PROCURA DELLA REPUBBLICA

PRESSO IL TRIBUNALE DI SASSARI

“ALLEGATO TECNICO”

ALL’APPENDICE DELLA DIRETTIVA IN MATERIA DI ACQUISIZIONE DI DATI DIGITALI

PROTOCOLLO OPERATIVO PER LA POLIZIA GIUDIZIARIA

PREMESSA E FUNZIONE DELL’ALLEGATO TECNICO

Il presente allegato tecnico costituisce parte integrante dell’Appendice alla direttiva in materia di acquisizione di dati digitali – Protocollo operativo per la polizia giudiziaria, adottata dalla Procura della Repubblica presso il Tribunale di Sassari, e ne integra le disposizioni sotto il profilo specialistico, con particolare riguardo alle modalità di repertamento, conservazione, acquisizione e documentazione delle fonti di prova digitali.

Esso ha finalità esclusivamente tecnico-operative ed è volto a fornire alla polizia giudiziaria criteri uniformi di condotta nell’esecuzione delle attività di perquisizione informatica, nel rispetto delle garanzie previste dal codice di procedura penale, dei principi di integrità, immodificabilità, tracciabilità e verificabilità della prova digitale, nonché delle esigenze di proporzionalità e minimizzazione dell’interferenza sui dati non pertinenti.

Le presenti disposizioni non sostituiscono la valutazione del caso concreto, né esauriscono tutte le possibili situazioni operative. In presenza di dubbi tecnici, criticità procedurali, dispositivi non convenzionali, sistemi cifrati, infrastrutture critiche, apparati speciali o contesti che presentino rischio di alterazione, distruzione o dispersione del dato, la polizia giudiziaria sospende ogni iniziativa non indispensabile e si raccorda immediatamente con il pubblico ministero procedente.

1. AMBITO DI APPLICAZIONE

Il presente allegato si applica alle attività concernenti dispositivi e sistemi suscettibili di contenere dati digitali, inclusi, a titolo esemplificativo e non esaustivo, telefoni cellulari, smartphone, tablet, computer desktop e portatili, server, supporti di memoria esterni, chiavette USB, memory card, unità SSD e HDD, sistemi cloud accessibili dal dispositivo, apparati IoT, dispositivi indossabili, SIM, eSIM e altri sistemi elettronici in grado di memorizzare, elaborare o trasmettere dati.

Le attività disciplinate comprendono l’identificazione della fonte di prova digitale, il repertamento fisico, l’isolamento del dispositivo, l’eventuale acquisizione live, l’estrazione

della copia-mezzo, la successiva selezione dei dati pertinenti ai fini della copia-fine, la documentazione delle operazioni e la conservazione in sicurezza dei reperti e delle copie.

2. PRINCIPI TECNICI GENERALI

In tutte le operazioni la polizia giudiziaria adotta le cautele necessarie ad evitare alterazioni del dato e a consentire la successiva verifica delle attività compiute.

L'operatore deve sempre privilegiare, quando tecnicamente praticabile, la metodologia meno invasiva idonea a garantire la preservazione del dato e l'efficacia investigativa. La scelta tra acquisizione integrale, acquisizione selettiva, acquisizione live o mero sequestro cautelativo del dispositivo deve essere effettuata sulla base del titolo giuridico disponibile, del contesto operativo, della tipologia del sistema, dell'eventuale presenza di cifratura, del rischio di cancellazione remota e della disponibilità di adeguata strumentazione tecnica.

Ogni operazione deve essere integralmente tracciata nel verbale, con indicazione delle ragioni che hanno giustificato le scelte tecniche adottate, specie nei casi in cui si sia reso necessario operare sul dispositivo originale acceso, in deroga al criterio ordinario della duplicazione forense in condizioni di minima alterazione.

3. CLASSIFICAZIONE TECNICA DELLE COPIE

Ai fini del presente allegato, per **copia manuale o live** deve intendersi la visualizzazione diretta dei contenuti del dispositivo mediante interazione con l'interfaccia utente, documentata, se possibile, mediante ripresa foto-video. Tale modalità ha carattere residuale e va limitata alle ipotesi in cui sia necessaria per salvaguardare dati altrimenti non acquisibili, ovvero per esigenze investigative urgenti autorizzate dall'autorità procedente.

Per **copia logica** deve intendersi l'estrazione dei dati resi accessibili dal sistema operativo o dalle applicazioni, con esclusione, di regola, delle aree non allocate e dei dati cancellati non più indicizzati. Essa può assumere forma semplice, selettiva o avanzata, a seconda dell'ampiezza dell'estrazione.

Per **copia file system o full file system** deve intendersi l'acquisizione estesa del contenuto strutturato del dispositivo, comprensiva dei file di sistema, dei database applicativi, dei log e delle ulteriori componenti accessibili mediante strumenti forensi evoluti.

Per **copia fisica o bit-by-bit** deve intendersi l'acquisizione dell'intero contenuto della memoria del dispositivo a livello grezzo, comprensiva delle aree allocate, non allocate e dello slack space, nei limiti consentiti dall'architettura hardware e dal sistema di protezione o cifratura presenti.

Per **copia-mezzo** deve intendersi la duplicazione forense, integrale o quanto più estesa possibile, del contenuto del dispositivo o della memoria di interesse, effettuata senza selezione investigativa del dato.

Per **copia-fine** deve intendersi la selezione dei soli dati pertinenti all'oggetto dell'indagine, estratti dalla copia-mezzo secondo i criteri e le parole chiave indicati dal pubblico ministero.

4. REGOLE GENERALI DI CONDOTTA OPERATIVA

Le attività di ricerca finalizzate all'individuazione delle fonti di prova digitali devono essere eseguite nel rispetto delle fasi individuate dalla norma ISO 27037:2012, che comprendono

l'identificazione delle potenziali fonti di prova digitali, il repertamento fisico, l'acquisizione del contenuto e la successiva preservazione dei reperti e dei dati acquisiti.

Prima di procedere a qualsiasi attività di manipolazione, la polizia giudiziaria deve effettuare una completa e puntuale documentazione dello stato dei luoghi e del dispositivo. In tale fase devono essere rilevati e descritti la collocazione del reperto, l'eventuale presenza di cavi collegati o dispositivi connessi, lo stato degli schermi, la presenza di notifiche visibili, i sistemi di sicurezza attivi e le condizioni esterne del dispositivo, con specifica evidenza di eventuali danneggiamenti, sigilli o accessori pertinenti. La documentazione deve essere preferibilmente supportata da rilievi fotografici e/o videoregistrazioni.

Deve essere prestata particolare attenzione alla conservazione degli elementi di prova di natura fisica, adottando ogni cautela idonea a evitare alterazioni o contaminazioni della scena del crimine. Prima di qualsiasi intervento sul dispositivo, deve essere valutata la necessità di procedere alla rilevazione di tracce utili sulla componente fisica, anche mediante accertamenti dattiloscopici o altri rilievi tecnico-scientifici.

È fatto divieto di consentire al soggetto sottoposto a perquisizione o a terzi di mantenere la disponibilità materiale del dispositivo una volta individuato. Eventuali attività di sblocco o forme di collaborazione devono essere previamente autorizzate e integralmente documentate a verbale, con puntuale indicazione delle modalità operative adottate.

L'operatore deve valutare sin dalle fasi iniziali la possibile presenza di sistemi di cifratura, di procedure di cancellazione automatica, di meccanismi di riavvio protetto o reset da remoto, nonché di connessioni a servizi cloud o di sistemi di sblocco basati su token, dispositivi prossimi, reti fidate o fattori biometrici. Tutte le attività devono essere documentate in modo completo, cronologico e verificabile, con indicazione degli orari, degli operatori intervenuti e delle operazioni effettuate. Deve inoltre essere descritto lo stato di ciascun dispositivo, con particolare riferimento alla condizione di accensione o spegnimento e alla presenza di misure di sicurezza attive.

Qualora emerga la necessità di acquisire dati da account cloud, servizi sincronizzati o piattaforme remote accessibili dal dispositivo, l'attività deve essere preventivamente coordinata con il pubblico ministero, sia ai fini dell'eventuale emissione di ordini di conservazione ai sensi dell'art. 254-bis c.p.p., sia per la definizione della corretta sequenza operativa tra cinturazione dell'account, acquisizione dei dati remoti e preservazione del contenuto locale del dispositivo.

5. DISPOSITIVI MOBILI – Criteri tecnico-operativi

Nell'ambito dei dispositivi mobili, la polizia giudiziaria deve procedere, in via preliminare, all'identificazione del terminale, annotando tutti gli elementi utili alla sua univoca individuazione, tra cui marca, modello, IMEI, numero seriale, nonché la presenza di SIM fisiche, eSIM, eventuali memorie esterne, lo stato di accensione e di blocco, il livello di carica, la presenza di accessori collegati e ogni ulteriore elemento rilevante ai fini investigativi.

Il dispositivo deve essere isolato dalle comunicazioni di rete nel più breve tempo possibile, al fine di prevenire fenomeni di sincronizzazione, alterazione o cancellazione remota dei dati. L'isolamento deve essere realizzato, in relazione alle caratteristiche del caso concreto, mediante attivazione della modalità aereo, disattivazione delle interfacce radio, inserimento in appositi contenitori schermati ovvero mediante l'adozione di ulteriori misure idonee a garantire l'isolamento elettromagnetico. Qualora sussista il rischio che la modalità aereo non

sia sufficiente a impedire il traffico dati, o che specifici dispositivi consentano comunque la ricezione di comandi remoti tramite reti alternative, deve essere privilegiato l'isolamento fisico del terminale.

Nel caso in cui il dispositivo sia rinvenuto acceso e sbloccato, la polizia giudiziaria deve valutare con priorità l'opportunità di mantenerlo in tale stato, adottando, ove possibile e nei limiti consentiti, ogni misura idonea a impedirne il blocco automatico. In tale fase devono essere documentati lo stato dello schermo, le applicazioni aperte, le sessioni attive, le comunicazioni visibili, gli account configurati, le notifiche e ogni altro dato volatile di immediato interesse investigativo. Qualora non siano disponibili le credenziali di accesso o sussista il rischio di perdita delle condizioni di accessibilità, può rendersi necessario procedere ad acquisizione in modalità live ovvero al collegamento immediato a idonea strumentazione forense, purché l'attività sia adeguatamente motivata e integralmente documentata.

Qualora il dispositivo sia acceso ma in stato di blocco, deve essere valutato se esso si trovi in una fase successiva al primo sblocco utile all'utente, tale da consentire una più ampia capacità di acquisizione forense. In presenza di incertezza, il dispositivo deve essere mantenuto alimentato e, ove possibile, collegato a idonea strumentazione di conservazione forense, evitando operazioni di spegnimento o riavvio che possano compromettere l'accesso ai dati.

Nel caso in cui il dispositivo sia spento, la polizia giudiziaria deve valutare l'opportunità di procedere alla sua accensione tenendo conto del titolo giuridico, delle indicazioni dell'autorità procedente, della disponibilità di credenziali di accesso, del rischio di attivazione di meccanismi di protezione e della disponibilità di strumenti tecnici idonei all'acquisizione. In assenza di condizioni favorevoli, il dispositivo deve essere repertato, posto in sicurezza e destinato a successive attività specialistiche.

Le memorie esterne, le SIM, le eSIM e ogni altro modulo associato al terminale devono essere oggetto di autonomo repertamento, etichettatura e documentazione, anche fotografica, e devono essere conservati separatamente, con indicazione dei dati identificativi e delle relazioni con il dispositivo principale.

5.1 Possibili casi concreti

Con riferimento ai dispositivi mobili dotati di sistema operativo Apple iOS, qualora lo schermo risulti bloccato mediante codice di sicurezza, può essere possibile attivare la modalità aereo accedendo al centro di controllo mediante scorrimento del dito sullo schermo e selezionando l'apposita icona. Tale operazione non è tuttavia sempre garantita, in quanto sui dispositivi più recenti l'accesso a tali funzionalità può essere subordinato allo sblocco del terminale.

Per i dispositivi dotati di sistema operativo Android, l'attivazione della modalità aereo può avvenire, a seconda della configurazione del dispositivo, mediante pressione prolungata del tasto di accensione ovvero tramite accesso al menu rapido mediante scorrimento sullo schermo e selezione dell'apposita icona. Anche in questo caso, la possibilità di attivare tale funzione può risultare limitata dalla presenza di meccanismi di blocco, quali PIN, password o sequenza grafica.

In ogni caso, l'operatore deve verificare in concreto la possibilità di attivare la modalità aereo senza procedere allo sblocco del dispositivo e, qualora ciò non sia possibile o non sia ritenuto affidabile ai fini dell'isolamento, deve privilegiare l'adozione di misure di isolamento fisico

del terminale, anche mediante l'impiego di dispositivi schermanti idonei a impedire le comunicazioni radio.

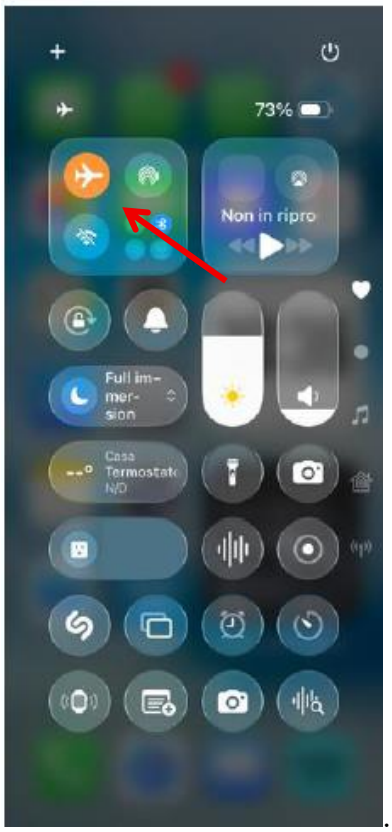

Figura 1- Modelli iOS

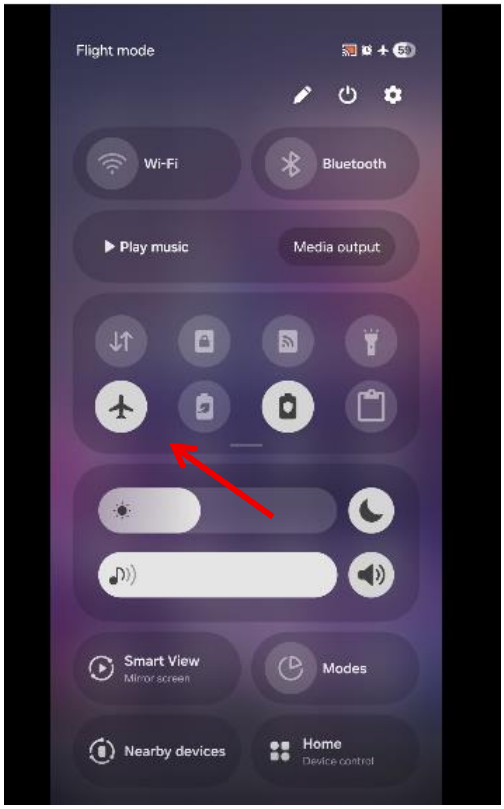

Figura 2- Modelli Android

5.2 Ulteriori indicazioni operative e cautele tecniche

Alcuni modelli di smartphone di recente generazione, sia basati su sistema operativo iOS sia Android, sono soggetti a politiche di sicurezza che determinano il riavvio automatico del dispositivo a seguito di un periodo prolungato di inattività. In tali ipotesi, ove tecnicamente possibile, la polizia giudiziaria deve procedere senza ritardo all'esecuzione della copia forense sul posto ovvero al collegamento del dispositivo a idonea strumentazione forense, al fine di preservarne lo stato operativo ed evitare l'attivazione di tali meccanismi.

I medesimi dispositivi possono risultare suscettibili di ricevere comandi di reset remoto anche qualora posti in modalità aereo o in stato di apparente spegnimento, mediante canali di comunicazione alternativi, inclusi Bluetooth, NFC o ulteriori reti di prossimità. In presenza di tale rischio, il dispositivo deve essere immediatamente isolato mediante busta schermata di tipo Faraday o altro presidio idoneo; ogni attività di acquisizione deve essere eseguita in condizioni tecniche tali da escludere interferenze o alterazioni da remoto.

Per taluni dispositivi dotati di particolari misure di sicurezza o di funzionalità assimilabili ai cosiddetti criptofonini, il reset o la compromissione dei dati può essere determinato anche da operazioni apparentemente ordinarie, quali l'attivazione della modalità aereo, il riavvio del terminale o il collegamento a strumentazione forense. In tali circostanze, la polizia giudiziaria deve adottare la soluzione tecnica meno invasiva e maggiormente conservativa, dandone espressamente atto nel verbale.

La polizia giudiziaria, nel caso fosse possibile, deve acquisire e annotare tutte le informazioni utili relative a profili di posta elettronica, account social, credenziali eventualmente note, appunti, supporti cartacei o altri elementi dai quali possano desumersi dati di accesso o informazioni rilevanti ai fini dell'indagine, anche mediante richiesta al soggetto che ha la disponibilità del dispositivo.

Qualora si proceda al sequestro di un dispositivo utilizzato, anche promiscuamente, da conviventi, familiari dell'indagato o da altri soggetti, deve essere data espressa indicazione nel verbale dell'identità dell'utilizzatore o dei possibili utilizzatori, ove noti.

La polizia giudiziaria deve richiedere al soggetto che ha la disponibilità del dispositivo le eventuali credenziali di accesso o i codici di sblocco, dandone atto nel verbale unitamente all'esito della richiesta. In caso di mancata collaborazione e qualora il sistema di protezione consista in una sequenza grafica, può essere valutata, con adeguata cautela tecnica e dandone atto nel verbale, l'osservazione del display mediante luce radente al fine di rilevare eventuali tracce compatibili con la sequenza di sblocco. Qualora il soggetto dichiari l'assenza di sistemi di sicurezza, tale circostanza deve essere verificata, per quanto possibile, mediante accertamenti tecnici.

Nel caso di dispositivo rinvenuto acceso, lo stato del terminale deve essere documentato mediante rilievi fotografici e, ove opportuno, videoregistrazioni, dando atto della presenza o assenza di blocchi allo schermo, delle notifiche visibili, delle sessioni attive e di ogni ulteriore elemento utile.

Deve essere verificata l'eventuale presenza di sistemi di sblocco automatico, inclusi token Bluetooth, dispositivi fidati, funzionalità di smart lock o analoghi meccanismi di prossimità, con espressa indicazione delle risultanze nel verbale.

Qualora il dispositivo sia rinvenuto acceso e sbloccato e non siano disponibili le credenziali di accesso, la polizia giudiziaria deve verificare senza ritardo la presenza di sistemi di protezione e, ove tecnicamente possibile, adottare le misure necessarie a mantenerlo nello stato di sblocco. Qualora sussista il rischio di perdita dell'accesso o il sospetto della presenza di particolari meccanismi di sicurezza, può procedersi, nei limiti consentiti, ad acquisizione manuale ovvero in modalità live, con puntuale descrizione delle operazioni nel verbale.

Qualora siano disponibili credenziali valide, deve essere verificata la possibilità di procedere immediatamente all'acquisizione dei dati mediante gli strumenti tecnici a disposizione. In caso positivo, la copia forense deve essere eseguita sul posto. In caso contrario, ove non sussistano rischi di alterazione, perdita o cancellazione dei dati, il dispositivo può essere spento e repertato per successive attività di acquisizione.

Nel caso in cui il dispositivo acceso risulti bloccato e non siano disponibili i codici di sblocco, qualora esso si trovi in stato successivo al primo sblocco utile (AFU – After First Unlock), non si deve procedere allo spegnimento né al riavvio e il terminale deve essere mantenuto alimentato fino al collegamento con idonea strumentazione forense. Qualora il dispositivo si trovi in stato anteriore al primo sblocco utile (BFU – Before First Unlock), può essere valutato lo spegnimento, salvo diversa valutazione tecnica o investigativa. Qualora non sia possibile determinare con immediatezza lo stato del dispositivo, esso deve essere mantenuto alimentato fino alla verifica mediante adeguata strumentazione forense.

Nel caso di dispositivo rinvenuto spento, la polizia giudiziaria deve valutare la condotta operativa da adottare in relazione al contesto investigativo, alle esigenze dell'indagine, alla disponibilità di idonea strumentazione tecnica, alle indicazioni dell'autorità giudiziaria, nonché all'eventuale disponibilità delle credenziali di sblocco.

Ove tecnicamente opportuno e compatibile con le esigenze di preservazione del dato, la polizia giudiziaria può procedere, previa rimozione dell'eventuale SIM fisica e delle memorie rimovibili presenti, all'accensione del dispositivo al solo fine di verificare la presenza di misure di sicurezza. In tale fase, ove necessario, può interloquire con il soggetto che ha la disponibilità del dispositivo, dandone atto nel verbale. In ogni caso, si applicano, per quanto compatibili, le disposizioni previste per i dispositivi rinvenuti in stato acceso.

Il dispositivo deve essere etichettato secondo una nomenclatura idonea a garantirne l'univoca identificazione nell'ambito del materiale sequestrato, con puntuale annotazione nel verbale. Il repertamento deve comprendere, di regola, la memoria interna, le eventuali memorie esterne rimovibili, nonché le SIM e le eSIM associate.

Devono essere altresì repertati, ove disponibili e pertinenti, i cavi di connessione, i caricabatteria, eventuali supporti software di interfaccia, ulteriori batterie o memorie, la documentazione relativa all'utenza, le confezioni originali delle SIM e ogni appunto, supporto cartaceo o documento dal quale possano desumersi credenziali, codici o ulteriori informazioni utili ai fini dell'indagine.

Con riguardo alle SIM, la polizia giudiziaria deve acquisire e annotare, ove disponibili, i dati identificativi, inclusi ICCID e ulteriori codici pertinenti. Ove possibile, può essere richiesto al gestore il codice PIN della SIM, distinto da quello di sblocco del dispositivo. Deve essere altresì dato atto nel verbale dell'avviso rivolto al soggetto di astenersi dal richiedere il duplicato o la portabilità della SIM.

Il dispositivo e i relativi accessori devono essere posti immediatamente in sicurezza mediante idonee misure di protezione contro manomissioni, danneggiamenti o alterazioni, anche mediante utilizzo di buste antieffrazione, contenitori schermati o buste di Faraday, ove necessario in relazione alla tipologia del reperto.

Può essere allegata agli atti apposita scheda reperto recante gli elementi identificativi del dispositivo, dei supporti associati e delle attività eseguite, secondo i modelli esemplificativi del presente documento.

6. ACQUISIZIONE FORENSE DI DISPOSITIVI MOBILI

L'acquisizione forense dei dispositivi mobili deve essere eseguita, di regola, mediante l'impiego di strumenti specialistici riconosciuti, aggiornati e idonei al caso concreto, individuando la modalità di estrazione più adeguata in relazione al modello del dispositivo, al sistema operativo, alla versione software e allo stato di protezione del terminale.

Quando tecnicamente possibile, l'operatore deve privilegiare un approccio di acquisizione progressiva, iniziando da modalità meno invasive e valutando successivamente la praticabilità di estrazioni più estese. Resta ferma la necessità di documentare integralmente ogni attività svolta, inclusi i tentativi non riusciti, nonché di dare atto che l'interazione con i software di acquisizione può determinare la generazione di tracce sul dispositivo.

Devono essere annotati nel verbale, con precisione e completezza, lo strumento utilizzato, il relativo produttore, la versione del software, la tipologia di estrazione eseguita, l'eventuale impiego di moduli hardware accessori, l'esito dell'operazione, il formato dei file generati, il percorso di salvataggio dei dati, i valori hash calcolati e ogni eventuale criticità riscontrata nel corso delle operazioni. Qualora si proceda ad acquisizione manuale o in modalità live, le schermate visualizzate nel corso delle operazioni devono essere documentate mediante screenshot o videoregistrazione dello schermo; tale documentazione è allegata al verbale e conservata unitamente alla copia-mezzo.

Nel caso di dispositivi protetti da cifratura, l'operatore deve acquisire, ove possibile, le chiavi, i token, le credenziali, i codici di sblocco, i backup associati e ogni ulteriore informazione utile a consentire la successiva accessibilità e intellegibilità del dato. È fatto divieto di effettuare tentativi ripetuti e non autorizzati di accesso che possano determinare il blocco del dispositivo, l'incremento dei tempi di attesa o la cancellazione automatica del contenuto.

7. COMPUTER E SISTEMI INFORMATICI – Criteri tecnico-operativi

Nel caso di computer o sistema informatico rinvenuto acceso, la polizia giudiziaria deve valutare preliminarmente la condotta operativa da adottare in relazione al contesto investigativo, alle caratteristiche del sistema, alle competenze tecniche disponibili, alla strumentazione utilizzabile e alle disposizioni impartite dall'autorità giudiziaria procedente.

La polizia giudiziaria può procedere allo spegnimento del dispositivo qualora ritenga preferibile rinviare l'acquisizione dei dati a un momento successivo. Lo spegnimento deve essere eseguito, di regola, mediante la procedura prevista dal sistema operativo; qualora ciò non sia possibile o risulti sconsigliabile nel caso concreto, può procedersi all'interruzione dell'alimentazione, dandone atto nel verbale. La scelta della modalità di spegnimento deve tenere conto del rischio di danneggiamento del sistema derivante da interruzioni improvvise, nonché della possibilità che lo spegnimento ordinato attivi processi automatici idonei ad alterare o cancellare i dati.

Prima di procedere allo spegnimento, deve essere valutata l'eventuale presenza di sistemi di cifratura, in quanto la perdita dello stato operativo può compromettere o rendere non immediatamente intellegibile la successiva acquisizione dei dati. Ogni informazione disponibile in ordine alla presenza di volumi cifrati, chiavi di accesso, password o ulteriori misure di protezione deve essere acquisita e puntualmente verbalizzata.

Qualora sia ritenuto opportuno mantenere il dispositivo acceso, la polizia giudiziaria deve procedere alla documentazione preliminare dello stato del sistema mediante rilievi fotografici e, ove opportuno, videoregistrazioni, dando atto dello schermo, delle sessioni aperte e degli elementi visibili di interesse investigativo. Ogni successiva interazione con il sistema — navigazione tra cartelle, apertura di applicazioni, consultazione di file — deve essere documentata in modo continuativo mediante screenshot sequenziali o videoregistrazione dello schermo, con annotazione nel verbale delle operazioni compiute nell'ordine in cui sono state eseguite.

Se il dispositivo acceso risulta bloccato, devono essere annotate le informazioni visibili relative agli account presenti nella schermata di accesso e devono essere richieste al soggetto le credenziali di accesso, nonché informazioni in ordine all'eventuale presenza di sistemi di cifratura o di altre misure di sicurezza, dandone atto nel verbale. In caso di mancata disponibilità o di esito negativo delle credenziali fornite, il dispositivo deve essere spento, salvo diversa valutazione tecnica o investigativa. Qualora, invece, siano fornite credenziali valide, la polizia giudiziaria procede all'accesso e alle attività tecniche consentite dal caso concreto.

Una volta ottenuto l'accesso al sistema, la polizia giudiziaria deve valutare, in relazione al contesto investigativo e alle indicazioni dell'autorità procedente, se procedere alla documentazione preliminare delle connessioni di rete e successivamente al loro isolamento, se interrompere immediatamente ogni comunicazione di rete e wireless, ovvero se mantenere temporaneamente attive le connessioni per esigenze investigative o per la natura del sistema esaminato. La scelta adottata deve essere espressamente motivata nel verbale.

La polizia giudiziaria deve acquisire e documentare i programmi in esecuzione, le eventuali comunicazioni attive, le sessioni aperte, le macchine virtuali, le connessioni di rete, gli account utilizzati e ogni altro elemento volatile o suscettibile di rapida alterazione. Ove tecnicamente possibile e rilevante ai fini investigativi, deve procedere all'acquisizione della memoria RAM mediante strumenti forensi idonei, dandone compiuta evidenza nel verbale.

In presenza di sistemi di cifratura attivi, devono essere acquisiti, ove possibile, le chiavi, le credenziali o gli elementi necessari alla successiva decifratura dei dati, inclusi i dati utili al recupero delle chiavi di protezione del sistema.

Ove possibile e consentito, la polizia giudiziaria deve procedere all'acquisizione dei dati dal dispositivo, nonché, se del caso, alla cinturazione degli account cloud o al download dei dati remoti associati. La priorità tra tali attività deve essere determinata in relazione al contesto

investigativo, tenendo conto dell'esigenza di impedire alterazioni dei dati remoti e, al contempo, di preservare i dati presenti localmente sul sistema.

Al termine delle operazioni, il dispositivo deve essere spento mediante la procedura ritenuta più idonea, in relazione alle caratteristiche del sistema e alle esigenze di preservazione della prova.

Qualora il dispositivo sia rinvenuto acceso e già sbloccato, la polizia giudiziaria deve procedere senza ritardo alla documentazione dello stato del sistema e degli elementi rilevanti, potendo altresì procedere, ove necessario, all'acquisizione della memoria volatile, al recupero di eventuali chiavi di cifratura attive, all'acquisizione dei dati cloud e all'estrazione forense dei dati, secondo le priorità imposte dal caso concreto.

L'esame del dispositivo in stato di esecuzione è in particolare indicato nei casi in cui il sistema non sia fisicamente rimovibile, siano presenti programmi o comunicazioni attive, il dispositivo svolga funzioni essenziali o sia connesso a infrastrutture, servizi, sistemi di videosorveglianza o ambienti condivisi, ovvero quando risultino rilevanti i dati volatili o siano presenti volumi cifrati la cui intellegibilità dipenda dal mantenimento dello stato operativo.

Qualora il dispositivo acceso risulti bloccato e la misura di sicurezza non sia nota, la polizia giudiziaria deve procedere alla documentazione dello schermo mediante rilievi fotografici o videoregistrazioni, annotare nel verbale gli identificativi degli account visibili e, salvo diversa valutazione tecnica o investigativa, procedere allo spegnimento del sistema secondo la modalità ritenuta più appropriata.

8. ACQUISIZIONE FORENSE DI COMPUTER E SUPPORTI DI MEMORIA

L'acquisizione dei supporti di memoria rimovibili o fisicamente estraibili deve essere eseguita, di regola, mediante duplicazione forense utilizzando dispositivi di write-blocker hardware idonei a impedire scritture sul supporto originale. Qualora tale modalità non risulti tecnicamente praticabile, la polizia giudiziaria può ricorrere a procedure alternative che garantiscano, per quanto possibile, il controllo delle operazioni di scrittura e la successiva verificabilità dell'attività svolta.

Per i sistemi nei quali lo smontaggio fisico della memoria non sia possibile o risulti idoneo a compromettere l'integrità del dispositivo, l'operatore può procedere mediante tecniche di acquisizione in modalità live ovvero attraverso l'utilizzo di ambienti di avvio forense esterno. Tali attività devono essere eseguite con adeguata competenza specialistica e devono essere integralmente documentate, con specifica indicazione delle modifiche eventualmente apportate alle impostazioni del sistema e dei possibili effetti sull'integrità del dato.

Qualora si renda necessario accedere al BIOS o all'UEFI del sistema al fine di modificare l'ordine di avvio o disabilitare funzionalità di sicurezza che impediscono l'avvio controllato di un ambiente forense, tali operazioni devono essere limitate allo stretto necessario, adeguatamente motivate sotto il profilo tecnico e descritte in modo dettagliato nel verbale.

Al termine delle operazioni di acquisizione devono essere calcolati e annotati i valori hash dell'immagine forense ottenuta, con indicazione dell'algoritmo utilizzato. Ove tecnicamente possibile, deve essere calcolato e annotato anche il valore hash del supporto originale o del contenuto acquisito nella fase iniziale, al fine di consentire la successiva verifica di corrispondenza tra originale e copia.

9. SUPPORTI RIMOVIBILI, SIM, MEMORIE ESTERNE E ALTRI REPERTI DIGITALI

Le unità di memoria rimovibili, ivi comprese chiavette USB, hard disk esterni, SSD esterni, memory card, microSD e dispositivi analoghi, devono essere trattate quali reperti autonomi e, come tali, oggetto di separata descrizione, etichettatura, confezionamento e conservazione.

Qualora tali supporti risultino collegati a un sistema acceso, la loro rimozione deve essere preceduta da una valutazione tecnica in ordine alla possibile presenza di volumi cifrati, file aperti, operazioni di scrittura in corso o processi dipendenti dal dispositivo. Ove la rimozione immediata comporti il rischio di perdita di dati o di compromissione della prova, la polizia giudiziaria deve privilegiare l'esecuzione di una copia forense in situ, prima di procedere al distacco fisico del supporto.

Con riferimento alle SIM e alle eSIM, devono essere acquisiti e annotati, ove tecnicamente rilevabili, i dati identificativi, inclusi ICCID, IMSI, operatore di rete, numero associato, nonché eventuali codici PIN e PUK disponibili. Deve essere inoltre documentata la relazione tra la SIM o eSIM, il dispositivo e l'utenza di interesse investigativo.

10. DATI CLOUD, ACCOUNT, SINCRONIZZAZIONI E CINTURAZIONE

Qualora dal dispositivo risultino accessibili account cloud, caselle di posta elettronica, servizi di backup, piattaforme social, applicazioni di messaggistica, archivi remoti o altre risorse telematiche riconducibili al soggetto, la polizia giudiziaria deve preliminarmente distinguere tra i dati presenti localmente sul dispositivo e quelli conservati, anche solo in parte, su sistemi remoti o nella disponibilità di terzi fornitori di servizi.

L'accesso agli account, la loro messa in sicurezza, il download dei contenuti remoti, le procedure di esportazione o takeout dei dati, nonché ogni attività incidente sulle credenziali o sugli assetti di accesso, devono essere eseguiti esclusivamente nei limiti del titolo legittimante, nel rispetto delle disposizioni impartite dal pubblico ministero e delle eventuali autorizzazioni necessarie.

La scelta tra la prioritaria messa in sicurezza degli account e l'acquisizione dei dati remoti, anche mediante procedure di esportazione o takeout, ovvero l'acquisizione del contenuto locale del dispositivo, deve essere effettuata sulla base di una valutazione motivata del caso concreto. Tale valutazione deve tenere conto del rischio di alterazione, sincronizzazione, cancellazione o dispersione dei dati remoti, del pericolo di perdita dei dati presenti localmente, della presenza di sessioni attive, della volatilità delle credenziali e del rischio di reset remoto.

Ogni accesso, attività di preservazione, esportazione, takeout, download, modifica autorizzata delle credenziali o dei parametri di accesso, nonché ogni operazione di messa in sicurezza degli account, deve essere integralmente documentata nel verbale, con indicazione degli orari, degli account o servizi interessati, delle operazioni eseguite, degli strumenti utilizzati, dei dati acquisiti, dei supporti di destinazione e dei relativi valori hash, ove tecnicamente calcolabili.

11. DOCUMENTAZIONE, VERBALE E TRACCIABILITÀ

Il verbale delle operazioni deve contenere, oltre agli elementi previsti dal protocollo generale, una descrizione tecnicamente adeguata e sufficientemente dettagliata da consentire

la completa ricostruzione delle attività compiute e la verifica della correttezza metodologica delle operazioni svolte.

A tal fine, devono essere riportati lo stato iniziale del dispositivo, le decisioni operative assunte e le relative motivazioni tecniche, nonché gli strumenti utilizzati, con indicazione del produttore e della versione software. Devono inoltre essere descritti l'eventuale impiego di ambienti live o di dispositivi write-blocker, le modifiche inevitabili intervenute sul sistema, i tentativi di acquisizione effettuati, gli esiti conseguiti, i valori hash calcolati, i supporti di destinazione utilizzati, le modalità di sigillatura e conservazione adottate e ogni ulteriore elemento rilevante ai fini della tracciabilità e verificabilità delle operazioni.

Qualora si proceda ad acquisizione manuale ovvero in modalità live, la polizia giudiziaria deve descrivere in modo puntuale e sequenziale le operazioni eseguite, dando atto delle modalità di navigazione, dei contenuti visualizzati, delle schermate documentate, delle applicazioni aperte, degli account osservati, dei file consultati e delle ragioni che hanno reso necessario il ricorso a tale modalità operativa. Gli screenshot o le videoregistrazioni dello schermo acquisiti nel corso delle operazioni costituiscono documentazione forense a tutti gli effetti; il loro valore hash deve essere calcolato e annotato nel verbale, e i file relativi devono essere conservati unitamente alla copia-mezzo.

12. CONSERVAZIONE, CATENA DI CUSTODIA E SICUREZZA

12.1 Catena di custodia

La polizia giudiziaria deve garantire, in ogni fase delle operazioni, la tracciabilità e la continuità della catena di custodia dei dispositivi e dei dati acquisiti, assicurando che ogni passaggio sia documentato, verificabile e riferibile a soggetti determinati.

A tal fine, tutte le attività di presa in carico, trasferimento, analisi, duplicazione e conservazione devono essere annotate nel verbale, con indicazione della data, dell'orario, del luogo, degli operatori intervenuti e delle operazioni eseguite. Deve essere inoltre garantita la corrispondenza tra i reperti acquisiti e quelli successivamente analizzati, mediante idonei sistemi di etichettatura e identificazione univoca.

Tutti i reperti digitali, gli apparati sequestrati, le copie-mezzo, le copie-fine, i supporti contenenti riversamenti, i file hash, i report di acquisizione e ogni ulteriore materiale tecnico prodotto devono essere inseriti in una catena di custodia continua, tracciabile e verificabile, idonea a garantirne la riferibilità e l'integrità.

Ogni operazione di trasferimento, consegna, apertura, duplicazione, sigillatura o accesso deve essere puntualmente documentata, con indicazione della data, dell'orario, dell'operatore, del luogo e della finalità dell'attività.

12.2 Integrità dei dati e verifiche

L'integrità dei dati acquisiti deve essere garantita mediante l'impiego di funzioni di hash crittografico idonee, calcolate sia sui dati originari, ove tecnicamente possibile, sia sulle copie forensi realizzate.

I valori hash devono essere annotati nel verbale e associati in modo univoco ai rispettivi supporti e file acquisiti, al fine di consentire la verifica della corrispondenza tra originale e copia. In caso di duplicazione o trasferimento dei dati, devono essere effettuate verifiche di integrità mediante confronto dei valori hash.

Qualora non sia possibile procedere al calcolo dell'hash sul dispositivo originario, tale circostanza deve essere espressamente indicata nel verbale, unitamente alle motivazioni tecniche e alle misure alternative adottate per garantire l'affidabilità del dato.

Eventuali anomalie riscontrate nel corso delle verifiche di integrità devono essere immediatamente documentate, con indicazione delle possibili cause e delle conseguenze sull'utilizzabilità del dato.

12.3 Conservazione e sicurezza dei supporti

I supporti contenenti i dati acquisiti devono essere custoditi in condizioni tali da impedirne l'alterazione, la manomissione o l'accesso non autorizzato, mediante l'adozione di idonee misure di sicurezza, anche fisica e ambientale.

La conservazione deve avvenire in ambienti sicuri, ad accesso controllato, con adeguata protezione da danneggiamenti fisici, campi elettromagnetici, umidità, urti, temperature elevate e manomissioni. Ogni eventuale apertura, accesso o utilizzo dei supporti deve essere tracciato e documentato.

Le copie forensi devono essere conservate su supporti affidabili e, ove possibile, duplicati, assicurando la separazione tra copia di lavoro e copia di conservazione. L'accesso ai dati deve essere limitato ai soli soggetti autorizzati e deve essere oggetto di tracciamento.

La copia-mezzo non può essere utilizzata per finalità diverse da quelle autorizzate e non può essere restituita, cancellata o alterata se non su disposizione del pubblico ministero. La copia-fine costituisce il supporto destinato alla trasmissione all'autorità procedente, secondo le modalità previste dal protocollo generale.

12.4 Produzione e verificabilità

In sede di produzione all'autorità giudiziaria deve essere garantita la piena corrispondenza tra i dati acquisiti e quelli prodotti, mediante verifica dei valori hash e adeguata documentazione delle operazioni svolte.
Deve essere inoltre assicurata la possibilità di ripetere le operazioni di verifica e analisi, mediante la conservazione degli strumenti utilizzati, delle versioni software impiegate e della documentazione tecnica relativa alle procedure adottate.

13. STRUMENTAZIONE TECNICA

Per l'esecuzione delle attività disciplinate dal presente allegato, la polizia giudiziaria deve impiegare strumenti hardware e software specialistici riconosciuti in ambito forense, purché aggiornati, validati e idonei rispetto alla specifica attività da svolgere.

In ambito mobile possono essere utilizzati, tra gli altri, sistemi di estrazione e analisi quali Cellebrite UFED/Inseyets, GrayKey, MSAB XRY, Oxygen Forensics, Magnet Axiom, nonché ulteriori strumenti equivalenti. In ambito di computer forensics e acquisizione di

supporti di memoria possono essere impiegati duplicatori forensi, dispositivi write-blocker hardware, software di imaging e analisi, sistemi di acquisizione in modalità live e distribuzioni forensi dedicate, a condizione che la scelta dello strumento risulti coerente con le caratteristiche del reperto e con le finalità investigative.

L'indicazione degli strumenti sopra richiamati ha carattere meramente ricognitivo e non tassativo.

Prima dell'impiego operativo, ogni strumento deve essere stato oggetto di validazione, anche mediante test su reperto campione o mediante riferimento a documentazione tecnica del produttore o di enti riconosciuti in ambito forense. L'operatore deve verificare, prima di ogni acquisizione, che lo strumento sia aggiornato all'ultima versione disponibile compatibile con il caso concreto e che risponda correttamente alle operazioni preliminari di test.

Nel verbale devono essere annotati: la denominazione dello strumento, il produttore, la versione del software e dell'eventuale modulo hardware impiegato, nonché l'esito del test preliminare di funzionalità. La documentazione tecnica prodotta automaticamente dallo strumento nel corso delle operazioni — inclusi i report di acquisizione, i file di log e gli audit trail generati dal software — costituisce parte integrante della documentazione forense e deve essere conservata unitamente alla copia-mezzo e trasmessa all'autorità giudiziaria su richiesta.

L'utilizzo concreto deve essere supportato da adeguata competenza tecnica dell'operatore e deve essere integralmente documentato nel verbale, con indicazione delle motivazioni della scelta e delle modalità di impiego.

14. CLAUSOLA FINALE

Il presente allegato tecnico deve essere interpretato ed applicato in modo coordinato con il Protocollo operativo per la polizia giudiziaria e con le direttive impartite, di volta in volta, dal pubblico ministero procedente.

In tutte le situazioni non espressamente disciplinate, nonché nei casi in cui l'operatore ritenga che la concreta esecuzione dell'attività possa comportare un rischio significativo di alterazione del dato, di dispersione della prova, di lesione di diritti fondamentali ovvero di superamento dei limiti del titolo autorizzatorio, la polizia giudiziaria deve sospendere senza ritardo le attività non urgenti e procedere al tempestivo raccordo con il pubblico ministero per le determinazioni del caso.

Il presente allegato tecnico costituisce parte integrante della direttiva in materia di acquisizione di dati digitali adottata dalla Procura della Repubblica di Sassari.

Sassari, 08/04/2026

Il Procuratore della Repubblica
Armando Mammone

ARMANDO MAMMONE
MINISTERO DELLA GIUSTIZIA
08.04.2026 10:37:18 GMT+01:00

GLOSSARIO

Il presente glossario raccoglie i principali termini tecnici utilizzati nell'Allegato Tecnico, con lo scopo di facilitarne la comprensione e garantire uniformità nell'interpretazione delle disposizioni operative.

Account cloud: Profilo utente registrato presso un fornitore di servizi di archiviazione o elaborazione remota (es. iCloud, Google Drive, OneDrive), accessibile tramite Internet e suscettibile di contenere dati sincronizzati con il dispositivo locale.

AFU – After First Unlock: Stato operativo del dispositivo mobile successivo al primo sblocco da parte dell'utente dopo l'accensione. In tale stato le chiavi crittografiche sono attive in memoria e il contenuto del dispositivo è generalmente più accessibile agli strumenti forensi.

Audit trail: Registro cronologico generato automaticamente dal software forense che documenta tutte le operazioni eseguite, consentendo la successiva verifica e ricostruzione dell'attività svolta.

BFU – Before First Unlock: Stato operativo del dispositivo mobile anteriore al primo sblocco da parte dell'utente dopo l'accensione. In tale stato le chiavi crittografiche non sono ancora caricate in memoria e il contenuto del dispositivo è protetto da cifratura completa, con limitata accessibilità forense.

BIOS / UEFI: Firmware di avvio del sistema informatico residente su un chip della scheda madre. Il BIOS (Basic Input/Output System) e il suo successore UEFI (Unified Extensible Firmware Interface) gestiscono l'inizializzazione dell'hardware e l'ordine di avvio del sistema operativo. La modifica temporanea di tali impostazioni può essere necessaria per avviare ambienti forensi esterni.

Busta di Faraday: Contenitore realizzato con materiale conduttore che crea una gabbia elettromagnetica, impedendo al dispositivo al suo interno di ricevere o trasmettere segnali radio (GSM, Wi-Fi, Bluetooth, NFC, GPS). Utilizzata per isolare fisicamente il dispositivo e prevenire cancellazioni o comandi remoti.

Catena di custodia: Sequenza documentata e verificabile di tutte le operazioni di presa in carico, trasferimento, analisi, duplicazione e conservazione dei reperti e dei dati acquisiti, idonea a garantire la riferibilità, l'integrità e la continuità della prova digitale dalla raccolta sino alla produzione in giudizio.

Cifratura (crittografia): Processo di codifica dei dati mediante algoritmi crittografici che li rendono illeggibili in assenza della chiave di decifratura. La cifratura può essere applicata all'intero dispositivo (full-disk encryption), a singole partizioni o a specifici file e applicazioni.

Cinturazione dell'account: Operazione finalizzata a mettere in sicurezza un account cloud o di posta elettronica, impedendo l'accesso non autorizzato, la modifica o la cancellazione dei dati in esso contenuti, tipicamente mediante variazione delle credenziali o attivazione di misure di blocco concordate con il pubblico ministero.

Copia file system / full file system: Acquisizione estesa del contenuto strutturato del dispositivo, comprensiva dei file di sistema, dei database applicativi, dei log e delle ulteriori componenti accessibili mediante strumenti forensi evoluti, inclusi dati non direttamente visibili all'utente.

Copia fisica / bit-by-bit: Acquisizione dell'intero contenuto della memoria del dispositivo a livello grezzo (raw), comprensiva delle aree allocate, non allocate e dello slack space, a prescindere dal sistema operativo. Consente il recupero di dati cancellati e offre la massima completezza forense.

Copia logica: Estrazione dei dati resi accessibili dal sistema operativo o dalle applicazioni, con esclusione, di regola, delle aree non allocate e dei dati cancellati non più indicizzati. Può assumere forma semplice, selettiva o avanzata a seconda dell'ampiezza dell'estrazione.

Copia manuale / live: Modalità di acquisizione consistente nella visualizzazione diretta dei contenuti del dispositivo mediante interazione con l'interfaccia utente, documentata mediante ripresa foto-video. Ha carattere residuale ed è limitata alle ipotesi di urgenza o di impossibilità tecnica di procedere diversamente.

Copia-fine: Selezione dei soli dati pertinenti all'oggetto dell'indagine, estratti dalla copia-mezzo secondo i criteri e le parole chiave indicati dal pubblico ministero. Costituisce il supporto destinato alla trasmissione all'autorità procedente.

Copia-mezzo: Duplicazione forense, integrale o quanto più estesa possibile, del contenuto del dispositivo o della memoria di interesse, effettuata senza selezione investigativa del dato. Costituisce la base dalla quale viene successivamente estratta la copia-fine.

Criptofonino: Dispositivo mobile dotato di particolari misure di sicurezza hardware e software, spesso con sistemi operativi modificati, cifratura avanzata delle comunicazioni e meccanismi di cancellazione automatica dei dati attivabili da remoto o in seguito a tentativi di accesso non autorizzati.

eSIM (Embedded SIM): SIM elettronica integrata direttamente nella scheda madre del dispositivo, non rimovibile fisicamente. Può essere riprogrammata per ospitare profili di diversi operatori telefonici e presenta specifiche criticità in sede di repertamento.

Hash / Valore hash: Sequenza alfanumerica di lunghezza fissa ottenuta applicando una funzione matematica (algoritmo di hash, es. MD5, SHA-1, SHA-256) a un insieme di dati. Funge da impronta digitale crittografica: qualsiasi modifica, anche minima, ai dati produce un hash completamente diverso, consentendo la verifica dell'integrità della copia forense rispetto all'originale.

HDD (Hard Disk Drive): Unità di archiviazione dati basata su dischi magnetici rotanti. A differenza degli SSD, i dati cancellati possono permanere nelle aree non allocate e nello slack space, risultando recuperabili mediante tecniche forensi.

ICCID (Integrated Circuit Card Identifier): Codice univoco di identificazione della scheda SIM, impresso fisicamente sulla scheda stessa e leggibile dal sistema. Consente di identificare la SIM indipendentemente dal dispositivo in cui è inserita.

IMEI (International Mobile Equipment Identity): Codice numerico di 15 cifre che identifica univocamente il dispositivo mobile a livello hardware, indipendentemente dalla SIM inserita. Può essere rilevato dal dispositivo acceso, dall'etichetta fisica o dalla confezione originale.

IMSI (International Mobile Subscriber Identity): Codice univoco memorizzato nella SIM che identifica l'utente presso la rete dell'operatore telefonico. Distinto dall'ICCID (identifica la scheda) e dall'IMEI (identifica il dispositivo).

IoT (Internet of Things): Insieme di dispositivi fisici dotati di sensori, software e connettività di rete che consentono loro di raccogliere e scambiare dati (es. smartwatch, telecamere di sorveglianza, assistenti vocali, dispositivi domotici). Possono costituire fonti di prova digitale rilevanti ai fini investigativi.

ISO 27037:2012: Norma internazionale pubblicata dall'International Organization for Standardization che definisce le linee guida per l'identificazione, la raccolta, l'acquisizione e la preservazione delle prove digitali. Fornisce i principi metodologici di riferimento per le attività di digital forensics.

Modalità aereo: Funzione del dispositivo mobile che disabilita tutte le interfacce di comunicazione wireless (GSM/LTE, Wi-Fi, Bluetooth, NFC). Utilizzata per isolare il dispositivo

dalla rete, sebbene su alcuni modelli recenti possa non garantire l'inibizione completa di tutti i canali di comunicazione.

NFC (Near Field Communication): Tecnologia di comunicazione wireless a corto raggio (tipicamente entro 4 cm) che consente lo scambio di dati tra dispositivi ravvicinati. Può essere utilizzata per trasmettere comandi anche quando il dispositivo è in apparente stato di inattività.

RAM (Random Access Memory): Memoria volatile del sistema informatico nella quale risiedono temporaneamente i dati in elaborazione, i programmi in esecuzione, le chiavi crittografiche attive e le sessioni aperte. Il suo contenuto va perduto allo spegnimento del dispositivo; la sua acquisizione (memory dump) richiede strumenti forensi specialistici e deve essere effettuata a sistema acceso.

Repertamento: Attività di individuazione, raccolta fisica, etichettatura, documentazione e messa in sicurezza del reperto digitale sul luogo del sequestro o della perquisizione, nel rispetto dei principi di integrità e tracciabilità della prova.

SIM (Subscriber Identity Module): Scheda a circuito integrato che memorizza le credenziali di identificazione dell'utente presso la rete dell'operatore telefonico, nonché contatti, messaggi e altri dati. Può essere fisica (rimovibile) o virtuale (eSIM).

Slack space: Spazio residuo all'interno di un cluster del disco che non è occupato dai dati del file corrente. Può contenere frammenti di dati appartenenti a file precedentemente memorizzati in quel cluster, recuperabili mediante analisi forense a livello fisico.

Smart lock: Funzionalità dei dispositivi mobili che consente lo sblocco automatico in presenza di determinate condizioni di fiducia (dispositivo Bluetooth abbinato, rete Wi-Fi nota, posizione geografica, riconoscimento vocale o fisico). La sua presenza deve essere verificata e documentata in sede di repertamento.

SSD (Solid State Drive): Unità di archiviazione dati basata su memoria flash. A differenza degli HDD, la gestione interna dei dati può rendere più difficile il recupero di dati cancellati e impone specifiche cautele nelle procedure di acquisizione forense.

Takeout / Esportazione dati: Procedura offerta dai principali fornitori di servizi cloud (es. Google Takeout, Apple Data & Privacy) che consente di scaricare una copia dei dati associati a un account. Utilizzata in ambito forense per acquisire il contenuto di account remoti nei limiti del titolo legittimante.

Write-blocker: Dispositivo hardware (o software equivalente) interposto tra il supporto originale e il sistema di acquisizione, che impedisce qualsiasi operazione di scrittura sul supporto esaminato, garantendo la sua integrità durante le operazioni di duplicazione forense.