Ordine degli Ingegneri
della Provincia di Palermo

Evento Formativo

Acquisizione, custodia e analisi di fonti di prova digitale: Smartphone

Relatore: Brig. Capo CC - dott. Claudio Scaduto
Data: 02/04/2026
Responsabile scientifico: ing. Dario Ferrante

Base fondamentale della digital forensics

Lo standard internazionale ISO/IEC 27037 contiene le linee guida per l'**identificazione**, la **raccolta**, **l'acquisizione**, la **conservazione** e il **trasporto di evidenze digitali** al fine di facilitarne lo scambio fra più Paesi utilizzando protocolli metodologici comuni. Lo standard è applicabile in qualsiasi ambito (civile, penale, stragiudiziale), senza fare riferimento a specifici ordinamenti né a norme giuridiche.

Perché uno standard internazionale nel sistema giudiziario italiano?

Il sistema accusatorio italiano, **la prova (digital evidence)** si forma principalmente nel dibattimento, durante la fase del processo e nel contraddittorio tra le parti (pubblico ministero e avvocati) davanti a un giudice terzo. Gli elementi raccolti durante le indagini preliminari sono, di regola, **solo fonti di prova.**

La prova digitale è per sua natura fragile e facilmente **alterabile**.

L'adozione di questo standard assicura che il trattamento del dato segua **best practice** riconosciute, **garantendo l'integrità e l'ammissibilità della fonte di prova** in sede giudiziaria, conformemente alle esigenze della computer forensics.

Panoramica

Lo **smartphone** è considerato dalla giurisprudenza italiana come un **"domicilio informatico"**, uno spazio virtuale privato protetto dalla legge dove si conservano dati, foto e messaggi. Accedervi senza autorizzazione, anche tra partner, **viola l'art. 615-ter del Codice Penale** (accesso abusivo a sistema informatico), punibile con la reclusione.

La giurisprudenza della Corte di Cassazione ha evoluto significativamente la tutela del "domicilio informatico", assimilando lo **smartphone a uno spazio privato inviolabile**.

La recente sentenza della Cassazione Penale, Sez. VI, n. 543 del 3 dicembre 2025 pongono limiti severi al sequestro indiscriminato e all'acquisizione dei dati, prediligendo **la copia forense selettiva (fine)** rispetto al sequestro "**grezzo**" dell'intero dispositivo.

Quadro normativo

Cass. Pen. 2744/2025: Ha sancito il divieto di sequestro indiscriminato (c.d. "pesca a strascico") di dispositivi elettronici. **Il sequestro deve essere mirato**.

Cass. Pen. 35933/2025: Il sequestro è nullo se il pubblico ministero non motiva in modo specifico **quali dati cerca e per quale motivo**, non potendo acquisire l'intero contenuto del telefono indiscriminatamente.

Cass. Pen. 13585/2025: Sottolinea la necessità di proporzionalità e specificità nel sequestro di materiale informatico.

Quadro normativo

La Cassazione impone una chiara distinzione tra l'acquisizione fisica del telefono e l'acquisizione logica dei dati.

Copia Fine (Selettiva/Forense): È la procedura auspicata. Consiste nell'estrapolazione dei soli dati pertinenti alle indagini tramite tecniche forensi che garantiscono l'integrità del dato (hash code), proteggendo la privacy dell'utente per i dati irrilevanti.

Copia Grezza/Integrale: L'acquisizione "bit-to-bit" di tutto il contenuto. La Cassazione ritiene illegittimo il trattenimento prolungato di questa copia integrale se non strettamente necessario, imponendo una rapida analisi e la distruzione dei dati non rilevanti.

Perquisizione e Sequestro: Ausiliario di PG ex art.348 c.p.p.

L'ausiliario di Polizia Giudiziaria nelle perquisizioni informatiche è un tecnico esperto, nominato ex art. 348 c.p.p., che supporta gli ufficiali nella ricerca e acquisizione di dati digitali, operando sotto il loro controllo. Garantisce l'integrità delle prove informatiche (copia forense), agisce come pubblico ufficiale e non può rifiutare l'incarico.

Perquisizione e Sequestro: come operare

È di fondamentale importanza che gli operatori siano adeguatamente informati sulla situazione in essere prima di iniziare le loro attività:

1. tipo di avvenimento
2. data e ora accadimento
3. sequestro o acquisizione, presenza di dati volatili, presenza di attività di rete, etc.
4. tool, accessori, competenze specifiche necessarie
5. ricordare a chiunque interverrà sulla scena di disattivare il Wi-Fi e il Bluetooth dei propri terminali, in modo da non interagire con quelli presenti in loco

Perquisizione e Sequestro: identificazione

Il processo di identificazione è devoluto alla ricerca dei dispositivi digitali pertinenti alle indagini, stabilendo quale apparato e in grado, almeno teoricamente, di memorizzare informazioni digitali attendibili ed inerenti al caso investigativo.

Trattandosi di smartphone gli stessi devono essere in pieno **possesso** dell'indagato o comunque nella **sua disponibilità**, prevede una fase di valutazione, e di **collaborazione** dello stesso indagato per fornire i **codici di sblocco**.

Perquisizione e Sequestro: raccolta

Dopo la fase di identificazione (individuazione del dispositivo e associazione all'utente), si passa al repertamento (o sequestro), che deve garantire l'integrità della prova digitale. Questa fase prevede la documentazione accurata dello stato dello smartphone:

Stato di conservazione (Fisico): Si descrivono le condizioni esterne del dispositivo (es. graffi, rotture dello schermo, presenza di cover, danneggiamenti evidenti). È fondamentale fotografare lo smartphone da diverse angolazioni prima di toccarlo.

Perquisizione e Sequestro: raccolta

Stato operativo (Acceso o Spento):

Se acceso: Si documenta se è sbloccato o bloccato (PIN/Pattern), se è attiva la modalità aereo, il livello di batteria e l'orario di rinvenimento, il dispositivo viene immediatamente inserito in una **gabbia di Faraday** per isolarlo dalle reti cellulari, Wi-Fi e Bluetooth, impedendo la ricezione di nuovi dati (che sovrascriverebbero quelli vecchi) o la cancellazione remota da parte di terzi.

Se spento: Si documenta lo stato e si evita di accenderlo per non alterare i dati.

Perquisizione e Sequestro: raccolta

In ambito di digital forensics, lo stato (acceso o spento) di uno smartphone determina l'intera strategia di acquisizione dei dati e la possibilità stessa di accedere alle prove. Questa distinzione è cruciale a causa della crittografia moderna e della volatilità delle informazioni.

Perquisizione e Sequestro: raccolta

Se lo smartphone è acceso, **l'obiettivo primario è impedire che si spenga o si blocch**i.

Accesso ai Dati (AFU): Se l'utente lo ha già sbloccato almeno una volta dall'accensione, il dispositivo si trova in stato **AFU (After First Unlock)**. In questo stato, molte chiavi di crittografia sono caricate in memoria, permettendo l'estrazione di un volume di dati significativamente maggiore rispetto a un dispositivo bloccato. È obbligatorio **isolare** il telefono dalla rete tramite modalità aereo o l'uso di una **borsa di Faraday** per evitare comandi di cancellazione remota **(remote wipe)**, mantenendo la carica collegandolo ad una fonte di alimentazione esterna per evitare lo spegnimento accidentale

Perquisizione e Sequestro: raccolta

Perquisizione e Sequestro: raccolta

Se lo smartphone viene rinvenuto spento, **la regola aurea è lasciarlo spento fino all'arrivo in laboratorio.**

Crittografia (BFU): Al riavvio, il dispositivo entra in stato **BFU (Before First Unlock)**.

In questa fase, la maggior parte dei dati è criptata e inaccessibile senza il codice di sblocco dell'utente, limitando l'analisi a pochissimi file di sistema non sensibili. L'accensione del dispositivo altera inevitabilmente numerosi file di sistema e log temporali, compromettendo l'integrità della "scena del crimine digitale"

Perquisizione e Sequestro: raccolta

Una volta repertati i dispositivi spenti vengono inseriti all'interno di buste specifiche per la custodia, spesso sono **buste di sicurezza numerate,** queste hanno una striscia adesiva antimanomissione.

Perquisizione e Sequestro: raccolta

Il verbale di repertamento riporterà dunque: marca/modello, IMEI, stato fisico, stato operativo (acceso/spento), eventuali danni, ora del blocco della rete e la posizione esatta in cui è stato rinvenuto.

Nonché l'eventuale busta di sicurezza utilizzata, o se lo stesso è stato inserito all'interno di una busta di faraday e posto sotto carica per evitare il passaggio dallo stato AFU allo stato BFU.

Acquisizione

Distinzione delle operazioni in base al C.P.P.:

Accertamenti Ripetibili (Art. 359 C.P.P.): Se l'estrazione dei dati non modifica il contenuto del telefono (es. una copia logica standard), può essere fatta dal consulente tecnico del PM senza preavviso alla difesa, non assistono alle operazioni tecniche.

Accertamenti Irripetibili (Art. 360 C.P.P.): Se l'acquisizione comporta il rischio di modificare i dati (es. rooting del dispositivo, chip-off, o manovre su uno smartphone acceso che potrebbero causarne il blocco definitivo), è obbligatorio dare avviso all'indagato, alla difesa che ha il diritto di nominare un proprio consulente per assistere alle operazioni, e alla parte offesa.

Possono assistere i difensori ed eventuali consulenti.

Acquisizione

Strumenti come **Cellebrite, MSAB o Magnet** offrono garanzie tecniche specifiche:

Write-Blocking: Il software comunica con il telefono in "sola lettura". Impedisce fisicamente al computer di inviare dati verso lo smartphone, evitando qualsiasi alterazione.

Calcolo dell'Hash: Al termine dell'acquisizione, il software genera un codice alfanumerico univoco (es. SHA-256). Se viene alterata la copia l'Hash cambierà, rivelando la manomissione.

Reportistica: Generano un verbale tecnico che elenca la versione del software usato, l'ora di inizio/fine e i numeri seriali del dispositivo, fondamentale per la catena di custodia.

Acquisizione

Differenze tra i principali strumenti

Cellebrite UFED: Il leader di mercato, celebre per la capacità di superare i blocchi schermo su migliaia di modelli Android e iOS.

Magnet GrayKey: Specializzato quasi esclusivamente nel mondo Apple; è uno dei pochi strumenti in grado di eseguire estrazioni complete di iPhone protetti da passcode complessi.

MSAB Raven e Xry Pro: Il primo molto usato dalle forze di polizia per triage rapidi sul campo, permette di estrarre solo i dati essenziali in pochi minuti, il secondo stesse funzioni di UFED, unica differenza la mole di dispositivi compatibili, si hanno risultati eccellenti con dispositivi Samsung.

Acquisizione

Tipologie di estrazione supportate dai vari software forensi sono:

Estrazione Logica: È il metodo di acquisizione meno invasivo il software interroga il telefono e quest'ultimo risponde inviando i dati che è abituato a gestire normalmente (rubrica, SMS, foto nella galleria). Non recupera quasi mai i dati cancellati.

Estrazione File System: Copia l'intera gerarchia dei file, inclusi database di app come WhatsApp, log di sistema e file nascosti.

Estrazione Fisica (Dump): È la copia "bit a bit" dell'intera memoria flash. Permette di recuperare dati cancellati e frammenti di database. È la più complessa a causa della crittografia moderna che spesso la rende impossibile senza chiavi specifiche.

Acquisizione

Spesso i software forensi sopra descritti riversano i dati all'interno di cartelle, nel cui interno troviamo i file contenenti i dati estratti e del quale non spesso vengono individuati gli HASH se non utilizzando i software di reportistica dei produttori, risulta buona norma riversare le crtelle in un unico archivio **.rar privo di compressione** e di calcolarne il suo HASH.

Il risultato ottenuto sarà una ulteriore garanzia e certificazione del dato estratto.

Anche in futuro si può ancor prima di avviare il software di reportistica, verificare il codice HASH, e verificare la corretta corrispondenza con il verbale di accertamento tecnico.

Conservazione

La conservazione (preservation) per smartphone è la fase critica che segue il sequestro, finalizzata a proteggere i dati contenuti nel dispositivo da alterazioni, cancellazioni accidentali o accessi remoti non autorizzati. L'obiettivo principale è garantire l'integrità e l'ammissibilità delle fonti di prove digitali in sede giudiziaria, mantenendo una "**catena di custodia**" (chain of custody) ininterrotta.

Conservazione

Ecco i punti chiave della conservazione in ambito mobile forensics:

Isolamento dalla rete: Il dispositivo deve essere isolato per impedire la ricezione di comandi da remoto inserendo lo smartphone in busta di Faraday.

Gestione dello stato di accensione: Se il telefono è acceso, si cerca di mantenerlo tale per evitare che la crittografia renda i dati inaccessibili una volta spento (AFU/BFU). Se è spento, si mantiene tale.

Alimentazione continua: È cruciale prevenire lo spegnimento per esaurimento batteria.

Evitare alterazioni: Non bisogna utilizzare il dispositivo, navigare nelle app o modificare le impostazioni. Ogni interazione deve essere documentata per garantire che la prova non sia stata manipolata.

Copia Forense (Acquisizione): Una volta preservato, si procede all'acquisizione, verificandone l'integrità tramite algoritmi di hashing (es. SHA-256).

Conservazione

Catena di Custodia (Chain of Custody): Documentazione meticolosa che traccia chi ha avuto in carico il dispositivo, quando e quali operazioni sono state eseguite, fondamentale per la validità legale della prova.

Senza una catena di custodia rigorosa, l'attendibilità della prova può essere facilmente contestata, poiché non è possibile dimostrare che i dati non siano stati alterati o manipolati durante le fasi di indagine.

Trasporto

La catena di custodia non riguarda solo il reperto fisico, ma si estende al trasporto del dato digitale, ovvero il passaggio delle informazioni estratte dal laboratorio al tribunale o tra consulenti. In questa fase, il rischio maggiore non è il danneggiamento fisico, ma l'alterazione del bit o l'accesso non autorizzato.

Trasporto

Il Trasporto del Reperto Fisico (Smartphone):

Se lo smartphone deve essere spostato da un ufficio all'altro:

1. **Sigilli antimanomissione:** Il dispositivo viene inserito in buste di sicurezza con numerazione univoca. **Se la busta viene aperta, il sigillo mostra segni evidenti di effrazione.**
2. **Verbale di consegna:** Ogni spostamento fisico richiede un documento firmato da chi consegna e chi riceve, indicando ora esatta e motivo del trasferimento.
3. **Schermatura continua:** Se il dispositivo è acceso, deve viaggiare all'interno di una borsa di Faraday per evitare connessioni accidentali a celle telefoniche durante il tragitto.

Trasporto

Il Trasporto del Dato Estratto (Copia Forense)

Una volta effettuata l'estrazione, i dati vengono solitamente trasferiti su supporti esterni Hard Disk e Pendrive.

1. **Calcolo dell'Hash:** Prima di muovere il file, si genera l'impronta digitale (MD5, SHA-1 o SHA-256). All'arrivo, il destinatario ricalcola l'HASH se i due codici coincidono, la catena di custodia del dato è integra.
2. **Crittografia:** Per proteggere la privacy e l'integrità, il supporto di trasporto deve essere crittografato. La password viene comunicata attraverso un canale separato.
3. **Verbale di consegna:** Ogni spostamento fisico richiede un documento firmato da chi consegna e chi riceve, indicando ora esatta e motivo del trasferimento.

Analisi

L'analisi forense su smartphone è sensibilmente più complessa rispetto a quella sui computer a causa della natura dinamica del software e delle protezioni hardware. Quando si lavora su una copia forense, le criticità principali che un analista deve affrontare sono legate alla decifrazione, alla frammentazione dei dati e alla volatilità delle app.

Analisi

Crittografia e Decifrazione

Quasi tutti gli smartphone moderni (Android 10+ e iOS) utilizzano la **File-Based Encryption (FBE)**.

- **La Criticità:** Se la copia forense è stata eseguita "a freddo" (telefono spento) senza le chiavi di decifrazione, l'immagine ottenuta sarà un ammasso di dati illeggibili.
- **L'Analisi:** L'analista deve spesso ricorrere ad acquisizioni di tipo Advanced Logical o File System, che estraggono i dati mentre il dispositivo è "decifrato" (acceso e sbloccato), rendendo la copia forense un'istantanea dei file già in chiaro.

Analisi

Dati "Volatili" e Applicazioni di Messaggistica

Le app come WhatsApp, Telegram o Signal non salvano tutto in database semplici.

- **Database Criptati:** Molte app hanno database interni (.db.crypt14, ecc.) con chiavi di cifratura univoche salvate nell'area protetta del sistema (Keystore/Keychain). Se la copia forense non include queste chiavi (accessibili solo con permessi di Root o Jailbreak), i messaggi non sono visualizzabili.
- **Messaggi Effimeri:** I contenuti che "spariscono" o le chat segrete spesso non lasciano tracce nella memoria fisica (NAND), rendendo la copia forense inutile per quel reperto specifico se non acquisita in tempo reale.

Analisi

Cancellazione e Trimming (Garbage Collection)

A differenza degli Hard Disk meccanici, le memorie Flash degli smartphone usano il comando TRIM.

- **La Criticità:** Quando un file viene cancellato, il sistema operativo pulisce fisicamente le celle di memoria quasi immediatamente per ottimizzare le prestazioni.
- **L'Analisi:** Il recupero di file cancellati da una copia forense di uno smartphone moderno è estremamente difficile, se non impossibile, rispetto ai vecchi dispositivi. I software di analisi già mensionati difficelmente riescono a ricostruire tali dati. L'analista cercherà quindi nei WAL files (Write-Ahead Logs) di SQLite, che potrebbero contenere frammenti di dati prima che vengano scritti nel database principale.

Analisi

Cloud Sourcing e Sincronizzazione

Lo smartphone è spesso solo un "terminale" di dati che risiedono altrove.

- **La Criticità:** Una copia forense locale potrebbe mostrare solo una parte della verità. Se l'utente ha visualizzato una foto salvata su Google Photos o iCloud senza scaricarla, quella foto non sarà nella copia fisica del telefono, ma solo nelle miniature (thumbnails) o nella cache.
- **L'Analisi:** L'esperto deve distinguere tra ciò che è fisicamente presente sul chip e ciò che è una referenza cloud, evitando di trarre conclusioni errate sulla disponibilità offline del dato.

Analisi

Integrità del File System (Proprietary OS)

I produttori (soprattutto in ambito Android) modificano pesantemente il sistema operativo (ONEUI, ColorOS).

La Criticità: Gli strumenti forensi potrebbero non interpretare correttamente il file system di un modello specifico, portando a una "falsa" integrità o a errori di parsing (interpretazione errata di date e orari).

Analisi

La fase finale è quella dove l'analista deve dedicare la massima attenzione nello studio dei report generati dai software di acquisizione, poiché secondo l'attuale giurisprudenza, che sottolinea l'importanza di una scansione temporale specifica per le fasi di estrapolazione (copia mezzo) e analisi selettiva (copia fine), che avvengono nel rispetto del principio di proporzionalità.

Questa raddoppia di fatto i tempi di analisi, di fatti si devono avere quesiti specifici dei dati da ricercare, senza omettere qualora vengono ravvisati reati differenti da quelli che si stanno contestando all'indagato, ed avvisando nel caso della consulenza tecnica il PM che ha conferito l'incarico che suggerirà lo stralcio di quei dati.

Ordine degli Ingegneri
della Provincia di Palermo

Grazie per l’attenzione