



# OPEN SOURCE TOOLS FOR MOBILE FORENSICS

MATTIA EPIFANI

SANS EUROPEAN DIGITAL FORENSICS SUMMIT

PRAGUE, 6 OCTOBER 2013



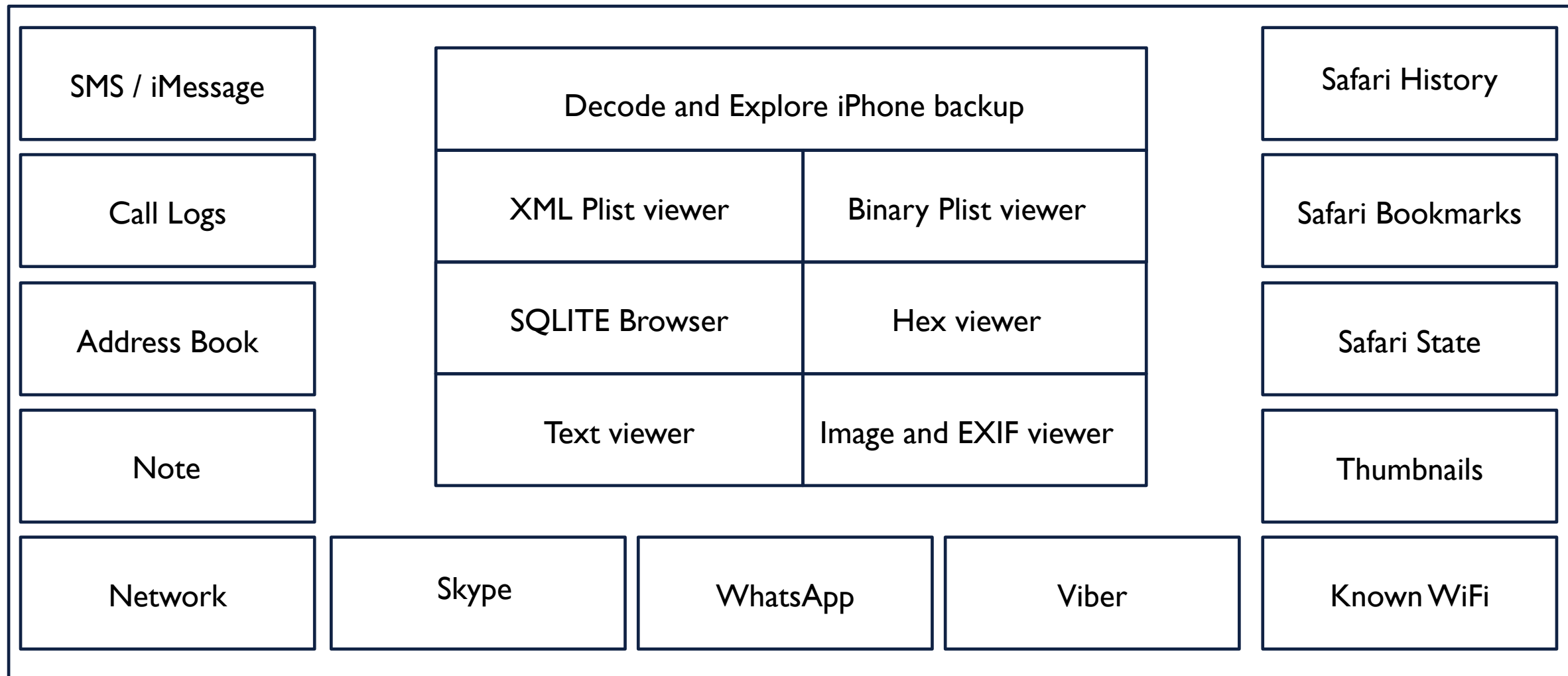
# SUMMARY

- Introduction to 3 open source tools for Mobile and Computer Forensics
- Developed by Italian teams
- iPhone Backup Analyzer
- WhatsApp Xtract
- Skype Xtractor

# IPHONE BACKUP ANALYZER

- Open source tool for iPhone Backup analysis
- Python 2.7 with QT graphical interface
- Multi platform (Windows, Linux, Mac OS X)
- **Main module** (decoder and viewers) and **Plugins**
  
- **Mario Piccinelli** (Brescia University) – Lead Developer
  - Mattia Epifani, Sandro Rossetti, Fabio Sangiacomo, Nicodemo Gawronsky
  - **We need plugin developers! Join us!**
  
- **<http://www.ipbackupanalyzer.com>**

# IPHONE BACKUP ANALYZER



# IPHONE BACKUP ANALYZER – MAIN WINDOW

The screenshot displays the main interface of the iPhone Backup Analyzer (iPBA 2). The window is titled "iPBA 2" and features a menu bar with "File", "Plugins", and "Reports". Below the menu bar is a toolbar with icons for file operations. The interface is divided into several sections:

- Backup Info:** Displays device details such as Unique Identifier, Device Name (iPhone4 del Mario), Last Backup Date (2013-02-19 09:31:08), Phone Number (+39...), iTunes Version (11.0.1), Serial Number, Display Name (iPhone4 del Mario), IMEI, ICCID, Product Version, Product Type (iPhone3,1), and GUID.
- Backup filesystem:** A table listing files from the backup, including image files (IMG\_0103.JPG to IMG\_0171.JPG) and a video file (IMG\_0122.MOV).
- Selected file info:** Provides detailed metadata for the selected file (IMG\_0154.JPG), including Element type, Permissions, Data hash, User id, Group id, Last modify time, Last access time, Creation time, File Key, and Element properties (from mddb file).
- Analysis Tools:** Several windows are open for analysis:
  - Status.plist - Hex editor:** Shows a hex dump of the file's data.
  - IMG\_0154.JPG - Image Viewer:** Displays a preview of the image.
  - Info.plist - Plist Viewer:** Shows the metadata dictionary for the image, including Target Identifier, Product Type (iPhone3,1), Device Name, iBooks Data 2, Build Version, Last Backup Date, Phone Number, Sync Settings, and Unique Identifier.

At the bottom of the main window, there is a note: "(right click on file to show appropriate viewers)".

# IPHONE BACKUP ANALYZER – SQLITE AND PLIST

Qt call\_history.db - SQLite Browser

<< Records 1-100 >>

Name	#
_SqliteDatabaseProperties	17
call	100
sqlite_sequence	2
data	5

ROWID	address	date	duration	flags	IN	
1	7009	+39[REDACTED]	1363523109	222	5	-1
2	7010	+39[REDACTED]	1363537927	81	4	-1
3	7011	+39[REDACTED]	1363542244	79	5	-1
4	7012	+39[REDACTED]	1363543070	24	1507332	-1
5	7013	+39[REDACTED]	1363543493	163	5	-1
6	7014	+39[REDACTED]	1363543997	0	1769477	51
7	7015	+39[REDACTED]	1363544013	0	1769477	51
8	7016	+39[REDACTED]	1363544043	0	1769477	51
9	7017	+39[REDACTED]	1363544116	0	1769477	51
10	7018	+39[REDACTED]	1363544190	0	1769477	51
11	7019	+39[REDACTED]	1363544234	0	1769477	51

Qt Manifest.plist - Plist Viewer

Data

- <dict>
  - Version  
9.1
  - BackupKeyBag
  - Lockdown
    - <dict>
  - WasPasscodeSet  
True
  - Applications
    - <dict>
  - IsEncrypted  
False
  - SystemDomainsVersion  
16.0
  - Date  
2013-04-02 07:35:32.847069

# IPHONE BACKUP ANALYZER – CALLS AND MESSAGES

Qt Call History

Calls list

	ID	Address	Date	Duration	Flags	Name
1	6737	[REDACTED]	2013-02-01 19:15:51	0:00:00	Incoming	
2	6738	[REDACTED]	2013-02-01 22:34:43	0:14:27	Outgoing	[REDACTED]
3	6739	[REDACTED]	2013-02-02 12:14:19	0:00:14	Outgoing	[REDACTED]
4	6740	[REDACTED]	2013-02-02 14:02:26	0:02:13	Incoming	
5	6741	[REDACTED]	2013-02-02 16:18:49	0:06:14	Outgoing	
6	6742	[REDACTED]	2013-02-02 20:08:23	0:10:26	Outgoing	[REDACTED]
7	6743	[REDACTED]	2013-02-02 21:12:20	0:00:00	Outgoing	[REDACTED]
8	6744	[REDACTED]	2013-02-02 21:14:14	0:02:50	Outgoing	[REDACTED]
9	6745	[REDACTED]	2013-02-02 21:21:11	0:00:00	Outgoing	
10	6747	[REDACTED]	2013-02-03 14:49:03	0:12:27	Incoming	

Calls data

Qt Messages Browser

Messages from last reset:  
Incoming: 3185  
Outgoing: 1684  
Lifetime messages:  
Incoming: 3185  
Outgoing: 1684  
Counter:  
Last reset: 0

Chat

- +39 [REDACTED]
- +39 [REDACTED]
- +39 [REDACTED]
- +39 [REDACTED]
- 4333
- +39 [REDACTED]
- +39 [REDACTED]
- oneclub
- +39 [REDACTED]
- 3informa
- +39 [REDACTED]

oneclub

	Date	Text
1	2010-01-06	
2	Received on: 2010-01-06 10:07:55	Musica, Giochi, Chat e tanto altro...GRATIS per una settimana su OneClub! <a href="http://treclub.tre.it/p-3club/H3GMSCHP/fr">http://treclub.tre.it/p-3club/H3GMSCHP/fr</a>

# IPHONE BACKUP ANALYZER – WHATSAPP AND SKYPE

Qt WhatsApp Browser

Contacts Chats

	Contact Name	Contact JID	# Msg	# Unread	La
1	[REDACTED]	39[REDACTED]@s.whatsapp.net	7	0	2012
2	[REDACTED]	39[REDACTED]@s.whatsapp.net	1	0	2012
3	[REDACTED]	39[REDACTED]@s.whatsapp.net	1	0	2012
4	[REDACTED]	39[REDACTED]@s.whatsapp.net	2	0	2012

From Msg Date

4	[REDACTED]@s.whatsapp.net	2012-05-29 20:16:58	[REDACTED]
5	Me	2012-05-23 18:00:09	Occheri :-)
6	[REDACTED]@s.whatsapp.net	2012-05-23 16:55:41	[REDACTED]
7	Me	2012-10-09 12:55:09	[REDACTED]

Qt Skype Browser

Contacts Calls Chat Messages File Transfers Group Chats Voice

Timestamp	Remote	Status
05-06-2012 19:10:30	[REDACTED]	Cancelled at Origin
05-06-2012 19:11:17	+39[REDACTED]	Accepted
06-06-2012 17:13:13	+39[REDACTED]	Accepted
06-06-2012 18:54:56	+39[REDACTED]	Accepted
06-06-2012 19:03:42	+39[REDACTED]	Accepted
07-06-2012 15:00:49	+39[REDACTED]	Accepted
07-06-2012 15:02:49	+39[REDACTED]	Accepted

Field	Value
Timestamp	06-06-2012 18:54:56
Duration	00:08:16
Status	Accepted
Call type	Unknown (4)
Host identity	[REDACTED]
Remote host	+39[REDACTED]



# WHATSAPP XTRACT

- Open Source tool for WhatsApp extraction and analysis
- Python 2.7
- Multi platform (Windows, Linux, Mac OS X)
- By now supports iOS and Android
  
- **Fabio Sangiacomo** (Genoa University) – Lead Developer
  - Mattia Epifani, Francesco Picasso, Marco Scarito
  - **We need help to improve support (Blackberry, Windows Phone, Symbian, etc.)**
  
- **<http://blog.digital-forensics.it/2012/05/whatsapp-forensics.html>**
- **<http://code.google.com/p/hotoloti/>**

# WHATSAPP XTRACT – IOS TABLES

Tables

- ZWACONTACT
  - Fields
    - Z\_PK
    - Z\_ENT
    - Z\_OPT
    - ZABUSERID
    - ZSORT
    - ZSECTION
    - ZFIRSTNAME
    - ZFULLNAME
    - ZIMAGEHASH
    - ZINDEXNAME
    - ZTOKENS
- ZWACONTACTSECTION
- ZWAFAVORITE
- ZWAPHONE
  - Fields
    - Z\_PK
    - Z\_ENT
    - Z\_OPT
    - ZCONTACT
    - ZFAVORITE
    - ZSTATUS
    - ZLABEL
    - ZPHONE
    - ZWHATSAPPID

ZWASTATUS

- Fields
  - Z\_PK
  - Z\_ENT
  - Z\_OPT
  - ZPHONE
  - ZDATE
  - ZPICTUREDATE
  - ZPICTUREID
  - ZPICTUREPATH
  - ZTEXT
  - ZWHATSAPPID
- Z\_METADATAA
- Z\_PRIMARYKEY

← Contacts.sqlite

ChatStorage.sqlite →

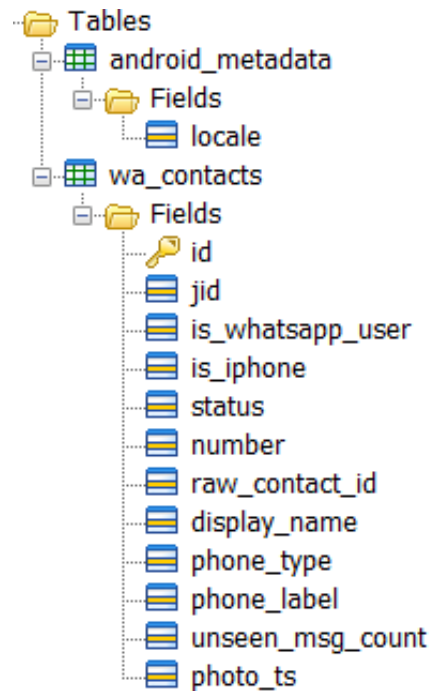
Tables

- ZWABLACKLISTITEM
- ZWACHATPROPERTIES
- ZWACHATSESSION
  - Fields
    - Z\_PK
    - Z\_ENT
    - Z\_OPT
    - ZCONTACTABID
    - ZDELETED
    - ZMESSAGECOUNTER
    - ZUNREADCOUNT
    - ZGROUPINFO
    - ZLASTMESSAGE
    - ZPROPERTIES
    - ZLASTMESSAGEDATE
    - ZCONTACTJID
    - ZLASTMESSAGETEXT
    - ZPARTNERNAME
    - ZSAVEDINPUT
- ZWAGROUPINFO
  - Fields
    - Z\_PK
    - Z\_ENT
    - Z\_OPT
    - ZSTATE
    - ZCHATSESSION
    - ZLASTMESSAGEOWNER
    - ZCREATIONDATE
    - ZSUBJECTTIMESTAMP
    - ZOWNERJID
    - ZPICTUREID
    - ZPICTUREPATH
    - ZSUBJECTOWNERJID
- ZWAGROUPMEMBER
- ZWAMESSAGEWORD
- Z\_METADATAA
- Z\_PRIMARYKEY
- ZWAMEDIAITEM
  - Fields
    - Z\_PK
    - Z\_ENT
    - Z\_OPT
    - ZFILESIZE
    - ZMEDIASAVED
    - ZMOVIEDURATION
    - ZMESSAGE
    - ZHACCURACY
    - ZLATITUDE
    - ZLONGITUDE
    - ZMEDIALOCALPATH
    - ZMEDIAURL
    - ZTHUMBNAILOCALPATH
    - ZVCARDNAME
    - ZVCARDSTRING
    - ZXMPPTHUMBPATH
    - ZTHUMBNAILDATA
- ZWAMESSAGE
  - Fields
    - Z\_PK
    - Z\_ENT
    - Z\_OPT
    - ZGROUPEVENTTYPE
    - ZISFROMME
    - ZMESSAGESTATUS
    - ZMESSAGETYPE
    - ZSORT
    - ZCHATSESSION
    - ZGROUPMEMBER
    - ZLASTSESSION
    - ZMEDIAITEM
    - ZMESSAGEGDATE
    - ZFROMJID
    - ZPUSHNAME
    - ZSTANZAID
    - ZTEXT
    - ZTOJID

# WHATSAPP XTRACT – ANDROID DECRYPTION

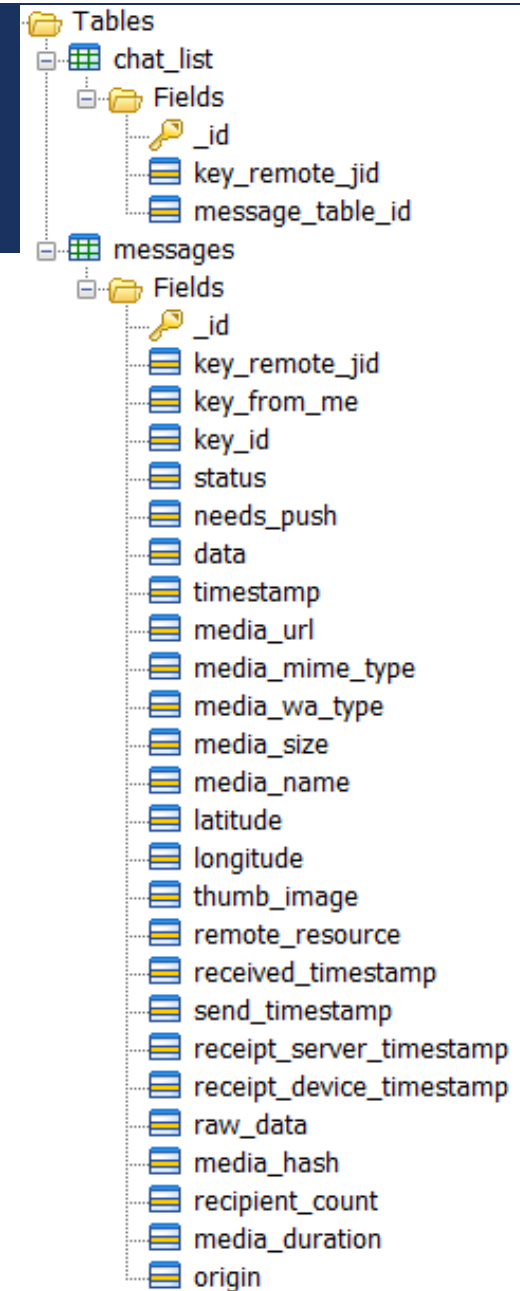
- WhatsApp Database Encryption Project (Corjens, Spruyt and Wieringa)  
[https://www.os3.nl/\\_media/2011-2012/students/ssn\\_project\\_report.pdf](https://www.os3.nl/_media/2011-2012/students/ssn_project_report.pdf)
- Vulnerability in the Android implementation of the 192-bit AES cypher
- It is possible to extract the **encryption key** from the software package  
***346a23652a46392b4d73257c67317e352e3372482177652c***
- Few code lines....and the database is decrypted!

# WHATSAPP XTRACT – ANDROID TABLES



← `wa.db`

`msgstore.db` →



# WHATSAPP XTRACT – REPORT

*Zena Forensics*



WhatsApp  Xtract



<u>PK</u>	<u>Contact Name</u>	<u>Contact ID</u>	<u>Status</u>	<u># Msg</u>	<u># Unread Msg</u>	<u>Last Message</u>
25	<a href="#">Alessio</a> █████	39339 █████@s.whatsapp.net	Disponibile	11	0	2012-05-10 15:47:00
17	<a href="#">C</a> █████	39339 █████-1327778754@g.us	N/A	316	0	2012-05-10 08:58:51
2	<a href="#">Eka</a> █████	39349 █████@s.whatsapp.net	Catanese sugnu!	222	0	2012-05-08 23:10:35
26	<a href="#">Marta</a> █████	39333 █████@s.whatsapp.net	Yup!☺	15	0	2012-05-07 15:20:17
15	<a href="#">M</a> █████	39339 █████-1327702706@g.us	N/A	3433	0	2012-05-07 13:36:22
8	<a href="#">L</a> █████	39339 █████@s.whatsapp.net	Disponibile	104	0	2012-05-07 00:43:01
33	<a href="#">Alice</a> █████	39339 █████@s.whatsapp.net	Cane portato a capodanno, portato tutto l'anno.	43	0	2012-05-06 22:42:45

# WHATSAPP XTRACT – REPORT

Chat session # 6665: 39334 [REDACTED]

<a href="#">PK</a>	<a href="#">Chat</a>	<a href="#">Msg date</a>	<a href="#">From</a>	<a href="#">Msg content</a>
4414	39334 [REDACTED]	2012-12-10 10:48:07	me	Confermo disponibilità x domani! Fammi sapere i dettagli.. se serve passo nel pomeriggio
4415	39334 [REDACTED]	2012-12-10 14:03:03	39334 [REDACTED]	Se vuoi fare un passò io sono in ufficio fino alle 1845 così ti spieghiamo un po'
4416	39334 [REDACTED]	2012-12-10 14:07:09	me	Ok, tra un'oretta o poco più arrivo xke alle 1730 dovrò scappare
4422	39334 [REDACTED]	2012-12-10 18:36:28	39334 [REDACTED]	Appuntamento ore 5 qui da noi! :-)) a domani!
4423	39334 [REDACTED]	2012-12-10 18:37:08	me	Ottimo! 🙌 a domani!
4424	39334 [REDACTED]	2012-12-10 19:06:05	39334 [REDACTED]	A domani!
6646	39334 [REDACTED]	2013-02-01 17:14:36	39334 [REDACTED]	   <a href="#">Image</a>
6647	39334 [REDACTED]	2013-02-01 17:14:29	me	Ok grazie!
6648	39334 [REDACTED]	2013-02-01 17:15:12	39334 [REDACTED]	<a href="#">Audio (online)</a>   <a href="#">Audio (offline)</a>
6650	39334 [REDACTED]	2013-02-01 17:15:53	39334 [REDACTED]	

# SKYPE XTRACTOR

- Open source tool for Skype analysis
- Both for computer and mobile version
- Python 2.7
- Multi platform (Windows, Linux)
  
- **Nicodemo Gawronski** (DEFT Team) – Lead Developer
  - Mattia Epifani, Davide Gabrini
  - **We need testers! Join us!**
  
- **<http://www.skypextractor.com/>**


# SKYPE XTRACTOR

- Extract
  - Account info
  - Contacts info
  - Calls
  - Chats
  - File transfer
  - Voice mails
  - Deleted and modified messages (Chat Sync)
  
- Report
  - CSV
  - HTML (filters included)
  - PDF (under development)



# SKYPE XTRACTOR

```
root# python skype.py --chatsync main.db
```



Skype Xtract [Accounts](#) [Calls](#) [Chat Summary](#) [Contacts](#) [File Transfers](#) [Group Chat](#) [Voice Mails](#) [Chat Sync](#)

This Database contains 84 messages. Click [Here](#) to view them all!

Show  entries Search all columns:

Chat	Participants	Total messages	From	To	Size (Kb)	Extracted from
<a href="#">#darth.vader404/\$3bc344545a701e6f_View</a>	darth.vader404 dr_zaius_42 john.seldon3 nicodemo.j.gawronski	14	26-07-2013 08:45:55	26-07-2013 09:14:06	8.63 Kb	#darth.vader404/\$3bc344545a701e6f
<a href="#">#darth.vader404/\$d1e9e1a1f8c86bf0_View</a>	darth.vader404 dr_zaius_42 nicodemo.j.gawronski oliverj.morton	3	26-07-2013 08:45:28	26-07-2013 08:45:32	5.47 Kb	#darth.vader404/\$d1e9e1a1f8c86bf0
<a href="#">darth.vader404_dr_zaius_42_View</a>	darth.vader404 dr_zaius_42	26	26-07-2013 08:40:30	26-07-2013 14:14:37	13.2 Kb	#darth.vader404/\$dr_zaius_42;a540c44927a671:#dr_zaius_42/\$darth.vader404;1083f17e243de6
<a href="#">darth.vader404_john.seldon3_View</a>	darth.vader404 john.seldon3	14	14-06-2013 13:28:11	14-06-2013 14:34:12	8.84 Kb	#darth.vader404/\$john.seldon3;e29660443c896
<a href="#">darth.vader404_nicodemo.j.gawronski_View</a>	#darth.vader404/\$nicodemo.j.gawronski;52e9e1a76118560e	21	14-06-2013 15:38:31	26-07-2013 15:14:01	12.25 Kb	#darth.vader404/\$nicodemo.j.gawronski;52e9e1a76118560e;#nicodemo.j.gawronski/\$darth.vader404;c5590e;#darth.vader404/\$nicodemo.j.gawronski;cf30aa;#darth.vader404/\$nicodemo.j.gawronski;cf8466
<a href="#">darth.vader404_oliverj.morton_View</a>	#darth.vader404/\$oliverj.morton;2951df834ff2cf5a	6	26-07-2013 08:41:23	26-07-2013 09:51:06	6.53 Kb	#darth.vader404/\$oliverj.morton;2951df834ff2c;#oliverj.morton/\$darth.vader404;5f4f3342a925c
<input type="text" value="Search Chat"/>	<input type="text" value="Search party"/>	84 <a href="#">View All</a>			32.31 Kb	

Showing 1 to 6 of 6 entries ◀ Previous Next ▶

Q&A?

# Mattia Epifani

- Digital Forensics Expert
- Owner @ REALITY NET – System Solutions
- President @ DFA Association
- CEH, CHFI, CCE, CIFI, ECCE, AME, ACE, MPSC

Mail [mattia.epifani@realitynet.it](mailto:mattia.epifani@realitynet.it)

Linkedin <http://www.linkedin.com/in/mattiaepifani>

