CORSO AVANZATO DI DIGITAL FORENSICS

Acquisizione forense di messaggi da app di messaggistica

WhatsApp, Telegram, Signal, Messenger e Instagram: dispositivo, client e cloud, provider

Relatore: Vincenzo Calabrò

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

Programma e obiettivi della mezza giornata

Parte	Contenuto	Durata
1	Dove stanno i messaggi e che cosa va dimostrato	30 min
2	Quadro normativo e standard	40 min
	Pausa	15 min
3	Metodo: dispositivo, client e cloud, provider	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 dispositivi e account di prova, mai su dati reali.

Al termine lo studente è in grado di

- indicare, per ciascuna app, dove risiede il messaggio e chi può consegnarlo;
- scegliere fra dispositivo, client collegati e provider in base a ciò che va dimostrato e al titolo giuridico disponibile;
- acquisire e leggere i database delle app con strumenti open source, documentando ogni passaggio;
- esaminare un’acquisizione altrui e riconoscerne i punti contestabili.

PARTE 1 · 30 MINUTI

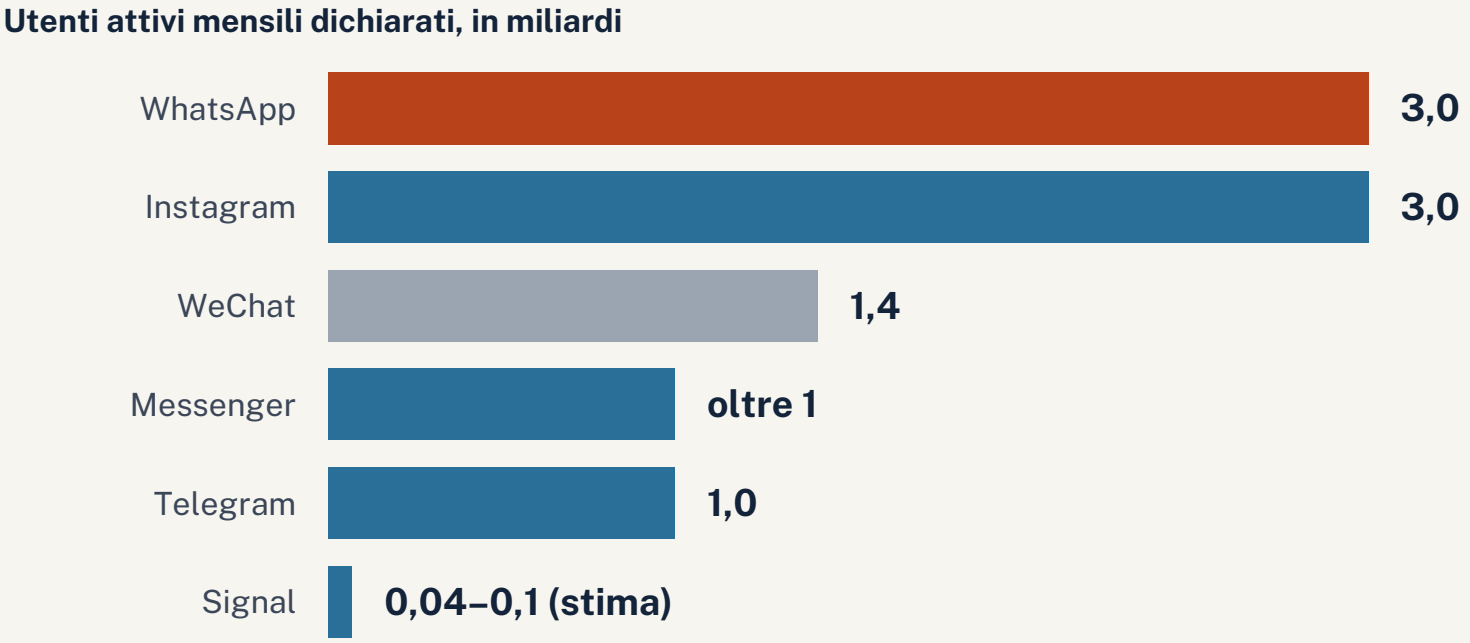
Dove stanno i messaggi

Un messaggio esiste in più copie, su sistemi diversi e con protezioni diverse. Prima di acquisire occorre sapere quale copia si sta cercando.

Le app di messaggistica in numeri

3 mld

di utenti attivi ogni mese dichiarati da WhatsApp nel 2025.



Conseguenza operativa. In quasi ogni fascicolo compare almeno una di queste app. Le prime due appartengono allo stesso gruppo, ma oggi proteggono i messaggi in modo opposto.

Fonti: comunicazioni di Meta, Tencent e Telegram (2025). Per Instagram il dato riguarda l'intera piattaforma. Signal non pubblica dati: stime di terzi. WeChat è riportata per confronto.

Le copie di uno stesso messaggio



Altre copie, spesso dimenticate

Backup cloud
Google Drive, iCloud o archivio del fornitore, con chiavi e regole proprie

Dispositivi collegati
Client web e desktop che ricevono una copia della conversazione

Export dell'utente
File prodotti dall'app su richiesta, fuori dal suo controllo una volta salvati

Le copie non coincidono: un messaggio cancellato su un telefono può sopravvivere sull'altro, in un backup della sera prima o su un computer collegato.

Cifratura e backup: lo stato a novembre 2026

App	Protezione dei messaggi	Il provider può leggerli	Backup
WhatsApp	End-to-end di default dal 2016, con il protocollo Signal	No	Google Drive o iCloud; la cifratura end-to-end del backup è facoltativa
Signal	End-to-end di default	No	Secure Backups facoltativi dal 2025, con chiave di recupero di 64 caratteri
Telegram	Chat cloud cifrate fra client e server; end-to-end soltanto nelle chat segrete	Sì, per le chat cloud	La cronologia cloud risiede già sui server
Messenger	End-to-end di default dal dicembre 2023	No, per le chat end-to-end	Archiviazione protetta sui server Meta, sbloccata da un PIN
Instagram	Opzione end-to-end ritirata dopo l’8 maggio 2026	Sì	Messaggi conservati sui server Meta

La colonna centrale decide la strategia: dove il provider non legge, il contenuto si ottiene soltanto da un dispositivo o da un backup di cui si possiede la chiave.

Fonti: documentazione tecnica dei fornitori; Signal, Introducing Signal Secure Backups, 8 settembre 2025; annunci Meta del 2023 e del 2026. Da riverificare a ogni incarico.

La volatilità dei messaggi

Messaggi effimeri

Su WhatsApp la scadenza è a 24 ore, 7 giorni o 90 giorni; Signal e Telegram offrono timer analoghi. Il conteggio avviene sul dispositivo e prosegue anche senza rete.

Modifica e cancellazione

Il mittente può correggere o eliminare un messaggio già consegnato. Nel database resta talvolta la traccia dell'operazione, non sempre il testo originario.

Visualizzazione singola

Foto, video e messaggi vocali che si aprono una volta sola: dopo l'apertura il contenuto è rimosso dal dispositivo di chi lo ha ricevuto.

Che cosa dice la ricerca. Heath, MacDermott e Akinbi (2023) hanno cercato i messaggi effimeri di WhatsApp, Snapchat e Telegram su telefono, desktop e cloud. Uno studio del 2024 su Android privo di root riferisce recuperi parziali dai log delle notifiche.

Il tempo utile si misura in ore. Preservare il dispositivo viene prima di qualunque analisi.

Fonti: Forensic Science International: Digital Investigation 46 (2023), 301585; Evergreen 11(1), 2024, pp. 516–524.

Che cosa occorre poter dimostrare

Contenuto

Il testo, gli allegati, le risposte e le reazioni come risultano nel database, compresi i messaggi modificati o eliminati di cui resti traccia.

Attribuzione

La catena account, numero, dispositivo, persona. I primi tre anelli sono tecnici; l'ultimo richiede elementi esterni alla chat.

Tempo

L'ora di invio e di ricezione, espressa in UTC, con lo scarto fra l'orologio del dispositivo e un riferimento certo.

Integrità e completezza

La corrispondenza fra ciò che si produce e ciò che si è acquisito, e la conversazione intera invece di una selezione di parte.

Uno screenshot risponde, e male, soltanto alla prima domanda. Le altre tre richiedono il dato da cui lo screenshot è stato generato.

Le vie di acquisizione a confronto

	Contenuto	Messaggi cancellati	Dati di account e accesso	Senza l’interessato	Riesame di terzi
Estrazione dal dispositivo	**Sì**	In parte	In parte	In parte	**Sì**
Export e client collegati	**Sì**	No	No	No	In parte
Backup locale o cloud	In parte	In parte	No	In parte	**Sì**
Richiesta al provider	In parte	No	**Sì**	**Sì**	In parte

«In parte» dipende dall’app, dalla chiave disponibile e dal livello di estrazione. Per il provider il contenuto esiste solo dove i messaggi non sono cifrati end-to-end.

Nessuna via copre tutte le colonne. Un’acquisizione solida ne combina almeno due e ne confronta i risultati.

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

PARTE 2 · 40 MINUTI

Quadro normativo e standard

Dal 2023 la giurisprudenza ha cambiato la qualificazione giuridica dei messaggi. La tecnica segue: il titolo con cui si acquisisce conta quanto lo strumento.

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; primo studio forense su WhatsApp

2016
WhatsApp cifra end-to-end di default; dir. (UE) 2016/680

2018
CLOUD Act negli Stati Uniti

2020
EncroChat: le chat cifrate entrano nei processi

2021
WhatsApp: backup cifrati end-to-end, facoltativi

2023
Corte cost. n. 170: i messaggi sono corrispondenza; Messenger end-to-end

2024
Cass. SU 23755 e 23756; CGUE C-548/21; nuova policy di Telegram

2025
SWGDE 18-F-003 v2.0; Signal Secure Backups

2026
e-Evidence applicabile dal 18 agosto; Instagram ritira l’opzione end-to-end

Nella seconda riga le novità arrivano ogni anno: una prassi appresa nel 2022 oggi va ricontrollata punto per punto.

Italia: da documento a corrispondenza

Fino al 2023

Per l'orientamento allora prevalente in Cassazione i messaggi già ricevuti e conservati nella memoria del telefono erano documenti, acquisibili a norma dell'art. 234 c.p.p.

Per tutte: Cass. pen., sez. V, n. 1822/2018.

Corte cost. n. 170/2023

E-mail e messaggi WhatsApp restano corrispondenza, tutelata dall'art. 15 Cost., anche dopo la ricezione e la lettura, finché conservano attualità per chi li ha scambiati.

La disciplina di riferimento diventa il sequestro di corrispondenza dell'art. 254 c.p.p.

Ricadute per chi acquisisce

- Occorre un provvedimento motivato dell'autorità giudiziaria; la polizia giudiziaria consegna il materiale senza prenderne conoscenza (art. 254, comma 2).
- Il verbale deve indicare il titolo in forza del quale si è avuto accesso alle chat, non soltanto la procedura tecnica.
- Cass. pen., sez. VI, n. 1269/2025 è tornata sui limiti dell'acquisizione: la motivazione va letta per esteso prima di citarla.

Fonti: Corte cost., sent. 27 luglio 2023, n. 170; Cass. pen., sez. V, n. 1822/2018; sez. VI, n. 1269/2025. Riferimenti da riscontrare sulle banche dati ufficiali.

Italia: gli strumenti del codice e la riforma in discussione

Art. c.p.p.	Che cosa consente	Rilievo per le chat
247, co. 1-bis	Perquisizione di sistemi informatici con misure che conservino i dati originali	Accesso al telefono e ai client collegati
254	Sequestro di corrispondenza	Messaggi, dopo Corte cost. n. 170/2023
254-bis	Sequestro di dati presso i fornitori di servizi	Richieste al provider, con copia e obbligo di conservazione
354, co. 2	Accertamenti urgenti della polizia giudiziaria	Preservazione e duplicazione immediata
360	Accertamenti tecnici non ripetibili	Estrazioni che modificano lo stato del dispositivo

In discussione: art. 254-ter

Il disegno di legge S. 806, approvato dal Senato il 10 aprile 2024 e passato alla Camera come C. 1822, affida al giudice, su richiesta del pubblico ministero, il sequestro di dispositivi e sistemi informatici e regola duplicazione e selezione dei contenuti. Ad agosto 2025 l'iter non era concluso: lo stato attuale va verificato.

Fonti: codice di procedura penale come modificato dalla L. 48/2008; Senato, A.S. 806; Camera, A.C. 1822 e relativo dossier.

Chat cifrate acquisite all’estero: le decisioni del 2024

Cass. SU n. 23755/2024

I messaggi Sky ECC già decifrati e detenuti dall’autorità straniera entrano come atti di un altro procedimento. Può chiederli il pubblico ministero con ordine europeo di indagine, senza autorizzazione preventiva del giudice.

Cass. SU n. 23756/2024

Se il materiale proviene da intercettazioni svolte all’estero, l’utilizzo segue la disciplina dell’art. 270 c.p.p. sui risultati di intercettazioni disposte in altri procedimenti.

CGUE, C-670/22

Sul caso EncroChat la Corte ammette l’ordine emesso dal pubblico ministero, ma impone al giudice di scartare la prova sulla quale la difesa non sia in grado di prendere posizione in modo efficace.

Che cosa cambia per il consulente

- La difesa riceve dati già decifrati, di regola senza i dati grezzi e senza la descrizione del procedimento di decifratura.
- La verifica tecnica possibile riguarda integrità, completezza e coerenza interna di ciò che è stato consegnato: hash, formati, metadati, continuità delle conversazioni.

Fonti: Cass. pen., Sez. Un., 29 febbraio 2024 (dep. 14 giugno 2024), nn. 23755 e 23756; CGUE, Grande Sezione, 30 aprile 2024, C-670/22.

Unione europea: accesso al telefono e richieste ai fornitori

CGUE, C-548/21

L’accesso della polizia ai dati di un telefono non è riservato ai reati gravi. Richiede però, salvo urgenza, l’autorizzazione preventiva di un giudice o di un’autorità indipendente, il rispetto della proporzionalità e l’informazione dell’interessato.

Grande Sezione, 4 ottobre 2024, sulla dir. (UE) 2016/680.

Reg. (UE) 2023/1543

Dal 18 agosto 2026 l’autorità di uno Stato membro rivolge l’ordine di produzione direttamente al fornitore che offre servizi nell’Unione: risposta entro 10 giorni, 8 ore in caso di emergenza.

L’ordine di conservazione blocca i dati per 60 giorni.

Dir. 2014/41/UE

L’ordine europeo di indagine resta lo strumento per ottenere prove già in possesso di un’altra autorità giudiziaria, come nei procedimenti nati da EncroChat e Sky ECC.

Il canale diretto verso i fornitori è operativo da pochi mesi. La prassi applicativa, anche verso Meta e Telegram, è ancora in formazione.

Fonti: CGUE, C-548/21, ECLI:EU:C:2024:830; Reg. (UE) 2023/1543 e dir. (UE) 2023/1544; dir. 2014/41/UE.

Oltre l’Unione: trattati e diritto statunitense

Trattati

- **Convenzione di Budapest** (2001): conservazione rapida dei dati (artt. 16 e 17), ordine di produzione (art. 18), assistenza fra Stati (artt. 29–31).
- **Convenzione ONU contro la criminalità informatica**: adottata il 24 dicembre 2024, aperta alla firma ad Hanoi il 25 ottobre 2025.
- **Rogatoria**: resta la via per i contenuti detenuti da fornitori statunitensi quando manca un canale diretto.

Stored Communications Act: a ogni titolo un perimetro

Titolo	Che cosa ottiene
Subpoena	Dati di base dell’abbonato
Ordine ex § 2703(d)	Altri record dell’account, esclusi i contenuti
Search warrant	Contenuti conservati; per WhatsApp informazioni del profilo, gruppi e rubrica, se disponibili

Meta, WhatsApp e Signal rispondono secondo il diritto statunitense: il perimetro della richiesta va deciso prima di scriverla.

Fonti: Convenzione sulla criminalità informatica, Budapest, 23 novembre 2001; 18 U.S.C. §§ 2701–2712; WhatsApp, Information for Law Enforcement Authorities.

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 classifica gli strumenti in cinque livelli di estrazione.

SWGDE 18-F-003 v2.0 · 2025

Raccolta, preservazione, gestione e acquisizione dei dispositivi mobili. Ricorda 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.

Nessuno di questi documenti descrive una singola app. Fissano il metodo; lo schema dei database va ricavato ogni volta dalla versione installata.

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
Autenticità del contenuto	Il database dell’app estratto dal dispositivo o dal backup, con il suo hash; lo screenshot serve soltanto a illustrare
Attribuzione	Identificativo dell’account e numero, dati di registrazione chiesti al provider, elenco dei dispositivi collegati, IMEI o numero di serie
Collocazione nel tempo	Timestamp del database in UTC, scarto dell’orologio annotato a verbale, riscontro sul dispositivo dell’interlocutore
Integrità	Hash di ogni file e dell’archivio, marca temporale apposta alla chiusura
Completezza	Conversazione intera, file di journal compresi, con versione dell’app e dello schema
Legittimità dell’accesso	Provvedimento dell’autorità giudiziaria oppure consenso scritto del titolare, richiamati nel verbale
Ripetibilità	Strumenti a codice aperto, comandi riportati per esteso, copia di lavoro consegnata alla controparte

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 strumenti

Tre vie, dal dispositivo al provider, e per ciascuna app i file che contano. Gli strumenti sono tutti a codice aperto e si provano nel laboratorio della parte successiva.

I livelli di estrazione



Classificazione NIST: salendo crescono invasività, tempo e competenze richieste.

Manuale. L'operatore sfoglia l'app e fotografa lo schermo. Altera lo stato dei messaggi e non restituisce dati verificabili.

Logica. Backup e file che il sistema concede: è il livello del laboratorio. Il contenuto dipende da ciò che ciascuna app lascia esportare.

Full file system. Nella prassi attuale si colloca fra il secondo e il terzo livello: apre le cartelle private delle app e, con le chiavi, i database cifrati.

Chip-off e oltre. Con la cifratura basata su file il contenuto letto dalla memoria resta cifrato: oggi serve di rado.

Il livello raggiunto va dichiarato nella relazione: determina che cosa si è potuto vedere e che cosa no.

Fonte: Ayers, Brothers e Jansen, Guidelines on Mobile Device Forensics, NIST SP 800-101 Rev. 1, 2014.

La preservazione del dispositivo

1. **Annotare lo stato**: acceso o spento, sbloccato o bloccato, carica residua, ora mostrata dal dispositivo e ora di riferimento.
2. **Isolare dalla rete**: modalità aereo, Wi-Fi e Bluetooth disattivati, oppure contenitore schermato.
3. **Mantenere l'alimentazione** e, quando il titolo lo consente, impedire il blocco automatico.
4. **Censire ciò che sta attorno**: computer con client desktop, sessioni web aperte, account di backup.
5. **Sigillare e documentare**: fotografie, numero di serie, catena di custodia compilata sul momento.

Tre avvertenze

Un telefono sbloccato che si spegne torna allo stato precedente al primo sblocco, con i dati dell'utente di nuovo cifrati.

L'isolamento non arresta i timer dei messaggi effimeri già ricevuti.

Aprire l'app per controllare segna i messaggi come letti e modifica il database.

Isolare ha un costo: i messaggi non ancora consegnati restano sul server. La scelta va annotata insieme alle sue ragioni.

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

Dove cercano i parser: i database delle cinque app

App	Android, sotto /data/data	iOS, nel contenitore dell'app
WhatsApp	`com.whatsapp/databases/msgstore.db`	`Shared/AppGroup/*/ChatStorage.sqlite`
Telegram	`org.telegram.messenger/files/cache4.db`	`telegram-data/account-*/postbox/db/db_sqlite`
Signal	`org.thoughtcrime.securesms/databases/signal.db`	`Shared/AppGroup/*/grdb/signal.sqlite`
Messenger	`threads_db2 e msys_database*`	`lightspeed-userDatabases/*.db`
Instagram	`com.instagram.android/databases/direct.db`	`Application Support/DirectSQLiteDatabase/*.db`

Sono tutti database SQLite. Quelli di Signal sono cifrati con SQLCipher e si aprono soltanto con la chiave custodita dal sistema operativo.

Senza root o jailbreak queste cartelle non sono leggibili: l'estrazione logica arriva ai backup, non ai database vivi.

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

WhatsApp: i file che contano

Android

msgstore.db: tabelle message, chat e jid; orari in millisecondi dall'epoca Unix. I contatti stanno in **wa.db**.

Backup locale: msgstore.db.crypt14 o .crypt15 nella cartella Databases, sotto Android/media/com.whatsapp.

Chiave: file key nell'area privata dell'app, oppure chiave di 64 cifre se il backup è cifrato end-to-end.

iOS

ChatStorage.sqlite: tabelle ZWAMESSAGE, ZWACHATSESSION e ZWAMEDIAITEM, nel contenitore condiviso dell'app.

Orari in secondi dal 1° gennaio 2001, da convertire prima di ogni confronto con Android.

Backup di iTunes o Finder: il file è compreso e si individua tramite Manifest.db.

Tre attenzioni

- **Schema**: negli anni le tabelle sono cambiate; uno strumento non aggiornato perde righe senza segnalarlo.
- **Identificativi**: accanto a numero@s.whatsapp.net compaiono identificativi @lid, da ricondurre al numero.
- **Journal**: i messaggi più recenti possono trovarsi in msgstore.db-wal e non ancora nel file principale.

Fonti: Anglano, Digital Investigation 11(3), 2014; codice di ALEAPP e iLEAPP; documentazione di wa-crypt-tools.

Telegram: cloud, chat segrete e client desktop

Chat cloud

La cronologia risiede sui server. Sul telefono resta una copia parziale: cache4.db su Android, db_sqlite su iOS.

Il testo è serializzato in campi binari: non basta una query, occorre un parser.

Chat segrete

Cifrate end-to-end, esistono soltanto sui due dispositivi che le hanno aperte. Non si sincronizzano e non compaiono nell'export.

Per queste il dispositivo è l'unica fonte.

Telegram Desktop

Cartella tdata con i dati locali cifrati. Da Impostazioni, Avanzate, l'export nativo produce la cronologia cloud in HTML o in JSON.

Il JSON riporta identificativo, data e mittente di ogni messaggio.

Riferimenti di ricerca. Anglano, Canonico e Guazzone (2017) hanno descritto gli artefatti su Android; Jaeckel, Spranger e Labudde (2025) quelli su iOS, dove il database è un archivio chiave-valore.

Con un account accessibile, l'export da Desktop è la via più rapida. Va però trattato come un prodotto dell'utente, non come un'estrazione.

Fonti: Digital Investigation 23 (2017), pp. 31–49; Forensic Science International: Digital Investigation, DFRWS EU 2025; codice di ALEAPP e iLEAPP.

Signal: tutto sul dispositivo, tutto cifrato

Telefono

signal.db su Android e signal.sqlite su iOS sono cifrati con SQLCipher. La chiave sta nel keystore o nel keychain: serve un’estrazione che arrivi fin lì.

Un backup di iTunes non contiene i messaggi.

Signal Desktop

Database SQLCipher con chiave in config.json, nelle versioni recenti protetta dalle funzioni del sistema operativo.

Uno studio del 2025 ne descrive la decifratura su Windows.

Secure Backups · 2025

Facoltativi. Archivio cifrato end-to-end rinnovato ogni giorno, protetto da una chiave di recupero di 64 caratteri generata sul dispositivo e mai inviata ai server.

Senza quella chiave l’archivio non si apre.

Dal provider. A una richiesta valida Signal dichiara di poter fornire due soli dati: la data di creazione dell’account e la data dell’ultima connessione al servizio.

La domanda preliminare: si dispone di un dispositivo sbloccato, o di una chiave?

Fonti: Signal, Introducing Signal Secure Backups, 8 settembre 2025; signal.org/bigbrother; Forensic Science International: Digital Investigation 54 (2025), 301941.

Messenger e Instagram: un gruppo, due regimi

Messenger

Cifratura end-to-end di default dal dicembre 2023. Le chat protette vivono sul dispositivo e nell'archiviazione protetta, che l'utente sblocca con un PIN.

Android: threads_db2 per lo storico, msys_database per le versioni attuali.

iOS: i file sotto lightspeed-userDatabases.

Instagram

Dopo l'8 maggio 2026 i messaggi diretti non sono più cifrati end-to-end: il contenuto resta sui server Meta.

Android: direct.db, accanto ai file ig_msys_database.

iOS: i file sotto DirectSQLiteDatabase.

Per entrambe. Dal Centro gestione account la funzione «Scarica le tue informazioni» consegna al titolare i messaggi in JSON o in HTML. È un export dell'utente, con i limiti di ogni export.

Per Messenger il contenuto si cerca sul dispositivo. Per Instagram può arrivare anche dal provider, con il titolo adeguato.

Fonti: annunci Meta del dicembre 2023 e del 2026; codice di ALEAPP e iLEAPP, versioni del 28 novembre 2026.

Client collegati, export e copie nel cloud

App	Client collegati	Export nativo	Copia nel cloud
WhatsApp	Web e Desktop, fino a quattro dispositivi oltre al telefono	Esporta chat: file di testo, con o senza media	Backup su Google Drive o iCloud
Telegram	Desktop e Web, con l'intera cronologia cloud	Da Desktop, in HTML o JSON	La cronologia stessa
Signal	Desktop, collegato al telefono	Nessuno in formato leggibile	Secure Backups, se attivati
Messenger	messenger.com e app desktop	Scarica le tue informazioni	Archiviazione protetta
Instagram	instagram.com	Scarica le tue informazioni	Server Meta

Un client collegato vale doppio. È un secondo luogo da acquisire ed è un secondo luogo dal quale altri possono avere letto: l'elenco dei dispositivi collegati va sempre documentato.

Un export è una dichiarazione. Lo produce l'utente, omette i messaggi eliminati e, se è un file di testo, si modifica con un editor.

Fonti: documentazione dei fornitori consultata a novembre 2026. Funzioni e limiti cambiano con le versioni delle app.

Che cosa può consegnare il provider

	Contenuto dei messaggi	Dati di registrazione	Accessi e indirizzi IP	Contatti e gruppi
WhatsApp	No	**Sì**	**Sì**	In parte
Signal	No	In parte	In parte	No
Telegram	No	In parte	In parte	No
Messenger	In parte	**Sì**	**Sì**	In parte
Instagram	**Sì**	**Sì**	**Sì**	In parte

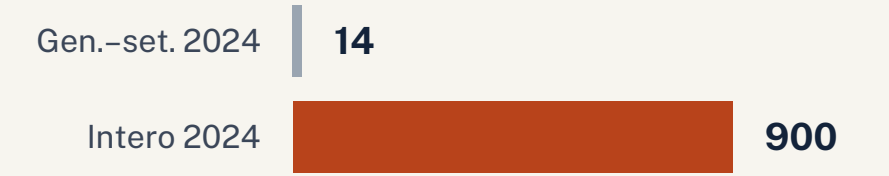
- **Signal**: soltanto la data di creazione dell'account e quella dell'ultima connessione.
- **Telegram**: dal settembre 2024 numero di telefono e indirizzi IP a fronte di richieste valide; dichiara di non consegnare i messaggi.
- **Messenger**: «in parte» riguarda le conversazioni non protette end-to-end e quelle segnalate dagli utenti.

Sintesi di quanto i fornitori dichiarano: linee guida per le autorità di WhatsApp e Meta, signal.org/bigbrother, informativa di Telegram. Il risultato dipende dal titolo giuridico.

I canali di richiesta al provider

1. **Conservazione**: la richiesta di congelamento dei dati precede ogni altra, perché i log hanno vita breve.
2. **Decreto dell'autorità giudiziaria** (art. 254-bis c.p.p.), trasmesso attraverso i portali che i fornitori riservano alle autorità.
3. **Ordine europeo di produzione**, dal 18 agosto 2026, verso i fornitori che offrono servizi nell'Unione.
4. **Rogatoria** verso gli Stati Uniti, quando si chiedono contenuti.
5. **Richiesta d'urgenza**, nei casi di pericolo imminente per la vita o l'incolumità.

Telegram, richieste statunitensi evase



Utenti interessati: 108 nei primi nove mesi, 2.253 a fine anno. In mezzo, il cambio di policy del settembre 2024.

La disponibilità di un fornitore non è un dato stabile: va verificata sul rapporto di trasparenza più recente prima di impostare la richiesta.

Fonti: Reg. (UE) 2023/1543; dati del transparency report di Telegram per il 2024, riferiti dalla stampa specializzata a gennaio 2025.

La cassetta degli strumenti open source

Strumento	A che cosa serve	Limite da conoscere
adb	Colloquio con un dispositivo Android e copia dei file accessibili	Senza root non legge le cartelle private delle app
libimobiledevice	Informazioni e backup di un iPhone con ideviceinfo e idevicebackup2	Il backup non contiene tutte le app: Signal ne resta fuori
wa-crypt-tools	Decifratura dei backup WhatsApp crypt12, crypt14 e crypt15	Richiede il file della chiave o la chiave di 64 cifre
ALEAPP e iLEAPP	Parsing di estrazioni Android e iOS, con report navigabile	Dipendono dallo schema della versione dell'app
sqlite3	Query dirette sui database, per verifica manuale	Va usato su una copia, in sola lettura, con i file di journal
sha256sum, tar, ots	Hash, archivio e marca temporale del fascicolo	La marca OpenTimestamps non è qualificata ai sensi di eIDAS

Il codice aperto non rende lo strumento corretto. Permette a chiunque di controllare che cosa ha fatto, ed è questo che conta in contraddittorio.

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

La validazione degli strumenti

Versione

Annotare versione dell’app, del sistema operativo e dello strumento. Per un progetto su Git la versione è il commit: quello usato per queste slide è del 28 novembre 2026.

Doppio riscontro

Ogni risultato rilevante si ottiene due volte: con il parser e con una query scritta a mano sullo stesso database. I conteggi devono coincidere.

Verità nota

Prima del caso reale, lo strumento si prova su un dispositivo di test con messaggi inviati dall’esaminatore, di cui si conoscono testo e orario.

Prove indipendenti

Il programma Computer Forensics Tool Testing del NIST pubblica i rapporti di prova sugli strumenti di acquisizione mobile: vanno consultati e citati.

Uno strumento che non riconosce uno schema nuovo non sempre avverte: restituisce meno righe. Soltanto il confronto dei conteggi lo rivela.

Fonti: NIST, Computer Forensics Tool Testing Program; SWGDE 20-F-005-1.0; codice di ALEAPP.

PARTE 4 · 70 MINUTI

Laboratorio guidato

Dal dispositivo di prova al fascicolo sigillato, con strumenti a codice aperto. Le schermate provengono da un dataset sintetico costruito per il corso.

Scenario e regole del laboratorio

Scenario

Uno studio legale consegna il telefono Android di un cliente. Il cliente afferma di avere scambiato tre messaggi WhatsApp dopo mezzogiorno del 28 novembre 2026. Una prima copia del database, fatta da un collaboratore, ne mostra soltanto quattro, tutti del mattino.

Quesito. Acquisire la conversazione e riferire che cosa risulta, spiegando la differenza fra le due copie.

Cartella di lavoro: caso02. Contiene due acquisizioni dello stesso database, un backup cifrato e la relativa chiave di prova.

Regole

Soltanto dispositivi e account creati per il corso. Il dataset è sintetico: schema ridotto, numeri 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
$ python3 -m venv ~/venv-wa && ~/venv-wa/bin/pip install wa-crypt-tools
$ git clone https://github.com/abrignoni/ALEAPP
$ git clone https://github.com/abrignoni/iLEAPP
# i parser si avviano dopo: pip install -r requirements.txt nella rispettiva cartella
```

CONTROLLO DELLE VERSIONI, DA RIPORTARE A VERBALE

```
$ adb version
$ ~/venv-wa/bin/pip show wa-crypt-tools
$ git -C ALEAPP log -1 --format=%H%n%cI
```

Perché un ambiente virtuale. Le librerie di wa-crypt-tools restano separate da quelle di sistema e la versione installata si documenta con un solo comando. Nella preparazione del corso: wa-crypt-tools 0.1.0.

Comandi di installazione eseguiti il 28 novembre 2026 su Ubuntu 24.04. L’installazione dei requisiti dei parser segue i rispettivi README.

Passo 2: identificare il dispositivo e il suo orologio

ANDROID, CON DEBUG USB AUTORIZZATO

```
$ adb devices -l
$ adb shell getprop ro.product.model
$ adb shell getprop ro.build.version.release
$ adb shell date -u ; date -u
$ adb shell dumpsys package com.whatsapp | grep versionName
```

IPHONE, DOPO L'ABBINAMENTO CON LA POSTAZIONE

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

Lo scarto dell'orologio. Le due date in UTC, lette una dopo l'altra, misurano di quanto il dispositivo anticipa o ritarda. Quel valore accompagna ogni orario della relazione.

Il prezzo del collegamento. Attivare il debug USB e autorizzare la postazione modifica le impostazioni del telefono: l'operazione va descritta, non taciuta.

Sintassi verificata sull'help di adb 34 e di libimobiledevice. L'esecuzione richiede un dispositivo collegato.

Passo 3: gli export prodotti dalle app

WhatsApp

Dalla chat: Altro, Esporta chat. Si ottiene un file di testo, con o senza allegati.

Mancano gli identificativi dei messaggi e gli orari dipendono dalle impostazioni locali del telefono.

Telegram Desktop

Impostazioni, Avanzate, Esporta dati di Telegram. Scegliere il formato JSON, leggibile da un programma.

Ogni messaggio porta identificativo, data e mittente. Le chat segrete restano escluse.

Messenger e Instagram

Centro gestione account, Le tue informazioni e autorizzazioni, Scarica le tue informazioni.

Meta prepara l’archivio in differita e avvisa quando è pronto: va previsto nei tempi.

ALLA RICEZIONE DI OGNI EXPORT

```
$ sha256sum export/* | tee export.sha256
$ date -u +%Y-%m-%dT%H:%M:%SZ
```

L’export documenta ciò che l’utente vede oggi. Entra nel fascicolo come riscontro dell’estrazione, non al suo posto.

Passo 4: acquisizione logica da Android

BACKUP LOCALE DI WHATSAPP, LEGGIBILE SENZA ROOT

```
$ adb shell ls -l /sdcard/Android/media/com.whatsapp/WhatsApp/Databases
$ adb pull -a /sdcard/Android/media/com.whatsapp/WhatsApp/Databases backup/
$ sha256sum backup/* | tee backup.sha256
# -a conserva data e ora dei file; i backup sono msgstore.db.crypt14 o .crypt15
```

Che cosa si ottiene

Il backup cifrato più recente e quelli dei giorni precedenti, quando l'utente ha attivato il backup locale. Senza la chiave restano illeggibili.

Che cosa resta fuori

Il database vivo in /data/data/com.whatsapp/databases e il file key richiedono root o un'estrazione full file system. Il vecchio adb backup non compare più nell'help di adb 34.

Un backup della notte precedente può contenere messaggi che la mattina dopo sono stati eliminati dal database vivo.

Sintassi di adb pull verificata sull'help di adb 34. I percorsi valgono per Android 11 e successivi.

Passo 5: lo stesso database, due risultati

```
studente@vm:~/caso02$ ls -l acquisizione_A acquisizione_B
acquisizione_A:
total 16
-rw-r--r-- 1 studente studente 16384 Nov 28 15:25 msgstore.db

acquisizione_B:
total 56
-rw-r--r-- 1 studente studente 16384 Nov 28 15:25 msgstore.db
-rw-r--r-- 1 studente studente 32768 Nov 28 15:25 msgstore.db-shm
-rw-r--r-- 1 studente studente  4152 Nov 28 15:25 msgstore.db-wal
studente@vm:~/caso02$ sqlite3 -readonly acquisizione_A/msgstore.db "SELECT count(*) FROM message"
4
studente@vm:~/caso02$ sqlite3 -readonly acquisizione_B/msgstore.db "SELECT count(*) FROM message"
7
studente@vm:~/caso02$
```

Che cosa è successo. Il file msgstore.db è identico nelle due cartelle. La seconda conserva anche msgstore.db-wal, il journal in cui SQLite scrive le transazioni recenti prima di riversarle nel file principale.

La regola. I tre file si copiano insieme e si aprono su una copia, in sola lettura. Aprire l'originale in scrittura riversa il journal e cambia l'impronta del reperto.

I tre messaggi di mezzogiorno esistevano. Mancavano dalla prima copia perché chi l'ha fatta ha preso un file su tre.

Schermata originale, prodotta il 28 novembre 2026 su un dataset sintetico con schema ridotto.

Passo 6: decifrare il backup con wa-crypt-tools

```
studente@vm:~/caso02$ ls -l backup
total 8
-rw-r--r-- 1 studente studente  65 Nov 28 15:27 chiave-di-prova.hex
-rw-r--r-- 1 studente studente 786 Nov 28 15:27 msgstore.db.crypt15
studente@vm:~/caso02$ wadecrypt $(cat backup/chiave-di-prova.hex) backup/msgstore.db.crypt15 backup/msgstore.db
keyfactory.py:46        : [I] The keyfile could not be opened.
key15.py:54     : [I] Crypt15 / Raw key loaded
wadecrypt.py:271        : [I] Done
studente@vm:~/caso02$ sha256sum acquisizione_A/msgstore.db backup/msgstore.db
8b6aaf0e18dbce31208ff58134aee0102e7b095b146e39ad80e14beec0157610  acquisizione_A/msgstore.db
8b6aaf0e18dbce31208ff58134aee0102e7b095b146e39ad80e14beec0157610  backup/msgstore.db
studente@vm:~/caso02$ wadecrypt 0000000000000000000000000000000000000000000000000000000000000000 backup/msgstore.db.crypt15
backup/errata.db
keyfactory.py:46        : [I] The keyfile could not be opened.
key15.py:54     : [I] Crypt15 / Raw key loaded
db15.py:155     : [E] Authentication tag mismatch: MAC check failed.
    This probably means your backup is corrupted.
wadecrypt.py:261        : [E] I can't recognize decrypted data. Decryption not successful.
    The key probably does not match with the encrypted file.
    Or the backup is simply empty. (check with --force)
wadecrypt.py:271        : [I] Done
studente@vm:~/caso02$
```

La chiave. wadecrypt accetta il file encrypted_backup.key oppure la chiave esadecimale di 64 cifre che WhatsApp mostra all’utente quando attiva il backup cifrato end-to-end.

Il controllo. Il database decifrato ha la stessa impronta della copia in chiaro. Con una chiave errata lo strumento si arresta e lo dichiara: non produce un file plausibile ma sbagliato.

Schermata originale del 28 novembre 2026: backup di prova cifrato con waencrypt e chiave generata per l’esercizio, wa-crypt-tools 0.1.0.

Variante iPhone: il backup con libimobiledevice

BACKUP CIFRATO E LETTURA CON ILEAPP

```
$ 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 di dati che quello in chiaro esclude, fra cui il keychain.

Che cosa contiene

ChatStorage.sqlite di WhatsApp sì. I messaggi di Signal no. Per Telegram la copia locale della cache, se presente.

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 abbinato alla postazione.

Passo 7: leggere la conversazione

```
studente@vm:~/caso02$ cat query.sql
SELECT datetime(m.timestamp/1000,'unixepoch') AS utc,
       CASE m.from_me WHEN 1 THEN 'inviato' ELSE 'ricevuto' END AS verso,
       j.raw_string AS chat, m.text_data AS testo
FROM message m
JOIN chat c ON c._id = m.chat_row_id
JOIN jid  j ON j._id = c.jid_row_id
ORDER BY m.timestamp;
studente@vm:~/caso02$ sqlite3 -readonly -header -column acquisizione_B/msgstore.db < query.sql
utc                 verso     chat                        testo
------------------  --------  --------------------------  ----------------------------------------
2026-11-28 10:00:00  ricevuto  390000000001@s.whatsapp.net  Buongiorno, conferma la riunione di oggi?
2026-11-28 10:01:35  inviato   390000000001@s.whatsapp.net  Confermo, alle 15 in sede.
2026-11-28 10:10:00  ricevuto  390000000002@s.whatsapp.net  Le invio il documento entro sera.
2026-11-28 10:11:00  inviato   390000000002@s.whatsapp.net  Grazie, lo attendo.
2026-11-28 12:00:00  ricevuto  390000000001@s.whatsapp.net  Cambio di programma: ci vediamo alle 17.
2026-11-28 12:01:00  inviato   390000000001@s.whatsapp.net  Va bene, alle 17.
2026-11-28 12:30:00  ricevuto  390000000002@s.whatsapp.net  Documento inviato adesso.
studente@vm:~/caso02$ sha256sum acquisizione_B/msgstore.db*
8b6aaf0e18dbce31208ff58134aee0102e7b095b146e39ad80e14beec0157610  acquisizione_B/msgstore.db
675d1935a09b08436af370d66781b5369a64d9c7581c344651f754b9e3b70cc1  acquisizione_B/msgstore.db-shm
e6a7c8bcc05f24c554da718fa762034e2291cd2948e951a4ff8df1b00fd88df6  acquisizione_B/msgstore.db-wal
studente@vm:~/caso02$
```

La query. Unisce message, chat e jid, converte i millisecondi in UTC e traduce from_me in «inviato» o «ricevuto». Si salva in un file e si allega alla relazione.

Il parser. Su un'estrazione completa lo stesso elenco si ottiene con **python3 ALEAPP/aleapp.py -t fs -i estrazione/ -o report/**. I due conteggi vanno confrontati.

Schermata originale del 28 novembre 2026 su dataset sintetico con schema ridotto. Su un database reale la query va adattata allo schema della versione installata.

Chiusura: verifica incrociata e sigillo

Domanda	Dove guardare
I due interlocutori hanno lo stesso messaggio?	Stesso identificativo del messaggio (key_id) nei database dei due telefoni
L'orario regge?	timestamp e received_timestamp, corretti dello scarto dell'orologio
La copia è completa?	Conteggio per conversazione, confrontato con export e backup
L'account è di quella persona?	Dati di registrazione chiesti al provider, SIM, dispositivi collegati

SIGILLO DEL FASCICOLO

```
$ find caso02 -type f -exec sha256sum {} + | tee caso02.sha256
$ tar -cf caso02.tar caso02 caso02.sha256 && sha256sum caso02.tar
$ ots stamp caso02.tar
```

La marca OpenTimestamps prova che l'archivio esisteva a una certa data. Dove occorre l'efficacia prevista da eIDAS si aggiunge una marca temporale qualificata.

Fonti: Reg. (UE) n. 910/2014, artt. 41 e 42; documentazione di OpenTimestamps.

Errori ricorrenti

Errore	Conseguenza
Aprire l’app sul telefono «per dare un’occhiata»	Messaggi segnati come letti, timer avviati, database modificato
Lasciare il dispositivo in rete	Sincronizzazioni, cancellazioni a distanza, nuovi messaggi dopo il sequestro
Copiare il solo file principale del database	Mancano i messaggi più recenti, ancora nel journal
Produrre screenshot o export come unica fonte	Nessuna risposta su integrità, orari e messaggi eliminati
Trascurare fuso orario e scarto dell’orologio	Sequenze di eventi ricostruite in ordine sbagliato
Usare un parser non aggiornato allo schema	Righe perse senza alcun avviso
Dimenticare client collegati e backup	Si rinuncia alle copie in cui i messaggi eliminati sopravvivono
Estrarre tutto quando serviva una chat	Violazione della proporzionalità, con rischio di inutilizzabilità

Metà di questi errori si commette prima ancora di avviare uno strumento.

Limiti legali ed etici

Il titolo

In sede penale, provvedimento dell'autorità giudiziaria: dopo Corte cost. n. 170/2023 i messaggi sono corrispondenza. In sede privata, consenso scritto e informato del titolare dell'account.

I terzi

Ogni chat contiene dati personali degli interlocutori, che non hanno prestato alcun consenso. Si acquisisce e si espone soltanto ciò che serve al quesito.

I reati dietro l'angolo

Leggere le chat 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 fra coniugi o colleghi.

La proporzione

La copia integrale del dispositivo è uno strumento di selezione, non il risultato. Ciò che eccede il quesito va restituito o distrutto, e la scelta va documentata.

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

Riferimenti: artt. 15 Cost., 615-ter e 616 c.p., 254 c.p.p.; Reg. (UE) 2016/679; 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: la chat del dirigente

Scenario di fantasia

Una società contesta a un dirigente di avere comunicato a un concorrente informazioni riservate attraverso WhatsApp e Telegram. Il dirigente nega e produce la propria versione delle conversazioni. In parallelo pende un procedimento penale.

Incarico. Come consulenti della società, valutare ciò che è agli atti e indicare che cosa manca.

Che cosa c’è nel fascicolo

N.	Reperto
1	Dodici screenshot della chat WhatsApp, prodotti dal dirigente
2	Export in formato testo della stessa chat, senza hash
3	msgstore.db dal telefono aziendale, con hash, senza file di journal
4	Export JSON da Telegram Desktop del computer aziendale
5	Risposta del provider: dati di registrazione e indirizzi IP

Nessun verbale riporta l’ora del dispositivo al momento dell’acquisizione.

Caso di studio: il lavoro in gruppo

1

Per ciascun reperto, a quali delle quattro domande risponde: contenuto, attribuzione, tempo, integrità e completezza?

2

Nel reperto 3 che cosa può mancare? Con quale operazione, ancora possibile, lo si accerta?

3

Se gli screenshot del dirigente e il database del telefono aziendale divergono, quali spiegazioni tecniche vanno escluse prima di parlare di alterazione?

4

Che cosa resta da chiedere al dirigente, alla società e al provider, e con quale titolo giuridico per ciascuna richiesta?

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. Per Corte cost. n. 170/2023 i messaggi WhatsApp letti e conservati nel telefono sono

A. corrispondenza tutelata dall'art. 15 Cost.
B. documenti acquisibili a norma dell'art. 234 c.p.p.
C. dati di traffico

2. Il file msgstore.db-wal contiene

A. una copia di sicurezza del database
B. transazioni recenti non ancora riversate nel file principale
C. la chiave di cifratura del backup

3. Per decifrare msgstore.db.crypt15 occorre

A. il codice di sblocco del telefono
B. soltanto wa-crypt-tools
C. il file della chiave oppure la chiave di 64 cifre

4. A una richiesta valida Signal dichiara di poter fornire

A. i messaggi degli ultimi trenta giorni
B. rubrica e gruppi dell'utente
C. data di creazione dell'account e data dell'ultima connessione

Quiz di verifica: domande 5–8

5. Per la CGUE (C-548/21) l’accesso della polizia ai dati di un telefono

A. richiede di regola l’autorizzazione preventiva di un giudice o di un’autorità indipendente
B. è ammesso soltanto per i reati gravi
C. non incontra limiti se il telefono è sbloccato

6. Le chat segrete di Telegram

A. sono comprese nell’export da Telegram Desktop
B. risiedono sui server come le chat cloud
C. esistono soltanto sui dispositivi che le hanno aperte

7. Isolare il telefono dalla rete

A. arresta i timer dei messaggi effimeri
B. impedisce nuove sincronizzazioni, ma non arresta i timer già avviati
C. rende superflua l’annotazione dell’ora del dispositivo

8. Dopo l’8 maggio 2026 i messaggi diretti di Instagram

A. non sono più cifrati end-to-end e restano sui server Meta
B. sono cifrati end-to-end di default
C. non vengono più conservati dal fornitore

Quiz di verifica: soluzioni

N.	Risposta	Perché
1	A	La tutela dell’art. 15 Cost. non cessa con la lettura del messaggio
2	B	È il journal di SQLite: si copia insieme al file principale
3	C	Lo strumento applica la chiave, non la ricava
4	C	Sono i due soli dati che il servizio dichiara di conservare
5	A	Salvo urgenza; la gravità del reato non è l’unico criterio
6	C	Non passano dal cloud e non entrano nell’export
7	B	Il conteggio avviene sul dispositivo e non dipende dalla rete
8	A	L’opzione end-to-end è stata ritirata: il contenuto è presso il fornitore

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

IN SINTESI

Un messaggio si acquisisce dove risiede, con il titolo che lo consente, e si riscontra su una seconda copia

Prima di toccare

Stabilire quale copia si cerca e con quale titolo. Preservare il dispositivo, annotarne l'ora, censire client collegati e backup.

Durante

Copiare i database con i loro journal, lavorare su copie, calcolare gli hash subito. Ogni risultato due volte: parser e query.

Dopo

Dichiarare livello di estrazione, versioni e limiti. Distinguere ciò che è accertato da ciò che è compatibile con i dati.

Le app cambiano a ogni versione. Il metodo resta: sapere dove guardare, saperlo dimostrare, saperne dichiarare i limiti.

Fonti: norme e giurisprudenza

Italia

- Costituzione, art. 15; c.p.p., artt. 234, 247, 254, 254-bis, 354 e 360; c.p., artt. 615-ter e 616
- L. 18 marzo 2008, n. 48
- Corte cost., sent. 27 luglio 2023, n. 170
- Cass. pen., Sez. Un., 29 febbraio 2024 (dep. 14 giugno 2024), nn. 23755 e 23756
- Cass. pen., sez. V, n. 1822/2018; sez. VI, n. 1269/2025
- Senato, A.S. 806, e Camera, A.C. 1822, XIX legislatura: introduzione dell'art. 254-ter c.p.p.

Unione europea e ambito internazionale

- CGUE, Grande Sezione, 4 ottobre 2024, C-548/21
- CGUE, Grande Sezione, 30 aprile 2024, C-670/22
- Dir. (UE) 2016/680; dir. 2014/41/UE
- Reg. (UE) 2023/1543 e dir. (UE) 2023/1544
- Reg. (UE) 2016/679; Reg. (UE) n. 910/2014
- Convenzione sulla criminalità informatica, Budapest, 2001; Convenzione ONU contro la criminalità informatica, 2024
- Stored Communications Act, 18 U.S.C. §§ 2701–2712; CLOUD Act, 2018

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

Fonti: standard, documentazione e strumenti

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

Strumenti

- ALEAPP e iLEAPP, github.com/abrignoni
- wa-crypt-tools, github.com/ElDavoo/wa-crypt-tools
- Android SDK Platform-Tools, libimobiledevice, SQLite, OpenTimestamps

Documentazione dei fornitori

- WhatsApp, Information for Law Enforcement Authorities
- WhatsApp, Encryption Overview, technical white paper
- Signal, Introducing Signal Secure Backups, 8 settembre 2025
- Signal, Government requests, signal.org/bigbrother
- Telegram, Privacy Policy e transparency report
- Meta, annunci sulla cifratura end-to-end di Messenger (dicembre 2023) e di Instagram (2026)
- Meta, Tencent, Telegram: comunicazioni sugli utenti attivi, 2025

Documentazione consultata a novembre 2026. Le pagine dei fornitori vengono aggiornate senza preavviso: annotare la data di consultazione.

Fonti: letteratura scientifica

- Anglano C., Forensic analysis of WhatsApp Messenger on Android smartphones, Digital Investigation 11(3), 2014, pp. 201–213
- Anglano C., Canonico M., Guazzone M., Forensic analysis of Telegram Messenger on Android smartphones, Digital Investigation 23, 2017, pp. 31–49
- Heath H., MacDermott Á., Akinbi A., Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data?, Forensic Science International: Digital Investigation 46, 2023, 301585
- Jaeckel L., Spranger M., Labudde D., Forensic analysis of Telegram Messenger on iOS smartphones, Forensic Science International: Digital Investigation, DFRWS EU 2025
- Decrypting messages: Extracting digital evidence from Signal Desktop for Windows, Forensic Science International: Digital Investigation 54, 2025, 301941
- Studio sui messaggi effimeri di WhatsApp su Android privo di root, Evergreen 11(1), 2024, pp. 516–524
- Cohn-Gordon K., Cremers C., Dowling B., Garratt L., Stebila D., A Formal Security Analysis of the Signal Messaging Protocol, Journal of Cryptology 33, 2020
- Rösler P., Mainka C., Schwenk J., More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema, IEEE EuroS&P 2018

Autori, pagine e DOI vanno riscontrati sulle pagine degli editori prima della citazione. Per due voci è indicato il solo titolo o l’argomento.

CORSO AVANZATO DI DIGITAL FORENSICS

Grazie per l'attenzione

Vincenzo Calabrò

www.vincenzocalabro.it



Inquadra per aprire il sito