“Android Forensics: Simplifying Cell Phone Examinations”

Jeff Lessard, Gary Kessler 2010

Presented By: Manaf Bin Yahya
Outlines

- Introduction
- Mobile Forensics
- Physical analysis
- Logical analysis
- CelleBrite Device (UFED)
- Summary of Results
- Conclusion
Introduction

Mobile Phone → Smart phone

- Not just for phone calls.
- Fully functioning computers capable of accessing and storing.
Smart phone users

- Number of Smartphones Around the World
  Top 1 Billion -- Projected to Double by 2015

- 1.038 billion, to be exact. It’s taken 16 years to pass 1 billion.
Smart phone users

Mobile phone subscribers per 100 inhabitants 1997-2007

- Developed
- Developing
- World
Android users

- According to informationweek.com, there were **300 million Android devices** in use as of February 28, 2012
- According to the International Data Corporation (IDC)
Android

• an **open-sourced** operating system (OS) whose growth has thrived due to its customization.
• Android’s developer, Google, allows manufacturers access to the Android source code to customize as they please.
• The very first beta released on Nov. 2007, but never saw the light until Sep. 2008.
• Android is not limited to smartphones. Other devices include tablets, netbooks, car navigation and TVs.
Open Handset Alliance (OHA)
Criminals

- committing fraud over e-mail
- harassment through text messages
- trafficking of child pornography
- communications related to narcotics
- etc...
valuable probative information

- Call history
- Contact List
- text message data
- e-mail
- Browser history
- chat logs
- Images and Videos
- etc ...
Smart phone Difficulties

• general lack of hardware, software, and/or interface **standardization** within the industry (Storage media, operating system and the effectiveness of certain tools).

• different model cell phones of same manufacture may require different approach.
Mobile Forensics

There are six main steps in a Mobile Forensic Procedure:
1) Consultancy (Discussing and Understanding).
2) Data Preservation.
3) Data Collection (Forensic Examination).
4) Data Recovery (Carving).
5) Computer Forensic Analysis.
6) Expert Reports & Testimony.
Consultancy (Android Architecture)
Android Architecture

- Linux Version 2.6.x for core system services (C Language)
Similar to Sun’s **Java Runtime** Environment, streamlined to suit constrained resources.

It hides the underlying Linux complexities using core libraries written in Java.

Provides a powerful SDK which enables handling different devices configurations seamlessly.
Android Architecture

- Android Application runs in its own process, with its own instance of the Dalvik VM.
- Security is permissions-based and attached at the process level by assigning user and group identifiers to the applications.
Android Architecture

Libraries:
- Surface Manager
- OpenGL | ES
- SGL
- Media Framework
- FreeType
- SSL
- SQLite
- WebKit
- libc
Android Architecture

- No limited application
- Equality of each app.
- Parallel running
Two main types of memory:
• Random-Access Memory (RAM)
• Flash Memory (operating system and user data)

Files can be stored on:
• Device storage
• Removable secure digital (SD) memory card
Data Preservation

• RAM on a mobile phone is volatile (plug a device in to allow it to charge)
• disable network Communications (attacker has the ability to wipe a device Remotely).
• Faraday bag tool
Data Examination

Collecting from:
- Device storage
- Removable SD card

- Physical Examination
- Logical Examination
Rooting

• to gain access to the root directory (/) and having the appropriate permissions to take root actions.

• It allows an owner full control to read, modify, and write data to their device.

• needs to have a third party program installed on the device in order to get root permissions.

• If it is not possible to root a device (less efficient Examination)
Rooting

• Set the Phone to USB Debugging Mode
• insert a fresh SD card in the phone
• set up the Android Development Tools (ADT) on the host
• In the Windows command line, move to the Android SDK folder, navigate to the tools subfolder
Rooting

- Run the Android development bridge (ADB) devices command.
- The method to obtain root is specific to each phone and OS **variant**

```bash
> adb push asroot2 /data/local/
> adb shell chmod 0755 /data/local/asroot2
> adb shell
$ /data/local/asroot2 /system/bin/sh
# mount -o remount,rw -t yaffs2 /dev/block/mtdblock3 /system
# cd /system/bin
# cat sh>su
# chmod 4755 su
```
Paper’s Three Approach

- Physical analysis with FTK on dd Image.
- Logical analysis of specific databases.
- CelleBrite Device (UFED)

“Sprint HTC Hero”
Acquiring Physical Image

- Connecting the device via a data cable
- Setting the Phone to ‘Mount as a Disk Drive’ Mode
- Use write blocker to ensure the integrity of the data
- AccessData’s FTK Imager
AccessData’s FTK Imager

- Create New Disk Image
- Select ‘Physical Drive’ as Source Type
- Source Drive Selection
AccessData’s FTK Imager

- Select **image type**
- Enter Evidence item information
- Selecting the image destination
- **Creating** the disk image
## FTK Imager image summary screen

<table>
<thead>
<tr>
<th>Section</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>sdcard2.001</td>
</tr>
<tr>
<td>Sector count</td>
<td>15949824</td>
</tr>
<tr>
<td><strong>MD5 Hash</strong></td>
<td></td>
</tr>
<tr>
<td>Computed hash</td>
<td>e3cbc7b88bc00cbc30227c528f31ade2</td>
</tr>
<tr>
<td>Report Hash</td>
<td>e3cbc7b88bc00cbc30227c528f31ade2</td>
</tr>
<tr>
<td>Verify result</td>
<td>Match</td>
</tr>
<tr>
<td><strong>SHA1 Hash</strong></td>
<td></td>
</tr>
<tr>
<td>Computed hash</td>
<td>6c86800c1841e4a0aa80d1783248660d7ff06594</td>
</tr>
<tr>
<td>Report Hash</td>
<td>6c86800c1841e4a0aa80d1783248660d7ff06594</td>
</tr>
<tr>
<td>Verify result</td>
<td>Match</td>
</tr>
</tbody>
</table>
Another Approach

there are six files of interest located in /dev/mtd/ (flash):

- mtd0 → handles miscellaneous tasks
- mtd1 → holds a recovery image
- mtd2 → contains the boot partition
- mtd3 → contains system files
  - mtd4 → holds cache
- mtd5 → holds user data
Another Approach

- Navigate to the AndroidSDK\tools directory,
- Execute the ADB shell command
- Enter the /data/local/asroot2 /system/bin/sh instruction.
- Now dd command can be used to image the memory files, using the command:

```
dd if=/dev/mtd/mtd0 of=/sdcard/mtd0.dd bs=1024
```
After data carving:
• 207 (HTML), and (PDF) documents
• 12,709 (BMP), (GIF), (JPEG), and (PNG) Images
Recovered documents

- Most of the recovered documents were not of a real evidentiary value.
- only four files were complete snapshots of Web pages
Recovered documents

the single recovered PDF file (2 MB)
• phone book information
• Facebook status updates
• **Google search history**
• YouTube videos visited
• music played from the SD card
• text messages
• browser history
Recovered images

**mtd3.dd**
- file contained images for different applications.
- Backgrounds for a labyrinth style game;
- Images for bookmarks, weather, alarm clocks, and widgets;
- grids for Sudoku games;
- icons

**mtd5.dd**
- contact photos
- Downloads from browser Web pages
- pictures taken with the Hero's camera
- cover art from Pandora
- image previews of videos from SprintTV and YouTube
- icons from applications
Recovered images

`mtd4.dd` file contains contents of the Android cache (e-mails).
Searching (Search Tool)

- Quite powerful but in order to use it, an examiner needs to have an idea of what to search for.

- Search for j.lessard802@gmail.com, for example, yielded 1628 hits over 92 files.

```
j.lessard802@gmail.com  >.67 à..67c$Ryan and Ysa I quite impressed with the talk they gave our class. Maybe impre....Ryan and Ysa<br><br>I quite impressed with the talk they gave our class. Maybe impressed isn't quite the right word for it - perhaps amazed they let everyone in to their life like that. I never really thought about the difficulty of communicating across cultures and how it would impact a relationship. Specifically if they didn't speak each other's language. I guess the international language is truly dance.<br>
```
Searching (Search Tool)

- Android browser stores passwords in plaintext right next to a username and (URL).
Logical Examination

• Same initial steps of Physical Examination
• Physical Examination:
  • Access deleted Information
  • Difficult to recover fragmented data
  • Difficult to read results
Logical Examination Results

• Contents of the /data/data directory.
• “154 subdirectories were found”
Logical Examination Results

- /data/data/com.htc.htctwitter/databases/htc_hrip.db
- 1460 Twitter updates were found
Logical Examination Results

• /data/data/com.android.browser/databases/browser.db
• Usernames, URLs, plaintext passwords, data typed into forms, web browser history and search history

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>237</td>
<td>237</td>
<td>where the wild partie</td>
<td>1259461432984</td>
</tr>
<tr>
<td>238</td>
<td>238</td>
<td>pulp fiction soundtrack</td>
<td>1259465046279</td>
</tr>
<tr>
<td>239</td>
<td>239</td>
<td>ball and chain lyrics</td>
<td>1259469379237</td>
</tr>
<tr>
<td>240</td>
<td>240</td>
<td>sublime scarlet bego</td>
<td>1259469890406</td>
</tr>
<tr>
<td>241</td>
<td>241</td>
<td>party hard lyrics</td>
<td>1259472218623</td>
</tr>
</tbody>
</table>
Logical Examination Results

- `/data/data/com.android.browser/gears/geolocation.db`, (the last known location as reported by the GPS satellites)
- `/data/data/com.google.android.apps.maps/database/search_history.db`, *(all searches entered into the Google maps)*

<table>
<thead>
<tr>
<th>_id</th>
<th>data1</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>camp heartland ny</td>
</tr>
<tr>
<td>10</td>
<td>west milford</td>
</tr>
<tr>
<td>11</td>
<td>loc: north st at lafour</td>
</tr>
<tr>
<td>12</td>
<td>23 hazen drive</td>
</tr>
<tr>
<td>13</td>
<td>44.477128,-73.1986</td>
</tr>
</tbody>
</table>
Logical Examination Results

- /data/data/com.android.providers.telephony/databases/
- (mmssms.db) database contains the MMS and SMS messages

<table>
<thead>
<tr>
<th>person</th>
<th>date</th>
<th>protocol</th>
<th>read</th>
<th>status</th>
<th>type</th>
<th>reply</th>
<th>suil</th>
<th>body</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>1255386664946</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>2</td>
<td></td>
<td></td>
<td>Well I have to be at both</td>
</tr>
<tr>
<td>24</td>
<td>1255386710649</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td></td>
<td>Ok i will see what i am doing</td>
</tr>
<tr>
<td>24</td>
<td>1255386765399</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>2</td>
<td></td>
<td></td>
<td>Cool. Thanks!</td>
</tr>
<tr>
<td>58</td>
<td>1255438621715</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>2</td>
<td></td>
<td></td>
<td>Btw. I found your soap a</td>
</tr>
<tr>
<td>30</td>
<td>1255447130041</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>0</td>
<td></td>
<td>Anciello:</td>
</tr>
</tbody>
</table>
Logical Examination Results

/data/data/com.google.android.providers.gmail/databases (accessing Gmail via the application)

<table>
<thead>
<tr>
<th></th>
<th>fromAddress</th>
<th>toAddress</th>
<th>ccAddress</th>
<th>bccAddress</th>
<th>replyTo</th>
<th>dateSentUtc</th>
<th>dateReceivedUtc</th>
<th>subject</th>
<th>snippet</th>
<th>listName</th>
<th>messageID</th>
<th>body</th>
<th>bodyLength</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>&quot;Jeff Lessard&quot; @gmail.com, &quot;Jeff&quot; @lessard.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td></td>
<td></td>
<td>1253792250000</td>
<td>1253792251136</td>
<td><a href="http://www.sjol.com">http://www.sjol.com</a></td>
<td>2</td>
<td>&quot;<a href="http://www.sjol.com">http://www.sjol.com</a>&quot;</td>
<td></td>
<td></td>
<td>0.1k</td>
</tr>
<tr>
<td>2</td>
<td>&quot;Jeff Lessard&quot; @gmail.com, &quot;Jeff&quot; @lessard.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td></td>
<td></td>
<td>1253760399000</td>
<td>1253760399082</td>
<td></td>
<td>0</td>
<td>&quot;[email protected]&quot;</td>
<td></td>
<td></td>
<td>0.1k</td>
</tr>
<tr>
<td>3</td>
<td>&quot;Jeff Lessard&quot; @gmail.com, &quot;Jeff&quot; @lessard.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td></td>
<td></td>
<td>1253665558000</td>
<td>1253665558023</td>
<td>Annotated Bib</td>
<td>2</td>
<td>&quot;Possible topics:&quot;</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>&quot;Jeff Lessard&quot; @gmail.com, &quot;Jeff&quot; @lessard.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td></td>
<td></td>
<td>1253651918000</td>
<td>1253651918035</td>
<td></td>
<td>2</td>
<td>&quot;[email protected]&quot;</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>&quot;Jeff Lessard&quot; @gmail.com, &quot;Jeff&quot; @lessard.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td></td>
<td></td>
<td>1253561905000</td>
<td>125365190542</td>
<td></td>
<td>2</td>
<td>&quot;[email protected]&quot;</td>
<td></td>
<td></td>
<td>0.1L</td>
</tr>
<tr>
<td>6</td>
<td>&quot;Jeff Lessard&quot; @gmail.com, &quot;Jeff&quot; @lessard.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td></td>
<td></td>
<td>1253564950000</td>
<td>12536495052</td>
<td>Re: bib</td>
<td>2</td>
<td>&quot;[email protected]&quot;</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>&quot;Jeff Lessard&quot; @gmail.com, &quot;Gray C. Kestle&quot; @graykester.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td>&quot;Jeff Lessard&quot; @gmail.com</td>
<td></td>
<td></td>
<td>1253569442000</td>
<td>1253656042873</td>
<td></td>
<td>0</td>
<td>&quot;[email protected]&quot;</td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>
Logical Examination Results

- `/data/data/com.android.providers.contacts/databases/contacts.db`
- Call history including phone number, date, length (seconds), type of call (1 = incoming, 2 = outgoing, 3 = missed), and name from a phonebook look up, if available

<table>
<thead>
<tr>
<th>date</th>
<th>duration</th>
<th>type</th>
<th>new</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>802</td>
<td>1259863545274</td>
<td>180</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>7184</td>
<td>1259867306816</td>
<td>11</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1-8454</td>
<td>1259888256724</td>
<td>19</td>
<td>2</td>
<td>1 Mike Anc</td>
</tr>
<tr>
<td>2-8367</td>
<td>1259894559824</td>
<td>18</td>
<td>2</td>
<td>1 Kathleen</td>
</tr>
<tr>
<td>3478</td>
<td>1259894632167</td>
<td>0</td>
<td>3</td>
<td>0 Kristen W</td>
</tr>
<tr>
<td>7-1658</td>
<td>1259899516646</td>
<td>5</td>
<td>2</td>
<td>1 Shannon</td>
</tr>
<tr>
<td>7184</td>
<td>1259939617232</td>
<td>38</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5382</td>
<td>1259962242105</td>
<td>72</td>
<td>1</td>
<td>1 Simi Max</td>
</tr>
</tbody>
</table>
Logical Examination Results

contacts.db
- contact names
- number of times contacted
- the time of the most recent contact
- contact photo file (if used)
- custom ringtone (if used)
- last time the contact information was updated
CelleBrite Universal Forensic Extraction Device (UFED)

Standalone hardware device that is designed to pull:
- contact lists
- address books
- pictures, videos, music
- text messages
- call history
- device identifying information.
CelleBrite (UFED)

- **Communicates** with a cell phone via a data cable, infrared (IR), or BlueTooth (BT).
- Can **acquire** data (logically and physically)

- To connect the HTC Hero to the UFED, USB storage and USB debugging both need to be turned on.
CelleBrite (UFED) Results

Phone identifying information from the UFED

<table>
<thead>
<tr>
<th>Selected Manufacturer:</th>
<th>HTC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected Model:</td>
<td>HTC Hero CDMA (Android)</td>
</tr>
<tr>
<td>Detected Manufacturer:</td>
<td>sprint</td>
</tr>
<tr>
<td>Detected Model:</td>
<td>HERO200</td>
</tr>
<tr>
<td>Revision:</td>
<td>1.5 CUPCAKE eng.u70000.20090921.205629</td>
</tr>
<tr>
<td>MEID:</td>
<td>260113178313016459 (HEX: A1000007C69D8B)</td>
</tr>
<tr>
<td>IMSI:</td>
<td>310006032060645</td>
</tr>
<tr>
<td>Extraction start date/time:</td>
<td>11/06/09 16:39:45</td>
</tr>
<tr>
<td>Extraction end date/time:</td>
<td>11/06/09 16:51:23</td>
</tr>
<tr>
<td>Phone Date/Time:</td>
<td>11/06/09 20:38:51 (GMT)</td>
</tr>
<tr>
<td>Connection Type:</td>
<td>USB Cable</td>
</tr>
<tr>
<td>UFED Version:</td>
<td>Software: 1.1.2.4 UFED, Full Image: 1.0.2.4, Tiny Image: 1.0.2.1</td>
</tr>
<tr>
<td>UFED S/N:</td>
<td>5518965</td>
</tr>
</tbody>
</table>
CelleBrite (UFED)

- **1070 SMS messages**, 56 contacts, 107 incoming calls, 192 outgoing calls, 49 missed calls, 69 pictures, and one video.
- each category 100% correctly
CelleBrite (UFED)
Summary of Results

dd analysis with FTK

- **Pros:**
  - Found deleted text messages and contacts
  - Found passwords with relative ease.

- **Cons:**
  - Required root access
  - Results extremely fragmented
  - Countless hours would have to be spent to try to locate and piece everything together
Summary of Results

Logical analysis of specific databases

- **Pros:**
  - Recovered virtually everything (call history, Web and search history, pictures, MMS/SMS messages, e-mail data with complete messages, and even GPS data, voice mail and passwords).

- **Cons:**
  - Required root access
  - did not find all deleted data.
Data extraction with the CelleBrite UFED

**Pros:**

- Recovered MMS/SMS messages, call logs, photos, video, and contact information.
- Simple stand-alone method.

**Cons:**

- Logical extraction only (for HTC Hero)
- did not recover e-mails, browser, or search history.
Conclusion

- Cell phones are becoming even more sophisticated and able.
- Android forensics is still in its infancy, steps are being made to meet the new technology.
- the standardization will make mobile forensics simpler in the long run

- **Future Work:**
  - learning about new operating systems and developing new forensic methods
  - more tools will be adding support as Android (similar to Cellebrite)
THANK YOU!!!