rowid</th>
<th><em>PK</em></th>
<th><em>ENT</em></th>
<th><em>OPT</em></th>
<th><em>FAVORITE</em></th>
<th><em>READ</em></th>
<th><em>STARRED</em></th>
<th><em>UNREAD_ITEMS</em></th>
<th><em>ZINBOUNDTOBURNER</em></th>
<th><em>ZUPDATED</em></th>
<th><em>ZNOTE</em></th>
<th><em>ZNUMBER</em></th>
<th><em>ZTAGS</em></th>
<th><em>UPDATEDSTRING</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>48</td>
<td>[NULL]</td>
<td>0</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>395680076.091352</td>
<td>[NULL]</td>
<td>+12084490827</td>
<td>[NULL]</td>
<td>2013-07-16 15:07:56 +0000</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>5</td>
<td>36</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>395683582.239858</td>
<td>[NULL]</td>
<td>7023</td>
<td>[NULL]</td>
<td>2013-07-16 15:49:48 +0000</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>20</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>395686649.887916</td>
<td>[NULL]</td>
<td>1852</td>
<td>[NULL]</td>
<td>2013-07-16 16:57:29 +0000</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>5</td>
<td>9</td>
<td>[NULL]</td>
<td>0</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>395690126.872656</td>
<td>[NULL]</td>
<td>5257</td>
<td>[NULL]</td>
<td>2013-07-16 17:55:26 +0000</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>5</td>
<td>10</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>[NULL]</td>
<td>395690239.25198</td>
<td>[NULL]</td>
<td>7416</td>
<td>[NULL]</td>
<td>2013-07-16 17:58:01 +0000</td>
</tr>
<tr>
<td>rowid</td>
<td>ZPK</td>
<td>Z_CNT</td>
<td>Z_OFF</td>
<td>Z_CONNECTED</td>
<td>ZFAVORITE</td>
<td>ZREAD</td>
<td>ZCALLITEMTOMBURNER</td>
<td>ZDATE</td>
<td>ZLASTPLAYED</td>
<td>ZBODY</td>
<td>ZCALL_SHARE_URL</td>
<td>ZRECORDING_URL</td>
<td>ZSID</td>
</tr>
<tr>
<td>-------</td>
<td>-----</td>
<td>-------</td>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>-------</td>
<td>---------------------</td>
<td>-------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------</td>
<td>------</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>2</td>
<td>6</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>2</td>
<td>7</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>2</td>
<td>9</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>17</td>
<td>17</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>18</td>
<td>18</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>19</td>
<td>19</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
</tbody>
</table>
## ZTARGETS

### rows 0-0

<table>
<thead>
<tr>
<th>rowid</th>
<th>Z_PK</th>
<th>Z_ENT</th>
<th>Z_OPT</th>
<th>ZTARGETTOPERSON</th>
<th>ZNUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>7</td>
<td>1</td>
<td>1</td>
<td>130444496771</td>
</tr>
</tbody>
</table>
## SQLite Table Summary

**Before/After Trial 1**

<table>
<thead>
<tr>
<th>Table</th>
<th>Row Count</th>
<th>Table</th>
<th>Row Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZBURNER</td>
<td>0</td>
<td>ZBURNER</td>
<td>0</td>
</tr>
<tr>
<td>ZCALLITEM</td>
<td>19</td>
<td>ZCALLITEM</td>
<td>19</td>
</tr>
<tr>
<td>ZCREDITS</td>
<td>1</td>
<td>ZCREDITS</td>
<td>1</td>
</tr>
<tr>
<td>ZENTITY</td>
<td>0</td>
<td>ZENTITY</td>
<td>0</td>
</tr>
<tr>
<td>ZINBOUNDBOUNDEMUMBER</td>
<td>6</td>
<td>ZINBOUNDBOUNDNUMBER</td>
<td>6</td>
</tr>
<tr>
<td>ZPERSON</td>
<td>1</td>
<td>ZPERSON</td>
<td>1</td>
</tr>
<tr>
<td>ZTARGETS</td>
<td>1</td>
<td>ZTARGETS</td>
<td>1</td>
</tr>
<tr>
<td>Z_PRIMARYKEY</td>
<td>7</td>
<td>Z_PRIMARYKEY</td>
<td>7</td>
</tr>
<tr>
<td>Z_METADATA</td>
<td>1</td>
<td>Z_METADATA</td>
<td>1</td>
</tr>
</tbody>
</table>

**After Trial 2**

<table>
<thead>
<tr>
<th>Table</th>
<th>Row Count</th>
<th>Table</th>
<th>Row Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZBURNER</td>
<td>0</td>
<td>ZBURNER</td>
<td>0</td>
</tr>
<tr>
<td>ZCALLITEM</td>
<td>19</td>
<td>ZCALLITEM</td>
<td>19</td>
</tr>
<tr>
<td>ZCREDITS</td>
<td>1</td>
<td>ZCREDITS</td>
<td>1</td>
</tr>
<tr>
<td>ZENTITY</td>
<td>0</td>
<td>ZENTITY</td>
<td>0</td>
</tr>
<tr>
<td>ZINBOUNDBOUNDEMUMBER</td>
<td>6</td>
<td>ZINBOUNDBOUNDNUMBER</td>
<td>6</td>
</tr>
<tr>
<td>ZPERSON</td>
<td>1</td>
<td>ZPERSON</td>
<td>1</td>
</tr>
<tr>
<td>ZTARGETS</td>
<td>1</td>
<td>ZTARGETS</td>
<td>1</td>
</tr>
<tr>
<td>Z_PRIMARYKEY</td>
<td>7</td>
<td>Z_PRIMARYKEY</td>
<td>7</td>
</tr>
<tr>
<td>Z_METADATA</td>
<td>1</td>
<td>Z_METADATA</td>
<td>1</td>
</tr>
</tbody>
</table>
**Z_PRIMARYKEY**

<table>
<thead>
<tr>
<th>rowid</th>
<th>Z_ENT</th>
<th>Z_NAME</th>
<th>Z_SUPER</th>
<th>Z_MAX</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Burner</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>CallItem</td>
<td>0</td>
<td>19</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>Credits</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>Entity</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>InboundNumber</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>Person</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>Targets</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

After Trial 1

<table>
<thead>
<tr>
<th>rowid</th>
<th>Z_ENT</th>
<th>Z_NAME</th>
<th>Z_SUPER</th>
<th>Z_MAX</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Burner</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>CallItem</td>
<td>0</td>
<td>19</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>Credits</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>Entity</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>InboundNumber</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>Person</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>Targets</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Android device</th>
<th>iOS device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapchat data was recoverable</td>
<td>Minimal Snapchat data was recoverable</td>
</tr>
<tr>
<td>- ‘Clear Feed’ removes log</td>
<td>- ‘Clear Feed’ removes log</td>
</tr>
<tr>
<td>Received Snapchat images were recoverable based on time elapsed</td>
<td>No Snapchat images were recovered</td>
</tr>
<tr>
<td>No data was recoverable from Burner app regardless of how it was removed from the device</td>
<td>All data from Burner app was recoverable for burner numbers that were not manually deleted</td>
</tr>
</tbody>
</table>
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 Sulcebrarger
- Harry Wu
References


Picture References

- www.snapchat.com
- www.burnerapp.com
- http://greggornation.files.wordpress.com/2012/12/snapchat-icon.png?w=587
- http://www/lg.com/uk/images/lg-mobile-phones/e960/gallery/medium02.jpg
- http://us.123rf.com/400wm/400/400/alexwhite/alexwhite1209/alexwhite120900032/15308285-shopping-cart-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://fs02.androidpit.info/ali/x03/8171403-1374702400804-144x144.png
Questions?

“Your smartphone is overqualified.”