Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

# CrypTO CONFERENCE

Politecnico di Torino 1859
Telsy A TIM ENTERPRISE BRAND
DISMA

Politecnico di Torino

# Cybercrime, crittografia e informatica forense

CrypTO Conference, Torino, 22 maggio 2025

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

**Paolo Dal Checco, Consulente Informatico Forense, Forenser Srl**

# CHI SONO

- Laurea e Ph.D. in Informatica, Università di Torino
- Consulente Informatico Forense (10+ anni, 2k+ perizie informatiche)
- CTP, CTU informatico, 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»

# CYBERCRIME

- <*sàibëkraim*> s. ingl., usato in it. al masch. – Reato nel quale la condotta o l'oggetto materiale del crimine sono correlati a un sistema informatico o telematico, ovvero perpetrato utilizzando un tale sistema o colpendolo (rispettivamente, si parla di *computer as a tool* e *computer as a target*). [fonte: Treccani]

# INFORMATICA FORENSE

- **Informatica forense** o **digital forensics** (in passato **computer forensics**)
- Disciplina che mira a **individuare**, **acquisire**, **preservare** e **analizzare** evidenze digitali
- Il fine è quello di ricostruire comportamenti rilevanti in **contesti tipicamente giudiziari e di cybercrime**
- La fase più delicata è ovviamente quella della **acquisizione forense** o **copia forense**, con rischi di:
  - **modifica**/alterazione del dato
  - non poter **acquisire** il dato
  - non poter **accedere/interpretare** al dato

# LA CRITTOGRAFIA E L'INFORMATICA FORENSE

- Da un lato è una **tutela** crescente per gli utenti e la loro libertà
- Dall'altro rappresenta un **ostacolo** per le perizie informatiche forensi
- Vediamo **tre scenari** nei quali ho avuto esperienza diretta di come la crittografia ha lanciato una sfida e come è stata ~~sconfit~~… ehm, aggirata.

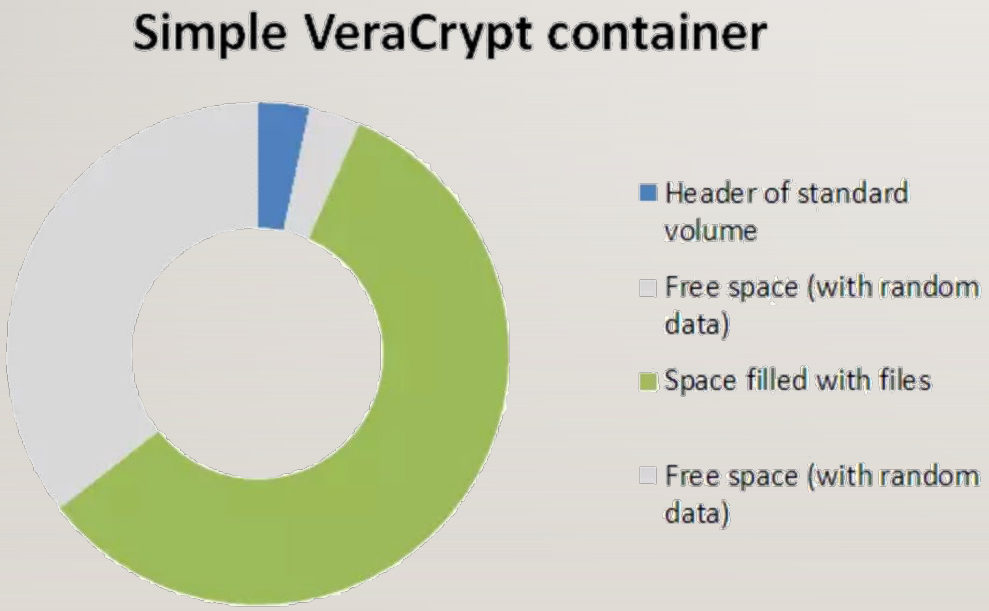
# 1) LA CRITTOGRAFIA NEGLI HARD DISK

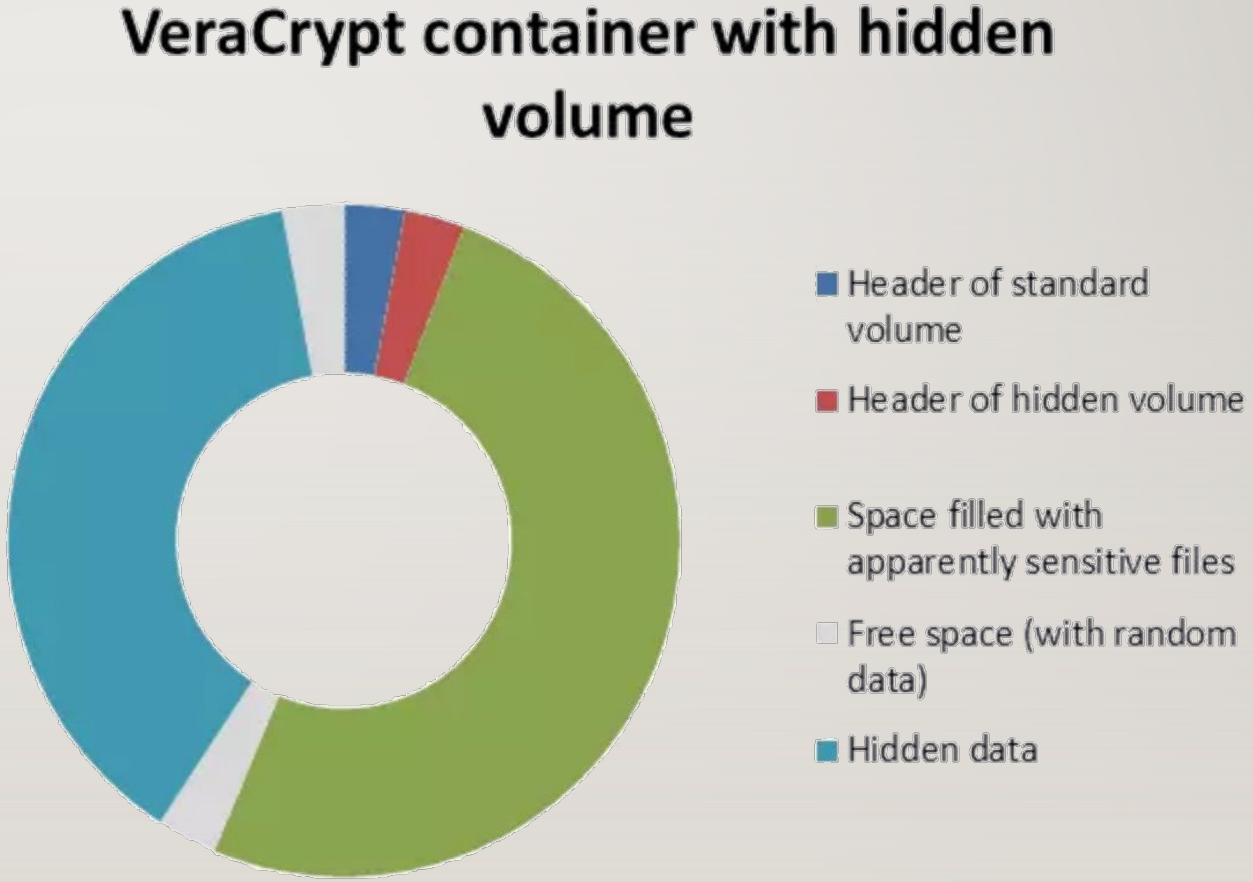
- In diverse perquisizioni operate come CT della Procura della Repubblica ho trovato dischi cifrati
- In genere tramite True/VeraCrypt, BitLocker, LUKS, FileVault2, EFS o tool minori
- Quando è stato possibile fare copia forense, si è poi presentato il problema di decifrarli
- Software utilizzati: Hashcat, John the Ripper o tool proprietari (Elcomsoft, Passware, etc...)


hashcat
advanced
password
recovery

# 1) LA CRITTOGRAFIA NEGLI HARD DISK

- Caso più interessante: Veracrypt con «hidden volume» per «plausible deniability»



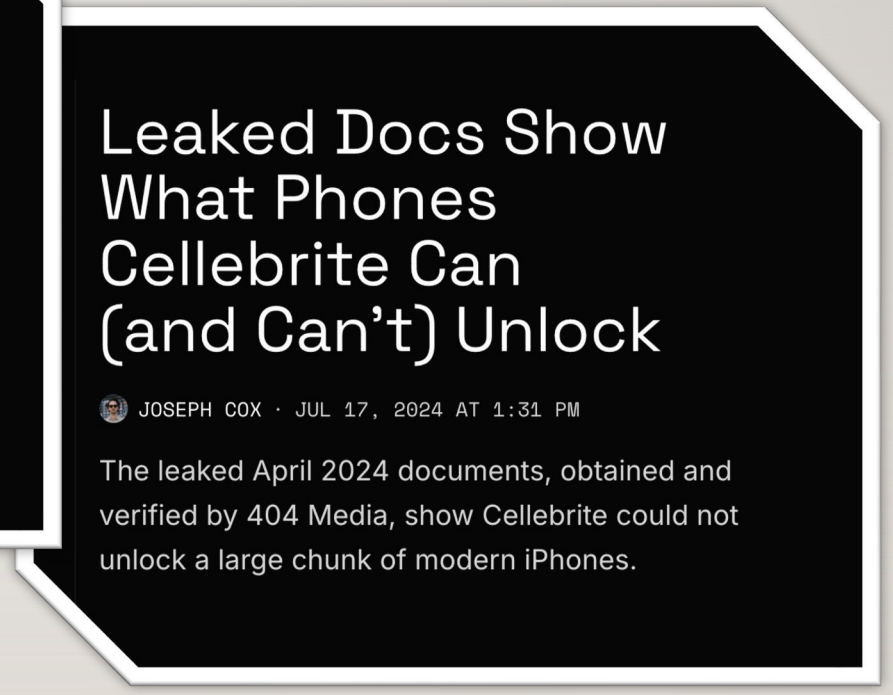
# 2) LA CRITTOGRAFIA NEGLI SMARTPHONE

- FBE/FDE – File Based/Full Disk Encryption
- Secure Enclave / Titan, coprocessore che gestisce le chiavi
- Crittografia end-to-end: per alcuni dati su iCloud + Advanced Data Protection (no in UK)
- Backup iTunes cifrati, Keychain, etc…
- Backup Whatsapp cifrato
- IM con archivi locali cifrati

# 2) LA CRITTOGRAFIA NEGLI SMARTPHONE

- Caso più interessante: smartphone protetti da PIN/Password:
  - Se lo smartphone è spento o sono trascorsi 3 giorni dall'ultimo unlock → **brute force**
  - Se lo smartphone è acceso ed è stato sbloccato entro i tre giorni (AFU) → **AFU Bypass**

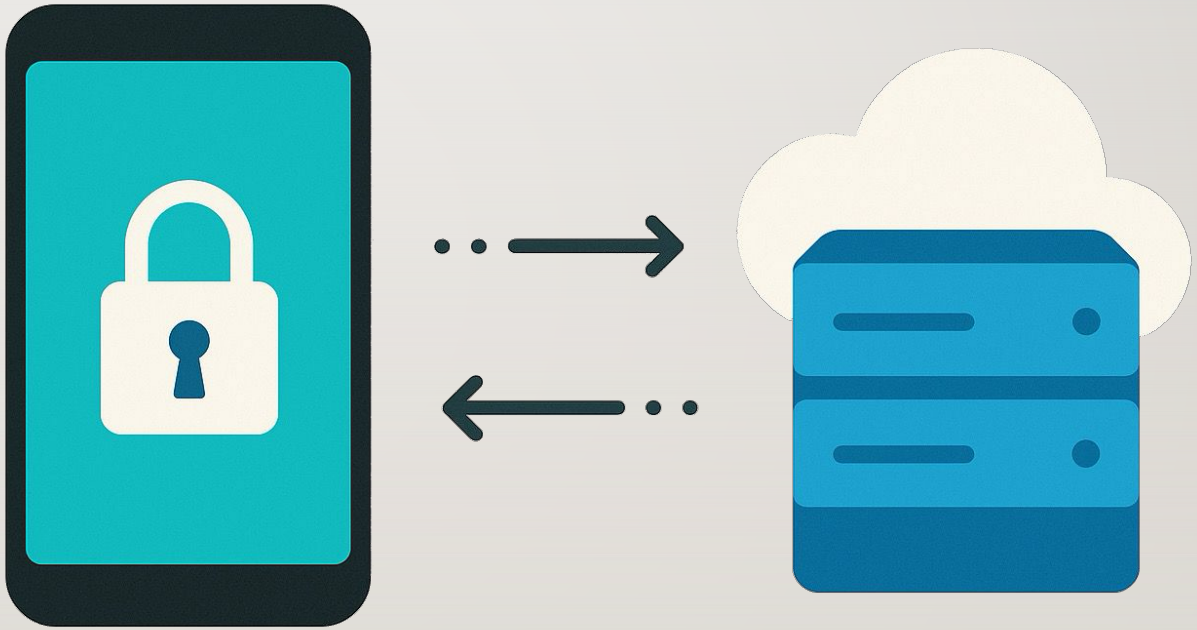

https://www.404media.co/leaked-docs-show-what-phones-cellebrite-can-and-cant-unlock/




https://www.404media.co/leaked-documents-show-what-phones-secretive-tech-graykey-can-unlock-2/

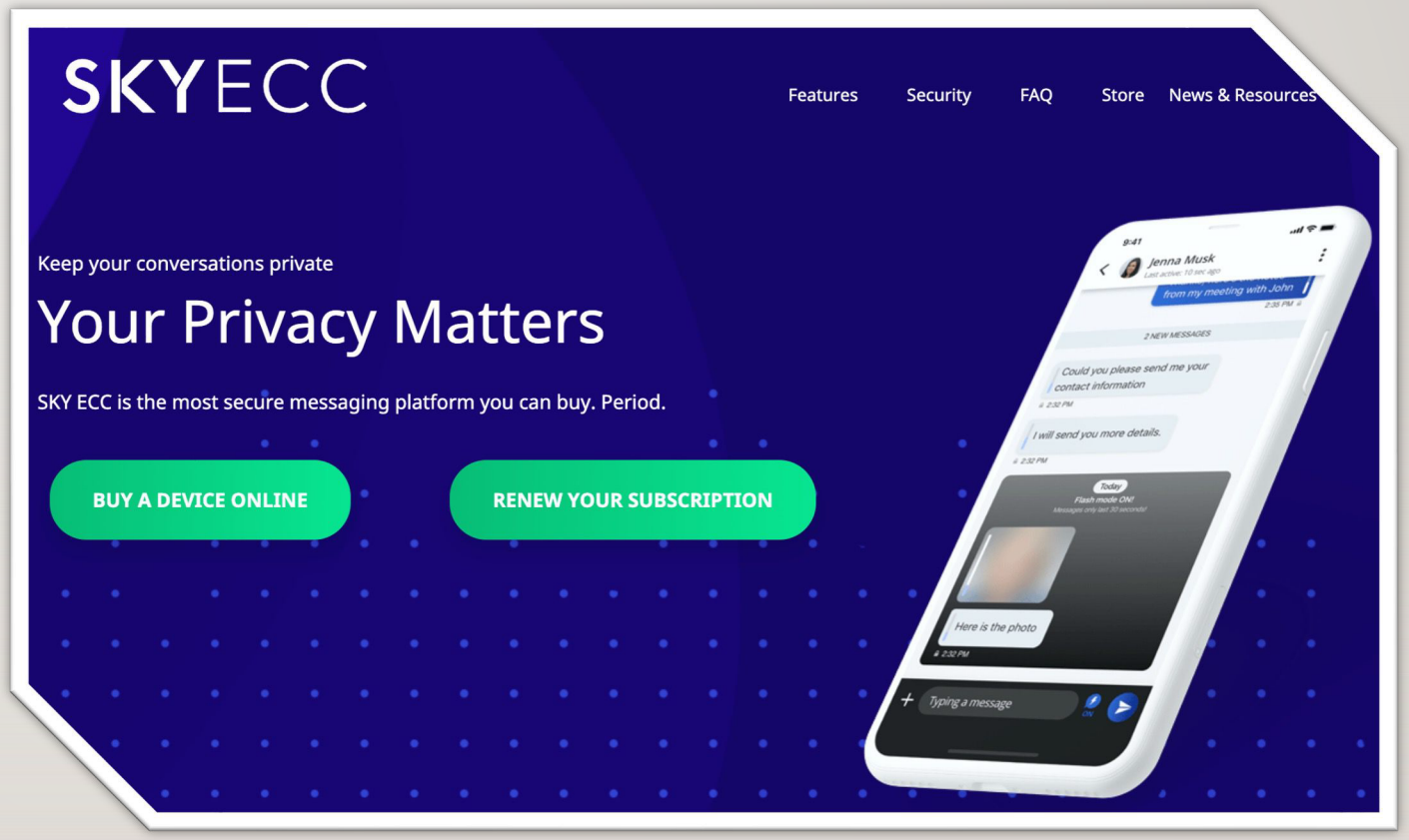
# 3) LA CRITTOGRAFIA NELLE COMUNICAZIONI

- Buona parte delle comunicazioni ormai sono cifrate: Whatsapp, iMessage, Telegram (per private chat), etc…
- La soluzione più semplice è il **sequestro** del dispositivo oppure l'installazione di **captatori/malware**



# 3) LA CRITTOGRAFIA NELLE COMUNICAZIONI

- Caso più interessante: SkyECC (ma anche Encrochat, Anom, IBC, BBM)
- Telefono blindato, comunicazioni cifrate via E2EE ma… server su OVH
- Le autorità francesi hanno decifrato i messaggi e attribuito le utenze
- Su lavialibera.it un'ottima spiegazione nell'articolo di Rosita Rijtano di come è stato aggirato l'ostacolo della cifratura end-to-end




https://web.archive.org/web/20201109032321/http://www.skyecc.com/


Grazie
per
l'attenzione