Open Source Mobile Device Forensics

Heather Mahalik

Device Acquisition

iOS Devices

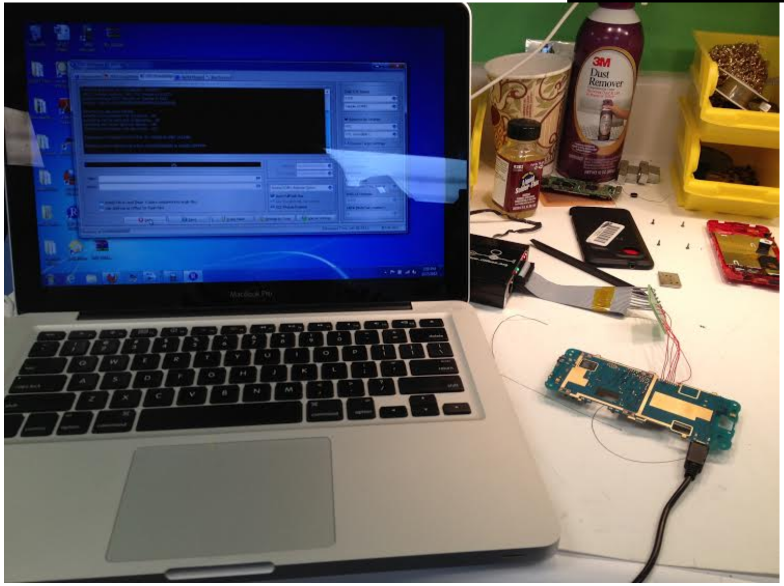
- Zdziarski Methods
- Boot Rom Vulnerability Exploits
  - Custom Ramdisk via SSH
  - The iPhone Data Protection Tools
- iTunes

Android Devices

- viaLogical
- ADB Backup
- OSAF Toolkit
- Santoku
- DD
  - Not supported for all devices
- JTAG/Chip-off

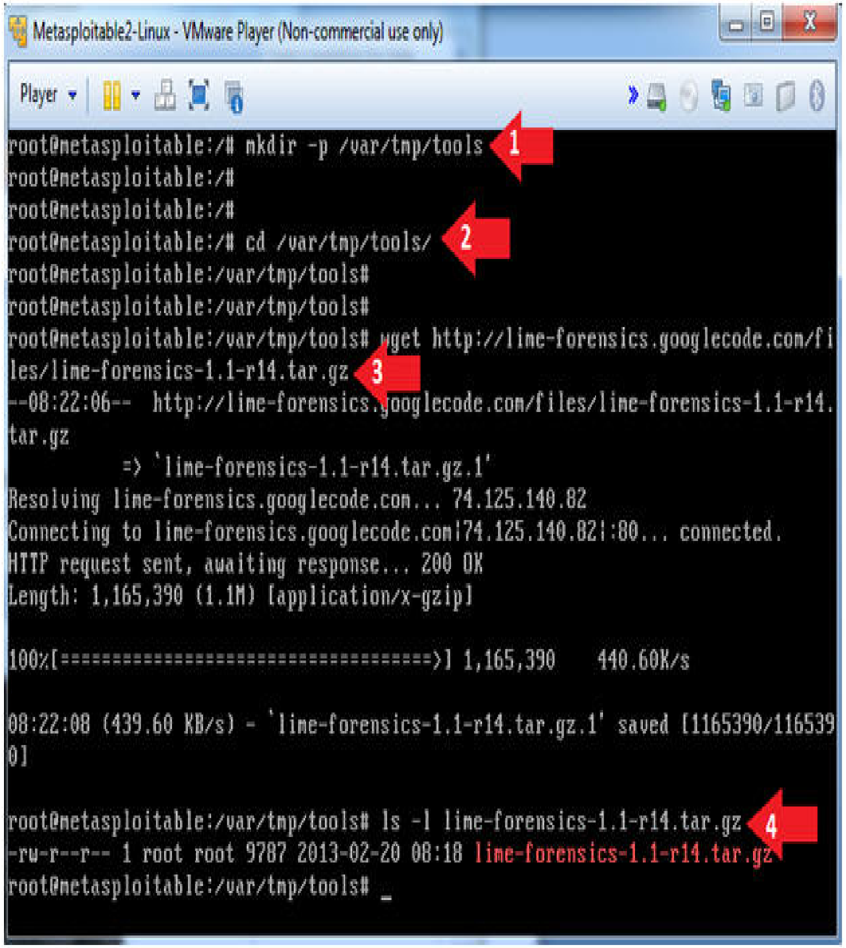
Considerations

- How old is the device?
- Is the device locked?
- Is the device damaged?
- Are you Law Enforcement?



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


Metasploitable2-Linux - VMware Player (Non-commercial use only)
Player
1
2
3
4

```
root@metasploitable:/# mkdir -p /var/tmp/tools
root@metasploitable:/#
root@metasploitable:/#
root@metasploitable:/# cd /var/tmp/tools/
root@metasploitable:/var/tmp/tools#
root@metasploitable:/var/tmp/tools#
root@metasploitable:/var/tmp/tools# wget http://lime-forensics.googlecode.com/fi
les/lime-forensics-1.1-r14.tar.gz
--08:22:06--  http://lime-forensics.googlecode.com/files/lime-forensics-1.1-r14.
tar.gz
           => `lime-forensics-1.1-r14.tar.gz.1'
Resolving lime-forensics.googlecode.com... 74.125.140.82
Connecting to lime-forensics.googlecode.com|74.125.140.82|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1,165,390 (1.1M) [application/x-gzip]

100%[====================================>] 1,165,390    440.60K/s

08:22:08 (439.60 KB/s) - `lime-forensics-1.1-r14.tar.gz.1' saved [1165390/116539
0]

root@metasploitable:/var/tmp/tools# ls -l lime-forensics-1.1-r14.tar.gz
-rw-r--r-- 1 root root 9787 2013-02-20 08:18 lime-forensics-1.1-r14.tar.gz
root@metasploitable:/var/tmp/tools# _
```

Analytical Tools…to Name a Few

iOS Devices

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

Android Devices

- Autopsy
  - Android Module
- WhatsApp Extract
  - wa.db and msgstore.db
- Scalpel
- SQLite Browser
- Hex Editor
- Anything capable of mounting EXT
- FTK Imager
- Customized scripts
- Manual examination

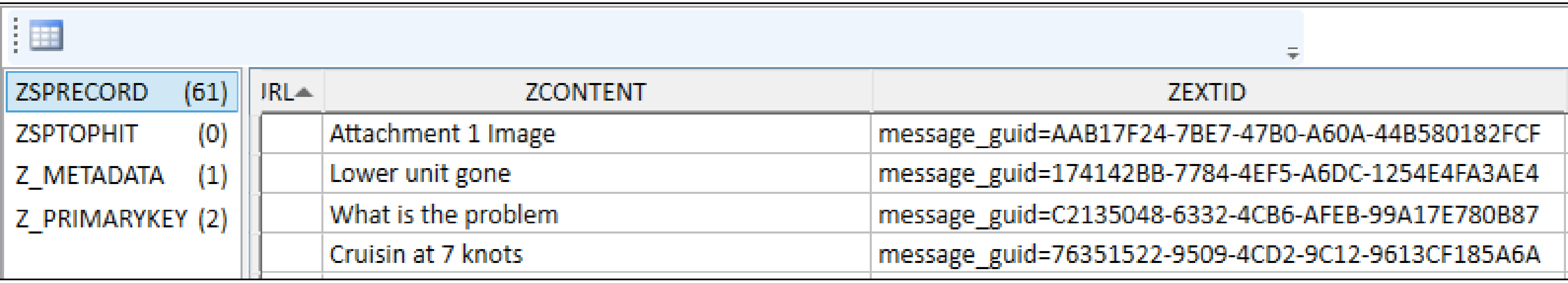
Reality Check!

- Commercial tools are expensive
  - They still miss data
  - They don't parse third party applications completely
  - They omit relevant databases when extracting data
  - They don't support all devices
- Open Source tools
  - See above!

Example – iOS Examination

/private/var/mobile/library/Spotlight/com.apple.mobilesms/

– smssearchindex.sqlite



ZSPRECORD	(61)
ZSPTOPHIT	(0)
Z_METADATA	(1)
Z_PRIMARYKEY	(2)

IRL▲	ZCONTENT	ZEXTID
	Attachment 1 Image	message_guid=AAB17F24-7BE7-47B0-A60A-44B580182FCF
	Lower unit gone	message_guid=174142BB-7784-4EF5-A6DC-1254E4FA3AE4
	What is the problem	message_guid=C2135048-6332-4CB6-AFEB-99A17E780B87
	Cruisin at 7 knots	message_guid=76351522-9509-4CD2-9C12-9613CF185A6A

- Provides SMS message data
  - Active and deleted messages
  - Should be compared to sms.db
  - May show traces of attachments (metadata)

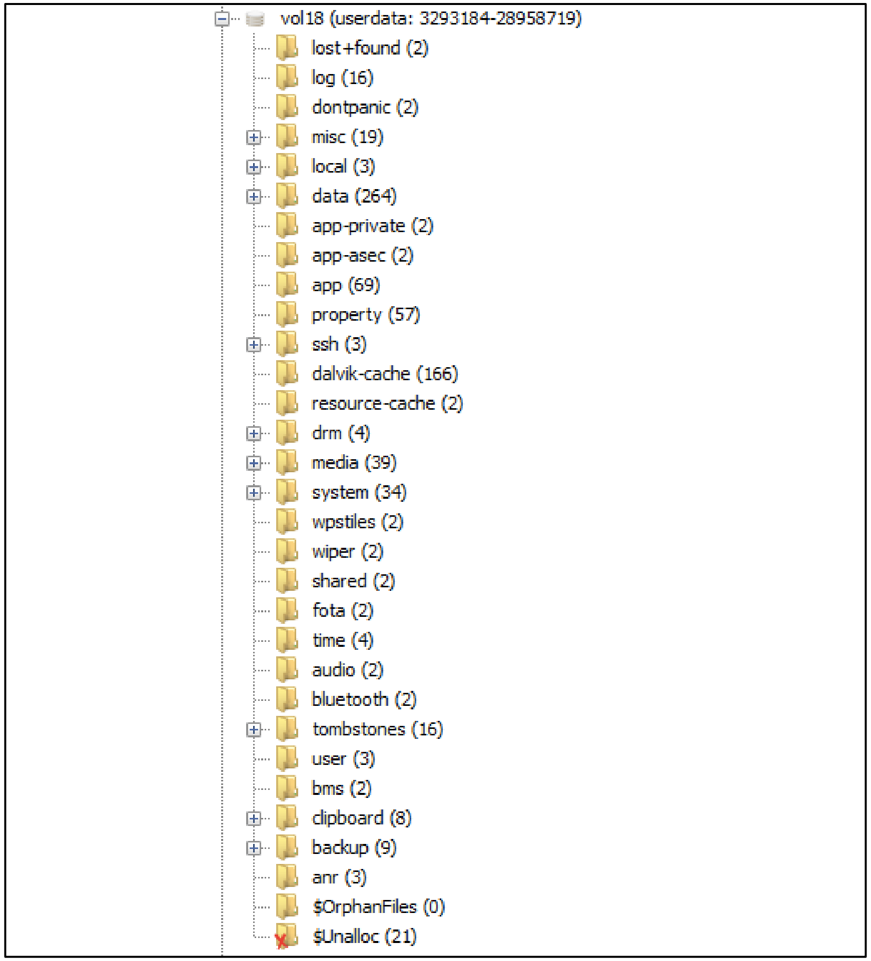
**Not commonly parsed by any tool!*

Autopsy

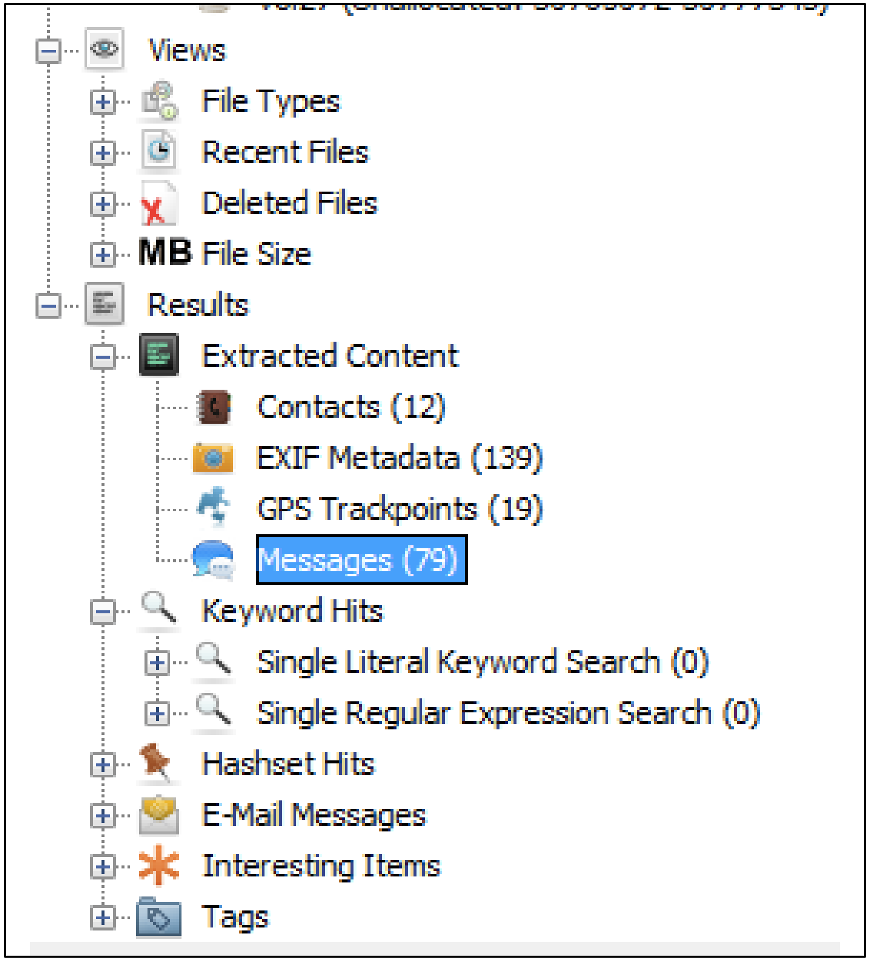
- GUI built on The Sleuth Kit
- Next version (v3.1.1) will include Android module
- Customizable
- Complete analytical platform
- Android dumps can be loaded as normal disk images or file folders

© 2014, Basis Technology

Android Examination



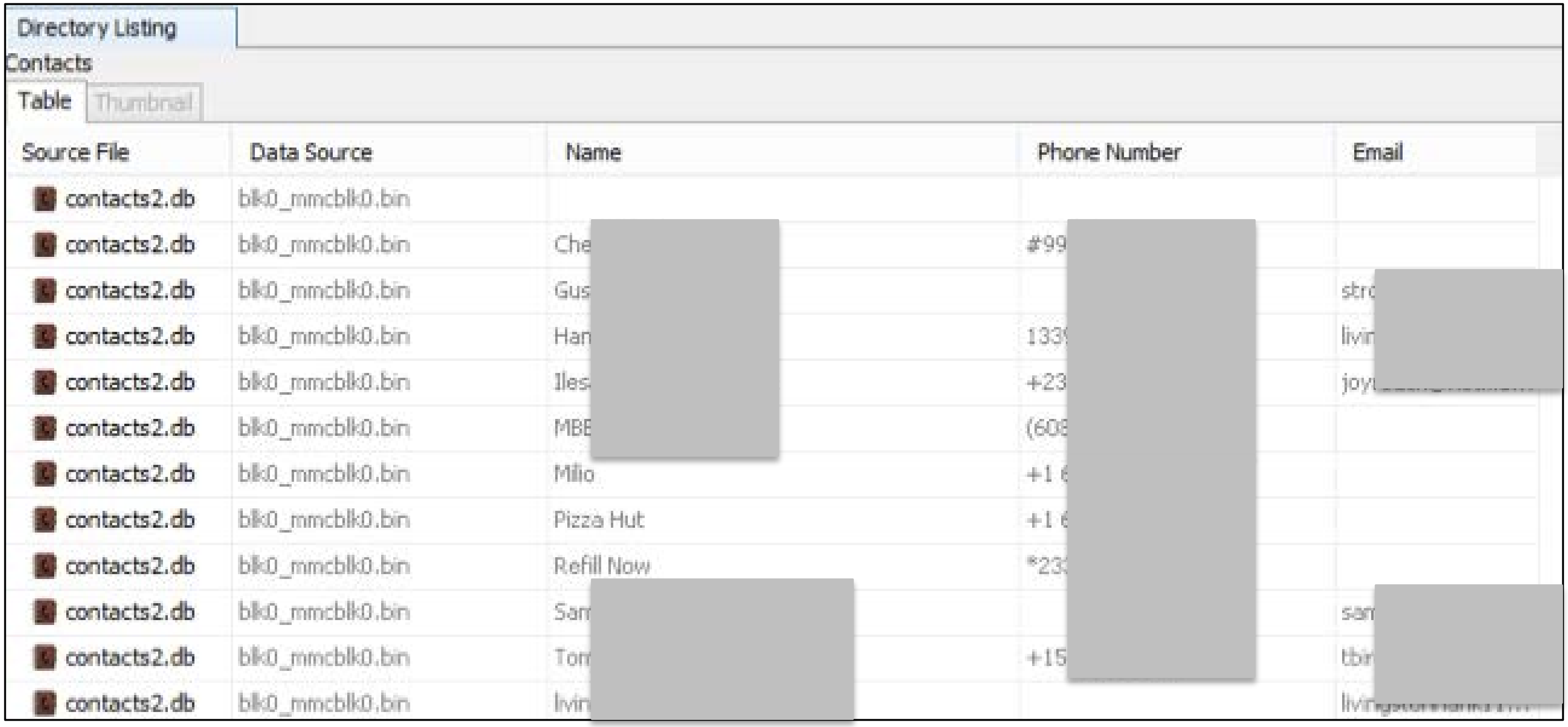
- vol18 (userdata: 3293184-28958719)
  - lost+found (2)
  - log (16)
  - dontpanic (2)
  - misc (19)
  - local (3)
  - data (264)
  - app-private (2)
  - app-asec (2)
  - app (69)
  - property (57)
  - ssh (3)
  - dalvik-cache (166)
  - resource-cache (2)
  - drm (4)
  - media (39)
  - system (34)
  - wpstiles (2)
  - wiper (2)
  - shared (2)
  - fota (2)
  - time (4)
  - audio (2)
  - bluetooth (2)
  - tombstones (16)
  - user (3)
  - bms (2)
  - clipboard (8)
  - backup (9)
  - anr (3)
  - $OrphanFiles (0)
  - $Unalloc (21)



- Views
  - File Types
  - Recent Files
  - Deleted Files
  - MB File Size
- Results
  - Extracted Content
    - Contacts (12)
    - EXIF Metadata (139)
    - GPS Trackpoints (19)
    - Messages (79)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Tags

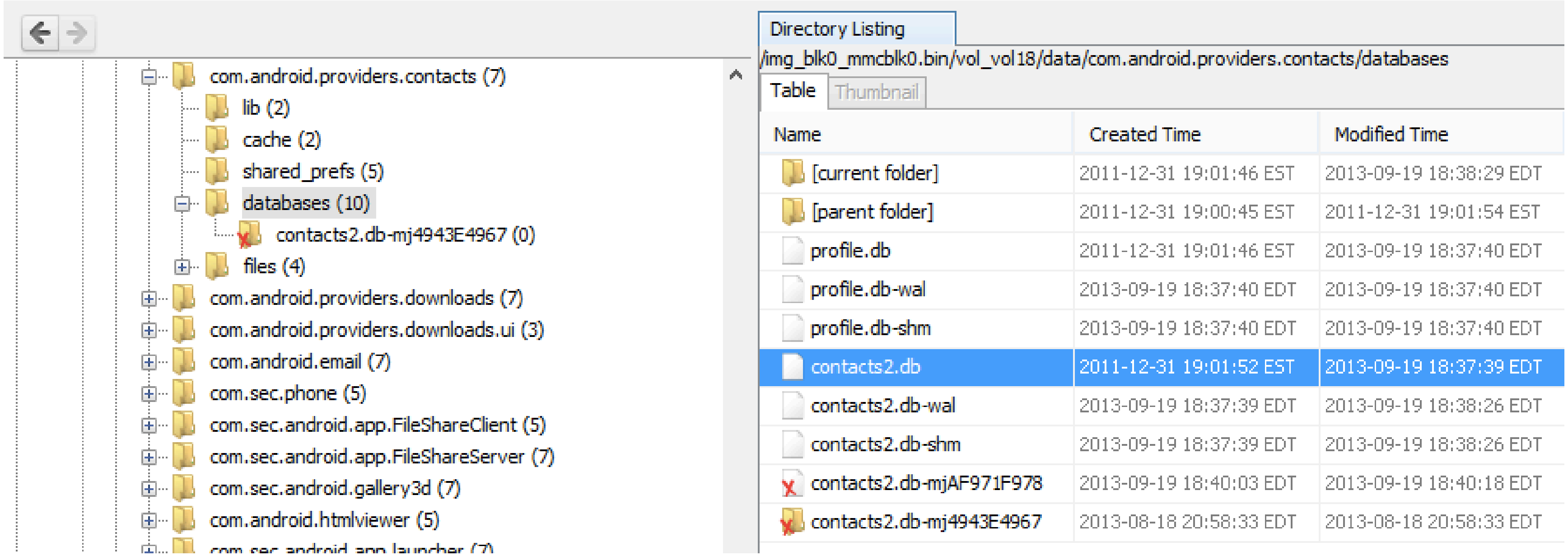
Examining Contacts

- Parsed from Contacts2.db file
  - Raw_contacts and ABPerson



Source File	Data Source	Name	Phone Number	Email
contacts2.db	blk0_mmcblk0.bin			
contacts2.db	blk0_mmcblk0.bin	Che[redacted]	#99[redacted]	
contacts2.db	blk0_mmcblk0.bin	Gus[redacted]	[redacted]	str[redacted]
contacts2.db	blk0_mmcblk0.bin	Han[redacted]	133[redacted]	livi[redacted]
contacts2.db	blk0_mmcblk0.bin	Iles[redacted]	+23[redacted]	joy[redacted]
contacts2.db	blk0_mmcblk0.bin	MBE[redacted]	(60[redacted]	
contacts2.db	blk0_mmcblk0.bin	Milo	+1 6[redacted]	
contacts2.db	blk0_mmcblk0.bin	Pizza Hut	+1 6[redacted]	
contacts2.db	blk0_mmcblk0.bin	Refill Now	*23[redacted]	
contacts2.db	blk0_mmcblk0.bin	San[redacted]	[redacted]	sam[redacted]
contacts2.db	blk0_mmcblk0.bin	Tom[redacted]	+15[redacted]	tbi[redacted]
contacts2.db	blk0_mmcblk0.bin	Ivin[redacted]		livi[redacted]

Examining the Raw Contacts (1)



- com.android.providers.contacts (7)
  - lib (2)
  - cache (2)
  - shared_prefs (5)
  - databases (10)
    - contacts2.db-mj4943E4967 (0)
  - files (4)
- com.android.providers.downloads (7)
- com.android.providers.downloads.ui (3)
- com.android.email (7)
- com.sec.phone (5)
- com.sec.android.app.FileShareClient (5)
- com.sec.android.app.FileShareServer (7)
- com.sec.android.gallery3d (7)
- com.android.htmlviewer (5)
- com.sec.android.app.launcher (7)

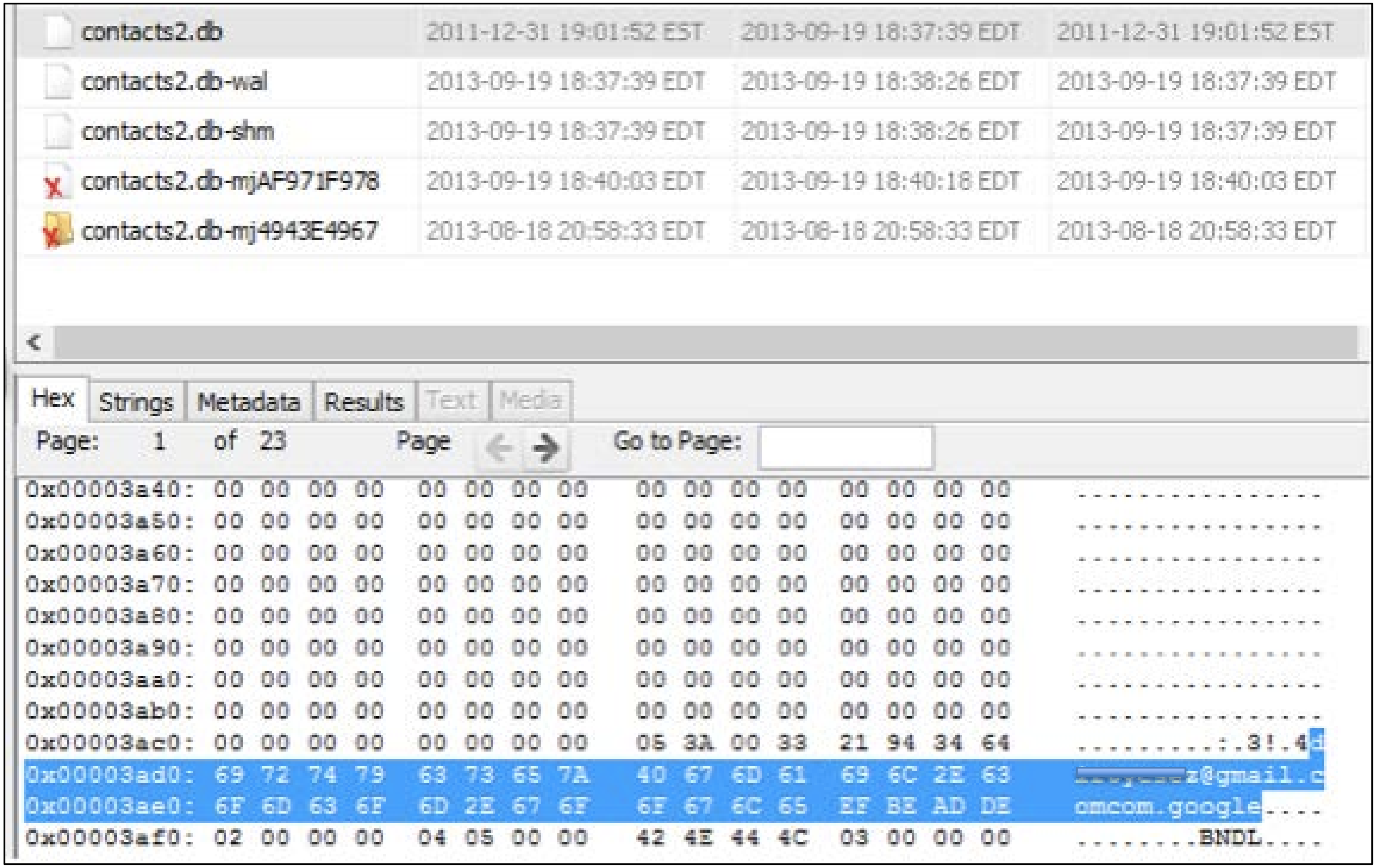
Directory Listing

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

Table | Thumbnail

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

Examining the Raw Contacts (2)



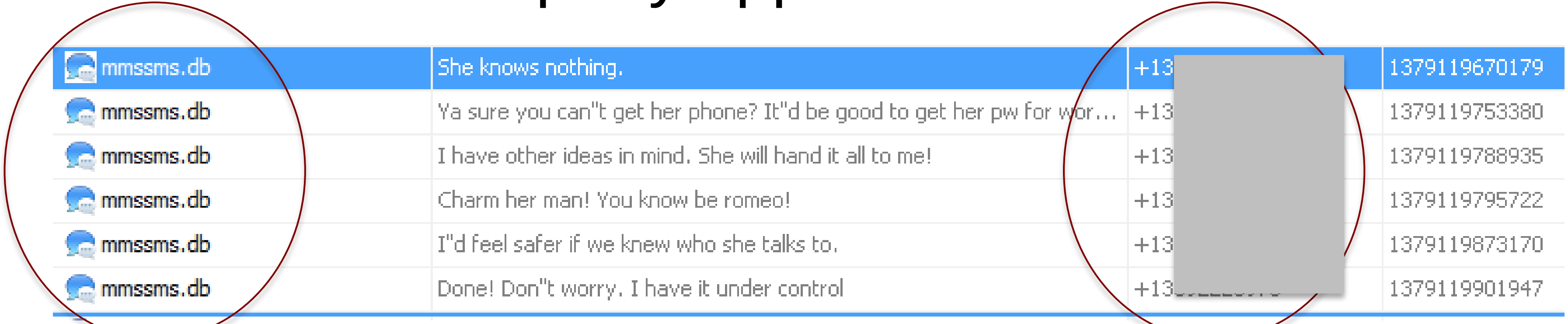
contacts2.db	2011-12-31 19:01:52 EST	2013-09-19 18:37:39 EDT	2011-12-31 19:01:52 EST
contacts2.db-wal	2013-09-19 18:37:39 EDT	2013-09-19 18:38:26 EDT	2013-09-19 18:37:39 EDT
contacts2.db-shm	2013-09-19 18:37:39 EDT	2013-09-19 18:38:26 EDT	2013-09-19 18:37:39 EDT
contacts2.db-mjAF971F978	2013-09-19 18:40:03 EDT	2013-09-19 18:40:16 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

Page: 1 of 23 Page Go to Page:

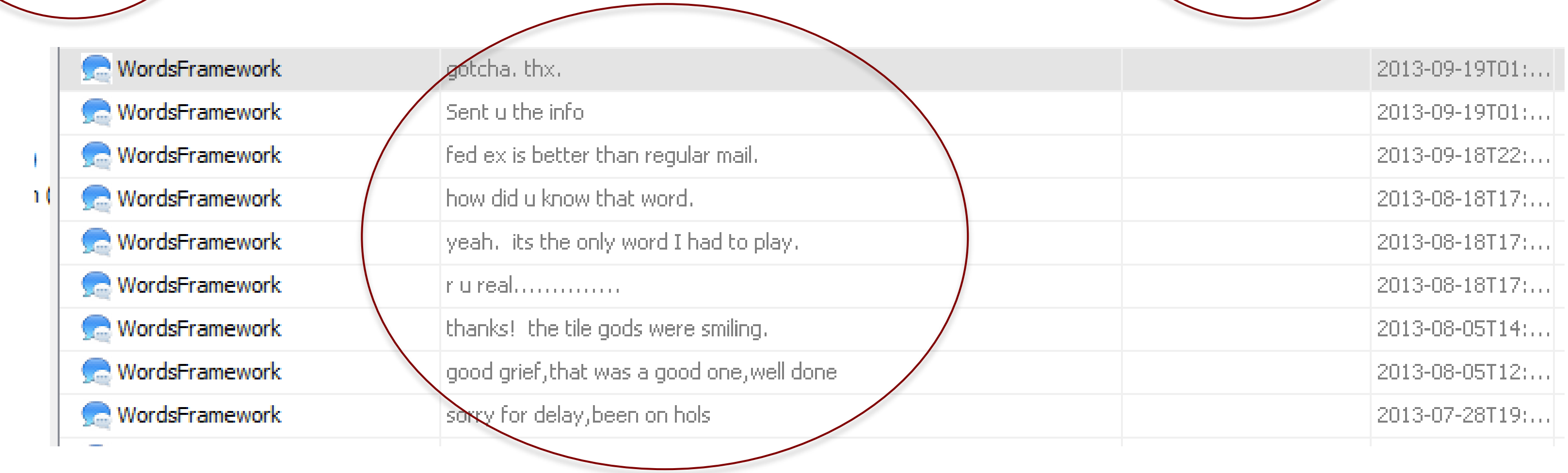
```
0x00003a40: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
0x00003a50: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
0x00003a60: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
0x00003a70: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
0x00003a80: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
0x00003a90: 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   ................
0x00003ab0: 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  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   [redacted]z@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....
```

Parsing Messages and Chats

- Parses messages and chats from SMS, MMS and some third party applications



mmssms.db	She knows nothing.	+13[redacted]	1379119670179
mmssms.db	Ya sure you can"t get her phone? It"d be good to get her pw for wor…	+13[redacted]	1379119753380
mmssms.db	I have other ideas in mind. She will hand it all to me!	+13[redacted]	1379119788935
mmssms.db	Charm her man! You know be romeo!	+13[redacted]	1379119795722
mmssms.db	I"d feel safer if we knew who she talks to.	+13[redacted]	1379119873170
mmssms.db	Done! Don"t worry. I have it under control	+13[redacted]	1379119901947



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:…

Encoding Built into Autopsy

- Encryption vs. Encoding
- Base64 decoder built into Autopsy Android module

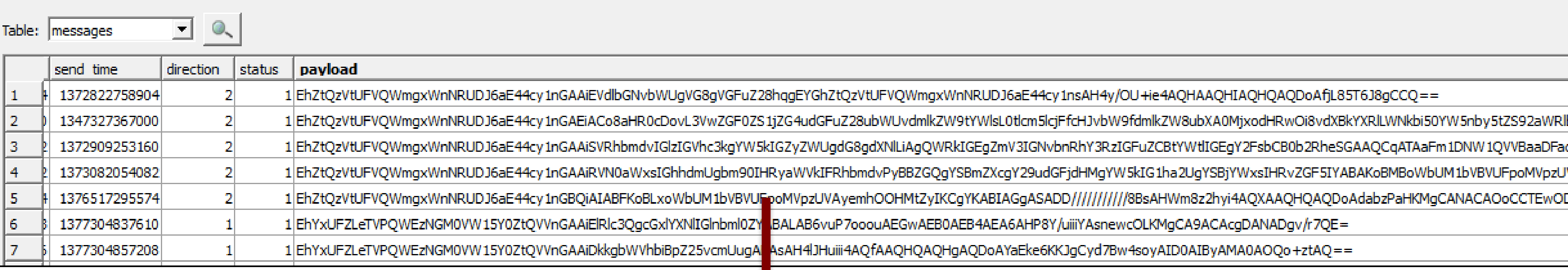
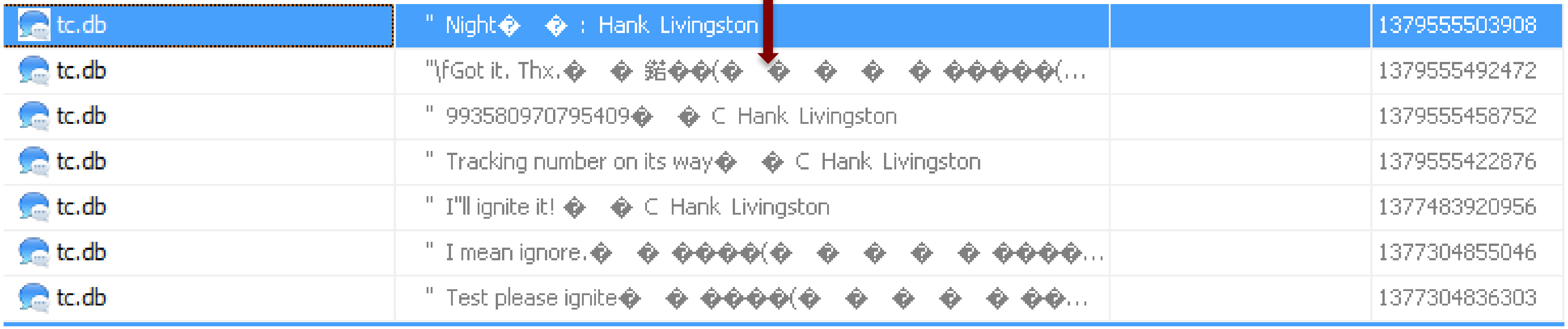


Table: messages

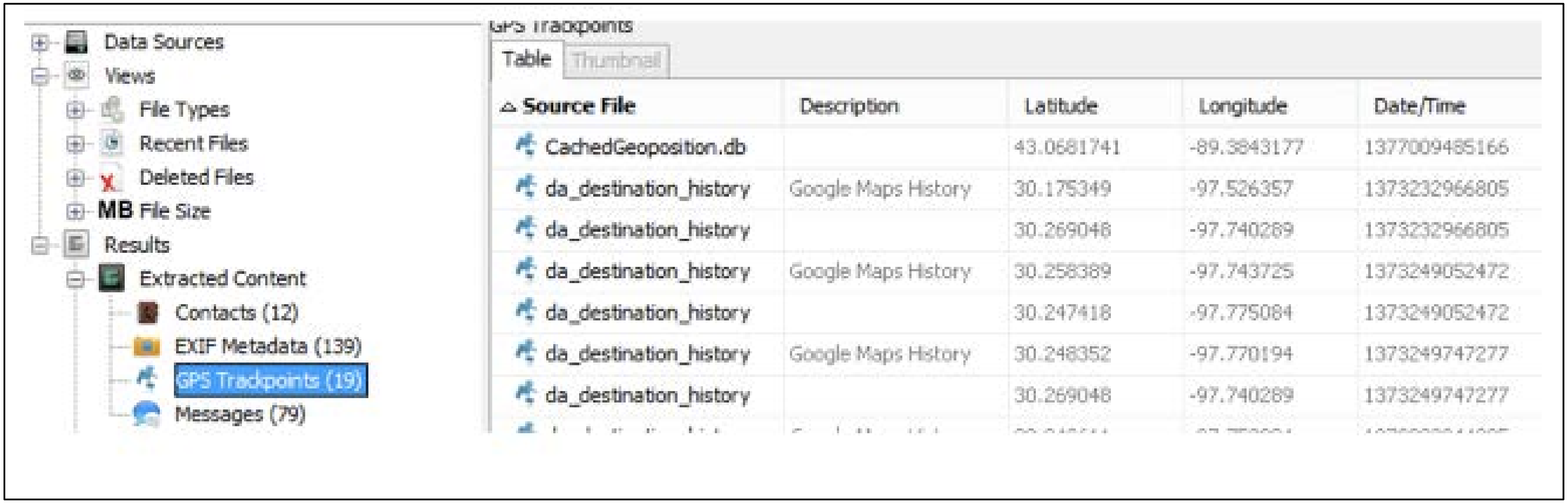
		send time	direction	status	payload
1	4	1372822758904	2	1	EhZtQzVtUFVQWmgxWnNRUDJ6aE44cy1nGAAiEVdlbGNvbWUgVG8gVGFuZ28hqgEYGhZtQzVtUFVQWmgxWnNRUDJ6aE44cy1nsAH4y/OU+ie4AQHAAQHIAQHQAQDoAfjL85T6J8gCCQ==
2	0	1347327367000	2	1	EhZtQzVtUFVQWmgxWnNRUDJ6aE44cy1nGAEiACo8aHR0cDovL3VwZGF0ZS1jZG4udGFuZ28ubWUvdmlkZW9tYWlsL0tlcm5lcjFfcHJvbW9fdmlkZW8ubXA0MjxodHRwOi8vdXBkYXRlLWNkbi50YW5nby5tZS92aWRl
3	2	1372909253160	2	1	EhZtQzVtUFVQWmgxWnNRUDJ6aE44cy1nGAAiSVRhbmdvIGlzIGVhc3kgYW5kIGZyZWUgdG8gdXNlLiAgQWRkIGEgZmV3IGNvbnRhY3RzIGFuZCBtYWtlIGEgY2FsbCB0b2RheSGAAQCqATAaFm1DNW1QVVBaaDFac
4	2	1373082054082	2	1	EhZtQzVtUFVQWmgxWnNRUDJ6aE44cy1nGAAiRVN0aWxsIGhhdmUgbm90IHRyaWVkIFRhbmdvPyBBZGQgYSBmZXcgY29udGFjdHMgYW5kIG1ha2UgYSBjYWxsIHRvZGF5IYABAKoBMBoWbUM1bVBVUFpoMVpzU
5	4	1376517295574	2	1	EhZtQzVtUFVQWmgxWnNRUDJ6aE44cy1nGBQiAIABFKoBLxoWbUM1bVBVUFpoMVpzUVAyemhOOHMtZyIKCgYKABIAGgASADD////////////8BsAHWm8z2hyi4AQXAAQHQAQDoAdabzPaHKMgCANACAOoCCTEwOD
6	8	1377304837610	1	1	EhYxUFZLeTVPQWEzNGM0VW15Y0ZtQVVnGAAiElRlc3QgcGxlYXNlIGlnbml0ZY[illegible]BALAB6vuP7ooouAEGwAEB0AEB4AEA6AHP8Y/uiiiYAsnewcOLKMgCA9ACAcgDANADgv/r7QE=
7	6	1377304857208	1	1	EhYxUFZLeTVPQWEzNGM0VW15Y0ZtQVVnGAAiDkkgbWVhbiBpZ25vcmUugA[illegible]AsAH4lJHuiii4AQfAAQHQAQHgAQDoAYaEke6KKJgCyd7Bw4soyAID0AIByAMA0AOQo+ztAQ==



tc.db	" Night� � : Hank Livingston		1379555503908
tc.db	"\fGot it. Thx.� � 掿��(� � � � � ������(…		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

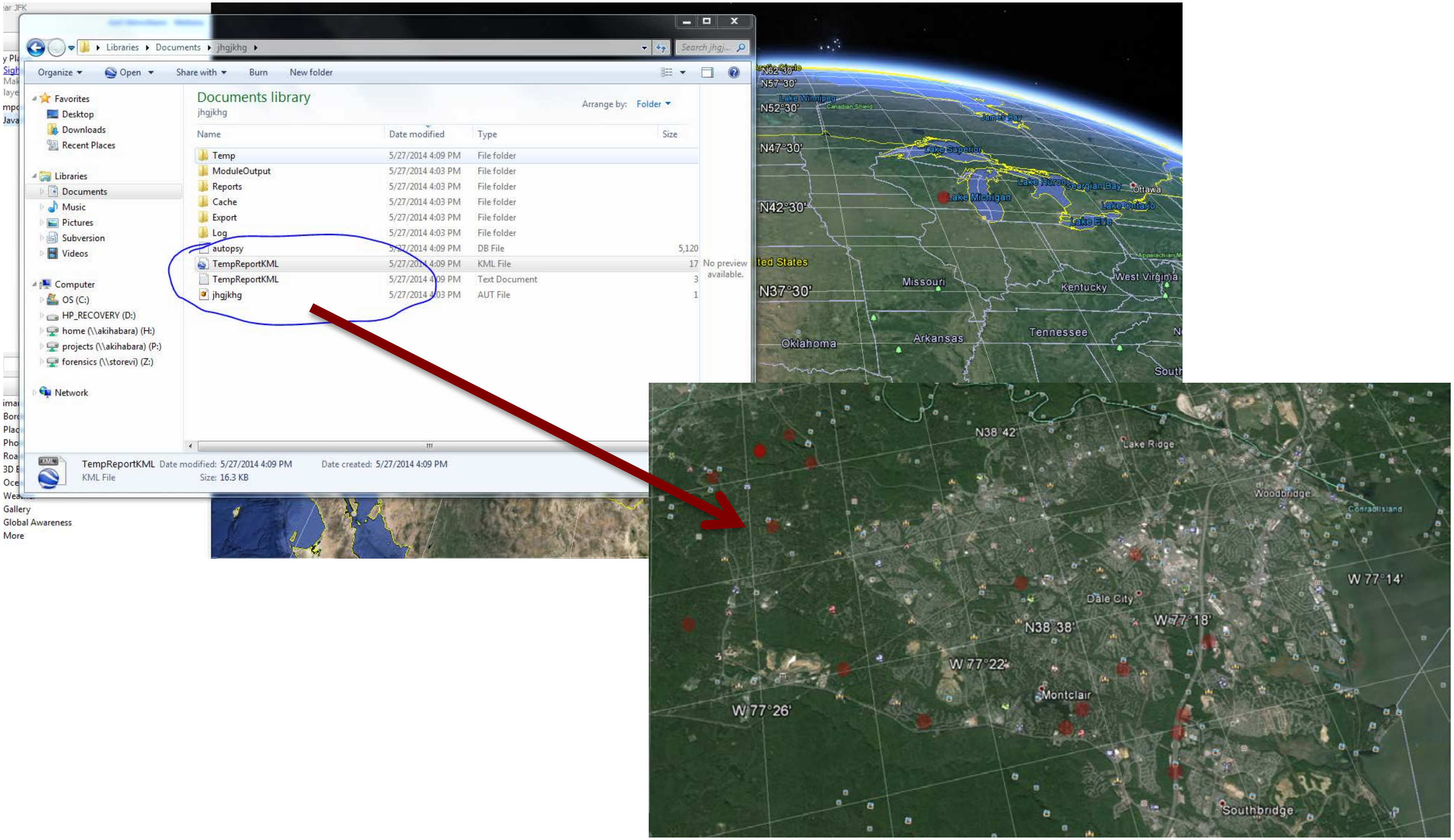
Geolocation Support

- Google Maps, Browser, Cache and EXIF location parsing



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

Geolocation Reporting



Libraries ▸ Documents ▸ jhgjkhg ▸

Documents library
jhgjkhg

Arrange by: Folder

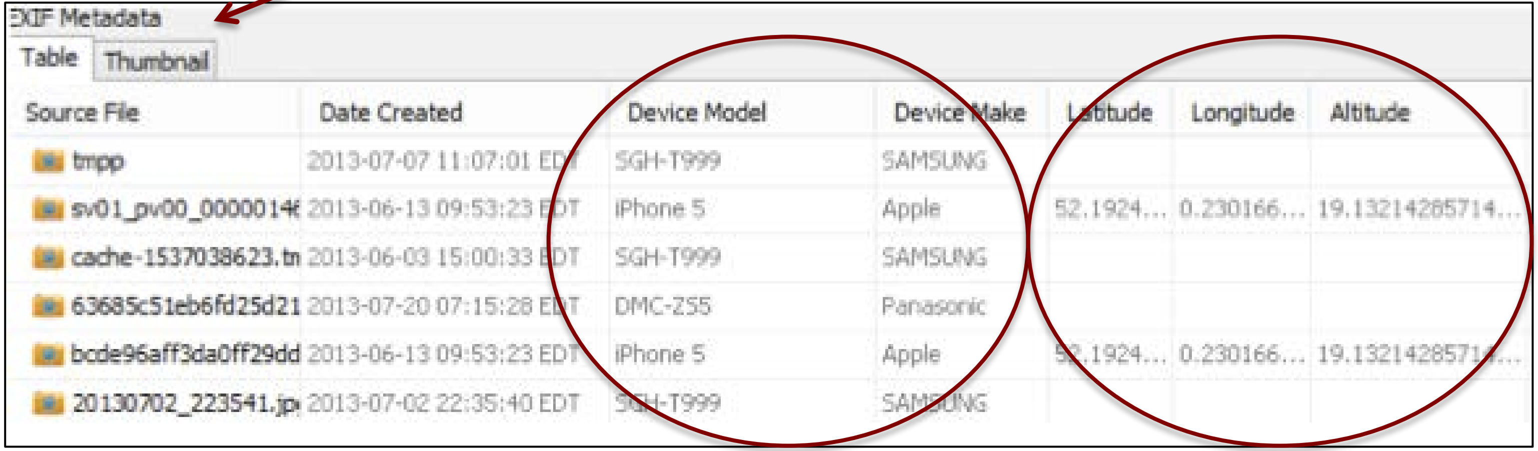
Name	Date modified	Type	Size
Temp	5/27/2014 4:09 PM	File folder	
ModuleOutput	5/27/2014 4:03 PM	File folder	
Reports	5/27/2014 4:03 PM	File folder	
Cache	5/27/2014 4:03 PM	File folder	
Export	5/27/2014 4:03 PM	File folder	
Log	5/27/2014 4:03 PM	File folder	
autopsy	5/27/2014 4:09 PM	DB File	5,120
TempReportKML	5/27/2014 4:09 PM	KML File	17
TempReportKML	5/27/2014 4:09 PM	Text Document	3
jhgjkhg	5/27/2014 4:03 PM	AUT File	1

No preview available.

TempReportKML Date modified: 5/27/2014 4:09 PM Date created: 5/27/2014 4:09 PM
KML File Size: 16.3 KB

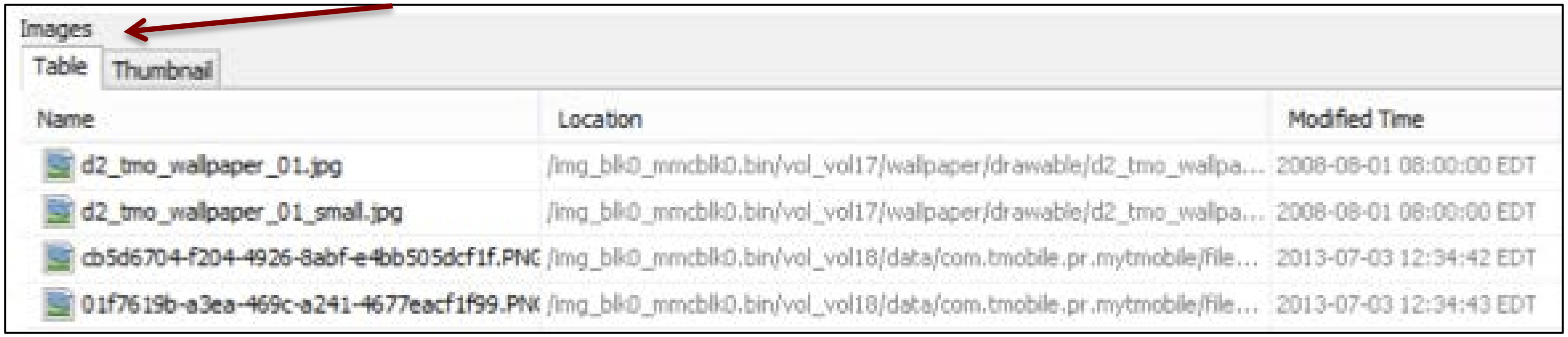
Examining Multimedia Files

- EXIF Parser



Source File	Date Created	Device Model	Device Make	Latitude	Longitude	Altitude
tmpp	2013-07-07 11:07:01 EDT	SGH-T999	SAMSUNG			
sv01_pv00_000014(	2013-06-13 09:53:23 EDT	iPhone 5	Apple	52.1924...	0.230166...	19.1321428571 4...
cache-1537038623.tn	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...	19.1321428571 4...
20130702_223541.jp	2013-07-02 22:35:40 EDT	SGH-T999	SAMSUNG			

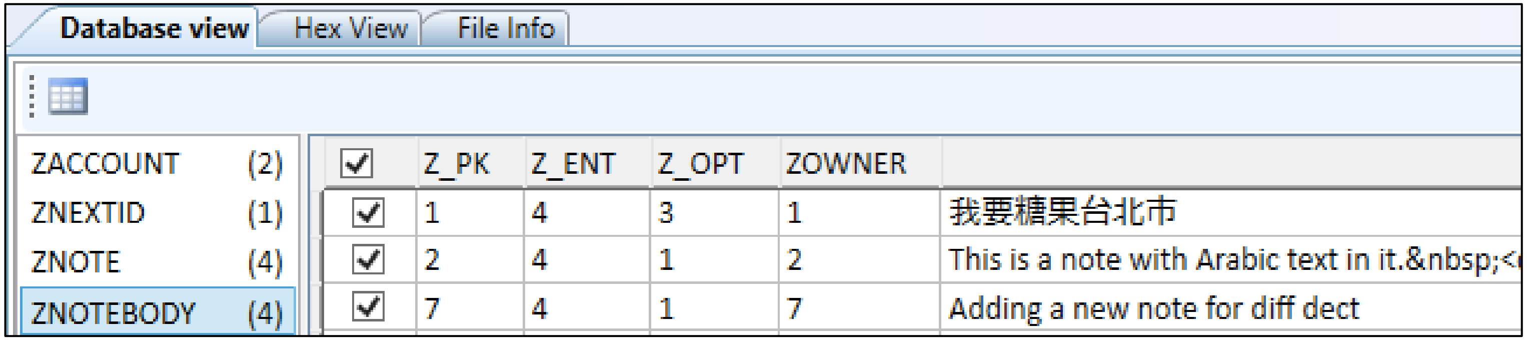
- Graphics and Videos



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.PN(	/img_blk0_mmcblk0.bin/vol_vol18/data/com.tmobile.pr.mytmobile/file...	2013-07-03 12:34:43 EDT

Recovering Deleted SQLite Data

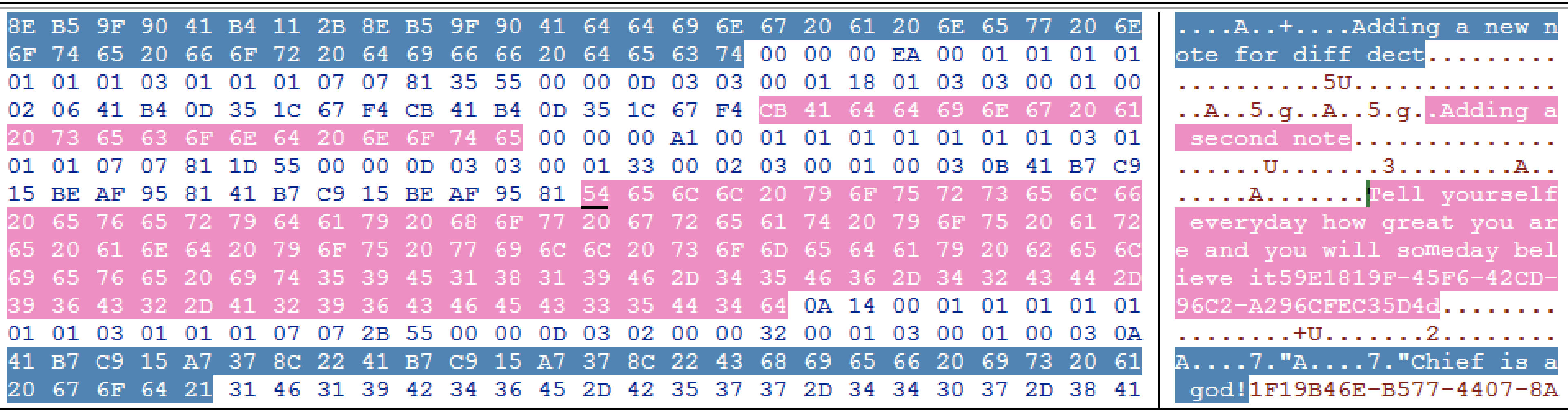
- Active files shown in viewer



ZACCOUNT (2)
ZNEXTID (1)
ZNOTE (4)
ZNOTEBODY (4)

☑	Z_PK	Z_ENT	Z_OPT	ZOWNER	
☑	1	4	3	1	我要糖果台北市
☑	2	4	1	2	This is a note with Arabic text in it. <
☑	7	4	1	7	Adding a new note for diff dect

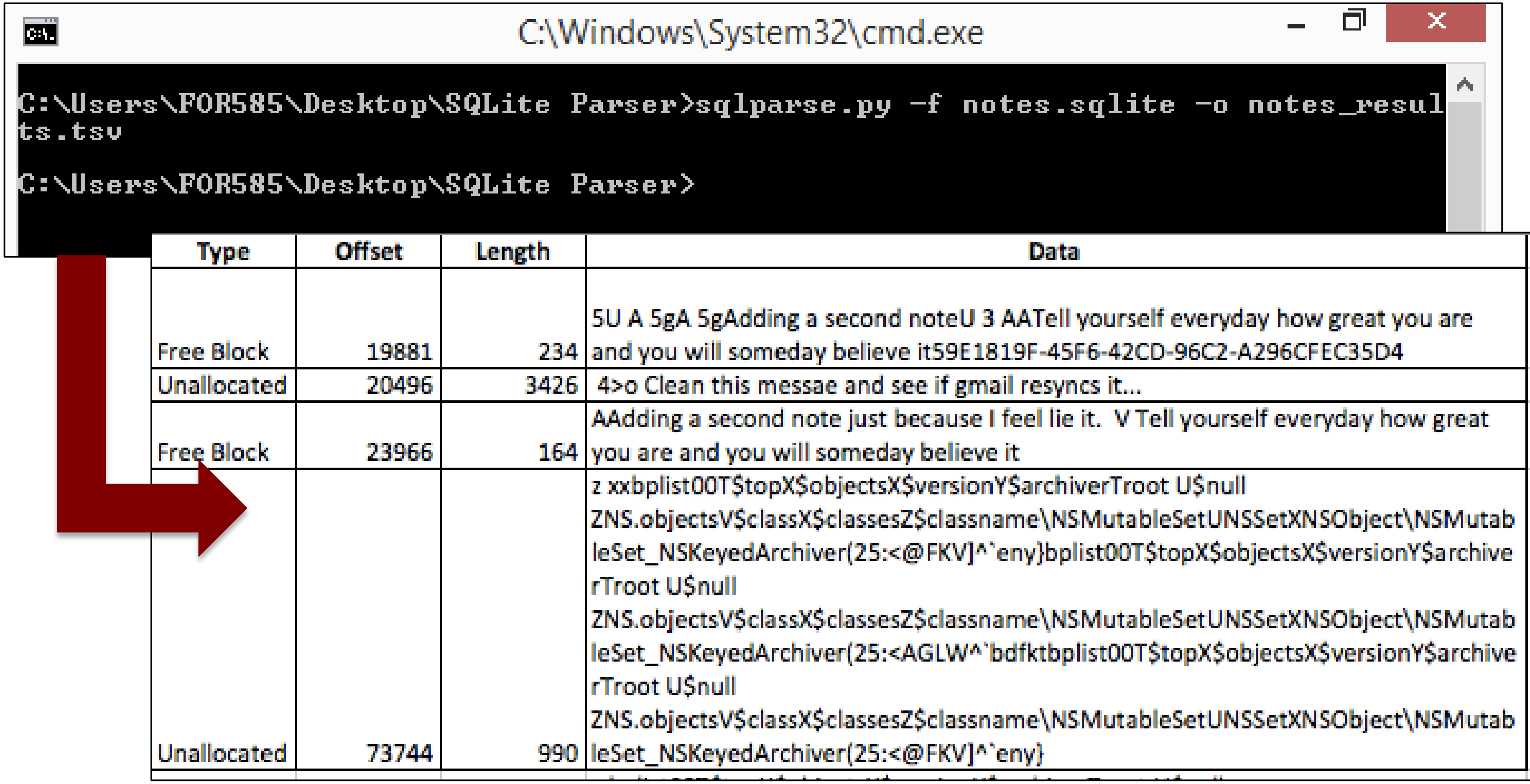
- Deleted must be examined/recovered in Hex



```
8E B5 9F 90 41 B4 11 2B 8E B5 9F 90 41 64 64 69 6E 67 20 61 20 6E 65 77 20 6E   ....A..+....Adding a new n
6F 74 65 20 66 6F 72 20 64 69 66 66 20 64 65 63 74 00 00 00 EA 00 01 01 01 01   ote for diff dect.........
01 01 01 03 01 01 01 07 07 81 35 55 00 00 0D 03 03 00 01 18 01 03 03 00 01 00   ..........5U..............
02 06 41 B4 0D 35 1C 67 F4 CB 41 B4 0D 35 1C 67 F4 CB 41 64 64 69 6E 67 20 61   ..A..5.g..A..5.g..Adding a
20 73 65 63 6F 6E 64 20 6E 6F 74 65 00 00 00 A1 00 01 01 01 01 01 01 01 03 01    second note..............
01 01 07 07 81 1D 55 00 00 0D 03 03 00 01 33 00 02 03 00 01 00 03 0B 41 B7 C9   ......U.......3........A..
15 BE AF 95 81 41 B7 C9 15 BE AF 95 81 54 65 6C 6C 20 79 6F 75 72 73 65 6C 66   .....A.......Tell yourself
20 65 76 65 72 79 64 61 79 20 68 6F 77 20 67 72 65 61 74 20 79 6F 75 20 61 72    everyday how great you ar
65 20 61 6E 64 20 79 6F 75 20 77 69 6C 6C 20 73 6F 6D 65 64 61 79 20 62 65 6C   e and you will someday bel
69 65 76 65 20 69 74 35 39 45 31 38 31 39 46 2D 34 35 46 36 2D 34 32 43 44 2D   ieve it59E1819F-45F6-42CD-
39 36 43 32 2D 41 32 39 36 43 46 45 43 33 35 44 34 64 0A 14 00 01 01 01 01 01   96C2-A296CFEC35D4d........
01 01 03 01 01 01 07 07 2B 55 00 00 0D 03 02 00 00 32 00 01 03 00 01 00 03 0A   ........+U.......2........
41 B7 C9 15 A7 37 8C 22 41 B7 C9 15 A7 37 8C 22 43 68 69 65 66 20 69 73 20 61   A....7."A....7."Chief is a
20 67 6F 64 21 31 46 31 39 42 34 36 45 2D 42 35 37 37 2D 34 34 30 37 2D 38 41    god!1F19B46E-B577-4407-8A
```

Custom Scripts

- Mari DeGrazia's SQLite Parser



```
C:\Users\FOR585\Desktop\SQLite Parser>sqlparse.py -f notes.sqlite -o notes_resul
ts.tsv

C:\Users\FOR585\Desktop\SQLite Parser>
```

Type	Offset	Length	Data
Free Block	19881	234	5U A 5gA 5gAdding a second noteU 3 AATell yourself everyday how great you are and you will someday believe it59E1819F-45F6-42CD-96C2-A296CFEC35D4
Unallocated	20496	3426	4>o Clean this messae and see if gmail resyncs it...
Free Block	23966	164	AAdding a second note just because I feel lie it. V Tell yourself everyday how great you are and you will someday believe it
Unallocated	73744	990	z xxbplist00T$topX$objectsX$versionY$archiverTroot U$null ZNS.objectsV$classX$classesZ$classname\NSMutableSetUNSSetXNSObject\NSMutableSet_NSKeyedArchiver(25:<@FKV]^`eny}bplist00T$topX$objectsX$versionY$archiverTroot U$null ZNS.objectsV$classX$classesZ$classname\NSMutableSetUNSSetXNSObject\NSMutableSet_NSKeyedArchiver(25:<AGLW^`bdfktbplist00T$topX$objectsX$versionY$archiverTroot U$null ZNS.objectsV$classX$classesZ$classname\NSMutableSetUNSSetXNSObject\NSMutableSet_NSKeyedArchiver(25:<@FKV]^`eny}

References, Sources and Suggested Reading

- http://www.zdziarski.com/blog/wp-content/uploads/2013/05/iOS-Forensic-Investigative-Methods.pdf
- www.az4n6.blogspot.com
- https://viaforensics.com/blog/
- http://www.sleuthkit.org/
- Practical Mobile Forensics –Bommisetty, Mahalik, Tamma
- www.smarterforensics.com
- https://code.google.com/p/lime-forensics/

Questions

Heather Mahalik

Basis Technology

www.basistech.com

hmahalik@basistech.com

Twitter: @heathermahalik