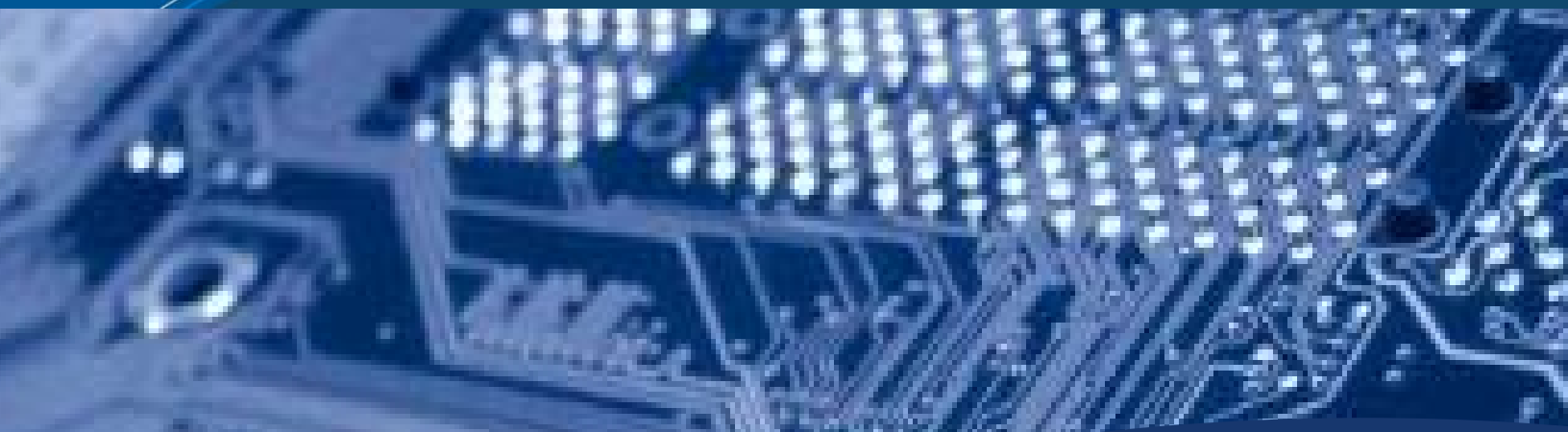
CHAMPLAIN COLLEGE

LCDI

The Senator Patrick Leahy Center for Digital Investigation



IEF for Mobile Devices

Written & Researched by

Scott Barrett & Kayla Williford

175 Lakesid Room 300A

Phone: 802/865-5744

Fax: 802/865-6446

http://www.lcdi.champlain.edu

Disclaimer:

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

Contents

Introduction

INTERNET EVIDENCE FINDER™ (IEF) is used by thousands of forensic examiners around the world to recover and analyze Internet communications for digital investigations. Renowned for ease-of-use, simplicity, and comprehensiveness, IEF Standard and IEF Advanced are revolutionary tools that allow organizations to build the best possible cases and investigations (Magnet Forensics Inc., 2013).

For this project, we will be using IEF Advanced to analyze images from Android and iOS devices. Our goal is to learn what information IEF extracts from these devices and how that can help law enforcement and forensic investigators.

Background

We were unable to find information on any previous projects that involve the mobile version of IEF. However, the LCDI has done previous research on the non-mobile version of IEF, which can be found at http://computerforensicsblog.champlain.edu/2013/06/12/internet-evidence-finder/.

Purpose and Scope

The purpose of our research is to discover what mobile applications are supported by IEF Mobile and what artifacts can be extracted by IEF. This will be beneficial to the LCDI as well as law enforcement, as they will be able to use this information to see how well IEF Mobile preforms and what information they can retrieve from an iOS or Android device with IEF.

Research Questions

1. What applications are supported by IEF?
2. What artifacts can IEF extract from an iOS or Android mobile device?

Terminology

Applications- Software that achieves a specific task designated by its user.

Artifacts- Data generated by user interaction that can be collected and examined.

Carve- A technique used to search for files based on the data and content.

Cellebrite- A forensic tool that can extract information from mobile phones.

Dropbox- A cloud service application that allows users to upload data into storage that is kept on Dropbox's servers.

Facebook- A social media application used to interact and communicate with friends and family.

Foursquare- An application that lets users check into locations to show others where they are and where they frequent.

IEF- Internet Evidence Finder

Image- A copy of a physical storage device.

Instagram- An online social application that allows users to share photos and videos with others.

Kik Messanger- An application used for chatting over wifi instead of SMS.

Skype- An application that lets users message and call eachother over wifi instead of using the phone's service.

Snapchat- An application that lets users send pictures with short captions to communicate.

Twitter- A social media application used to communicate with friends and family.

UFED Physical Analyzer- An application that works with Cellebrite to extract data from mobile devices.

WhatsApp- A social application that allows users to message eachother without needing to pay for SMS.

Methodology and Methods

Our team will use an iPhone 3GS and an Android Galaxy Appeal that have been factory reset to generate data and will keep a log of all of our activity throughout the projecy. We will download and generate data using the applications that IEF Advance supports (See IEF Artifacts (Mobile)). After our researchers have generated and logged data from the iPhone and the Android phone, we will use Cellebrite to create an image of both phones. We will then load the images we created into IEF v6.2 to see what artifacts can be found, what artifacts couldn't be found, and then compare this to IEF's list of supported artifcats. It is important to not that the phones we use at the LCDI are recycled between projects, so even when they are factory reset, there may still be information from past projects on them.

Figure 1: IEF Artifacts (Mobile)

3rd Party Apps	iOS	Android
What's App	This search will carve and parse What'sApp messages. IEF can recover message sender, conversation partner, message text and date/time stamp of the message from the sqlite database. Deleted sqlite records can also be recovered from unallocated space.	This search will carve and parse What'sApp messages. IEF can recover message sender, conversation partner, message text and date/time stamp of the message from the sqlite database. Deleted sqlite records can also be recovered from unallocated space.
Kik	This search will carve and parse Kik messages. IEF can recover message sender, conversation partner, message text and date/time stamp of the message from the sqlite database. Deleted sqlite records can also be recovered from unallocated space.	This search will carve and parse Kik messages. IEF can recover message sender, conversation partner, message text and date/time stamp of the message from the sqlite database. Deleted sqlite records can also be recovered from unallocated space.
Snapchat	This search will recover deleted Snapchat photos from unallocated space. If the Snapchat photo or video has not been viewed, it will also be recovered	This search will recover deleted Snapchat photos from unallocated space and meta-data related to deleted and live snapchat transfers. If the Snapchat photo or video has not been viewed, it will also be recovered.
Google Talk	Not supported	This search will parse Google Talk Contacts as well as messages. Recovered data includes user name, message text, date/timestamp and recipient
Sino Weibo	This search will parse for Sino Weibo messages. IEF can recover chat messages, posts, and user info with GPS and date/time info present for some artifacts.	This search will parse and carve for Sino Weibo messages. IEF can recover chat messages, posts, and user info with GPS and date/time info present for some artifacts.
AIM (AOL Instant Messenger)	This search will parse and carve for AIM messages. IEF can recover the sender, receiver, message, date/timestamp, latitude/longitude for each message.	This search will parse for AIM messages and buddies, it will also carve for AIM messages. IEF can recover the sender, receiver, message, date/timestamp, latitude/longitude of a message as well as the buddy name, IDs, avatar for each AIM user.
Skype	This search will parse Skype history records from the SQLite files Skype uses to store its data. This includes messages, group chat info, calls, accounts, contacts, file transfers, voicemails, and SMS messages. IEF can also carve Skype messages from	This search will parse Skype history records from the SQLite files Skype uses to store its data. This includes messages, group chat info, calls, accounts, contacts, file transfers, voicemails, and SMS messages. IEF can also carve Skype messages from

	unallocated space.	unallocated space.
Facebook	This search will parse Facebook friend and message records from the SQLite files Facebook uses to store its data. IEF can also carve Facebook messages from unallocated space.	This search will parse Facebook contacts, friends, pictures, messages and user records from the SQLite files Facebook uses to store its data. IEF can also carve Facebook messages from unallocated space.
Instagram	This search will parse the folder that contains the instagram uploaded and profile pictures.	This search will parse and carve the json file that stores usernames, date/timestamp photos uploaded and profile pictures. Instagram data can be found in unallocated space.
Foursquare	This search will parse and carve the sqlite databases that store the Foursquare check-in locations including the latitude and longitude that can be viewed in the world map found in IEF report viewer. This information can be found in unallocated space as well.	This search will parse the sqlite databases that store the Foursquare check-in locations including the latitude and longitude that can be viewed in the world map found in IEF report viewer. Other recovered fields include address, date/time of checkin and user that checked in. IEF will also parse and carve the Foursquare json file that stores a lot of the same information that is found in the sqlite file. This information can be found in unallocated space as well.
Dropbox	This search will parse and carve the sqlite databases that store the Dropbox uploads. This information can be found in unallocated space as well. Data recovered can include file names, dates/times, user ID's, file sizes, and more.	This search will parse and carve the sqlite databases that store the Dropbox uploads. This information can be found in unallocated space as well. Data recovered can include file names, dates/times, user ID's, file sizes, and more.
Google Maps	This search will parse Google Map search locations. This information is pulled out as X,Y,Z coordinates found the Google Maps SQLite database(includes rebuilding surrounding areas in report viewer)	Listed above under 'Native Phone Apps: Maps'
Gmail	Not supported	This search will parse the gmail application sqlite database to recover email summary, recipient, sent status, html body. IEF will decompress the email body to display it in plain text.
Twitter	This search will carve and parse the Twitter sqlite database to recover tweets, date/timestamps of the tweets as well as Twitter friends (followers). This data can be extracted from unallocated space.	This search will carve and parse the Twitter sqlite database to recover tweets, date/timestamps of the tweets as well as Twitter friends (followers). This data can be extracted from unallocated space.

Appendix A(iOS) shows the logs for the interactions on the iPhone.

Appendix B(Android) shows the logs for the interactions on the Android phone.

Equipment Used

Table 1: Equipment and Software (iOS)

Item	Identifier	Size/Specification
iPhone 3GS iOS	v. 4.2	8GB
Internet Evidence Finder	*v. 6.2.1*	*Used to view artifacts created on a device.*
Cellebrite		*Used to create image files of mobile devices.*
Kik Messenger	*v. 5.5.3*	*A messanger application used to generate data*
Snapchat		*Messenger application used to generate data*
Dropbox	*v. 1.5.5*	*Cloud Service used to generate data*
Facebook	*v. 4.1.1*	*A social media application used to generate data*
Twitter	*v. 4.3.2*	*A social media application used to generate data*
Skype	*v. 3.7.40*	*An application with the ability to call and send messages used to generate data*
Foursquare	*v. 4.2.3*	*A social media application used to generate data*
Maps		*Used to generate data*
Browser		*The internet application used to generate data*
Notes		*A note taking application used to generate data*
Gmail		*Email service used to generate data*

Table 2: Equipment and Software (Android)

Item	Identifier	Size/Specification
Android phone	*OS v.2.3.6*	Galaxy Appeal i827
Internet Evidence Finder	*v.6.2.1*	*Used to view artifacts created on a mobile device*
Cellebrite Touch		*Used to create image files*
Snapchat	*v.4.0.08*	*A social networking application used to generate data*
Kik Messenger	*v.6.7.0*	*A social networking application used to generate data*
Skype	*v.4.4.0.31835*	*A social networking application used to generate data*
Facebook	*v.1.8.2*	*A social networking application used to generate data*
Foursquare	*v.2013.10.07*	*A social-location application used to generate data*
Dropbox	*v.2.3.10.4*	*A Cloud Service application used to generate data*
Twitter	*v.4.1.8L*	*A social networking application used to generate data*
Instagram	*v.4.1.2*	*A social networking application used to generate data*
Gmail	*v.2.3.5.2*	*Email used to generate data*

Data Collection

Data was collected from the mobile devices with the use of the mobile forensic tool Cellebrite. Cellebrite created a disc image file of the phone and we then import the disk image file into IEF using the mobile feature. IEF then creates a report of the artifacts found on the disk image file.

Recovered Artifacts

Table 3: (iOS)

Recovered Artifact	Amount Found
Paresed Search Queries	*1*
iOS iMessage/SMS	*1*
iOS KiK Messenger Messages	*3*
iOS Kik Messenger Users	*2*
iOS SMS Carved	*34*
Skype Accounts- iefforensics	*1*
Skype Calls- iefforensics	*4*
Skype Carved Messenges	*1*
Skype Chat Messages	*17*
Skype Chatsync Messages	*8*
Skype Contacts- iefforensics	*2*
iOS Email	*10*
iOS Email Fragments	*182*
AMR Files	*7*
iOS Snapshots	*2*
Pictures	*13,780*
Videos	*1*
iOS Notes	*1*
iOS Foursquare Locations	*1*
Browser Activity	*25*
iOS Google Map Coordinates	*82*
iOS Safari Bookmarks	*1*
iOS Safari History	*9*
Safari History Carved	*18*

Table 4: (Android)

Data Collected	Number of

	Items Collected
Dropbox activity under Cloud Services	*6*
Twitter activity under Cloud Services	*2*
Text messages	*3*
Android Emails	*35*
Android Gmail	*15*
AMR files	*17*
Pictures	*15,980*
Instagram Posts	*171*
Twitter Tweets Carved	*317*
Browser Activity	*201*

Analysis

The data for analysis came form the disk image file (an image of the mobile devices that we generated activity on) created by Cellebrite. We logged interaction on all of the applications that Magnet Forensics states are supported by IEF Mobile. We expect that IEF Mobile will be able to extract the artifacts of the applications that we logged interactions with. There were approximately 34 texts (sent and received) found by IEF that were not logged on the iOS device and 1 text found on the Android device. These texts from previous use of the phones and were still able to be extracted even after a factory reset (see Figures 2, 3, and 4 in Recovered Artifact Examples: IEF). We found that in the iOS and Anroid devices not many artifacts from supported applications were found. Facebook and Twitter are two major applications that are supported by IEF Mobile, but their artifacts were not found in the iOS device. We considered this to be an important find, seeing as both applications are promenant social networking applications and not being able to analyze them is disappointing.

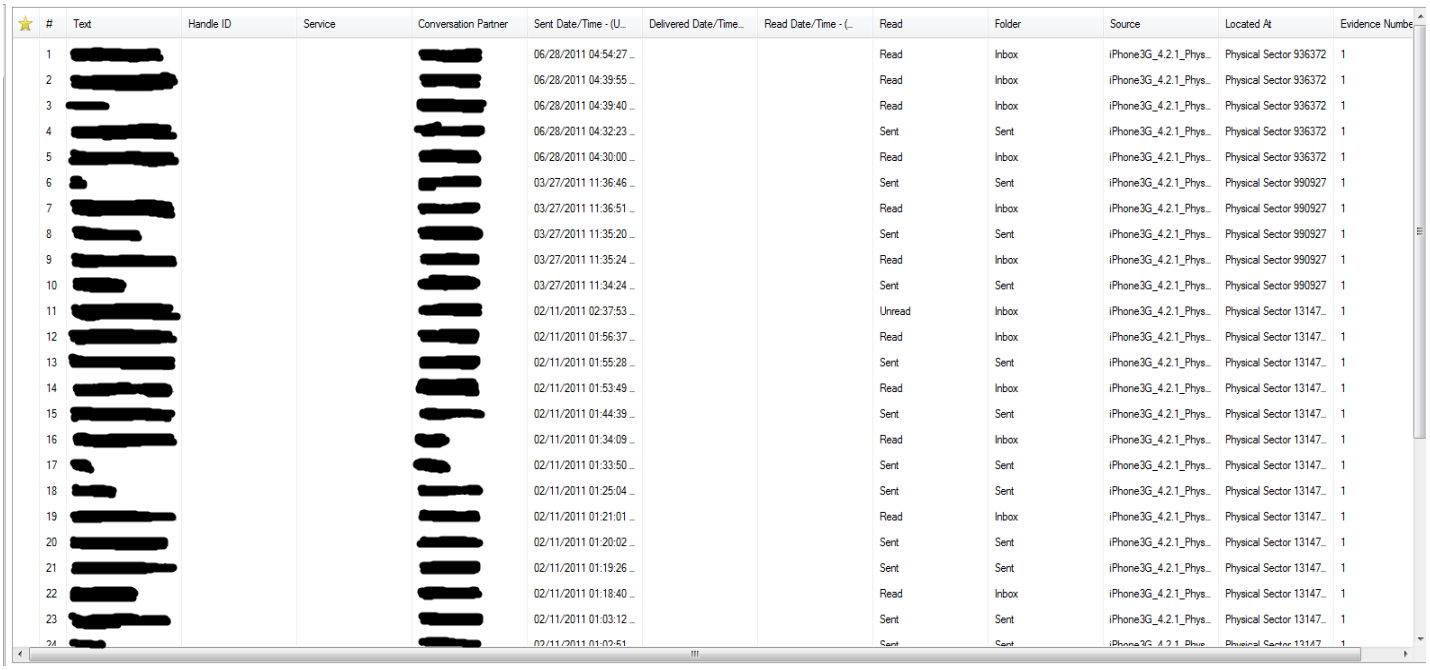
IEF Compared to Cellebrite

We compared our findings from the Android phone as imaged by both IEF and Cellebrite. When compared to IEF, we did not retrieve as much data when using UFED Physical Analyzer, a tool that works with Cellebrite, but the data we did extract was more detailed. With UFED Physical Analyzer, we found the exact pictures we took when using Cellebrite, along with other photos that had been downloaded through applications (see screenshots in Recovered Artifact Examples: Cellebrite for specific examples of what was extracted). When

using IEF, we were able to recover deleted information; however, with Cellebrite, we could see an attempted call log from Skype that was not recovered by IEF.

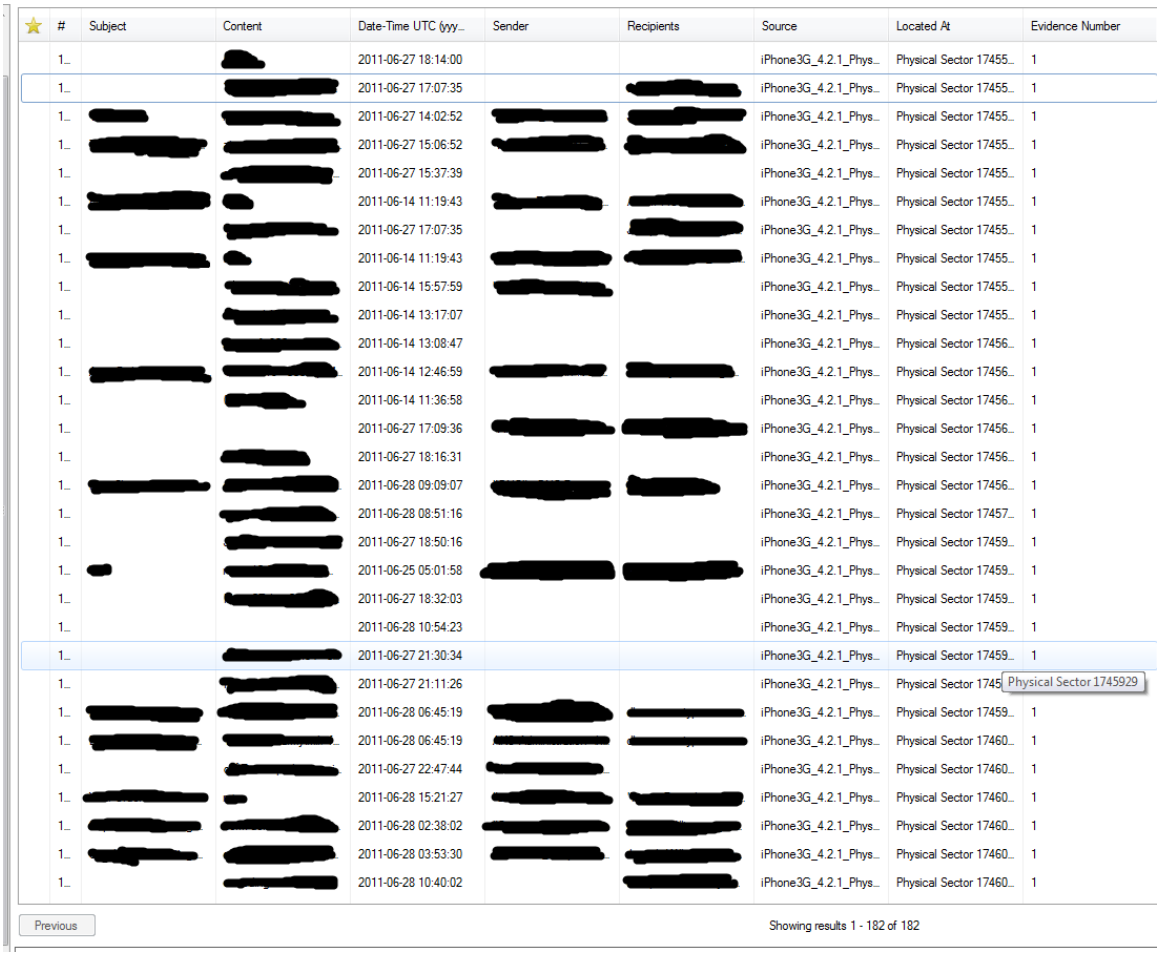
Recovered Artifact Examples: IEF

Figure 2: Texts From Before Factory Reset(iOS)



#	Text	Handle ID	Service	Conversation Partner	Sent Date/Time - (U...	Delivered Date/Time...	Read Date/Time - (...	Read	Folder	Source	Located At	Evidence Numbe
1	[redacted]			[redacted]	06/28/2011 04:54:27 ...			Read	Inbox	iPhone3G_4.2.1_Phys...	Physical Sector 936372	1
2	[redacted]			[redacted]	06/28/2011 04:39:55 ...			Read	Inbox	iPhone3G_4.2.1_Phys...	Physical Sector 936372	1
3	[redacted]			[redacted]	06/28/2011 04:39:40 ...			Read	Inbox	iPhone3G_4.2.1_Phys...	Physical Sector 936372	1
4	[redacted]			[redacted]	06/28/2011 04:32:23 ...			Sent	Sent	iPhone3G_4.2.1_Phys...	Physical Sector 936372	1
5	[redacted]			[redacted]	06/28/2011 04:30:00 ...			Read	Inbox	iPhone3G_4.2.1_Phys...	Physical Sector 936372	1
6	[redacted]			[redacted]	03/27/2011 11:36:46 ...			Sent	Sent	iPhone3G_4.2.1_Phys...	Physical Sector 990927	1
7	[redacted]			[redacted]	03/27/2011 11:36:51 ...			Read	Inbox	iPhone3G_4.2.1_Phys...	Physical Sector 990927	1
8	[redacted]			[redacted]	03/27/2011 11:35:20 ...			Sent	Sent	iPhone3G_4.2.1_Phys...	Physical Sector 990927	1
9	[redacted]			[redacted]	03/27/2011 11:35:24 ...			Read	Inbox	iPhone3G_4.2.1_Phys...	Physical Sector 990927	1
10	[redacted]			[redacted]	03/27/2011 11:34:24 ...			Sent	Sent	iPhone3G_4.2.1_Phys...	Physical Sector 990927	1
11	[redacted]			[redacted]	02/11/2011 02:37:53 ...			Unread	Inbox	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
12	[redacted]			[redacted]	02/11/2011 01:56:37 ...			Read	Inbox	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
13	[redacted]			[redacted]	02/11/2011 01:55:28 ...			Sent	Sent	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
14	[redacted]			[redacted]	02/11/2011 01:53:49 ...			Read	Inbox	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
15	[redacted]			[redacted]	02/11/2011 01:44:39 ...			Sent	Sent	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
16	[redacted]			[redacted]	02/11/2011 01:34:09 ...			Read	Inbox	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
17	[redacted]			[redacted]	02/11/2011 01:33:50 ...			Sent	Sent	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
18	[redacted]			[redacted]	02/11/2011 01:25:04 ...			Sent	Sent	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
19	[redacted]			[redacted]	02/11/2011 01:21:01 ...			Read	Inbox	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
20	[redacted]			[redacted]	02/11/2011 01:20:02 ...			Sent	Sent	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
21	[redacted]			[redacted]	02/11/2011 01:19:26 ...			Sent	Sent	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
22	[redacted]			[redacted]	02/11/2011 01:18:40 ...			Read	Inbox	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
23	[redacted]			[redacted]	02/11/2011 01:03:12 ...			Sent	Sent	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1
24	[redacted]			[redacted]	02/11/2011 01:02:51 ...			Sent	Sent	iPhone3G_4.2.1_Phys...	Physical Sector 13147...	1

Figure 3: Email Fragments From Before Factory Reset(iOS)



#	Subject	Content	Date-Time UTC (yyy...	Sender	Recipients	Source	Located At	Evidence Number
1...			2011-06-27 18:14:00			iPhone3G_4.2.1_Phys...	Physical Sector 17455...	1
1...			2011-06-27 17:07:35			iPhone3G_4.2.1_Phys...	Physical Sector 17455...	1
1...			2011-06-27 14:02:52			iPhone3G_4.2.1_Phys...	Physical Sector 17455...	1
1...			2011-06-27 15:06:52			iPhone3G_4.2.1_Phys...	Physical Sector 17455...	1
1...			2011-06-27 15:37:39			iPhone3G_4.2.1_Phys...	Physical Sector 17455...	1
1...			2011-06-14 11:19:43			iPhone3G_4.2.1_Phys...	Physical Sector 17455...	1
1...			2011-06-27 17:07:35			iPhone3G_4.2.1_Phys...	Physical Sector 17455...	1
1...			2011-06-14 11:19:43			iPhone3G_4.2.1_Phys...	Physical Sector 17455...	1
1...			2011-06-14 15:57:59			iPhone3G_4.2.1_Phys...	Physical Sector 17455...	1
1...			2011-06-14 13:17:07			iPhone3G_4.2.1_Phys...	Physical Sector 17455...	1
1...			2011-06-14 13:08:47			iPhone3G_4.2.1_Phys...	Physical Sector 17456...	1
1...			2011-06-14 12:46:59			iPhone3G_4.2.1_Phys...	Physical Sector 17456...	1
1...			2011-06-14 11:36:58			iPhone3G_4.2.1_Phys...	Physical Sector 17456...	1
1...			2011-06-27 17:09:36			iPhone3G_4.2.1_Phys...	Physical Sector 17456...	1
1...			2011-06-27 18:16:31			iPhone3G_4.2.1_Phys...	Physical Sector 17456...	1
1...			2011-06-28 09:09:07			iPhone3G_4.2.1_Phys...	Physical Sector 17456...	1
1...			2011-06-28 08:51:16			iPhone3G_4.2.1_Phys...	Physical Sector 17457...	1
1...			2011-06-27 18:50:16			iPhone3G_4.2.1_Phys...	Physical Sector 17459...	1
1...			2011-06-25 05:01:58			iPhone3G_4.2.1_Phys...	Physical Sector 17459...	1
1...			2011-06-27 18:32:03			iPhone3G_4.2.1_Phys...	Physical Sector 17459...	1
1...			2011-06-28 10:54:23			iPhone3G_4.2.1_Phys...	Physical Sector 17459...	1
1...			2011-06-27 21:30:34			iPhone3G_4.2.1_Phys...	Physical Sector 17459...	1
1...			2011-06-27 21:11:26			iPhone3G_4.2.1_Phys...	Physical Sector 1745	
1...			2011-06-28 06:45:19			iPhone3G_4.2.1_Phys...	Physical Sector 17459...	1
1...			2011-06-28 06:45:19			iPhone3G_4.2.1_Phys...	Physical Sector 17460...	1
1...			2011-06-27 22:47:44			iPhone3G_4.2.1_Phys...	Physical Sector 17460...	1
1...			2011-06-28 15:21:27			iPhone3G_4.2.1_Phys...	Physical Sector 17460...	1
1...			2011-06-28 02:38:02			iPhone3G_4.2.1_Phys...	Physical Sector 17460...	1
1...			2011-06-28 03:53:30			iPhone3G_4.2.1_Phys...	Physical Sector 17460...	1
1...			2011-06-28 10:40:02			iPhone3G_4.2.1_Phys...	Physical Sector 17460...	1

Physical Sector 1745929

Previous

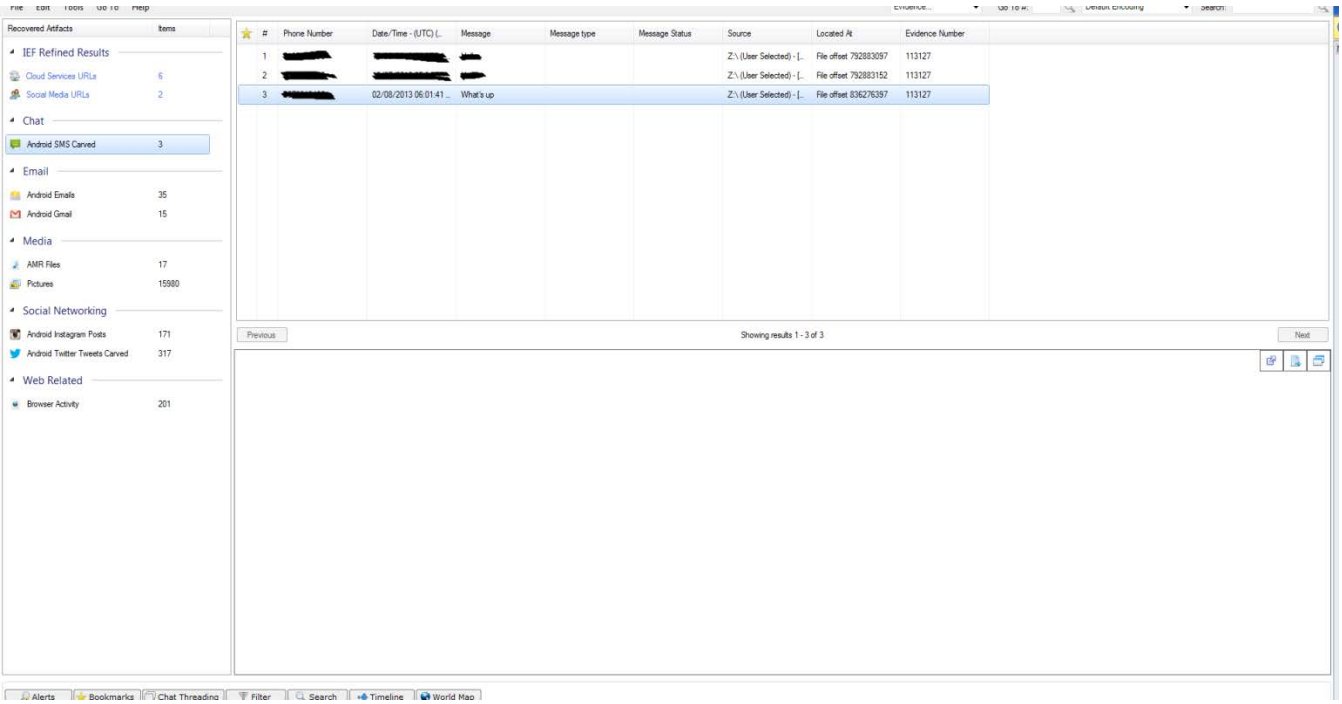
Showing results 1 - 182 of 182

Figure 4: Google Searches From Before Factory Reset(iOS)

#	Search Term	Search Engine	Google Original Sear...	URL	Web Page Title	Artifact	Artifact ID	Date/Time - (UTC) (...	Source	Located At	Evidence Number
1	iphone 3gs	Google	Iphone 3g	http://www.google.co...	iphone 3gs - Google S...	Safari History	3	10/24/2013 02:12:34 ...	iPhone3G_4.2.1_Phys...	n/a	1
2	http://www.magnetfor...	Google		http://www.google.co...	IEF Advanced | Magn...	Safari History	5	10/24/2013 02:06:36 ...	iPhone3G_4.2.1_Phys...	n/a	1
3	lef mobile forensics	Google	lef mobile forensics	http://www.google.co...	lef mobile forensics - G...	Safari History	6	10/24/2013 02:06:02 ...	iPhone3G_4.2.1_Phys...	n/a	1
4	http://en.wikipedia.or...	Google		http://www.google.co...	Liver - Wikipedia, the f...	Safari History Carved	9	06/26/2011 10:30:45 ...	iPhone3G_4.2.1_Phys...	Physical Sector 949413	1
5	http://www.mamashe...	Google		http://www.google.co...	The Human Liver: fun...	Safari History Carved	10	06/26/2011 05:17:56 ...	iPhone3G_4.2.1_Phys...	Physical Sector 949413	1
6	liver	Google		http://www.google.co...	liver - Google Search	Safari History Carved	11	06/26/2011 05:17:25 ...	iPhone3G_4.2.1_Phys...	Physical Sector 949413	1
7	http://en.wikipedia.or...	Google		http://www.google.co...	Dialysis - Wikipedia, th...	Safari History Carved	17	06/26/2011 04:52:50 ...	iPhone3G_4.2.1_Phys...	Physical Sector 949413	1
8	dialysis	Google		http://www.google.co...	dialysis - Google Search	Safari History Carved	18	06/26/2011 04:51:56 ...	iPhone3G_4.2.1_Phys...	Physical Sector 949413	1

Figure 5: Grey Squares(iOS)

Figure 6: Recovered Text Message From Before Factory Reset (Android)



Recovered Artifact Examples: Cellebrite

Figure 7: Extraction summary of data (Android)

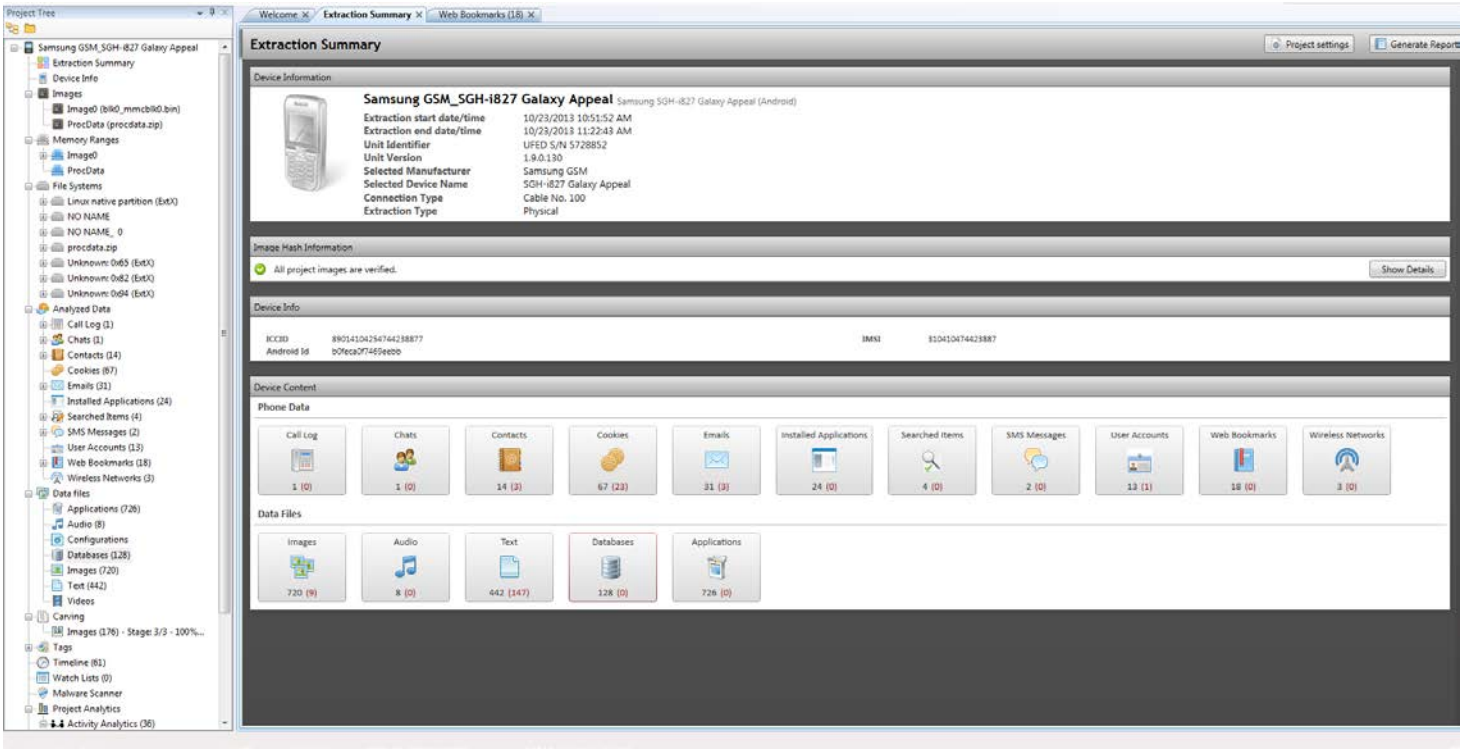


Figure 8: Timeline Log (Android)

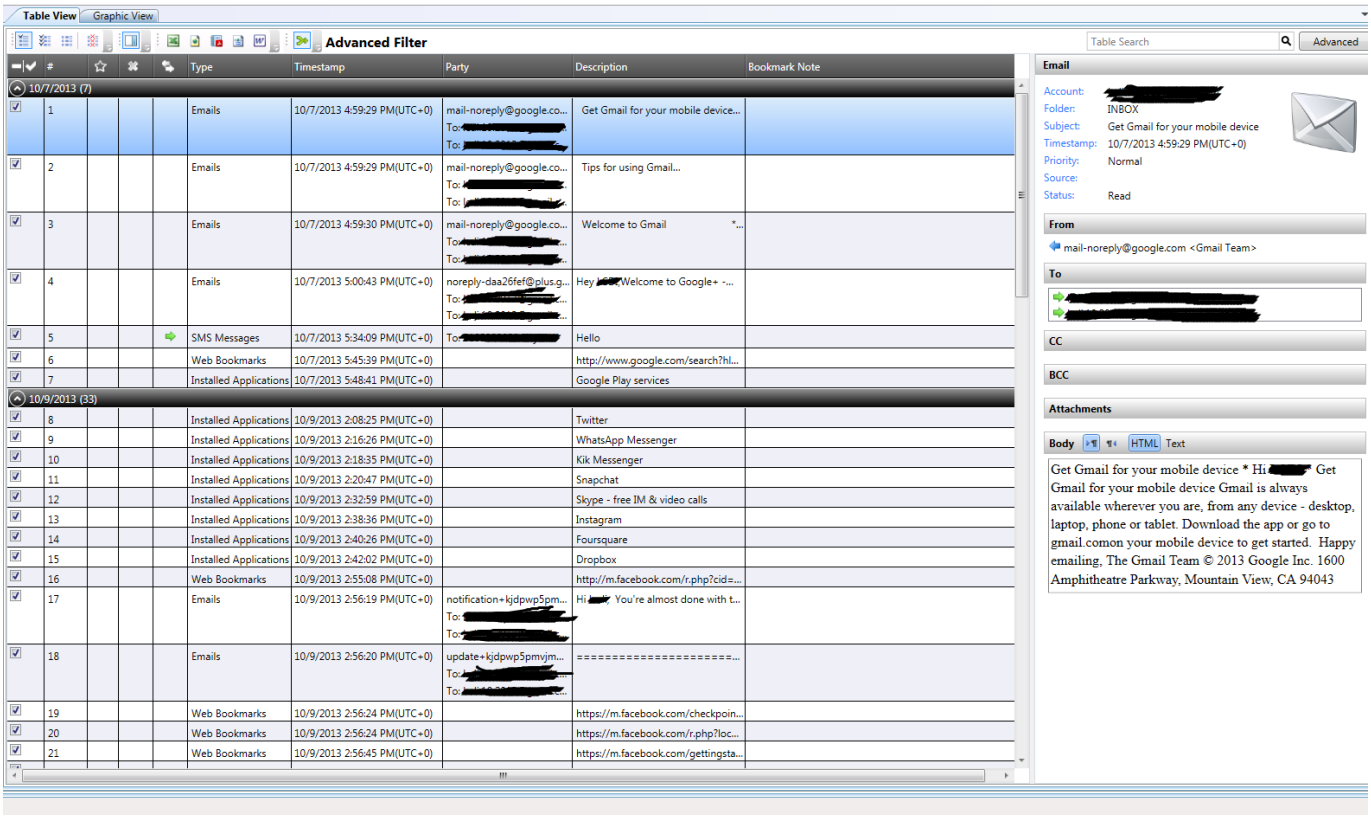


Figure 9: Photos Extracted (Android)

Figure 10: Applications Downloaded (Android)

#	Name	Version	Description	Identifier	Application ID	Purchase Date	Deleted Date
0				com.google.android.apps.b...			
1				com.google.android.gm			
2				com.google.android.voices...			
3				com.facebook.katana			
4				com.google.android.apps....			
5				com.google.android.music			
6				com.yellowpages.android.y...			
7				com.sec.spp.push			
8				com.mobitv.client.tv			
9				com.google.android.talk			
10				com.google.android.street			
11				com.telenav.app.android.ci...			
12				com.google.android.youtube			
13				com.google.android.apps.p...			
14				com.samsung.swift.app.kies...			
15	Dropbox			com.dropbox.android		10/9/2013 2:42:02 PM(UTC+0)	
16	Foursquare			com.joelapenna.foursquared		10/9/2013 2:40:26 PM(UTC+0)	
17	Google Play services			com.google.android.gms		10/7/2013 5:48:41 PM(UTC+0)	
18	Instagram			com.instagram.android		10/9/2013 2:38:36 PM(UTC+0)	
19	Kik Messenger			kik.android		10/9/2013 2:18:35 PM(UTC+0)	
20	Skype - free IM & video calls			com.skype.raider		10/9/2013 2:32:59 PM(UTC+0)	
21	Snapchat			com.snapchat.android		10/9/2013 2:20:47 PM(UTC+0)	
22	Twitter			com.twitter.android		10/9/2013 2:08:25 PM(UTC+0)	
23	WhatsApp Messenger			com.whatsapp		10/9/2013 2:16:26 PM(UTC+0)	

Results

While IEF Mobile was unable to find all of the information that was logged onto the iOS device, it did recover a large amount of data. The results will be written in the order it was presented through IEF. The first data we received was a set of Google searches that were made on the phone. The first three emails listed in IEF were generated during the project, with the remaining emails coming from before the factory reset and dated 2011 (see Figure 4 in Recovered Artifact Examples). The next artifacts were from Kik. IEF showed only the usernames involved in messages that were conducted but was able to recover the message log even after it was deleted from the application. The carved SMS was especially interesting, as the phone was not activated and was unable to send or receive any text messages. We did not think we would retrieve any artifacts for SMS, but IEF found 34 messages sent and received from 2011 (see Figure 2 in Recovered Artifact Examples). IEF was able to retrieve the majority of the generated data through Skype, including the Skype accounts from the phone, all the incoming and outgoing calls, the contacts, and the messages we logged even though we deleted them. IEF was able to recover the emails that we received from the Gmail account we created, but it did not find the email that we deleted. IEF also found 182 email fragments, mostly from before the reset (see Figure 3 in Recovered Artifact Examples). Also, IEF recovered seven voicemails that were left on the phone after the factory reset. There was a staggering amount of pictures found: 13,780 in total. We used the skin tone slider to find our pictures, as we knew what colors were prominent in the ones we took. We found the 3 pictures that we took, but the other pictures are either gray squares (see Figure 5 in Recovered Artifact Examples) or pictures

that we believe were automatically stored from Facebook. The only video that was found is a Dropbox tutorial saved by the application. We did not create any videos on the phone, so we were surprised when one was recovered. We made two notes on the phone, one to keep and the other to delete. IEF was able to find the note that we kept on the phone but did not find the deleted note. The only data IEF found for Foursquare is the location that we checked in at, not the comment we had writtten. For web artifacts, IEF listed browser activity and Safari separately. For browser history, it showed 25 urls that were not visited by us and must have been accessed before the reset. For the artifact named Safari History, IEF found all of the data that we had created. Additionally, IEF carved 18 urls and only the first two were logged by us. The others were accessed before the factory reset. Lastly, IEF retrieved 82 Google Map Coordinates. We could not definitively tell if they were from our actions or from before the factory reset because of the lack of timestamps. To see the results that IEF found for iOS, see IEF Results (iOS).

For Android, we were unable to find all the information we logged. IEF recovered most of our created Dropbox and Twitter activity under Cloud Services URLs. Text messages were found with the date and time they were sent. Aditionally, two of the three SMS we found were generated by us, but never went through. The other SMS found was sent in February 2013 by a previous user. Emails through the Gmail account were seen with the date and times they were sent, along with who sent the email. Complete pictures were recovered, both pictures that we took as well as pictures we believe were previously taken in other research here at the LCDI. In addition, logos and default photos stored on the phone were recovered. Our generated Instagram activity was specifically intriguing. We were able to see posts made by users from our feeds on Instagram and on Twitter, including exact texts of what the application generated. IEF also found tweets that we deleted (“Goodmorning Twitter” was one such tweet). No deleted Instagram posts were found.

There were four major applications that IEF did not gather any artifacts from on the iOS device: Twitter, Facebook, Snapchat, and Dropbox. All of these are said to be supported by IEF; however, we believe that IEF couldn’t analyze these applications because the phone and applications were older than the currently supported versions. Some applications were not able to be downloaded and therefore not able to be checked for compatibility with IEF. The applicaitions that were not able to be downloaded on the IOS phone because of the age of the phone were What’s App, Instagram, and Google Maps. On the Android phone, no activity could be logged by What’s App and Google Maps.

Figure 11: IEF Results (iOS)

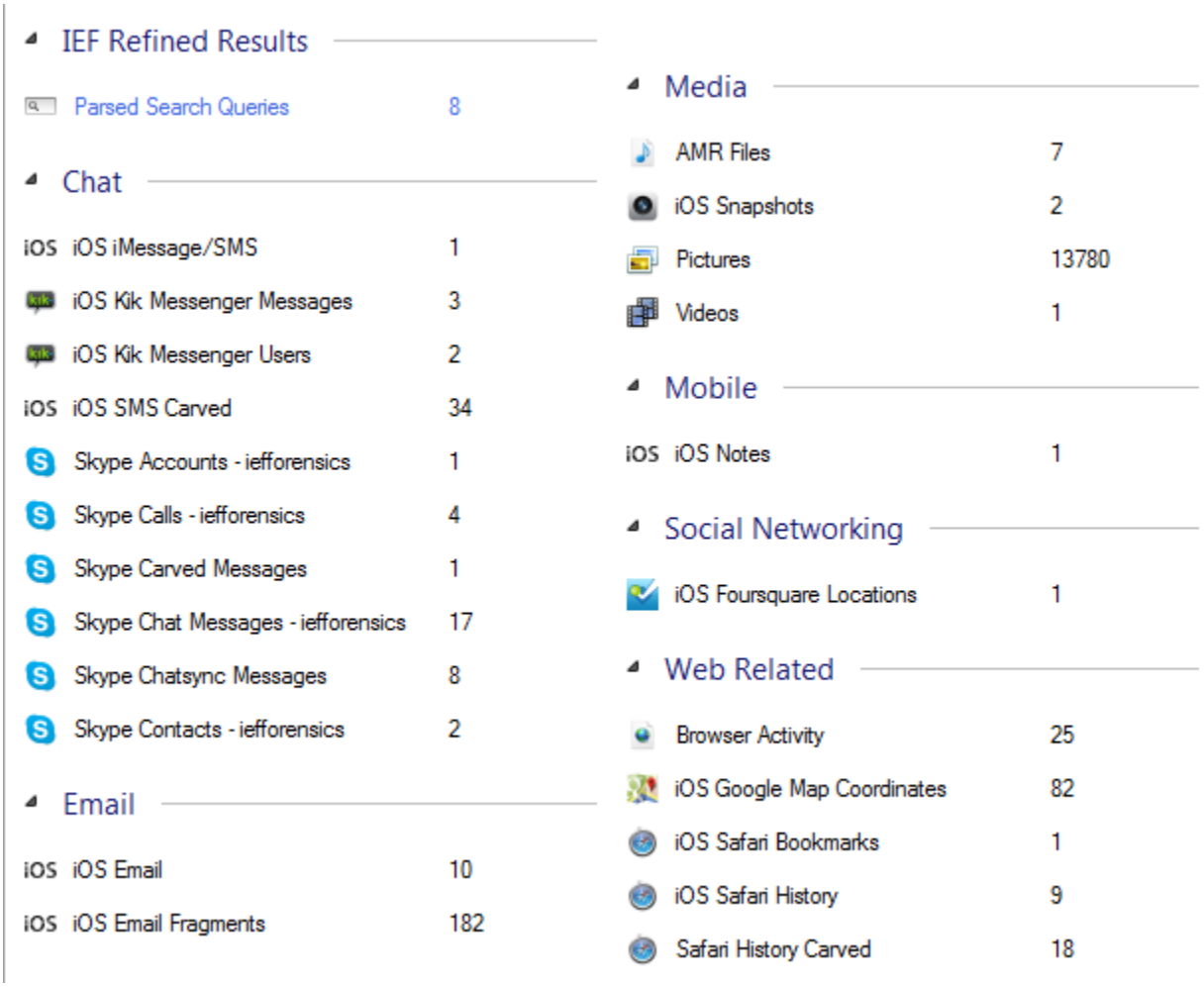


Figure 12: IEF Results (Android)

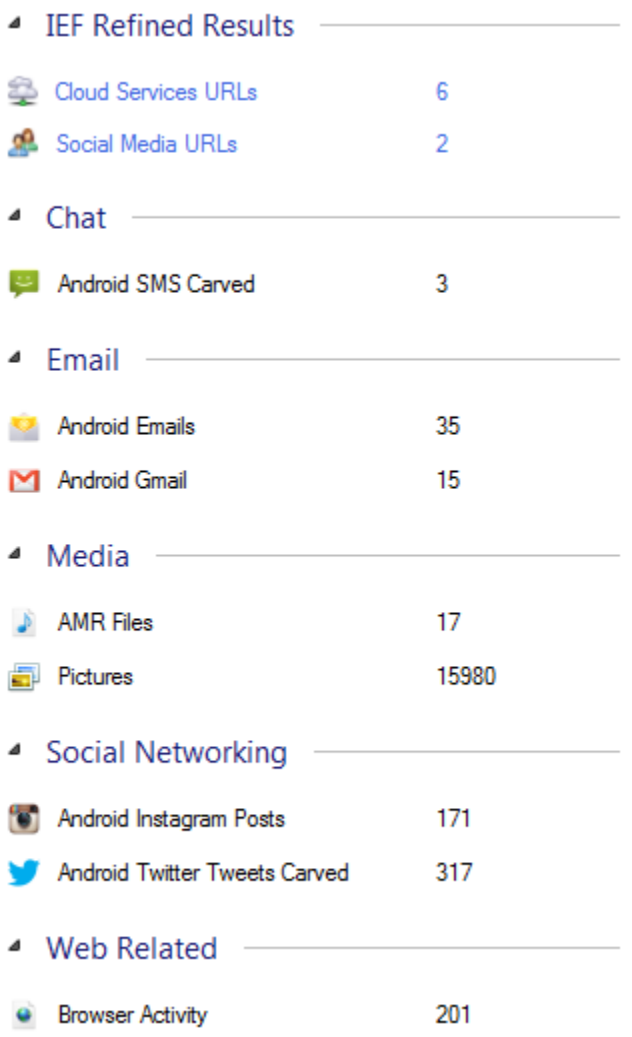


Table 5: IEF Supported Applications

Applications that are said to be supported	Was data recovered?(Android)	Was data recovered?(iOS)
Facebook	No	No
Instagram	Yes	No
Twitter	Yes	No
What's App	No	No
Kik Messenger	No	Yes
Skype	No	Yes
Flickr	No	No
Foursquare	No	Yes

Google Maps	No	No
Contacts	No	No
Dropbox	Only URLs	No
Gmail	Yes	Yes
SMS	Yes	Yes
Pictures	Yes	Yes

Conclusion

The applications that Magnet Forensics claims are supported by IEF Mobile for iOS devices are SMS, voicemail, browser, Maps, pictures, notes, call logs, email, application snapshots, What's App, Kik, Snapchat, Sino Weibo, AIM (AOL Instant Messenger), Skype, Facebook, Instagram, Foursquare, Dropbox, Google Maps, and Twitter.

For Android devices the list of supported applications is: What's App, Kik, Snapchat, Google Talk, Sino Weibo, AIM (AOL Instant Messanger), Skype, Facebook, Instagram, Foursquare, Dropbox, Gmail, Twitter and Yahoo Messenger.

The artifacts that were able to be extracted from an iOS device were: Google searches, Kik messages and users, SMS, Skype accouts, Skype call logs, Skype chats, Skype contacts, Email, AMR files, iOS snapshots, pictures, videos, notes, Foursquare locations, browser activity, Google map coordinates, Safari bookmars, and Safari history.The artifacts that were able to be extracted from an Android device were: Dropbox, Instagram, Twitter, SMS, and Gmail. Interestingly enough, IEF carved data even after the phone had been factory reset. We are not sure what dictates what data gets saved and what gets deleted when a factory reset is completed.

Not retrieving any data from either popular social networking application (Facebook or Snapchat) on both phones, was disappointing. We expected to find generated data on these applications, but it was interesting still to discover what data could be extracted from other applications.

See Recovered Artifacts

Further Work

A large amount of data was not able to be created on the phones because of their age. We couldn't make outgoing calls or texts and we couldn't revieve calls or texts, as the phones were not activated. We were also

unable to get voicemails because the phones were not activated. Additionally, since the phones were older, they could not be updated to the most recent iOS or Android version. This meant that we could not download or use certain applications, as they were only compatible with the newer versions of the operating systems. This limited the amount of data we could create. Even after the factory reset, we still are able to pull data from previous users. The LCDI uses these phones for different expieriments and research projects, so some of the pictures and text messages in this case were pulled from previous work.

We followed up this research by comparing what IEF Mobile could extract to Cellebrite's internal artifact extracter. See IEF Compared to Cellebrite & Recovered Artifact Examples: Cellebrite for our findings.

Appendix A(iOS)

Time	Action/Variable	User Interface/Software	Comments
	Date:10/17/2013		
10:02am		Factory Reset the iPhone	
10:37am	Activated with iTunes		
10:38 am	Opened App Store	Opened App Store	Asked to join a wifi network. I connected to ChampStudent.
10:39 am	Reopened App Store	Apple Store	
10:42 am	Searched for “whats app”	Apple Store	
10:43 am	Tried to download “WhatsApp Messenger”	Aooke Store	Prompted me to make a new Apple ID Account.
11:04 am	Signed in with the LCDI Apple ID		
11:05 am	Tried to download “Whats App Messenger”	Apple Store	Phone needs to update but won’t connect to itunes.
11:10 am	Downloaded “KiK”	Apple Store	Had to be an older version because the iPhone would not update to the newest version.
10:13 am	Downloaded “SnapChat”	Apple Store	Had to be an older version.
10:15 am	Downloaded “skype”	Apple Store	Had to be an older version.
10:18 am	Downloaded “Facebook”	Apple Store	Had to be an older version.
10:21 am	Downloaded “Instagram”	Apple Store	Had to be an older version.
10:24 am	Downloaded “Foursqaure”	Apple Store	Had to be an older version.
11:27 am	Downloaded “Dropbox”	Apple Store	Had to be an older version.

11:32 am	Tried to downloaded "Google Maps"	Apple Store	Graphics were not up to par and Google maps wouldn't download.
11:33 am	Downloaded "Twitter"	Apple Store	Had to be an older version.
11:44 am	Tried to send a text.		A "No Sim Card" error came up and the text didn't send.
11:47 am	Created a fake Gmail for all the applications that will need an email.		Named it iefforensics@gmail.com Password: **********
11:49 am		Made a KiK account.	
12:05pm	Sent a message to KiK team. "We strike at midnight."		Got a response "I'm smart. Its just random. You would be surprised what I can do at a moments notice."
12:08 pm	Deleted the conversation.	KiK	
12:16 pm	Created a Snapchat account.	Snapchat	
12:16 pm	Opened a snapchat from teamsnapchat.	Snapchat	Picture was just a black screen.
12:18 pm	Sent a snapchat to teamsnapchat.	Snapchat	
12:22 pm	Deleted the snapchat I had from teamsnapchat.	Snapchat	
12:29 pm	Created a Skype Account		
12:30 pm	Logged into Skype on the phone.	Skype	
12:39 pm	Made a Skype test call.	Skype	It lasted 16 seconds.
12:39 pm	Sent a message to "Skype	Skype	

	test call”		
12:45 pm	Deleted the message log.	Skype	
12:45 pm	Tried to call my personal phone with Skype.	Skype	Said I needed Skype credits so the call didn’t go through.
	Date:10/21/2013		
9:15am	Sent a Skype contact request from my personal Skype account to the iPhones.	Skype	
9:16am	Accepted the contact request.	Skype	
9:18am	Sent a Skype IM from the iPhone Skype to my personal Skype.	Skype	Sent “Hello”. Did not receive the message.
9:22am	Sent a message to the iPhone from my phone.	Skype	I sent “Hello.” When I sent my message I received the one I got from the iPhone.
9:23am	Sent a message from the iPhone to my phone.	Skype	Sent “Test” and this time my phone got it immediately.
9:27am	Sent a message from my phone to the iPhone	Skype	Sent “1”
9:28am	Sent a message from the iPhone to my phone.	Skype	Sent “2”
9:28am	Sent a message from my phone to the iPhone	Skype	Sent “3”
9:29am	Sent a message from the iPhone to my phone.	Skype	Sent “4”
9:29am	Sent a message from my phone to the iPhone	Skype	Sent “5”

9:31am	Called me phone from the iPhone and let it go without answering.	Skype	
9:34am	Made another call to my phone from the iPhone this time I picked up.	Skype	Call lasted around 13 seconds.
9:35am	Tried calling the iPhone from my phone but it didn't register that I was calling on the iPhone.	Skype	
9:36am	Made another call from my phone to the iPhone and this time it went through and I answered it.	Skype	
9:42am	Went to m.facebook.com/r.php?cid=6628568379 to create an account for Facebook	Facebook	
9:46am	Tried to create a Facebook account but it was not working.	Safari/Facebook	Will try later.
9:47am	Tried to sign-up for an Instagram account on the app but it wouldn't let me because the app is out of date.		
9:50am	Created a foursquare account.	Foursquare	
9:50am	Enabled the app to use		

	"current location"		
9:52am	Checked into The Patrick Leahy Center for Digital Investigation.	Foursquare	Unlocked the "Newbie" badge, got 6 points. Wrote "gathering data for ief mobile forensics" in the description
9:55am	Allowed Twitter to use my "currant location."	Twitter	
9:56am	Created a Twitter account.	Twitter	
10:10am	Followed Barak Obama	Twitter	@BarakObama
10:11am	Followed Kevin Heart	Twitter	@KevinHart4real
10:11am	Followed Twitter	Twitter	@twitter
10:12am	Followed CNN Breaking News	Twitter	@cnnbrk
10:22am	Retweeted one of CNN Breaking News' tweets.	Twitter	The tweet was "NSA spied on 70 million calls made in France during 30-day period, French newspaper says, citing Snowden documents on.cnn.com/1iSQQq"
10:24am	Favorited the same tweet as stated above.	Twitter	
10:25am	Retweeted one of Kevin Heart's tweets.	Twitter	The tweet was "I had a great time last night until I got the DAMN BILL!!! #AllOfMyFriendsPutTheirHeadsDown…unstagram.com/p/fqybdCYg-/"
10:26am	Viewed the Instagram picture that was in the Kevin Heart tweet.	Twitter	The Picture did not load but the comments did.
10:36am	Replied to Kevin Heart's tweet.	Twitter	Said, "That's insane!"
10:37am	Sent a tweet.	Twitter	Said, "Gathering data for use with Ief mobile

			forensics”
10:38am	Deleted the tweet that I sent.	Twitter	
10:39am	Sent a tweet.	Twitter	Said, “Gathering data for use with IEF Mobile Forensics! #work
10:46am	Followed NASA	Twitter	@NASA
10:51am	Created a DropBox account	DropBox	
10:53am	Let DropBox use my “current location”	DropBox	
10:57am	Took a picture of the LCDI wallpaper.	Camera	
10:58am	Took a picture of my watch.	Camera	
10:58am	Took a picture of the desktop computer.	Camera	
10:59am	Uploaded all three of the photos to the DropBox.	DropBox	
11:00am	Deleted the photo of my watch and the desktop computer.	Camera	
11:01am	Uploaded copies of the picture of the watch and the picture of the desktop.	DropBox	
11:01am	It also downloaded the pictures back to the phone.		
11:04am	Tried to upload a photo to the Twitter from DropBox but it did not work.	DropBox	

11:12am	Tweeted a picture of the LCDI wallpaper.	Twitter	Had the text “Desktop wallpaper” with it.
11:27am	Tried again to send a Snapchat to the iPhone from my phone but it didn’t go through.	Snapchat	
11:30am	Signed into Facebook.	Facebook	
11:43am	Allowed Facebook to use the “current location’	Facebook	
11:45am	Posted a status	Facebook	Said “Gathering data for ief mobile forensics”
11:49am	Deleted the post	Facebook	
11:50am	Posted a status and tagged that I was at the LCDI	Facebook	Said “Gathering data for IEF Mobile Forensics” I geotagged The Senator Patrick Leahy Center for Digital Investigation (LCDI)
11:52am	Liked my own status	Facebook	
11:54am	Commented on my status	Facebook	Said “comment”
11:55am	Edited the comment	Facebook	Changed it to “test”
11:55am	Wrote another comment on the status	Facebook	Said “deleted comment”
11:56am	Deleted the second comment	Facebook	I deleted the comment that said “deleted comment”
12:04pm	Posted the picture of the LCDI wallpaper	Facebook	With the text “wallpaper”
12:06pm	Posted the picture of the desktop computer and tagged the LCDI location	Facebook	Had the text “should be deleted” and I geotagged The Senator Patrick Leahy Center for Digital Investigation (LCDI)
12:07pm	Deleted the picture of the	Facebook	

	desktop computer.		
12:15pm	Accidently sent a friend request to Scott Barrette.	Facebook	
12:16pm	Canceled the request.	Facebook	
12:17pm	Sent a friend request to myself.	Facebook	
12:17pm	I accepted the friend request on my personal account	Facebook	
12:24pm	Linked the iPhone's Snapchat with Facebook.	Facebook	
12:29pm	Sent a Facebook message from the iPhone to my phone.	Facebook	Said "Hello"
12:30pm	Sent a Facebook message from my phone to the iPhone.	Facebook	Said "Hello"
12:31pm	Sent a Facebook message from the iPhone to my phone.	Facebook	Said "1"
12:32pm	Sent a Facebook message from my phone to the iPhone.	Facebook	Said "2"
12:32pm	Sent a Facebook message from the iPhone to my phone.	Facebook	Said "3"
12:33pm	Sent a Facebook message from my phone to the	Facebook	Said "4"

	iPhone.		
12:33pm	Sent a Facebook message from the iPhone to my phone.	Facebook	Said “5”
12:34pm	Deleted the Facebook conversation.	Facebook	
12:36pm	Made a note.	Note	Said “This note will be kept”
12:37pm	Made a note.	Note	Said “This note will be deleted”
12:38pm	Deleted the second note.	Note	Deleted the note that said “This note will be deleted”
12:39pm	Opened Maps	Maps	
12:40pm	Got driving directions from the Lcdi to 24 Winooski Falls Way	Maps	
12:41pm	Cleared the Directions	Maps	
12:43pm	Opened the Mail app	Maps	
12:44pm	Connected the iefforensics email to the app	Email	
12:44pm	The app downloaded the emails that were on the account.	Email	
12:45pm	Viewed all the emails.	Email	There were 11 emails that I opened.
12:46pm	Deleted the DropBox email.	Email	Only one I deleted.
	Date:10/24/2013		
10:03am	Opened Safari	Safari	“m.facebook.com%2Fr.php&_rdr” Was loaded.
10:05am	When to Google.	Safari	“www.google.com/”

10:06am	Searched “ief mobile forensics”	Safari	
10:06am	Clicked on a link.		Brought me to “www.magnetforensics.com/software/internet-evidence-finder/ief-advanced”
10:08am	When back to Google.	Safari	“www.google.com”
10:12am	Went to Google images.	Safari	www.google.com/imghp?tbm=isch
10:12am	Searched “iphone 3gs”	Safari	
10:13am	Clicked on a picture	Safari	Went to the full image. “www.technobuffalo.com/wp-content/uploads/2012/07/iphone-3gs.jpeg”
10:16am	Went back to Google.	Safari	“www.google.com”
10:48am	Opened the App Store.		
10:49am	Searched for Google Maps.		
10:50am	Tried to download Google Maps again because I forgot that It was able to download due to out of date graphics capability.		

Appendix B(Android)

Time	Action / Variable	User Interface / Software	Comments
	Date: 10/7/13		
1:17pm	Opened Google Play	Google Play	After making a google account(on computer) tryed to log into Google Play using this account
1:19pm	Signed Into Google Account		Kept loosing wifi, so took longer than it should have “No Connection. Couldn’t connect to the server.”
1:24pm	Connecting to email, through made gmail account		“Setup could not finish Cannot safely connect to serve. (Read error: ssl=0x302a88: I/O error during system call, Connection timed out.”
1:31pm	Downloaded Twitter	Twitter	Using Gmail Account, to access twitter *Wifi keeps disconnecting*
1:33pm	Send text message (SMS) *Hello*		Sent text to my own number, trying to connect and send, never sent
	Date: 10/9/13		
10:11am	Opened Camera and took pictures	Camera	
10:12am	Opened email, set account	Email	Messages from account already on the phone
10:16am	Installed WhatsApp Messenger	WhatsApp through Google Play	
10:18am	Installed KIK messenger	KIK Messenger	

		through Google Play	
10:20am	Installed Snapchat	Snapchat through Google Play	
10:30am	Opened Google Maps and searched “Champlain College Bookstore”	Google Maps	
10:33am	Installed Skype	Skype through Google Play	
10:36am	Facebook Already Installed	Facebook through Google Play	
10:38am	Installed Instagram	Instagram through Google Play	
10:40am	Installed foursquare	Foursquare through Google Play	
10:42am	Installed Dropbox	Dropbox through Google Play	
10:50am	Registered for Instagram	Instagram	Followed ‘Instagram’ Liked ‘Instagram’s’ balloon photo Took photo and posted it with title “Keyboard”
10:56am	Registered for Facebook	Facebook	Opened app and logged in Updated a status “Hello Facebook”

10:57am	Opened Email to confirm Facebook	Email	Confirmed Facebook account and was directed to “facebook.com”
11:04am	Opened Twitter and made an account	Twitter	Followed “Oprah Winfrey” & “Drizzy” (Drake) Generated tweet “Hello Twitter”
11:09am	Opened KiK and made an account	Kik	Sent message to Kik Team “Hello Kik” Got message back saying “I was standing in the park wondering why frisbees got bigger as they get closer. Then it hit me.”
11:14am	Opened Dropbox and registered	Dropbox	Opened “Getting Started” Allowed access to camera and downloaded pictures from gallery. Whole phone vibrated for a bit.
11:24am	Opened Foursquare & registered	Foursquare	Connected and ‘signed in’ to Lakeside and wrote “Hello” Unlocked “Newbie Badge” and “Mobile Badge”
11:28am	Opened Skype and registered	Skype	Got black screen
11:30am	Opened Snapchat and made account	Snapchat	Opened snap from ‘Team Snapchat’ took photo and sent to “Team Snapchat”
11:34am	Opened Talk	Talk	Set status as Hello
11:35am	Opened Contaccts	Contacts	Saved Personal Number in the phone Called through Skype, didn’t go through sent message through messaging, didn’t go through
	Date: 10/16/13		
10:33am	Opened Email	Email	Checked emails , verified foursquare. Directed to

			https://foursquare.com/login?continue=lcdi.10.2013%40gmail.com Wrote in password
10:38am	Opened Instagram, liked "Instagram"s photo from 2 days ago	Instagram	Added a picture in Instagram, then immediately deleted it.
10:41am	Opened Twitter, followed "@DrakeKnowledge"	Twitter	Retweeted @DrakeKnowledge "You are never too old for a Disney Movie"
10:43am	Made a tweet, then deleted it "Good Morning"	Twitter	Deleted tweet
10:45am	Opened Snapchat	Snapchat	Resent Snapchat from last week, never sent
	Date: 10/23/13		
10:54am	Opened Twitter	Twitter	Made tweet "Hi" "failed to send"

References

Magnet Forensics Inc. (2013). *Internet Evidence Finder*. Retrieved October 07 2013, from Magnet Forensics: http://www.magnetforensics.com/software/internet-evidence-finder/