MODULO 01 · AGOSTO 2026

# Fondamenti di Digital Forensics

Principi, catena di custodia, standard internazionali
e ruolo del perito nel procedimento

IDENTIFY → ACQUIRE → PRESERVE → ANALYZE → PRESENT

Corso di Laurea Magistrale in Sicurezza Informatica

# Al termine del modulo lo studente sarà in grado di

### 01 · DEFINIRE

La prova digitale e i principi di **integrità**, **autenticità** e **ripetibilità** che ne condizionano il valore probatorio

### 02 · COLLOCARE

La disciplina nel quadro normativo italiano ed europeo e negli standard tecnici internazionali (ISO, NIST)

### 03 · DOCUMENTARE

Una catena di custodia formalmente corretta, redigendo il verbale di acquisizione su un caso simulato

Il modulo distingue sistematicamente il piano **tecnico** (metodologia e strumenti) dal piano **processuale** (ammissibilità e valore della prova): la competenza del forenser risiede nella loro integrazione.

SCHEMA DEL MODULO

# La mappa del modulo: dalla prova al dibattimento

01 · LA PROVA

### La prova digitale

- Caratteristiche
- Tipologie di evidenza
- Valore probatorio

→

02 · IL PROCESSO

### Il processo forense

- ISO/IEC 27037
- Ripetibilità
- Ruoli: DEFR e DES

→

03 · LE REGOLE

### Regole e norme

- Artt. 359–360 c.p.p.
- L. 48/2008
- Catena di custodia

→

04 · LE MINACCE

### Minacce alla prova

- Anti-forensics
- Errori operativi
- Contromisure

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

# Definizione e requisiti della prova digitale

La prova digitale è **qualsiasi informazione con valore probatorio memorizzata o trasmessa in forma binaria** (SWGDE). A differenza della prova fisica, può essere duplicata perfettamente ma anche alterata senza lasciare tracce apparenti: la sua affidabilità dipende interamente dal metodo con cui è trattata.

### Integrità

Il dato non deve subire modifiche dall'acquisizione alla presentazione. Garantita tecnicamente da funzioni hash e write blocker.

### Autenticità

Il reperto deve provenire dalla fonte dichiarata. Garantita dalla documentazione della catena di custodia.

### Ripetibilità

Un terzo, con gli stessi dati e metodi, deve poter riprodurre i risultati. Fondamento della scientificità della perizia.

# Dove nasce la prova: una tassonomia delle fonti

La prova digitale non coincide con «il computer». Ogni categoria di fonte ha proprietà tecniche (volatilità, accessibilità, controllo) che determinano come acquisirla e quali garanzie adottare:

- **Supporti locali**: dischi, SSD (con le complicazioni di TRIM e wear leveling), supporti rimovibili
- **Sistemi in esecuzione**: memoria, processi, sessioni (la fonte più volatile)
- **Rete**: traffico, log di apparati, flussi (fonte distribuita e deperibile)
- **Cloud e SaaS**: dati presso terzi, giurisdizione variabile
- **Dispositivi personali e IoT**: smartphone, wearable, domotica, veicoli

**ESEMPIO**

Indagine per accesso abusivo: la stessa condotta lascia tracce sul laptop dell'autore (fonte locale), sul firewall aziendale (rete), nei log del provider di posta (cloud) e sul suo smartwatch, che registra dove si trovava.

Le quattro fonti richiedono regimi di acquisizione diversi; per questo l'indagine comincia dalla mappa delle fonti.

# Le cinque fasi del processo forense

FASE 1

### Identificazione

Riconoscere le potenziali fonti di prova sulla scena

FASE 2

### Acquisizione

Copiare i dati con metodo forensicamente valido

FASE 3

### Conservazione

Proteggere integrità e tracciabilità nel tempo

FASE 4

### Analisi

Esaminare i dati in risposta al quesito

FASE 5

### Presentazione

Esporre metodo e risultati nella relazione

**Documentazione continua.** Ogni operazione è verbalizzata: chi, cosa, quando, dove, come e perché. La documentazione è parte integrante del processo: un'operazione non documentata non ha valore processuale.

APPROFONDIMENTO · DENTRO ISO/IEC 27037

# Ruoli e principi dello standard di acquisizione

Lo standard distingue due figure operative, con competenze e perimetri diversi:

- **DEFR** (Digital Evidence First Responder): il primo intervenuto, che identifica, mette in sicurezza e raccoglie; deve saper *non* fare ciò che spetta allo specialista
- **DES** (Digital Evidence Specialist): lo specialista, che acquisisce nei casi complessi (sistemi accesi, cifratura, RAID) e supporta l'analisi

E quattro principi che attraversano tutto il processo: **auditability** (ogni azione ricostruibile da terzi), **repeatability**, **reproducibility** (stesso risultato anche con strumenti diversi), **justifiability** (ogni scelta motivata).

**ESEMPIO · IL CONFINE DEFR/DES**

Perquisizione in azienda: il DEFR trova un server acceso con volumi cifrati montati. La mossa corretta è congelare la scena, documentare lo stato e chiamare il DES per la live acquisition, senza «provare qualcosa».

Il confine di competenza è esso stesso una garanzia: molti inquinamenti nascono da operatori che eccedono il proprio ruolo.

I quattro principi sono la griglia con cui verrà valutata ogni relazione del corso; conviene applicarli come domande di controllo («un terzo potrebbe ricostruire ciò che ho fatto?»).

APPROFONDIMENTO · ARTT. 359-360 C.P.P.

# Accertamenti ripetibili e irripetibili

### Accertamento ripetibile (art. 359)

L'operazione non consuma né altera la fonte: può essere rieseguita da altri, in contraddittorio differito. L'analisi condotta su una **copia forense verificata** è il caso tipico: l'originale resta intatto, chiunque può ripartire da esso.

### Accertamento irripetibile (art. 360)

L'operazione modifica o consuma la fonte: lo stato osservato non esisterà più. Scattano le garanzie **anticipate**: avviso alle parti, facoltà di nominare consulenti, partecipazione all'atto. L'acquisizione di un sistema acceso ne è il paradigma.

**ESEMPIO 1 · RIPETIBILE**

Il CTU riceve l'immagine E01 con hash verificato e vi cerca i documenti rilevanti: la difesa potrà rifare la stessa ricerca sulla stessa immagine. Nessun avviso preventivo necessario.

**ESEMPIO 2 · IRRIPETIBILE**

Il server è acceso con volumi cifrati montati: spegnere significa perdere le chiavi. L'acquisizione live altera lo stato e non è rieseguibile: si procede ex art. 360, con le parti avvisate.

# Chi fa che cosa: perito, CTU, CTP

| Figura | Chi lo nomina | Funzione e vincoli |
|---|---|---|
| Perito | Il giudice (dibattimento penale) | Ausiliario del giudice; risponde al quesito formulato; obbligo di verità e terzietà |
| CTU | Il giudice (civile) o il PM (consulente del PM nel penale) | Consulente tecnico d'ufficio; stesso statuto di terzietà del perito nel proprio ambito |
| CTP | Le parti | Consulente di parte: partecipa alle operazioni, formula osservazioni, redige memorie; è comunque tenuto al rigore metodologico |

**ESEMPIO ·** Nel caso ransomware del modulo 12: il CTU acquisisce e analizza l'immagine; il CTP della società assiste alle operazioni irripetibili e verifica gli hash; all'esito, contesta nella memoria la completezza dei log esaminati.

Deontologia comune a tutte le figure: competenza effettiva, dichiarazione dei limiti, conservazione della documentazione, riservatezza.

# Le fonti che governano la prova digitale

| Fonte | Natura | Oggetto |
|---|---|---|
| ISO/IEC 27037:2012 | Standard tecnico | Identificazione, raccolta, acquisizione e conservazione della prova |
| ISO/IEC 27042:2015 | Standard tecnico | Analisi e interpretazione della prova digitale |
| NIST SP 800-86 | Linea guida | Integrazione delle tecniche forensi nella risposta agli incidenti |
| Convenzione di Budapest (2001) | Trattato internazionale | Criminalità informatica e cooperazione giudiziaria |
| L. 48/2008 | Legge nazionale | Ratifica della Convenzione: obblighi di conservazione e non alterazione (artt. 244, 247, 352 c.p.p.) |
| Artt. 359–360 c.p.p. | Codice di rito | Accertamenti tecnici ripetibili e irripetibili; garanzie del contraddittorio |

**Nota metodologica.** Gli standard tecnici, pur privi di forza di legge, definiscono la *best practice* rispetto alla quale il giudice valuta l'affidabilità dell'operato del perito: scostarsene senza motivazione espone la prova a contestazione.

# Che cosa ha cambiato la ratifica nel codice di rito

La Convenzione di Budapest (2001) è il primo trattato internazionale sulla criminalità informatica: armonizza i reati, disciplina la conservazione rapida dei dati e fonda la cooperazione tra Stati. L'Italia la ratifica con la **L. 48/2008**, che innesta nel c.p.p. un principio ricorrente:

nelle ispezioni, perquisizioni e sequestri su sistemi informatici (artt. 244, 247, 352, 354 c.p.p. novellati) si adottano **«misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»**, con copia su adeguato supporto e conformità all'originale.

### LA LETTURA OPERATIVA

Il legislatore indica i **risultati** (conservazione, non alterazione, conformità) e lascia aperta la scelta degli strumenti. Write blocker, copia bit-a-bit e hash sono il modo in cui la tecnica realizza quei risultati; per questo la best practice tecnica diventa rilevante in giudizio pur non essendo legge.

Chi se ne discosta deve poter dimostrare che il proprio metodo ha comunque garantito il risultato richiesto.

Completano il quadro: data retention e acquisizione dei dati di traffico (disciplina speciale), e il regolamento **e-Evidence** per gli ordini europei di produzione, ripreso nel modulo 5.

CATENA DI CUSTODIA · CHAIN OF CUSTODY

# La biografia documentata del reperto

Registro cronologico e ininterrotto di ogni passaggio del reperto: chi lo ha avuto in custodia, quando, dove, con quale finalità e con quali operazioni.

Una catena interrotta o lacunosa, pur non invalidando automaticamente la prova, ne **indebolisce l'autenticità** e apre al controesame della difesa.

### Contenuto minimo del verbale

- Identificazione univoca del reperto (marca, modello, seriale)
- Data, ora e luogo di ogni presa in carico
- Generalità e qualifica di chi opera
- Operazioni svolte e strumenti impiegati
- Valori hash calcolati e loro verifica
- Sigilli, supporti di destinazione, condizioni di conservazione

`SHA-256(reperto) = SHA-256(copia) ⇒ integrità verificabile da chiunque, in ogni momento`

APPROFONDIMENTO · ANTI-FORENSICS

# Conoscere l'avversario del metodo

| Tecnica | Obiettivo | Contromossa del corso |
|---|---|---|
| Wiping / cancellazione sicura | Distruggere il dato | Residui in journal, cloud e backup (M3, M5) |
| Timestomping | Falsificare la cronologia | Confronto $SI/$FN e fonti temporali (M3) |
| Cifratura e hidden volume | Rendere illeggibile | Chiavi in RAM, strategia live (M2, M4, M6) |
| Steganografia | Nascondere dentro l'innocuo | Anomalie statistiche, confronto con originali |
| Fileless e living-off-the-land | Non lasciare file | Memory forensics (M4) |
| Log tampering | Riscrivere la storia | Correlazione di fonti indipendenti (M5) |

**Anche l'occultamento lascia tracce**: l'installazione del wiper, il pattern degli zeri, l'incoerenza dei timestamp. Spesso la prova più eloquente è la documentazione del **tentativo di far sparire i dati** e del momento in cui è avvenuto.

APPROFONDIMENTO · ERRORI TIPICI E CONSEGUENZE

# Come si perde una prova: casistica degli errori

| Errore | Che cosa compromette | Prevenzione |
|---|---|---|
| Accendere o navigare il reperto originale | Timestamp alterati, integrità contestabile | Write blocker e lavoro solo su copia |
| Hash calcolato tardi o mai | Impossibile provare che la copia è fedele | Doppio hash in acquisizione, a verbale |
| Catena di custodia con lacune temporali | Autenticità indebolita, controesame facile | Registro continuo, passaggi firmati |
| Atto irripetibile senza garanzie ex art. 360 | Rischio di inutilizzabilità dell'accertamento | Qualificare l'atto prima di compierlo |
| Relazione senza metodo dichiarato | Risultati non verificabili, perizia svalutata | Strumenti, versioni e passi documentati |

**ESEMPIO** · Scenario ricorrente nella prassi: un amministratore IT, in buona fede, «dà un'occhiata» al PC dell'indagato prima dell'arrivo del consulente. I timestamp di accesso di centinaia di file risultano aggiornati e la difesa può sostenere l'inquinamento della prova. L'errore è organizzativo: nessuno aveva stabilito chi potesse intervenire sul sistema e quando.

LABORATORIO · LETTURE · VERIFICA

# Dalla teoria al verbale

### Laboratorio

Su un caso simulato: redazione del **verbale di acquisizione** e della **catena di custodia** di un reperto, con identificazione univoca, operazioni e hash.

`DELIVERABLE: verbale + modulo CoC compilato`

### Letture obbligatorie

- ISO/IEC 27037:2012 (testo integrale)
- NIST SP 800-86, capp. 1–3
- E. Casey, *Digital Evidence and Computer Crime*, capp. 1–2

### Verifica

Il verbale concorre alla valutazione del progetto di laboratorio (40% del voto finale); i contenuti teorici rientrano nella prova scritta.

**Prossimo modulo:** l'acquisizione forense.

> I principi di metodo visti nel modulo si applicano a qualunque strumento forense.

# Grazie per l'attenzione

**Vincenzo Calabrò**

Domande, materiali del corso e contatti sul sito del docente

vincenzocalabro.it