MODULO 02 · AGOSTO 2026

Acquisizione Forense

Copia bit-a-bit, funzioni hash, live forensics e acquisizione in scenari complessi

```
dd if=/dev/sda of=evidence.img • sha256sum evidence.img
```

Al termine del modulo lo studente sarà in grado di

01 · ESEGUIRE

Una copia forense bit-a-bit con write blocker, nei formati RAW, E01 e AFF4, documentandola a verbale

02 · VERIFICARE

L'integrità mediante funzioni hash (MD5, SHA-256), conoscendone proprietà crittografiche e limiti

03 · DECIDERE

La strategia di acquisizione (live o post-mortem) in funzione dell'ordine di volatilità e del contesto giuridico

Premessa metodologica. L'acquisizione è l'unica fase non ripetibile per definizione quando la fonte è volatile: ogni scelta compiuta qui vincola l'intera indagine e va motivata prima di essere attuata.

SCHEMA DEL MODULO

Il percorso dell'acquisizione in quattro fasi

01 · PREPARAZIONE

Prima di toccare

- Strategia live/post-mortem
- Ordine di volatilità
- Write blocker

02 · COPIA

La copia forense

- Bit-a-bit
- RAW, E01, AFF4
- Specificità SSD e RAID

03 · VERIFICA

L'integrità

- Hash MD5 + SHA-256
- Doppio hash
- Coincidenza delle copie

04 · DOCUMENTAZIONE

La memoria scritta

- Verbale di acquisizione
- Copie master e di lavoro
- Conservazione nel tempo

Le quattro aree si susseguono nelle slide del modulo nello stesso ordine dello schema: ciascuna presuppone la precedente.

La copia bit-a-bit: un duplicato integrale

La copia forense riproduce **ogni settore del supporto**, incluse aree non allocate, slack space e file cancellati, tutto ciò che una copia logica ignora. Il **write blocker** (hardware o software) impedisce qualunque scrittura verso la fonte durante l'operazione.

Formato	Caratteristiche
RAW (dd)	Flusso grezzo, massima compatibilità, nessun metadato
E01 (EWF)	Compressione, hash integrati, metadati del caso; standard de facto
AFF4	Formato aperto, supporta immagini sparse e acquisizioni parziali

Funzioni hash

Impronta a lunghezza fissa del contenuto: copie identiche hanno lo stesso hash.

```
MD5 → 128 bit, collisioni note
SHA-1 → 160 bit, deprecato
SHA-256 → standard attuale
```

Prassi: **doppio hash** (MD5 + SHA-256) calcolato in acquisizione e riportato a verbale.

APPROFONDIMENTO · WRITE BLOCKER

Il write blocker: la garanzia fisica dell'integrità

Hardware

Dispositivo fisico interposto tra reperto e workstation: blocca le scritture a livello di protocollo (SATA, USB, NVMe) ed è **indipendente dal sistema operativo**.

Prassi: standard per ogni acquisizione da supporto fisico, con test funzionale periodico.

Software

Blocco imposto dal sistema operativo (policy, driver, mount read-only nelle distro forensi come CAINE). Più flessibile ed economico, ma la garanzia dipende dalla **corretta configurazione**, da verificare e verbalizzare a ogni sessione.

ESEMPIO · Un disco NTFS collegato a Windows senza protezione viene modificato dal sistema in pochi secondi (aggiornamento del $LogFile, eventuale replay del journal, metadati del volume): l'hash del disco cambia anche se nessun file utente è stato aperto. Senza write blocker non si può dimostrare con precisione che cosa sia stato alterato.

APPROFONDIMENTO · FUNZIONI HASH

Proprietà e limiti di una funzione hash

Una funzione hash crittografica mappa un input di qualunque dimensione in un'impronta a lunghezza fissa, con tre proprietà:

- **Determinismo**: lo stesso input produce sempre lo stesso output
- **Effetto valanga**: un bit diverso cambia radicalmente l'impronta
- **Resistenza alle collisioni**: trovare due input con lo stesso hash è arduo

L'hash attesta l'**identità del contenuto**; provenienza e data richiedono catena di custodia e marca temporale.

ESEMPIO · EFFETTO VALANGA

```
SHA-256("forensica")
b0c1...9f42 (impronta A)

SHA-256("forensicA")
7d8e...03ab (impronta B)
```

Una maiuscola cambia l'impronta (valori illustrativi).

Sulle collisioni MD5. Le tecniche note permettono di costruire *a tavolino* due file con lo stesso MD5, ma non di trovare un secondo file che collida con un reperto dato (second preimage). Per la verifica d'integrità il rischio pratico è quindi remoto; il doppio hash MD5+SHA-256 elimina comunque l'obiezione.

SSD: quando il supporto decide da solo

A differenza del disco magnetico, l'SSD ha un controller attivo che riorganizza i dati per conto proprio, anche sotto write blocker:

- **TRIM**: il sistema comunica i blocchi liberati e il controller li azzera in background, così i file cancellati diventano presto irrecuperabili
- **Garbage collection**: il firmware consolida e ripulisce autonomamente, anche a sistema spento ma alimentato
- **Wear leveling**: i dati migrano fisicamente tra celle; l'indirizzo logico non dice dove i byte stanno davvero
- **Over-provisioning**: un'area riservata invisibile all'host, non raggiungibile dall'imaging ordinario

CONSEGUENZE OPERATIVE

- **Tempestività**: su SSD con TRIM attivo, ogni ora riduce il recuperabile
- **Due hash a distanza di tempo possono divergere** per attività del controller: annotare l'orario esatto di ogni calcolo
- In relazione: dichiarare tipo di supporto e stato TRIM, e calibrare le aspettative sul carving (modulo 3)

La copia resta valida come fotografia del contenuto logico al momento T, ma l'originale non può dirsi immutabile.

LIVE VS POST-MORTEM · RFC 3227

L'ordine di volatilità governa la sequenza

Dal più volatile al meno volatile

1. Registri CPU e cache
2. Memoria RAM e tabelle di rete
3. Processi in esecuzione
4. Dischi e supporti di massa
5. Log remoti e backup
6. Supporti di archiviazione offline

Post-mortem

Sistema spento, supporto rimosso, copia con write blocker. Massima ripetibilità, ma i dati volatili sono perduti (RAM, cifratura attiva).

Live forensics

Sistema acceso: si acquisiscono RAM, processi e connessioni **prima** dello spegnimento. Ogni azione altera lo stato: va limitata e motivata a verbale.

Con cifratura full-disk attiva o in un'indagine su malware residente, la **live acquisition** è di norma necessaria.

APPROFONDIMENTO · LIVE ACQUISITION OPERATIVA

Sistema acceso: la sequenza operativa

1. **Fotografare lo stato**: schermo, ora di sistema vs ora reale, dispositivi collegati, prima di toccare qualunque cosa
2. **Valutare**: cifratura attiva, sessioni aperte, processi sospetti
3. **Acquisire la RAM** da supporto esterno preparato, con strumento minimale (WinPmem), hash immediato dell'output
4. **Raccogliere i volatili residui**: connessioni, processi, utenti collegati; ogni comando va annotato con l'ora
5. **Decidere lo spegnimento**: shutdown ordinato (scrive su disco) o distacco (rischio di corruzione), motivando la scelta
6. **Passare al post-mortem**: disco rimosso, write blocker, copia forense

ESEMPIO · LA SCELTA AL PASSO 5

Server con database transazionale attivo e BitLocker: il distacco brutale rischia di corrompere il database; lo shutdown ordinato scrive su disco ma la RAM, con le chiavi, è già salva dal passo 3.

Decisione: shutdown ordinato, motivato a verbale. Il quesito investigativo (il contenuto del database) ha pesato più della minimizzazione delle scritture.

La sequenza segue l'ordine di volatilità: ogni azione che altera lo stato si compie solo *dopo* aver salvato ciò che quell'azione distruggerebbe.

APPROFONDIMENTO · RAID E VOLUMI LOGICI

Quando il «disco» è un'astrazione su più dischi

Nei server il dato vive su array RAID e volumi logici (LVM, Storage Spaces): nessun singolo disco contiene il file system leggibile. Due strategie di acquisizione:

- **Logica (dal volume montato)**: si acquisisce il volume come il sistema lo presenta; è semplice, ma richiede il sistema acceso e perde le aree sotto l'astrazione
- **Fisica (disco per disco)**: si copiano i membri singolarmente e si **ricostruisce l'array in laboratorio**; serve conoscere livello RAID, ordine dei dischi, dimensione di stripe e offset (dai metadati del controller o per inferenza)

ESEMPIO · RAID 5 IN LABORATORIO

Tre immagini E01 dai tre membri; i metadati indicano RAID 5, stripe 64 KB, ordine 0-1-2. La ricostruzione software produce il volume virtuale, il cui hash viene calcolato e verbalizzato come «volume ricostruito», distinto dagli hash dei membri.

Con parametri errati il file system risulta illeggibile: la ricostruzione è parte del metodo e va documentata in relazione, parametri inclusi.

Membri degradati o sostituiti di recente: l'array funziona, ma questi dischi possono contenere uno stato diverso dagli altri. Vanno acquisiti tutti i membri, compresi quelli guasti.

SCENARI COMPLESSI DI ACQUISIZIONE

Quando il supporto non è un disco sulla scrivania

Sistemi cifrati

BitLocker, FileVault, LUKS: a sistema spento il dato è inaccessibile senza chiave. Priorità: acquisire la RAM (che può contenere le chiavi) e documentare lo stato di cifratura.

Cloud e SaaS

Il dato risiede presso un provider, spesso all'estero: acquisizione via API o export certificato, questioni di giurisdizione, cooperazione ex regolamento e-Evidence.

Dispositivi mobili

Isolamento radio (modalità aereo, gabbia di Faraday), acquisizione logica o fisica secondo il modello. Trattazione estesa nel modulo 6.

Criterio generale. Quando l'acquisizione integrale è impossibile o sproporzionata, si procede per **acquisizione selettiva motivata**: perimetro, criteri di selezione e limiti vanno dichiarati a verbale, a tutela della completezza e del contraddittorio.

Un estratto di verbale, riga per riga

```
Reperto R-01: HDD [marca/modello], S/N [___], 1 TB,
rimosso dal PC [___] in data [gg/mm/aaaa] ore [hh:mm].

Acquisizione: workstation LAB-02, write blocker
[marca/modello, fw ___], FTK Imager v[___],
formato E01; inizio ore [hh:mm], termine ore [hh:mm].

Verifica: MD5 [valore], SHA-256 [valore],
ricalcolati sulla copia: coincidenti.
Copia su supporto S-07, sigillo n. [___].
Operatore: [nome, qualifica, firma].
```

Perché ogni riga conta

- **Seriale e orari**: ancorano il reperto nel tempo e nella catena
- **Strumenti e versioni**: rendono l'operazione riproducibile
- **Doppio hash verificato**: l'integrità diventa un fatto controllabile
- **Sigillo e supporto**: la custodia prosegue senza soluzione di continuità
- **Firma**: identifica il responsabile

Il verbale si redige **durante** le operazioni: se ricostruito a posteriori, è un semplice resoconto privo del valore di atto.

La gestione delle copie nel lungo periodo

Lo schema a tre livelli

- **Originale**: sigillato, custodito, toccato solo se indispensabile
- **Copia master**: la E01 verificata, mai usata per lavorare
- **Copie di lavoro**: derivate dalla master per ogni analisi, modificabili senza conseguenze

Ogni derivazione è registrata: da quale copia, quando, con che hash.

Il tempo lungo del processo

Un procedimento può durare più della vita utile dei supporti. Prassi: ridondanza su supporti distinti, **ricalcolo periodico degli hash** verbalizzato, migrazione programmata verso supporti nuovi (con hash di partenza e arrivo), ambienti a temperatura e umidità controllate.

ESEMPIO · VERIFICA A TRE ANNI

Appello fissato tre anni dopo l'acquisizione. La difesa chiede di verificare l'integrità: il laboratorio esibisce il registro dei ricalcoli periodici (stesso SHA-256 a ogni verifica) e produce una nuova copia di lavoro dalla master, con hash coincidente.

Grazie al registro la questione si risolve subito, senza un'udienza dedicata.

LABORATORIO · LETTURE · VERIFICA

Acquisire, verificare, verbalizzare

Laboratorio

- Imaging con **FTK Imager** e **Guymager** (E01 e RAW)
- Calcolo e verifica del doppio hash
- Acquisizione live di RAM da VM

`DELIVERABLE: immagine verificata + verbale`

Letture obbligatorie

- RFC 3227, *Guidelines for Evidence Collection and Archiving*
- Linee guida ENFSI sull'acquisizione forense
- Documentazione tecnica FTK Imager

Verifica

L'immagine acquisita in questo modulo sarà il reperto di lavoro dei moduli 3 e 4: eventuali errori si ripercuoteranno sulle analisi.

Prossimo modulo: analisi di file system e artefatti.

> La solidità processuale della prova dipende in larga parte dalla correttezza dell'acquisizione.

Grazie per l'attenzione

Vincenzo Calabrò

Domande, materiali del corso e contatti sul sito del docente

vincenzocalabro.it