UNIVERSITÀ DI MACERATA

l'umanesimo che innova

L'ANDROID FORENSICS E IL RECUPERO DEI DATI CANCELLATI

"I molteplici profili della sicurezza"

Macerata, 2 Dicembre 2016

Anna Biselli

CHI SONO?

Anna Biselli

- Laureata in Informatica

- Membro Camelug

- Membro IISFA

- Junior Penetration Tester

ARGOMENTI

- Cos'è la Digital Forensics
- Database SQLite: cos'è e che ruolo ha nell'acquisizione di dati cancellati
- Acquisizione SMS
- Acquisizione Skype
- Acquisizione Messenger Facebook
- Acquisizione Telegram
- Acquisizione Whatsapp
- Un breve accenno sull'Antiforensics

COS'È LA DIGITAL FORENSICS

"Nuova intersezione tra il mondo giuridico e informatico che consiste nello specializzarsi in quei reati definiti crimini informatici (cioè quei reati introdotti nel Codice Penale dalla legge 547/93)"

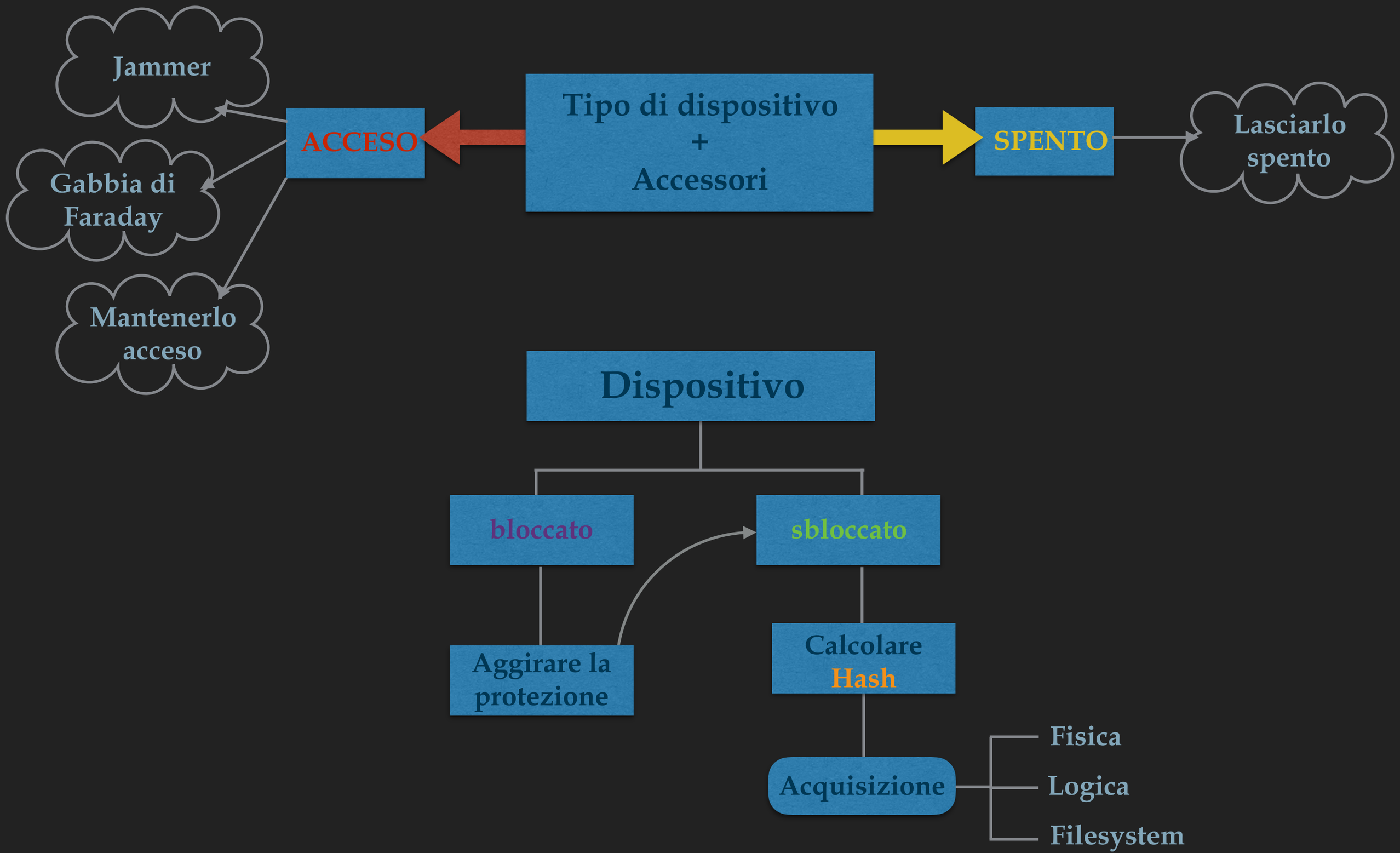
L'illecito informatico, pur essendo un illecito penale di nuova generazione è ormai il più diffuso. In questo nuovo contesto sono coinvolti sia il diritto che l'informatica, formando così una vera e propria disciplina orientata all'attività investigativa digitale.

CHI È L'INFORMATICO FORENSE

Come l'investigatore deve immedesimarsi nel criminale per capire le sue prossime mosse, l'informatico forense deve avere la conoscenza della persona con cui ha a che fare, la professionalità di un operatore dell'IT e la conoscenza di base del diritto

Da questa esigenza ha preso corpo
la nascita di sezioni specializzate delle forze dell'ordine, come ad esempio la Polizia Postale e delle Comunicazioni, il GAT-Gruppo Anticrimine Tecnologico della Guardia di Finanza, i RIS-Reparti Investigazioni Scientifiche dei Carabinieri con le sezioni specializzate come la RTI-Sezione Telematica del Reparto Tecnologie Informatiche operante all'interno del RaCIS-Raggruppamento Carabinieri Investigazioni Scientifiche.

SEQUESTRO E ANALISI DI UN DISPOSITIVO MOBILE



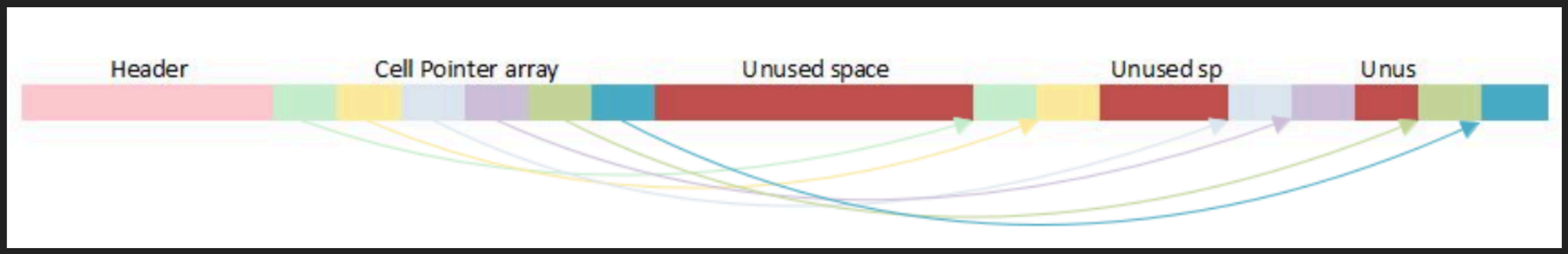
DATABASE SQLITE

CARATTERISTICHE:

- sicuro
- integro
- consistente
- condivisibile
- persistente
- scalabile

Ogni applicazione negli smartphone ha un database.

Un database può essere considerato come una raccolta di dati correlati, memorizzati su un supporto di memoria di massa e progettati per essere fruiti da diverse applicazioni e utenti



ACQUISIZIONE SMS

SANTOKU → AFLogicalOSE → Acquisizione Logica

```
santoku@ubuntu: ~
File  Edit  Tabs  Help
$ aflogical-ose -h

run 'aflogical-ose' with usb debugging enabled in your android device

santoku@ubuntu:~$ adb devices
List of devices attached
55fa5db0        device

santoku@ubuntu:~$ aflogical-ose
Make sure android device is connected to USB
[sudo] password for santoku:

295 KB/s (28794 bytes in 0.095s)
        pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk
Success

Starting: Intent { cmp=com.viaforensics.android.aflogical_ose/com.viaforensics.a
ndroid.ForensicsActivity }

Press enter to pull /sdcard/forensics into ~/aflogical-data/

pull: building file list...
pull: /sdcard/forensics/20150619.1111/SMS.csv -> /home/santoku/aflogical-data/20
150619.1111/SMS.csv
pull: /sdcard/forensics/20150619.1111/MMSParts.csv -> /home/santoku/aflogical-da
ta/20150619.1111/MMSParts.csv
pull: /sdcard/forensics/20150619.1111/Contacts Phones.csv -> /home/santoku/aflog
ical-data/20150619.1111/Contacts Phones.csv
pull: /sdcard/forensics/20150619.1111/MMS.csv -> /home/santoku/aflogical-data/20
150619.1111/MMS.csv
```

adb devices: per verificare che il device è connesso al programma

aflogical-ose: per installare l'applicazione nel device

SMS.csv - Gnumeric

File Edit View Insert Format Tools Statistics Data Help

L19: Dammi 2 minuti e sono li

	H	I	J	K	L	M	N	O	P	Q
19	−1	1	0		Dammi 2 minuti e sono	393916263333	0	0	1	1
20	−1	2			Pronto		0	0	1	1
21	−1	2			È andata via la corrente		0	0	1	1
22	−1	1	0		ALL-IN 300 sara? attiva p	393916263333	0	0	1	1
23	−1	1	0		ALL-IN 300 sara? attiva p	393916263333	0	0	1	1
24	−1	2			Ho cancellato il tuo contatto che avevo		0	0	1	1
25	−1	1	0		Bene bene 😄	393492000200	0	0	1	1
26	−1	2			Sembra bene! Non mi arrivano i messac		0	0	1	1
27	−1	1	0		Com'è andata? 😄	393492000200	0	0	1	1
28	−1	2			Ciao amore,che fai?		0	0	1	1
29	−1	2			Non ci lamentiamo dai...un pò freddino,		0	0	1	1
30	−1	1	0		Bene ! Com'è il tempo a	393492000200	0	0	1	1
31	−1	2			Bene grazie! Tu?		0	0	1	1
32	−1	2			Ciao come stai?		0	0	1	1
33	−1	1	0		Ciao	393492000200	0	0	1	1
34	−1	1	0		ALL-IN 300 sara? attiva p	393916263333	0	0	1	1

SMS.csv Sum = 0

ACQUISIZIONE SMS

SANTOKU →  → Acquisizione Filesystem

Il database che contiene tutti i messaggi è “logs.db”

em Browser ✕ | logs.db ✕

31 records

Date	Read	Type	Body
2015-06-18 08:18:07	✓	Inbox	Com'è andata? 😀
2015-06-18 08:14:59	✓	Sent	Ciao amore,che fai?
2015-06-18 08:13:26	✓	Sent	Non ci lamentiamo dai...un pò freddino
2015-06-18 08:11:41	✓	Inbox	Bene ! Com'è il tempo a Civitanova?

```
1  select*
2  from logs
```

Durata: 0.001 secondi * Col: 10 Row: 2/2

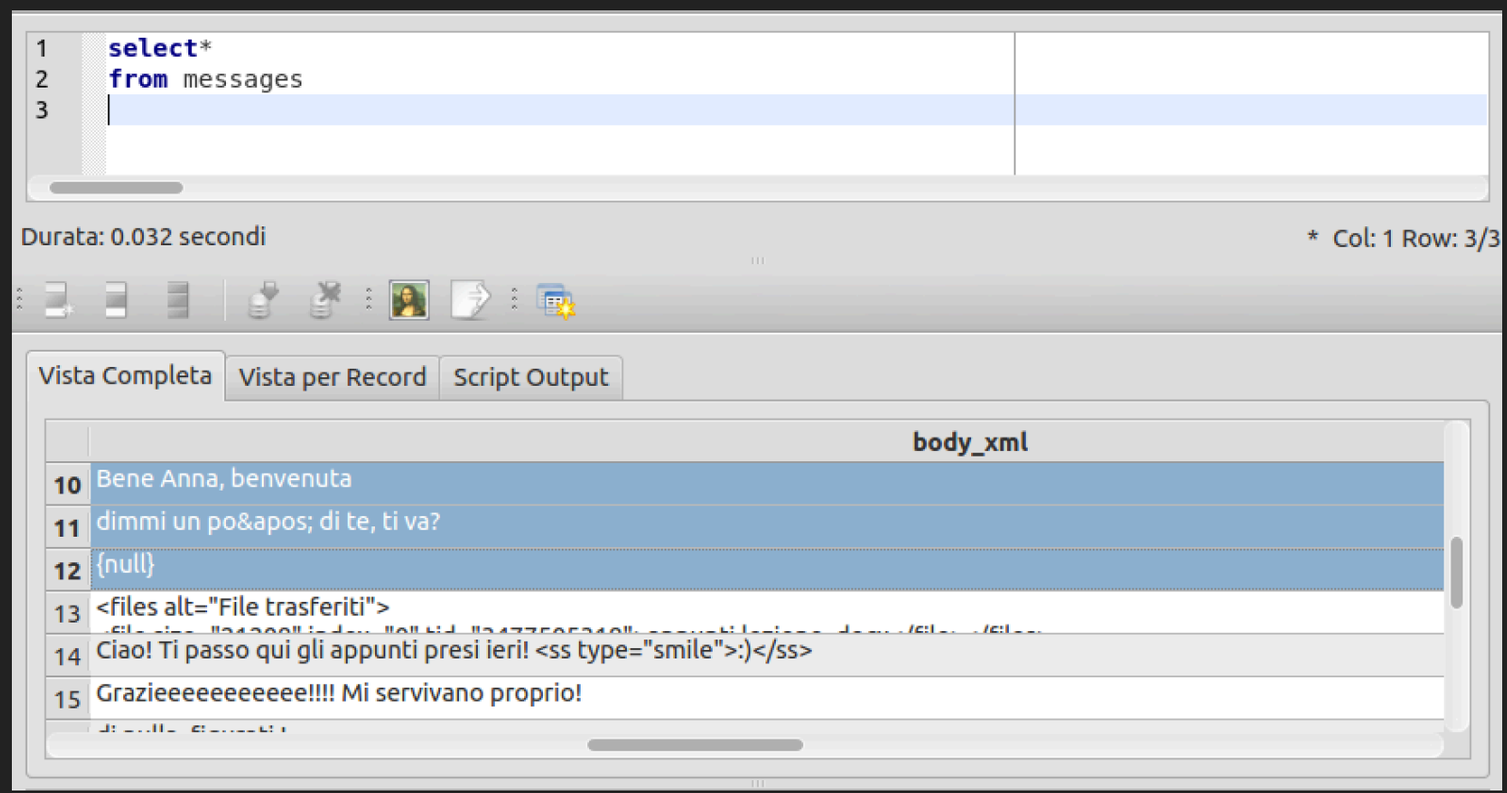
Vista Completa | Vista per Record | Script Output

	messageid	logtype	frequent	contactid	raw_contact_id	m_subject	m_content	sns_
10	10	300	{null}	16	16	{null}	Bene ! Com'è il tempo a Civitanova?	{null}
11	11	300	{null}	16	16	{null}	Non ci lamentiamo dai...un…	{null}
12	13	300	{null}	19	19	{null}	Ciao amore,che fai?	{null}
13	14	300	{null}	19	{null}	{null}	Configuro questo modem …	{null}
14	16	300	{null}	19	19	{null}	Eh,questa era una prova u…	{null}
15	17	300	{null}	19	{null}	{null}	Com'è andata? 😀	{null}

ACQUISIZIONE SKYPE

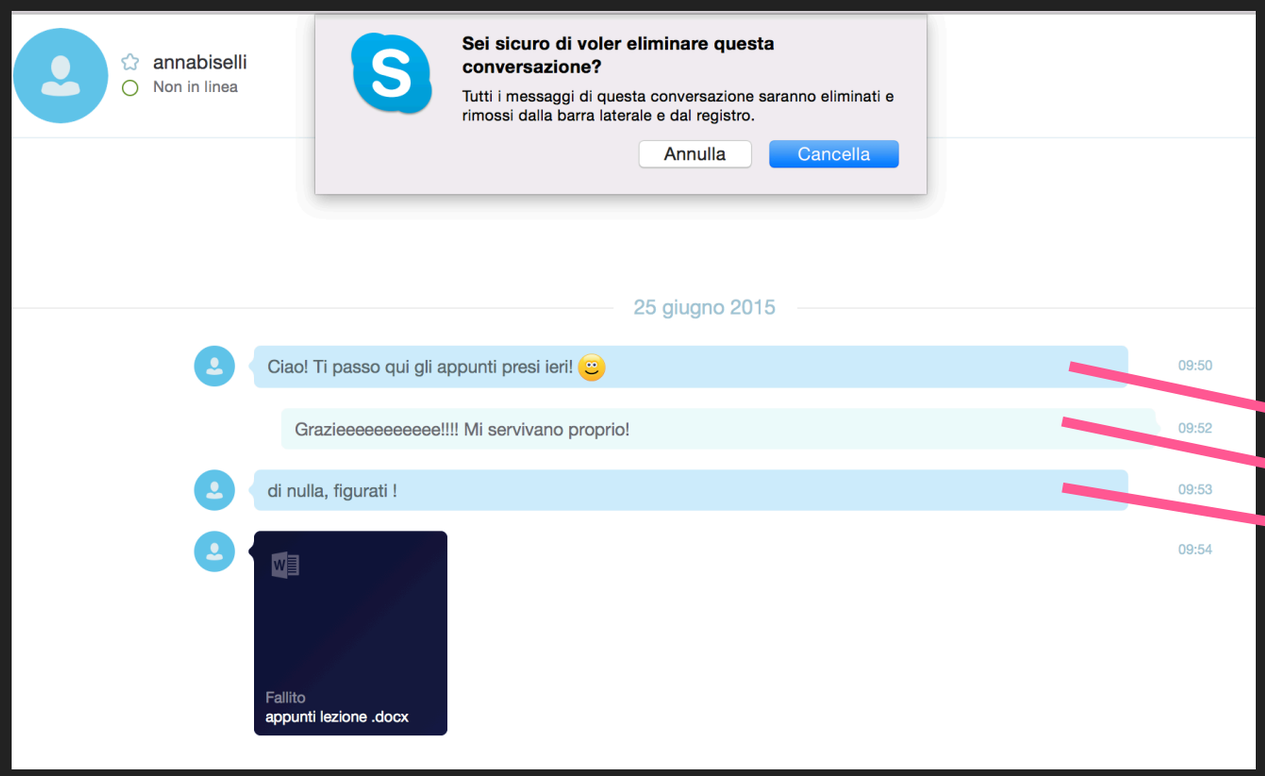
Si è creato un profilo Skype (annarossi) e si è finta una conversazione con “infinito2006”

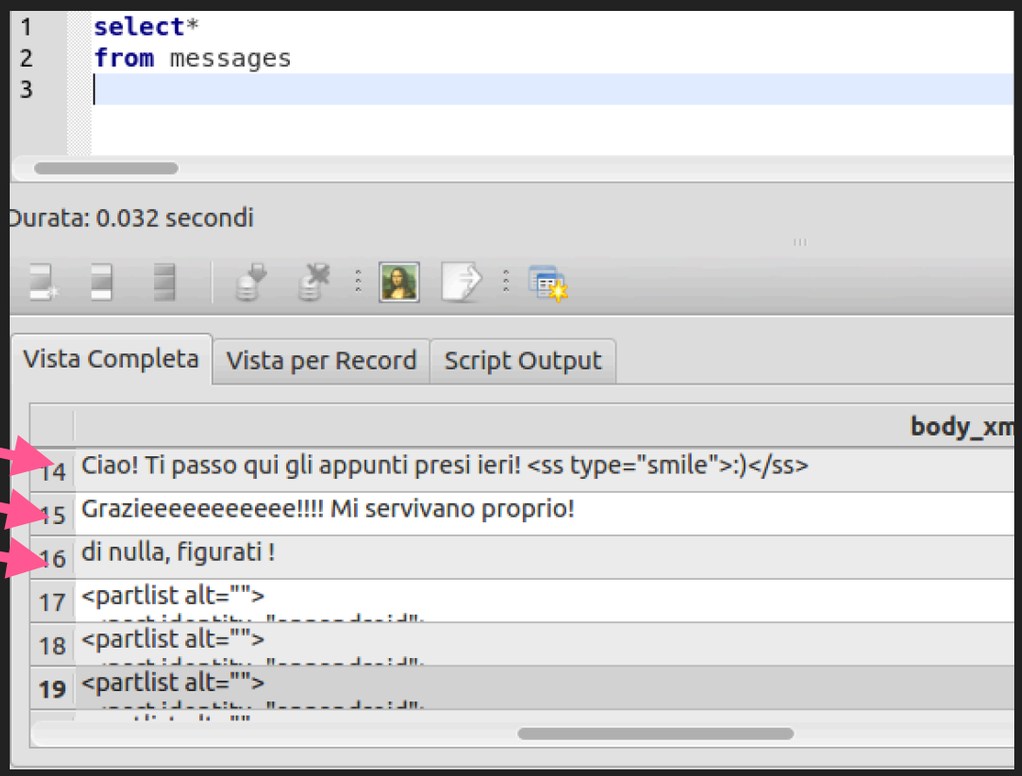
Dopo l’acquisizione, nella tabella *messages* di “main.db” si troveranno tutti i messaggi



ACQUISIZIONE SKYPE

Anna Rossi in questo caso inizia una chat con l'utente "annabiselli" che verrà completamente cancellata

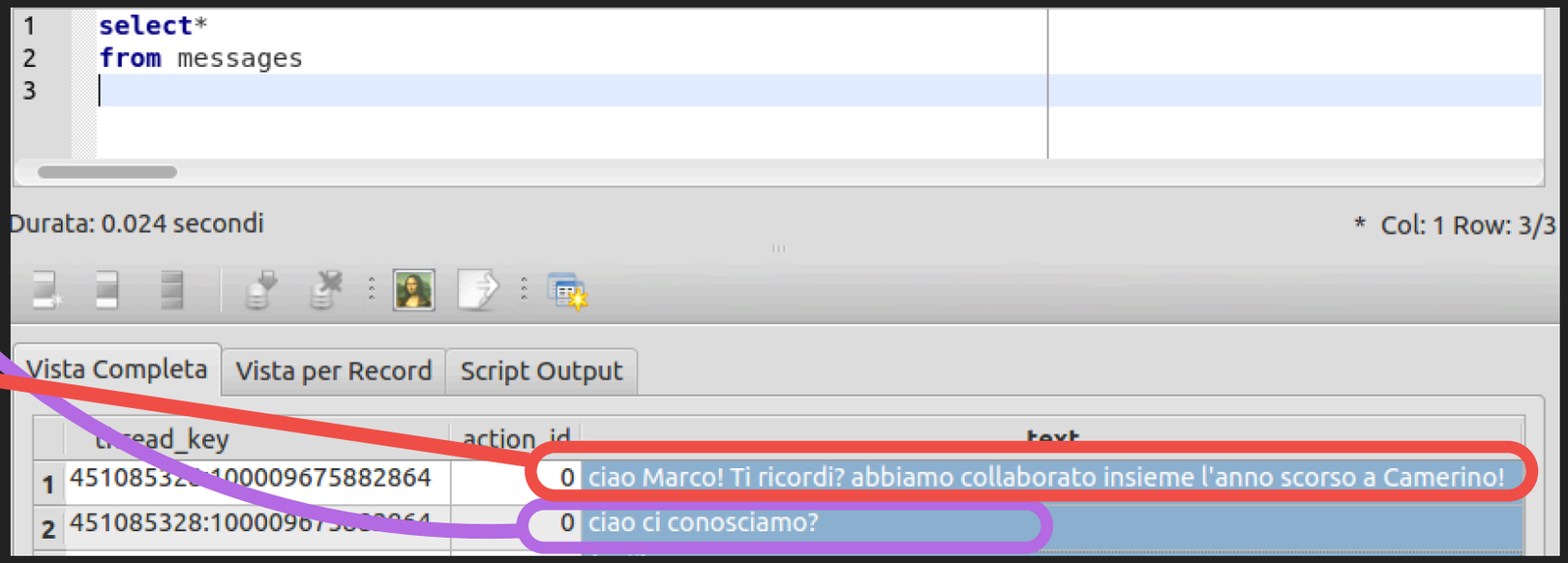




Aprendo il database con Sqliteman si nota che non ci sono differenze tra i messaggi automatici che Skype invia quando si aggiunge un contatto, tra quelli non cancellati e tra i cancellati

ACQUISIZIONE MESSENGER FACEBOOK

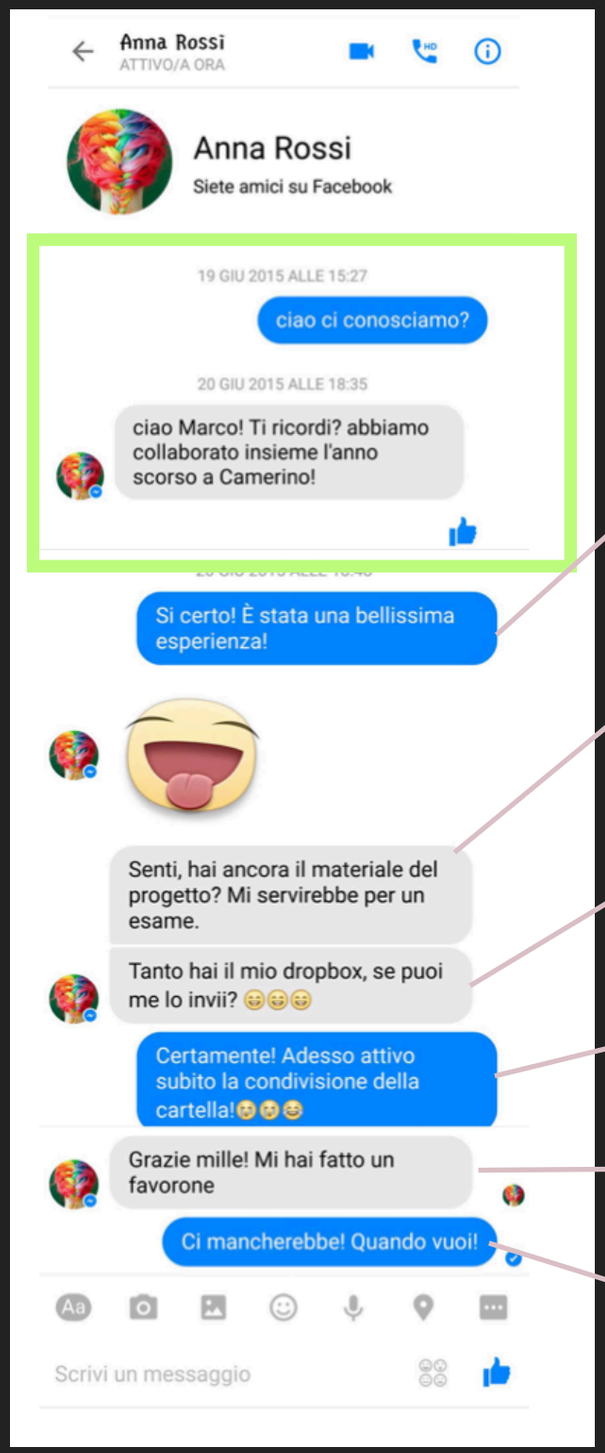
Si è creato il profilo facebook di Anna Rossi e si sono scambiati dei messaggi di chat con il suo amico Marco



I dati delle chat di messenger si trovano dopo un'aquisizione del Filesystem nel file "Threads_db2".

ACQUISIZIONE MESSENGER FACEBOOK

Si ipotizzi che della chat tenutasi con Marco rimangano solo i primi tre messaggi:




```
34 00 53 69 20   882864.Si certo!
74 61 74 61 20    .. stata una be
69 6D 61 20 65   llissima esperie
22 65 6D 61 69   nza!{"email":nul
```

```
74 69 2C 20 68   4.Senti, hai anc
6C 20 6D 61 74   ora il materiale
70 72 6F 67 65    del progetto? M
76 69 72 65 62   i servirebbe per
73 61 6D 65 2E    un esame.{"emai
```

```
00 54 61 6E 74   82864.Tanto hai
6F 20 64 72 6F   il mio dropbox,
6F 69 20 6D 65   se puoi me lo in
F0 9F 98 84 F0   vii? ..........
```

```
38 38 32 38 36   09675882864.Cert
65 21 20 41 64   amente! Adesso a
20 73 75 62 69   ttivo subito la
76 69 73 69 6F   condivisione del
72 74 65 6C 6C   la cartella!....
```

```
34 00 47 72 61   882864.Grazie mi
4D 69 20 68 61   lle! Mi hai fatt
66 61 76 6F 72   o un favorone{"e
```

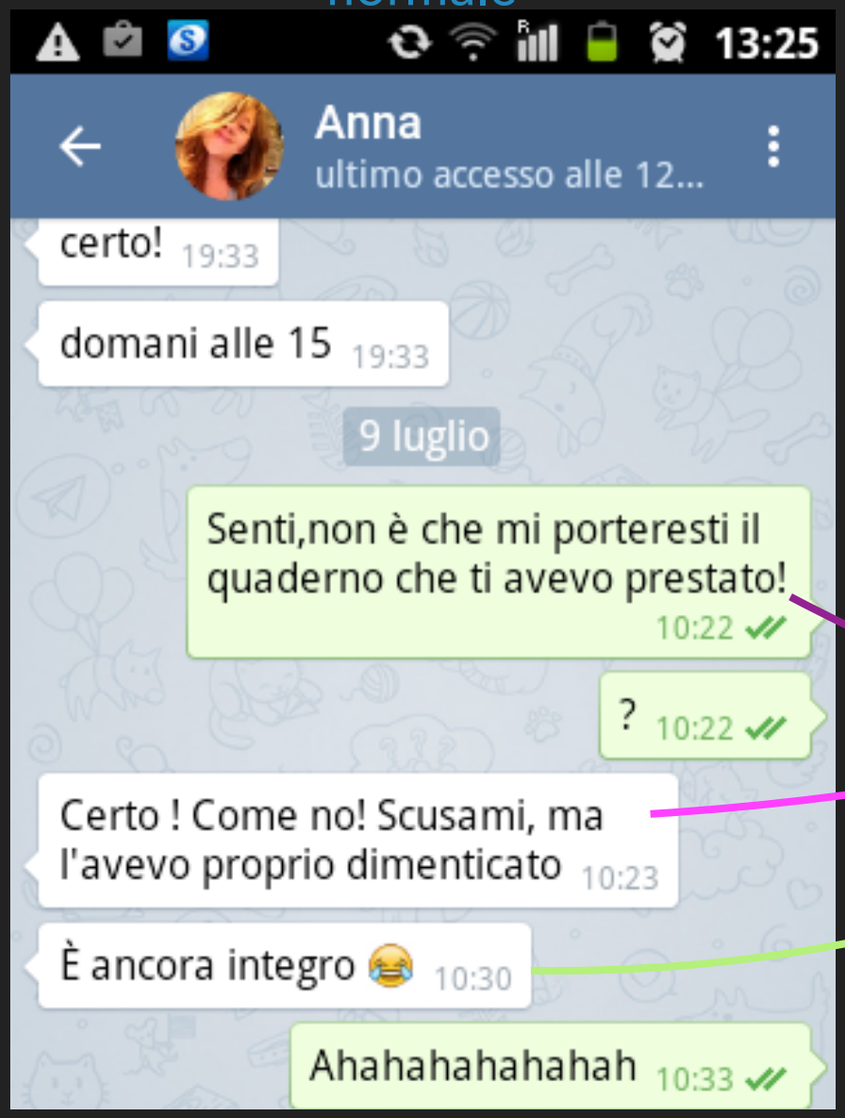
```
34 00 43 69 20   882864.Ci manche
21 20 51 75 61   rebbe! Quando vu
65 6D 61 69 6C   oi!{"email":null
```

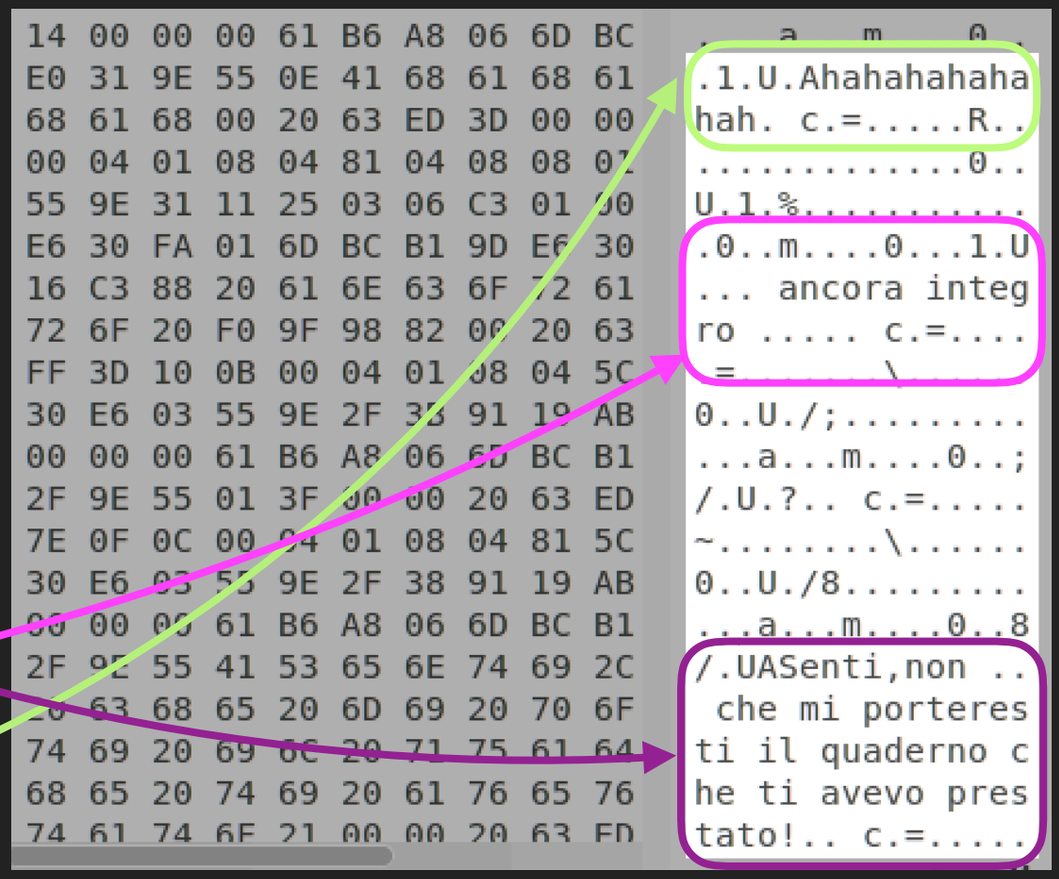
Tra le tabelle del database non si trovano i messaggi cancellati, quindi si cerca nell'esadecimale

ACQUISIZIONE TELEGRAM

Telegram ha il suo database nominato “cache4.db”.
Le conversazioni costruite sono 2: una normale con Anna Biselli e una “crittata” con Alessandro

“normale”





I messaggi si trovano solo spulciando nell’ esadecimale del database perchè Telegram filtra tutti i dati con BLOB (Binary Large Object) che non viene riconosciuto dalla maggior parte dei database.

ACQUISIZIONE TELEGRAM


```
CB FC FF 00 00 00 00 4A 26 72   .......J&r.m...a
B6 A8 06 C0 32 9E 55 16 41 75   ....2.U.Autodist
72 75 7A 69 6F 6E 65 20 66 72   ruzione fra....
63 ED 3D 00 00 00 00 FF 45 FF   c.=.....E.......
CB A6 0B 00 06 01 08 04 64 08   ........d.......
6F 00 00 00 00 03 55 9E 32 C2   o.....U.2..UUU..
```

```
00 00 A6 CB FC FF 00 00 00 00   ..........J&r.m.
B1 9D 61 B6 A8 06 C2 32 9E 55   ..a....2.U.3.. c
ED 3D 00 00 00 00 FF 45 FF FF   .=.....E........
```

```
9D 61 B6 A8 06 C3 32 9E 55 01   .a....2.U.2.. c.
```

```
61 B6 A8 06 C4 32 9E 55 01 31   a....2.U.1.. c.=
```

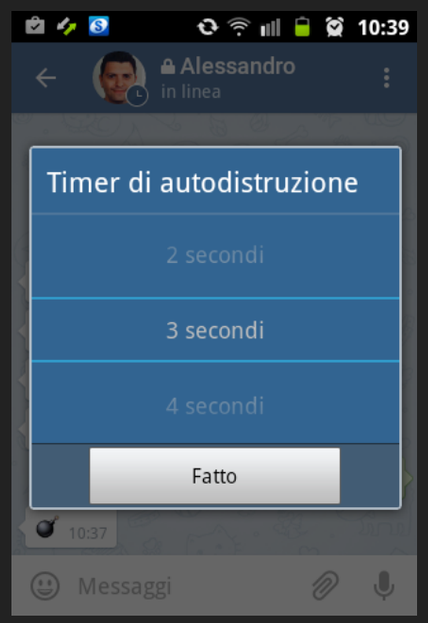
```
04 74 09 08 01 00 03 D6 91 6F   .t.......o.....U
9E 32 D8 F8 55 55 55 03 00 00   .2..UUU.........
00 00 00 61 B6 A8 06 6D BC B1   ...a...m...J&r..
32 9E 55 08 42 55 4D 21 F0 9F   2.U.BUM!........
63 ED 3D 00 00 00 00 FF 49 FF   c.=.....I.......
CB A2 0B 00 06 01 08 04 6C 08   ........l.......
```

Come si può notare, le chat segrete sono salvate in locale in plaintext come un qualunque altro messaggio non cancellato.

ACQUISIZIONE TELEGRAM

Per recuperare i cancellati, si sono eliminati diversi messaggi della chat che Anna Rossi ha scambiato con Anna e si è impostato il timer di autodistruzione nella chat con Alessandro

Probabilmente i messaggi, una volta cancellati, vanno a finire in una porzione di memoria non recuperabile, perchè non vi è traccia nelle acquisizioni fatte



Telegram è chiaro quando parla del timer di autodistruzione:

"il messaggio scompare da entrambi i dispositivi e non lascia traccia"

quindi è probabile che questo tipo di messaggio effettivamente non venga salvato in locale

ACQUISIZIONE WHATSAPP

Per l'acquisizione di Whatsapp viene riportata la chat tra Anna Rossi e Leo


```
1  select*
2  from messages
3
```

Durata: 0.043 secondi

* Col: 1 Row: 3/3

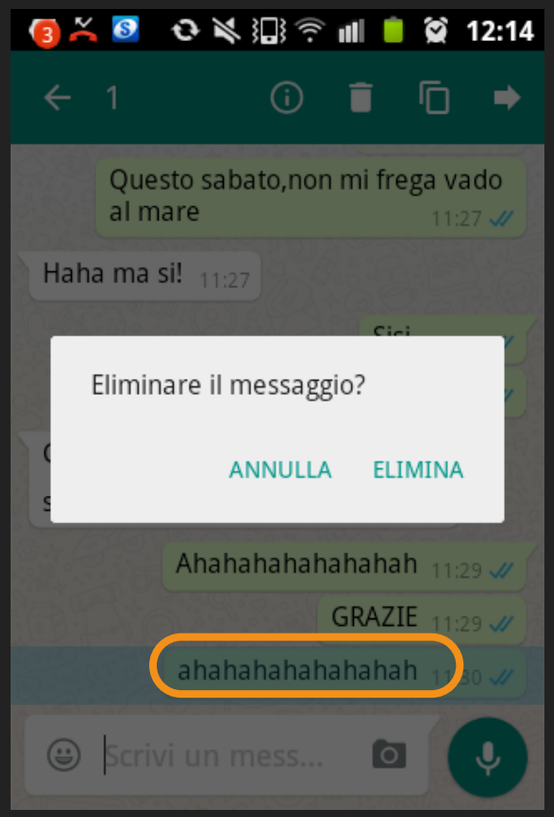
Vista Completa | Vista per Record | Script Output

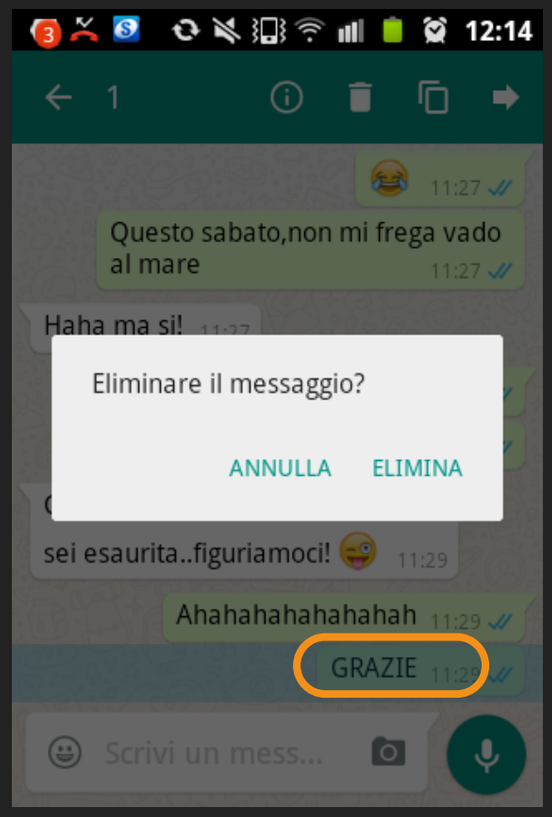
	needs_push	data	timestamp	media_url	media_mime_type
24	0	Sisi.	1436434158145	{null}	{null}
25	0	Sennò mi esaurisco	1436434176414	{null}	{null}
26	0	Già non parti bene quando non sei esaurita..figuriamoci! 😜	1436434222000	{null}	{null}
27	0	Ahahahahahahahah	1436434235075	{null}	{null}
28	0	GRAZIE	1436434244474	{null}	{null}
29	0	ahahahahahahahah	1436434253998	{null}	{null}

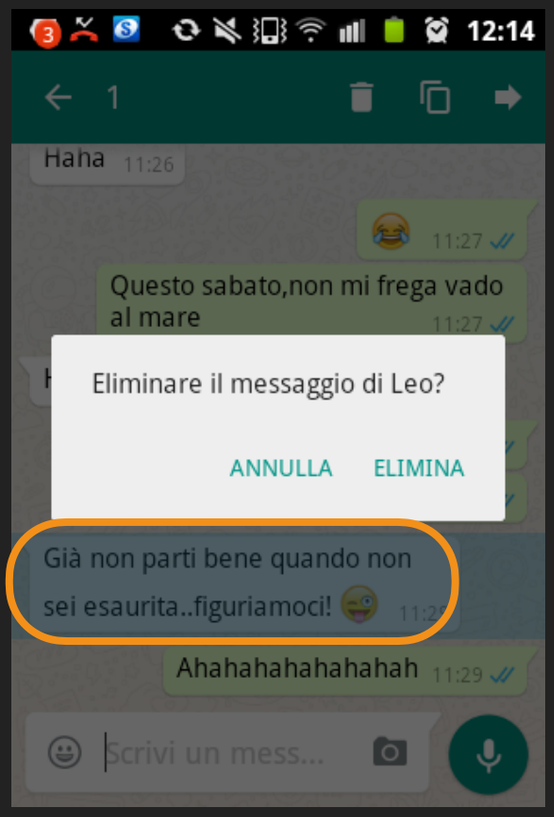
Il database di riferimento è "msgstore.db"

ACQUISIZIONE WHATSAPP

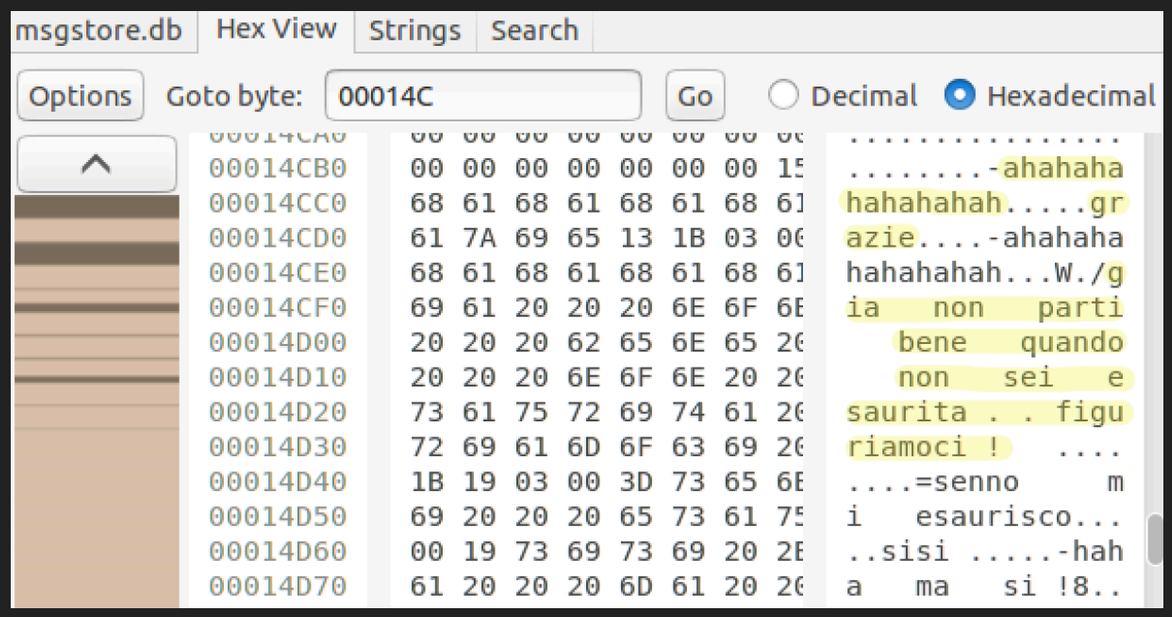
Per fare una prova si cancellano i seguenti messaggi:







Nel database msgstore non c'è traccia dei cancellati, quindi si va a cercare nell'esadecimale



Nell'esadecimale non solo si trovano i messaggi cancellati, ma anche tutta la conversazione per intero come quella prima di essere modificata

ANTI-FORENSICS

L’Anti-forensics è definita :

“Insieme di tecniche che mirano a confondere i tool, o usare i tool e i loro risultati per confondere l'analista forense”

E se qualcuno riuscisse a modificare il testo di una vostra chat?
Senza andare troppo lontano, anche nella vita di tutti i giorni si possono immaginare le conseguenze di una chat “scomoda” nel proprio cellulare!

ESPERIMENTI

Sempre nello stesso cellulare, si è costruita una **falsa prova** nell'applicazione di messaggistica più utilizzata Whatsapp:

1. Cambiare il testo di un messaggio ricevuto in precendenza
2. Aggiungere ex-novo un messaggio ricevuto

ESPERIMENTI

I passi da fare tramite **AFLogicalOSE**:

- assicurarsi di avere i permessi di root
- scaricarsi il database msgstore.db tramite il comando:

  adb pull /data/data/com.whatsapp/databases/msgstore.db/home

- ricaricare il database modificato nel cellulare tramite il comando:

  adb push /home/santoku/Desktop/msgstore.db /data/data/com.whatsapp/databases/msgstore.db

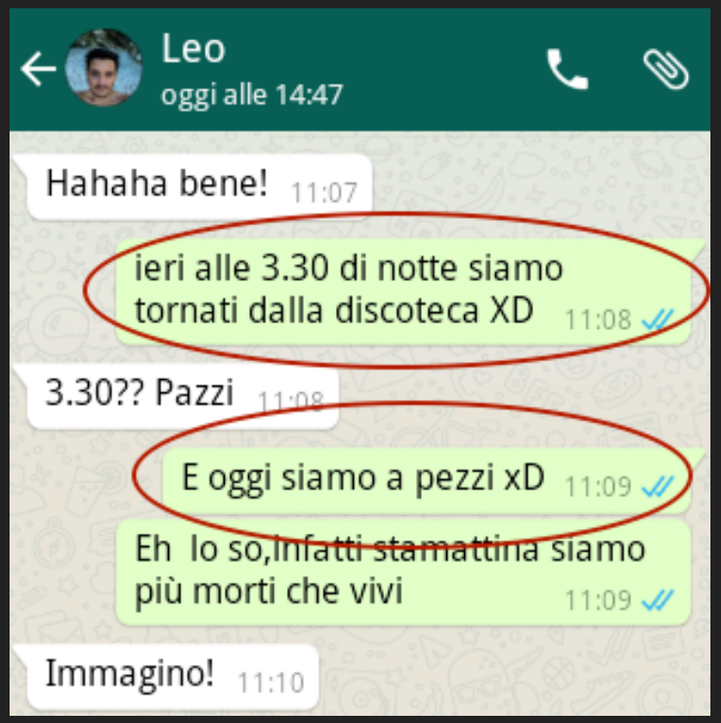
1-Cambiare il testo di un messaggio ricevuto in precendenza

Ciao
Ciao leo!allora,ti aggiorno sul progetto:ABBIAMO FINITO!
□□□□□
Hahaha bene!
ieri alle 3.30 di notte abbiamo finito le parti in latex
3.30?? Pazzi
E oggi basta solo unire i pezzi xD
Eh lo so,infatti stamattina siamo più morti che vivi
Immagino!
ahahahahahahah

Messaggi reali

Ciao
Ciao leo!allora,ti aggiorno sul progetto:ABBIAMO FINITO!
□□□□□
Hahaha bene!
ieri alle 3,30 di notte siamo tornati dalla discoteca! ;)
3.30?? Pazzi
E oggi siamo a pezzi XD
Eh lo so,infatti stamattina siamo più morti che vivi
Immagino!
ahahahahahahah

Messaggi modificati



Il risultato nel cellulare sarà questo

2-Aggiungere ex-novo un messaggio ricevuto

	key_remote_jid	key_from_me	key_id	status	needs_push	data
	Filter	Filter	Filter	Filter	Filter	Filter
19	3934940513…	1	1436430303-14	13	0	Sennò mi esaurisco
20	3934940513…	1	1436430303-15	13	0	Ahahahahah…
21	3934940513…	1	1436430303-2	13	0	
22	3934940513…	1	1436430303-3	13	0	ieri alle 3.30 di notte siamo t…
23	3934940513…	1	1436430303-4	13	0	E oggi siamo a pezzi xD
24	3934940513…	1	1436430303-5	13	0	Eh lo so,infatti stamattina si…
25	3934940513…	1	1436430303-6	13	0	ahahahahah…
26	3934940513…	1	1436430303-7	13	0	Tu stai a lav…
27	3934940513…	1	1436430303-8	13	0	sisi
28	3934940513…	1	1436430303-9	13	0	Assolutamente
29	3932960412…	1	1456326780.--20	13	0	ciao! come stai?
30	3932960412…	1	1456326780.--21	13	0	Ora non ti posso rispon…
31	3934684097…	0	154409093454086530-1	13	0	Tutto bene! Tu?

Il problema riscontrato è il come determinare un key_id valido affinchè Whatsapp lo riconosca; secondo gli altri key_id presenti la struttura è:

- stringa di 18 caratteri
- "-"seguito dal n° progressivo dei messagi scambiati da quell'utente in quella chat

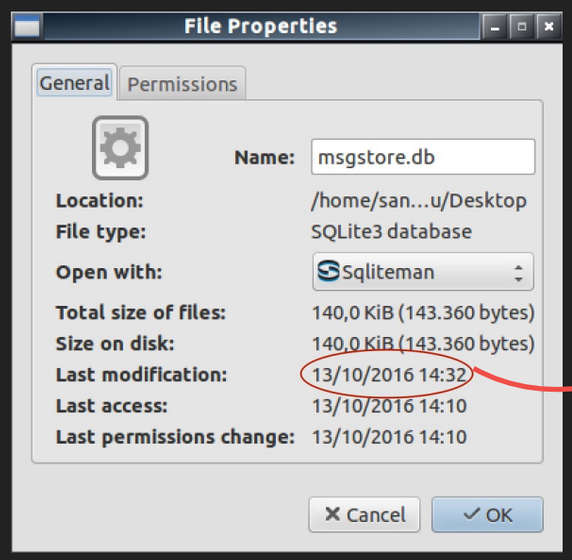
Quindi si è generato un id a caso: "154409093454086530-1"

COME DISTINGUERE SE UN MESSAGGIO È STATO DAVVERO INVIATO/RICEVUTO?

Si è pensato di lanciare da terminale del telefono il comando *"stat msgstore.db"*

```
# stat msgstore.db
  File: msgstore.db
  Size: 143360          Blocks: 280        IO Block:
4096   regular file
Device: b312h/45842d    Inode: 46049       Links: 1
Access: (0666/-rw-rw-rw-)  Uid: ( 2000/   shell)   Gi
d: ( 2000/   shell)
Access: 2016-10-13 14:32:54.000000000
Modify: 2016-10-13 14:36:53.000000000
Change: 2016-10-13 14:36:53.000000000
```

Access è l'ora in cui viene creato il database di Whatsapp per la prima volta. In questo caso corrisponde alla data dell'ultimo salvataggio, dopo la creazione del messaggio malevolo, di msgstore.db.



Infatti, secondo le proprietà del file msgstore.db modificato la data "Last modification" coincide con Access:

Mentre la data vera dell'istallazione di whatsapp nel dispositivo si trova con *"stat com.whatsapp"*

```
com.noshufou.android.su
com.joeykrim.rootcheck
eu.thedarken.rootvalidator
com.koushikdutta.superuser
com.lockwhatsapp.chatlock
jackpal.androidterm
ru.meefik.busybox
# stat com.whatsapp
  File: com.whatsapp
  Size: 4096            Blocks: 8          IO Block:
4096   directory
Device: b312h/45842d    Inode: 45712       Links: 8
Access: (0751/drwxr-x--x)  Uid: (10089/  app_89)   Gi
d: (10089/  app_89)
Access: 2015-06-19 10:15:56.000000000
Modify: 2016-09-04 18:23:53.000000000
Change: 2016-09-04 18:23:53.000000000
```

CONCLUSIONI

“L’interdisciplinarietà
ha sempre portato ad un'evoluzione,
perchè si è costretti ad uscire dagli
schemi convenzionali
e rimettere tutto in discussione…
Da questo punto di vista
la Digital Forensics
può essere la spinta giusta
per far sì che le cose cambino!”

Grazie per l’attenzione

CONTATTI

TWITTER: @AnnaBiselli

LINKEDIN: http://bit.ly/2gdmQkF

EMAIL: anna.biselli@hotmail.it