

MODULO S3.2 • AGOSTO 2026

Mobile avanzato, IoT e Veicoli

Oltre lo smartphone: stati di sicurezza,
app, oggetti connessi e mezzi di trasporto

```
python3 aleapp.py -t fs -i ./estrazione -o ./report • ileapp • sqlite3
```

Corso di Laurea Magistrale in Sicurezza Informatica

Al termine del modulo lo studente sarà in grado di

01 • VALUTARE

Lo stato di sicurezza del dispositivo sequestrato e le tecniche di estrazione praticabili in quello stato

02 • ANALIZZARE

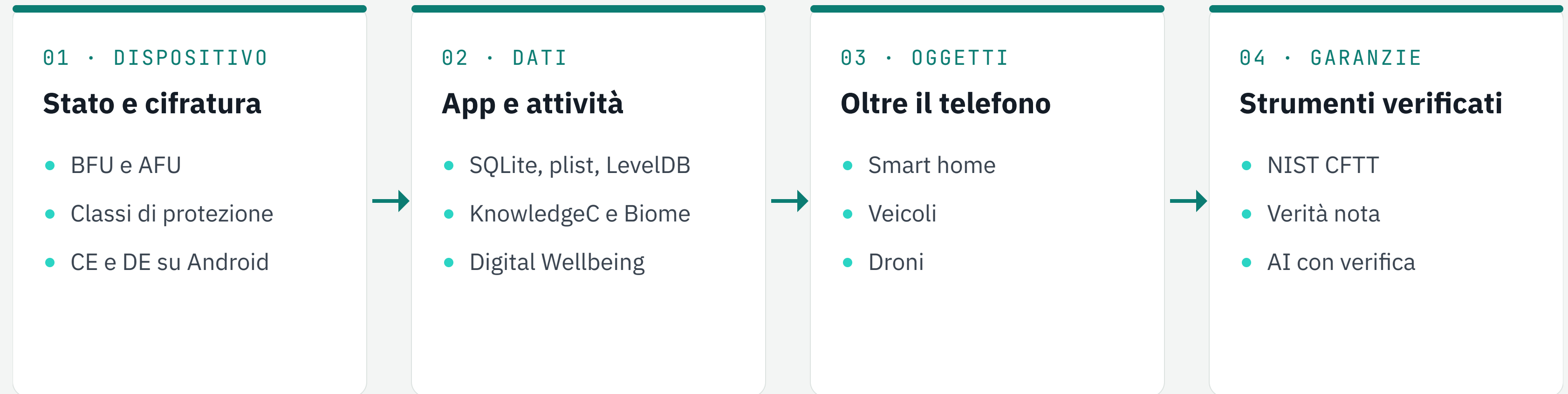
Dati di app, oggetti connessi e veicoli oltre i parser automatici, risalendo ai file sorgente

03 • VALIDARE

Strumenti di estrazione e parser su dataset con verità nota, dichiarandone versioni e limiti

Prerequisiti. Il modulo presuppone M6 Mobile forensics e i moduli core di metodo (M1-M3) e di AI (M7-M8): acquisizione, artefatti e validazione umana si applicano qui a fonti meno standardizzate.

Dal dispositivo protetto agli oggetti connessi



Le quattro aree si susseguono nelle slide del modulo nello stesso ordine dello schema: ciascuna presuppone la precedente.

BFU e AFU: lo stato decide l'estrazione

In stato **BFU** (before first unlock), cioè acceso ma mai sbloccato dopo l'ultimo riavvio, gran parte dei dati utente resta cifrata con chiavi derivate dal codice. Dopo il primo sblocco (**AFU**) quelle chiavi restano in memoria anche a schermo bloccato. Su iOS la classe di protezione predefinita protegge i file fino alla prima autenticazione dopo l'avvio.

Su Android la cifratura per file separa lo storage **DE** (device encrypted), leggibile dopo l'avvio, dallo storage **CE** (credential encrypted), accessibile solo dopo lo sblocco. Al sequestro conviene quindi mantenere il dispositivo alimentato e isolato dalla rete, annotando a verbale lo stato in cui è stato trovato.

Le versioni recenti di iOS riavviano il dispositivo dopo un lungo periodo senza sblocco, riportandolo in BFU: il tempo fra sequestro ed estrazione va documentato.

ESEMPIO • IL TELEFONO CHE SI SPEGNE IN DEPOSITO

Uno smartphone sequestrato acceso, in AFU, resta in deposito senza alimentazione e si spegne dopo due giorni.

Al laboratorio arriva in BFU e l'estrazione possibile è molto più limitata. La relazione ricostruisce la sequenza dal verbale, perché spiega la distanza fra ciò che il dispositivo conteneva e ciò che è stato estratto.

Oltre il parser: leggere i dati delle app alla fonte

SQLite e WAL

Messaggi e stati delle app risiedono quasi sempre in database **SQLite**. Il file **-wal** può contenere transazioni non consolidate e record cancellati: si acquisisce con il database e si analizza su copia, perché l'apertura può consolidarlo.

plist, protobuf, LevelDB

Le preferenze iOS stanno in file **plist**, spesso binari; molte app serializzano i dati in **protobuf**, senza nomi di campo; le app basate su tecnologie web usano archivi **LevelDB**. Ogni decodifica va dichiarata.

Cache e allegati

Miniature e allegati in cache sopravvivono spesso alla cancellazione del messaggio. Nome e percorso del file suggeriscono la conversazione di provenienza; il collegamento va dimostrato con i riferimenti nel database.

ESEMPIO • Il parser non riconosce una app di messaggistica poco diffusa. L'analista ricostruisce lo schema del database e recupera dal WAL tre messaggi cancellati; la relazione riporta query, hash dei file e logica di interpretazione.

La giornata registrata dal telefono

I sistemi mobili registrano di continuo l'uso del dispositivo. Su iOS il database **KnowledgeC** e, nelle versioni recenti, i flussi **Biome** annotano app in primo piano, stato dello schermo, blocco e sblocco. Su Android i dati di **usage stats** e di **Digital Wellbeing** conservano aperture e chiusure delle app con orari precisi.

Sono fonti preziose per ricostruire una giornata, da interpretare con prudenza. Un evento registrato descrive lo stato del sistema e non prova da solo un'azione volontaria: un evento di sistema può portare un'app in primo piano. I timestamp vanno convertiti dichiarando epoca e fuso orario.

La struttura di questi database cambia fra versioni del sistema: va dichiarata la versione e verificata l'interpretazione su un dispositivo di test.

ESEMPIO • L'ALIBI DELLO SCHERMO ACCESO

L'indagato sostiene di aver dormito dalle 23 alle 7. I dati di attività registrano lo sblocco del telefono alle 2:14 e l'app di messaggistica in primo piano per sei minuti.

Il dato è compatibile con un uso attivo. La relazione valuta anche l'ipotesi che a usarlo fosse un'altra persona e cerca riscontri nei messaggi inviati in quell'intervallo.

La casa connessa: tre livelli di dati

Il dispositivo

Hub, telecamere, serrature e altoparlanti conservano poco in locale: configurazioni, log brevi, a volte una cache di eventi. L'estrazione è spesso invasiva e specifica del modello.

L'app companion

Sullo smartphone associato l'app di gestione registra dispositivi, utenti autorizzati, notifiche e anteprime degli eventi. È di solito il livello più accessibile, con le tecniche già viste per le app.

Il cloud dell'account

Cronologia dei comandi vocali, clip delle telecamere, aperture della serratura con l'utente che le ha eseguite. Si ottiene dal fornitore o con l'esportazione dei dati dell'account, nei limiti del titolo giuridico.

ESEMPIO • Furto in abitazione senza segni di effrazione. Il log della serratura, esportato dal cloud dell'account, registra un'apertura alle 15:52 con un codice temporaneo creato due giorni prima; la telecamera dell'ingresso salva una clip alle 15:53. Le due fonti provengono da sistemi diversi e concordano: la relazione le presenta con orari normalizzati e provenienza dichiarata.

Il veicolo come testimone

L'infotainment conserva i dati dei telefoni associati via Bluetooth o cavo: identificativi, rubriche e registri delle chiamate sincronizzati, talvolta messaggi. Il navigatore registra destinazioni e percorsi; altri moduli annotano eventi come apertura delle porte e accensione, spesso con data e posizione.

La telematica del costruttore invia posizione e stato del veicolo a server remoti, raggiungibili solo con richiesta formale. L'estrazione locale richiede strumenti specializzati, a volte la rimozione del modulo, e la copertura varia molto fra costruttori e anni di produzione: va verificata prima di impegnarsi con il committente.

Il veicolo conserva dati di più conducenti e dei loro telefoni: il perimetro dell'acquisizione va definito rispetto al quesito e alla tutela dei terzi.

ESEMPIO • IL TELEFONO NELL'AUTO A NOLEGGIO

Un'auto a noleggio è stata usata per un trasporto illecito; il conducente nega e nessun telefono è stato sequestrato.

L'infotainment conserva l'associazione Bluetooth con uno smartphone, il nome del dispositivo, la rubrica sincronizzata e un percorso del navigatore. Il dato collega il veicolo a un telefono; l'attribuzione alla persona richiede riscontri, ad esempio i tabulati di quell'utenza.

Droni: log di volo e telemetria

Il velivolo

Il drone registra la telemetria di volo (posizione, quota, velocità, batteria) e salva foto e video con metadati di posizione sulla scheda di memoria, da acquisire con write blocker e hash.

L'app di controllo

Lo smartphone o il radiocomando con l'app di pilotaggio conserva registri di volo propri, spesso più completi: decollo, traiettoria, rientro. È una fonte parallela per verificare i dati del velivolo.

I limiti

Alcuni registri sono cifrati o in formati proprietari che cambiano con il firmware, e la posizione dipende dal segnale satellitare. Formato, versione, strumento di decodifica e incertezza vanno dichiarati.

ESEMPIO • Un drone sorvola un istituto penitenziario e viene recuperato a terra. La scheda contiene due video con coordinate; il registro dell'app, sullo smartphone sequestrato a un sospettato, riporta un decollo da un parcheggio a 800 metri e un percorso coerente con i video. La concordanza fra le due fonti collega il velivolo a quel dispositivo di controllo.

Validare gli strumenti prima di fidarsi dei report

Parser e strumenti di estrazione sbagliano in modi poco visibili: un campo letto con l'epoca sbagliata, un record cancellato ignorato, mittente e destinatario invertiti. Il programma **NIST CFTT** (Computer Forensics Tool Testing) pubblica metodologie e rapporti di test sugli strumenti forensi, inclusi quelli per dispositivi mobili.

In laboratorio si valida su dataset con **verità nota**: dispositivi di test con attività documentate o immagini di riferimento pubbliche descritte. Si confrontano almeno due strumenti, si verificano a mano le discrepanze sul file sorgente e si registrano le versioni, perché un aggiornamento può cambiare l'esito.

In relazione vanno nome e versione di ogni strumento, esito della validazione e discrepanze risolte, con la stessa logica del protocollo di M8.

ESEMPIO • DUE STRUMENTI, DUE ORARI

Due suite di analisi riportano orari diversi di un'ora per lo stesso messaggio.

Nel database il valore è in UTC e una suite lo mostra senza conversione e senza indicarlo. Verificata la conversione sul file sorgente e su un dispositivo di test, la relazione riporta l'orario con il fuso dichiarato e annota il comportamento dello strumento, con le versioni di entrambi.

Strumenti di AI sui dati estratti: usi e verifiche

Classificazione dei media

Modelli di visione ordinano migliaia di immagini per categoria (documenti, denaro, screenshot) e segnalano quelle da esaminare per prime. Soglie e validazione su campione, come in M8, restano obbligatorie.

Note vocali e traduzioni

La trascrizione automatica rende ricercabili centinaia di note vocali e la traduzione automatica permette il triage di chat in lingue diverse. Ciò che entra nel fascicolo va ascoltato o tradotto da una persona qualificata.

OCR degli screenshot

Gli screenshot contengono testo invisibile alla ricerca per parole chiave. L'OCR lo rende indicizzabile, con errori su caratteri simili e testo piccolo: ogni frase citata va riletta sull'immagine originale.

ESEMPIO • Un'estrazione contiene 3.200 note vocali in due lingue. Trascrizione automatica e ricerca semantica individuano 41 note pertinenti; un interprete qualificato le ascolta e ne conferma 38, correggendo due nomi propri. La relazione dichiara modello e versione, criteri di ricerca e campione di controllo sulle note scartate.

Due estrazioni, una giornata da ricostruire

Laboratorio

- Logica e full file system a confronto, su immagini pubbliche
- Due parser, discrepanze verificate sui file sorgente
- Timeline di una giornata dai database di attività

DELIVERABLE: report e timeline

Letture obbligatorie

- NIST SP 800-101 Rev. 1, *Guidelines on Mobile Device Forensics*
- R. Tamma et al., *Practical Mobile Forensics*, 4a ed.
- Documentazione di ALEAPP e iLEAPP

Verifica

Si valuta la tracciabilità di ogni evento fino al file sorgente.

Prossimo modulo: M11 Profili giuridici ed etici (traccia core), oppure il modulo base della seconda specializzazione scelta.

Con app rare, oggetti connessi e veicoli conta la capacità di risalire al dato grezzo e di documentarlo.



Grazie per l'attenzione

Vincenzo Calabrò

Domande, materiali del corso e contatti
sul sito del docente



vincenzocalabro.it