

# Mobile Forensics con Strumenti Open Source

30 novembre 2013, Udine




**Paolo Dal Checco**

Consulente di Informatica Forense



## Paolo Dal Checco

- PhD in Computer & Network Security @uniTO 
- Consulente Informatico Forense
- Lavoro per Procure, Tribunali, Avvocati, Aziende e privati

- Co-titolare Studio DiFoB (Torino) 

e Digit Law (Milano)



- Uno dei fondatori della DEFT Association 

- Socio CLUSIT, IISFA



# Sommario

- Cenni sulla Mobile Forensics
- Repertazione, Acquisizione e modalità di estrazione dati
- Un esempio di software commerciale: UFED
- Estrazione logica da dispositivi iOS con OSS
- Analisi di dispositivi iOS con OSS
- Estrazione logica da dispositivi Android con con OSS
- Analisi di dispositivi Android con OSS
- Tool Open Source per la Mobile Forensics



# Mobile Forensics

- Ramo della Digital Forensics, di cui fa parte la Computer Forensics, la disciplina che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione, l'impiego ed ogni altra forma di trattamento del dato informatico
- All'inizio era il cellulare...
- ... ormai si tende a identificare come "mobile" tutto ciò che ha capacità di è portatile, talvolta ha capacità di comunicazione, memoria interna/ esterna
- Esempi: cellulari, smartphone, tablet, PNA (navigatori), MP3 player ma anche fotocamere/videocamere, registratori digitali, etc...
- Ci concentreremo prevalentemente sui cellulari/smartphone/tablet perché sul resto si può spesso operare con strumenti utilizzati per la computer/disk forensics



# Componenti di un mobile device

1. Device (marca, modelo, s/n)
2. SIM Card
3. Flash Card (Internal Memory)
4. Mass Storage (External memory)
5. Cloud (Dropbox, iCloud, GDrive, etc...)



# 1. Dispositivo

- In genere scritto sul retro del dispositivo, dietro la batteria
- Si può ricavare dall'IMEI (che si legge sul retro oppure si ottiene “chiamando” il “\*#06#”)
  - ◆ Valore univoco attribuito al cellulare sulla rete
  - ◆ [www.numberingplans.com](http://www.numberingplans.com), [www.trackimei.com](http://www.trackimei.com)
- Utilizzare in mancanza di altro le caratteristiche fisiche (dimensione, forma, etc...)



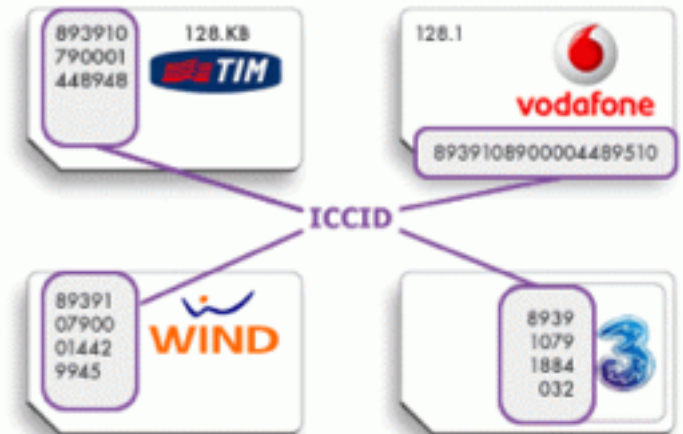
## 2. SIM

- Subscriber Identity Module (SIM)
- Permette il collegamento del dispositivo con la rete GSM/3G
- Due codici: ICCID (Integrated Circuit Card Identification) e IMSI (International Mobile Subscriber Identity)
- Sempre meno utilizzata nei dispositivi mobili per memorizzare dati rilevanti, va comunque analizzata e conosciuta



## 2. SIM (ICCID)

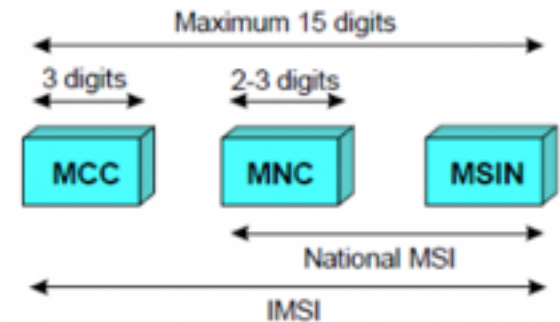
- ICCID (Integrated Circuit Card IDentification)
- Codice univoco stampato sul dorso della scheda e la identifica univocamente
- Formattazione precisa:
  - XX (prime due cifre): codice standard per l'identificazione di un sistema con scopi di telecomunicazione (89 per l'Italia)
  - XX (terza e quarta cifra): 39 solo per l'Italia, corrisponde al prefisso internazionale assegnato al paese in cui opera dato gestore e varia a seconda delle nazioni
  - XX(X) (due o tre cifre): codice identificativo del gestore, così suddiviso: 01 TIM, 10 Vodafone, 88 Wind, 99 H3G, 007 Noverca e 008 Fastweb
  - XXXXXXXX (tutte le cifre restanti fino alla fine del codice ICCID): identificativo del singolo chip





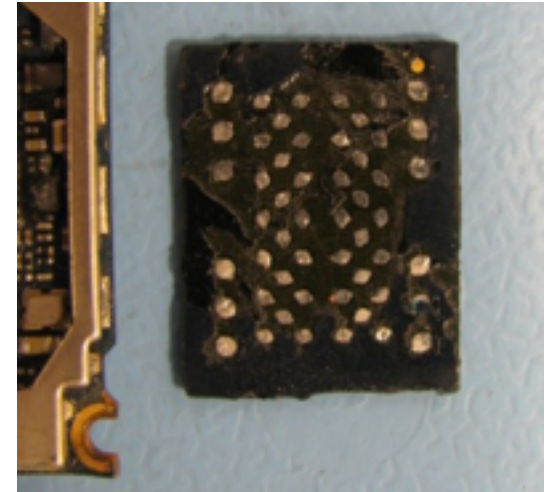
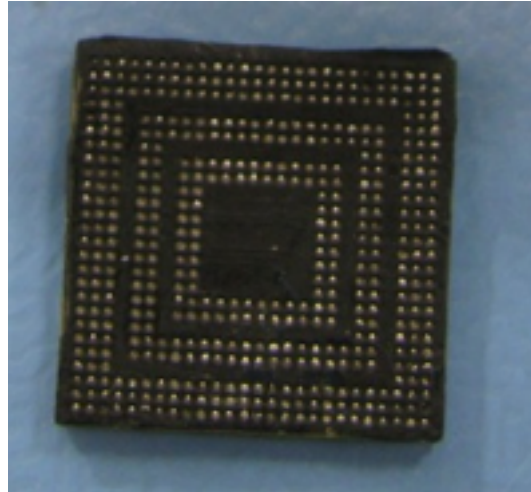
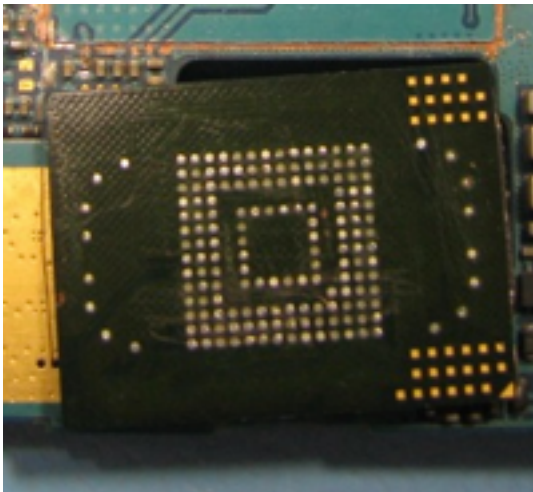
## 2. SIM (IMSI)

- International Mobile Subscriber Identity
- Codice che identifica una coppia SIM-operatore telefonico, ossia la SIM in una rete GSM
- lungo 15 cifre e così strutturato:
  - XXX - MCC (Mobile Country Code), 222 per l'Italia.
  - XX - MNC (Mobile Network Code), l'identificativo della compagnia telefonica in rete. Coincidono con quelli presenti sull'ICCID (01 TIM, 10 Vodafone, 88 Wind, 99 H3G, 007 Noverca e 008 Fastweb);
  - XXXXXXXXXXXX - MSIN (Mobile Subscriber Identification Number), un numero univoco che identifica ciascuna utenza.



# 3. Memoria interna

- Diversi form factor e socket
- NAND chips
- Operazioni di base: leggi pagina, scrivi pagina (tutti bit a 0), cancella blocco (tutti i bit a 1)



## 4. Memoria aggiuntiva

- Può contenere diversi dati essenziali: fotografie, filmati, SMS (in alcuni Nokia si può scegliere...), backup, Whatsapp, etc...
- Se in fase di sequestro... sequestrare pure quella (ci sono casi in cui ciò non è stato fatto!)
- L'esame si può fare in parallelo con gli strumenti per la mobile forensics o separatamente, con gli strumenti tradizionali per digital forensics



# 5. Cloud

- Il dispositivo può non contenere tutti i dati ma i riferimenti per potervi accedere... è legale farlo?
- Discorso molto ampio, ci vorrebbe un seminario solo per quello
- Valutare la presenza di client per Cloud come Dropbox, iCloud, Google Drive, SkyDrive, etc...
- Può rappresentare un problema perché in taluni casi (es. iCloud) permette all'utilizzatore di operare da remoto sul cellulare



# Repertazione

- Sempre utili linee guida: RFC 3227 e ISO 27037
- Se spento
  - ◆ lasciare spento
  - ◆ sequestrare anche eventuali schede di memoria e la batteria (per risparmiarsi problemi in seguito se disponibili prendere anche cavetti, caricabatteria, confezione SIM, software, etc...)
  - ◆ documentare stato del telefono
  - ◆ non lasciare la batteria all'interno o isolarla per evitare che si accenda inavvertitamente o suoni la

# Repertazione

- Se acceso
  - ◆ Documentare data/ora ed eventuali info su display, valutare possibile encryption o lock
  - ◆ Spegnerlo togliendo la batteria o se si ritiene importante, mantenerlo acceso **ma isolato da tutto (jammer, gabbia di faraday, airplane mode)**



# Acquisizione

- Acquisire il più possibile impattando il meno possibile
- Nel momento in cui lo si accende, NON lasciare la SIM originaria e NON farlo connettere al WiFi, Bluetooth, evitare che riceva il GPS
- Se è richiesta SIM e se deve essere quella fornita con il telefono: SIM cloning (IMSI, ICCID)
- Tre tipi di acquisizione: SIM, memoria interna, memoria esterna
- Non tratteremo l'acquisizione da Cloud e l'acquisizione dei dati presso l'operatore

# Acquisizione SIM

- Sempre meno fruttuosa, permette comunque in taluni casi di ottenere:
  - ◆ ICCID (Integrated Circuit Card Identification)
  - ◆ IMSI (International Mobile Subscriber Identity)
  - ◆ Rubrica (Abbreviated Dialing Numbers – ADN)
  - ◆ Registro chiamate (Last Dialed Number – LDN)
  - ◆ Short Message Service (SMS)
  - ◆ Location information (LOCI)





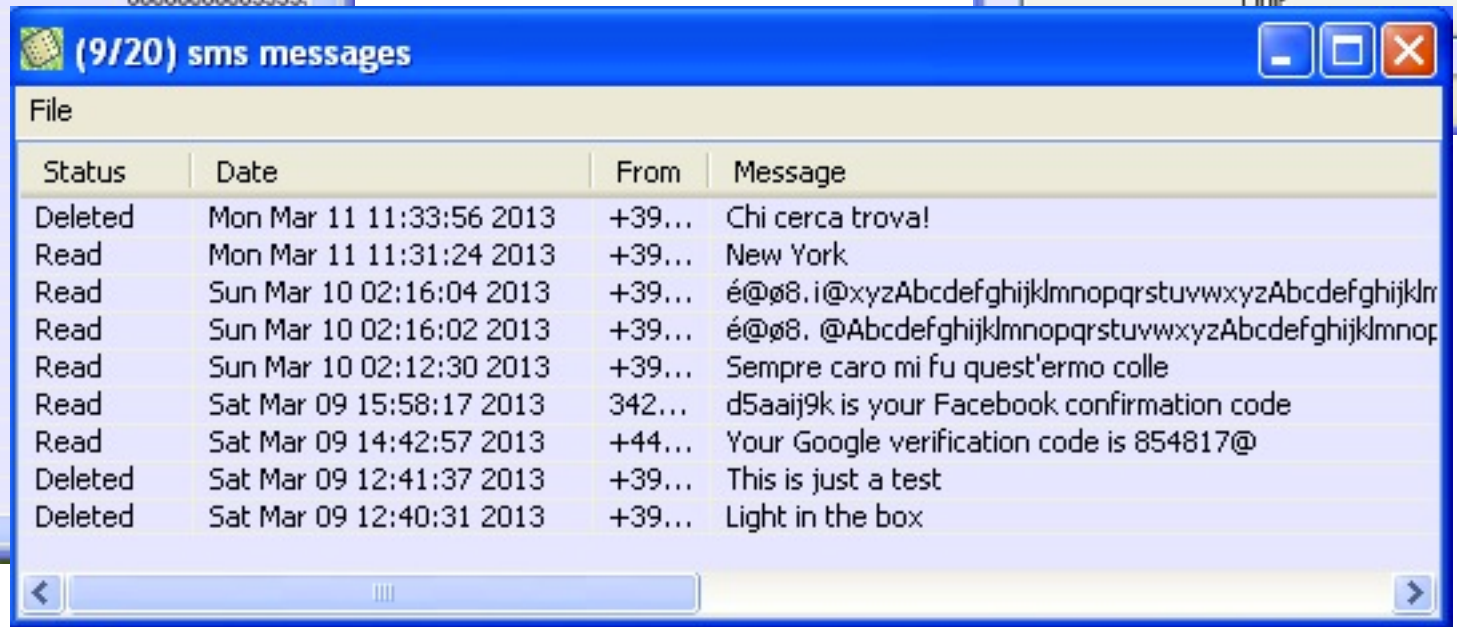
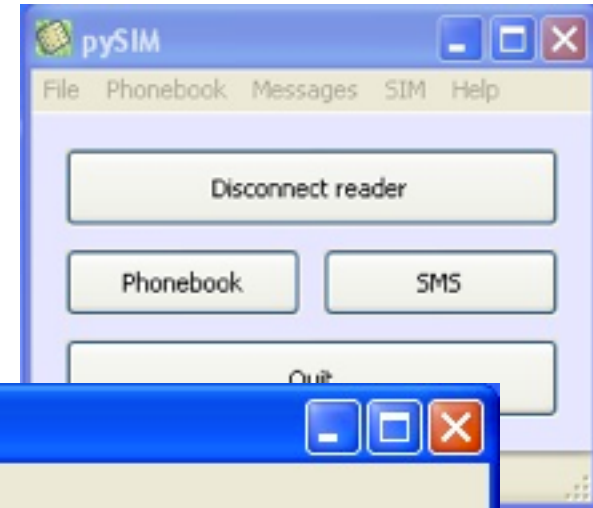
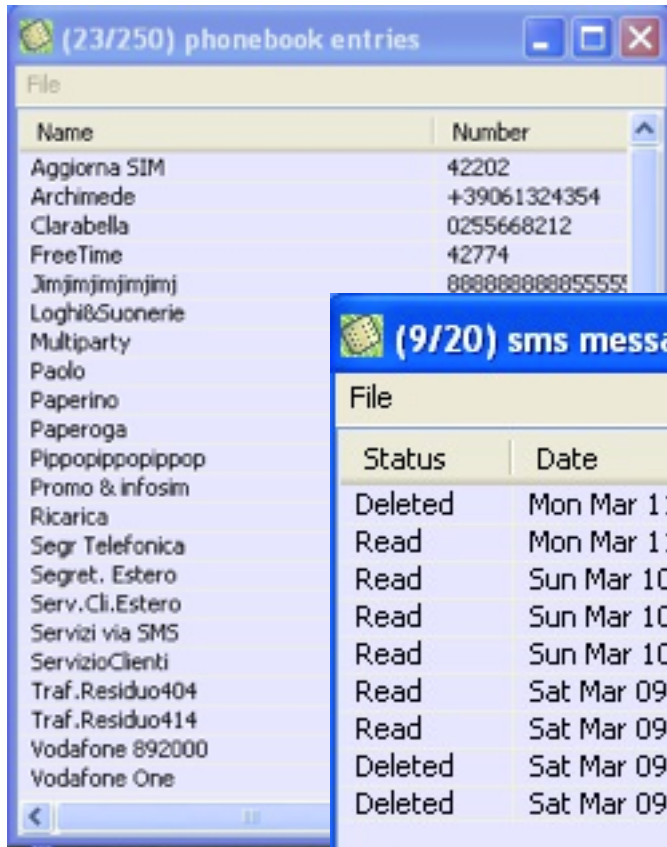
# Acquisizione SIM (challenge)

- Per cominciare, un test sulla SIM forensics, ormai in disuso ma ancora talvolta necessaria
- Acquistata SIM di un operatore Italiano, inserita in cellulare “vecchio”, popolati contatti, inviati e ricevuti SMS
- Cancellati due contatti:
  - “Topolino”
  - “Minnie”
- Cancellati tre SMS:
  - "Light in the box"
  - "This is just a test"
  - "Chi cerca trova!"



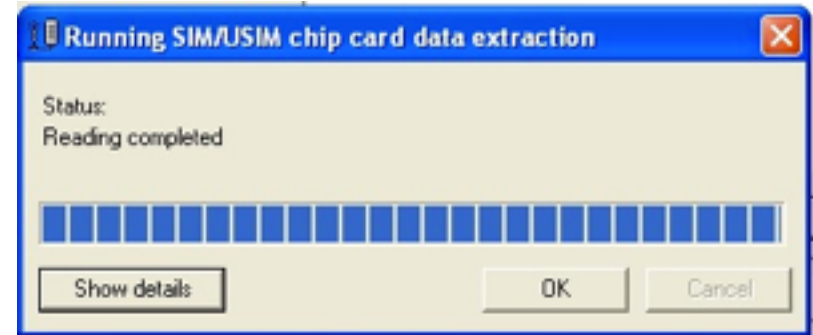
# Acquisizione SIM (challenge)

Free/OSS: pySIM



# Acquisizione SIM (challenge)

Free/OSS: TULP2G



Nr.	Ext. Type	Int. Type	Part	Timestamp
9	read	TextMessageType	All/1	11-03-13 11:31:24 GMT+01
Service Centre Address		Originating Address		
+393-200000003		+393-200000000		
Content				
New York				

Entry	Name	Second Name	
1	Paolo		3496
2			
3	Paperino		0255
4	Archimede		+390
5	Paperoga		0115
6	Jimjimjimjimjimj		8888
7	Pippopippopippop		4646
8	Zio Paperone		+390

Nr.	Ext. Type	Int. Type	Part	Timestamp
10	recovered	TextMessageType	All/1	11-03-13 11:33:56 GMT+01
Service Centre Address		Originating Address		
+393-200000000		+393-200000000		
Content				
Chi cerca trova!				



# Acquisizione SIM (challenge)

## Software Commerciale: Paraben

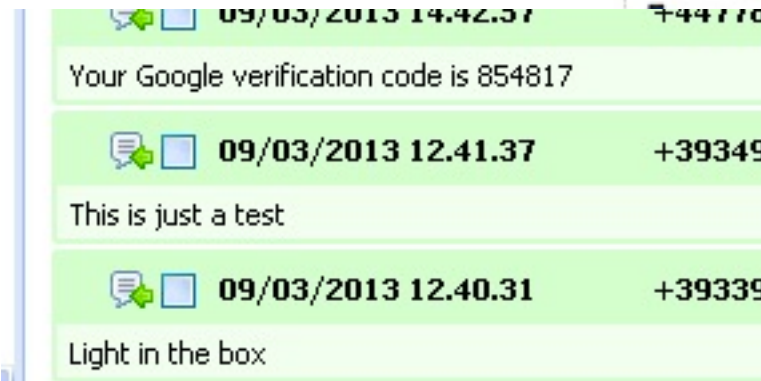
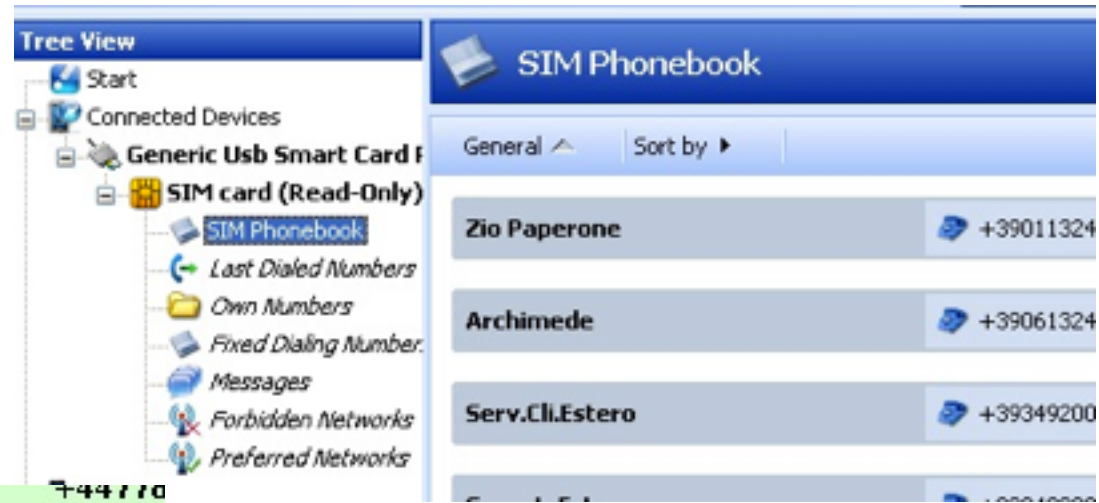
Deliver SMS (deleted)						
Record number	Status	Service Center	Originating Address	Service center time stamp	Text	Formatted Text
01	Free space	+3933333333	+3933333333	09/03/2013 12:40:31 GMT+1	Light in the box	<a href="#">Data &gt;&gt;</a>
02	Free space	+3933333333	+3933333333	09/03/2013 12:41:37 GMT+1	This is just a test	<a href="#">Data &gt;&gt;</a>
10	Free space	+3933333333	+3933333333	11/03/2013 11:33:56 GMT+1	Chi cerca trova!	<a href="#">Data &gt;&gt;</a>

SIM Abbreviated Dialing Numbers						
Record number	Name					
1	Paolo				349600	
3	Paperino				025568	
4	Archimede				+39061	
5	Paperoga				011523	
6	Jimjimjimjimjimj				888888	
7	Pippopippopippop				464646	
8	Zio Paperone				+39011	
10	Clarabella				025566	
82	Serv.Cli.Estero				+39349	
83	Aggiorna SIM				42202	
84	Promo & infocim				42070	
Is not set	Is not requested	SME to SME protocol	GSM	yes		
Is not set	Is not requested	SME to SME protocol	GSM	yes		



# Acquisizione SIM (challenge)

## Software Commerciale: MOBILedit!



- Nessuno dei software provati ha recuperato i due contatti cancellati
- Stessi risultati anche con altri tool
- Uno dei tool prometteva il carving fisico ma ha dovuto correggere... il manuale

# Acquisizione memoria esterna

- Paragonabile all'analisi di un disco o una SD
- In genere vi sono memorizzati dati multimediali e documenti
- Può contenere anche SMS, backup, Whatsapp, etc...
- Acquisire con copia forense (write blocker + dd)
- Poi Testdisk, Photorec, Autopsy, TSK, log2timeline, etc....



# Acquisizione memoria interna

- Non facile, si esegue tramite strumenti (hardware o software) dedicati, OSS o commerciali
- Tre modalità standard:
  - ◆ **Logica**: copia delle informazioni che il sistema operativo mette a disposizione (sincronizzazione)
  - ◆ **File System**: copia (completa o parziale) dei file presenti all'interno della memoria (backup)
  - ◆ **Fisica**: acquisizione bit a bit dell'intero contenuto della memoria NAND presente nel dispositivo, meglio se con bootloader
- Se nessuna funziona, tentare **JTAG**, **Flasher Box** o **CHIP OFF**



# Panoramica dei software commerciali

- Cellebrite UFED
- Micro Systemation XRY
- Oxygen Forensics
- Paraben Device Seizure
- MOBILEdit
- ViaForensics
- Elcomsoft
- FTS iXAM
- Katana Forensics Lantern
- Tarantula





# Cellebrite UFED

## Descrizione

- Uno degli strumenti di acquisizione forense più utilizzati, insieme a **XRY** della Micro Systemation
- Sviluppato da Cellebrite (1999), società con centinaia di dipendenti di cui 1/2 R&D
- Opera su mercato privato e governativo/militare
- UFED P.A. vincitore dei Forensic 4cast Awards 2012 e non solo
- Non è una panacea, lo cito perché rappresenta più o meno lo standard dei tool di analisi forense per cellulari
- es. ad oggi esegue Physical Extraction di iPhone fino al 4, iPad fino all'1 come tutti gli altri software
- device supportati: <http://www.cellebrite.com/mobile-forensics/support/ufed-supported-devices>

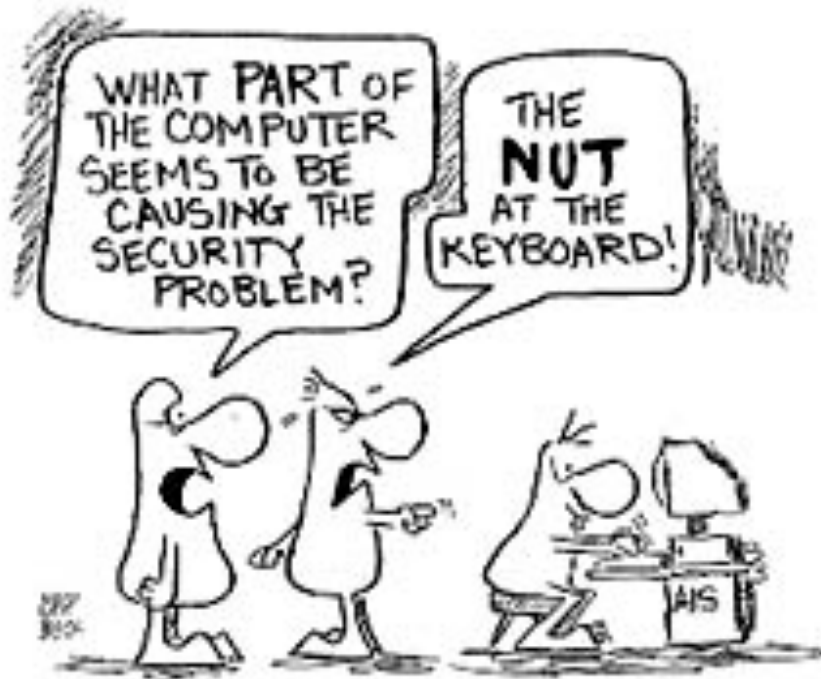
# Cellebrite UFED

Phone Data					
Application Usage 15 (0)	Calendar 446 (5)	Call Log 34 (0)	Chats 4 (0)	Contacts 1049 (45)	Installed Applications 39 (0)
Instant Messages 9 (0)	IP Connections 95 (0)	Locations 508 (0)	MMS Messages 2 (0)	Notes 17 (0)	Passwords 13 (0)
SMS Messages 43 (5)	User Accounts 17 (0)	User Dictionary 1313 (0)	Web Bookmarks 3 (0)	Web History 7 (0)	Wireless Networks 45 (0)
Data Files					
Images 10245 (68)	Videos 19 (0)	Audio 141 (0)	Text 170 (2)	Databases 98 (0)	Configurations 3032 (106)



# Principi di sviluppo

## Per software commerciali e non



- **Reverse Engineering** (codice ma anche interfacce nascoste, JTAG, cavi di manutenzione)
- **Vulnerabilità**, errori umani, gestione errata degli **stati del sistema**
- Utilizzo di **Specifiche Tecniche**, quando disponibili (quasi mai)

# Encryption

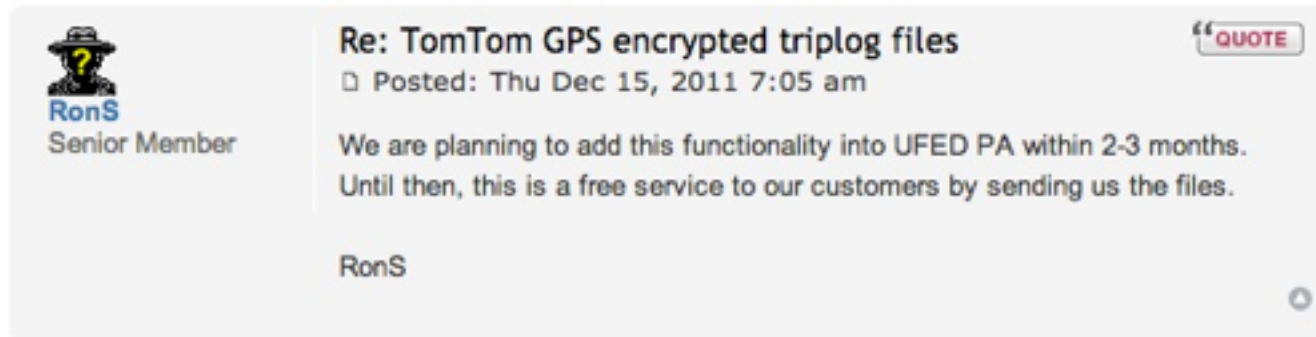
## Un problema sempre più rilevante

- Sempre più utilizzata su PC ma anche su Mobile (Android, Blackberry, iOS)
- Spesso non si può bypassare e diventa un ostacolo insormontabile, **almeno tecnicamente**
- Motivo per il quale è necessario valutare la presenza di strumenti di cifratura, prima di spegnere un dispositivo, soprattutto se il proprietario **non può o non vuole** fornire i dati di accesso
- Vediamo un caso in cui l'encryption è stata risolta positivamente:  
TomTom Triplog

# Encryption

## TomTom e i Triplog, problema risolto

- Numerosi navigatori TomTom registrano un log (granularità 5 secondi) dei viaggi percorsi. Basta che il dispositivo sia acceso e il log viene salvato, criptato.
- Tramite reverse engineering è stata scovata da alcuni strumenti una vulnerabilità nell'algoritmo.
- UFED and XRY possono decriptare il file, bisogna inviare loro l'XML e si riceve in cambio la chiave, anche se...









# Cellebrite UFED

Quando si trova molto...

Tipo	Incluso nel rapporto	Totale
Account utenti	5	5
Applicazioni installate	57	57
Chat	8 (1 Eliminati)	8 (1 Eliminati)
● WhatsApp	4	4
● iMessage: +[redacted]	4 (1 Eliminati)	4 (1 Eliminati)
Connessioni IP	17	17
Contatti	58 (8 Eliminati)	58 (8 Eliminati)
● Non categorizzato	50	50
● Recently Contacted	8 (8 Eliminati)	8 (8 Eliminati)
Cookie	23	23

# Cellebrite UFED

Quando si trova molto...

 Cronologia	983	(514 Eliminati)	983	(514 Eliminati)
 Cronologia Web	15		15	
 Dispositivi Bluetooth	2		2	
 Dizionario utente	3920		3920	
● it_IT	3920		3920	
 E-mail	248	(89 Eliminati)	248	(89 Eliminati)
 [redacted]@gmail.com	195	(38 Eliminati)	195	(38 Eliminati)
● [Gmail]\AllMail	50		50	
● [Gmail]\Sent	69	(19 Eliminati)	69	(19 Eliminati)
● [Gmail]\Spam	2		2	
● [Gmail]\Starred	4		4	

# Cellebrite UFED






Quando si trova molto...

● Inbox	69	(19 Eliminati)	69	(19 Eliminati)
● [Gmail]\Trash	1		1	
✉ Non categorizzato	53	(51 Eliminati)	53	(51 Eliminati)
● x-apple-transient-drafts	2		2	
● Non categorizzato	51	(51 Eliminati)	51	(51 Eliminati)
🗺 Mappe	12		12	
● Google Maps	12		12	
📧 Messaggi MMS	273	(272 Eliminati)	273	(272 Eliminati)
● Inbox	126	(125 Eliminati)	126	(125 Eliminati)
● Sent	147	(147 Eliminati)	147	(147 Eliminati)
💬 Messaggi SMS	168	(109 Eliminati)	168	(109 Eliminati)
● Drafts	3		3	
● Inbox	73	(42 Eliminati)	73	(42 Eliminati)
● Sent	92	(67 Eliminati)	92	(67 Eliminati)
🔒 Password	36		36	







# Cellebrite UFED

Quando si trova molto...

 Posizioni	3		3
● Media Locations	3		3
 Reg. chiam	142	(42 Eliminati)	142 (42 Eliminati)
● Outgoing	104	(31 Eliminati)	104 (31 Eliminati)
● Incoming	30	(8 Eliminati)	30 (8 Eliminati)
● Missed	8	(3 Eliminati)	8 (3 Eliminati)
 Reti wireless	1		1
 Segnalibri Web	153		153
 Non categorizzato	153		153
● Root/Banca	4		4
● Root/BookmarksBar	3		3
● Root/Barzelle	19		19
● Root/Corel on the Web	6		6
● Root/Download Film	4		4







# Cellebrite UFED

Quando si trova molto...

 Voci calendario	14	(1 Eliminati)	14	(1 Eliminati)
● Calendario	13	(1 Eliminati)	13	(1 Eliminati)
● c...@gmail.com	1		1	
 File dati	18205	(246 Eliminati)	18205	(246 Eliminati)
● Applications	4145	(119 Eliminati)	4145	(119 Eliminati)
● Audio	149		149	
● Configurazioni	4145	(119 Eliminati)	4145	(119 Eliminati)
● Database	399		399	
● Immagini	8802	(8 Eliminati)	8802	(8 Eliminati)
● Testo	558		558	
● Video	7		7	
 File ricostruiti	0		0	
 File infetti	0		0	

# Cellebrite UFED

Quando non si trova nulla o quasi...

Type	Included in report	Total
 Call Log	1	1
● Unknown	1	1
 SMS Messages	2 (1 Deleted)	2 (1 Deleted)
● Sent	2 (1 Deleted)	2 (1 Deleted)
 Time Line	0	3 (1 Deleted)
 Data Files	168 (4 Deleted)	168 (4 Deleted)
● Applications	22	22
● Audio	10	10
● Configurations	4	4
● Databases	6 (1 Deleted)	6 (1 Deleted)
● Images	89	89
● Text	35 (3 Deleted)	35 (3 Deleted)
● Videos	2	2
 Carved Files	31286	31286
● Carved Images	31286	31286
 Infected Files	0	0

# Cellebrite UFED

Quando non si trova nulla o quasi...

## Call Log (1)

### Unknown (1)

#	Country code	Network code	Party	Time	Duration	Video call	Source	Del?
1			+39[REDACTED]	23/11/20[REDACTED] 16:08:30(UTC+0)	00:00:14			

## SMS Messages (2)

### Sent (2)

#	Party	Time	Status	Message	Del?
1	From: +39[REDACTED] To: 34[REDACTED]	23/11/20[REDACTED] 15:53:14(UTC+0)		PAIF QU5WZwaggEAAUMWiFchxQIA3gMCSVQEOsBIt3foDFM6LE+Nzn1wZ m6NdKIFAQcBCAQMAAEAFQGB	Yes
2	From: +39[REDACTED] To: 34[REDACTED]	23/11/20[REDACTED] 15:53:14(UTC+0)		PAIF QU5WZwaggEAAUMWiFchxQIA3gMCSVQEOsBIt3foDFM6LE+Nzn1wZ m6NdKIFAQcBCAQMAAEAFQGB	



# Software OS

## Le alternative ai software commerciali

- Vediamo ora quali alternative (o integrazioni) possiamo trovare ai software commerciali
- Alcuni software sono presenti in DEFT 8, altri saranno presenti in **DEFT 8.1**, è comunque possibile installarli su sistemi LINUX (es. Ubuntu)



# Software OS

## Cominciamo con le copie logiche di iOS e Android

- Esistono due ottimi prodotti Open Source per poter fare acquisizioni logiche (a.k.a. backup) di dispositivi iOS e Android
- IOS
  - libidevicebackup
- Android
  - adb
- Non sono propriamente forensically sound, ma a volte non ci sono alternative.



# Acquisizione logica di iOS

## libimobiledevice

- <http://www.libimobiledevice.org>
- supporta iPhone®, iPod Touch®, iPad® and Apple TV®
- non richiede jailbreak e non dipende da librerie esterne
- E' in grado di:
  - leggere informazioni circa il dispositivo
  - eseguire backup/restore del dispositivo
  - gestire icone SpringBoard®
  - gestire le applicazioni installate
  - leggere addressbook/calendars/notes e bookmarks
  - (utilizzando libgpod) sincronizzare musica e video



# Acquisizione logica di iOS

## libimobiledevice

- Ultima versione la 1.0.7 (dev/unstable 1.1.5), testata con iPod Touch 1G/2G/3G/4G/5G, iPhone 1G/2G/3G/3GS/4/4S/5/5C/5S, iPad 1/2/3/4/Mini/Air e Apple TV 2G/3G fino a iOS firmware 7.0.4 su Linux, Mac OS X e Windows.





# Acquisizione logica di iOS

## Tool forniti con libimobiledevice

- **idevicebackup**: create or restore backup for devices running iOS prior to
- **idevicebackup2**: create or restore backup for devices running iOS 4 or later
- **idevicedate**: display the current date or set it on a connected device
- **idevicedebugserverproxy**: remote debugging proxy
- **idevicediagnostics**: interact with the diagnostics interface of a device
- **ideviceenterrecovery**: make a device with the supplied 40-digit UDID enter recovery mode
- **idevice\_id**: prints the device name or a list of attached devices, showing the UDID which is a 40-digit hexadecimal number of the device for which the name should be retrieved
- **ideviceinfo**: shows information about the first connected device
- **idevicepair**: manage pairings with devices and host
- **ideviceprovision**: manages provisioning profiles on a device
- **idevicescreenshot**: gets a screenshot from the connected device
- **idevicesyslog**: relays syslog of a connected device
- **plistutil**: reads and convert plist files to and from XML format



# Acquisizione logica di iOS

## idevicebackup2

```
root@ubuntu: /tmp
File Edit Tabs Help
root@ubuntu:/tmp# idevicebackup2
No command specified.
Usage: idevicebackup2 [OPTIONS] CMD [CMDOPTIONS] DIRECTORY
Create or restore backup from the current or specified directory.

commands:
  backup      create backup for the device
  restore     restore last backup to the device
  --system    restore system files, too.
  --reboot    reboot the system when done.
  --copy      create a copy of backup folder before restoring.
  --settings  restore device settings from the backup.
  --remove    remove items which are not being restored
  --password PWD supply the password of the source backup
  info        show details about last completed backup of device
  list        list files of last completed backup in CSV format
  unback      unpack a completed backup in DIRECTORY/_unback_/
  encryption on|off [PWD] enable or disable backup encryption
  NOTE: password will be requested in interactive mode if omitted
  changepw [OLD NEW] change backup password on target device
  NOTE: passwords will be requested in interactive mode if omitted

options:
  -d, --debug      enable communication debugging
  -u, --udid UDID  target specific device by its 40-digit device UDID
  -s, --source UDID use backup data from device specified by UDID
  -i, --interactive request passwords interactively
  -h, --help       prints usage information

root@ubuntu:/tmp#
```

# Acquisizione logica di iOS

## Preparazione del dispositivo

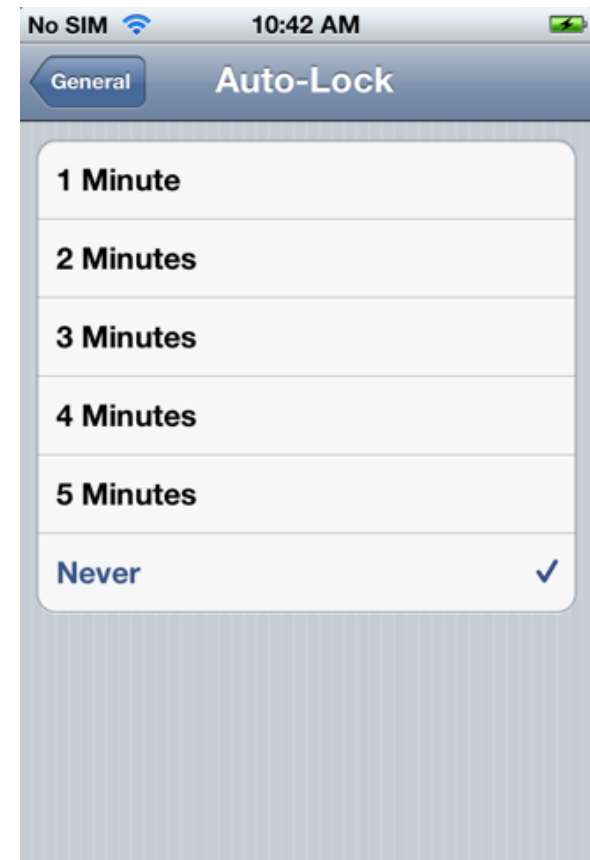
- Collegare il device al PC dove è installata la libimobiledevice (se VM verificare che il device sia “attached” al guest e non all’host)
- Sbloccare il dispositivo con il PIN (compare il seguente warning)



# Acquisizione logica di iOS

## Preparazione del dispositivo

- Se iOS > 7.0 autorizzare il paring con il PC (ancora instabile...)
- Disabilitare l'auto lock (per evitare che il processo di backup si blocchi)



# Acquisizione logica di iOS

## Preparazione del dispositivo

- Se il backup è protetto da password ed è nota, la si può disabilitare sul device tramite iTunes o idevicepair



**Automatically Back Up**

**iCloud**  
Back up the most important data on your iPhone to iCloud.

**This computer**  
A full backup of your iPhone will be stored on this computer.

**Encrypt iPhone backup**  
This will also back up account passwords used on this iPhone.

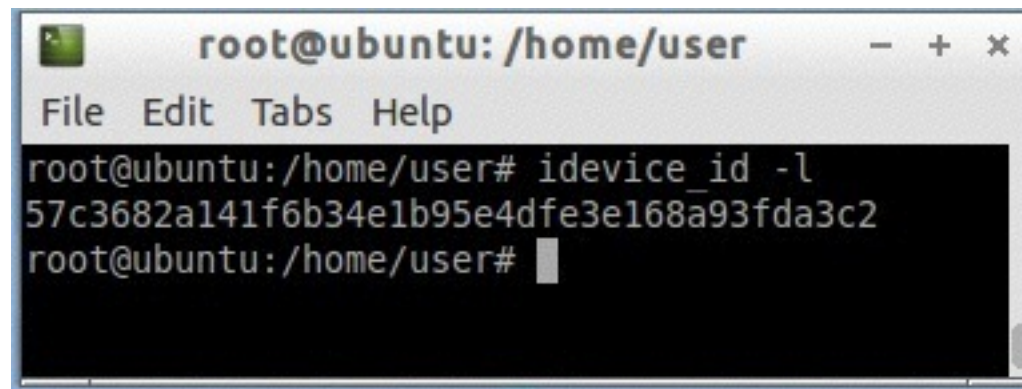
Change Password...

- Meglio comunque fare il backup criptato e poi decriptarlo successivamente tramite tool come iphone-dataprotection con lo script backup\_tool.py
- Se la password non è nota, si può tentare il brute force con il tool (commerciale) <http://www.elcomsoft.it/eppb.html>

# Acquisizione logica di iOS

## Testare la connettività con il device

- Testiamo la connessione con il dispositivo tramite il comando “`idevice_id -l`” ottenendo l’UUID del device



```
root@ubuntu: /home/user
File Edit Tabs Help
root@ubuntu:/home/user# idevice_id -l
57c3682a141f6b34e1b95e4dfe3e168a93fda3c2
root@ubuntu:/home/user#
```

- Altri comandi utili per reperire informazioni dai dispositivi sono “`ideviceinfo`” e “`idevicesyslog`”

# Acquisizione logica di iOS

## Avviare l'acquisizione

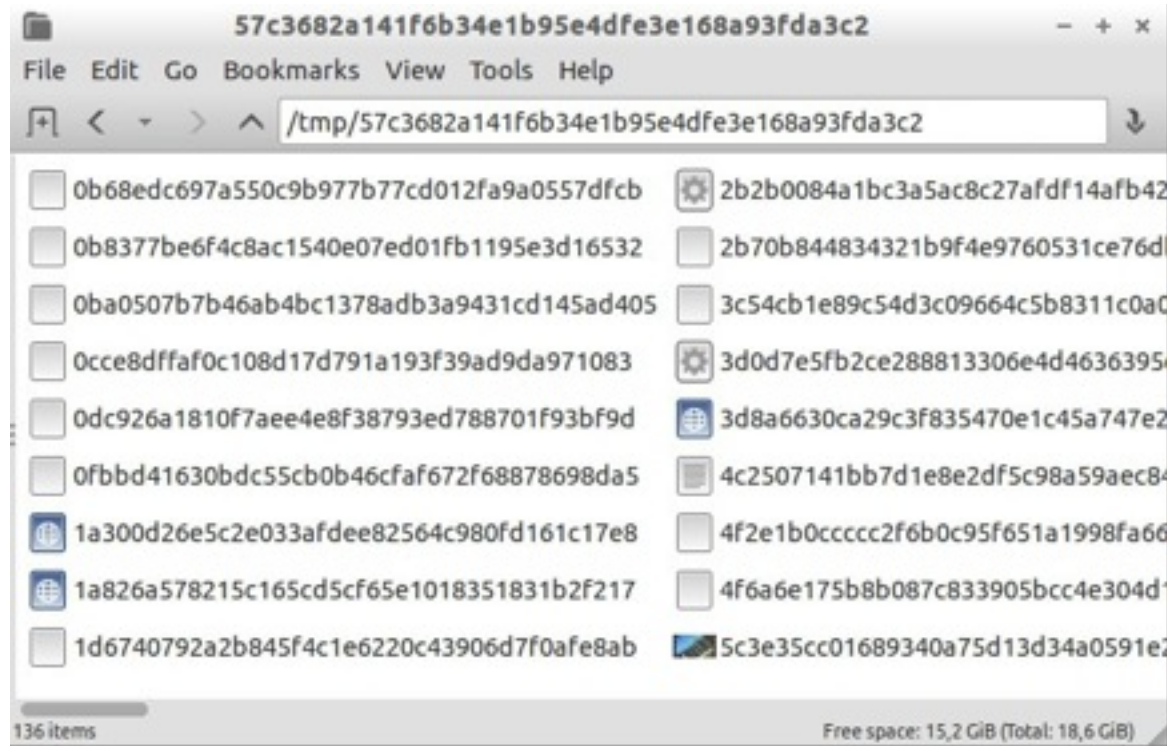
- Lanciamo il comando di backup tramite “`idevicebackup2 backup ./ folder`”

```
root@ubuntu: /tmp
File Edit Tabs Help
root@ubuntu:/home/user# idevice_id -l
57c3682a141f6b34e1b95e4dfe3e168a93fda3c2
root@ubuntu:/home/user# cd /tmp/
root@ubuntu:/tmp# idevicebackup2 backup ./
Backup directory is "./"
Started "com.apple.mobilebackup2" service on port 49205.
Negotiated Protocol Version 2.1
Starting backup...
Backup will be unencrypted.
Requesting backup from device...
Full backup mode.
[= ] 1% Finished
Receiving files
[=====] 100% (24.0 MB/24.0 MB)
[=====] 100% (24.0 MB/24.0 MB)
[=====] 100% (24.1 MB/24.0 MB)
[=====] 100% (24.1 MB/24.0 MB)
```

# Acquisizione logica di iOS

## Esaminare i dati ottenuti

- Nel folder prescelto, troveremo una cartella il cui nome corrisponde all'UDID del dispositivo acquisito

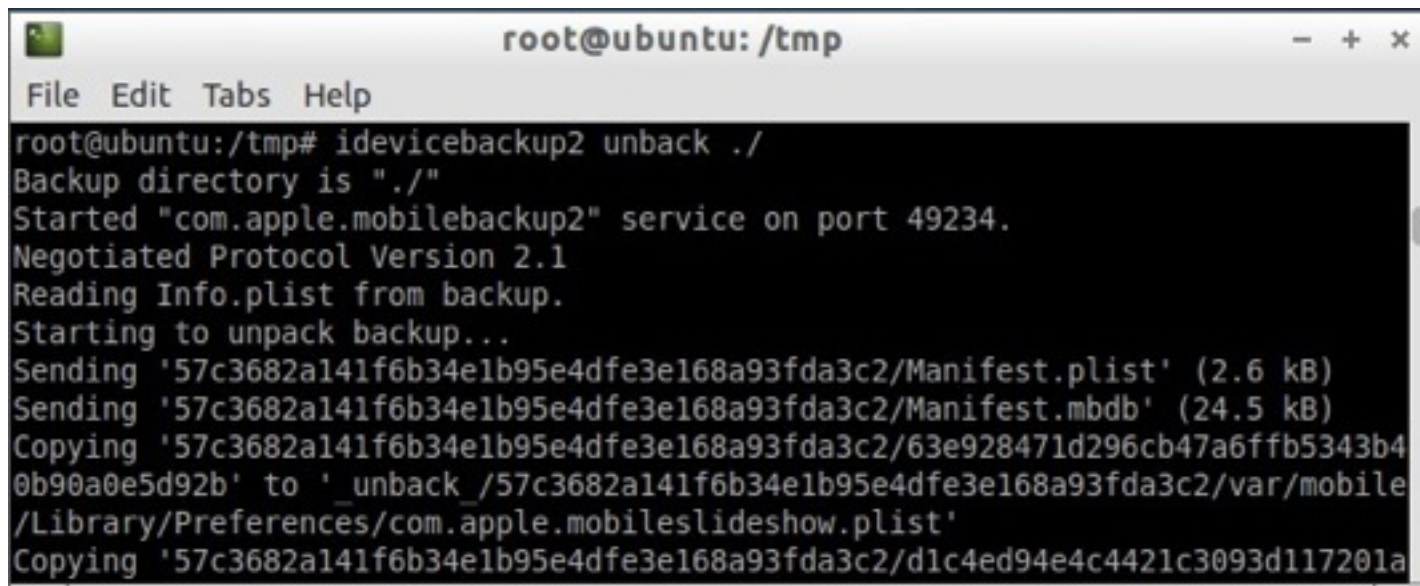




# Acquisizione logica di iOS

## Convertire i dati ottenuti

- Il folder conterrà file inintelligibili che, per poter fare un esame diretto, vanno convertiti tramite il comando “`idevicebackup2 unback ./folder`” (il dispositivo deve essere connesso oppure va specificato UDID)



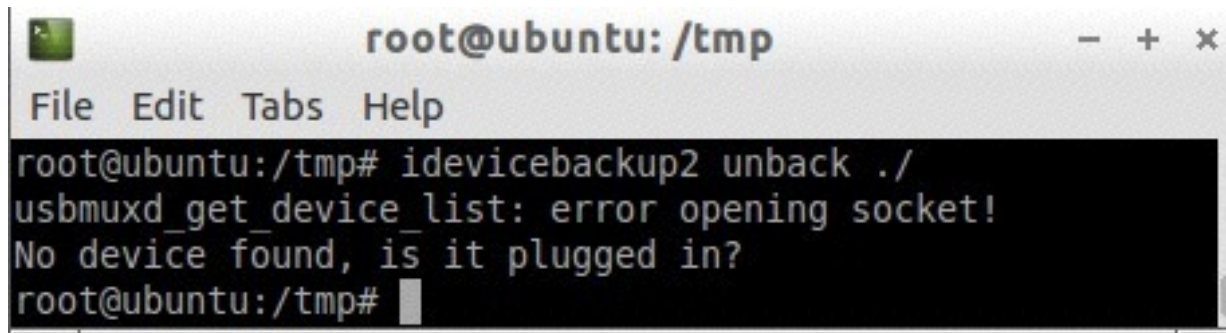
```
root@ubuntu: /tmp
File Edit Tabs Help
root@ubuntu:/tmp# idevicebackup2 unback ./
Backup directory is "./"
Started "com.apple.mobilebackup2" service on port 49234.
Negotiated Protocol Version 2.1
Reading Info.plist from backup.
Starting to unpack backup...
Sending '57c3682a141f6b34e1b95e4dfe3e168a93fda3c2/Manifest.plist' (2.6 kB)
Sending '57c3682a141f6b34e1b95e4dfe3e168a93fda3c2/Manifest.mbdb' (24.5 kB)
Copying '57c3682a141f6b34e1b95e4dfe3e168a93fda3c2/63e928471d296cb47a6ffb5343b40b90a0e5d92b' to '_unback_/57c3682a141f6b34e1b95e4dfe3e168a93fda3c2/var/mobile/Library/Preferences/com.apple.mobileslideshow.plist'
Copying '57c3682a141f6b34e1b95e4dfe3e168a93fda3c2/d1c4ed94e4c4421c3093d117201a
```

- “folder” deve essere quello dove sono contenuti gli UUID dei dispositivi da cui avete estratto i dati

# Acquisizione logica di iOS

## Convertire i dati ottenuti

- Quando si estrae il backup, il dispositivo deve essere connesso, altrimenti si ottiene un errore:



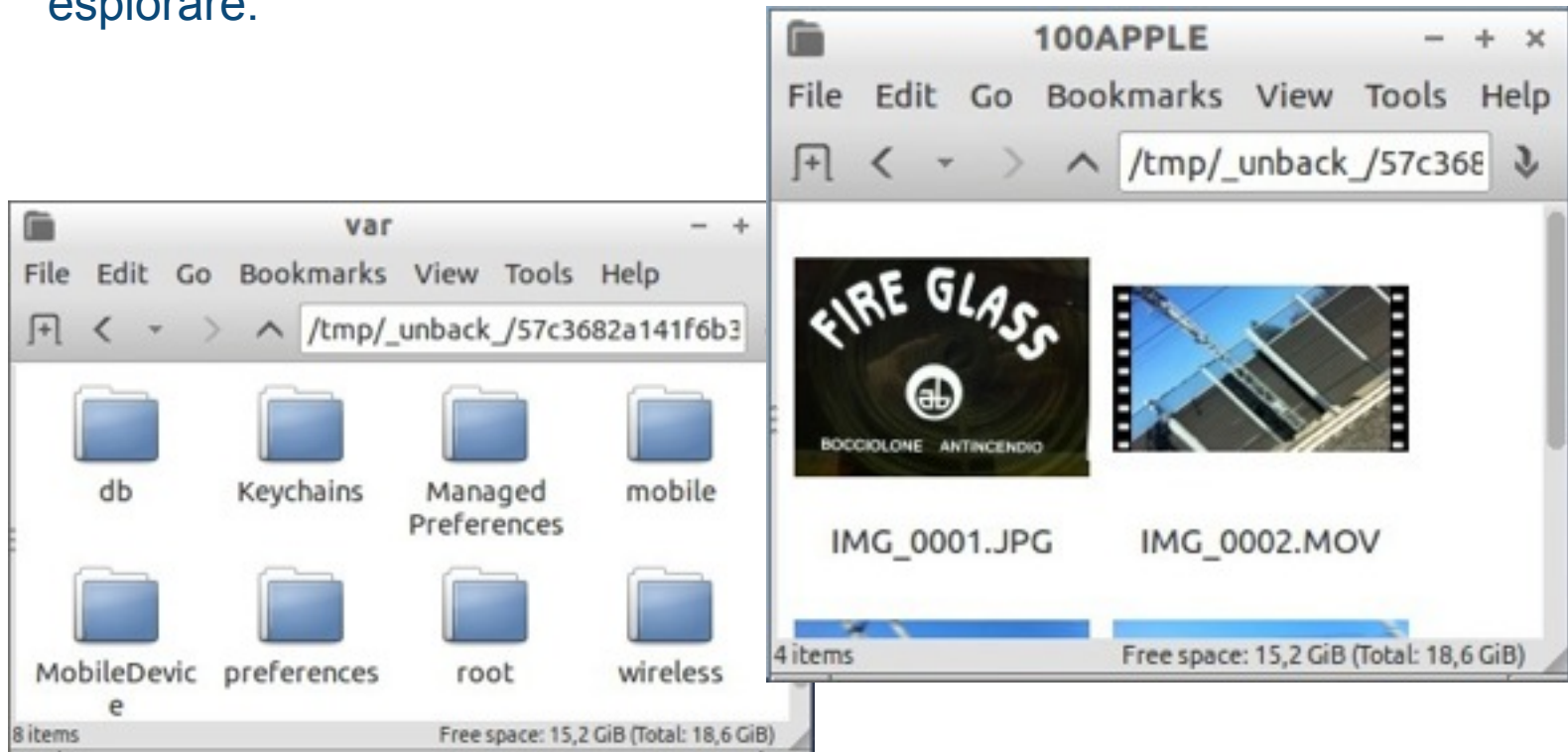
```
root@ubuntu: /tmp
File Edit Tabs Help
root@ubuntu:/tmp# idevicebackup2 unback ./
usbmuxd_get_device_list: error opening socket!
No device found, is it plugged in?
root@ubuntu:/tmp#
```

- “folder” deve essere quello dove sono contenuti gli UUID dei dispositivi da cui avete estratto i dati

# Acquisizione logica di iOS

## Convertire i dati ottenuti

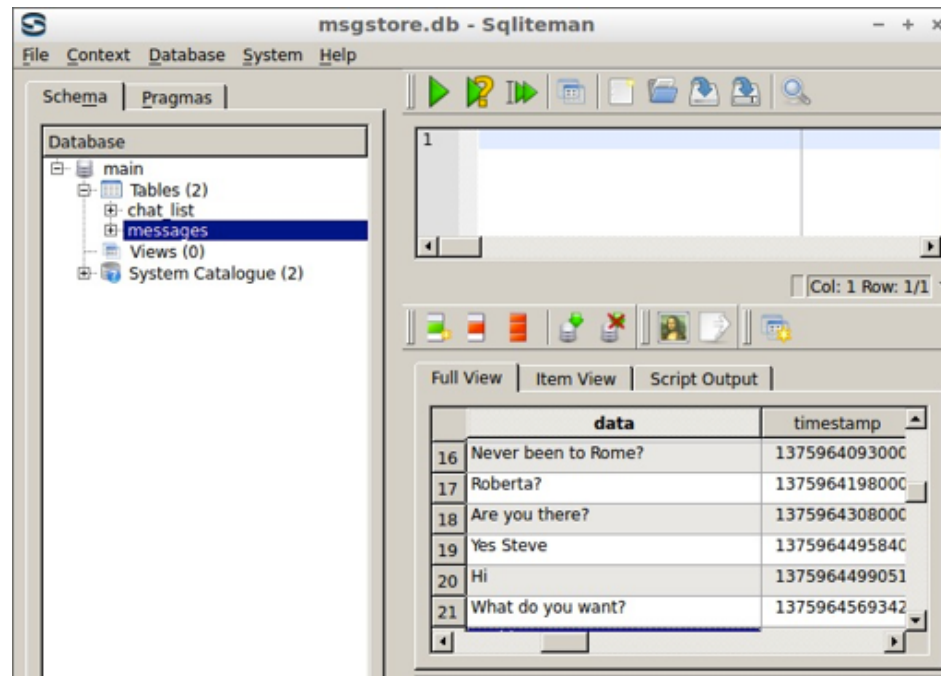
- La conversione conterrà diverse cartelle spesso autoesplicative da esplorare:



# Acquisizione logica di iOS

## Leggere i dati ottenuti

- Diversi database con contenuti rilevanti sono in formato SQLITE

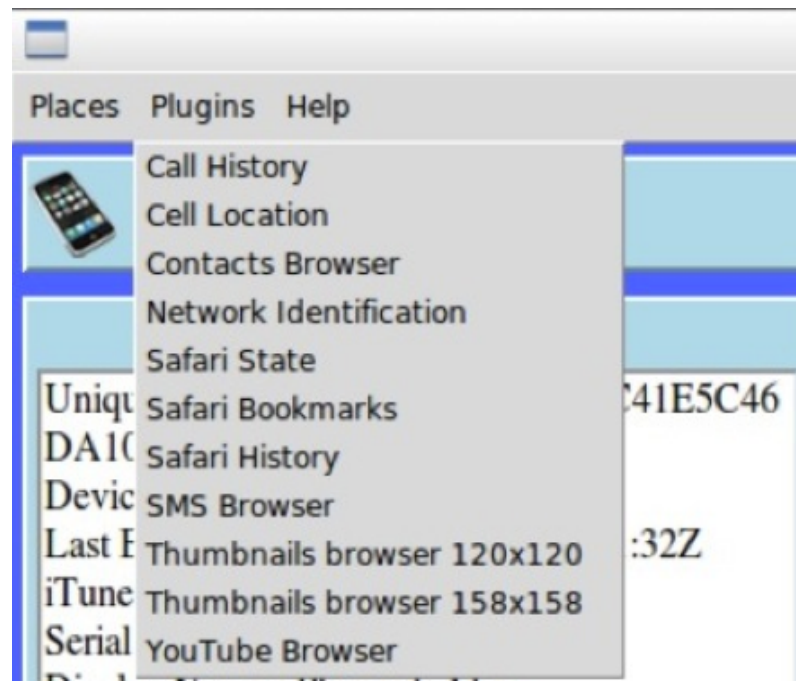


- Utilizziamo software come SQLiteMan per aprire i database, come ad esempio le chat Whatsapp

# Acquisizione logica di iOS

## Parsificazione dei dati ottenuti

- Più comodo ed esaustivo parificare i dati ottenuti tramite il tool scritto da Mario Piccinelli, "iPBA" ([www.iphonebackupanalyzer.com](http://www.iphonebackupanalyzer.com))



# Acquisizione logica di Android

## ADB

- ADB, Android Debug Bridge
- <http://developer.android.com/tools/help/adb.html>.
- Utility command line inclusa nell'SDK Google Android che permette di comunicare con l'emulatore Android o un device connesso via USB per:
  - Controllare il dispositivo via USB
  - Copiare file da e verso il dispositivo
  - Installare e disinstallare applicazioni
  - Eseguire comandi da shell
  - Aprire una shell sul dispositivo
  - Fare debug di applicazioni
  - Backup/restore (Android >= 4.0)



# Acquisizione logica di Android

## ADB

- Funziona attraverso la presenza di tre componenti:
  - **Un client**, che viene eseguito sulla macchina di sviluppo e si lancia tramite il comando “adb” oppure può essere utilizzato da applicazioni terze (es. il plugin ADT per Eclipse o il tool di debugging DDMS)
  - **Un server**, che gira sulla macchina di sviluppo in background e gestisce la comunicazione tra client e il demone dab sul dispositivo
  - **Un demone**, che gira come processo di background sul dispositivo



# Acquisizione logica di Android

## Preparazione del dispositivo

- Abilitare Developer Options -> USB Debugging
- Se manca il menù, andare in Impostazioni, About e premere 7 volte su Build Number



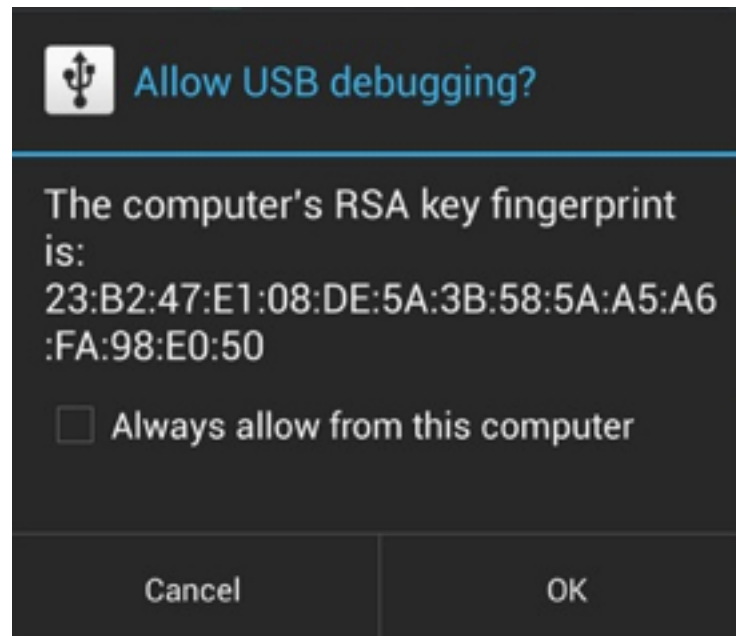
- Sbloccare il dispositivo e impedire di andare in lock automaticamente



# Acquisizione logica di Android

## RSA key fingerprint

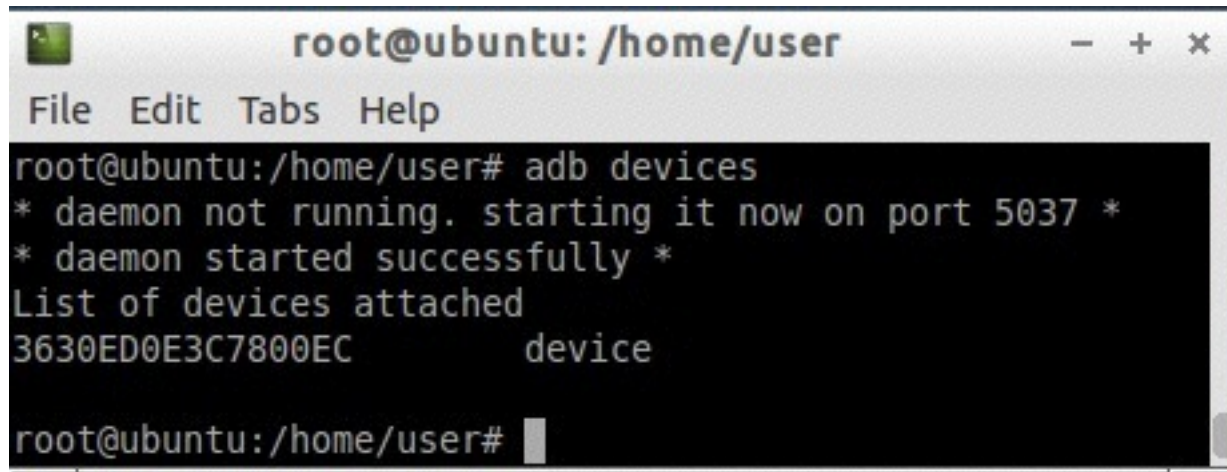
- Una volta connesso il dispositivo, se contiene Android 4.2.2 o superiori è necessario confermare il fingerprint del computer per autorizzare la connessione



# Acquisizione logica di Android

## List devices

- Per verificare se il dispositivo è stato riconosciuto, digitare “adb devices”



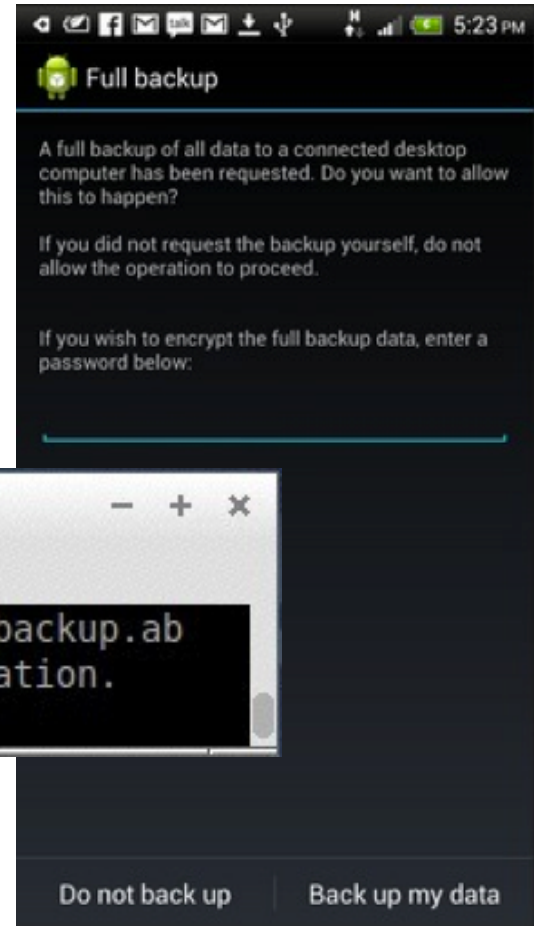
```
root@ubuntu: /home/user
File Edit Tabs Help
root@ubuntu:/home/user# adb devices
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
List of devices attached
3630ED0E3C7800EC      device
root@ubuntu:/home/user#
```

- Nel caso di problemi di connessione, provare a riavviare il server adb tramite il comando “adb kill-server” seguito dal comando “adb start-server”

# Acquisizione logica di Android

## List devices

- Avviare il backup tramite il comando “adb backup –apk –shared –all –f backup.ab” e confermare la richiesta di full backup
- E’ anche possibile criptare il backup inserendo una password nell’apposito campo

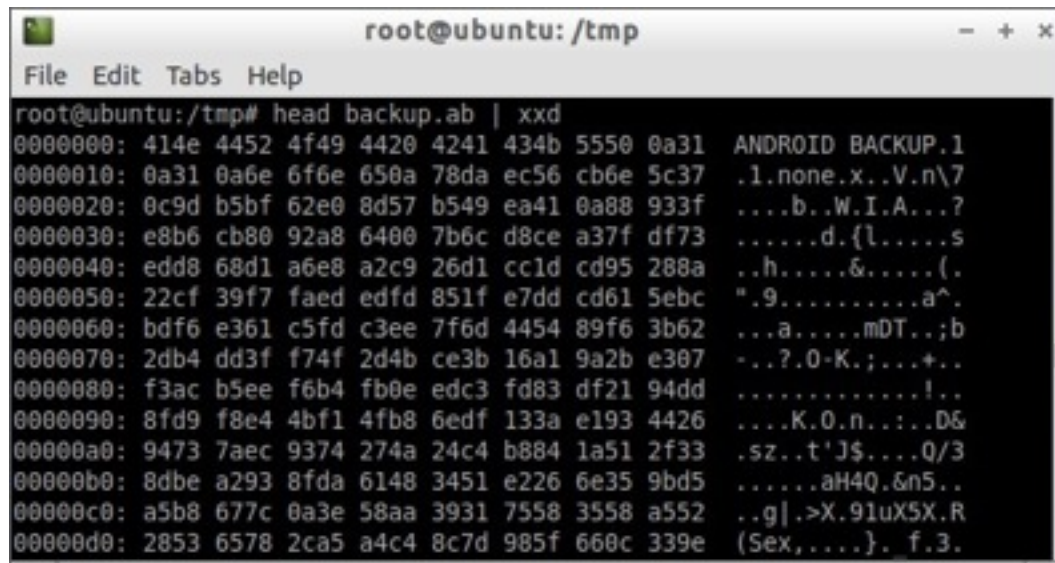


```
root@ubuntu: /tmp
File Edit Tabs Help
root@ubuntu:/tmp# adb backup -apk -shared -all -f backup.ab
Now unlock your device and confirm the backup operation.
```

# Acquisizione logica di Android

## Estrazione dei dati dai backup

- Il backup produce un archivio non immediatamente decomprimibile:



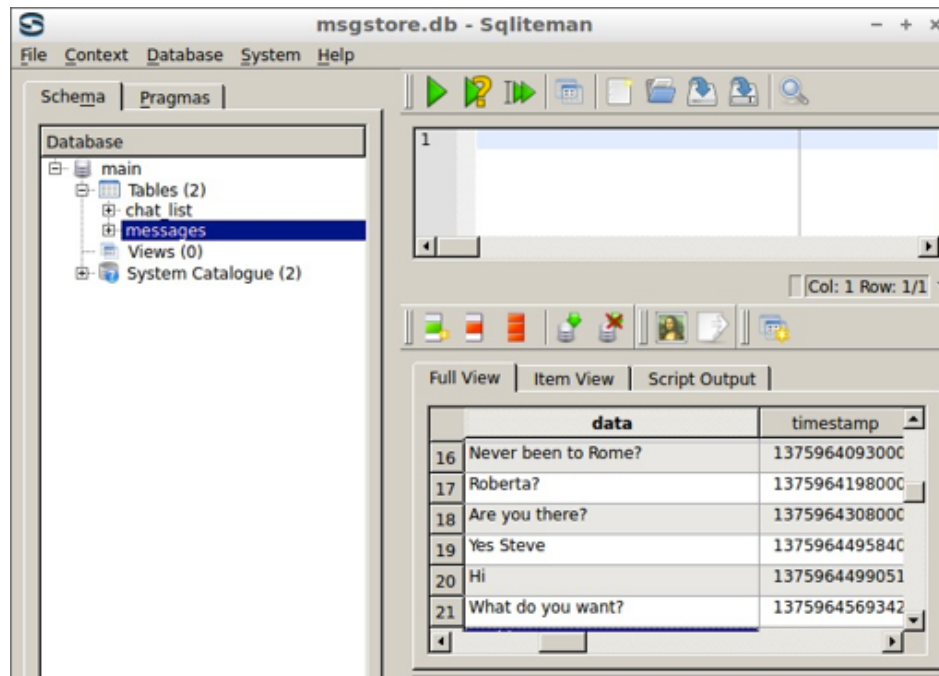
```
root@ubuntu: /tmp
File Edit Tabs Help
root@ubuntu:/tmp# head backup.ab | xxd
00000000: 414e 4452 4f49 4420 4241 434b 5550 0a31  ANDROID BACKUP.1
00000010: 0a31 0a6e 6f6e 650a 78da ec56 cb6e 5c37  .1.none.x.V.n\7
00000020: 0c9d b5bf 62e0 8d57 b549 ea41 0a88 933f  ...b.W.I.A...?
00000030: e8b6 cb80 92a8 6400 7b6c d8ce a37f df73  ....d.{l....s
00000040: edd8 68d1 a6e8 a2c9 26d1 ccl1 cd95 288a  ..h....&....(
00000050: 22cf 39f7 faed edfd 851f e7dd cd61 5ebc  ".9.....a^
00000060: bdf6 e361 c5fd c3ee 7f6d 4454 89f6 3b62  ...a....mDT.;b
00000070: 2db4 dd3f f74f 2d4b ce3b 16a1 9a2b e307  -..?.0-K.;...+..
00000080: f3ac b5ee f6b4 fb0e edc3 fd83 df21 94dd  ....!..
00000090: 8fd9 f8e4 4bf1 4fb8 6edf 133a e193 4426  ....K.O.n...D&
000000a0: 9473 7aec 9374 274a 24c4 b884 1a51 2f33  .sz..t'J$....Q/3
000000b0: 8dbe a293 8fda 6148 3451 e226 6e35 9bd5  ....aH4Q.&n5..
000000c0: a5b8 677c 0a3e 58aa 3931 7558 3558 a552  ..g|.>X.91uX5X.R
000000d0: 2853 6578 2ca5 a4c4 8c7d 985f 660c 339e  (Sex,....}. f.3.
```

- Per convertire l'archivio in un normale tar eseguire "dd if=backup.ab bs=1 skip=24|openssl zlib -d > backup.tar"
- Se il backup è criptato, utilizzare <http://sourceforge.net/projects/adbextractor> o <https://github.com/nelenkov/android-backup-extractor>

# Acquisizione logica di Android

## Analisi dei dati estratti

- Diversi database con contenuti rilevanti sono in formato SQLITE

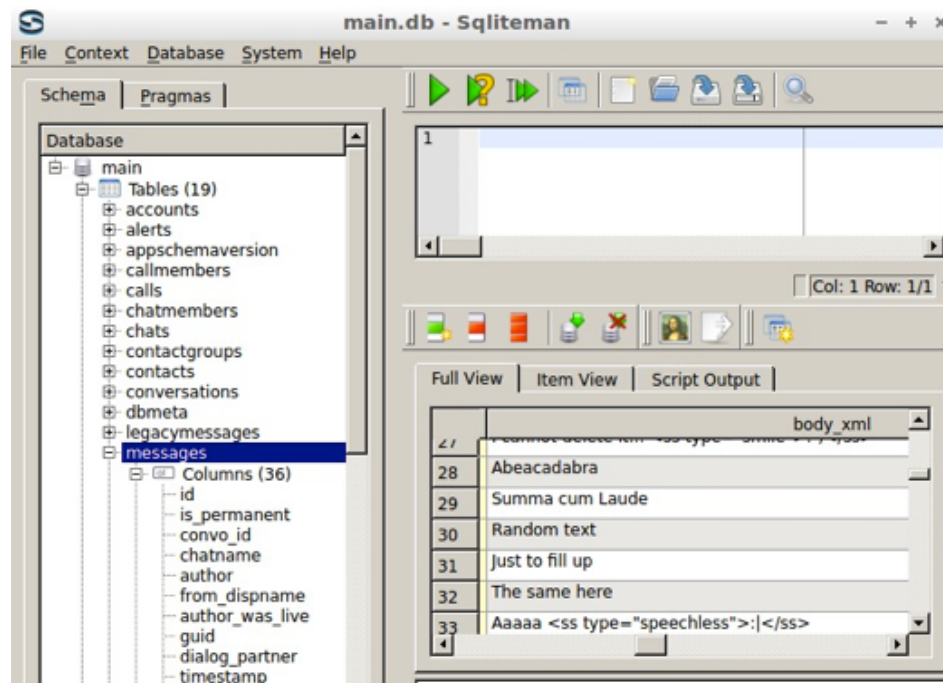


- Utilizziamo software come SQLiteMan per aprire i database, come ad esempio le chat Whatsapp

# Acquisizione logica di Android

## Analisi dei dati estratti

- Apriamo il database Skype nel folder “apps/com.skype.raider/” ”



- Lo stesso si può fare anche con i database Viber

# Acquisizione logica di Android

## Analisi dei dati estratti

- Per comodità, si possono usare i tool WhatsappXtract and SkypeXtract scaricabili da
  - <http://blog.digital-forensics.it/2012/05/whatsapp-forensics.html>
  - <http://www.skypextractor.com>.



The screenshot shows the WhatsAppXtract tool interface. At the top, it displays 'Zena Forensics' and 'WhatsApp Xtract' with a contact ID '390123456789@cs.whatsapp.net'. Below this is a table with columns: 'PK', 'Contact Name', 'Contact ID', 'Status', 'if Msg', 'if Unread Msg', and 'Last Message'. The main part of the interface shows a 'Chat session # 4: Giovanni' with a table of messages. The messages table has columns: 'PK', 'Chat', 'Msg date', 'From', 'Msg content', 'Msg status', 'Status Type', and 'Status Acc'. The messages are as follows:

PK	Chat	Msg date	From	Msg content	Msg status	Status Type	Status Acc
1114	Giovanni	2010-09-11 18:51:44	Giovanni	Ciao ☺	2		
1115	Giovanni	2010-09-14 18:24:14	me	Ciao! Ci vediamo sabato pomeriggio?	2		
1116	Giovanni	2010-09-14 19:25:08	Giovanni	Maggio sabato sera	2		
1114	Giovanni	2010-09-14 19:25:52	Giovanni	Andiamo a bere qualcosa	2		
1115	Giovanni	2010-09-14 19:26:14	me	OK	1		
1116	Giovanni	2010-09-14 19:26:14	me	 I Smile	1	10%	42001
1140	Giovanni	2010-10-14 14:14:14	Giovanni	Ciao!	2		



# Panoramica dei software OS

Non esistono molti software e spesso sono orientati a un solo task.

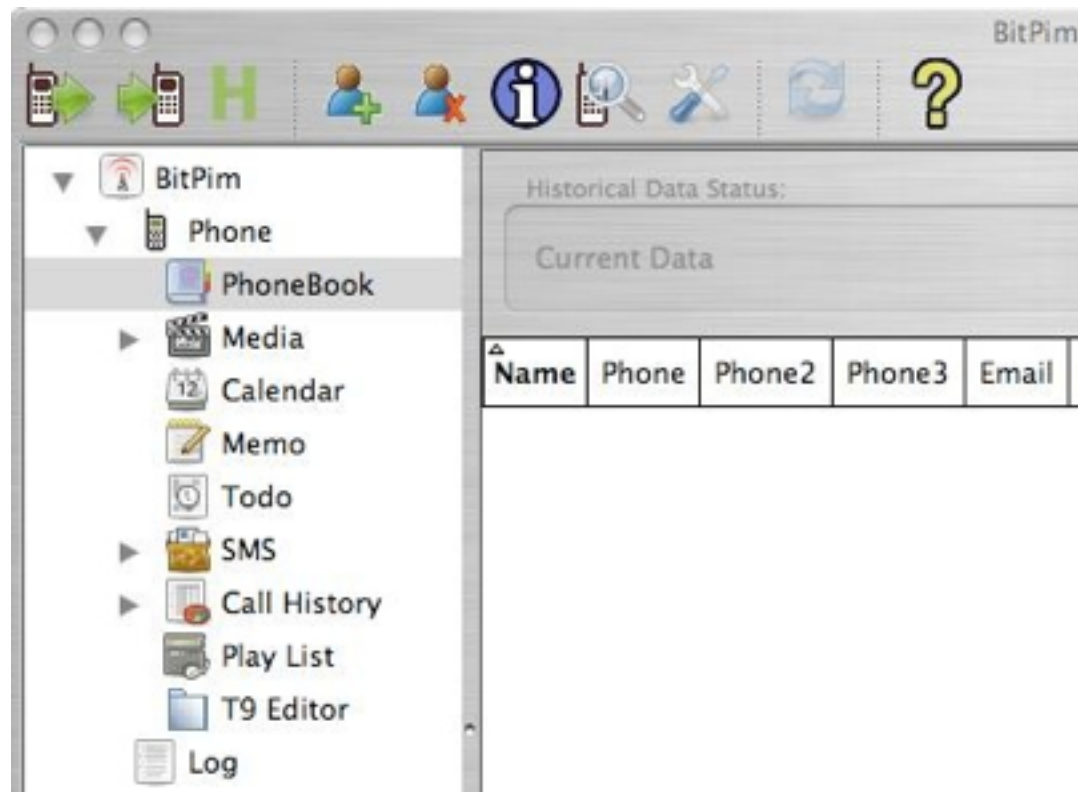
- Bitpim
- iPBA (iPhone Backup Analyzer)
- Sql lite database browser
- Bulk extractor
- Strings
- Foremost
- pySIM and TULP2G
- Hex editors come XXD and Ghex2





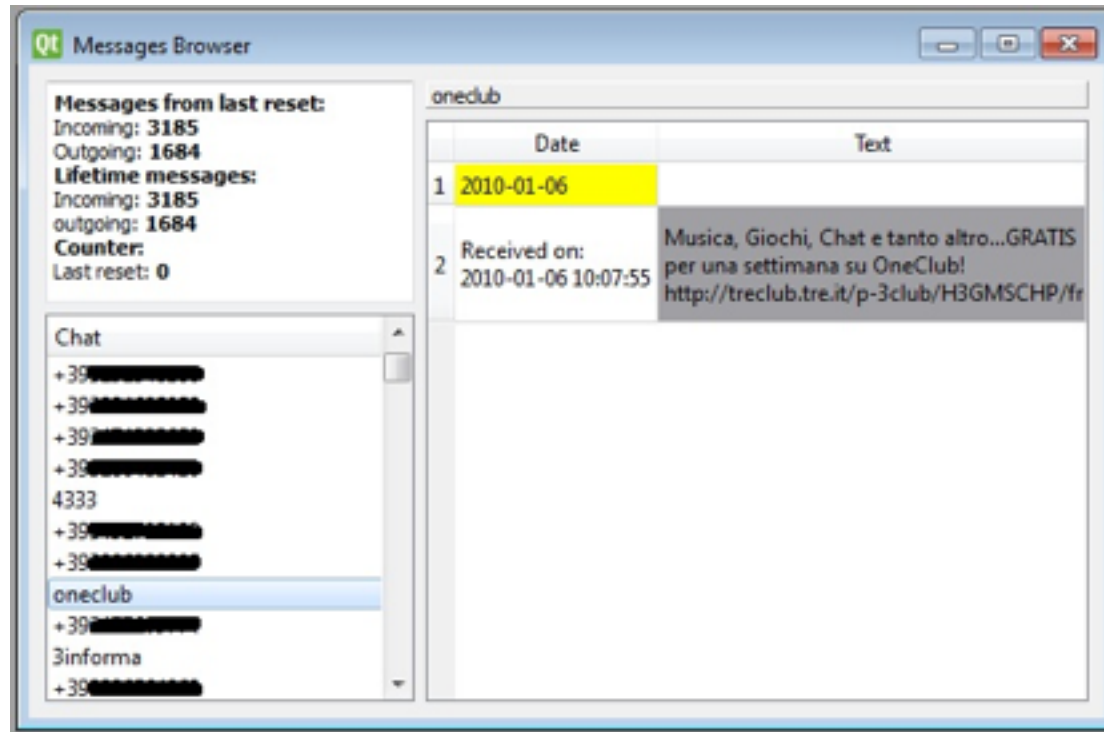
# Bitpim

- Acquisizione logica e parsing di dati da cellulari CDMA come LG, Samsung and Sanyo. Estrae Address book, SMS, Agenda, Photos, Memo



# iPBA

Software italiano che permette di analizzare iPhone Backups, con una GUI versatile ma anche un hex/text editor per approfondimenti. Estrae Address book, Call history, Sms, Browsing history (Safari), Whatsapp, Viber, Skype chat history e sono in fase di sviluppo diversi nuovi plugin



# Sqlite database browser

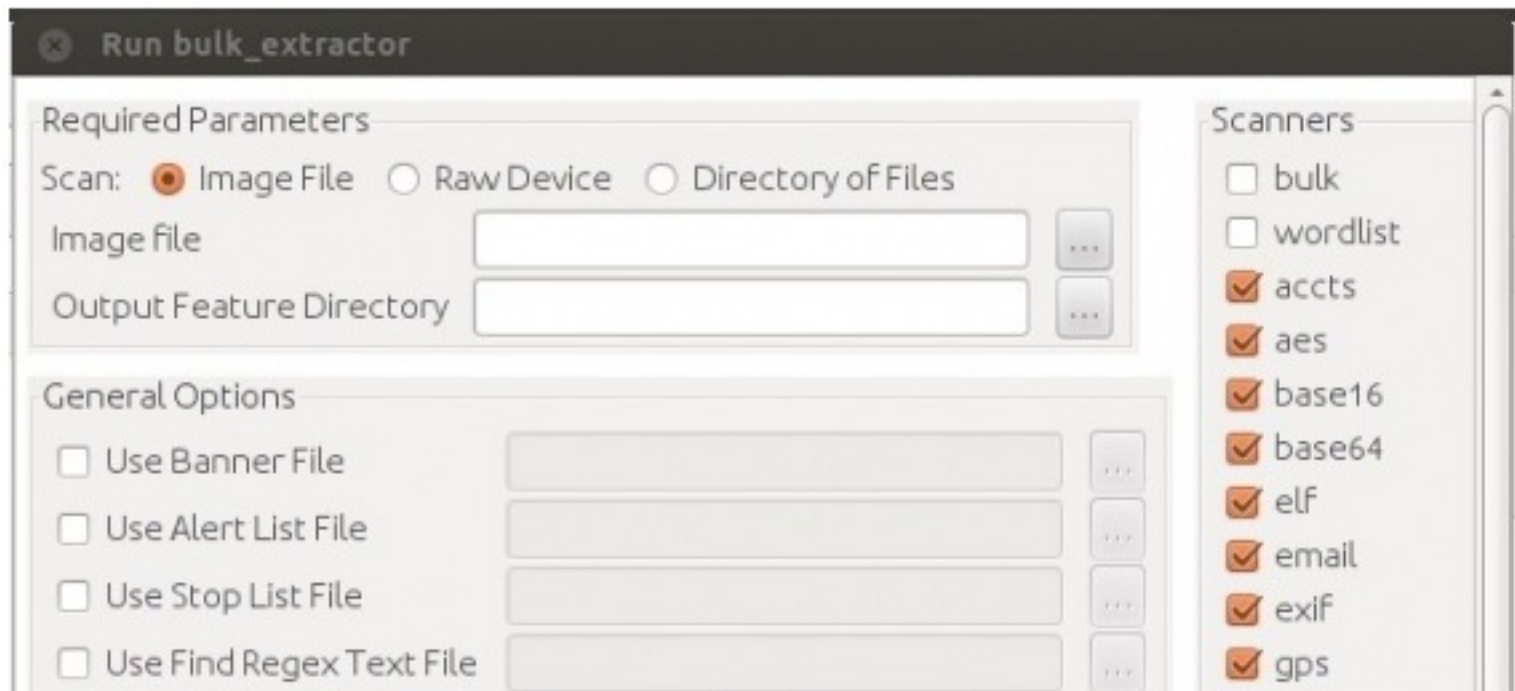
- Molte applicazioni usano i database sqlite per memorizzare i dati e le impostazioni, basti pensare a Chrome, Firefox, Skype, etc...

The screenshot shows the SQLite Database Browser application window. The title bar reads "SQLite Database Browser - C:/Users/Richard Drinkwater/Desktop/Chrome Export/History". The menu bar includes "File", "Edit", "View", and "Help". The toolbar contains icons for file operations and a help icon. Below the toolbar are three buttons: "Database Structure", "Browse Data", and "Execute SQL". A "Table:" dropdown menu is set to "urls". To the right of the dropdown are "New Record" and "Delete Record" buttons. The main area displays a table with the following columns: "id", "url", "title", "visit", "typed", "last visit time", "hidden", and "favicon ik". The table contains 51 records, with the 51st record (id 608) highlighted in blue. The record details are: id: 608, url: http://www.sqlite.org/fileformat2.html, title: File Format For SQLite Databases, visit: 1, typed: 0, last visit time: 12949409092779476, hidden: 0, favicon ik: 46. At the bottom of the window, there are navigation buttons: "< 1 - 51 of 51 >" and "Go to: 0".

id	url	title	visit	typed	last visit time	hidden	favicon ik
45	602 http://forensicsfromthesausagefactory.b	Forensics from the sausage factor	3	0	12949409095515476	0	45
46	603 http://www.blogger.com/navbar.g?target		3	0	12949409095932476	1	0
47	604 http://googleads.g.doubleclick.net/page		3	0	12949409095939476	1	0
48	605 http://googleads.g.doubleclick.net/page		3	0	12949409095942476	1	0
49	606 http://googleads.g.doubleclick.net/page		3	0	12949409095959476	1	0
50	607 http://www.sqlite.org/fileformat.html	SQLite Database File Format	1	0	12949409086333242	0	46
51	608 http://www.sqlite.org/fileformat2.html	File Format For SQLite Databases	1	0	12949409092779476	0	46

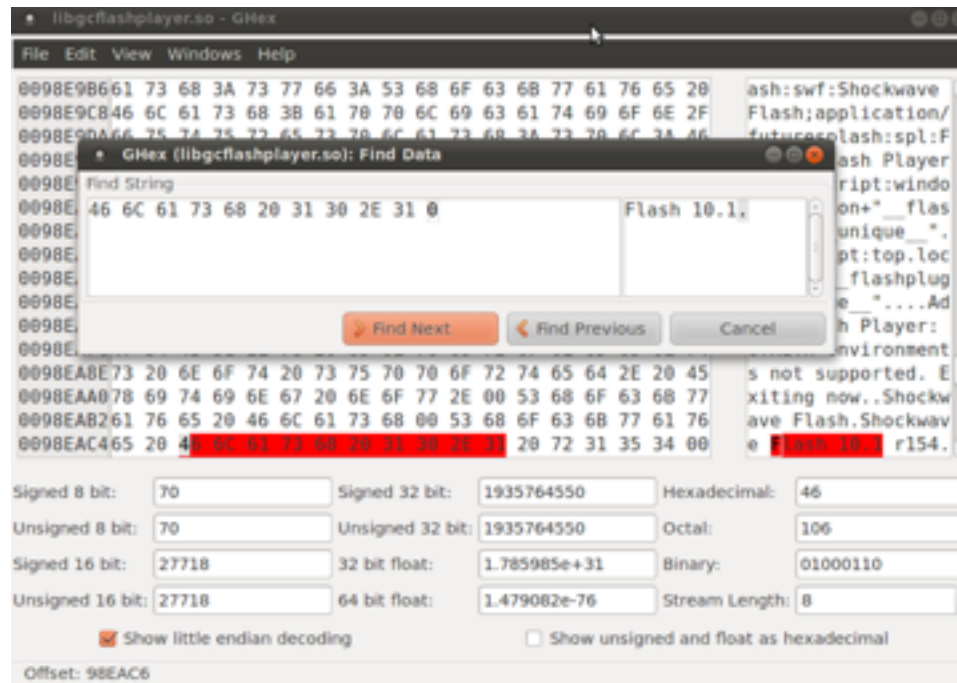
# Bulk extractor

- Parser dotato da poco anche di GUI che prende in input immagine o dispositivo raw oppure file ed estrae artefatti come indirizzi email, carte di credito, URL, ricerche su Google, numeri di telefono, wordlist, IP, custom parser, white/black list, REGEXP, etc..



# XXD e Ghex2

- Due dei più comuni editor di file esadecimali/ascii (ci sono poi anche hexdump, od, etc...) con due colonne: hex a sinistra e ASCII a destra
- Aprendo un file (immagine forense, etc..) con un editor esadecimale si riesce a farsi un'idea del tipo di contenuto, fare ricerche, osservare eventuali parti in chiaro, etc...



# Il caso “Le Iene”



- Nokia E72, Symbian 9.3
- Factory reset eseguito sul cellulare
- MicroSD interna formattata
- Obiettivo: recuperare tutto il possibile

# Il caso “Le lene” ci porta al...

- Come abbiamo deciso di procedere:
- Physical dump con UFED per la memoria interna
- Bit stream image per la microSD card
- Secondo physical analyzer, il physical dump del dispositivo non conterrebbe alcun dato...



## Call Log (1)

### Unknown (1)

#	Country code	Network code	Party	Time	Duration	Video call	Source	Del?
1			+39[REDACTED]	23/11/20[REDACTED] 16:08:30(UTC+0)	00:00:14			

## SMS Messages (2)

### Sent (2)

#	Party	Time	Status	Message	Del?
1	From: +39[REDACTED] To: 34[REDACTED]	23/11/20[REDACTED] 15:53:14(UTC+0)		PAIF QU5WZwaggEAAUMWIFcHxQIA3gMCSVQEOsBt3foDFM6LE+Nzn1wZ m6NdKIFAQcBCAQMAAEAIQGB	Yes
2	From: +39[REDACTED] To: 34[REDACTED]	23/11/20[REDACTED] 15:53:14(UTC+0)		PAIF QU5WZwaggEAAUMWIFcHxQIA3gMCSVQEOsBt3foDFM6LE+Nzn1wZ m6NdKIFAQcBCAQMAAEAIQGB	

# Il caso “Le Iene” ci porta al...





# ... parsing manuale!

```
13eab350:ffb2 c022 0000 [REDACTED] ..."  
13eab360:7563 636f 6c69 0700 0000 3380 616d 6f72 [REDACTED].....3.amor  
13eab370:2073 6f6e 6f20 6461 7661 6e74 6920 6120 sono davanti a  
13eab380:6172 6d61 6e69 2073 7520 7669 6120 6d61 armani su via ma  
13eab390:6e7a 6f6e 692e 2065 7361 7474 616d 656e nzoni. esattamen  
13eab3a0:7465 2064 6176 616e 7469 2061 1a2b 3339 te davanti a.+39  
13eab3b0:[REDACTED] 3831 1800 0000 0001 3476 [REDACTED]1.....  
13eab3c0:0000 0000 0000 0000 0000 0000 0000 0001 .....  
13eab3d0:0000 005a 0055 4112 a6b5 5fe1 0001 70c2 ...Z.UA..._...p.  
13eab3e0:2200 0014 4769 756c 6920 4a6f 6c6b 0700 "... [REDACTED]..  
13eab3f0:0500 0000 6302 311a 2b33 3933 [REDACTED] ....c.1.+39348 [REDACTED]
```

# Parsing manuale

Posso automatizzare il recupero degli sms in un Nokia E72?

Posso provarci, con il datacarving

- Identifico un header ed un possibile footer
- Se gli sms non hanno un footer, definisco un numero massimo di bit per passare al prossimo header



# Parsing manuale

## Header

03	90	2C	F0	54	E4	5F	E1	00	FF	B2	DD	23	00	00	0C	54	...	.T.	_	.....	#	...	T
77	65	65	74	79	02	00	04	00	33	20	54	77	65	65	65	65	weety	....	3	Tweeee			
65	65	65	65	74	79	3F	3F	3F	21	1A	2B	33	39	33	34	39	eeeety	???	!.	+39349			

## Footer

00	33	28	53	6E	20	61	6E	64	61	74	61	20	61	20	63	6F	.	3	(Sn	andata	a	co
6D	6F	20	4C	4F	4C	1A	2B	33	39								mo	LOL.	+39			
39	38	34	18	02	00	00	00	01	00	00	00	01	00	00	00	00	984.	.....				

# Parsing manuale

extension	case sensitive	size	header	footer
# SMS Nokia E72				
sms	y	200000	\x23\x00\x00\x0c	\x18\x02\x00\x00
sms+39	y	200000	\x1a\x2b\x33\x39	

I valori di header e footer sono in esadecimale

Il campo size rappresenta il massimo numero di byte che foremost recupera se non trova il footer

```
foremost -c /etc/foremost.conf -o sms/ dump.bin
```



# Parsing manuale

Recuperare immagini e video

- Utilizzo il mio carver di fiducia
  - ◆ Foremost
  - ◆ Photorec
  - ◆ Scalpel2

Sia sul dump ufed che sulla dd della microSD



# Parsing manuale

Recuperare dati della navigazione Internet

- Eseguo strings sull' immagine

```
strings dump.bin > output.txt
```

- Eseguo un grep di http://, https:// o www

```
grep http:// output.txt > navigazione.txt
```



# Grazie per l'attenzione! :-)

Per domande o contatti:

Dr. Paolo Dal Checco

paolo@dalchecco.it - @forensico

