



UNIVERSITÀ DEGLI STUDI DI MILANO
DIPARTIMENTO DI INFORMATICA

Mobile Device and Mobile Cloud Computing Forensics

Metodologie e tecniche investigative

Relatore:

Vincenzo G. CALABRÒ

Dipartimento di Informatica

Anno Accademico 2015-16

Mobile Forensics: Motivazione

Al giorno d'oggi il Mobile Device è la principale fonte di informazioni delle indagini giudiziarie perché:

- È ampiamente diffuso e utilizzato
- Rileva i contatti e lo scambio di informazioni
- Contiene dati personali e riservati
- Memorizza gli spostamenti
- Registra le abitudini quotidiane

...

**È un diario multimediale
in grado di raccontare
la nostra vita**



Mobile Forensics: Obiettivo

Mobile Forensics: branca della Digital Forensics che si occupa di identificare, raccogliere, preservare, acquisire, analizzare, valutare e presentare le evidenze digitali dei mobile device



Fonte: ISO/IEC 27037:2012

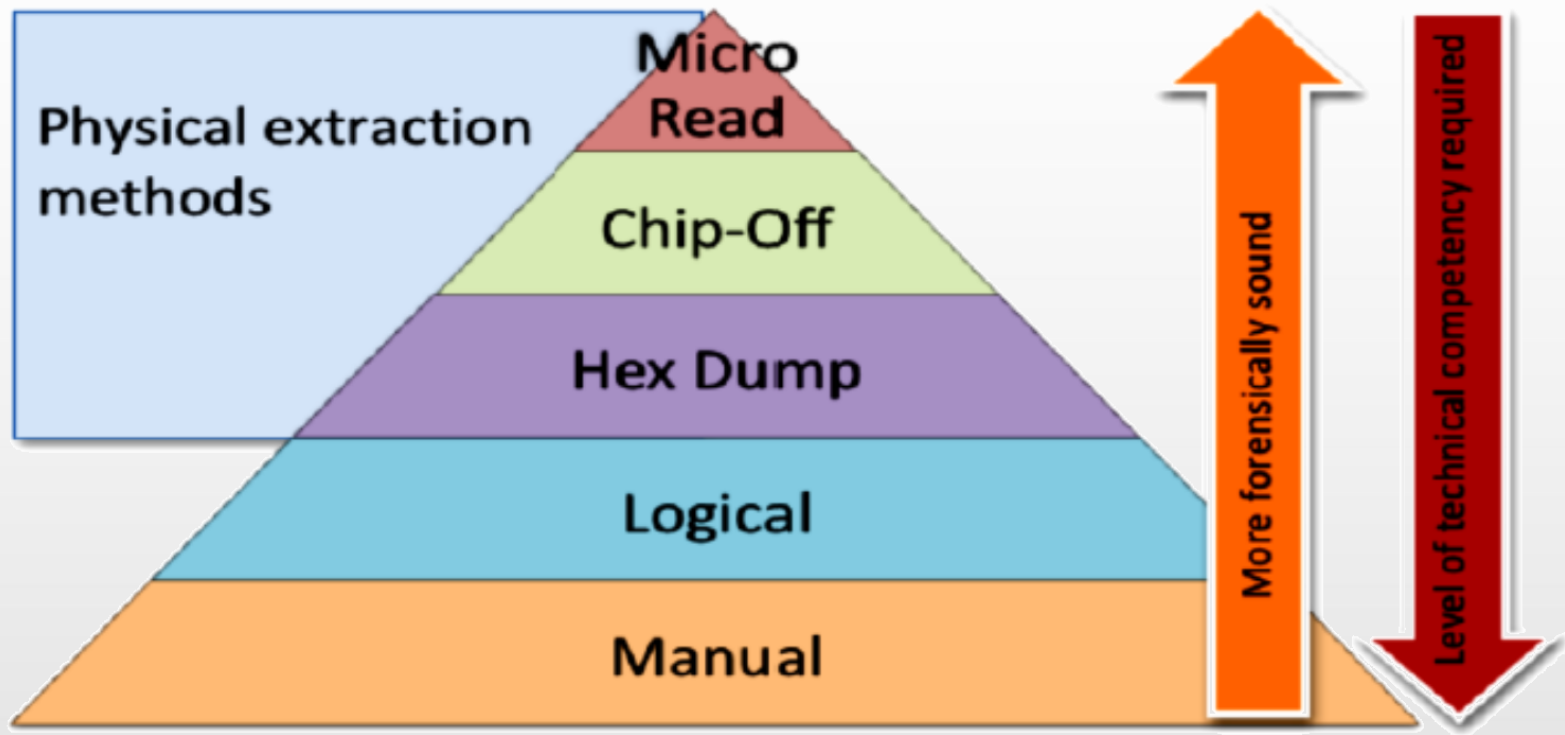


CRITICITÀ	1. Valutazione della scena del crimine 2. Isolamento del device 3. Imballaggio, trasporto e conservazione del device	1. Identificazione device 2. Selezione dei tools 3. <u>Scelta del metodo di acquisizione</u> 4. Supporti esterni	1. Selezione/valutazione delle evidenze 2. Scelta tool di analisi 3. Recupero dati cancellati 4. Generazione Timeline	1. Documentazione 2. Presentazione delle evidenze 3. Verifica del metodo 4. Validazione dei risultati



Mobile Forensics: Stato dell'arte

Classificazione dei metodi di ACQUISIZIONE



Fonte: NIST - Guidelines on Mobile Device Forensics



Mobile Forensics: Problema $\Rightarrow$ Soluzioni

Problema:

Le features di sicurezza implementate dai costruttori di mobile device - quali PIN, password, lock-pattern, crittografia - limitano fortemente il campo di ricerca dell'operatore forense

Soluzioni implementate:

1. Adoperare le tecniche di hacking, cracking e social engineering per bypassare i blocchi (**Acquisizione bit-a-bit**)
2. Acquisire solo le evidenze disponibili (**Acquisizione logica**)
3. Estendere le ricerche negli ambiti con cui il mobile device ha potuto interagire come l'ambiente di **Mobile Cloud Computing**



Caso di studio: Acquisizione bit-a-bit Android device

- Realizzazione dell'acquisizione bit-a-bit

- Acquisizione dei dati
- Realizzazione copia

Directory Listing - Editor

Directory Listing
/img_fulldump.bin/vol_vol11

Name	Modified Time
\$OrphanFiles	0000-00-00 00:00:00
\$Unalloc	0000-00-00 00:00:00
[current folder]	2016-04-22 15:57:08 CEST
[parent folder]	2016-04-22 15:57:08 CEST
app	2016-09-21 21:39:26 CEST
bin	2016-09-21 21:39:08 CEST
data	2014-11-26 05:40:13 CET
etc	2016-09-18 21:17:15 CEST
fonts	2014-11-26 05:57:20 CET
framework	2014-11-26 05:11:04 CET
lib	2016-09-21 21:39:08 CEST
lost+found	0000-00-00 00:00:00
media	2014-11-26 05:40:27 CET
mobile_toolkit	2014-11-26 05:40:29 CET
priv-app	2014-11-26 06:34:47 CET
res	2014-11-26 05:40:18 CET
sbin	2016-09-21 21:39:08 CEST
tts	2014-11-26 05:40:18 CET
usr	2014-11-26 05:40:29 CET
vendor	2014-11-26 05:11:04 CET
xbin	2016-09-21 21:39:08 CEST
build.prop	2014-11-26 07:00:05 CET

Storage 3 GB

GHz

Directory Listing - Editor

Directory Listing
img_fulldump.bin/vol_vol12

Name	Modified Time
\$OrphanFiles	0000-00-00 00:00:00
\$Unalloc	0000-00-00 00:00:00
[current folder]	2016-09-21 21:41:51 CEST
[parent folder]	2016-09-21 21:41:51 CEST
backup	2010-01-01 01:08:07 CET
lost+found	0000-00-00 00:00:00
recovery	2016-04-26 22:10:07 CEST
06012016-sms-blacklist-metac	2016-09-18 07:50:55 CEST
08202014-metadata.txt	2016-09-18 07:50:56 CEST
com.google.android.inputmet	2016-09-21 21:41:51 CEST
swapfile	2016-04-22 18:43:09 CEST
\$CarvedFiles	0000-00-00 00:00:00

vol1 (Unallocated: 0-18431)	1
vol4 (Linux (0x83): 18432-38911)	4
vol5 (Linux (0x83): 38912-59391)	5
vol6 (Unallocated: 59392-125951)	6
vol7 (Linux (0x83): 125952-138239)	7
vol8 (Unallocated: 138240-166911)	8
vol11 (Linux (0x83): 166912-2010111)	11
vol12 (Linux (0x83): 2010112-2268159)	12
vol13 (Linux (0x83): 2268160-7388159)	13
vol14 (Linux (0x83): 7388160-4294968318)	14

supporto esterno

image/sdcard/fulldump.bin

Directory Listing - Editor

Directory Listing
/img_fulldump.bin/vol_vol13

Name	Modified Time
\$OrphanFiles	0000-00-00 00:00:00
\$Unalloc	0000-00-00 00:00:00
[current folder]	2016-09-21 22:08:31 CEST
[parent folder]	2016-09-21 22:08:31 CEST
@btmkt	2015-11-29 18:29:29 CET
acdapi	2015-12-04 10:41:29 CET
aee_exp	2016-07-23 13:33:15 CEST
agps_supl	2016-09-21 21:57:11 CEST
amit	2010-01-01 01:06:34 CET
am	2016-09-21 22:02:10 CEST
app	2016-09-21 22:02:40 CEST
app-asec	2016-04-21 16:32:12 CEST
app-lib	2016-09-21 22:02:40 CEST
app-private	2010-01-01 01:06:34 CET
backup	2016-09-21 21:57:33 CEST
dalvik-cache	2016-09-21 22:02:40 CEST
data	2016-09-21 22:02:40 CEST
dontpanic	2010-01-01 01:06:34 CET
drm	2016-05-25 23:15:27 CEST
local	2016-04-22 17:47:18 CEST
lost+found	0000-00-00 00:00:00
mdl	2010-01-01 01:06:35 CET
media	2010-01-01 01:06:34 CET
mediadr	2015-11-28 09:27:10 CET
misc	2016-06-08 22:45:26 CEST
nfc_socket	2010-01-01 01:06:34 CET
nvrnm	2016-04-26 20:45:12 CEST
property	2016-09-21 21:57:36 CEST
resource-cache	2010-01-01 01:06:34 CET
sdxext2	2016-04-22 17:24:07 CEST
sec	2016-09-21 21:57:11 CEST
security	2010-01-01 01:06:34 CET
SF_dump	2016-04-22 16:00:03 CEST

Directory Listing - Editor

Directory Listing
/img_fulldump.bin/vol_vol14

Name	Modified Time
\$OrphanFiles	0000-00-00 00:00:00
\$Unalloc	0000-00-00 00:00:00
.android_secure	2016-04-26 21:45:56 CEST
.booster	2016-04-29 11:33:34 CEST
.d360data	2016-06-01 21:09:28 CEST
.estrong	2016-09-21 21:45:40 CEST
.FileExpert	2016-09-21 22:07:56 CEST
.YCLOU~1	2016-05-20 07:47:46 CEST
Android	2016-05-11 17:35:50 CEST
backups	2016-09-21 21:44:50 CEST
CamScanner	2016-09-13 22:50:26 CEST
DCIM	2016-09-19 22:35:06 CEST
dianxin	2016-09-21 21:44:44 CEST
Download	2016-09-21 21:44:44 CEST
image_cache	2016-09-21 21:51:22 CEST
LOST.DIR	2016-09-21 21:42:58 CEST
My Cloud	2016-09-20 22:12:36 CEST
MyFavorite	2016-05-19 22:09:40 CEST
NDrive	2016-08-26 17:25:06 CEST
Network Cell Info Lite	2016-06-01 21:02:12 CEST
Ringtones	2016-05-19 22:09:40 CEST
romtoolbox	2016-09-21 21:47:14 CEST
WhatsApp	2016-09-21 21:37:28 CEST
.adups	2016-04-26 23:19:00 CEST
.userReturn	2016-09-21 21:44:42 CEST
sys_lkr_fi	2016-04-29 11:34:16 CEST
\$FAT1	0000-00-00 00:00:00
\$FAT2	0000-00-00 00:00:00
\$MBR	0000-00-00 00:00:00



Caso di studio: Acquisizione Logica di iOS device

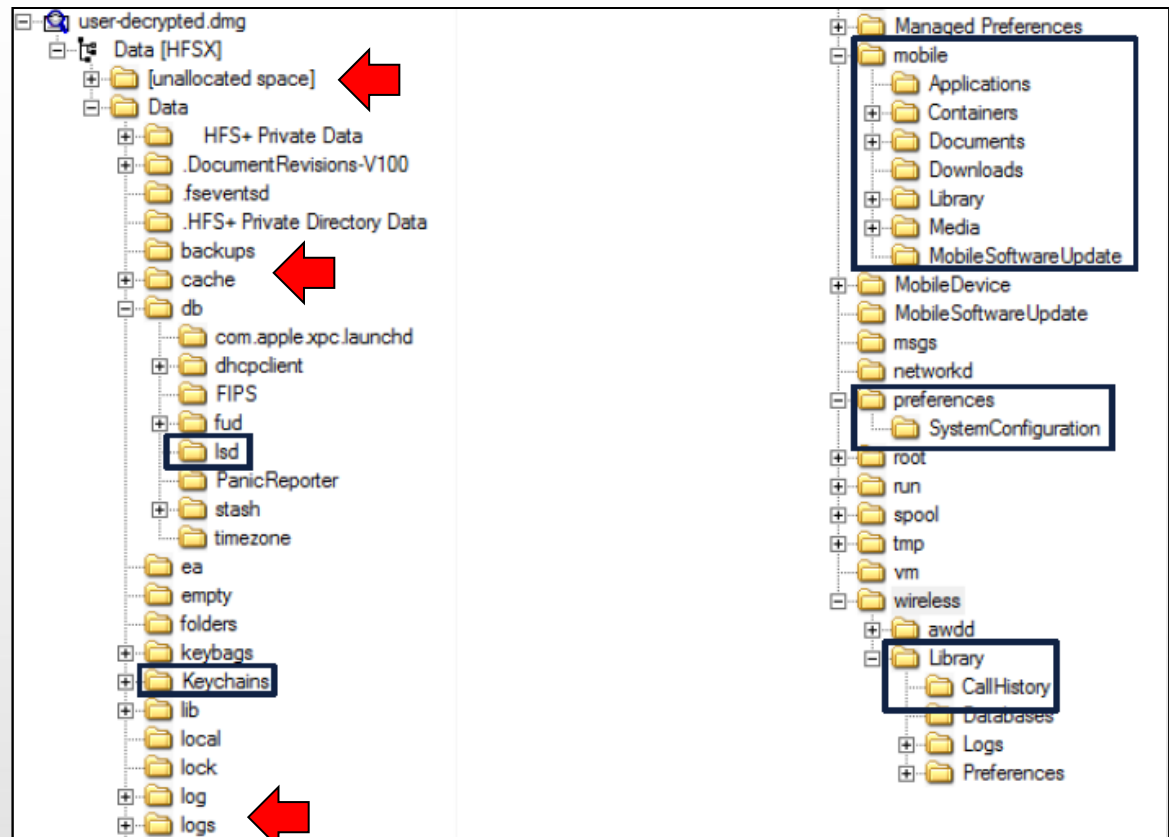
- Acquisizione logica di device con codice di blocco
 - Recupero del *lockdown certificate* e Cracking della password di backup
 - Acquisizione tramite Apple File Conduit (iTunes backup)

Device Target



Apple iPhone 4S (A1387)

Sistema Op. iOS 7.1.1
Processore Apple A5 1 GHz
RAM 512 MB
Storage 16 GB



Analisi dei risultati ottenuti

	Acquisizione bit-a-bit	Acquisizione logica
PRO	File system completo File cancellati Carving Unalloc Space Timeline dettagliata	Realizzazione veloce Basso rischio perdita dati Non richiede privilegi Non richiede tools forensi
CONTRO	Acquisizione privilegi Alto rischio perdita dati Blocchi di sicurezza Vincoli legali	File system parziale Nessun file cancellato Timeline incompleta No forensically sound



Mobile Cloud Computing

- I device possono essere configurati per effettuare un backup dei dati utente sulle piattaforme di cloud:
 - Android -> Google Drive
 - iOS -> iCloud
- Alcune applicazioni per dispositivi mobile (come WhatsApp, Facebook, Gmail, Skype) sfruttano l'ambiente cloud per realizzare i backup dei dati
- Perciò è possibile integrare l'insieme delle evidenze acquisite direttamente sui device e dai provider con quelle reperibili dalle piattaforme di cloud storage



Mobile Cloud Computing Forensics

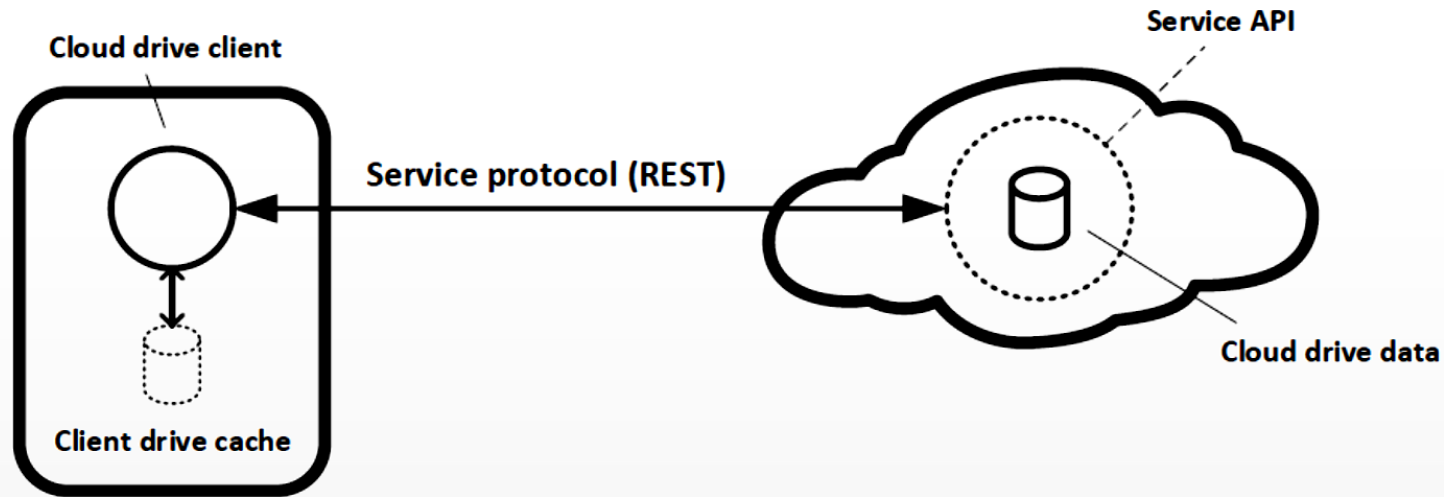


Diagramma di funzionamento dei cloud storage service, Fonte: The NIST Definition of Cloud Computing

Le attuali metodologie di acquisizione delle evidenze da cloud storage si basano su adattamenti delle tecniche tradizionali

- Acquisizione manuale
- Ricerca e estrazione degli artefatti client-side (*reverse-engineering*)
- Richiesta diretta al cloud storage provider (*rogatorie internazionali*)

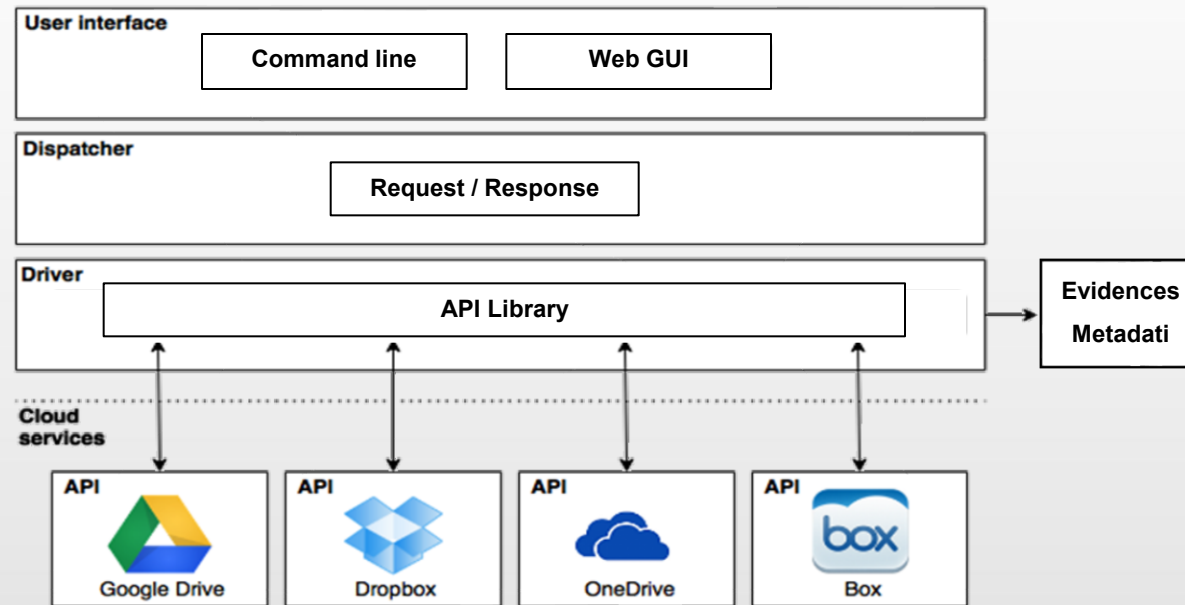
Soluzione innovativa

Fasi per acquisizione



Diagramma architetturale

La soluzione proposta, basata sulla ricerca di Roussevy, Barreto e Ahmed, sfrutta le API ufficiali dei fornitori dei servizi di cloud.



Fonte: Roussevy, Barreto, Ahmed



Caso di studio: WhatsApp da Google Drive

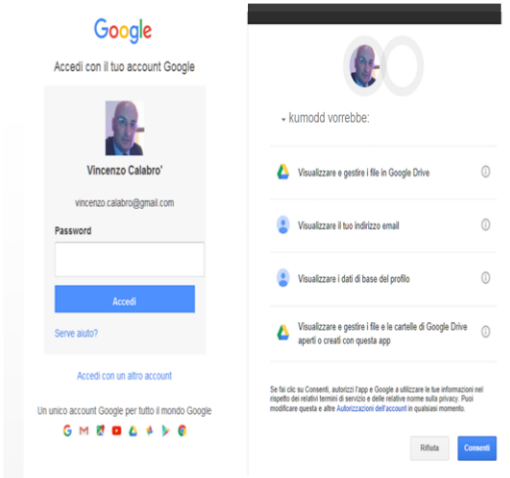
1. Autenticazione e autorizzazione *read-only* al cloud storage (OAuth 2.0)

Request GET `https://accounts.google.com/o/oauth2/v2/auth?scope=https://www.googleapis.com/auth/drive.readonly`

Response `https://oauth2.example.com/auth?code=4/P7q7W91a-oMsCeLvIaQm6bTrgtp7`

Request POST `/oauth2/v4/token`
Host: `www.googleapis.com`
code=`4/P7q7W91a-oMsCeLvIaQm6bTrgtp7`

Response { "access_token": "`1/fFBGRNJru1FQd44AzqT3Zg`",
"expires_in": 3920, "token_type": "Bearer" }



2. Discovery del contenuto del cloud storage

Request GET `https://www.googleapis.com/drive/v2/files?access_token=1/fFBGRNJru1FQd44AzqT3Zg`

Response { "kind": "drive#fileList", *<-- lista dei file dello storage -->*
"etag": "\"btSRMRFBFi3NMGgScYWZpc9YNCI/GRsLwCm7Uq8wQamJ1AhN5kQI\"",
"items": [
 { "kind": "drive#file",
 "id": "`0B3x8LGqSN2oXSjFUWEgxelZic28`",
 "title": "`msgstore.db.crypt12`",
 "mimeType": "application/octet-stream"
 },
],



Caso di studio: WhatsApp da Google Drive

3. Selezione del file d'interesse

Request GET https://www.googleapis.com/drive/v2/files/0B3x8LGqSN2oXSjFUWEgxelZic28?access_token=1/fFBGRNJru1FQd44AzqT3Zg

Response { "kind": "drive#file", <-- Download del metadata file-->
"id": "0B3x8LGqSN2oXSjFUWEgxelZic28",
"etag": "\"\ULTBkNKmycdCqkp_rFmHqVG1eVs/MTQyMzEyMjk4MjIzOQ\"",
"downloadUrl": "https://www.googleapis.com/drive/v2/files/0B3x8LGqS",
"createDate": ..., "modifiedDate": ..., "lastViewedByMeDate": ...,
"mimeType": "application/octet-stream",
"originalFilename": "msgstore.db.crypt12",
"md5Checksum": "cd3c797793b5e5ee72d7da5c896ad6e8",
"fileSize": "8434", "owners": ..., "lastModifyingUserName": ...

4. Acquisizione e Decodifica del file

msgstore.db - Oxygen Forensic® SQLite Viewer

File Guida

Apri Recover deleted records Viewer Search Esporta Stampa Column aliases Options Guida

Tables

- chat_list (1/0)
- frequents (1/0)
- group_participants (0/0)
- group_participants_hist... (0/0)
- media_refs (0/0)
- messages (4/0)
- messages_fts_content (2/0)
- messages_fts_segdir (2/0)
- messages_fts_segments (0/0)
- messages_links (0/0)

Table Data

#	_id	key_remote_jid	key_from_me	key_id	status	needs_push	data	timestamp
1	1	-1	0	-1	-1	0		0
2	2	3934207979@s.whatsapp.net	1	393B1C84619D24A7CC07B64F8F3AC3	6	0		147448658905
3	3	3934207979@s.whatsapp.net	1	F67941DD7AC28C927083AAD118EA7F	13	0	Ciao	147448658905
4	4	3934207979@s.whatsapp.net	0	DF7D3AAD675B8E5D5DEF595E056E55	13	0	Benvenuto	147448660900

Blocks containing deleted data

Table structure

SQL Editor



Conclusioni

Sono stati illustrati i risultati dei diversi metodi di acquisizione.

In particolare, il metodo *API-based* presenta alcune peculiarità che lo rendono innovativo rispetto agli altri:

- Consente di recuperare o integrare le evidenze
- Si basa sull'uso delle API ben documentate
- È facile dimostrare la completezza e la riproducibilità del processo
- È un procedimento flessibile di acquisizione *by-proxy*
- Comprende metadati *forensically sound*

Che cosa si potrà fare come prossimo passo:

- Migliorare e validare i protocolli di acquisizione dal cloud che includano anche le altre tipologie di servizio (PaaS, IaaS)
- Definire dei Livelli di Servizio (SLO/SLA) per i servizi cloud a sostegno dell'analisi forense (Secure-Logging-as-a-Service e Metodi di Acquisizione)
- Trovare un compromesso tra il diritto alla privacy e le esigenze di giustizia



Grazie per l'attenzione

