Forensic Analysis of Data Transience Applications in iOS and Android

Cindy Wu[1], BS*; Christopher Vance[1], BS; Cpl. Robert Boggs[2]; Terry Fenger[1], PhD

[1] Marshall University, 1401 Forensic Science Drive, Huntington, WV 25701

[2] West Virginia State Police, South Charleston, WV 25309

Abstract

The availability of mobile applications has greatly enhanced the capabilities of mobile phone users. Among these applications are data transient apps such as Snapchat (Snapchat Inc.) and Burner (Ad Hoc Labs, Inc.), which has become prevalent amongst mobile phone consumers. In Snapchat, users are able to share timed content that 'self-destructs' upon reaching the set duration, making it no longer accessible according to the privacy policies. The Burner application allows you to double a personal mobile phone as a burner phone, maintaining the privacy of the user. Upon expiration of those phone numbers, all history and logs associated with them are removed from the device. These application characteristics are ideal for criminals who want to be untraceable when committing crimes.

In a case requiring investigation of Snapchat data, time is of the essence when it comes to the Android due to the server ability to remove received snaps from accounts after a certain elapsed time period. The iOS device showed no recoverability of any significant snaps. Both devices showed communication logs, which disappeared upon using the 'clear feed' option. The recovery of Burner application data, however, seemed to be dependent upon the device in use and whether the burner number was expired or manually removed.

Introduction

Released in September 2011 by Evan Spiegel and Bobby Murphy, Snapchat is a socialization application that permits real-time picture chatting for iOS and Android devices. However, any content shared is given a time limit between one to ten seconds before the data is no longer accessible. Over 200 million snaps are shared daily. News speculation believes this would permit 'sexting'. While this may or may not be true, the possibilities of the shared content may be unfavorable in investigations. Amongst these shared moments may involve criminal activity which include, but are not limited to, drug deals and the distribution of child pornography.

Released in August 2012 by the founders of the Ad Hoc Labs, Inc., Greg Cohn and William Carter, Burner is a free application that allows users to double a personal phone as a burner phone. A user can simultaneously maintain multiple burner numbers at a low price, which have calling and texting capabilities while still maintaining their privacy on their personal iOS or Android device. A burner number is purchased in a package to determine its limitations whether it is a data limit or time limit. A user can also dispose of the number at any time prior to reaching those set limits. Upon disposing the burner number, all data and history is claimed to be lost.

Prefacing these applications with the ability of content termination, users may use these applications for the purposes of drug deals, distribution of child pornography, and other criminal activity, expecting any exchanged content to delete upon expiration. In these cases, the recoverability of artifacts becomes essential in investigations which includes, but is not limited to observing the transferred content, timestamps, and associations amongst individuals. Snapchat factors focused on message status, time elapsed, and the 'clear feed' option while Burner factors focused on time elapsed and expiration method.

With the growing popularity of third-party applications such as Snapchat and Burner, it is likely that criminals are lurking in the shadows of these apps to circumvent the law. As far as digital forensics goes, recovery of data and artifacts from these applications is essential in digital case investigations.

Materials and Methods

Devices:

- LG® Google Nexus 4 E960: Android v4.2.2 (Jelly Bean), Wi-Fi only
- Apple® iPod Touch 4G: 32 GB of internal memory, iOS v6.1.3, Wi-Fi only

Applications:

- Snapchat developed by Snapchat, Inc., Android v3.0.0 and iOS v5.0.0
- Burner developed by Ad Hoc Labs, Inc., Android v1.0.1 and iOS v1.6.7

Methods:

- Extraction and analysis of Android device physical images after data exchanges
- Extraction and analysis of iOS device file systems after data exchanges

Analysis Tools:

- Imaging Tools: Celebrite® UFED Touch v1.9.0.130 and Celebrite Physical Analyzer v3.7.2
- Data Analysis: AccessData® Forensic Toolkit v4.0

Snapchat Results

Android Device:

- Recovered an xml file showing a full log of Snapchat communication (extensive detail) of the snaps/videos if 'Clear Feed' option was not used
  - Snaps could not be linked back to a specific log entry
  - If recent snaps/videos sent, file names were temporarily listed in the log
- Recovered some received snaps with .nomedia and .DELETED extensions
  - Duplicates were present
  - Cannot link images to sender
  - After time elapsed, these images were no longer recoverable
- No videos or sent snaps could were recovered

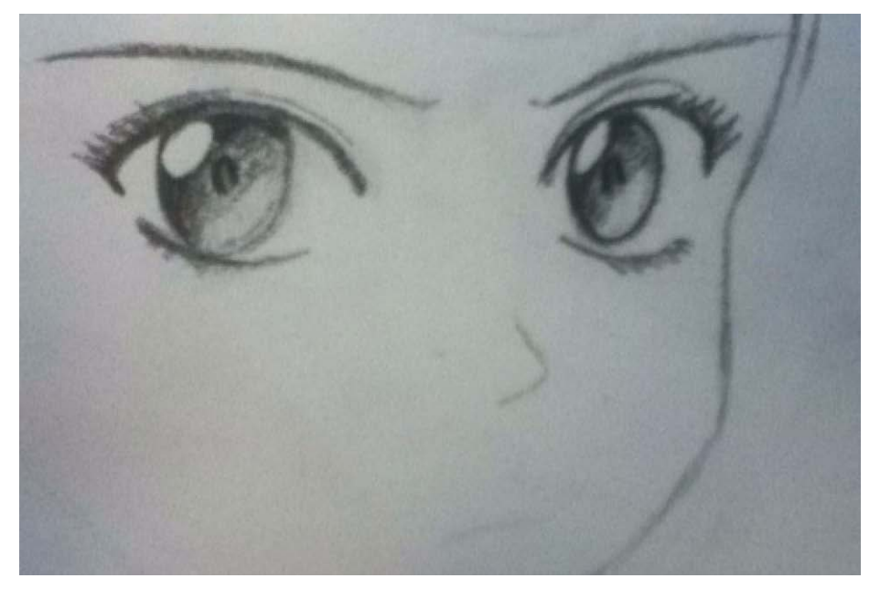


Figure 1. Received image file names:
h1a81hurcs00h1371043830917.jpg.nomedia
h1a81hurcs00h1371057362496.jpg.nomedia
h1a81hurcs00h1371057963128.jpg.nomeda
203835371300106153.DELETED

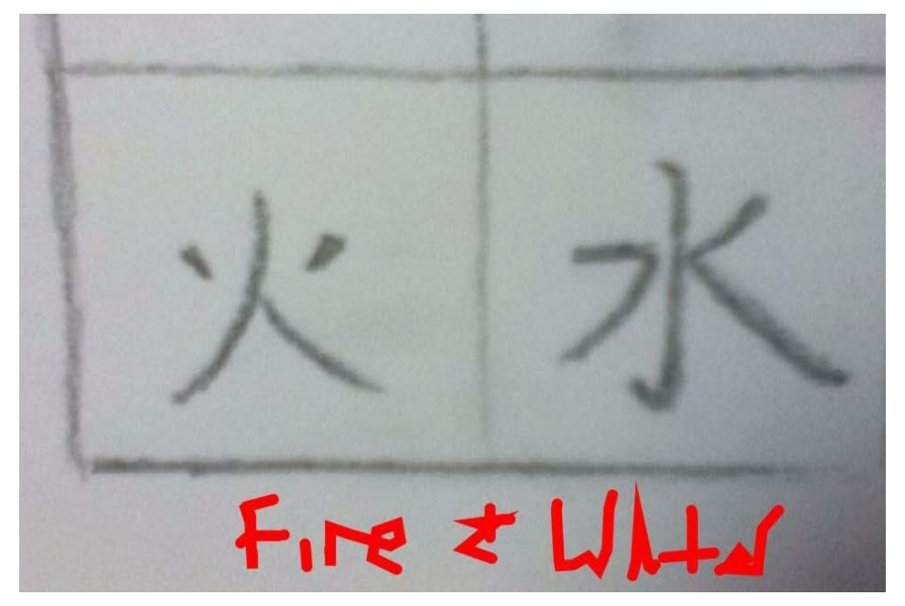


Figure 2. Received image file names:
h1a81hurcs00h1371055757416.jpg.nomedia
h1a81hurcs00h1371057362397.jpg.nomedia
63054551-740865716.DELETED
9049156885946773876.DELETED

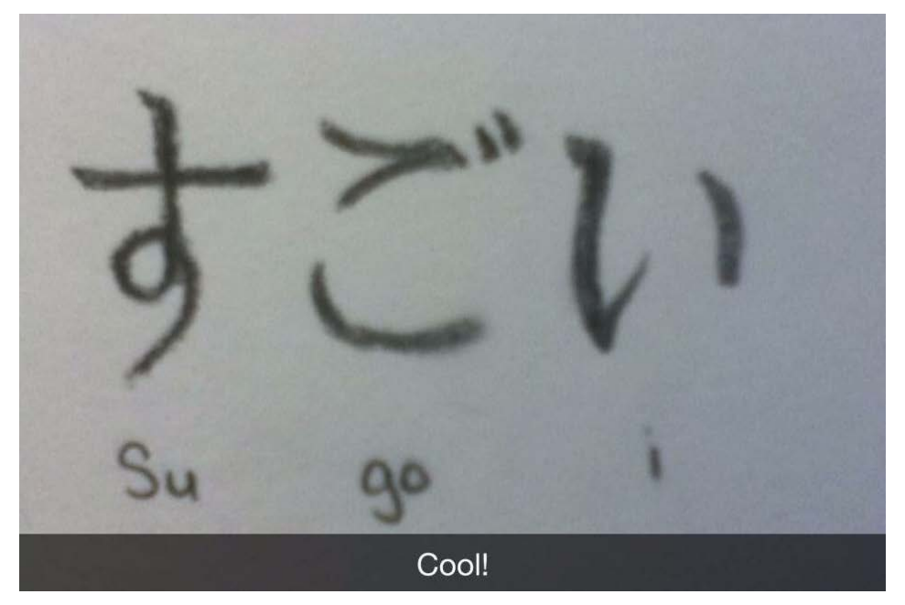


Figure 3. Received image file names:
h1a81hurcs00h1371056094700.jpg.nomedia
h1a81hurcs00h1371057362458.jpg.nomedia
h1a81hurcs00h1371062785258.jpg.nomedia
1703575864-713968389.DELETED
-5198092852378374.DELETED

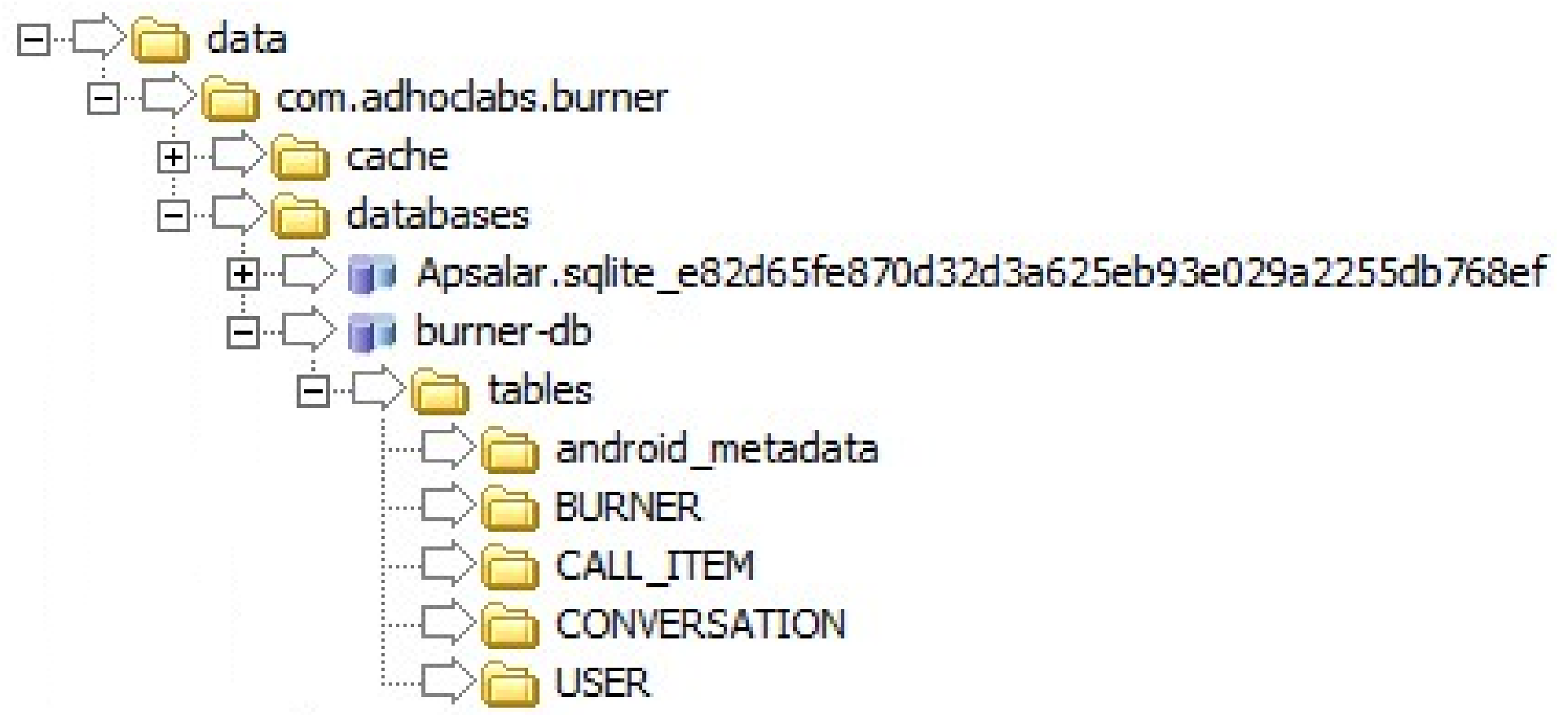
iOS Device:

- Recovered a full log of Snapchat communication (limited detail) if 'Clear Feed' option was not used
- Recovered most recent outgoing video
- No other recovered snaps or videos

Burner Results

Android Device:

- No data recovered after burner number was removed from device

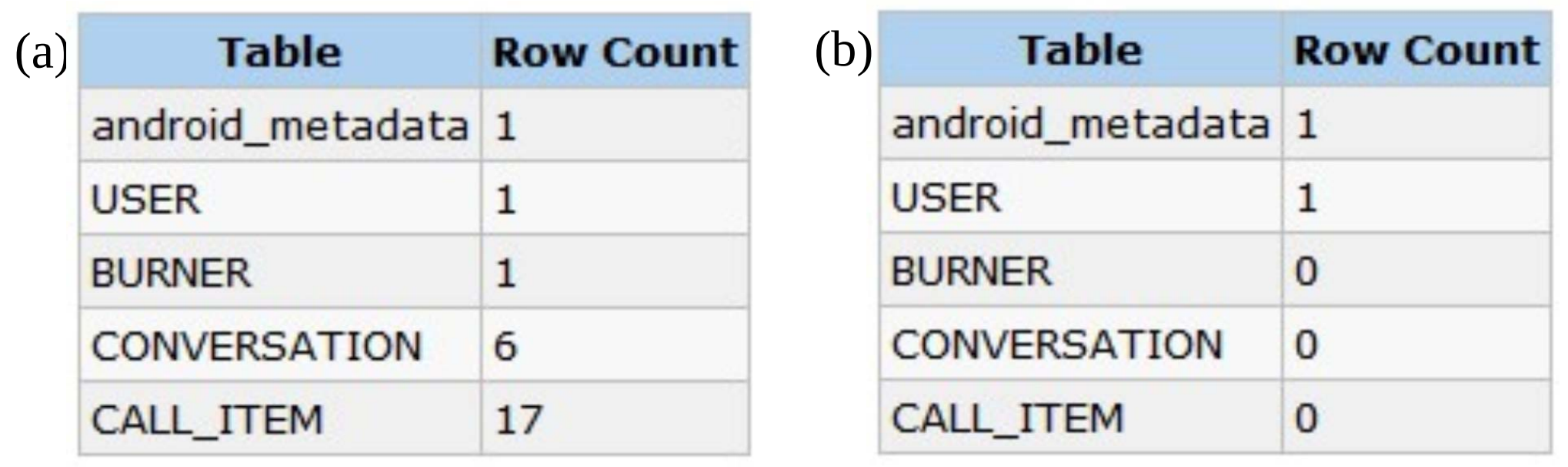


```
data
  com.adhoclabs.burner
    cache
    databases
      Apsalar.sqlite_e82d65fe870d32d3a625eb93e029a2255db768ef
      burner-db
        tables
          android_metadata
          BURNER
          CALL_ITEM
          CONVERSATION
          USER
```

Figure 4. Burner data location in the Android.

CALL_ITEM

- Conversation_ID: Which conversation a message is linked to in relation to the CONVERSATION table
- Type: Activity type of outbound sms (0), incoming sms (1), outbound call (2), or incoming call (3)
- Date: Timestamp
- Body: Message content; [NULL] indicates a call



(a)

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

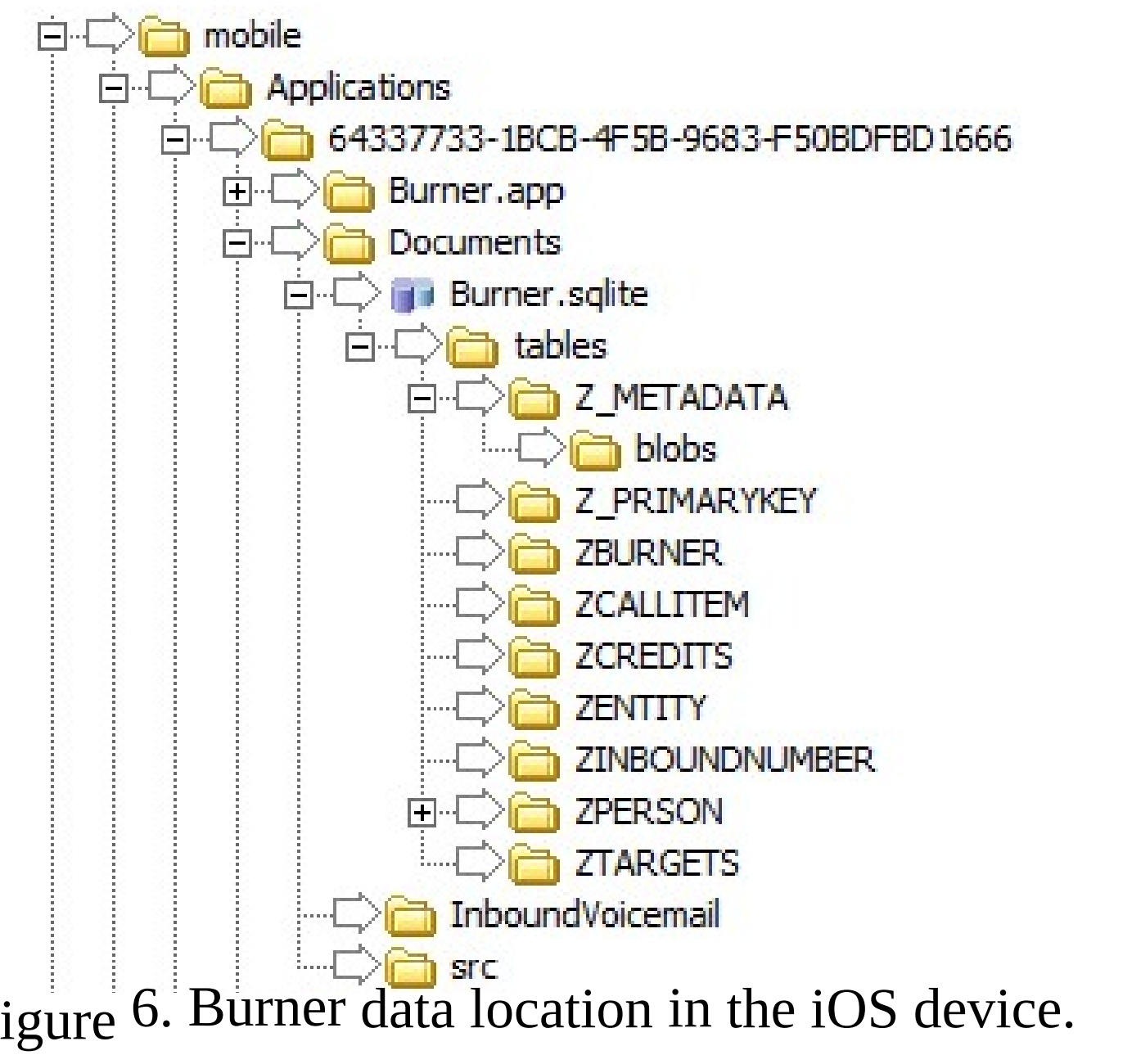
(b)

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

Figure 5. Summary of burner data for the Android device (a) before expiration of the first burner number and (b) after expiration of both burner numbers.

iOS Device:

- Data was recoverable as long as the burner number was not manually removed from the device.
- Previously automatically expired burner number data was recovered even after a second burner number was created and manually burned.

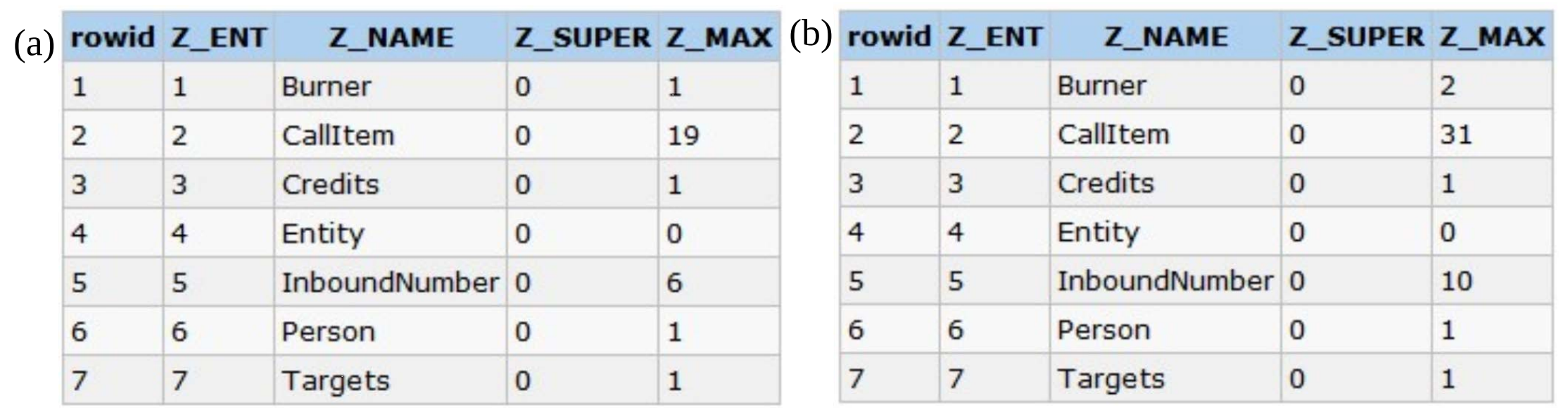


```
mobile
  Applications
    64337733-1BCB-4F5B-9683-F50BDFBD1666
      Burner.app
      Documents
        Burner.sqlite
          tables
            Z_METADATA
              blobs
            Z_PRIMARYKEY
            ZBURNER
            ZCALLITEM
            ZCREDITS
            ZENTITY
            ZINBOUNDNUMBER
            ZPERSON
            ZTARGETS
        InboundVoicemail
        src
```

Figure 6. Burner data location in the iOS device.

ZCALLITEM

- ZConnected: Whether connection was successful (1) or unsuccessful (0)
- ZCallItemToInboundNumber: Which conversation a message is linked to in relation to the ZINBOUNDNUMBER table
- ZDate: Timestamp of the message
- ZBody: Message content; [NULL] indicates a call
- ZType: Activity type (call, outbound call, sms, or outbound_sms)



(a)

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

(b)

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

Figure 7. ZPrimaryKey for the iOS device showing (a) before and after automatic expiration of the first burner number and (b) after the manual deletion of the second burner number.

Discussion and Conclusion

Investigation of Snapchat has shown that this third-party application removes snaps from the phone after a certain time has elapsed. In the iOS device, limited data was able to be recovered regarding contact, timestamp, and message ID. However, those most recently received snaps by the Android device, whether read or unread were recoverable and the reason for duplicates remain unexplained. The file names of recently sent snaps could be located in the log under 'snapsUpdatedSinceLastServerChange.' Full logs were able to be recovered for both testing devices as long as the 'Clear Feed' option was not used, which could prove a connection between two individuals. However, it was not possible to link a specific contact to an image recovered.

Investigation of the Burner app has shown that this third-party application removes all the data associated with a burner number for Android devices regardless of the manner in which it expires. No trace is left aside from the fact that a user account exists. On the iOS device, no trace of manually deleted burner numbers remained on the phone. However, all data associated with an automatically expired burner number was recoverable regardless of the time elapsed.

Future Work

Future research in this area should focus on similar third-party application that indicate that history will be wiped from the mobile device. Additionally, further research should be conducted on Snapchat to determine the estimated time before the server completely removes a snap and Burner app to test the mobile network capabilities involving calls and voicemails.

References

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>

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/>.

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>.

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

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

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

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

Image Sources

http://www.apple.com/ipod-touch/
http://www.burnerapp.com
http://www.lg.com/uk/images/lg-mobile-phones/e960/gallery/medium02.jpg
http://www.snapchat.com

Acknowledgements

The author thanks Dr. Terry Fenger, Cpl. Robert Boggs, Christopher Vance, the Marshall University Forensics Science Graduate Program, Jennifer Sulcebarger, Jamie Sternlicht, and Harry Wu for their support, facilities, and knowledge.