

MODULO 06 • S3.1 • AGOSTO 2026

Mobile Forensics

Il dispositivo più personale come fonte di prova:
estrazione, artefatti e il nodo della cifratura

iOS • Android • SQLite • backup • secure enclave

Corso di Laurea Magistrale in Sicurezza Informatica

Al termine del modulo lo studente sarà in grado di

01 • ISOLARE

Il dispositivo dalla rete (modalità aereo, gabbia di Faraday) per prevenire cancellazioni remote e alterazioni

02 • ESTRARRE

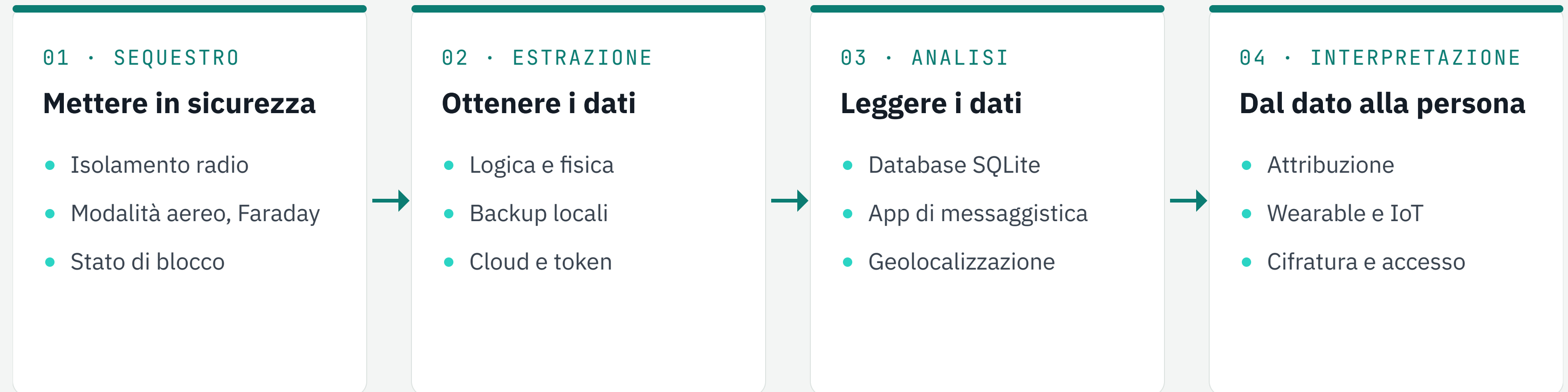
Dati con la tecnica adeguata al modello e al contesto: logica, file system o fisica, conoscendone copertura e limiti

03 • INTERPRETARE

Gli artefatti di iOS e Android (messaggistica, posizioni, pattern d'uso) dai database SQLite che li contengono

Specificità del dominio. Il dispositivo mobile non si può semplicemente spegnere e copiare, perché è di norma acceso, connesso e cifrato. Ogni scelta (isolare, mantenere acceso, estrarre subito) è una decisione forense con conseguenze irreversibili.

Dal sequestro all'interpretazione del dato mobile



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

Isolare il dispositivo nei primi istanti

Un dispositivo connesso può ricevere comandi di cancellazione remota, messaggi che sovrascrivono i vecchi e aggiornamenti che ne alterano lo stato. L'isolamento è la prima azione sulla scena:

- **Modalità aereo** se il dispositivo è sbloccato, verificando che Wi-Fi e Bluetooth siano davvero spenti
- **Gabbia/busta di Faraday** se è bloccato o non si vuole interagire: schermo i segnali radio senza toccare nulla
- **Alimentazione**: un dispositivo isolato cerca la rete e consuma più in fretta, per questo la busta si accoppia a un power bank
- **Mai spegnere d'impulso**: il riavvio porta il dispositivo in stato BFU

ESEMPIO • IL WIPE ARRIVATO TARDI

Scenario ricorrente nella prassi: smartphone sequestrato e lasciato connesso sul tavolo dell'ufficio; nella notte arriva il comando «cancella dispositivo» inviato dall'account del proprietario tramite i servizi di localizzazione.

Al mattino il dispositivo risulta riportato alle impostazioni di fabbrica e i dati non sono più recuperabili. Una busta di Faraday da pochi euro avrebbe impedito la ricezione del comando.

A verbale: stato del dispositivo al sequestro (acceso/spento, bloccato/sbloccato, livello batteria), misura di isolamento adottata e ora.

Tre livelli di profondità, copertura crescente

Tecnica	Che cosa ottiene	Limiti
Logica	Dati esposti dalle API del sistema: rubrica, messaggi, media, backup (iTunes/ADB)	Niente file cancellati né aree protette
File system	L'albero dei file accessibile, inclusi database applicativi e log	Richiede privilegi elevati; copertura variabile per app
Fisica	Immagine del supporto a basso livello, incluse aree non allocate	Spesso impraticabile sui modelli recenti con cifratura file-based

Strumenti commerciali

Cellebrite UFED, Oxygen Forensic Detective, MOBILedit: presentati a livello concettuale; copertura dei modelli e capacità di sblocco variano per versione e accordi di licenza.

Strumenti open source

ALEAPP / iLEAPP interpretano gli artefatti da estrazioni Android e iOS; **libimobiledevice** e ADB per acquisizioni logiche. Base dei laboratori del corso.

Backup locali e cloud: i dati fuori dal telefono

Quando il dispositivo è irraggiungibile (bloccato, distrutto, mai sequestrato), i suoi dati spesso esistono altrove. Il **backup iTunes/Finder** su un computer sequestrato contiene messaggi, foto e database delle app; se cifrato con password nota o recuperabile, è *più ricco* di quello in chiaro (include keychain e dati sanitari). Su Android lo stesso ruolo spetta a **Google One** e ai backup delle singole app.

Il **cloud** (iCloud, Google) conserva backup, foto, posizioni, messaggi sincronizzati. L'acquisizione passa per richieste al provider o per token di autenticazione trovati sui dispositivi dell'indagato: **strade giuridicamente diverse**, da percorrere con i titoli del modulo 11.

Il backup fotografa i dati alla data di esecuzione: il confronto con il dispositivo può indicare che cosa è stato cancellato e quando.

ESEMPIO • IL TELEFONO DISTRUTTO

L'indagato distrugge lo smartphone prima della perquisizione. Sul suo portatile, però, è presente un backup di tre settimane prima.

Dal backup: le chat rilevanti, il database delle posizioni e l'elenco delle app installate. La distruzione del dispositivo ha eliminato soltanto le ultime tre settimane. Anche la condotta distruttiva entra nella valutazione del giudice.

Dentro SQLite: WAL, free list e messaggi «cancellati»

Quasi ogni app mobile conserva i dati in database SQLite. Tre strutture interessano l'analista:

- **Il file principale (.db):** le tabelle come l'app le vede
- **Il WAL** (write-ahead log): le modifiche recenti non ancora consolidate, che può contenere versioni *precedenti* dei record e record poi «cancellati»
- **Free list e pagine non allocate:** la cancellazione di un record libera spazio senza azzerarlo; il contenuto resta finché non viene riusato (e finché un VACUUM non ripulisce)

Occorre acquisire **sempre insieme** .db, -wal e -shm e aprire il database solo da una copia: l'apertura può consolidare il WAL e alterare lo stato.

ESEMPIO • IL MESSAGGIO RITROVATO

L'utente ha eliminato una conversazione: nella tabella messaggi non c'è più. Il parsing delle pagine libere del database della messaggistica restituisce però il record integro (testo, timestamp, interlocutore), perché lo spazio non era stato riusato.

In relazione: recuperato da area non allocata del database X, con lo strumento Y, con il limite dichiarato che l'assenza di altri recuperi non prova che non esistessero altri messaggi.

WhatsApp, Telegram e Signal: tre architetture

WhatsApp

I messaggi, cifrati E2E in transito, sono conservati **in chiaro nel database locale** (msgstore su Android, ChatStorage.sqlite su iOS) e spesso nei backup. Con accesso al dispositivo sono di norma recuperabili.

Telegram

Le chat ordinarie vivono **sul cloud del provider**: dal dispositivo si recupera la cache locale, il resto dipende dalla cooperazione del gestore. Le «chat segrete» sono E2E e solo locali, e possono autodistruggersi.

Signal

Progettata per minimizzare le tracce: database locale cifrato con chiave nel keystore, **backup cloud solo facoltativo e cifrato**, metadati minimi anche lato server. Senza sblocco restano i metadati di contorno.

ESEMPIO • Stessa indagine, tre app: da WhatsApp si recuperano le chat complete con media; da Telegram la cache e l'elenco dei canali, senza le chat segrete; da Signal solo l'esistenza dell'app e i timestamp di utilizzo. La relazione deve spiegare *perché* gli esiti divergono: il perimetro del recuperabile dipende dall'architettura dell'app.

La vita dell'utente in database SQLite

Messaggistica

WhatsApp, Telegram, Signal: database locali con messaggi, allegati e metadati. La cifratura end-to-end protegge soltanto il transito: **la copia sul dispositivo ne è esclusa.**

Record cancellati talora recuperabili da free list e WAL del database.

Posizione

Celle agganciate, reti Wi-Fi viste, GPS delle foto (EXIF), cronologie delle app di mappe: fonti indipendenti da incrociare per collocare il dispositivo nello spazio e nel tempo.

Precisione eterogenea: dichiararla sempre in relazione.

Pattern d'uso

KnowledgeC (iOS) e UsageStats (Android): quando lo schermo era acceso, quale app in primo piano, quanto a lungo. È la prova che il dispositivo era «in mano» a qualcuno.

Salute e pagamenti: categorie particolari, trattamento da motivare.

Attribuzione. Il dispositivo, da solo, non identifica chi lo impugnava: l'attribuzione all'utente richiede la convergenza di più artefatti (biometria, pattern d'uso, contenuti).

Dove era il dispositivo: fonti e margini d'errore

Fonte	Precisione tipica	Avvertenze interpretative
GPS (EXIF foto, app di mappe)	Metri	Solo se attivo e a cielo visibile; EXIF alterabile
Wi-Fi (reti viste/agganciate)	Decine di metri	Prossimità a un access point; mappature non infallibili
Cella telefonica	Da centinaia di metri a chilometri	La cella agganciata non è sempre la più vicina
Cronologie delle app	Variabile	Stima del fornitore con metodologia non ispezionabile

ESEMPIO • CONVERGENZA E LIMITE • Alle 21:30 il dispositivo aggancia la cella del quartiere; alle 21:34 rileva la rete Wi-Fi del bar; alle 21:41 una foto con coordinate GPS lo colloca a 40 metri dal luogo del fatto. Le tre fonti indipendenti restringono l'area in cui si trovava **il dispositivo**; per collocarvi il proprietario serve l'attribuzione (slide successiva).

In relazione ogni collocazione indica fonte, margine d'errore e orario in UTC; sulla mappa va disegnato il cerchio d'incertezza.

Attribuire l'uso del dispositivo a una persona

L'attribuzione si costruisce per convergenza di indicatori: il solo possesso del dispositivo non basta a fondarla. Gli indicatori principali:

- **Sblocchi biometrici** negli istanti rilevanti: collegano l'uso a una caratteristica fisica della persona
- **Pattern d'uso** (KnowledgeC, UsageStats): quali app, a che ora, confrontabili con le abitudini note del soggetto
- **Contenuti autoriali**: messaggi con stile, informazioni o foto che solo quella persona poteva produrre
- **Contesto fisico**: videosorveglianza, testimoni, altri dispositivi della stessa persona coerenti per posizione

ESEMPIO • DUE LETTURE DELLO STESSO DATO

Il messaggio incriminato parte alle 22:17 dal dispositivo di A. **Lettura debole**: «è il telefono di A, quindi ha scritto A».

Lettura solida: alle 22:16 uno sblocco biometrico; alle 22:15 e 22:19 l'app abituale di A in uso; il testo contiene un dettaglio noto solo ad A; nessun segno di accesso remoto. Quattro elementi convergenti, con l'ipotesi alternativa (uso da parte di terzi) esaminata ed esclusa per iscritto.

La relazione discute sempre le **ipotesi alternative**: dispositivo prestato, lasciato sbloccato e incustodito, compromesso da remoto.

Smartwatch, fitness tracker e assistenti vocali

I dispositivi indossabili registrano ciò che nessun altro artefatto cattura: **battito cardiaco, passi, sonno, allenamenti georeferenziati**.

I dati risiedono su tre livelli (dispositivo, app companion sullo smartphone, cloud del produttore); il livello intermedio è spesso il più accessibile, con le tecniche di estrazione già viste.

Gli **assistenti vocali** domestici conservano cronologia dei comandi (e talvolta frammenti audio) nel cloud dell'account; serrature smart, termostati e contatori registrano presenze e abitudini. Il valore probatorio è spesso **negativo o di riscontro**, ad esempio per smentire un alibi o confermare un orario.

Il sensore registra i parametri di chi lo indossa, che può non essere il titolare; la precisione dei sensori consumer va dichiarata in relazione.

ESEMPIO • L'ALIBI E IL BATTITO

L'indagato dichiara di aver dormito a casa tutta la notte. Il suo fitness tracker registra invece, fra le 2:10 e le 3:40, frequenza cardiaca da attività fisica e 4.800 passi.

Il dato smentisce la versione dichiarata e riorienta l'indagine, pur senza indicare dove si trovasse l'indagato né che cosa facesse. In dibattimento la difesa chiederà chi indossava il dispositivo: il dato non lo indica, e l'analista deve riconoscerlo.

Il dibattito accesso investigativo vs sicurezza

La cifratura file-based ancorata all'hardware (Secure Enclave, Android Keystore) rende il contenuto inaccessibile senza codice di sblocco. Lo stato del dispositivo è decisivo: **AFU** (sbloccato almeno una volta dopo l'accensione) espone più chiavi in memoria di **BFU**.

Il precedente **Apple–FBI (San Bernardino, 2016)** ha posto il tema in termini sistemici: imporre al produttore di indebolire la cifratura protegge un'indagine ma espone tutti gli utenti. Il caso si chiuse con l'accesso ottenuto da un fornitore terzo, lasciando irrisolta la questione di principio.

Coordinate del dibattito

- Nessuna backdoor è selettiva: chiunque ottenga la chiave destinata all'autorità può usarla
- L'alternativa pratica: vulnerabilità e strumenti di sblocco di terze parti, con i loro costi e la loro opacità
- Obblighi di collaborazione dell'indagato: limiti del nemo tenetur se detegere

Una giornata ricostruita da un'estrazione

Laboratorio

- Analisi di un'estrazione Android pubblica con **ALEAPP**
- Esame dei database SQLite
- Cronologia degli spostamenti

DELIVERABLE: cronologia giornaliera documentata

Letture obbligatorie

- Mahalik et al., *Practical Mobile Forensics*
- Linee guida SWGDE sui dispositivi mobili
- Documentazione ALEAPP/iLEAPP

Verifica

Si valuta la distinzione tra dato, inferenza e attribuzione: ogni collocazione indica fonte e margine d'errore.

Prossimo modulo: S3.2 Mobile avanzato, IoT e veicoli.

Il modulo avanzato S3.2 estende lo stesso metodo a oggetti connessi, veicoli e droni.



Grazie per l'attenzione

Vincenzo Calabrò

Domande, materiali del corso e contatti
sul sito del docente



vincenzocalabro.it