

A hand holding a smartphone with a stylus, overlaid with text. The background is a blurred image of a person using a smartphone. The text is white and semi-transparent, overlaid on the image. The text reads: MSAB, CASO DI STUDIO, and Caso di studio con la Procura di Monza: recupero di prove cruciali da uno smartphone non funzionante. The year 2026 is in the bottom right corner.

MSAB

CASO DI STUDIO

Caso di studio con la Procura di
Monza: recupero di prove cruciali da
uno smartphone non funzionante

2026

Dal 2018, il V. Brig. Della Guardia di Finanza Salvatore Carannante, specialista in informatica forense presso la Procura di Monza, si occupa di indagini informatiche e relative ai dispositivi mobili, assumendo in seguito la responsabilità di guidare le attività forensi dell'unità, tra cui l'estrazione di prove, le indagini online e la collaborazione tra le forze dell'ordine.

Un caso particolarmente complesso ha messo in luce le sfide operative affrontate nell'ambito della digital forensics. Gli investigatori avevano il compito di esaminare uno smartphone collegato a un'indagine su abusi su minori. Il dispositivo, il moderno dispositivo Android era in condizioni critiche: la batteria era completamente scarica, non si accendeva e non erano visibili indicatori di ricarica. Di conseguenza, era impossibile accedere al sistema con metodi convenzionali.

Ciò comportava un alto rischio di perdita permanente dei dati. Senza strumenti forensi specializzati, l'accesso alla memoria interna del dispositivo sarebbe stato altamente improbabile. Allo stesso tempo, tutte le procedure dovevano rispettare rigorosi standard forensi, tra cui l'integrità dei dati, la ripetibilità, la tracciabilità e la conservazione della catena di custodia.

Per superare gli ostacoli tecnici presentati dal dispositivo, lo specialista forense ha eseguito un'estrazione forense fisica utilizzando MSAB XRY Pro.

Il dispositivo era in condizioni critiche: la batteria era completamente scarica, non si accendeva e non erano visibili indicatori di ricarica. Di conseguenza, era impossibile accedere al sistema con metodi convenzionali.

Questo metodo consente agli investigatori di acquisire una copia completa, bit per bit, della memoria interna del dispositivo. L'estrazione produce un'immagine forense completa del sistema di archiviazione, consentendo il recupero e l'analisi sia dei dati visibili che di quelli nascosti. Durante il processo vengono generati valori di hash crittografici (MD5 e SHA) per verificare l'integrità dell'immagine forense e garantire che le prove rimangano inalterate per tutta la durata delle indagini.

La tecnica ha permesso di recuperare dati attivi, contenuti cancellati, frammenti residui di informazioni e artefatti situati in aree di memoria precedentemente non allocate. Queste funzionalità sono particolarmente importanti quando non è possibile accedere a un dispositivo tramite il suo sistema operativo o quando i metodi di estrazione convenzionali falliscono.

Il V. Brig. Salvatore Carannante sottolinea che l'efficienza operativa della piattaforma ha svolto un ruolo fondamentale nelle indagini. Le estrazioni possono essere eseguite rapidamente, comprese le acquisizioni fisiche da dispositivi che altri strumenti forensi non sono in grado di elaborare. Anche la successiva fase di analisi risulta accelerata grazie all'ambiente XAMN, che consente agli investigatori di esaminare in modo significativo grandi volumi di dati estratti.

Altrettanto importante è l'interfaccia del software, progettata per guidare gli utenti attraverso il processo di estrazione:



Copia completa, bit per bit, della memoria interna del dispositivo.

“Il software è autoguidato con un’interfaccia intuitiva anche per chi non l’ha mai utilizzata. Il log spiega esattamente cosa sta facendo e come: è essenziale per la reportistica e il controllo giudiziario.”

Un altro elemento chiave del flusso di lavoro è il sistema di registrazione integrato nel software:

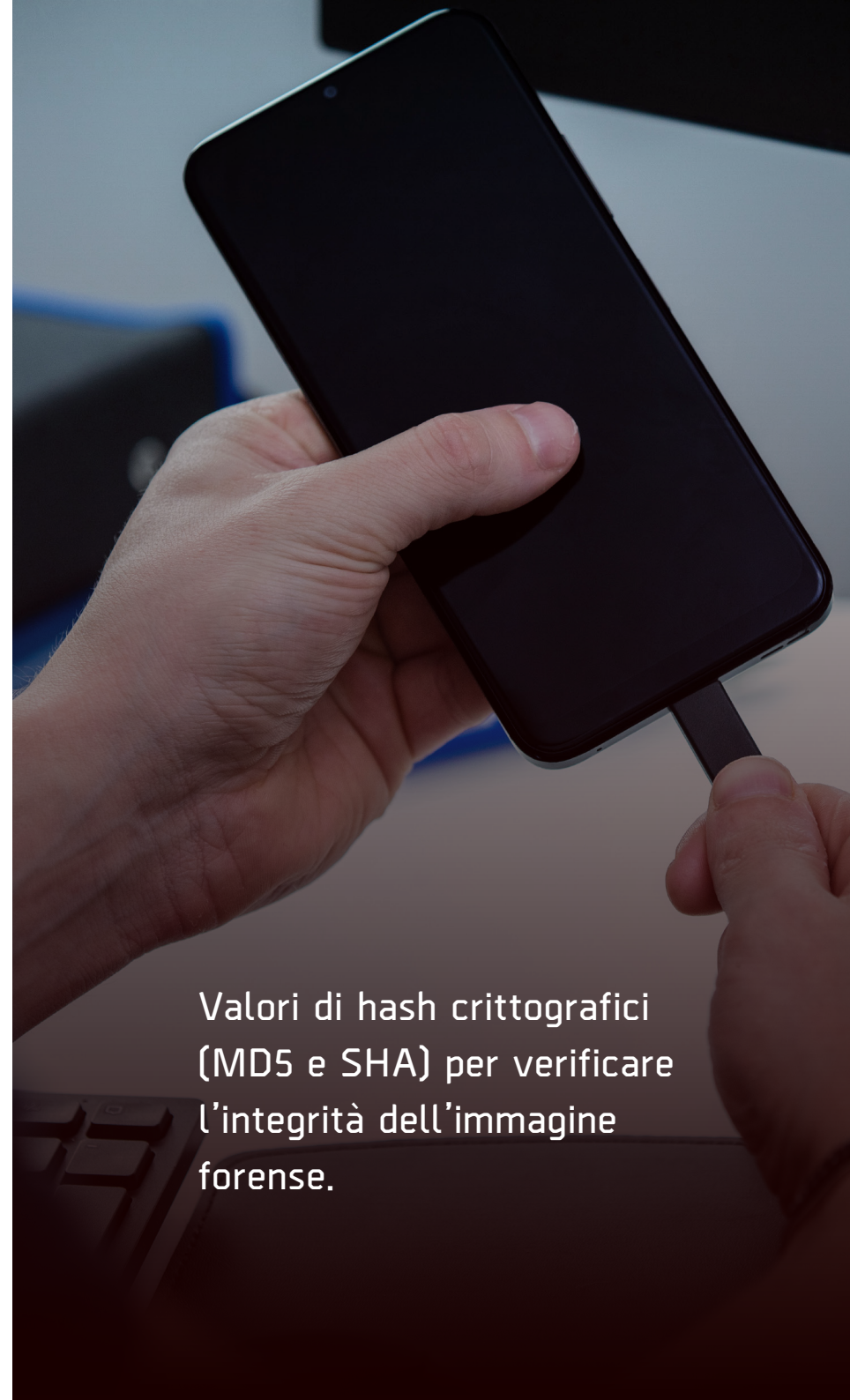
“I log sono fondamentali. Con altri software, gli errori sono spesso poco chiari ed è difficile capire perché un’estrazione fallisca. MSAB fornisce registri dettagliati, consentendomi di risolvere i problemi, verificare e mantenere il controllo dei dati sensibili senza condividerli esternamente.”

Questi registri forniscono agli investigatori un riferimento affidabile quando redigono relazioni tecniche e presentano i risultati nei procedimenti giudiziari.

L'estrazione fisica ha fornito, in ultima analisi, prove decisive per le indagini.

L'analisi dell'immagine forense ha rivelato messaggi di chat, file multimediali e tracce delle applicazioni collegate al presunto autore del reato. I metadati associati a questi file hanno permesso agli investigatori di ricostruire una cronologia delle comunicazioni tra la vittima e l'individuo responsabile dell'abuso.

È importante sottolineare che il processo forense ha consentito anche il recupero di dati cancellati che altrimenti sarebbero rimasti inaccessibili. Questi frammenti recuperati hanno contribuito a una ricostruzione cronologica più completa degli eventi e hanno rafforzato la base probatoria dell'indagine.



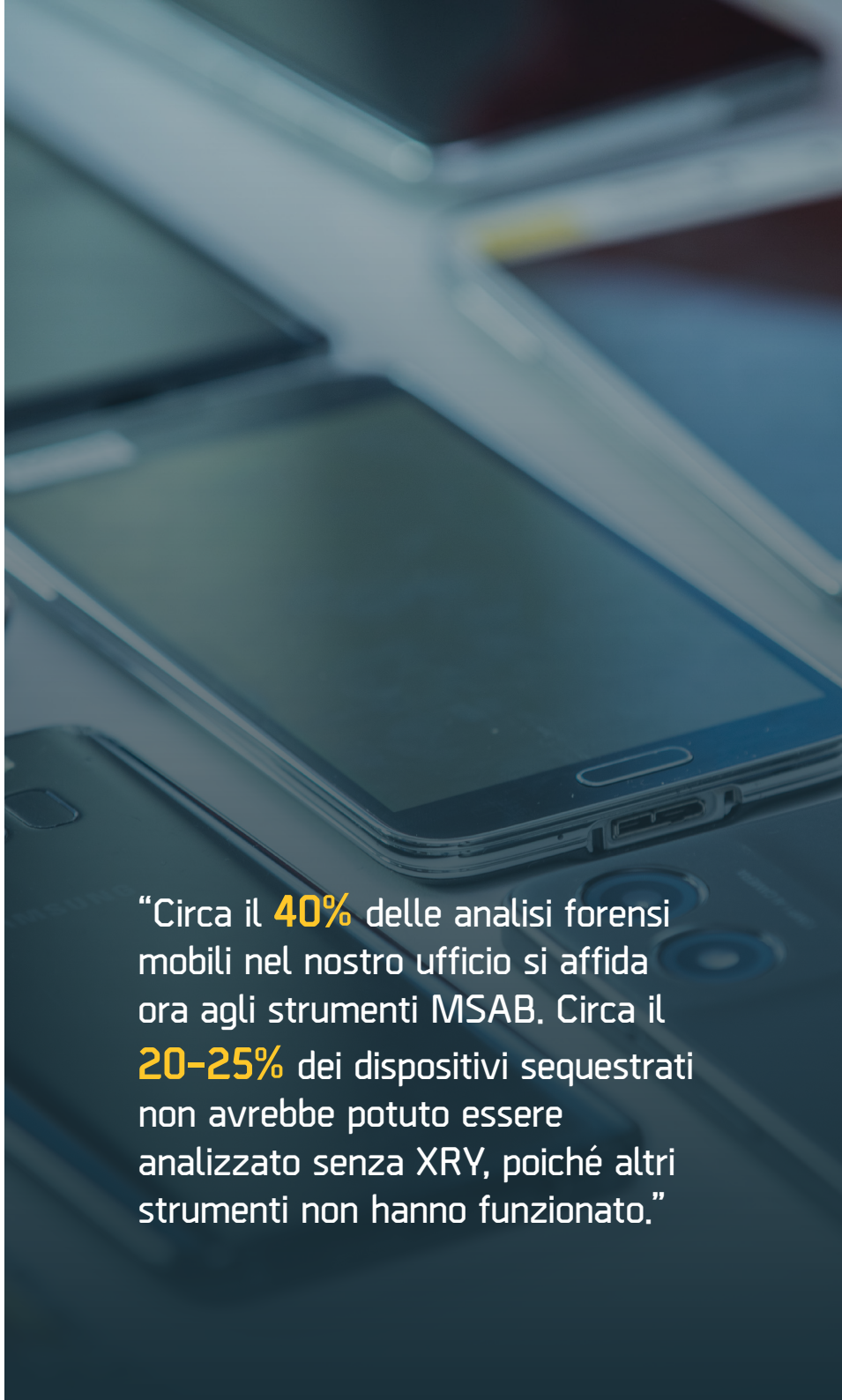
Valori di hash crittografici (MD5 e SHA) per verificare l'integrità dell'immagine forense.

Per il V. Brig. Salvatore Carannante, il momento in cui è stato possibile accedere con successo al dispositivo ha rappresentato una svolta nel caso:

“Quando ho collegato il dispositivo, l'ho estratto con XRY e ho visto i dati, quella è stata la svolta. Gli altri dispositivi contenevano solo informazioni parziali, che non erano sufficienti per attribuire le responsabilità all'autore del reato.”

L'indagine ha dimostrato come strumenti forensi mobili avanzati possano consentire agli investigatori di accedere a dati da dispositivi che inizialmente sembrano inaccessibili. Consentendo l'acquisizione e l'analisi della memoria completa del dispositivo nel rispetto di rigorosi standard forensi, la squadra investigativa è riuscita a prevenire la perdita di prove cruciali e a far progredire in modo significativo un'indagine penale delicata.

“Circa il 40% delle analisi forensi mobili nel nostro ufficio si affida ora agli strumenti MSAB. Circa il 20-25% dei dispositivi sequestrati non avrebbe potuto essere analizzato senza XRY, poiché altri strumenti non hanno funzionato.”



“Circa il **40%** delle analisi forensi mobili nel nostro ufficio si affida ora agli strumenti MSAB. Circa il **20-25%** dei dispositivi sequestrati non avrebbe potuto essere analizzato senza XRY, poiché altri strumenti non hanno funzionato.”