



Sushi-grade Smartphone Forensics on a Ramen Noodle Budget

Heather Mahalik

hmahalik@gmail.com

Twitter: @HeatherMahalik

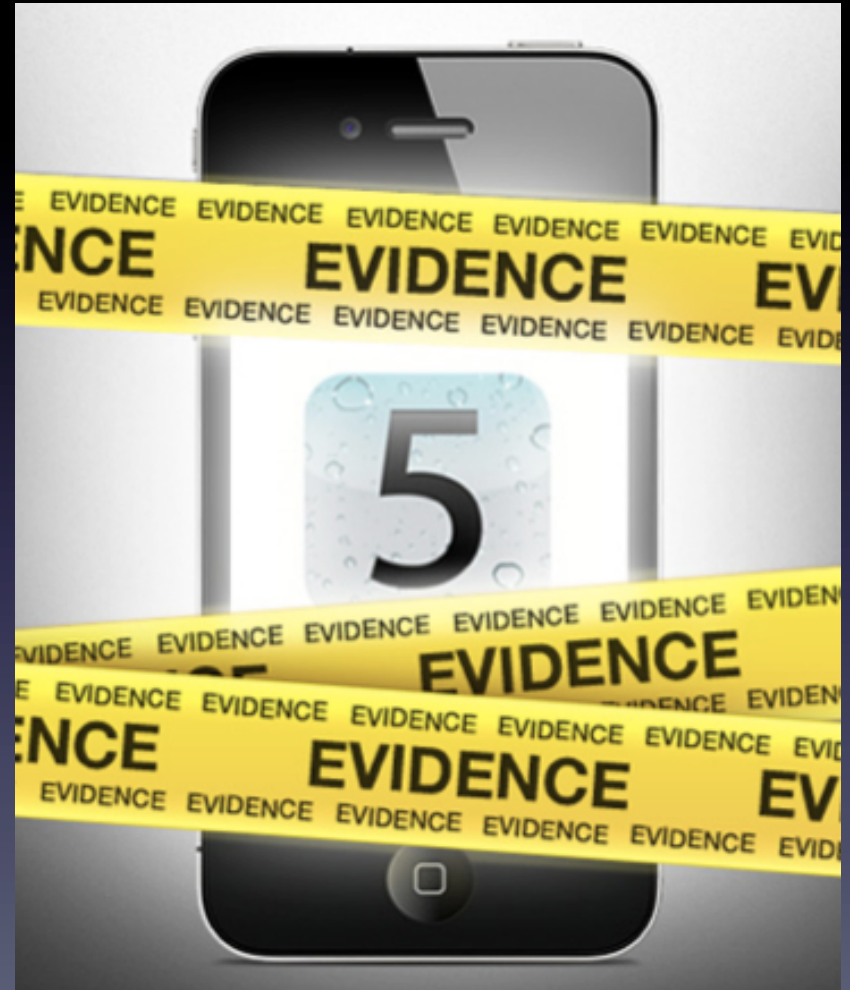
In progress: www.smarterforensics.com

I'm Not Rich... Now What?

- What is available for those with limited budgets?
- Is forensic acquisition of smartphones possible with open source tools?
- Are the analytical tools equal to the commercial products?
- Do the open source tools work as effectively as commercial tools?

iOS Acquisition Solutions

- Zdziarski Methods
- Boot Rom Vulnerability Exploits
 - Custom Ramdisk via SSH
 - The iPhone Data Protection Tools
- iTunes



Do these methods support iOS Physical Acquisition?

- It depends...
 - How old is the device?
 - Is the device locked?
 - Are you Law Enforcement?

iOS Analytical Support

- iPhone Backup Analyzer
- iExplorer
- iBackupBot
- Scalpel
- SQLite Browser
- Plist Editor
- WhatsApp Extract
 - Contacts.sqlite and ChatStorage.sqlite
- Manual examination!



Android Forensics for Free (or a Donation)

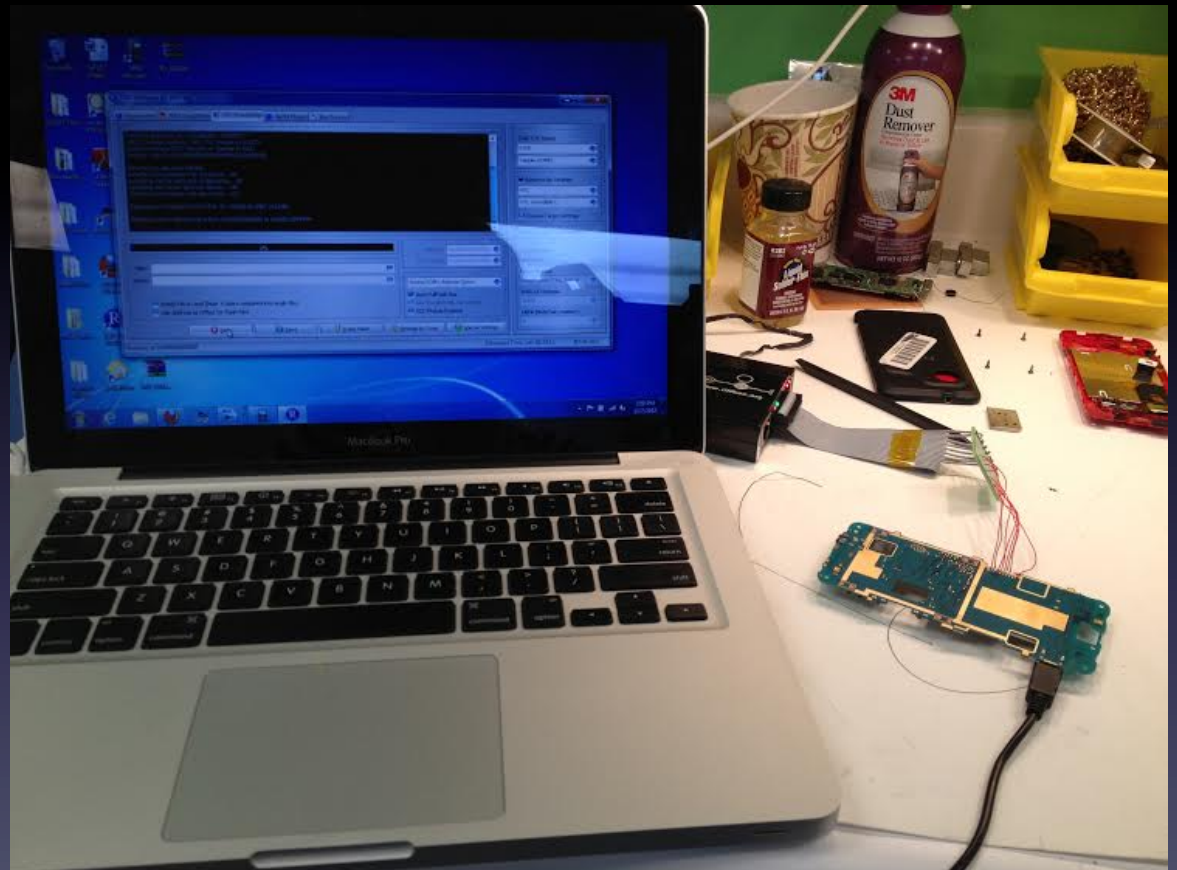
- Acquisition
- Memory Capture
- Analysis

PayPalTM



Android Acquisition

- viaLogical
 - OSE
 - LE
- ADB Backup
- OSAF Toolkit
- Santoku
- DD
 - Not supported for all devices



Android Memory Capture

- LiME (Linux Memory Extractor)
 - First tool to support full memory captures of Android smartphones!
 - TCP dump or saved to SD card
 - Uses ADB

Android Analysis

- Autopsy
 - OMF Module
- WhatsApp Extract
 - wa.db and msgstore.db
- Scalpel
- SQLite Browser
- Anything capable of mounting EXT

Commercial Tool Comparison

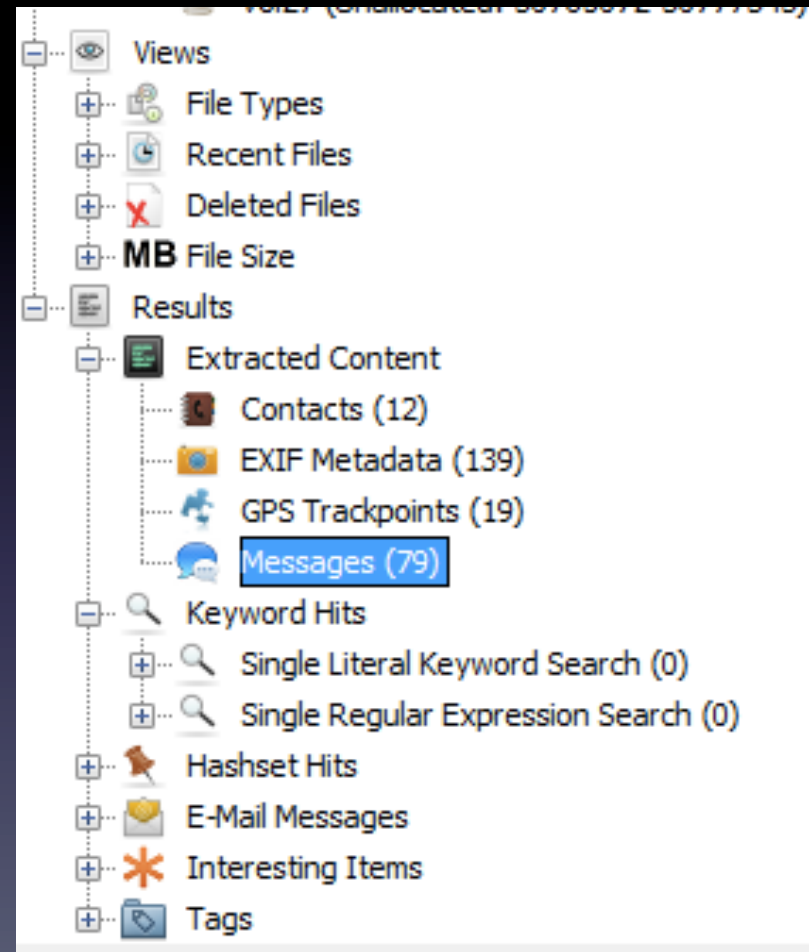
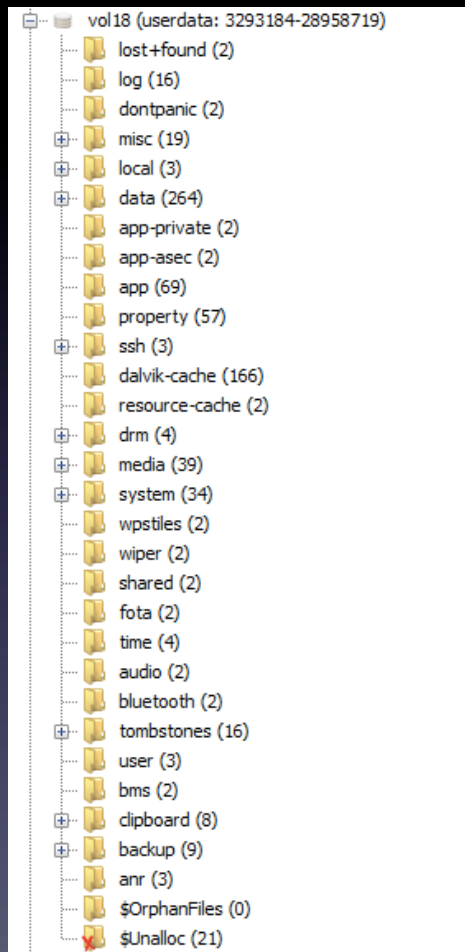
- Memory capture is weak!
- Able to physically acquire locked devices without using USB Debugging*
- One analytical platform for examining all data

Autopsy



- GUI built on The Sleuth Kit
- Next version will include OMF module
- Customizable
- Complete analytical platform
- Android images can be loaded as normal disk images or file folders

Android Examination in Autopsy (1)



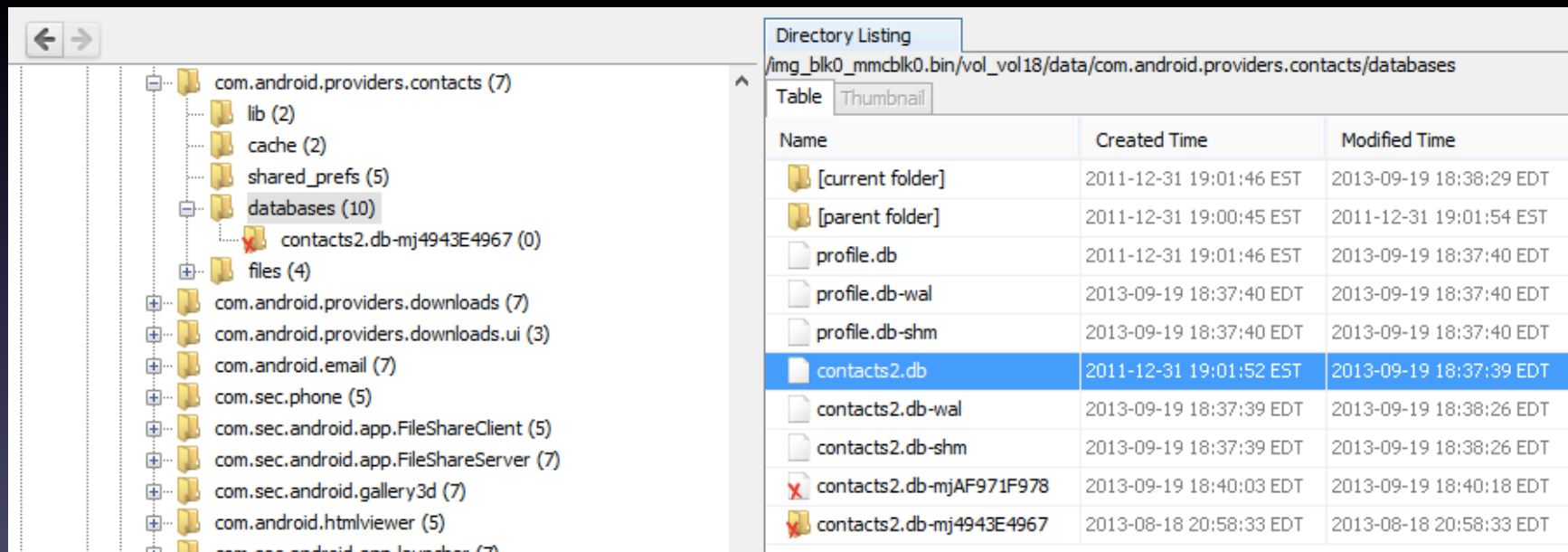
Android Examination in Autopsy (2)

Directory Listing	
Extracted Content	
Table	Thumbnail
Artifact Type	Child Count
 Contacts (12)	12
 EXIF Metadata (139)	139
 GPS Trackpoints (19)	19
 Messages (79)	79

Android Examination in Autopsy-Contacts (1)

Directory Listing				
Contacts				
Table Thumbnail				
Source File	Data Source	Name	Phone Number	Email
 contacts2.db	blk0_mmcbld0.bin			
 contacts2.db	blk0_mmcbld0.bin	Check Balance	#999#	
 contacts2.db	blk0_mmcbld0.bin	Gus Thomas		strozmac@gmail...
 contacts2.db	blk0_mmcbld0.bin	Hank	13392226970	livingstonhank11...
 contacts2.db	blk0_mmcbld0.bin	Ilesanmi Kehinde Femi	+2348032416096	joyreach@hotma...
 contacts2.db	blk0_mmcbld0.bin	MBE	(608) 244-2208	
 contacts2.db	blk0_mmcbld0.bin	Milio	+1 608-221-9400	
 contacts2.db	blk0_mmcbld0.bin	Pizza Hut	+1 608-221-0666	
 contacts2.db	blk0_mmcbld0.bin	Refill Now	*233	
 contacts2.db	blk0_mmcbld0.bin	Sammuell Llorente Cordeiro		sammuell.elloene...
 contacts2.db	blk0_mmcbld0.bin	Tommy Bozeman	+15179085064	tbird420_13@ya...
 contacts2.db	blk0_mmcbld0.bin	livingstonhank11@gmail.com		livingstonhank11...

Android Examination in Autopsy-Contacts (2)



The screenshot displays the Autopsy interface with a directory listing of an Android contacts database. The left pane shows a tree view of the file system, with the 'databases' folder selected. The right pane shows a table of files and folders within the selected directory.

Directory Listing

/img_blk0_mmcblk0.bin/vol_vol18/data/com.android.providers.contacts/databases

Name	Created Time	Modified Time
[current folder]	2011-12-31 19:01:46 EST	2013-09-19 18:38:29 EDT
[parent folder]	2011-12-31 19:00:45 EST	2011-12-31 19:01:54 EST
profile.db	2011-12-31 19:01:46 EST	2013-09-19 18:37:40 EDT
profile.db-wal	2013-09-19 18:37:40 EDT	2013-09-19 18:37:40 EDT
profile.db-shm	2013-09-19 18:37:40 EDT	2013-09-19 18:37:40 EDT
contacts2.db	2011-12-31 19:01:52 EST	2013-09-19 18:37:39 EDT
contacts2.db-wal	2013-09-19 18:37:39 EDT	2013-09-19 18:38:26 EDT
contacts2.db-shm	2013-09-19 18:37:39 EDT	2013-09-19 18:38:26 EDT
contacts2.db-mjAF971F978	2013-09-19 18:40:03 EDT	2013-09-19 18:40:18 EDT
contacts2.db-mj4943E4967	2013-08-18 20:58:33 EDT	2013-08-18 20:58:33 EDT

Android Examination in Autopsy-Contacts (3)

 contacts2.db	2011-12-31 19:01:52 EST	2013-09-19 18:37:39 EDT	2011-12-31 19:01:52 EST
 contacts2.db-wal	2013-09-19 18:37:39 EDT	2013-09-19 18:38:26 EDT	2013-09-19 18:37:39 EDT
 contacts2.db-shm	2013-09-19 18:37:39 EDT	2013-09-19 18:38:26 EDT	2013-09-19 18:37:39 EDT
 contacts2.db-mjAF971F978	2013-09-19 18:40:03 EDT	2013-09-19 18:40:18 EDT	2013-09-19 18:40:03 EDT
 contacts2.db-mj4943E4967	2013-08-18 20:58:33 EDT	2013-08-18 20:58:33 EDT	2013-08-18 20:58:33 EDT

<

Hex	Strings	Metadata	Results	Text	Media	
Page: 1 of 23	Page			Go to Page:		
0x00003a40:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
0x00003a50:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
0x00003a60:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
0x00003a70:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
0x00003a80:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
0x00003a90:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
0x00003aa0:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
0x00003ab0:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
0x00003ac0:	00 00 00 00	00 00 00 00	00 00 00 00	05 3A 00 33	21 94 34 64	:3!.4d
0x00003ad0:	69 72 74 79	63 73 65 7A	40 67 6D 61	69 6C 2E 63		irtycsez@gmail.c
0x00003ae0:	6F 6D 63 6F	6D 2E 67 6F	6F 67 6C 65	EF BE AD DE		omcom.google....
0x00003af0:	02 00 00 00	04 05 00 00	42 4E 44 4C	03 00 00 00		BNDL....

Android Examination in Autopsy-Messages (1)

- Includes 3rd Party App messages and chats, SMS and MMS messages
 - Current support Tango and Words With Friends
 - More being added as we speak...

Android Examination in Autopsy-Messages

 mmssms.db	She knows nothing.	+13392226970	1379119670179
 mmssms.db	Ya sure you can't get her phone? It'd be good to get her pw for wor...	+13392226970	1379119753380
 mmssms.db	I have other ideas in mind. She will hand it all to me!	+13392226970	1379119788935
 mmssms.db	Charm her man! You know be romeo!	+13392226970	1379119795722
 mmssms.db	I'd feel safer if we knew who she talks to.	+13392226970	1379119873170
 mmssms.db	Done! Don't worry. I have it under control	+13392226970	1379119901947

Android Examination in Autopsy-Tango

tc.db	" Night : Hank Livingston	137955503908
tc.db	"\fGot it. Thx. 銆? ? ? ? ? ? ? ? ? ? (...	1379555492472
tc.db	" 993580970795409 C Hank Livingston	1379555458752
tc.db	" Tracking number on its way C Hank Livingston	1379555422876
tc.db	" I'll ignite it! C Hank Livingston	1377483920956
tc.db	" I mean ignore. ? ? ? ? ? ? ? ? ? ? (...	1377304855046
tc.db	" Test please ignite ? ? ? ? ? ? ? ? ? ? (...	1377304836303

Android Examination in Autopsy-WWF

	WordsFramework	gotcha. thx.	2013-09-19T01:...
	WordsFramework	Sent u the info	2013-09-19T01:...
	WordsFramework	fed ex is better than regular mail.	2013-09-18T22:...
	WordsFramework	how did u know that word.	2013-08-18T17:...
	WordsFramework	yeah. its the only word I had to play.	2013-08-18T17:...
	WordsFramework	r u real.....	2013-08-18T17:...
	WordsFramework	thanks! the tile gods were smiling.	2013-08-05T14:...
	WordsFramework	good grief,that was a good one,well done	2013-08-05T12:...
	WordsFramework	sorry for delay,been on hols	2013-07-28T19:...

Reporting Location Information (1)

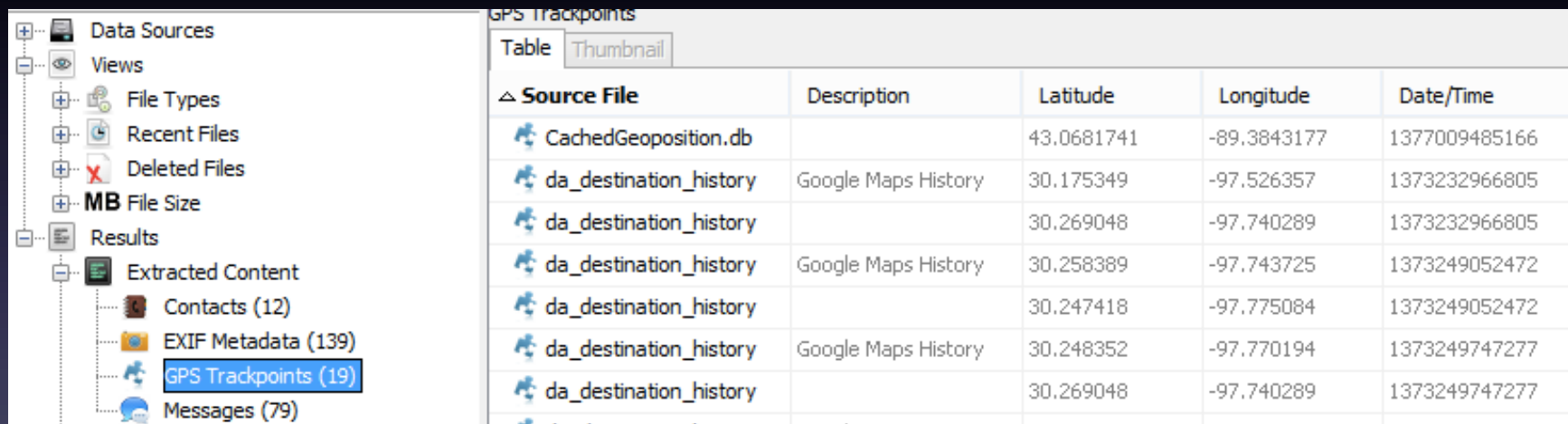
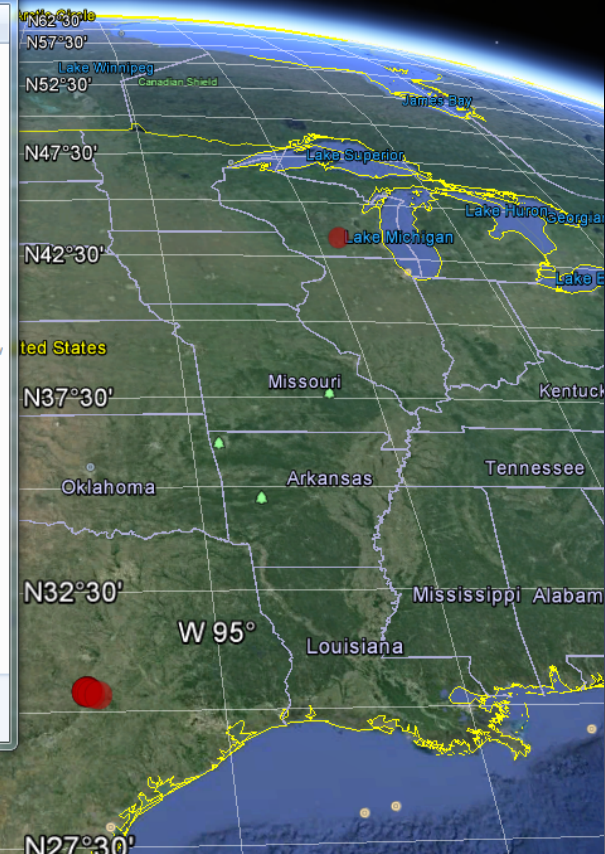
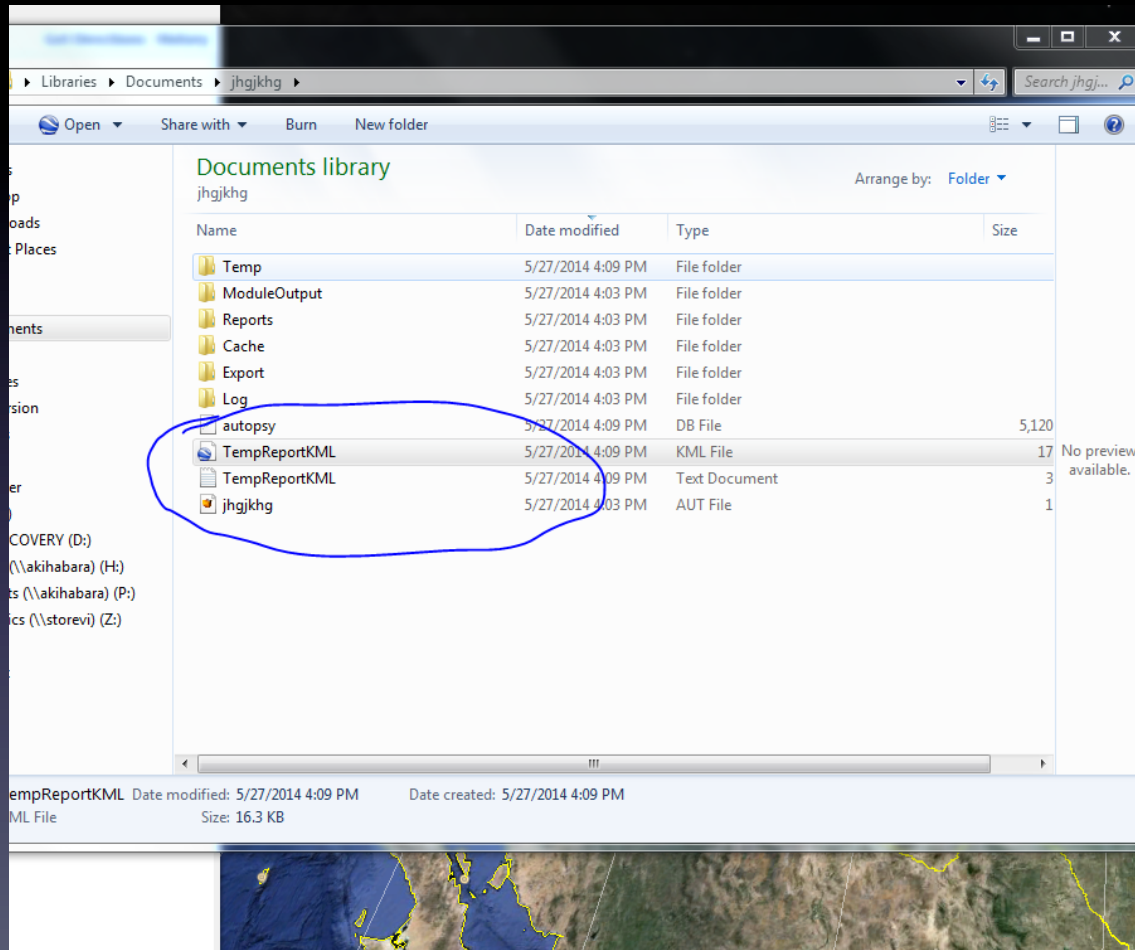


Table Thumbnail				
Source File	Description	Latitude	Longitude	Date/Time
CachedGeoposition.db		43.0681741	-89.3843177	1377009485166
da_destination_history	Google Maps History	30.175349	-97.526357	1373232966805
da_destination_history		30.269048	-97.740289	1373232966805
da_destination_history	Google Maps History	30.258389	-97.743725	1373249052472
da_destination_history		30.247418	-97.775084	1373249052472
da_destination_history	Google Maps History	30.248352	-97.770194	1373249747277
da_destination_history		30.269048	-97.740289	1373249747277
da_destination_history	Google Maps History	30.248352	-97.770194	1373249747277

Reporting Location Information (2)



Reporting Location Information (3)



Android Examination in Autopsy – Multimedia Files (1)

EXIF Metadata

Table Thumbnail						
Source File	Date Created	Device Model	Device Make	Latitude	Longitude	Altitude
 tmp	2013-07-07 11:07:01 EDT	SGH-T999	SAMSUNG			
 sv01_pv00_00000146	2013-06-13 09:53:23 EDT	iPhone 5	Apple	52.1924...	0.230166...	19.13214285714...
 cache-1537038623.tmp	2013-06-03 15:00:33 EDT	SGH-T999	SAMSUNG			
 63685c51eb6fd25d21	2013-07-20 07:15:28 EDT	DMC-ZS5	Panasonic			
 bcde96aff3da0ff29dd	2013-06-13 09:53:23 EDT	iPhone 5	Apple	52.1924...	0.230166...	19.13214285714...
 20130702_223541.jpg	2013-07-02 22:35:40 EDT	SGH-T999	SAMSUNG			

Android Examination in Autopsy – Multimedia Files (2)

Images		
Table Thumbnail		
Name	Location	Modified Time
 d2_tmo_wallpaper_01.jpg	/img_blk0_mmcblk0.bin/vol_vol17/wallpaper/drawable/d2_tmo_wallpa...	2008-08-01 08:00:00 EDT
 d2_tmo_wallpaper_01_small.jpg	/img_blk0_mmcblk0.bin/vol_vol17/wallpaper/drawable/d2_tmo_wallpa...	2008-08-01 08:00:00 EDT
 cb5d6704-f204-4926-8abf-e4bb505dcf1f.PNG	/img_blk0_mmcblk0.bin/vol_vol18/data/com.tmobile.pr.mytmobile/file...	2013-07-03 12:34:42 EDT
 01f7619b-a3ea-469c-a241-4677eacf1f99.PNG	/img_blk0_mmcblk0.bin/vol_vol18/data/com.tmobile.pr.mytmobile/file...	2013-07-03 12:34:43 EDT
 5fe879d8-ea67-4208-9a4a-b32635789cf5.PNG	/img_blk0_mmcblk0.bin/vol_vol18/data/com.tmobile.pr.mytmobile/file...	2013-07-07 12:06:31 EDT
 6561a584-1cb5-4186-a330-cf8ac6bcb7b7.PNG	/img_blk0_mmcblk0.bin/vol_vol18/data/com.tmobile.pr.mytmobile/file...	2013-07-07 12:06:32 EDT
 e2c4fe79-a80e-4d48-ae10-6829eb67629f.PNG	/img_blk0_mmcblk0.bin/vol_vol18/data/com.tmobile.pr.mytmobile/file...	2013-07-09 12:06:36 EDT
 c68ea421-46f0-47f1-ba6e-90f9afc6bf11.PNG	/img_blk0_mmcblk0.bin/vol_vol18/data/com.tmobile.pr.mytmobile/file...	2013-07-09 12:06:36 EDT
 e0c50f6f-2f3f-43f0-ae55-ccd6c4cb59c3.PNG	/img_blk0_mmcblk0.bin/vol_vol18/data/com.tmobile.pr.mytmobile/file...	2013-08-02 21:26:28 EDT

Android Examination in Autopsy – Multimedia Files (3)



Commercial Tools

- That's not why you are here!
 - Truth – they work well, but they cost a lot...



SANS DFIR Webcast Series

DIGITAL FORENSICS & INCIDENT RESPONSE

FOR585 Advanced Smartphone Forensics Course Available At:

SANSFIRE w/ Heather Mahalik – June 23 – 28

**SANS San Francisco w/ Cindy Murphy – July 14
– 19**

SANS Boston w/ Cindy Murphy – July 28 – Aug 2

VLIVE – August 19 – Sept 28th



Questions? Live Demo?

Heather Mahalik

hmahalik@gmail.com

Twitter: @HeatherMahalik

In progress: www.smarterforensics.com