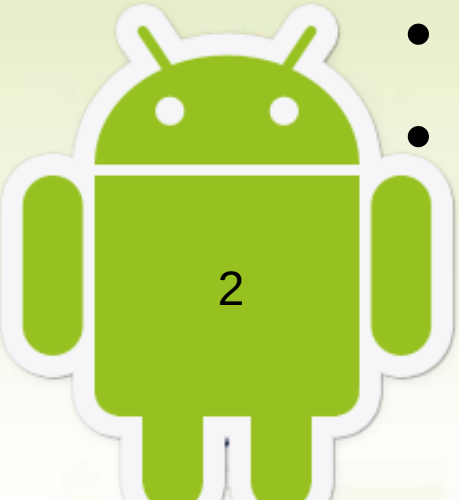
“Android Forensics: Simplifying Cell Phone Examinations”

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

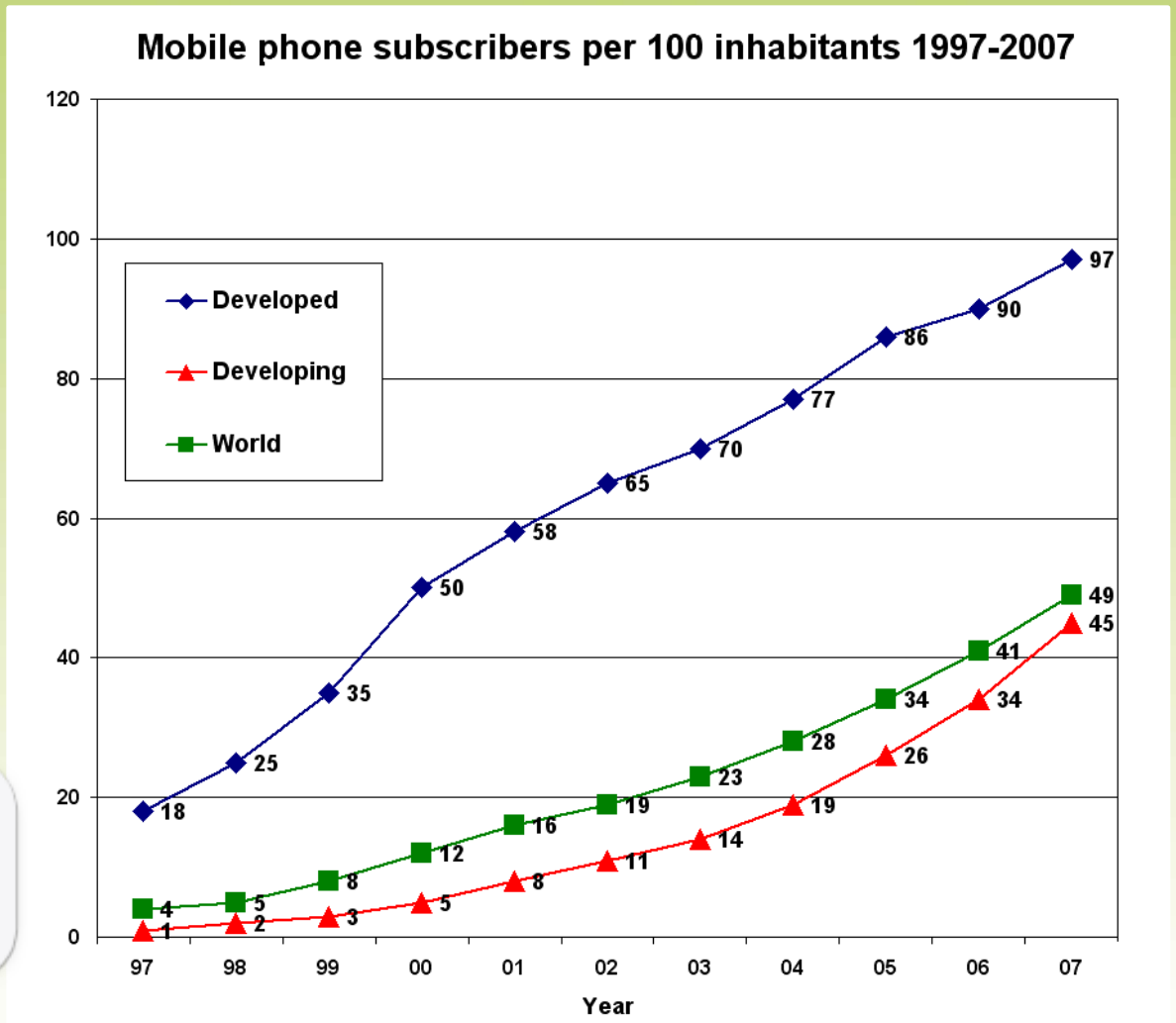
Mobile Phone → Smart phone

- Not just for phone calls.
- fully functioning computers capable of accessing and storing .

Smart phone users

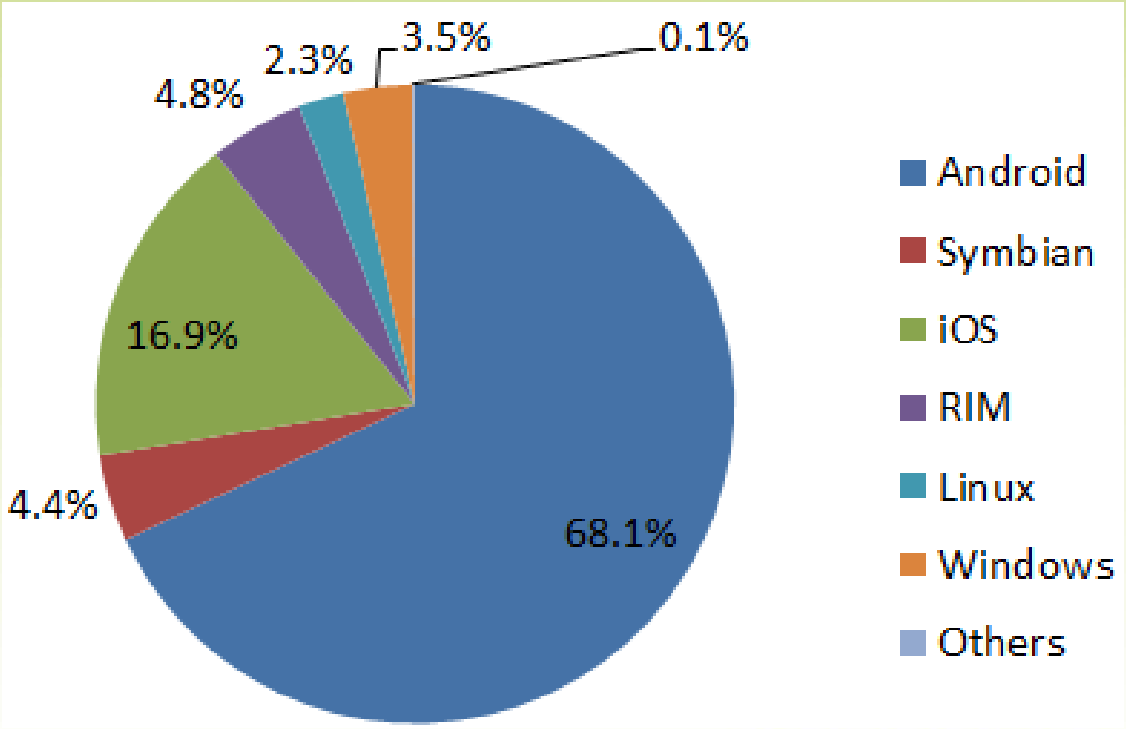
- Number of Smartphones Around the World Top 1 Billion -- Projected to Double by 2015
- 1.038 billion, to be exact. It’s taken 16 years to pass 1 billion.

Smart phone users



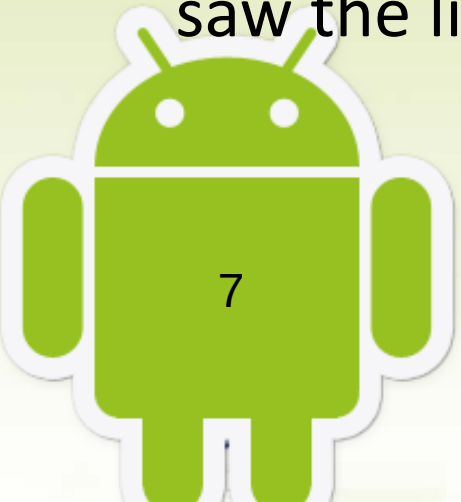
Android users

- 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)

Mobile Operators

中国移动通信 CHINA MOBILE
China unicom 中国联通
KDDI
NTT DoCoMo
Sprint
T-Mobile
vodafone
Telefónica

open handset alliance

Handset Manufacturers

acer
ASUS
GARMIN
htc smart mobility
HUAWEI
lenovo 联想移动
LG Electronics
MOTOROLA
SAMSUNG
Sony Ericsson
TOSHIBA

Semiconductor Companies

AKM
Audience
ARM
intel
ATHEROS
BROADCOM
MIPS TECHNOLOGIES
NVIDIA
ST ERICSSON

Software Companies

Ascender Corporation
ebay
Google
Living Image
myriad
NUANCE
OMRON
pv
SkyPoP

Commercialization Companies

Aplix Corporation
BORQS
noser
tat
TELECA
WIND RIVER

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

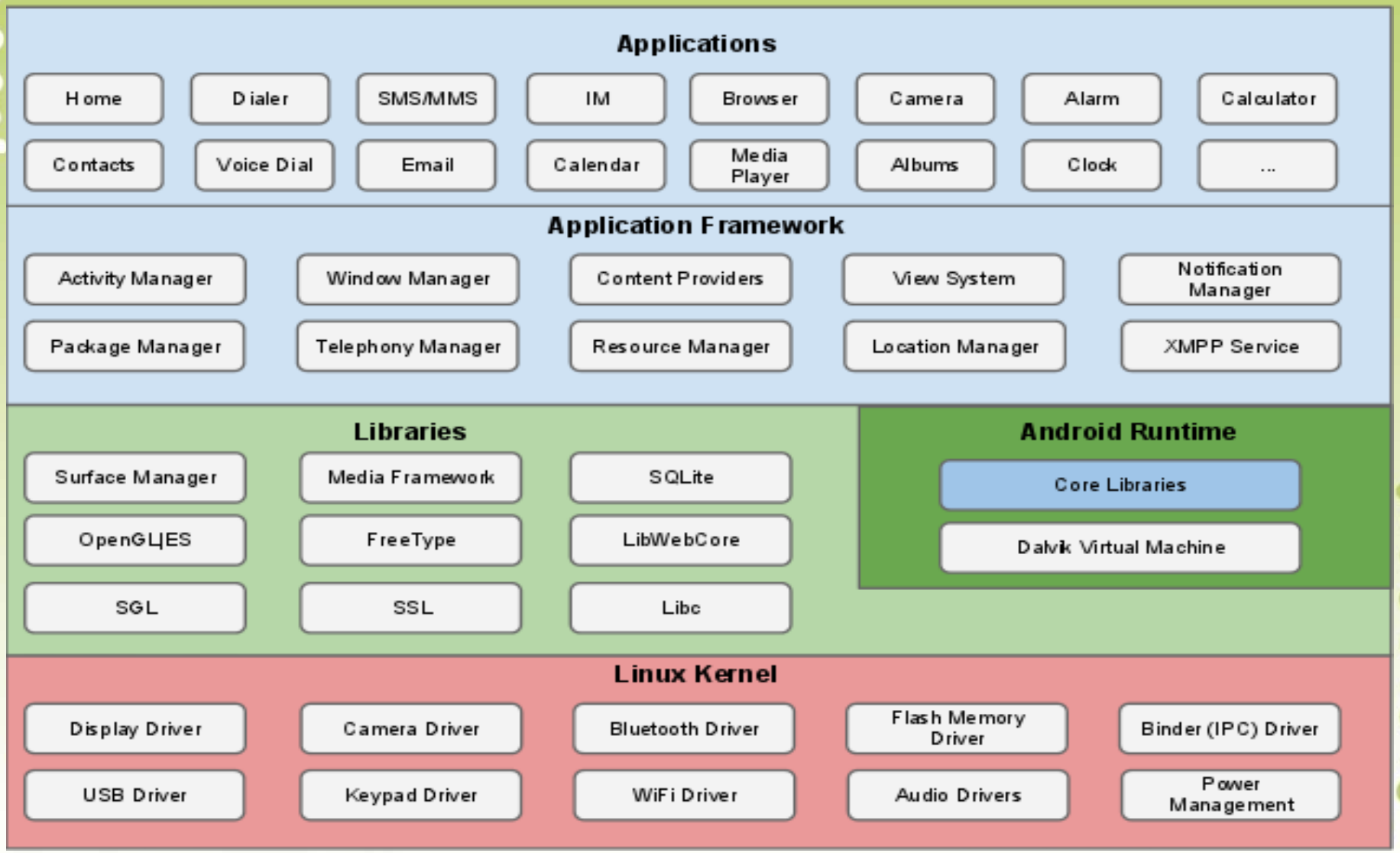
- general lack of hardware, software, and/or interface **standardization** within the industry (Storage media, operating system and the effectiveness of certain tools).
- different model cell phones of same manufacture may require different approach.

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)

Android Architecture

- 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

Android Architecture

- No limited application
- Equality of each apps.
- Parallel running

Android Devices Memory

- 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**

```
> 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)

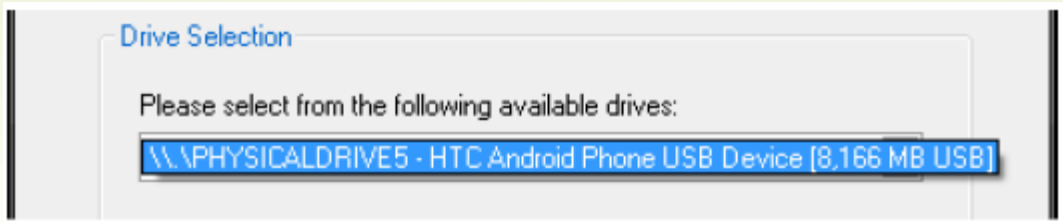
"Sprint HTC Hero"

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

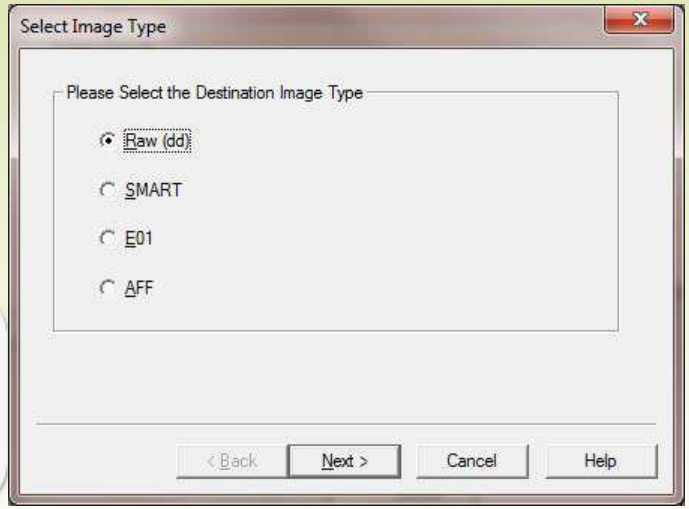
AccessData's FTK Imager

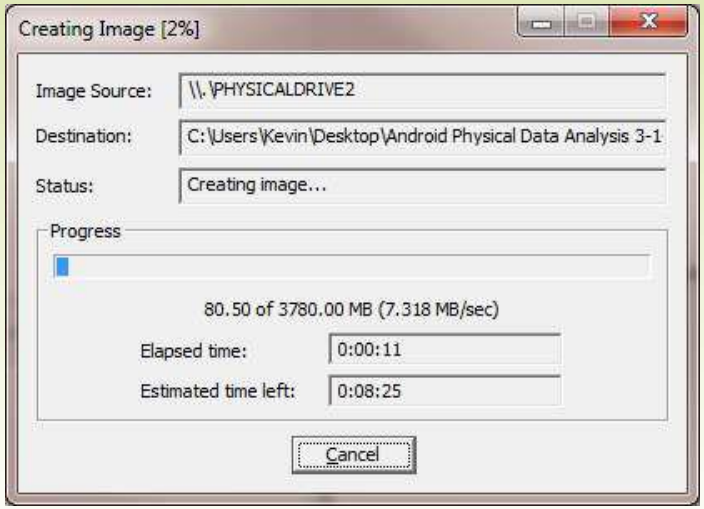
- Create New Disk Image
- Select '**Physical Drive**' as Source Type
- **Source Drive** Selection



AccessData's FTK Imager

- Select **image type**
- Enter Evidence item information
- Selecting the image destination
- **Creating** the disk image

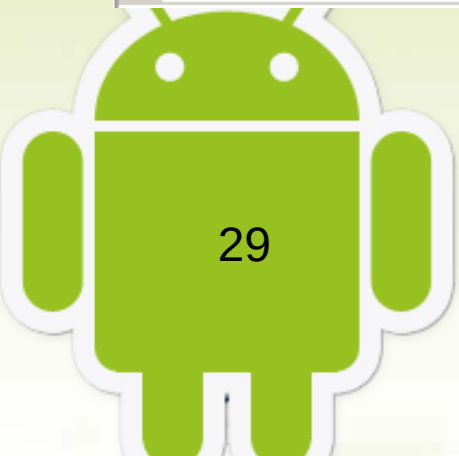




AccessData's FTK Imager

FTK Imager image summary screen

General	
Name	sdcard2.001
Sector count	15949824
MD5 Hash	
Computed hash	e3cbc7b88bc00cbc30227c528f31ade2
Report Hash	e3cbc7b88bc00cbc30227c528f31ade2
Verify result	Match
SHA1 Hash	
Computed hash	6c86800c1841e4a0aa80d1783248660d7ff06594
Report Hash	6c86800c1841e4a0aa80d1783248660d7ff06594
Verify result	Match



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
```

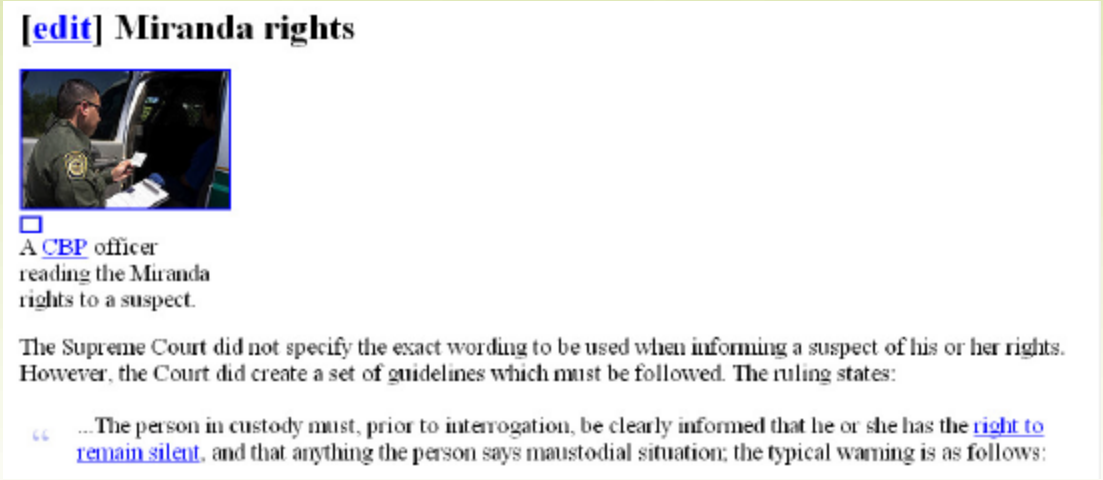
Examination of Memory

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



[edit] Miranda rights

A CBP officer reading the Miranda rights to a suspect.

The Supreme Court did not specify the exact wording to be used when informing a suspect of his or her rights. However, the Court did create a set of guidelines which must be followed. The ruling states:

> ...The person in custody must, prior to interrogation, be clearly informed that he or she has the right to remain silent, and that anything the person says maustodial situation; the typical warning is as follows:

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

amazon external hard drive
ST305004EXA101
runstar
touchscreen gloves amazon
conductive thread
conductive gloves
morgan freeman
samoyed puppies
party hard lyrics
sublime scarlet begonias lyrics
ball and chain lyrics
pulp fiction soundtrack
where the wild parties are woot

Recovered images

mtd3.dd

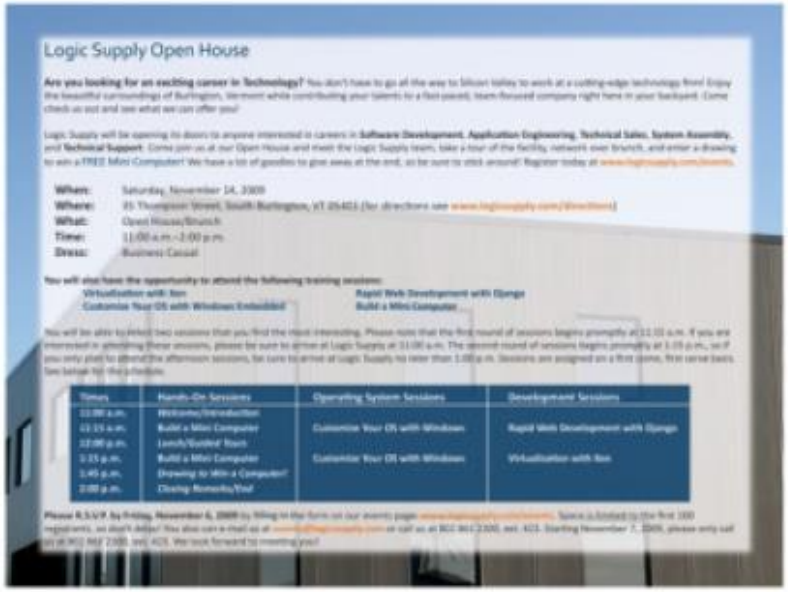
- file contained images for different applications.
- Backgrounds for a labyrinth style game;
- Images for bookmarks, weather, alarm clocks, and widgets;
- grids for Sudoku games;
- icons

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.

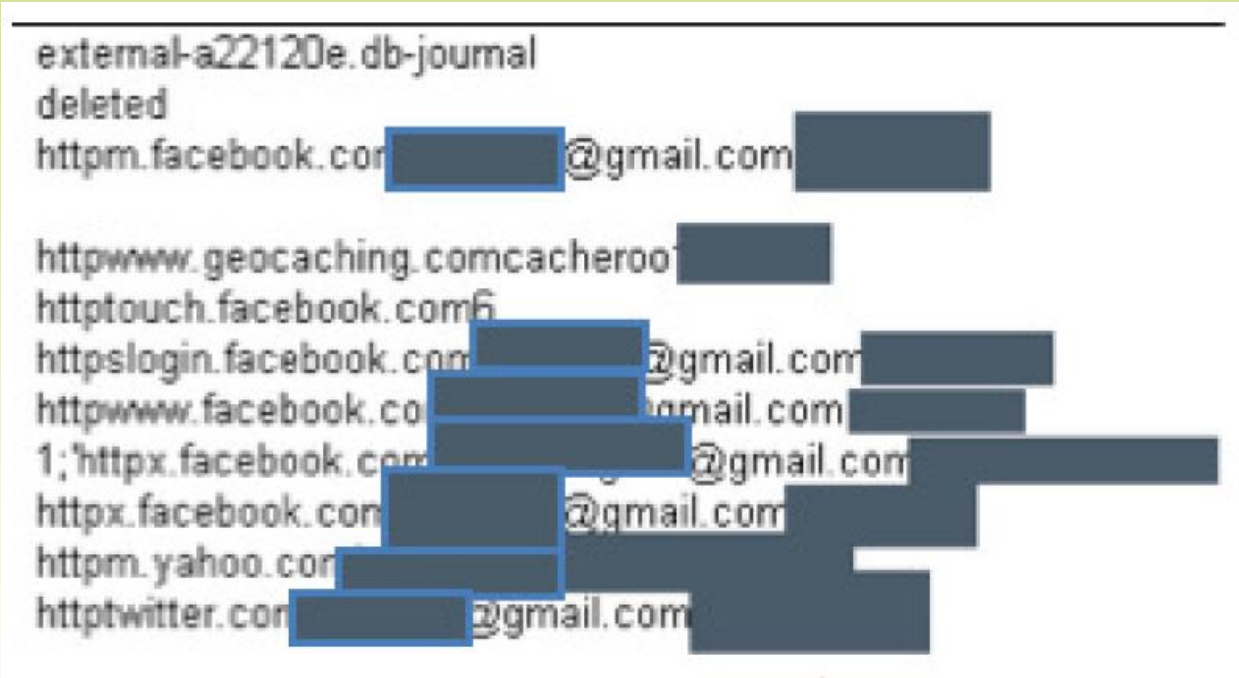
- Search for *j.lessard802@gmail.com*, for example, yielded 1628 hits over 92 files.

j.lessard802@gmail.com >..ö7`à..ö7c$Ryan and Ysa I quite impressed with the talk they gave our class. Maybe impre....Ryan and Ysa

I quite impressed with the talk they gave our class. Maybe impressed isnt 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 didnt speak each others language. I guess the international language is truly dance.

Searching (Search Tool)

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

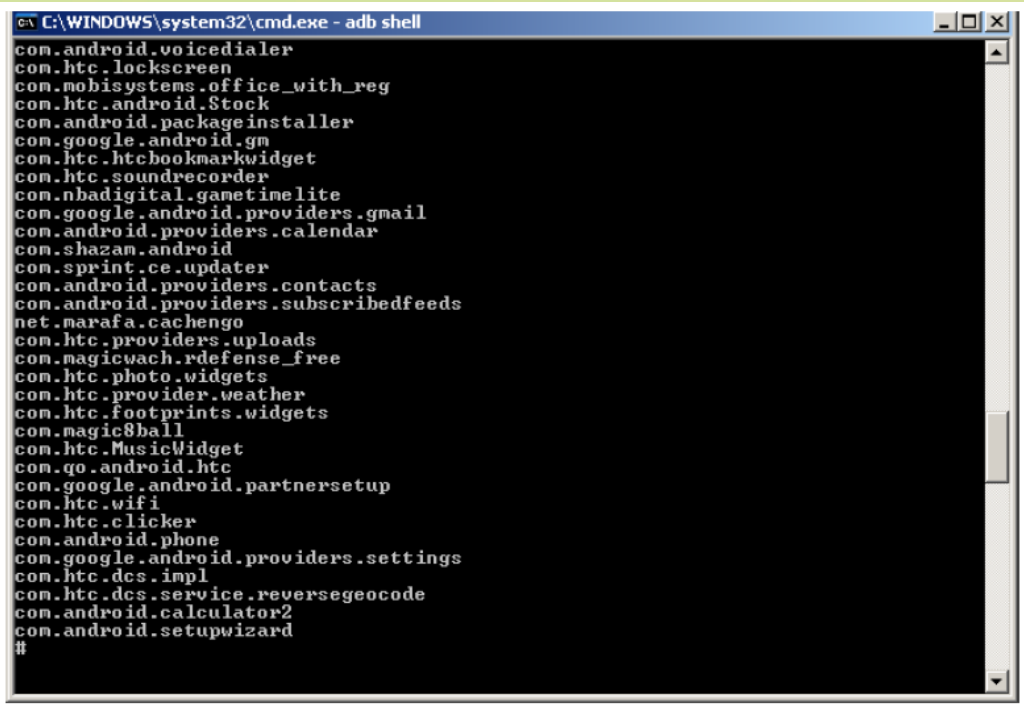


Logical Examination

- 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

	_id	name	screenname	status	location	description	profileimageurl	url	lastupdate	dirty	device_updates
1	14238320	Riva Dumont	rivadumont	@riseetyakker I agree with yo	Burlington	Do it with flair.	http://a3.twimg.com	http://rockthislovela	1256097022	0	0
2	15583056	Michael Therrien	michaeltherrien	Damn. Nice iMac update!!	Phone: 44.370289,		http://a1.twimg.com	http://www.mike-t.c	1256097022	0	0
3	17365011	Megan	gpoety	@zmeltin I was on for quite a t	Burlington, VT	I get really excited o	http://a3.twimg.com	http://www.linkedin.	1256097022	0	0
4	17467682	katmaund	katmaund	Courage ftinspiresme. Packing	Burlington, VT	recent grad, social n	http://a3.twimg.com	http://katmaund.blo	1256097022	0	0
5	19052423	Mat Kittle	mskittle2009	House now7777 Hurry please			http://a3.twimg.com	null	1256097022	0	0

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**

237	237	where the wild partie	1259461432984
238	238	pulp fiction soundtra	1259465046279
239	239	ball and chain lyrics	1259469379237
240	240	sublime scarlet bego	1259469890406
241	241	party hard lyrics	1259472218623

Logical Examination Results

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

Table: suggestions

	_id	data1
1	9	camp heartland ny
2	10	west milford
3	11	loc: north st at lafour
4	12	23 hazen drive
5	13	44.477128,-73.1986

Logical Examination Results

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

	person	date	protocol	read	status	type	reply_	sul	body
24		1255386664946		1	-1	2			Well I have.to be at both
24	10	1255386710649	0	1	-1	1	1		Ok i will see what i am d
24		1255386765399		1	-1	2			Cool. Thanks!
58		1255438621715		1	-1	2			Btw. I found your soap a
30		1255447130041	0	1	-1	1	0		Anciello:

Logical Examination Results

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

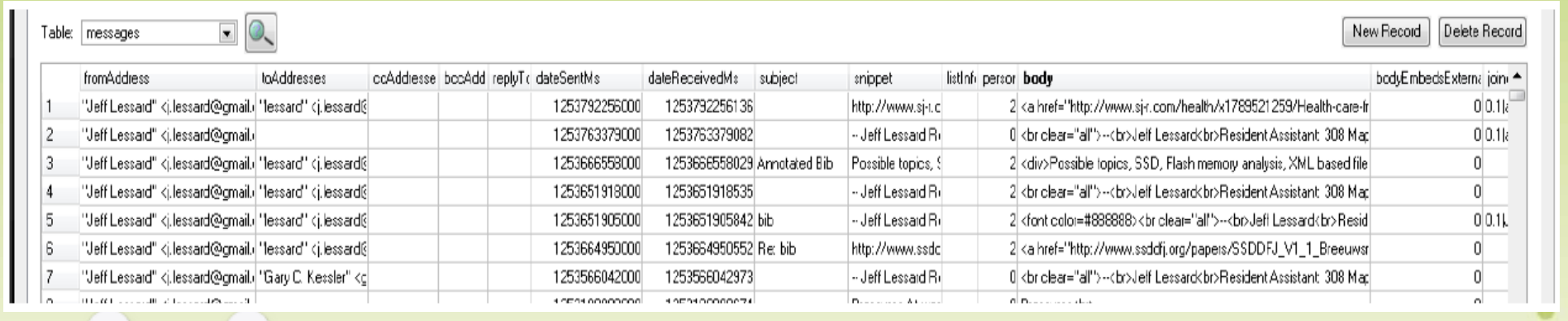


Table: messages

New Record | Delete Record

	fromAddress	toAddresses	ccAddresse	bccAdd	replyT	dateSentMs	dateReceivedMs	subject	snippet	listInf	person	body	bodyEmbedsExterna	join
1	"Jeff Lessard" <j.lessard@gmail.c	"lessard" <j.lessard@				1253792256000	1253792256136		http://www.sj-r.c		2	<a href="http://www.sj-r.com/health/x1769521259/Health-care-fr	0	0,1
2	"Jeff Lessard" <j.lessard@gmail.c					1253763379000	1253763379082		-- Jeff Lessard R		0	<br clear="all">-- Jeff Lessard Resident Assistant 308 Mac	0	0,1
3	"Jeff Lessard" <j.lessard@gmail.c	"lessard" <j.lessard@				1253666558000	1253666558029	Annotated Bib	Possible topics, S		2	Possible topics, SSD, Flash memory analysis, XML based file	0	
4	"Jeff Lessard" <j.lessard@gmail.c	"lessard" <j.lessard@				1253651918000	1253651918535		-- Jeff Lessard R		2	<br clear="all">-- Jeff Lessard Resident Assistant 308 Mac	0	
5	"Jeff Lessard" <j.lessard@gmail.c	"lessard" <j.lessard@				1253651905000	1253651905842	bib	-- Jeff Lessard R		2	<font color=#888888><br clear="all">-- Jeff Lessard Resid	0	0,1
6	"Jeff Lessard" <j.lessard@gmail.c	"lessard" <j.lessard@				1253664950000	1253664950552	Re: bib	http://www.ssdc		2	<a href="http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsr	0	
7	"Jeff Lessard" <j.lessard@gmail.c	"Gary C. Kessler" <g				1253566042000	1253566042973		-- Jeff Lessard R		0	<br clear="all">-- Jeff Lessard Resident Assistant 308 Mac	0	

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

	date	duration	type	new	name
)802	1259863545274	180	1	1	
7184	1259867306816	11	1	1	
I-8454	1259888256724	19	2	1	Mike Anc
2-8367	1259894559824	18	2	1	Kathleen
)478	1259894632167	0	3	0	Kristen W
7-1658	1259899516646	5	2	1	Shannon
7184	1259939617232	38	1	1	
5382	1259962242105	72	1	1	Simi Max

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

_id	name	firstName	lastName	times_contacted	last_time_contacted	custom_rin
1	Mike Butcher	Mike	Butcher	44	1259693729802	content://m
2	Shannon Maguire	Shannon	Maguire	188	1259899525601	/sdcard/Mu
3	Simi Maxfield	Simi	Maxfield	80	1260116630998	content://m
4	Lindsay Damici	Lindsay	Damici	27	1260145844463	/sdcard/Mu
5	Jan Lessard	Jan	Lessard	33	1260065377452	

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

Selected Manufacturer:	HTC
Selected Model:	HTC Hero CDMA (Android)
Detected Manufacturer:	sprint
Detected Model:	HERO200
Revision:	1.5 CUPCAKE eng.u70000.20090921.205629
MEID:	270113178313016459 (HEX: A1000007C69D8B)
IMSI:	310006032060645
Extraction start date/time:	11/06/09 16:39:45
Extraction end date/time:	11/06/09 16:51:23
Phone Date/Time: Connection Type:	11/06/09 20:38:51 (GMT) USB Cable
UFED Version:	Software: 1.1.2.4 UFED , Full Image: 1.0.2.4 , Tiny Image: 1.0.2.1
UFED S/N:	5518965

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

4	* Twitter	10/11/09 13:40:26 (GMT)	Read	Inbox	Phone
171658	* Shannon Maguire	10/11/09 06:18:47 (GMT)	Read	Inbox	Phone
052307	* Steve Charbonneau	10/11/09 04:19:44 (GMT)	Read	Inbox	Phone
052307	* Steve Charbonneau	10/11/09 03:49:45 (GMT)	Sent	Sent	Phone

CelleBrite (UFED)

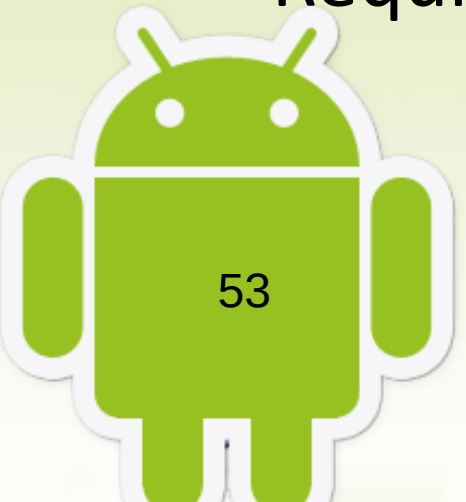
15	File Name: IMAG0028.jpg File Size: 879981 Bytes File Date/Time: 10/20/09 23:48:50 MD5: 124E531F4EBCB1424135F47990F3FFA9 SHA256: D7F16EBA C29C90A 0995C7C 777F625 ED16C61 8515BEB 6DF00E6 03EA9D4 9AD59FA	Resolution: 72x72 (unit: inch) Pixel Resolution: 2560x1712 Camera Make: HTC Camera Model: HERO200 Date/Time: 2009:10:20 23:48:49	
7	File Name: imagejpeg_2.jpg File Size: 68872 Bytes File Date/Time: 10/15/09 23:59:38 MD5: 7B2B667F81DA33D01D2A3DED60486C7F SHA256: 492F43B7 F7553B3 0FA6BCB EA70C58 1FEEF8C B9A502C A86F0AF 11F9A2B E42E416	Resolution: 72x72 (unit: inch) Pixel Resolution: 1280x960 Camera Make: LG Electronics Inc Camera Model: LG-VX8560 Date/Time: 0000:00:00 00:00:00	

#	File Name	File Size	File Date/Time	File Link
1	VIDEO0001.3gp MD5: 0569D5FE42A0AC9BB1AE797ED3BBC0F0 SHA256: 271A2C24 8A26480 2B536D8 0F46743 04DBC81 94398B3 B878EBD FA9524B 0F2949D	1250247 Bytes	10/20/09 23:47:13	VIDEO0001.3gp

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

o **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).

o **Cons**:

- Required root access
- did not find all deleted data.

Summary of Results

Data extraction with the CelleBrite UFED

o **Pros**:

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

o **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!!!