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

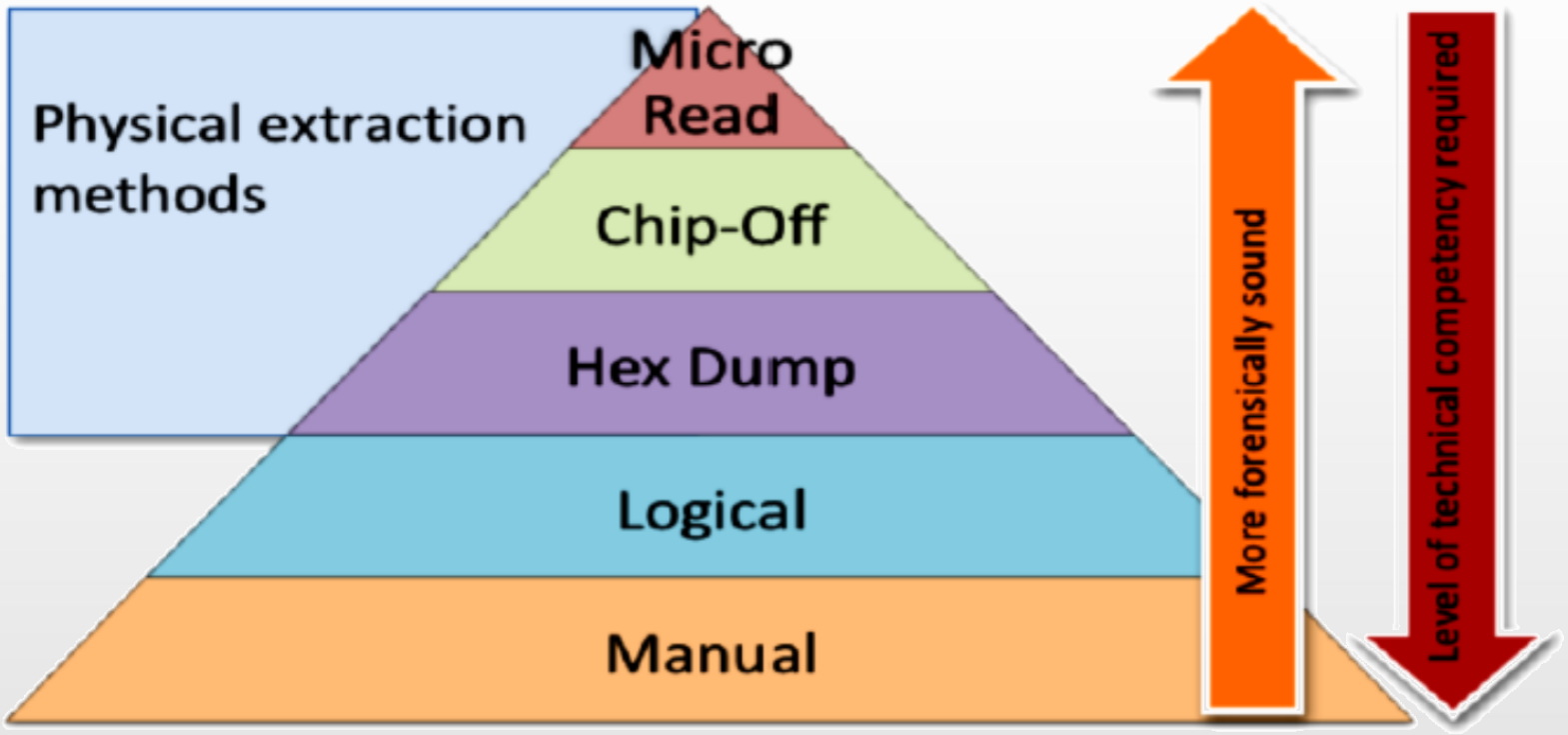
Mobile Forensics: branca della Digital Forensics che si occupa di identificare, raccogliere, preservare, acquisire, analizzare, valutare e presentare le evidenze digitali dei mobile device

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. **Scelta del metodo di acquisizione** 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 ⇒ Soluzioni

Problema:

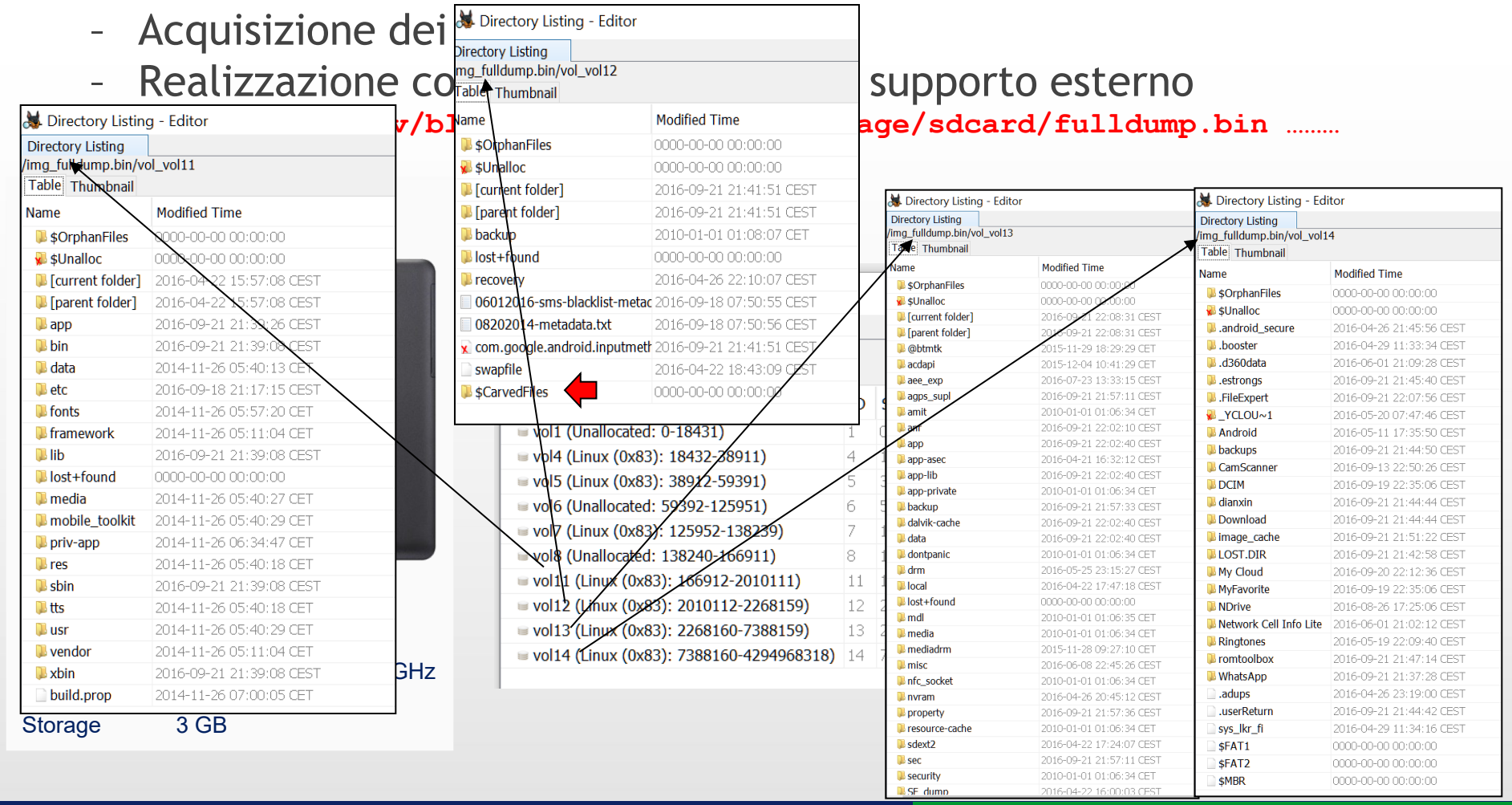
Le features di sicurezza implementate dai costruttori di mobile device - quali PIN, password, lock-pattern, crittografia – limitano fortemente il campo di ricerca dell'operatore forense

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
  - Realizzazione co supporto esterno



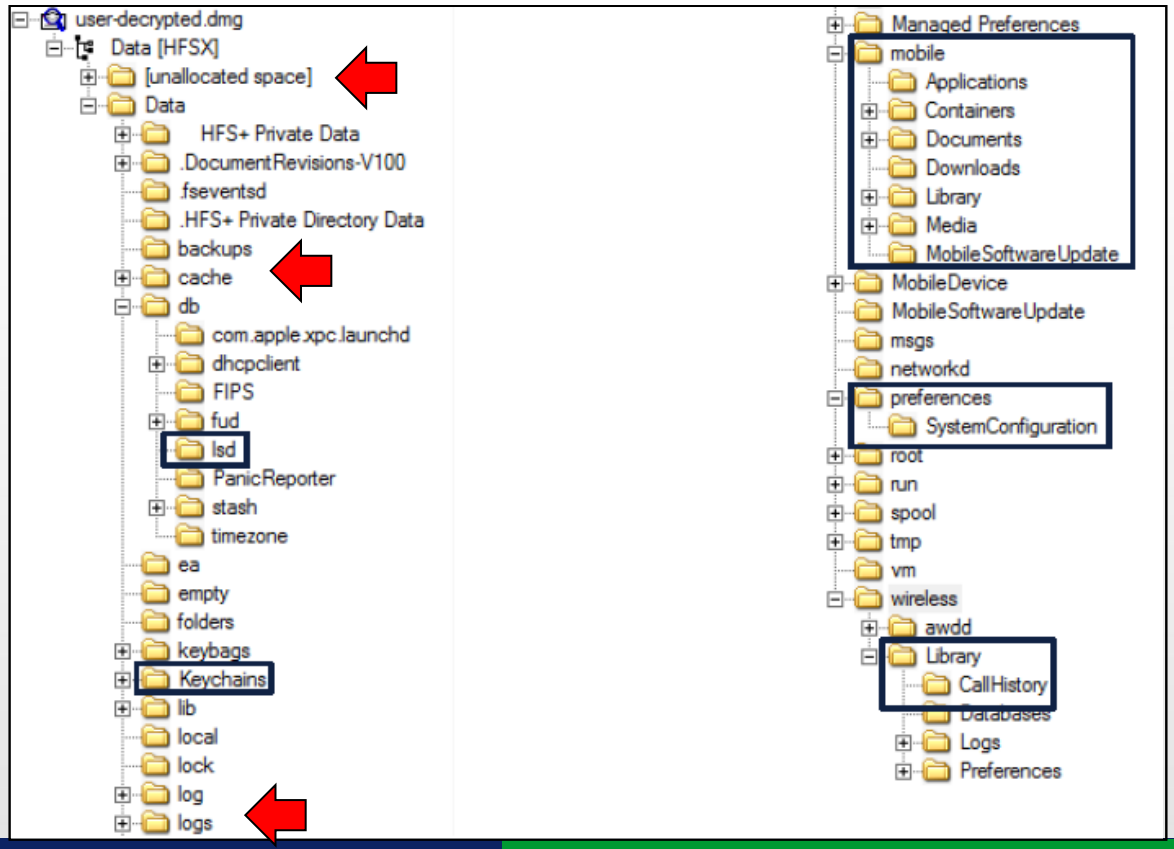
Caso di studio: Acquisizione Logica di iOS device

- 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

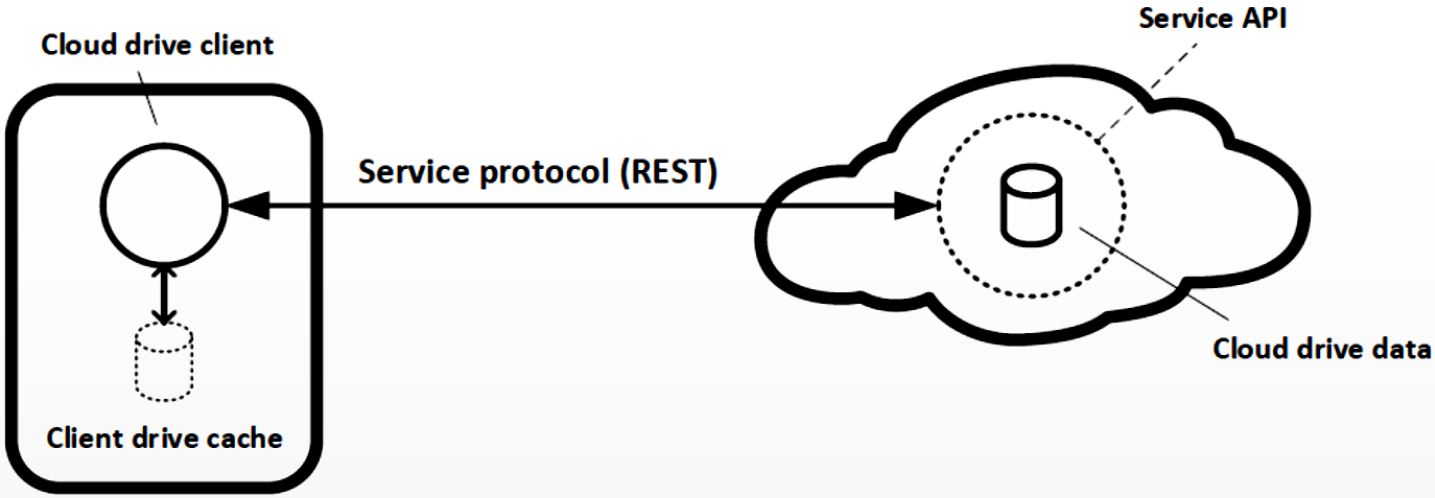


Diagramma di funzionamento dei cloud storage service, Fonte: The NIST Definition of Cloud Computing

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*)

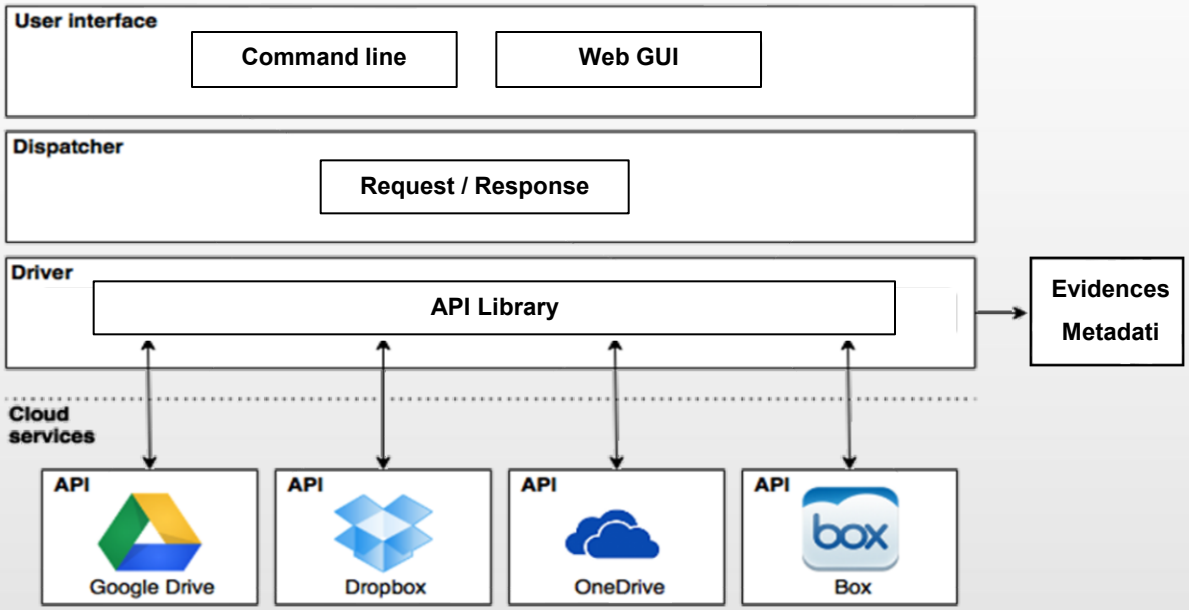
Soluzione innovativa

Fasi per acquisizione

Content Discovery → Target Selection → Target Acquisitation

Diagramma architetturale

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



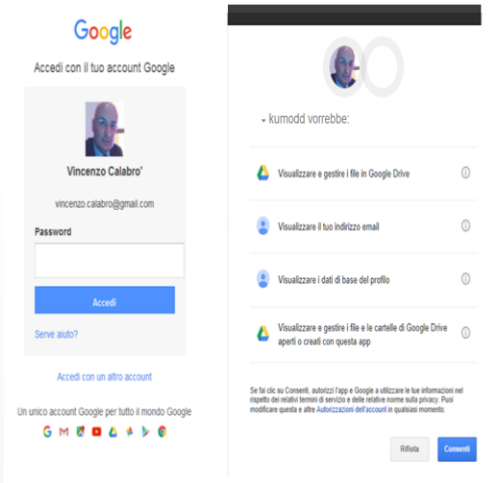
Fonte: Roussevy, Barreto, Ahmed

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"
                },
```

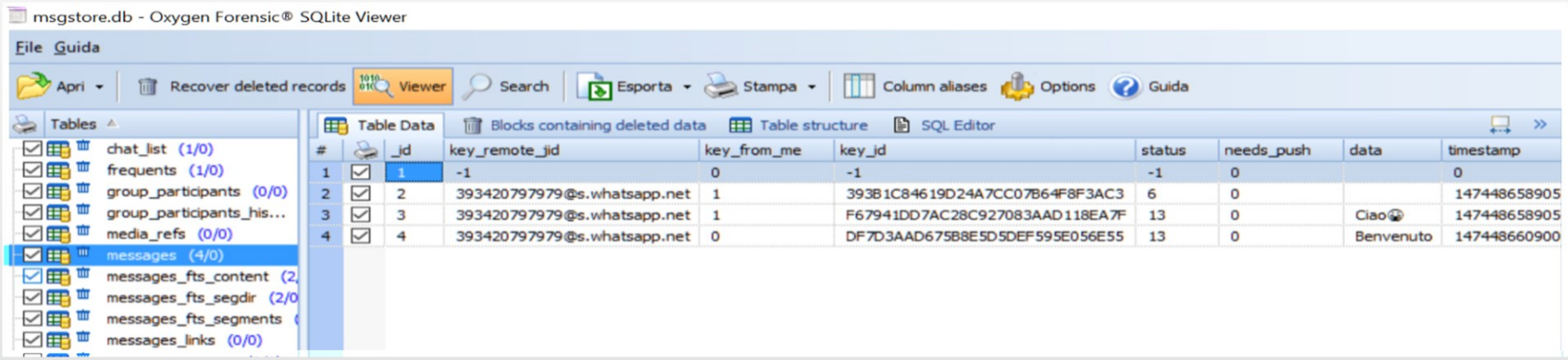
Caso di studio: WhatsApp da Google Drive

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/MTQyMzEyMjk4MjIz0Q\""
"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



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