Ordine Avvocati di Torino, Commissione Scientifica
In Collaborazione con Fondazione Fulvio Croce

LE INVESTIGAZIONI DIGITALI

GLI STRUMENTI DI CUI PUÒ DISPORRE IL DIFENSORE E IL LORO UTILIZZO

Paolo Dal Checco, Consulente Informatico Forense
Forenser Srl

Forenser
Digital Investigations

CHI SONO

- Laurea e Ph.D. in Informatica, Università di Torino
- Consulente Informatico Forense (10+ anni, 2k+ casi)
- CTP, CTU, Esperto, Perito del Giudice, CT del PM, Ausiliario di PG
- Collaborazioni con UniTO (Docente a Contratto corso Sicurezza Informatica @SUISS), UniGE (Master), UniMI e PoliMI (Master e Corsi di Perfezionamento)
- Interessi in mobile forensics, OSINT, cryptocurrency forensics, web forensics…. in sostanza tutti gli aspetti della digital forensics

ARGOMENTI DELLA TERZA PARTE DEL CORSO

- La copia forense degli smartphone: come produrla e visionarla, princìpi e strumenti della mobile forensics;
- Visualizzazione e uso informatico forense dei metadati EXIF di fotografie, video, documenti;
- L'acquisizione preliminare e cautelativa di chat, file audio, foto e video contenuti in smartphone.

SMARTPHONE E COPIE FORENSI

- Copia forense: copia del contenuto di un dispositivo tale da garantire i requisiti indicati nella Legge 48/2008, la ISO 27.037
- Detta anche copia «conforme», immagine forense, copia certificata, acquisizione forense, copia immagine
- A volte definita anche «copia di mezzo» (quando poi si produce la «copia di fine»)

SMARTPHONE E COPIE FORENSI

- Acquisizione e analisi di dispositivi mobili: “Mobile forensics”
- Acquisizione tramite:
  - un **software di acquisizione** installato su un personal computer
  - un **dispositivo hardware** dedicato all’estrazione dei dati
  - Estrazione del chip di memoria flash e acquisizione (**chip-off**)
  - Acquisizione tramite **Flasher box** o **JTAG**
- Problematiche relative alla **ripetibilità**: per diversi modelli è necessario avviare il cellulare tramite il suo sistema operativo
- Recentemente, si verifica sempre più spesso l’esigenza di **acquisizione via Cloud** (i documenti non sono sul dispositivo ma anche altrove, come iCloud o Dropbox)

SMARTPHONE E COPIE FORENSI

- Strumenti maggiormente utilizzati per l'acquisizione forense:
  - Cellebrite UFED
  - MSAB XRY
  - Oxygen Forensics
  - Elcomsoft Phone Breaker/iOS Toolkit

SMARTPHONE: SBLOCCO PASSWORD/PIN

- Possibile ma non per tutti i modelli
- In genere il vincolo per la fattibilità è la **complessità della password/pin code**
- Strumenti più utilizzati:
  - Cellebrite Premium
  - Grayshift Graykey
  - Elcomsoft
- Possono essere necessari da qualche giorno a diversi mesi

SMARTPHONE : MODALITÀ DI ACQUISIZIONE FORENSE

1

- Accesso diretto ai "record" memorizzati dal telefono all'interno delle diverse aree di interesse (es. Rubrica, messaggi, registro chiamate, ecc.)
- Problemi di accesso con passcode
- Metodo veloce

Logical

2

- Copia dei file del file system
- Recupero di maggiori informazioni
- Possibilità di recuperare record cancellati all'interno di file (es. SQLite deleted records, thumbnails)
- Problemi di accesso con passcode
- Richiede più tempo

Filesystem

3

- Copia bit-a-bit del dispositivo
- Possibilità di superare i blocci con codice
- Possibilità di recuperare record e interi file cancellati

Physical

SMARTPHONE E COPIE FORENSI: STRUMENTI

deft

SANTOKU

TSURUGI LINUX

SMARTPHONE E COPIE FORENSI: COME VISIONARLE

- Per visionare le copie forensi è necessario:
  1. avere il software con cui sono state generate;
  2. farsi generare un «portable case» o un «reader».
- Il «portable case» può consistere in un software da eseguire su di un PC, in una esportazione completa in file pdf (spesso composto da migliaia di pagine), un documento excel, etc…

SMARTPHONE E COPIE FORENSI: ALTERNATIVA

- L'alternativa a un software professionale, se non c'è tempo o non ci sono risorse, è:
  - Backup iTunes (ore Finder) per dispositivi Apple (facile da fare, attenzione alla password di backup, necessario poi un viewer per visionare il contenuto);
    - ~/Library/Application Support/MobileSync/Backup/ (Mac OS)
    - %appdata% o %USERPROFILE%, poi "Apple" o "Apple Computer" > MobileSync > Backup (Windows)
  - Backup ADB per dispositivi Android (più complesso visionare)
- Fatto il backup, si comprime il folder, si calcola valore hash, si applica marca temporale

METADATI

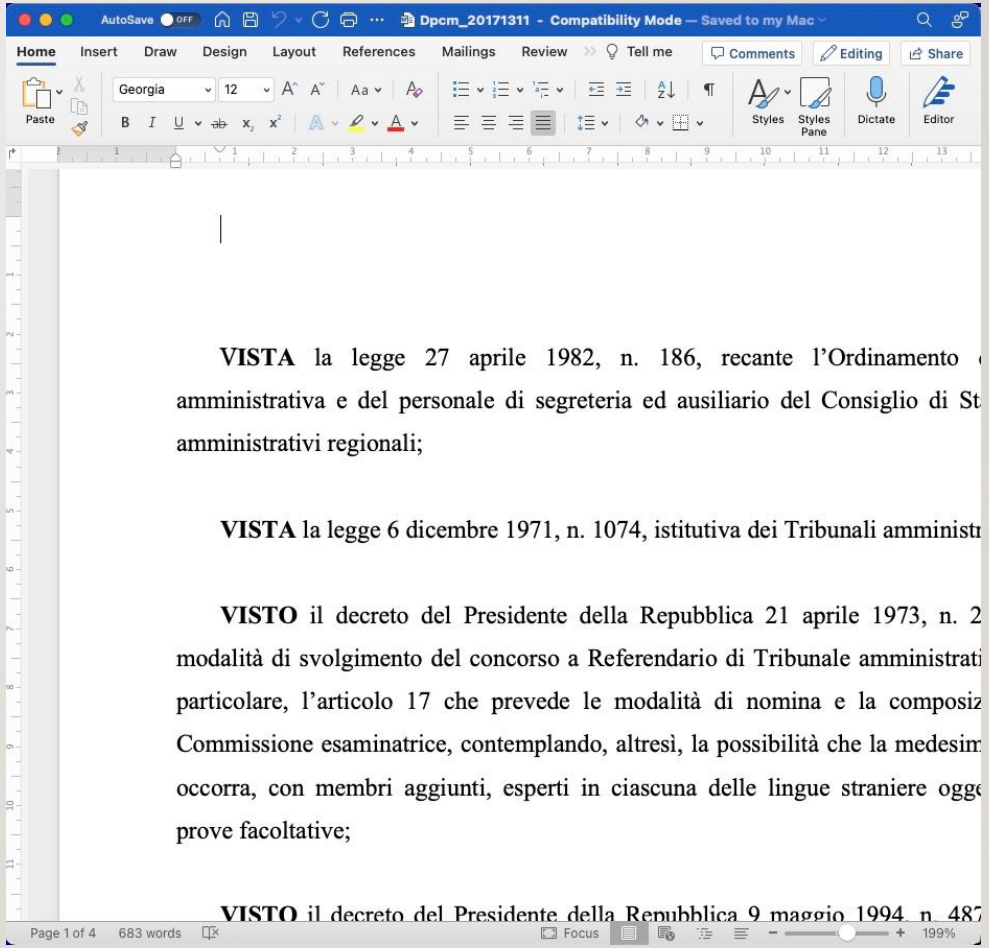
- In informatica forense consideriamo 2 tipi di metadati:
  - Dati contenuti nel file (**EXIF**)
  - Dati presenti all'esterno del file (**date filesystem**)
  - Dati relativi a caricamento su web (**upload** online)
  - Dati relativi trasferimento/**traffico** (es. tabulati)

METADATI

- I metadati interni ai file sono modificabili, con software gratuiti o persino parzialmente all'interno dello stesso programma (Word, etc…)
- I metadati esterni (data del file sul sistema, etc… anche sono modificabili, ma con maggiore difficoltà
- Possono acquisire validità se incrociati e ritenuti coerenti con altri dati (es. Timeline, metadati del filesystem, dati generati dal sistema operativo, etc…)

METADATI

- Esempio con file Word: https://www.governo.it/sites/governo.it/files/Dpcm_20171311.doc
- Metadati acquisibili:
  - Metadati EXIF nel file Word
  - Metadati sul webserver (data di caricamento)



METADATI

- Esempio con immagine: https://www.ordineavvocatitorino.it/sites/default/files/documents/News/News_2022/senza%20titolo%20(24%20di%20113).jpg
- Metadati acquisibili:
  - Metadati EXIF nella foto
  - Metadati sul webserver (data di caricamento)

VISUALIZZAZIONE E MODIFICA DI METADATI EXIF

- Strumenti per visionare e modificare dati exif:
  - ExifTool
  - https://exiftool.org/gui/
  - In parte con la funzione «Proprietà» del Sistema Operativo
- Le modifica di dati exif non lascia traccia, se fatta correttamente (alcuni strumenti permettono di fare un ripristino tramite il comando «exiftool -pdf-update:all= filename.pdf»

ACQUISIZIONE PRELIMINARE DI CHAT

- Principali app di chat/instant messaging: Whatsapp, Telegram, Signal
- Spesso usati anche Instagram, Facebook Messenger, Instagram, Twitter
- Ogni App ha un approccio diverso circa la memorizzazione dei messaggi: locale, cloud, locale+cloud
- L'ideale sarebbe sempre quello di fare copia forense del dispositivo dove chat/gruppo/messaggi sono comparsi o stati generati
- Non sempre è possibile, quindi si valuta di volta in volta l'alternativa migliore
- In caso di timore di scomparsa delle chat, **mettere lo smarthpone in airplane mode**

WHATSAPP

- Più utilizzata tra le App di comunicazione
- i messaggi sono memorizzati solo in locale (ma parte ora anche in cloud);
- I messaggi cancellati rimangono per un po' recuperabili: per quanto dipende da fattori spesso imprevedibili (backup giornalieri, cancellazione chat,
- Con Android e iOS si possono fare backup su cloud (Google Drive e iCloud) di messaggi e file multimediali
- Il database è modificabile, non con facilità, ma se ne deve tenere conto

WHATSAPP: IOS

- Su iOS il backup iTunes contiene anche le chat Whatsapp;
- Facile fare copia «forense» (o quantomeno più forense di una screenshot): è sufficiente fare backup iTunes e produrlo;
- Eventualmente, per non produrre l'intero dispositivo, si può sincronizzare Whatsapp su uno nuovo, passando per iCloud (backup dal dispositivo da acquisire, restore su di uno nuovo, backup iTunes del dispositivo nuovo)

WHATSAPP: ANDROID

- Su Android (che non esporta Whatsapp nel suo backup) il software memorizza gli ultimi backup, cifrati, nel folder /sdcard/WhatsApp/Databases o /storage/emulated/0/Android/media/com.whatsapp/Whatsapp/Databases
- Su Android, i dati multimediali sono in /storage/emulated/0/Android/media/com.whatsapp/Whatsapp/Media
- https://faq.whatsapp.com/618575946635920/?cms_platform=android

WHATSAPP: ACQUISIZIONE CON WHATSAPP WEB

- Valutare sempre la possibilità di fare un'acquisizione di Whatsapp Web
- Non vengono sincronizzati tutti i messaggi, solo gli ultimi giorni
- Valgono gli stessi princìpi e strumenti visti durante il secondo incontro (acquisizione di risorse web);

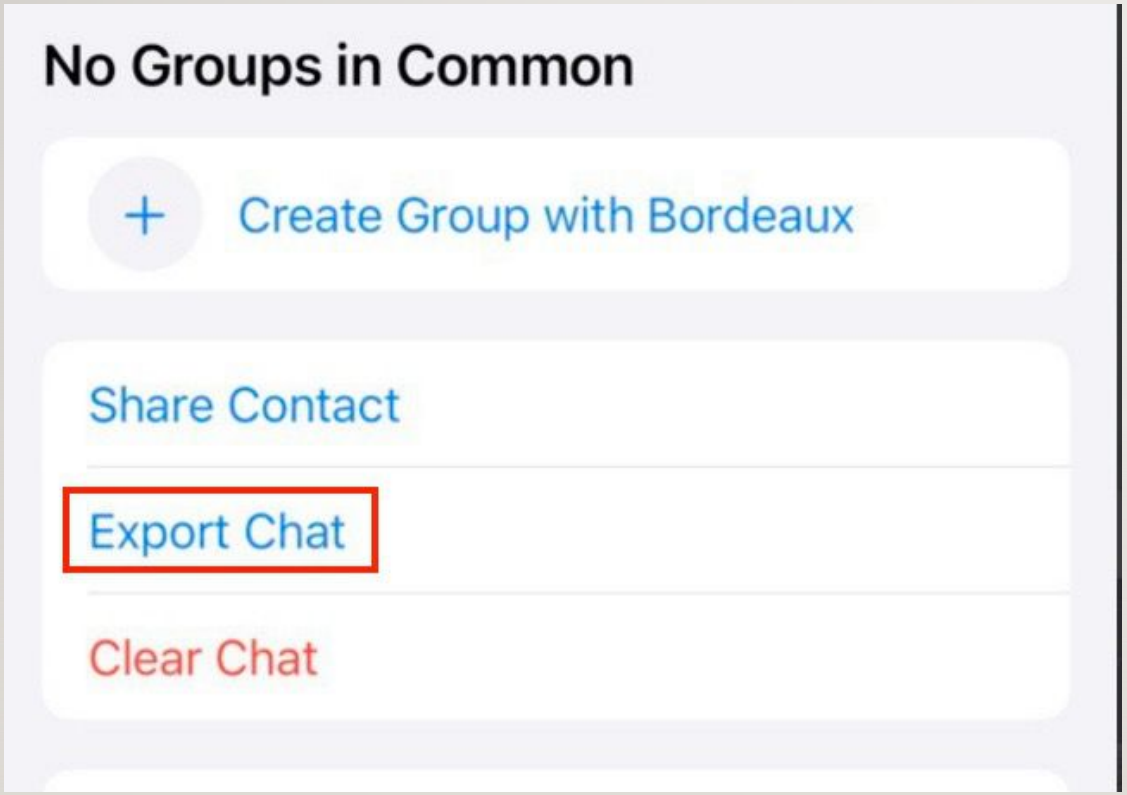
WHATSAPP: ACQUISIZIONE VIA WHATSAPP EXPORT

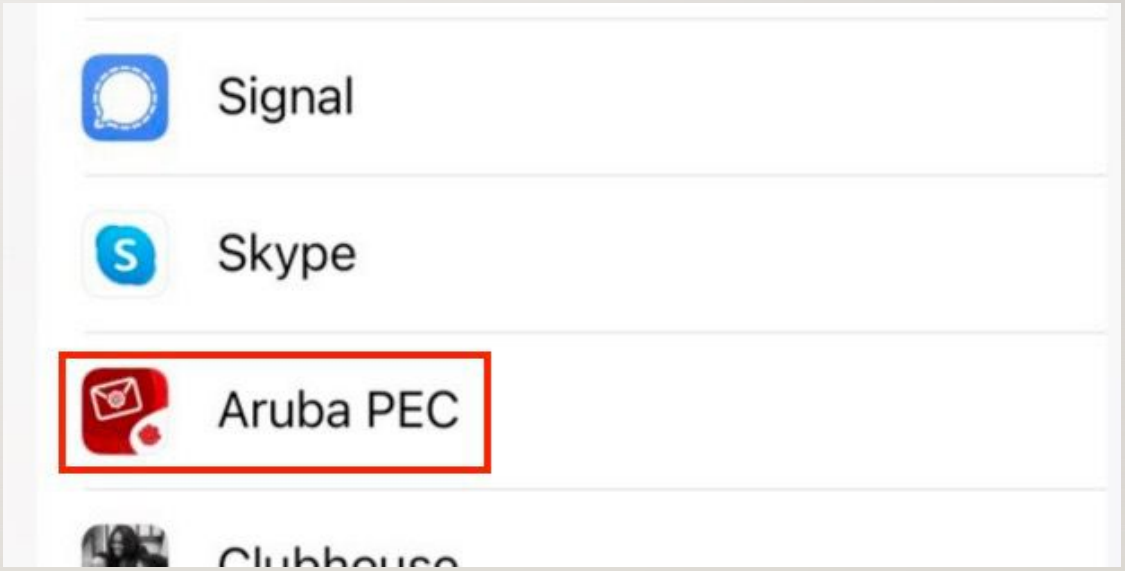
- Whatsapp permette di esportare le singole chat
- Purtroppo l'esportazione prevede la generazione di file di testo TXT (non forense) e di file multimediali separati
- È possibile chiedere di esportare inviando via mail
- Idea: filmare procedura di esportazione, registrando schermo e filmando da dispositivo esterno, riprendendo anche la rubrica dove c'è l'associazione tra nome e contatto
- Configurare PEC sullo smartphone da acquisire e su quello esterno

WHATSAPP: ACQUISIZIONE VIA WHATSAPP EXPORT

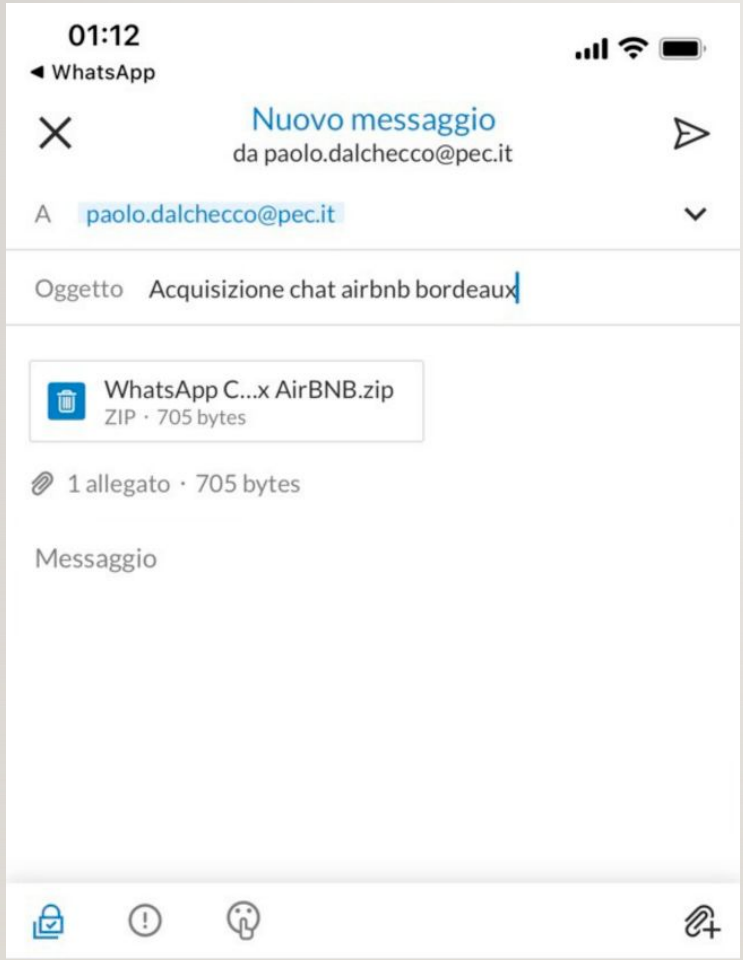
- Esportare la chat d'interesse selezionando la PEC come invio e destinazione
- Filmare fino all'invio della PEC
- Inviare tramite la stessa PEC lo screen recording fatto con il dispositivo che contiene la chat e il video fatto con il dispositivo esterno
- Problematico quando ci sono molti file multimediali (limite 30MB Posta Elettronica)

WHATSAPP: ACQUISIZIONE VIA WHATSAPP EXPORT





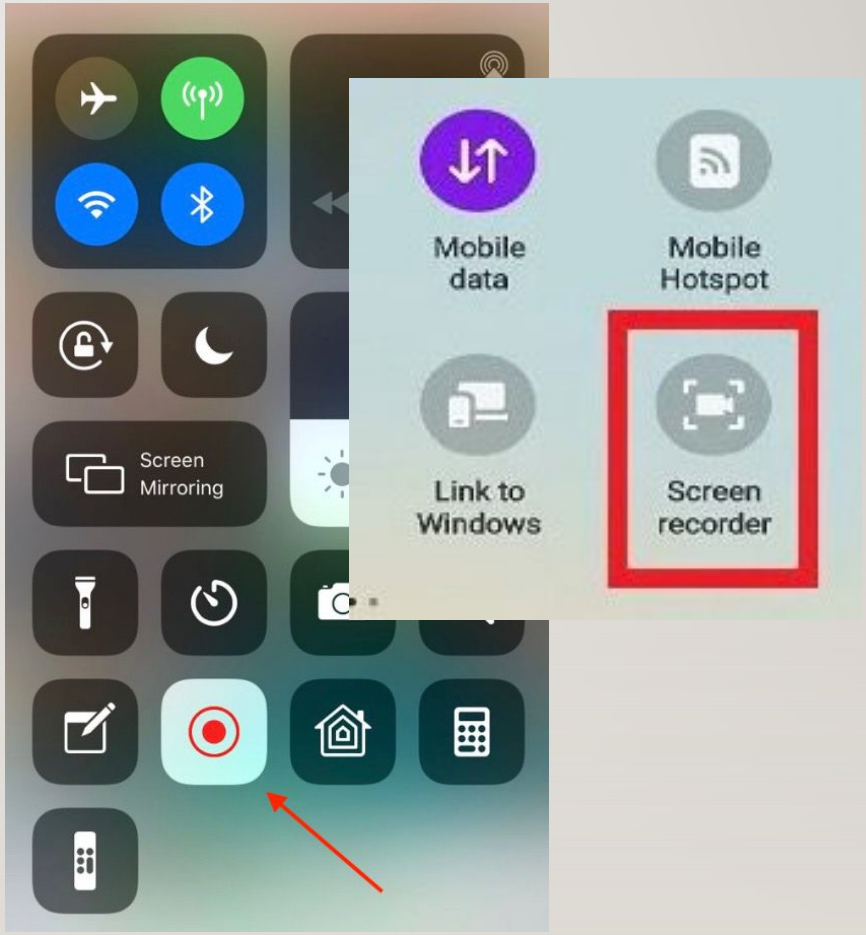
WHATSAPP: ACQUISIZIONE VIA WHATSAPP EXPORT



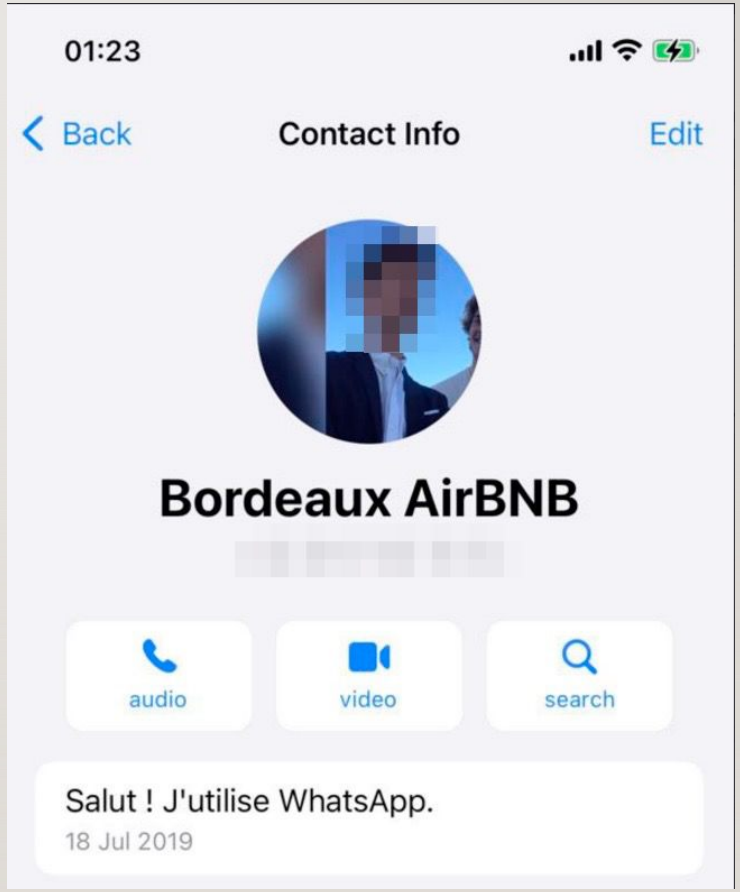
WHATSAPP: ACQUISIZIONE VIA WHATSAPP EXPORT

- Vero che abbiamo file di testo + file multimediali
- Abbiamo però il tutto che transita via PEC con il video che crea timing coerente
- Il video riprende l'associazione tra nome e utenza
- Se possibile riprendere anche altri elementi temporali (sito di quotidiano, Twitter, ora esatta, etc…)

```
[22/XX/22, 16:20:36] Bordeaux AirBNB: Messages and calls are end-to-end
outside of this chat, not even WhatsApp, can read or listen to them.
[22/XX/22, 16:20:36] Bordeaux AirBNB: Vous serez remboursez intégralemen
[22/XX/22, 17:12:17] Paolo: Salut Pier [...]
[22/XX/22, 17:12:39] Bordeaux AirBNB: Pas de soucis 🤗🤗🤗
[22/XX/22, 17:12:46] Bordeaux AirBNB: Je comprends tout à fait
[22/XX/22, 17:12:51] Bordeaux AirBNB: À bientôt alors
```



WHATSAPP: ACQUISIZIONE VIA WHATSAPP EXPORT



WHATSAPP: ACQUISIZIONE VIA WHATSAPP EXPORT

- Esportare la chat d'interesse selezionando la PEC come invio e destinazione
- Filmare fino all'invio della PEC
- Inviare tramite la stessa PEC lo screen recording fatto con il dispositivo che contiene la chat e il video fatto con il dispositivo esterno
- Problematico quando ci sono molti file multimediali (limite

TELEGRAM: APPROCCIO DIVERSO

- Chat non in locale (se non un limitato «mirror») ma in cloud
- Possibili più client
- Telegram Desktop ha una comoda funzione di Export (json/html)
- Telegram Web, ottima alternativa
- Identificare anche Telegram ID (username o nome utente cambiano, Telegram ID no):
  - Utilizzando client come Messenger Plus;
  - Inoltrando messaggio a **@userinfobot**

CONCLUSIONI

- La **copia forense degli smartphone** è opportuno venga fatta con strumenti opportuni ma ci sono alternative in caso di esigenze particolari
- I metadati EXIF interni ai file sono modificabili, diventano più robusti se coerenti con metadati esterni o meglio ancora con dati del sistema operativo in una copia forense
- Le chat possono essere acquisite in modi diversi, uno è quella della funzione di esportazione