



What One Digital Forensics Expert
Found On Hundreds of Hard Drives,
iPhones and Android Devices

© 2016 Monterey Technology Group Inc.

Sponsored by



Thanks to

• Made possible by



Data Recovery On Devices Purchased On EBay

When is erase is not really an erase...

Just How Do They Get There?

- Bankruptcy Proceedings
 - Do you really thing the bankruptcy court cares about your data?
 - If it cost money to do something rest assured it will not be done
- Equipment Liquidators
 - Again... If it cost money to do something rest assured it will not be done
- Employees
 - Make a few extra bucks selling discarded equipment

How Do you Retrieve The Data? (1)

- On a hard disk sold on eBay where nothing was done to the disk the data is simply readily available with no effort required to recover it
 - Yes some of the drives purchased on eBay were simply removed from a PC and nothing at all was done to protect the data that was on the disk

How Do you Retrieve The Data? (2)

- On a disk where the data was only erased you simply use a free tool like FTK Imager to recover the data
 - If the file allocation table was not overwritten by i.e. reformatting it still contains the "map" to all files and they easily retrieved from unallocated space
 - FTK shows all deleted files with a red X as the first character in the file name
 - You simply right click on the file and save it



Blanco File

- Erase Unwanted Files Easily, Quickly and Permanently with Blanco File
- As a participant in today's webinar, we're giving you Blanco File at 25% off! Just use Promo Code: **ULTIMATE25**
- <http://www.blanco.com/en/buy>

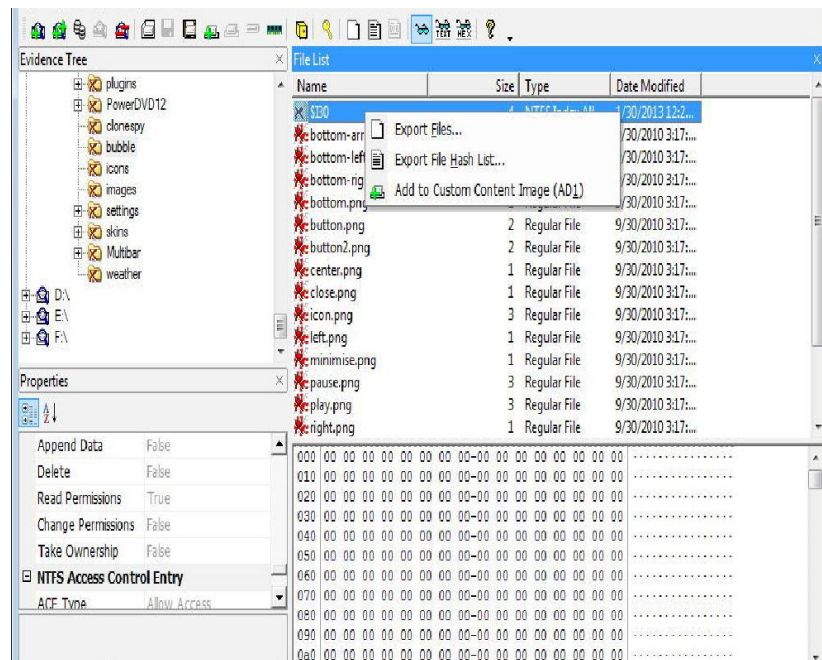
*Promotion expires on May 31, 2016.



Blanco File

- Demo by Tim Tutton

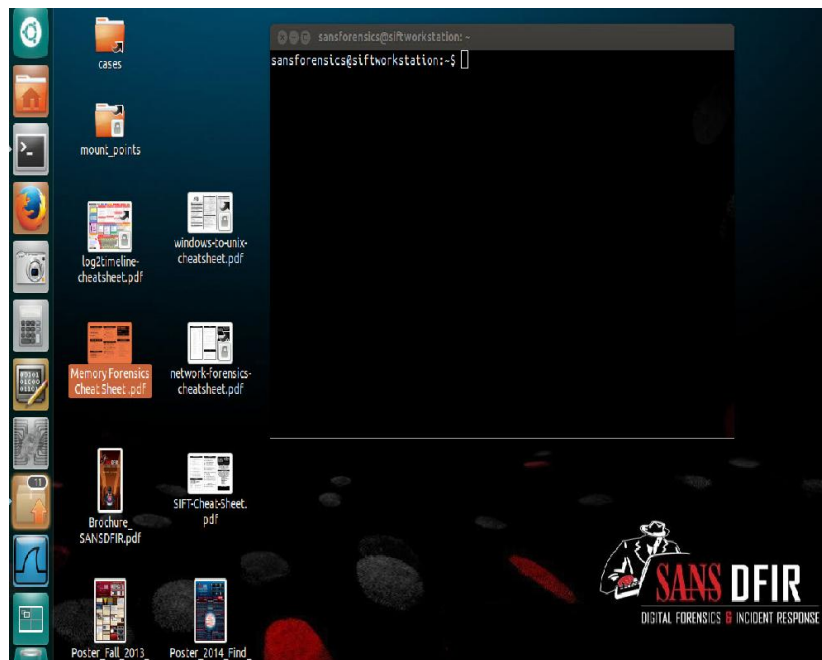
Recover Deleted Files - FTK Imager



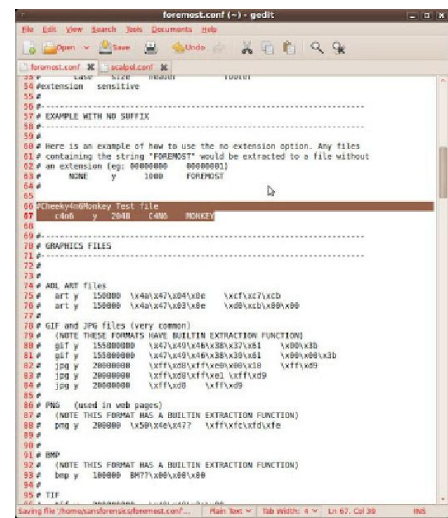
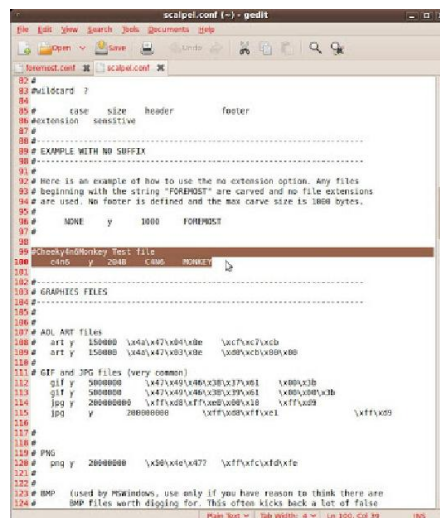
How Do you Retrieve The Data? (3)

- On a disk that was re-formatted you simply “carve” the data from unallocated space using a free tool contained in the SANS SIFT toolkit called Scapel / Foremost or any of the many alternatives
- Most every file has a known start called the Header and an end called the Footer
- You simply search unallocated space for the respective Header and carve the file out until you reach the Footer....

SANS SIFT Workstation



Carve All Files Based On Their Header And Footer Values



What About A Wiped Disk?

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
779e0411203	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411225	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411232	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411243	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411264	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411292	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411295	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411322	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411323	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411344	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411363	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411375	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411392	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411403	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411424	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411443	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411455	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411472	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411483	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411504	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411523	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411535	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411552	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411563	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411584	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411603	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411625	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411632	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411643	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411664	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411683	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411695	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411722	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411725	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411744	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411763	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411775	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00
779e0411792	00	0c	30	00	c0	00	03	00	c0	00	03	00	3c	00	c0	00

Sector 15332: 115 of 1953525 68

Offset:

779e0411200

Blancco 5

- Demo by Tim Tutten


Android Devices

- Data retrieval on an Android device is quite easy using free tools such as Magnet Acquire

Image With Magnet Acquire

OPTIONS

CHOOSE YOUR DEVICE

 ANDROID

Make	LGE
Model	LG-D852
OS	4.4.2
Privileged Access	Yes

[The device I'm looking for isn't showing up](#)

PROVIDE FEEDBACK

NEXT

Process The Image



What Can You Recover?

- A treasure trove of information is stored in an Android and can be recovered
- Logical analysis can provide:
 - Browser history, Call Logs, Contact Methods, External Image Media (meta data), External Image Thumbnail Media (meta data), External Media, Audio, and Misc. (meta data), External Videos (meta data), MMS, MMS Parts (includes full images sent via MMS), Organizations, People, SMS, List of all applications installed and version, Contacts – Extensions, Groups, Phones, Settings

What About A Factory Reset?

- A factory reset on an unencrypted Android device does not by default properly overwrite data.
- Hence, literally all user data is recoverable using the carving methods described earlier
- To get rid of the users data you need to encrypt the phone first and then do the factory reset to delete the key used for encryption
 - There is still a risk data could be recovered if the key is guessed

What About The iPhone

- On early iPhones like the iPhone 4 encryption was not mandatory
- Around version 5 recovery of deleted data was made easy as Apple did a poor job of properly handling the encryption key
- After version 5 Apple began to hide the key in hardware but exploits were discovered to reveal the key and allow access to the phones data
 - Remember the recent FBI case...

What About The iPhone

- A treasure trove of information is stored in the iPhone
 - For starters:
 - User accounts
 - Contacts
 - Call history
 - SMS Messages
 - Messages Google Mail and Yahoo! Messenger
 - Skype Chat
 - History of Google Maps, stored in iPhone and iPad
 - Dynamic Dictionary
 - Automatic Screen Shots
 - Most apps store data so the list simply goes on and on and on

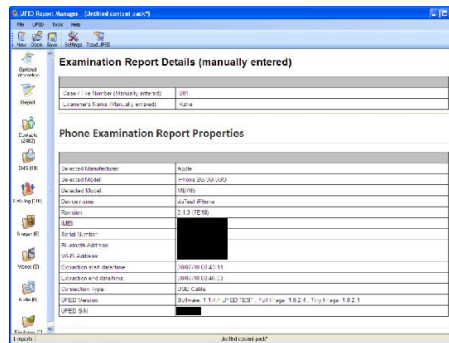
What About The iPhone

- Several tools can image a iPhone
- Simply put they are easy to use and works well with all of my other tools i.e. SANS SIFT, FTK, Net Analysis, IEF.....



Extract Phone Data Option

- You get what you would expect in a well formatted report
 - Call logs, Phone Book, SMS, Videos, Audio / Music



The File Dump Option (1)

- Not to overly simplify it, when you use the file system dump it mounts the file system and does a file by file copy while it also maintains the file system hierarchy.
- Software is great for reporting on the files system dump but it also works well when you import the data structure in and analyze it in tools like SIFT or FTK

The File Dump Option (2)

- What can you expect to get?
 - SMS, Contacts, Call Logs, MMS, Notes, Applications, Voice Mails, Calendar, Bluetooth, GPS, Notes, Bookmarks, Skype, Chat, Cookies, Bookmarks, Facebook
 - You also get lots and lots of plist files that contain a large amount of personal data

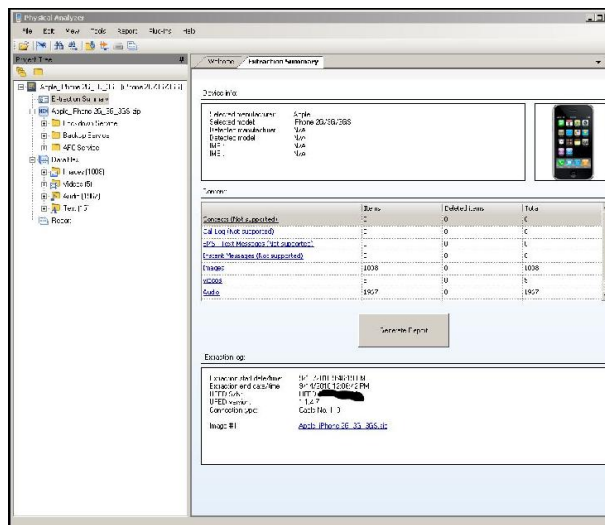
The File Dump Option (3)

- What your not going to get?
 - Well your not going to get email as it is separately encrypted and your not going to get some deleted files
 - let me clarify - if the deleted entry is only marked as deleted in the respective database then yes as the file is not really deleted you will get the entry.... I am talking about really deleted files from the storage media

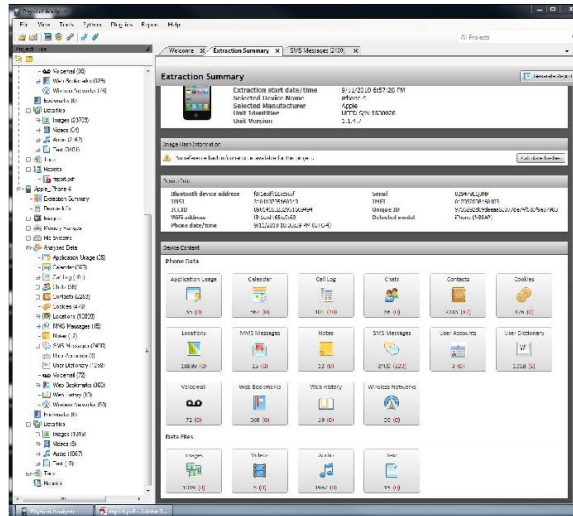
The File Dump Option (4)

Apple_iPhone 2G_3G_3GS	9/14/2010 12:06 PM	UFED Dump	1 KB
Apple_iPhone 2G_3G_3GS.z01	9/13/2010 11:00 PM	Z01 File	1,048,576 KB
Apple_iPhone 2G_3G_3GS.z02	9/14/2010 12:09 AM	Z02 File	1,048,576 KB
Apple_iPhone 2G_3G_3GS.z03	9/14/2010 1:18 AM	Z03 File	1,048,576 KB
Apple_iPhone 2G_3G_3GS.z04	9/14/2010 2:27 AM	Z04 File	1,048,576 KB
Apple_iPhone 2G_3G_3GS.z05	9/14/2010 3:36 AM	Z05 File	1,048,576 KB
Apple_iPhone 2G_3G_3GS.z06	9/14/2010 4:45 AM	Z06 File	1,048,576 KB
Apple_iPhone 2G_3G_3GS.z07	9/14/2010 5:53 AM	Z07 File	1,048,576 KB
Apple_iPhone 2G_3G_3GS.z08	9/14/2010 7:02 AM	Z08 File	1,048,576 KB
Apple_iPhone 2G_3G_3GS.z09	9/14/2010 8:11 AM	Z09 File	1,048,576 KB
Apple_iPhone 2G_3G_3GS.z10	9/14/2010 9:20 AM	Z10 File	1,048,576 KB
Apple_iPhone 2G_3G_3GS.z11	9/14/2010 10:29 AM	Z11 File	1,048,576 KB
Apple_iPhone 2G_3G_3GS.z12	9/14/2010 11:38 AM	Z12 File	1,048,576 KB
Apple_iPhone 2G_3G_3GS	9/14/2010 12:06 PM	zip Archive	451,255 KB

The Original File Dump Option



The Physical Analyzer



Application Usage Details

[illegible]

Call Log Including Deleted

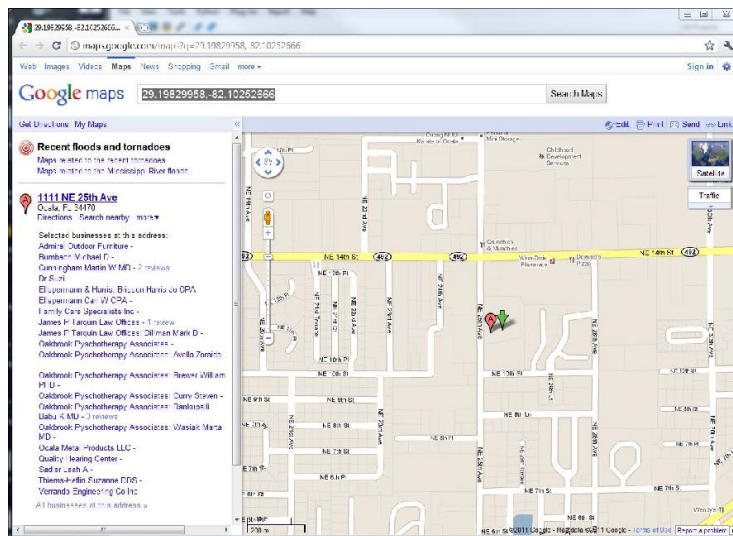
[illegible]

Skype Including Deleted

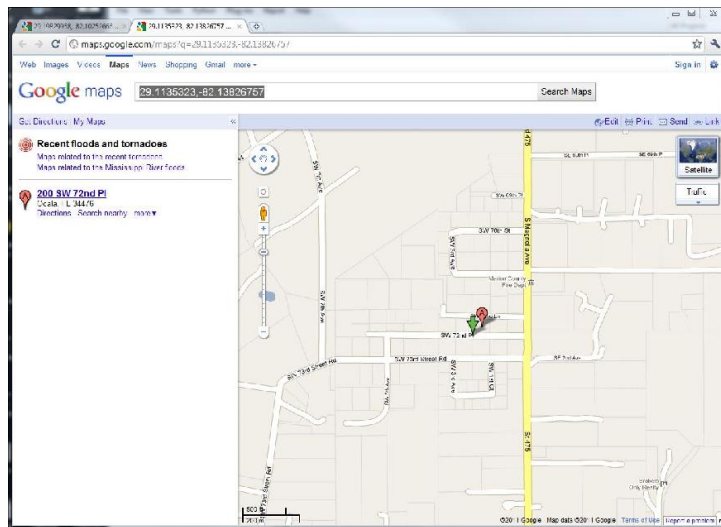
Report Details for WiFi

#	SSID	BSSID	Signal
1	3574-88-17-4764	3574-88-17-4764	100%
2	00-00-00-00-00-00	00-00-00-00-00-00	100%
3	00-00-00-00-00-00	00-00-00-00-00-00	100%
4	00-00-00-00-00-00	00-00-00-00-00-00	100%
5	00-00-00-00-00-00	00-00-00-00-00-00	100%
6	00-00-00-00-00-00	00-00-00-00-00-00	100%
7	00-00-00-00-00-00	00-00-00-00-00-00	100%
8	00-00-00-00-00-00	00-00-00-00-00-00	100%
9	00-00-00-00-00-00	00-00-00-00-00-00	100%
10	00-00-00-00-00-00	00-00-00-00-00-00	100%
11	00-00-00-00-00-00	00-00-00-00-00-00	100%
12	00-00-00-00-00-00	00-00-00-00-00-00	100%
13	00-00-00-00-00-00	00-00-00-00-00-00	100%
14	00-00-00-00-00-00	00-00-00-00-00-00	100%
15	00-00-00-00-00-00	00-00-00-00-00-00	100%
16	00-00-00-00-00-00	00-00-00-00-00-00	100%
17	00-00-00-00-00-00	00-00-00-00-00-00	100%
18	00-00-00-00-00-00	00-00-00-00-00-00	100%
19	00-00-00-00-00-00	00-00-00-00-00-00	100%
20	00-00-00-00-00-00	00-00-00-00-00-00	100%
21	00-00-00-00-00-00	00-00-00-00-00-00	100%
22	00-00-00-00-00-00	00-00-00-00-00-00	100%
23	00-00-00-00-00-00	00-00-00-00-00-00	100%
24	00-00-00-00-00-00	00-00-00-00-00-00	100%
25	00-00-00-00-00-00	00-00-00-00-00-00	100%
26	00-00-00-00-00-00	00-00-00-00-00-00	100%
27	00-00-00-00-00-00	00-00-00-00-00-00	100%
28	00-00-00-00-00-00	00-00-00-00-00-00	100%
29	00-00-00-00-00-00	00-00-00-00-00-00	100%
30	00-00-00-00-00-00	00-00-00-00-00-00	100%
31	00-00-00-00-00-00	00-00-00-00-00-00	100%
32	00-00-00-00-00-00	00-00-00-00-00-00	100%
33	00-00-00-00-00-00	00-00-00-00-00-00	100%
34	00-00-00-00-00-00	00-00-00-00-00-00	100%
35	00-00-00-00-00-00	00-00-00-00-00-00	100%
36	00-00-00-00-00-00	00-00-00-00-00-00	100%
37	00-00-00-00-00-00	00-00-00-00-00-00	100%
38	00-00-00-00-00-00	00-00-00-00-00-00	100%
39	00-00-00-00-00-00	00-00-00-00-00-00	100%
40	00-00-00-00-00-00	00-00-00-00-00-00	100%
41	00-00-00-00-00-00	00-00-00-00-00-00	100%
42	00-00-00-00-00-00	00-00-00-00-00-00	100%
43	00-00-00-00-00-00	00-00-00-00-00-00	100%
44	00-00-00-00-00-00	00-00-00-00-00-00	100%
45	00-00-00-00-00-00	00-00-00-00-00-00	100%
46	00-00-00-00-00-00	00-00-00-00-00-00	100%
47	00-00-00-00-00-00	00-00-00-00-00-00	100%
48	00-00-00-00-00-00	00-00-00-00-00-00	100%
49	00-00-00-00-00-00	00-00-00-00-00-00	100%
50	00-00-00-00-00-00	00-00-00-00-00-00	100%

Cell Towers -> Google Maps



WiFi to Google Maps



Lets Not Forget GPS

Locations (18899)

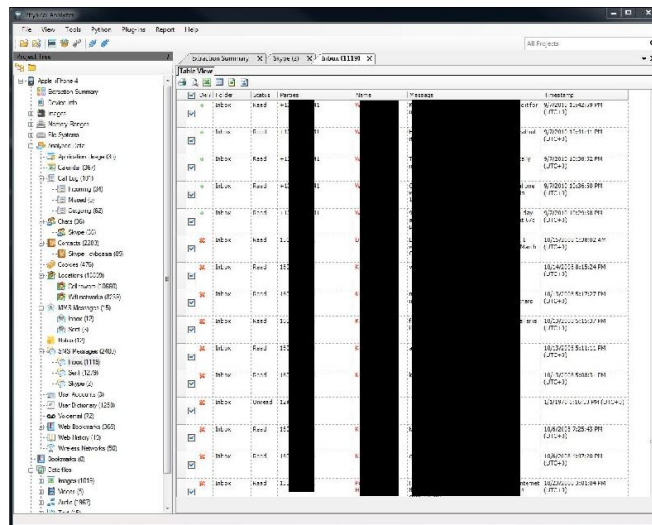
[Open in Google Earth](#) [Open in Google Maps](#)

Cell towers (10660)

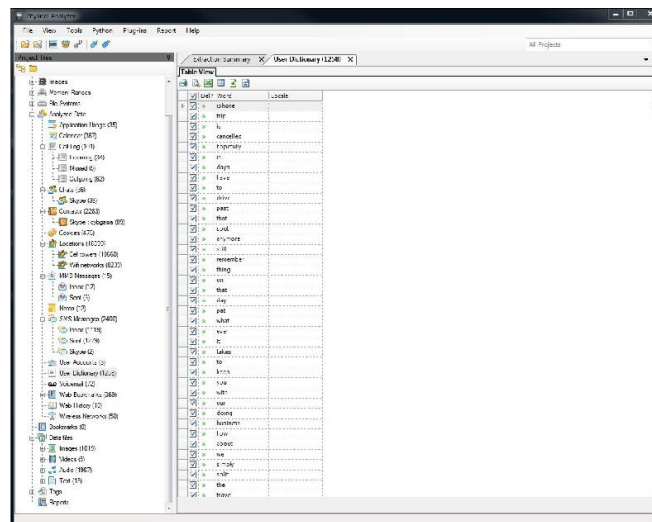
[Open in Google Earth](#) [Open in Google Maps](#)

#	Position	Info	Del?
1	(29.19538, 82.10233)	Description: MCC=310 MNC=410 LAC=27538 CI=230156703 Time: 6/26/2010 10:00:47 PM	
2	(29.18863, 82.06177)	Description: MCC=310 MNC=410 LAC=27733 CI=33278 Time: 6/26/2010 10:00:47 PM	
3	(28.65308, 82.15522)	Description: MCC=310 MNC=410 LAC=27397 CI=230938459 Time: 6/30/2010 3:14:51 PM	

Shows
Deleted Items
i.e. SMS



Dynamic
Dictionary -
Hmmm



Browser History

[illegible]

Works with my
SANS SIFT
Tools

The image displays two screenshots of a web browser showing the 'Skype Log Reports' interface.

Top Screenshot: The browser window shows the 'Skype Log Reports' page. The title bar indicates the URL is 'http://192.168.1.100:8080/SkypeLogReports/'. The page content includes a large heading 'Skype Log Reports' and a list of links on the left side: 'Show Home', 'Show Profile', 'Show Chat', 'Show Call', 'Show SMS Messages', 'Show Messages', 'Show View on Facebook', 'Show View on Twitter', and 'Show View on LinkedIn'.

Bottom Screenshot: The browser window shows a detailed report titled 'SKYPE TRANSACTION' for 'user name1' on '06/06/2010'. The report includes a table with columns: 'DATE', 'TIME', 'FILE', 'TRANSFER', and 'Sequence Number'. The table lists various transactions, including 'Chat Message', 'Call Message', and 'Call Session'. Some rows are redacted with a black box.

DATE	TIME	FILE	TRANSFER	Sequence Number
2010/06/06	10:10:00		0	
2010/06/06	10:10:00		202	
2010/06/06	10:10:00		203	
2010/06/06	10:10:00		204	
2010/06/06	10:10:00		205	
2010/06/06	10:10:00		206	
2010/06/06	10:10:00		207	
2010/06/06	10:10:00		208	
2010/06/06	10:10:00		209	
2010/06/06	10:10:00		210	
2010/06/06	10:10:00		211	

Works with NetAnalysis

[illegible]

ULTIMATE
WINDOWS
SECURITY
.COM

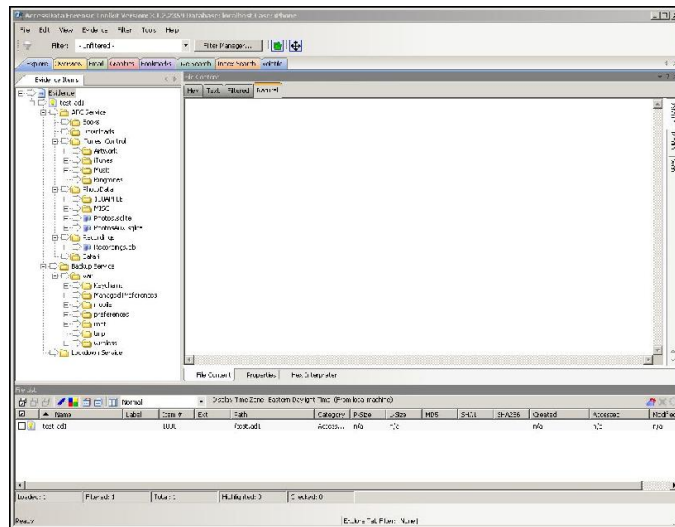


blanca

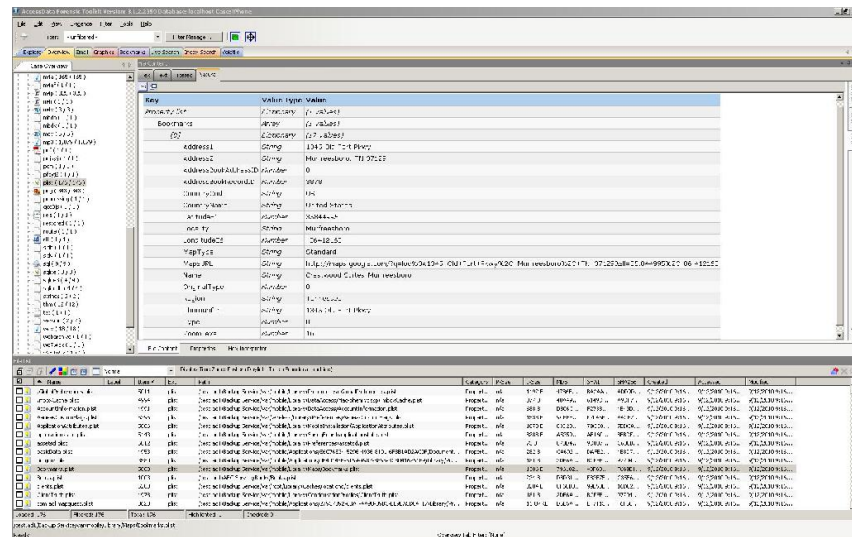
Works with
SQLiteSpy

The screenshot displays the QlikView Desktop application. On the left, the 'Data Model' pane shows a hierarchy: 'main' containing 'Table1 (0)', which includes fields like '7_MFANATZ', 'Z_7EMARKEY', 'ZACCOUNT', 'ZNEXTD', 'ZNOTE', 'ZNOTEBODY', 'ZNOTECHANGE', 'ZPROPERTI', and 'ZSTORE'. Below this, 'Collations (7)' is listed. The main workspace shows a data table with columns 'DIRECTIONS...', 'ZNOTE', '7Q IN', and '7M IN'. The table contains several rows of data, some of which are redacted with black boxes. The status bar at the bottom indicates 'Time: 0.42 ms' and '12 returns'.

Works with
FTK 3.X



Use FTK Plist View Capability



Is a Logical Analysis Enough? (1)

- For many a logical image that represents the logical file system as it appears to the operating system and it's analysis is sufficient
- A logical image does include both allocated and unallocated space hence deleted files can be recovered through carving

Is a Logical Analysis Enough? (2)

- Some information is maintained in databases on the iPhone and when deleted actually still exists but is simply marked in the database as deleted

Is A Logical Analysis Enough? (3)

- No longer seen by the user in the applications GUI hence some “deleted” information can in fact be recovered in a logical extraction.
- So yes a logical analysis may provide a significant amount of data but... it is of course not equivalent to a physical analysis, more about that in a few minutes

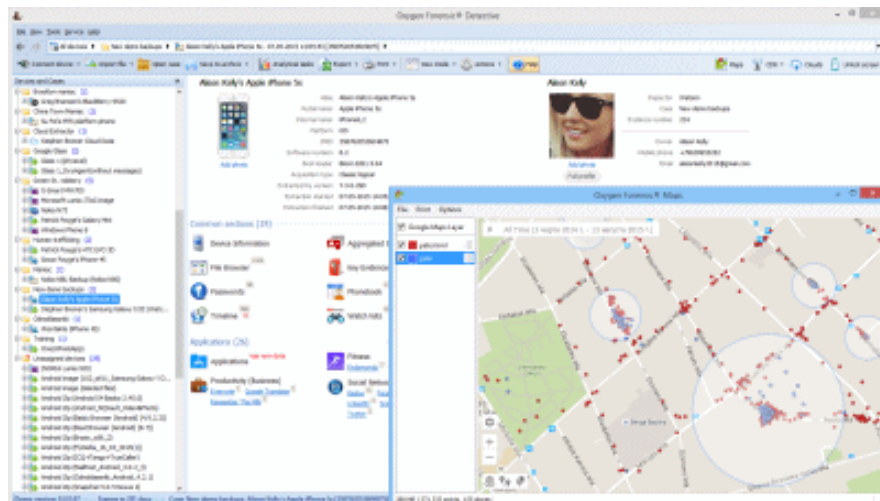
What is a Physical Analysis

- For starters a Physical image is a bit by bit copy of the entire physical data store including that which is outside of the operating systems view of the storage media's file structure.
 - A typical physical analysis allows you to access portions of the storage media that may not currently be in use by the phone. Now you can carve files from both allocated and unallocated space across all available storage media

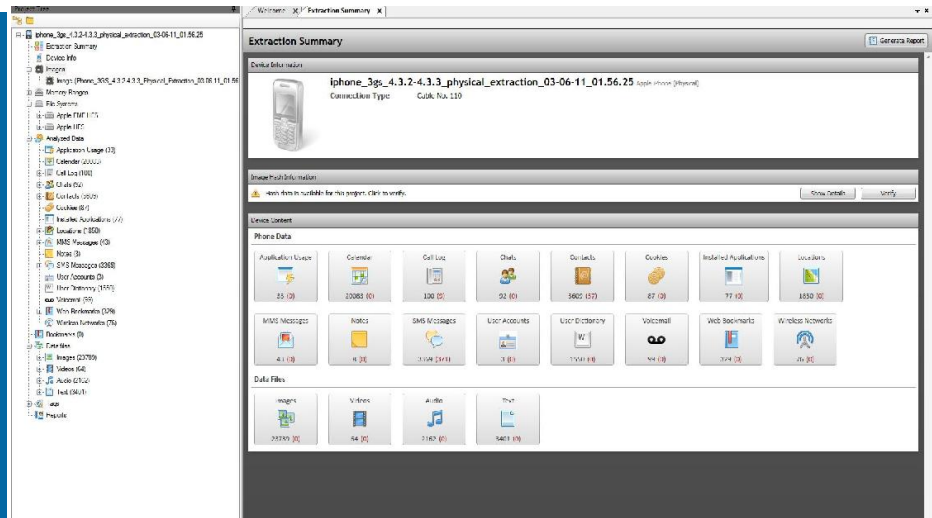
Now let's get Physical

- Significantly more data is typically found with a physical image such as deleted files including images and other user data that effectively needs to be carved from the physical image (includes all storage media both allocated and unallocated space including that which is outside the scope of the file system) just like on a PC or server hard disk.

Physical Analysis iPhone



Physical Analysis ROCKS!

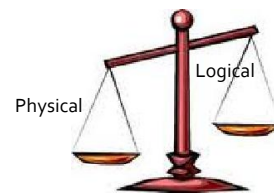


Logical vs. Physical (1)

- What did I get in my Physical Analysis vs. Logical Analysis
 - Additional evidence recovered included:
 - 22,000+ images
 - 59 videos
 - 1000+ audio files
 - 16,000+ locations
 - 60+ chats (included Facebook and Skype)
 - 30+ MMS
 - 3300+ text files
 - 36 Mac Mail Emails
 - 22 Gmail Emails
- Python Scripts to carve data are a big differentiator in Mobile device forensics!

Logical vs. Physical (2)

- Doing a logical analysis you have to consider that you are really only getting part of the evidence. Simply put in my opinion a thorough analysis requires a physical extraction and its more complete examination...



Final Thoughts

- Mobile Phone Data Recovery is not for everyone as it is an expensive undertaking to be able to cover the many phones in use today
 - I have done everything from throw away Samsung's, Blackberry's, Droids, iPhones and iPads without issue
- Apple (and everyone else) constantly makes changes that literally break any tool used to analyze their products i.e. the mandatory encryption in iPhone 4.x
- Physical Analysis is the future of Mobile Device data recovery

Blanco

- Demo by Tim Tuten
 - Blanco Mobile
 - Blanco Management Console

Final Thoughts

- Remember - Erasing, re-formatting, re-installing the OS, a factory reset and yes even encryption can still leave your data at risk
- If you are not overwriting the data across all physical storage media there is a risk that your data will be recovered



Questions?

Thanks for coming!

Contact:

phenry@vnetsecurity.com

phenry@sans.org