CORSO AVANZATO DI DIGITAL FORENSICS

Acquisizione forense da smartphone sbloccato e bloccato

Chiamate, messaggi, timeline delle attività e geolocalizzazione: che cosa si ottiene in ciascuno stato del dispositivo

Relatore: Vincenzo Calabrò

Materiale didattico con fonti normative e scientifiche aggiornate a novembre 2026.

Programma e obiettivi della mezza giornata

Parte	Contenuto	Durata
1	Lo smartphone come fonte di prova	30 min
2	Quadro normativo e standard	40 min
	Pausa	15 min
3	Metodo: stati del dispositivo e artefatti	50 min
4	Laboratorio guidato con strumenti open source	70 min
5	Caso di studio, quiz di verifica, bibliografia	35 min

Quattro ore complessive. In laboratorio si lavora su database sintetici costruiti per il corso, mai su dati reali.

Al termine lo studente è in grado di

- riconoscere lo stato di un dispositivo e dire che cosa se ne può ottenere, e per quanto tempo ancora;
- indicare dove risiedono chiamate, messaggi, attività e posizioni su Android e su iOS;
- costruire una timeline unificata in UTC e verificarne la plausibilità;
- scegliere, per un dispositivo bloccato, le vie lecite alternative all’accesso diretto.

PARTE 1 · 30 MINUTI

Lo smartphone come fonte di prova

Lo stesso telefono restituisce quasi tutto, una parte o quasi nulla secondo lo stato in cui lo si trova. Quello stato cambia da solo, con il passare delle ore.

I quattro stati di un dispositivo

Sbloccato

Schermo aperto

I dati dell'utente sono decifrati e le app rispondono. È la condizione più favorevole e la più breve: basta il blocco automatico per perderla.

Bloccato · AFU

After First Unlock

Dopo l'ultima accensione il codice è stato inserito almeno una volta. Gran parte delle chiavi è ancora in memoria, ma lo schermo è chiuso.

Bloccato · BFU

Before First Unlock

Dopo l'accensione il codice non è mai stato inserito. I dati dell'utente restano cifrati con chiavi che dipendono da quel codice.

Spento

Nessuna chiave in memoria

All'accensione il dispositivo si troverà in BFU. Spegnere un telefono acceso è una scelta che non si può annullare.

La direzione è una sola. Da sbloccato a bloccato, da AFU a BFU: ogni passaggio riduce ciò che si può ottenere, e soltanto il codice dell'utente permette di tornare indietro.

La prima annotazione del verbale è lo stato del dispositivo, con l'ora in cui è stato osservato.

Fonti: Apple Platform Security; documentazione Android sulla file-based encryption; SWGDE 18-F-003-2.0, 2025.

Quattro famiglie di evidenze, due luoghi

Evidenza	Sul dispositivo	Fuori dal dispositivo
Chiamate	Registro delle chiamate del sistema; chiamate delle app nei rispettivi database	Tabulati dell'operatore, con le celle agganciate
Messaggi	SMS e MMS nel database di sistema; iMessage; app di messaggistica	Backup nel cloud; per gli SMS, tabulati privi di contenuto
Attività	Registri d'uso delle app, dello schermo, di blocco e sblocco, dell'alimentazione	Quasi nulla: è una prova che esiste soltanto sul telefono
Posizione	Cache di localizzazione, reti Wi-Fi note, metadati delle foto, dati delle app	Celle presso l'operatore; cronologie nel cloud, quando attive

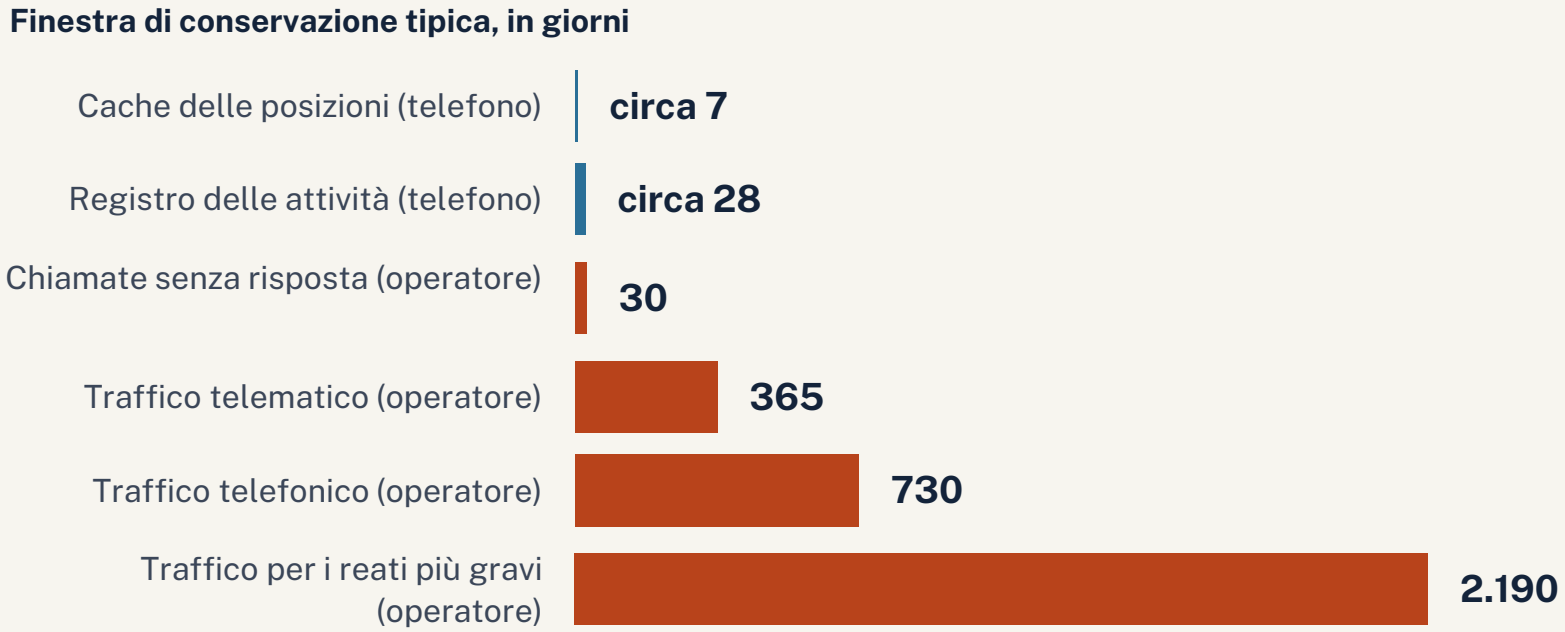
Le due colonne si controllano a vicenda. Una chiamata nel registro del telefono deve comparire nel tabulato, e viceversa. Quando non accade, la differenza è essa stessa un dato.

La terza riga è la più fragile. Le attività non hanno copie altrove e durano poche settimane: se il dispositivo si perde o si blocca, si perdono con lui.

Quanto dura ogni fonte

72 ore

senza sblocco, e un iPhone con iOS 18.1 o successivo si riavvia da solo, passando da AFU a BFU.



Il telefono dimentica in giorni, l'operatore in anni. Le due prime barre quasi non si vedono: è il motivo per cui il dispositivo si acquisisce subito.

Fonti: art. 132 d.lgs. 196/2003 e L. 167/2017 per l'operatore; per il telefono, valori indicativi su iOS riportati dalla letteratura tecnica, variabili con la versione.

Che cosa occorre poter dimostrare

Chi ha comunicato con chi

Numeri, verso, esito e durata di ogni chiamata; mittente, destinatario e testo di ogni messaggio. Il registro prova il contatto fra due utenze, non l'identità di chi parlava.

Che cosa faceva il telefono

Schermo acceso o spento, sblocchi, app in primo piano. È l'indizio più diretto che qualcuno lo stesse usando in quel momento.

Dove si trovava

Ogni posizione con la sua fonte e la sua accuratezza. Un punto ricavato da una cella non vale quanto un punto GPS, e va detto.

Quando

Tutte le fonti ricondotte a UTC, con lo scarto dell'orologio del dispositivo e il fuso in cui il telefono si trovava.

Le quattro risposte acquistano valore insieme: una chiamata, uno sblocco e una posizione nello stesso minuto raccontano più della loro somma.

Che cosa si ottiene in ciascuno stato

	Chiamate	Messaggi	Attività	Posizione
Dispositivo sbloccato	**Sì**	**Sì**	In parte	In parte
Dispositivo bloccato, AFU	In parte	In parte	In parte	In parte
Dispositivo bloccato, BFU	No	No	No	No
Operatore, backup e cloud	**Sì**	In parte	No	In parte

- **Sbloccato**: «in parte» perché attività e posizioni stanno in aree che il backup non copre e richiedono un'estrazione più profonda.
- **AFU**: «in parte» perché l'accesso dipende da strumenti specialistici, dal modello e dalla versione del sistema.
- **Ultima riga**: non dipende dallo stato del telefono. È la via che resta quando il dispositivo non si apre.

Valutazione qualitativa proposta per la discussione in aula; non deriva da una misurazione.

PARTE 2 · 40 MINUTI

Quadro normativo e standard

Sequestrare un telefono, aprirlo e chiedere i tabulati sono tre atti diversi, con tre titoli diversi. La tecnica viene dopo.

Venticinque anni di norme, standard e tecnologia

2001
Convenzione di Budapest sulla criminalità informatica

2008
L. 48/2008: perquisizioni e sequestri informatici nel c.p.p.

2012
ISO/IEC 27037 sulle prove digitali

2014
NIST SP 800-101 Rev. 1; Riley v. California sul telefono dell'arrestato

2017
L. 167/2017: tabulati conservati fino a 72 mesi per i reati più gravi

2018
Carpenter v. United States sui dati di cella

2021
CGUE C-746/18; d.l. 132/2021: tabulati con decreto del giudice

2023
Corte cost. n. 170; Google annuncia la cronologia delle posizioni sul dispositivo

2024
CGUE C-548/21; iOS 18 introduce il riavvio per inattività

2025
SWGDE 18-F-003 v2.0; Cass. n. 1269 sul consenso dell'indagato

2026
e-Evidence applicabile dal 18 agosto

In corso
Disegno di legge sull'art. 254-ter c.p.p.: sequestro dei dispositivi

Negli stessi anni i giudici hanno alzato le garanzie e i produttori hanno accorciato i tempi utili: le due spinte vanno nella stessa direzione.

Italia: sequestrare e ispezionare un telefono

Art. c.p.p.	Che cosa consente	Rilievo pratico
247, co. 1-bis	Perquisizione di sistemi informatici con misure che conservino i dati originali	Ricerca dentro il dispositivo
254	Sequestro di corrispondenza	Messaggi, dopo Corte cost. n. 170/2023
354, co. 2	Accertamenti urgenti della polizia giudiziaria	Isolamento, preservazione, copia immediata
360	Accertamenti tecnici non ripetibili, con avviso alle parti	Estrazioni che modificano lo stato del dispositivo

Proporzionalità

La giurisprudenza di legittimità chiede che il provvedimento indichi che cosa si cerca e in quale periodo, e che le copie dei dati estranei siano restituite o cancellate.

In discussione: art. 254-ter

Il disegno di legge approvato dal Senato nell'aprile 2024 affida al giudice il sequestro dei dispositivi e regola duplicazione e selezione dei contenuti. Lo stato dell'iter va verificato.

Fonti: c.p.p. come modificato dalla L. 48/2008; Corte cost., sent. n. 170/2023; Senato, A.S. 806, e Camera, A.C. 1822. Riferimenti da riscontrare sulle banche dati ufficiali.

Aprire un telefono bloccato: i limiti giuridici

Il codice

L’indagato non è tenuto a rivelarlo. Il rifiuto è esercizio del diritto di difesa e, secondo la Cassazione, non può valere come indizio di colpevolezza.

Il consenso

Per Cass. pen., sez. VI, n. 1269/2025 il consenso prestato da chi è già di fatto indagato non supplisce alla mancanza di un provvedimento dell’autorità giudiziaria.

L’impronta e il volto

In Italia manca una norma espressa sullo sblocco biometrico coattivo e la dottrina è divisa. Nei Paesi Bassi la Corte Suprema lo ha ammesso nel 2021 per l’impronta digitale.

Il tentativo di accesso

Per la Corte di giustizia (C-548/21) anche il tentativo di accedere ai dati di un telefono è un trattamento che richiede, salvo urgenza, l’autorizzazione preventiva di un giudice o di un’autorità indipendente.

Il consulente non decide se si può aprire. Documenta chi lo ha deciso, con quale atto, e che cosa ha fatto di conseguenza.

Fonti: Cass. pen., sez. VI, n. 1269/2025; CGUE, C-548/21; Cotti, Archivio Penale 2/2025; Hoge Raad, 9 febbraio 2021. Indicazioni didattiche, non pareri legali.

I tabulati: l’altra metà delle chiamate

Dato presso l’operatore	Conservazione
Traffico telefonico	24 mesi
Traffico telematico	12 mesi
Chiamate senza risposta	30 giorni
Reati di particolare gravità	fino a 72 mesi

Il tabulato riporta utenze, data, ora, durata e cella agganciata. Non contiene il contenuto delle comunicazioni.

Come si acquisiscono

- Dal 30 settembre 2021 con **decreto motivato del giudice**, su richiesta del pubblico ministero.
- Nei casi di urgenza provvede il pubblico ministero, che lo comunica al giudice entro 48 ore per la convalida.
- La riforma segue la sentenza della Corte di giustizia del 2 marzo 2021, C-746/18.

Registro del telefono e tabulato si confrontano riga per riga. Una chiamata cancellata dal dispositivo resta nel tabulato per due anni.

Fonti: art. 132 d.lgs. 196/2003, come modificato dal d.l. 132/2021, conv. in L. 178/2021; L. 167/2017, art. 24; CGUE, C-746/18.

Unione europea e Stati Uniti: tre decisioni da conoscere

CGUE, C-548/21 · 2024

L’accesso della polizia ai dati di un telefono non è riservato ai reati gravi, ma richiede di regola un’autorizzazione preventiva, il rispetto della proporzionalità e l’informazione dell’interessato.

Riley v. California · 2014

La Corte Suprema degli Stati Uniti esige di regola un mandato per esaminare il contenuto del telefono di una persona arrestata.

Carpenter v. United States · 2018

Lo stesso vale per lo storico delle celle agganciate: la posizione ricostruita nel tempo è protetta quanto il contenuto.

Posizioni presso i fornitori. Dal 2024 Google conserva la cronologia delle posizioni sul dispositivo dell’utente e non è più in grado di rispondere alle richieste per area geografica. Quella prova, oggi, sta di nuovo nel telefono.

Le tre corti partono dalla stessa premessa: un telefono racconta la vita intera di una persona, non un singolo fatto.

Fonti: CGUE, Grande Sezione, 4 ottobre 2024, C-548/21; Riley v. California, 573 U.S. 373 (2014); Carpenter v. United States, 585 U.S. 296 (2018); annunci Google, 2023–2024.

Gli standard tecnici per i dispositivi mobili

NIST SP 800-101 Rev. 1 · 2014

Guidelines on Mobile Device Forensics. Descrive preservazione, acquisizione, esame e relazione, e ordina i metodi di estrazione in cinque livelli di invasività crescente.

SWGDE 18-F-003 v2.0 · 2025

Raccolta, preservazione, gestione e acquisizione dei dispositivi mobili. Parte dal fatto che i dati di un apparecchio acceso cambiano di continuo e chiede di ridurne al minimo la manipolazione.

SWGDE 20-F-005 v1.0 · 2020

Best Practices for Mobile Device Forensic Analysis. Copre la fase successiva: l'analisi di applicazioni e database dopo l'acquisizione.

ISO/IEC 27037:2012

Identificazione, raccolta, acquisizione e conservazione della prova digitale, con i requisiti di verificabilità, ripetibilità, riproducibilità e giustificabilità.

Sono documenti di metodo. Dove stia oggi un registro delle chiamate, e in quale formato, lo si ricava dal dispositivo e dalla versione del sistema.

Fonti: Ayers, Brothers e Jansen, NIST SP 800-101 Rev. 1, 2014; SWGDE, documenti 18-F-003-2.0 e 20-F-005-1.0; ISO/IEC 27037:2012.

Dal requisito all’artefatto

Requisito	Che cosa lo soddisfa
Stato e identità del dispositivo	Fotografie, modello, numero di serie o IMEI, versione del sistema, stato osservato e ora dell’osservazione
Contatti fra utenze	Registro delle chiamate e database dei messaggi estratti, riscontrati sul tabulato dell’operatore
Presenza di un utilizzatore	Registri di sblocco, schermo e app in primo piano negli stessi minuti dell’evento
Luogo	Posizioni con fonte e accuratezza, confrontate con le celle del tabulato e con i metadati delle foto
Collocazione nel tempo	Ogni orario convertito in UTC dall’epoca propria della fonte, con lo scarto dell’orologio a verbale
Integrità	Hash di ogni file estratto e dell’archivio, marca temporale alla chiusura
Legittimità dell’accesso	Provvedimento per il sequestro, per l’esame del contenuto e, a parte, per i tabulati

La tabella si legge anche al contrario: ogni riga senza artefatto è una domanda che la controparte potrà porre.

PARTE 3 · 50 MINUTI

Metodo e artefatti

Prima lo stato del dispositivo e ciò che ne consegue, poi le quattro famiglie di evidenze una per una, con i file in cui risiedono.

Stato del dispositivo e cifratura

Stato	iOS	Android
BFU	Accessibili soltanto i dati privi di protezione; le classi legate al codice restano chiuse	Aperta la sola area «device encrypted»: impostazioni, sveglie, poco altro
AFU	In memoria le chiavi della classe predefinita per i dati delle app, protetti fino al primo sblocco	Aperta anche l'area «credential encrypted», con i dati dell'utente
Sbloccato	Disponibili tutte le classi, comprese quelle che si richiudono a ogni blocco	Come AFU, con in più l'interfaccia e le autorizzazioni dell'utente

72 ore

Da iOS 18.1 un iPhone bloccato da tre giorni si riavvia e torna in BFU. Nessun avviso, nessuna dipendenza dalla rete o dalla carica.

Porta dati

Su iOS, dopo un'ora di blocco, la connessione dati via cavo richiede lo sblocco. Collegare in ritardo equivale a non collegare.

Android

Dal 2025 Google ha annunciato un riavvio automatico analogo dopo tre giorni di blocco. Va verificato sul singolo dispositivo.

Fonti: Apple Platform Security; documentazione Android (file-based encryption); analisi pubbliche del riavvio per inattività, novembre 2024.

La preservazione, stato per stato

Se è sbloccato

Impedire che si blocchi: è l'unica occasione. Modalità aereo, poi acquisizione immediata o, se non è possibile, sospensione del blocco automatico nei limiti del titolo.

Se è bloccato e acceso

Non spegnerlo. Alimentarlo, isolarlo dalla rete con un contenitore schermato, annotare l'ora: da quel momento le 72 ore corrono. Consegna al laboratorio con priorità.

Se è spento

Lasciarlo spento. Accenderlo lo porta in BFU e, se trova la rete, lo espone a un comando di cancellazione a distanza.

In ogni caso. Non si provano codici: i tentativi falliti allungano i tempi di attesa e possono far scattare la cancellazione. Non si avvicina il telefono al volto o al dito di nessuno senza un titolo che lo preveda. Ogni gesto si annota con l'ora.

Chi interviene per primo decide, spesso senza saperlo, a quale riga della matrice apparterrà quel dispositivo.

Fonti: SWGDE 18-F-003-2.0, 2025; NIST SP 800-101 Rev. 1, 2014.

Quando il dispositivo non si apre: le vie lecite

Via	Che cosa può dare	Condizione
Codice dal titolare	Tutto ciò che dà un dispositivo sbloccato	Collaborazione volontaria e documentata
Computer abbinato	Backup locali già presenti; talvolta un nuovo backup	Disponibilità del computer e titolo che lo comprenda
Backup e account cloud	Registro chiamate, messaggi e altro, secondo ciò che l'utente sincronizzava	Credenziali o richiesta al fornitore; cifratura end-to-end assente
Operatore	Tabulati e celle: chiamate, SMS senza contenuto, posizione approssimata	Decreto del giudice
Altri dispositivi	Lo stesso contenuto visto dall'interlocutore, da un tablet, da un orologio	Titolo esteso a quei dispositivi
Laboratori specializzati	Estrazioni da dispositivi in AFU con strumenti commerciali riservati	Modello e versione supportati; forme dell'accertamento non ripetibile

Cinque vie su sei non toccano il telefono bloccato. Un dispositivo che non si apre riduce le fonti, raramente le azzera.

Sintesi didattica. Gli strumenti commerciali non sono oggetto del corso: vanno citati in relazione con versione, operazioni compiute e limiti dichiarati dal produttore.

Chiamate: registro del telefono e tabulato

Android

calllog.db, tabella calls: numero, data in millisecondi dall'epoca Unix, durata in secondi, tipo.

Tipo 1 ricevuta, 2 effettuata, 3 persa, 5 rifiutata. Alcuni produttori usano un database proprio.

iOS

CallHistory.storedata, tabella ZCALLRECORD: indirizzo, data in secondi dal 1° gennaio 2001, durata, origine, risposta.

Vi confluiscono anche FaceTime e le chiamate delle app integrate con il sistema.

Tre avvertenze

- **Capienza**: il registro è limitato e le voci più vecchie vengono eliminate; il tabulato copre due anni.
- **Cancellazioni**: una voce rimossa dall'utente sparisce dal registro, non dal tabulato.
- **Chiamate via dati**: quelle delle app di messaggistica non compaiono nel tabulato telefonico; restano nei database delle app.

Fonti: percorsi e tabelle ricavati dal codice di ALEAPP e iLEAPP, versioni del 28 novembre 2026; art. 132 d.lgs. 196/2003.

Messaggi: SMS, iMessage e app

Android · SMS e MMS

mmssms.db, tabella sms: indirizzo, data in millisecondi Unix, tipo (1 ricevuto, 2 inviato), testo. Gli MMS stanno in tabelle separate.

I messaggi RCS risiedono nel database dell'app Messaggi.

iOS · SMS e iMessage

sms.db, tabelle message, handle e chat: lo stesso database per entrambi i servizi, distinti da un campo. Date in nanosecondi dal 2001.

Gli eliminati restano recuperabili dall'utente per circa 30 giorni.

App di messaggistica

WhatsApp, Telegram, Signal e le altre hanno database propri, cifrature proprie e regole proprie.

Sono l'oggetto di un corso dedicato di questa serie.

Che cosa resta fuori dal telefono. Per gli SMS il tabulato conserva mittente, destinatario e ora, mai il testo. Per iMessage e per le app l'operatore vede soltanto traffico dati.

Per il contenuto di un messaggio il dispositivo, o un suo backup, resta la sola fonte.

Fonti: percorsi e tabelle ricavati dal codice di ALEAPP e iLEAPP, versioni del 28 novembre 2026; documentazione Apple e Google.

Timeline delle attività: che cosa faceva il telefono

iOS	Android	Che cosa dimostrano
knowledgeC.db registra per flussi: app in primo piano, uso delle app, dispositivo bloccato o sbloccato, schermo acceso. Nelle versioni recenti molti flussi sono passati ai file **Biome**. Il registro di alimentazione aggiunge batteria, ricarica e attività delle app.	**usagestats** conserva gli eventi di avvio e chiusura delle app; il database di **Benessere digitale** ne tiene una cronologia per app, con sblocchi e notifiche. Formati e profondità variano con la versione e con il produttore.	Che in un certo minuto lo schermo era acceso, il telefono sbloccato e una certa app in primo piano. È il dato che lega un messaggio o una posizione a un utilizzo attivo. Dimostrano l'uso del dispositivo. Chi lo usasse resta da provare.

Due limiti. Queste tracce coprono poche settimane e stanno in aree che un backup ordinario non contiene: richiedono un'estrazione completa del file system, quindi un dispositivo sbloccato o un laboratorio attrezzato.

È la famiglia di evidenze meno nota in aula e, spesso, la più decisiva.

Fonti: flussi e percorsi ricavati dal codice di ALEAPP e iLEAPP, versioni del 28 novembre 2026. Valori di conservazione indicativi.

Geolocalizzazione: fonti e accuratezza

Fonte	Che cosa contiene	Avvertenza
Cache di localizzazione iOS	Punti con coordinate, ora, accuratezza orizzontale e velocità	Copre circa una settimana
Luoghi significativi iOS	Luoghi frequentati, con le visite e la loro durata	Sono luoghi dedotti dal sistema, non singoli rilevamenti
Cronologia di Google Maps	Visite e percorsi, se l'utente l'ha attivata	Dal 2024 risiede sul dispositivo; di default conserva tre mesi
Reti Wi-Fi note	Reti a cui il telefono si è collegato, con l'ultimo collegamento	Collocano il telefono presso un punto di accesso, se la sua sede è nota
Fotografie	Coordinate e ora nei metadati EXIF	Ora locale, spesso senza indicazione del fuso
Celle, presso l'operatore	Cella agganciata a ogni chiamata o sessione dati	Indica un'area, da centinaia di metri a chilometri

Ogni punto si riporta con la sua fonte e il suo margine di errore. Un cerchio di due chilometri non è un indirizzo.

Fonti: percorsi ricavati dal codice di iLEAPP; annunci Google sulla cronologia delle posizioni, 2023–2024. Accuratezze indicative.

Il tempo: epoche, unità e fusi

Fonte	Epoca	Unità	Esempio
Android: chiamate, SMS	1° gennaio 1970, UTC	millisecondi	1795767160137
iOS: chiamate, attività, posizioni	1° gennaio 2001, UTC	secondi	817459961.25
iOS: sms.db	1° gennaio 2001, UTC	nanosecondi	817459961250000000
Chrome: cronologia	1° gennaio 1601, UTC	microsecondi	valore a 17 cifre
Fotografie: EXIF	nessuna: data e ora in chiaro	secondi	ora locale del dispositivo

La costante da ricordare. Fra le due epoche principali corrono 978.307.200 secondi. Leggere una data iOS come se fosse Unix la sposta indietro di 31 anni; l'errore inverso passa meno inosservato.

Il fuso. I database registrano in UTC, l'interfaccia mostra l'ora locale, le foto scrivono l'ora locale senza dirlo. La timeline si costruisce in UTC e si traduce soltanto alla fine.

I primi due esempi sono tratti dal dataset sintetico del laboratorio e corrispondono allo stesso istante, il 27 novembre 2026 alle 08:12 UTC.

Dove cercano i parser

Evidenza	Android	iOS
Chiamate	`com.android.providers.contacts/databases/calllog.db`	`CallHistoryDB/CallHistory.storedata`
SMS	`com.android.providers.telephony/databases/mmssms.db`	`Library/SMS/sms.db`
Attività	`system/usagestats/com.google.android.apps.wellbeing/`	`CoreDuet/Knowledge/knowledgeC.db` `Biome/`
Posizioni	Nei dati delle singole app, a partire da Google Maps	`Library/Caches/com.apple.routined/Cache.sqlite, Local.sqlite`

Sono database SQLite in aree che l'utente non vede. Un backup contiene chiamate e SMS; attività e posizioni richiedono l'estrazione completa.

Fonte: percorsi ricavati dal codice di ALEAPP e iLEAPP (github.com/abrignoni), versioni del 28 novembre 2026.

La cassetta degli strumenti open source

Strumento	A che cosa serve	Limite da conoscere
adb	Colloquio con un Android sbloccato: informazioni, registri di sistema, interrogazione di chiamate e SMS	Richiede il debug USB autorizzato dallo schermo sbloccato
libimobiledevice	Informazioni e backup di un iPhone abbinato alla postazione	L'abbinamento richiede il codice; il backup non contiene attività e posizioni
ALEAPP e iLEAPP	Parsing di estrazioni Android e iOS, con report per artefatto	Dipendono dallo schema della versione del sistema
sqlite3	Query dirette, conversione delle date, timeline unificata	Su una copia, in sola lettura, con i file di journal
ExifTool	Coordinate e orari nei metadati delle fotografie	L'ora è locale; il fuso va ricavato altrove
sha256sum, tar, ots	Hash, archivio e marca temporale del fascicolo	La marca OpenTimestamps non è qualificata ai sensi di eIDAS

Tutti questi strumenti presuppongono un dispositivo sbloccato o un'estrazione già fatta. Per quello bloccato valgono le vie lecite già viste.

Fonti: documentazione dei progetti (Android SDK Platform-Tools, libimobiledevice, ALEAPP, iLEAPP, SQLite, ExifTool, OpenTimestamps).

Validazione e limiti dell’inferenza

Versioni

Tabelle e formati cambiano a ogni versione del sistema. Si annotano versione del dispositivo, dello strumento e, per i progetti su Git, il commit usato.

Doppio riscontro

Ogni risultato rilevante si ottiene due volte: parser e query manuale, registro del telefono e tabulato, posizione del dispositivo e cella dell’operatore.

Anche gli strumenti semplici sbagliano

Nel preparare il laboratorio, una funzione di formattazione di sqlite3 ha restituito 3 per il valore 3,6: troncava invece di arrotondare. La colonna delle velocità è stata rifatta con un decimale.

Dispositivo e persona

Gli artefatti dicono che cosa ha fatto il telefono e dove si trovava. Che fosse nelle mani del suo titolare è un’inferenza, da sostenere con altri elementi.

In relazione si distingue ciò che il dato mostra da ciò che se ne deduce, e per la seconda parte si dichiara su che cosa poggia.

Fonti: NIST, Computer Forensics Tool Testing Program; SWGDE 20-F-005-1.0; osservazione diretta su sqlite3 nella preparazione del corso.

PARTE 4 · 70 MINUTI

Laboratorio guidato

Dalle date grezze alla timeline unificata, fino al controllo delle posizioni. Le schermate provengono da database sintetici costruiti per il corso.

Scenario e regole del laboratorio

Scenario

Il titolare di un telefono Android dichiara di essere rimasto in ufficio dalle 9 alle 12 del 27 novembre 2026. Ha consegnato il dispositivo sbloccato, con consenso scritto all'esame di chiamate, SMS e posizioni di quella mattina.

Quesito. Ricostruire la mattinata e dire se i dati sono compatibili con la dichiarazione.

Cartella di lavoro: caso04. Contiene il registro delle chiamate, il database degli SMS, una tabella di posizioni e, per l'esercizio sulle date, un registro chiamate in formato iOS.

Regole

I database sono sintetici: schema ridotto alle colonne che servono, numeri e coordinate di fantasia.

Si lavora su copie, in sola lettura. Gli originali si toccano una volta, per calcolarne l'hash.

Ogni comando finisce a verbale con data e ora in UTC, compresi quelli sbagliati.

Sette passi, dieci minuti ciascuno. A ogni passo corrisponde una riga del verbale.

Passo 1: la postazione

INSTALLAZIONE SU UBUNTU 24.04

```
$ sudo apt install adb libimobiledevice-utils sqlite3 libimage-exiftool-perl
$ git clone https://github.com/abrignoni/ALEAPP
$ git clone https://github.com/abrignoni/iLEAPP
```

VERSIONI, DA RIPORTARE A VERBALE

```
$ adb version ; sqlite3 --version ; exiftool -ver
# Android Debug Bridge 1.0.41 · SQLite 3.45.1 · ExifTool 12.76
$ git -C ALEAPP log -1 --format=%H%n%cI
```

Una postazione dedicata. Nessun account personale, nessuna sincronizzazione automatica, orologio allineato a una fonte certa prima di cominciare.

La versione è un dato. Uno stesso database letto con due versioni dello stesso strumento può dare conteggi diversi. A verbale va quella effettivamente usata.

Installazione eseguita il 28 novembre 2026 su Ubuntu 24.04 nella preparazione del corso.

Passo 2: stato, identità e orologio del dispositivo

ANDROID SBLOCCATO, CON DEBUG USB AUTORIZZATO

```
$ adb devices -l
$ adb shell getprop ro.product.model ; adb shell getprop ro.build.version.release
$ adb shell getprop persist.sys.timezone
$ adb shell date -u ; date -u
```

IPHONE ABBINATO ALLA POSTAZIONE

```
$ ideviceinfo -k ProductType ; ideviceinfo -k ProductVersion
```

Stato

Sbloccato, AFU o BFU, con l'ora in cui lo si è osservato e chi lo ha sbloccato.

Orologio

Le due date in UTC, lette una dopo l'altra, misurano lo scarto. Accompagna ogni orario della relazione.

Fuso

Serve per tradurre la timeline nell'ora che il titolare vedeva sullo schermo, e per leggere le foto.

Sintassi verificata sull'help di adb e di libimobiledevice. L'esecuzione richiede un dispositivo collegato.

Passo 3: acquisizione logica da Android sbloccato

```
SENZA ROOT, ATTRAVERSO LE INTERFACCE DEL SISTEMA
$ adb shell content query --uri content://call_log/calls > chiamate.txt
$ adb shell content query --uri content://sms > sms.txt
$ adb shell dumpsys usagestats > usagestats.txt
$ adb bugreport bugreport.zip
$ sha256sum chiamate.txt sms.txt usagestats.txt bugreport.zip | tee acquisizione.sha256
```

Che cosa si ottiene

Il contenuto del registro chiamate e degli SMS come lo espone il sistema, le statistiche d’uso delle app e un rapporto diagnostico con molti registri di servizio.

Che cosa resta fuori

I file dei database, con le righe eliminate e i journal: stanno sotto /data e richiedono root o un’estrazione completa. Alcuni sistemi limitano anche le interrogazioni.

È un’acquisizione di ciò che il telefono accetta di dire. Va descritta così, con i comandi usati e la loro uscita integrale.

Sintassi tratta dalla documentazione di adb. Comandi non eseguiti nella preparazione del corso: richiedono un dispositivo di prova.

Variante iPhone: backup cifrato e parsing

IPHONE SBLOCCATO E ABBINATO

```
$ idevicebackup2 encryption on PasswordDiProva
$ idevicebackup2 backup --full ios-backup/
$ sha256sum ios-backup/*/Manifest.db
$ python3 iLEAPP/ileapp.py -t itunes -i ios-backup/<UDID> -o report-ios/ --itunes_password PasswordDiProva
```

Perché cifrato

Il backup protetto da password comprende categorie che quello in chiaro esclude, fra cui il registro delle chiamate.

Che cosa contiene

Chiamate e sms.db sì. Il registro delle attività e la cache delle posizioni no: stanno fuori dal perimetro del backup.

Attenzione

Impostare la password modifica il dispositivo. Se una password esiste già e non è nota, il backup non si apre.

Sintassi verificata sull’help di idevicebackup2 e sul README di iLEAPP. L’esecuzione richiede un iPhone di prova.

Passo 4: leggere le date nel modo giusto

```
studente@vm:~/caso04$ sqlite3 -header -column android/calllog.db "SELECT date, datetime(date/1000,'unixepoch') AS utc, duration,
 type FROM calls"
date           utc                  duration  type
-------------  -------------------  --------  ----
1795767160137  2026-11-27 08:12:40  95        2
1795770185274  2026-11-27 09:03:05  0         3
1795772478411  2026-11-27 09:41:18  312       1
1795775270548  2026-11-27 10:27:50  48        2
1795778102685  2026-11-27 11:15:02  0         5
studente@vm:~/caso04$ sqlite3 -header -column ios/CallHistory.storedata "SELECT ZDATE, datetime(ZDATE,'unixepoch') AS errata, da
tetime(ZDATE+978307200,'unixepoch') AS corretta FROM ZCALLRECORD"
ZDATE         errata               corretta
------------  -------------------  -------------------
817459961.25  1995-11-27 08:12:41  2026-11-27 08:12:41
817468071.5   1995-11-27 10:27:51  2026-11-27 10:27:51
studente@vm:~/caso04$
```

Android. La colonna date è in millisecondi dall’epoca Unix: si divide per mille e si converte. Le cinque chiamate cadono fra le 08:12 e le 11:15 UTC.

iOS. La stessa conversione, applicata a ZDATE, colloca le chiamate nel 1995. Aggiungendo i 978.307.200 secondi che separano le due epoche si torna al 27 novembre 2026.

Schermata originale, prodotta il 28 novembre 2026 su database sintetici con schema ridotto.

Passo 5: la timeline unificata

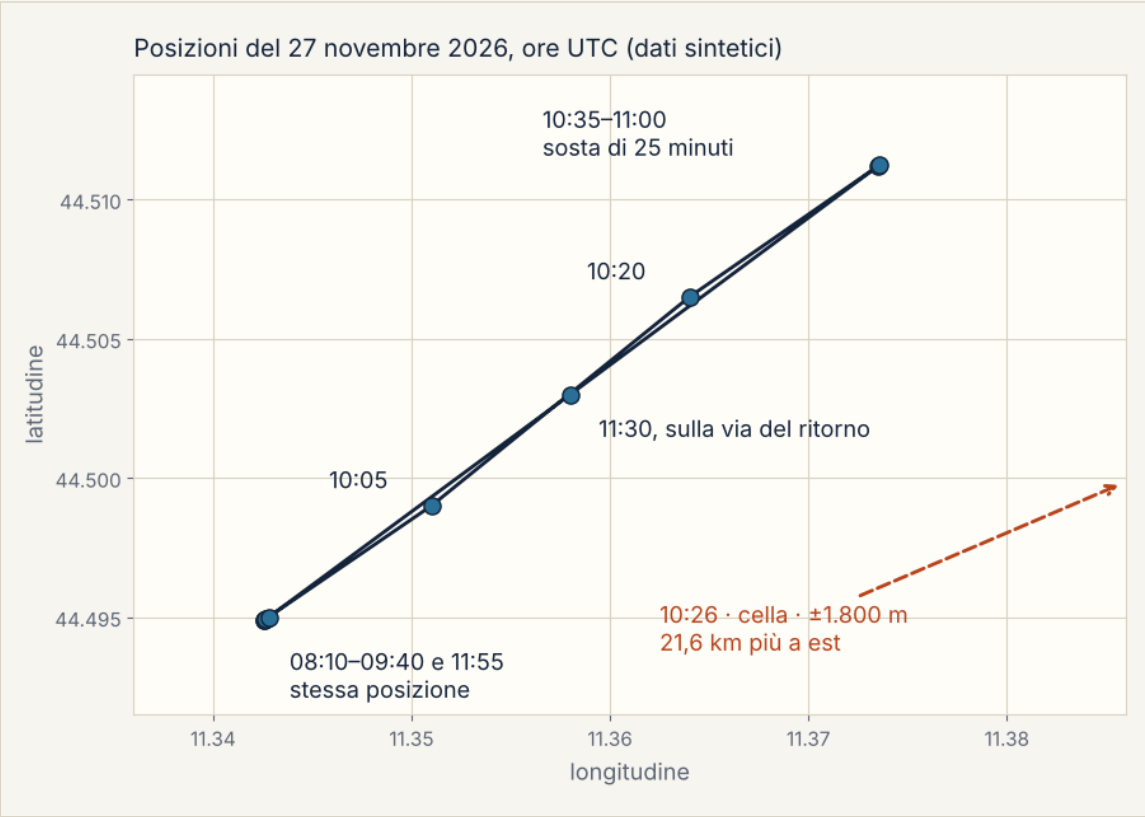
```
studente@vm:~/caso04$ sqlite3 -header -column :memory: < timeline.sql
utc                  fonte      dettaglio
-------------------  ---------  ----------------------------------------------------
2026-11-27 08:10:00  posizione  44.49490, 11.34260  +/- 12 m  (gps)
2026-11-27 08:12:40  chiamata   effettuata 390000000011 (95 s)
2026-11-27 08:40:00  posizione  44.49495, 11.34270  +/- 15 m  (gps)
2026-11-27 09:03:05  chiamata   persa 390000000022 (0 s)
2026-11-27 09:05:30  sms        ricevuto da 390000000022: Ti ho chiamato, richiamami
2026-11-27 09:06:10  sms        inviato a 390000000022: Sono in riunione, a dopo
2026-11-27 09:10:00  posizione  44.49488, 11.34255  +/- 18 m  (wifi)
2026-11-27 09:40:00  posizione  44.49492, 11.34262  +/- 14 m  (gps)
2026-11-27 09:41:18  chiamata   ricevuta 390000000022 (312 s)
2026-11-27 10:05:00  posizione  44.49900, 11.35100  +/- 10 m  (gps)
2026-11-27 10:20:00  posizione  44.50650, 11.36400  +/- 9 m  (gps)
2026-11-27 10:26:00  posizione  44.57300, 11.62000  +/- 1800 m  (cella)
2026-11-27 10:27:50  chiamata   effettuata 390000000011 (48 s)
2026-11-27 10:31:00  sms        inviato a 390000000011: Arrivo fra dieci minuti
2026-11-27 10:33:44  sms        ricevuto da 390000000011: Ti aspetto al solito posto
2026-11-27 10:35:00  posizione  44.51120, 11.37350  +/- 8 m  (gps)
2026-11-27 11:00:00  posizione  44.51125, 11.37360  +/- 11 m  (gps)
2026-11-27 11:15:02  chiamata   rifiutata 390000000022 (0 s)
2026-11-27 11:30:00  posizione  44.50300, 11.35800  +/- 13 m  (gps)
2026-11-27 11:55:00  posizione  44.49500, 11.34280  +/- 12 m  (gps)
studente@vm:~/caso04$
```

La query. Collega i tre database, riporta ogni fonte a UTC e le unisce in un solo elenco ordinato. Sta in un file, timeline.sql, che si allega alla relazione.

La lettura. Alle 10:27 una chiamata, alle 10:31 «Arrivo fra dieci minuti», alle 10:35 una posizione nuova, a oltre due chilometri dalla prima.

Schermata originale del 28 novembre 2026 su database sintetici. Numeri, testi e coordinate sono di fantasia.

Passo 6: le posizioni su una mappa



Che cosa mostra la traccia

- Dalle 08:10 alle 09:40 il telefono è fermo nello stesso punto.
- Fra le 10:05 e le 10:35 si sposta di oltre due chilometri verso nord-est.
- Resta fermo 25 minuti, poi rientra e alle 11:55 è di nuovo al punto di partenza.
- Un rilevamento delle 10:26 cade a più di venti chilometri: proviene da una cella, con un margine di 1.800 metri.

Rispetto alla dichiarazione. I dati non sono compatibili con una permanenza in ufficio dalle 9 alle 12: per circa due ore il telefono è stato altrove.

Figura originale, generata dai dati sintetici del laboratorio. Le coordinate non corrispondono a luoghi reali del caso.

Passo 7: il controllo di plausibilità

```
studente@vm:~/caso04$ sqlite3 -header -column posizioni.db < velocita.sql
utc       km     minuti  km_h   acc_m
--------  -----  ------  -----  ------
08:40:00  0.01   30      0.0    15.0
09:10:00  0.01   30      0.0    18.0
09:40:00  0.01   30      0.0    14.0
10:05:00  0.80   25      1.9    10.0
10:20:00  1.33   15      5.3    9.0
10:26:00  21.59  6       215.9  1800.0
10:35:00  20.71  9       138.1  8.0
11:00:00  0.01   25      0.0    11.0
11:30:00  1.54   30      3.1    13.0
11:55:00  1.50   25      3.6    12.0
studente@vm:~/caso04$ sha256sum android/*.db ios/* posizioni.db
e715552acd9cbf01d77b552dd2160e83aa3c44079e6adbf55a1fa5be7f805aac  android/calllog.db
8cfabef831fdb0731f587e8cdf1a519ea1b411b72603d1fcf741801a6b75b7f9  android/mmssms.db
3cda1c9f6757f956114e42d3f3b374819527ef35c3a39a2b62ab69c60ef7dacc  ios/CallHistory.storedata
a84d6a3a1aa956fb2b15a76eec37a280d433ec172f2e6f68c1c29766d3237bd4  posizioni.db
studente@vm:~/caso04$
```

Il calcolo. Distanza sulla sfera fra punti consecutivi, divisa per il tempo trascorso. Spostamenti a piedi fra 2 e 5 km/h, poi due valori fuori scala: 215,9 e 138,1 km/h.

La spiegazione. Il punto delle 10:26 viene da una cella e dichiara un margine di 1.800 metri. Si conserva nel fascicolo, si esclude dalla ricostruzione del percorso e si scrive perché.

Un rilevamento anomalo non si cancella: si motiva. Chi lo trova da solo, dopo, penserà che sia stato nascosto.

Schermata originale del 28 novembre 2026 su dati sintetici. In fondo, gli hash dei database esaminati.

Chiusura: riscontri esterni e sigillo

Che cosa resta da riscontrare

Dato del telefono	Riscontro esterno
Chiamate delle 09:41 e delle 10:27	Tabulato dell’operatore: utenze, ora, durata
Posizioni fra le 10:05 e le 11:30	Celle agganciate nello stesso intervallo
SMS delle 10:31 e delle 10:33	Telefono dell’interlocutore
Uso attivo del dispositivo	Registri di sblocco e di app in primo piano

SIGILLO

```
$ find caso04 -type f -exec sha256sum {} + \
    | tee caso04.sha256
$ tar -cf caso04.tar caso04 caso04.sha256
$ sha256sum caso04.tar
$ ots stamp caso04.tar
```

Nel fascicolo entrano anche timeline.sql e velocita.sql: chi riesamina deve poter rieseguire le stesse query sugli stessi file.

Fonti: Reg. (UE) n. 910/2014, artt. 41 e 42; documentazione di OpenTimestamps. La marca OpenTimestamps non è una marca temporale qualificata.

Errori ricorrenti

Errore	Conseguenza
Lasciare che un telefono sbloccato si blocchi	Si perde la condizione più favorevole, senza rimedio
Spegnere un dispositivo acceso e bloccato	Da AFU a BFU: le chiavi in memoria non tornano
Tenere il telefono in deposito per giorni prima dell'esame	Riavvio per inattività dopo 72 ore; tracce di attività che scadono
Provare codici «per tentativi»	Ritardi crescenti, possibile cancellazione dei dati
Leggere le date senza verificare epoca e unità	Eventi spostati di decenni, o di un'ora per il fuso
Trattare una posizione da cella come un punto GPS	Conclusioni sul luogo che il dato non sostiene
Fermarsi al registro del telefono	Si rinuncia al riscontro sul tabulato, che dura due anni
Attribuire alla persona ciò che ha fatto il dispositivo	Inferenza presentata come accertamento

I primi quattro si commettono sul luogo del sequestro; gli altri quattro alla scrivania. Nessuno richiede uno strumento per essere evitato.

Limiti legali ed etici

Tre atti, tre titoli

Il sequestro del dispositivo, l'esame del suo contenuto e l'acquisizione dei tabulati hanno presupposti diversi. Il titolo per uno non copre gli altri.

Il consenso

In sede privata serve il consenso scritto e informato del titolare, con l'indicazione di che cosa si esamina. In sede penale, per chi è indagato, non sostituisce il provvedimento.

I terzi

Chiamate e messaggi riguardano sempre almeno un'altra persona. Si estrae e si espone ciò che serve al quesito, per il periodo indicato dal titolo.

I reati dietro l'angolo

Esaminare il telefono altrui senza titolo può integrare l'accesso abusivo a sistema informatico (art. 615-ter c.p.) e la violazione di corrispondenza (art. 616 c.p.), anche in ambito familiare.

Su dati altrui serve un titolo, e la sua valutazione spetta a un legale.

Riferimenti: artt. 15 Cost., 615-ter e 616 c.p., 247, 254 e 360 c.p.p.; art. 132 d.lgs. 196/2003; CGUE, C-548/21. Indicazioni didattiche, non pareri legali.

PARTE 5 · 35 MINUTI

Caso di studio e verifica

Un fascicolo da esaminare in gruppo, otto domande a risposta chiusa, la sintesi e le fonti.

Caso di studio: due telefoni, un incidente

Scenario di fantasia

Un incidente stradale notturno. Il conducente sostiene che non stava usando il telefono. Il suo iPhone viene sequestrato acceso e bloccato; quello del passeggero, un Android, è consegnato sbloccato con consenso scritto.

Incarico. Come consulenti del pubblico ministero, valutare ciò che è agli atti e indicare che cosa manca.

Che cosa c'è nel fascicolo

N.	Reperto
1	iPhone del conducente, giunto in laboratorio dopo cinque giorni: è in BFU
2	Android del passeggero: chiamate e SMS estratti con adb
3	Tabulati delle due utenze, acquisiti con decreto del pubblico ministero
4	Fotografia dello schermo di «Benessere digitale» sul telefono del passeggero
5	Richiesta ad Apple del backup iCloud, senza risposta

Nessun verbale riporta lo stato dell'iPhone al momento del sequestro, né l'ora dell'ultimo blocco.

Caso di studio: il lavoro in gruppo

1

Che cosa si è perso sull'iPhone fra il sequestro e l'arrivo in laboratorio, e quale annotazione avrebbe permesso di accorgersene in tempo?

2

Quale delle quattro famiglie di evidenze risponderebbe al quesito «stava usando il telefono», e da quali fonti la si può ancora ottenere?

3

Il reperto 3 è utilizzabile così com'è? Che cosa va verificato sul titolo con cui è stato acquisito?

4

Che cosa può dire il telefono del passeggero sul comportamento del conducente, e con quali cautele va riferito?

Venti minuti in gruppi di tre, poi tre minuti di restituzione per gruppo. La risposta attesa è una tabella, non un racconto.

Quiz di verifica: domande 1–4

1. Un iPhone con iOS 18.1, acceso e bloccato da più di 72 ore

A. resta nello stato AFU
B. si riavvia da solo e passa in BFU
C. cancella i dati dell'utente

2. Un dispositivo è in BFU quando

A. dopo l'accensione il codice non è mai stato inserito
B. lo schermo è spento da più di un'ora
C. è collegato a un computer non abbinato

3. In Italia, dal 2021, i tabulati si acquisiscono

A. con decreto del pubblico ministero
B. su richiesta della polizia giudiziaria all'operatore
C. con decreto motivato del giudice, su richiesta del pubblico ministero

4. Il termine ordinario di conservazione del traffico telefonico è di

A. 12 mesi
B. 24 mesi
C. 6 mesi

Quiz di verifica: domande 5–8

5. Il valore 817459961 nel campo ZDATE di un registro iOS esprime

A. secondi dal 1° gennaio 1970
B. millisecondi dal 1° gennaio 1970
C. secondi dal 1° gennaio 2001

6. Una posizione ricavata da una cella, con margine di 1.800 metri

A. si conserva, e si motiva la sua esclusione dal percorso
B. si elimina dal fascicolo
C. vale quanto un rilevamento GPS

7. Il registro delle attività, con sblocchi e app in primo piano, dimostra

A. chi stava usando il telefono
B. che il dispositivo era in uso in quel momento
C. il contenuto dei messaggi scambiati

8. Dal 2024 la cronologia delle posizioni di Google Maps

A. è conservata sui server di Google per diciotto mesi
B. non viene più registrata
C. risiede sul dispositivo dell’utente

Quiz di verifica: soluzioni

N.	Risposta	Perché
1	B	Il riavvio per inattività riporta il dispositivo allo stato precedente al primo sblocco
2	A	Le chiavi che dipendono dal codice non sono ancora state ricavate
3	C	È la riforma del d.l. 132/2021; il pubblico ministero provvede da solo nei casi di urgenza
4	B	Dodici mesi per il traffico telematico, fino a 72 per i reati più gravi
5	C	Letto come Unix cadrebbe nel 1995; con 978.307.200 secondi in più è il 2026
6	A	Il dato resta nel fascicolo, la relazione spiega perché non entra nella ricostruzione
7	B	L’identità di chi lo usava è un’inferenza che richiede altri elementi
8	C	Google non la conserva più sui propri server: la prova è tornata nel telefono

Sei risposte esatte su otto sono la soglia per ritenere acquisiti i contenuti della giornata.

IN SINTESI

Lo stato del dispositivo decide che cosa si ottiene; il tempo decide per quanto ancora; il titolo decide se lo si può usare

Sul posto

Annotare stato e ora. Non far bloccare ciò che è aperto, non spegnere ciò che è acceso, non accendere ciò che è spento. Isolare e alimentare.

In laboratorio

Estrarre entro le 72 ore. Convertire ogni data dalla sua epoca a UTC. Unire chiamate, messaggi, attività e posizioni in una sola timeline.

In relazione

Riscontrare il telefono con il tabulato. Dichiarare fonte e margine di ogni posizione. Tenere distinto il dispositivo dalla persona.

Un telefono bloccato riduce le fonti senza azzerarle: operatore, backup e altri dispositivi restano. Un telefono lasciato scadere le azzera da solo.

Fonti: norme, giurisprudenza e standard

Norme e giurisprudenza

- Costituzione, art. 15; c.p.p., artt. 247, 254, 354 e 360; c.p., artt. 615-ter e 616
- L. 18 marzo 2008, n. 48
- D.lgs. 30 giugno 2003, n. 196, art. 132, come modificato dal d.l. 132/2021, conv. in L. 178/2021; L. 167/2017, art. 24
- Corte cost., sent. 27 luglio 2023, n. 170
- Cass. pen., sez. VI, n. 1269/2025
- Senato, A.S. 806, e Camera, A.C. 1822, XIX legislatura: art. 254-ter c.p.p.
- CGUE, 2 marzo 2021, C-746/18; CGUE, Grande Sezione, 4 ottobre 2024, C-548/21
- Reg. (UE) 2023/1543; Reg. (UE) n. 910/2014, artt. 41 e 42
- Riley v. California, 573 U.S. 373 (2014); Carpenter v. United States, 585 U.S. 296 (2018)
- Hoge Raad, 9 febbraio 2021, sullo sblocco con impronta digitale

Standard e linee guida

- Ayers R., Brothers S., Jansen W., Guidelines on Mobile Device Forensics, NIST SP 800-101 Rev. 1, 2014
- SWGDE, Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition, 18-F-003-2.0, 2025
- SWGDE, Best Practices for Mobile Device Forensic Analysis, 20-F-005-1.0, 2020
- ISO/IEC 27037:2012
- NIST, Computer Forensics Tool Testing Program

I riferimenti giurisprudenziali vanno riscontrati sulle banche dati ufficiali prima di essere citati in un atto.

Fonti: letteratura, documentazione e strumenti

Letteratura scientifica e tecnica

- Chernyshev M., Zeadally S., Baig Z., Woodward A., Mobile Forensics: Advances, Challenges, and Research Opportunities, IEEE Security & Privacy 15(6), 2017
- Barmpatsalou K., Cruz T., Monteiro E., Simoes P., Current and Future Trends in Mobile Device Forensics: A Survey, ACM Computing Surveys 51(3), 2018
- Cotti G., Accesso ai dispositivi elettronici e principio nemo tenetur se detegere, Archivio Penale 2/2025
- Edwards S., Knowledge is Power! Using the macOS/iOS knowledgeC.db Database to Determine Precise User and Application Usage, 2018
- Classen J., Reverse Engineering iOS 18 Inactivity Reboot, novembre 2024
- Magnet Forensics, Understanding the security impacts of iOS 18’s inactivity reboot, 2024

Documentazione dei produttori

- Apple, Apple Platform Security
- Android Open Source Project, File-Based Encryption
- Google, annunci sulla cronologia delle posizioni di Maps, 2023–2024

Strumenti

- ALEAPP e iLEAPP, github.com/abrignoni
- Android SDK Platform-Tools; libimobiledevice
- SQLite; ExifTool; OpenTimestamps

Autori, volumi e pagine vanno riscontrati sulle pagine degli editori prima della citazione.

CORSO AVANZATO DI DIGITAL FORENSICS

Grazie per l'attenzione

Vincenzo Calabrò

www.vincenzocalabro.it



Inquadra per aprire il sito