

MODULO 07

Fondamenti di Digital Forensics

Identificazione, acquisizione, preservazione, analisi e presentazione delle evidenze digitali con riferimento alle norme ISO/IEC 27037, 27042 e 27043: catena di custodia, hashing e ripetibilità.

ISO/IEC 27037

SHA-256

Autopsy / TSK

Abstract e obiettivi formativi

Abstract

Il modulo pone le basi metodologiche dell'informatica forense: principi di non alterazione e ripetibilità, acquisizione fisica e logica con write blocker, verifica d'integrità tramite hashing, strutture dei file system (NTFS, ext4, APFS), artefatti di Windows e recupero di file cancellati, fino alla relazione tecnica.

Obiettivi formativi (Bloom)

- **Applicare:** eseguire un'acquisizione forense correttamente documentata
- **Applicare:** mantenere e verificare la catena di custodia
- **Analizzare:** distinguere nelle strutture dei file system le tracce utili al recupero di evidenze

Traccia core

01

02

07

Detection & Response

03

04

05

06

o

Digital Forensics

08

09

10

11

o

Sicurezza dell'AI

06

12

13

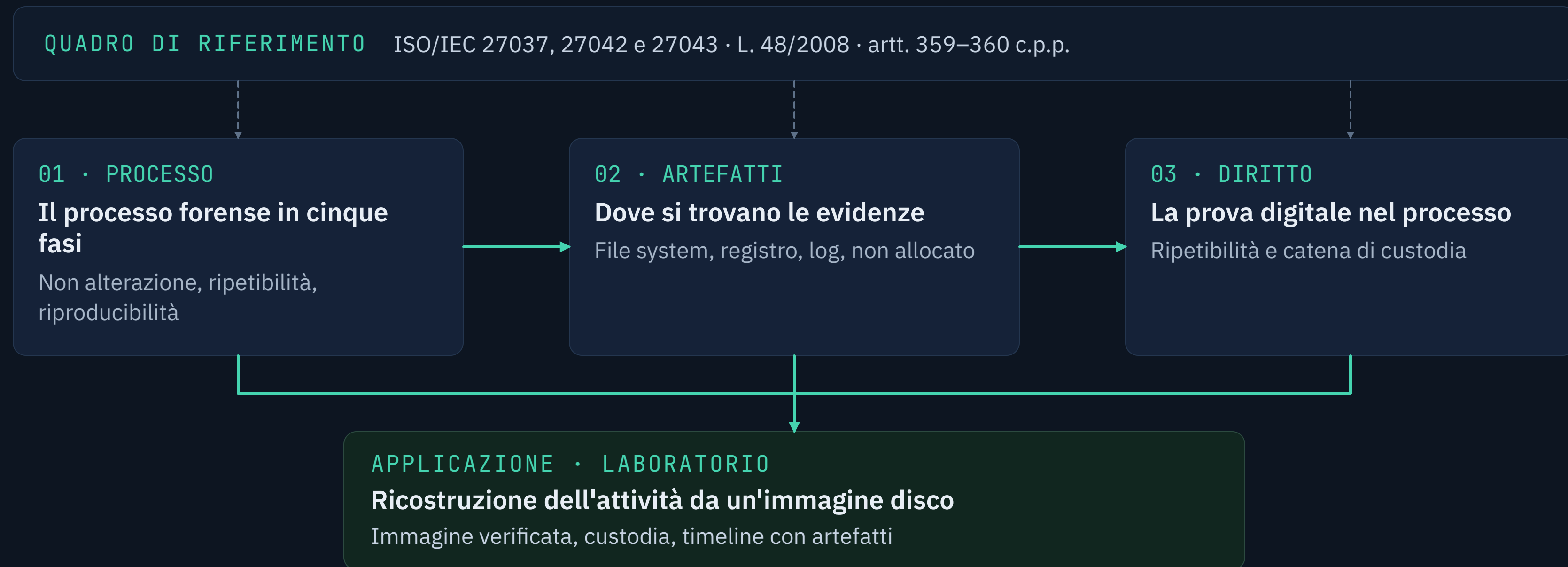
14

Traccia core

15

16

Evidenze digitali con valore di prova



Il processo forense in cinque fasi



Principi del metodo

Non alterazione: l'originale non si modifica e ogni accesso è mediato e documentato. **Ripetibilità e riproducibilità:** con gli stessi dati e lo stesso metodo si ottiene lo stesso risultato nello stesso ambiente di prova e, anche da parte di un terzo, in un ambiente diverso. L'hash calcolato all'acquisizione e verificato dopo l'analisi documenta l'integrità della copia.

Dove si trovano le evidenze

Artefatto	Cosa attesta	Dove si trova
MFT e timestamp	Esistenza, creazione e modifica dei file	File \$MFT del volume NTFS
Prefetch	Esecuzione di un programma, quando e quante volte	C:\Windows\Prefetch
Registro di sistema	Dispositivi USB, attività dell'utente, programmi recenti	Hive SYSTEM, SOFTWARE, NTUSER.DAT, Amcache.hve
Shellbag	Cartelle aperte, anche se poi cancellate o rimosse	NTUSER.DAT, UsrClass.dat
Log eventi	Accessi, servizi, errori, cancellazione log	C:\Windows\System32\winevt\Logs
Spazio non allocato	File cancellati recuperabili con il carving	Settori liberi del disco

La cancellazione ordinaria rimuove il riferimento al file e lascia i dati sul supporto finché i settori non vengono sovrascritti; il carving ricostruisce i file dal contenuto. Sulle unità SSD il comando TRIM può rendere i dati irrecuperabili in breve tempo.

La prova digitale nel processo

Quadro italiano

- L. 48/2008: ratifica della Convenzione di Budapest e misure tecniche che assicurino la conservazione dei dati originali
- Accertamenti ripetibili (art. 359 c.p.p.) e non ripetibili (art. 360 c.p.p.): per questi ultimi il pubblico ministero avvisa la persona sottoposta alle indagini, la persona offesa e i difensori
- Una copia forense eseguita correttamente rende ripetibili le analisi successive

Catena di custodia

- Chi, cosa, quando, dove, perché: ogni passaggio del reperto è registrato
- Hash come sigillo logico; sigilli fisici e custodia controllata
- Una lacuna nella catena espone l'evidenza a contestazione in dibattimento

Questioni tecniche e processuali



Funzioni hash e integrità della copia forense

Una funzione hash crittografica produce per ogni input un'impronta di lunghezza fissa: la modifica di un solo bit dell'input cambia l'impronta, ed è computazionalmente impraticabile trovare due input con la stessa impronta. Calcolare l'hash al momento dell'acquisizione, di preferenza con SHA-256, e verificarlo a ogni passaggio successivo dimostra che i dati analizzati sono identici a quelli acquisiti. Il **write blocker** interviene prima: impedisce che il collegamento del supporto alla workstation di acquisizione ne modifichi il contenuto, per esempio aggiornando i timestamp di accesso o il journal del file system.

Scenario didattico

Un disco da 500 GB viene acquisito in formato E01; lo SHA-256 calcolato sul dispositivo coincide con quello dei dati contenuti nell'immagine ed entrambi vengono riportati nel verbale. Sei mesi dopo, prima della consulenza di parte, il consulente ricalcola l'hash e ottiene lo stesso valore, quindi l'analisi si svolge su dati integri e chiunque può ripetere la verifica.

Limiti

Un hash mancante o calcolato solo a posteriori espone a contestazioni. Anche un hash corretto attesta soltanto l'integrità della copia, e non dimostra la correttezza dell'acquisizione né la provenienza del dato. Per MD5 e SHA-1, ancora diffusi negli strumenti e nei verbali, sono note collisioni costruibili, e per questo vanno affiancati o sostituiti da SHA-256.

Catena di custodia delle evidenze digitali

La **catena di custodia** è la documentazione ininterrotta della vita di un'evidenza: chi l'ha acquisita e con quali strumenti, dove è stata conservata, chi vi ha avuto accesso, per quale motivo e con quale esito. Con essa il giudice può escludere che l'evidenza sia stata alterata, sostituita o contaminata tra il sequestro e il dibattimento. Ogni passaggio di mano è registrato e firmato; un intervallo non documentato offre argomenti alla controparte. La L. 48/2008, di ratifica della Convenzione di Budapest, ha introdotto nel codice di procedura penale il richiamo a misure tecniche dirette ad assicurare la conservazione dei dati originali e a impedirne l'alterazione.

Scenario didattico

Un notebook sequestrato passa dall'ufficiale di polizia giudiziaria al deposito dei corpi di reato e poi al consulente tecnico. Il modulo di custodia registra tre consegne con data, ora, firma e stato dei sigilli. In udienza la difesa chiede conto di un intervallo di due giorni: il registro del deposito, con il numero di protocollo, documenta dove si trovava il reperto.

Ruolo dell'AI

Quando uno strumento di AI elabora un'evidenza, anche quel passaggio entra nella catena con versione del modello, parametri e hash dell'input e dell'output, e un'analisi automatica non registrata costituisce una lacuna (Modulo 14).

Ordine di volatilità e scelte di acquisizione

Le evidenze digitali hanno durate diverse. La RFC 3227 ordina le fonti dalla più volatile alla più stabile. In testa vengono registri e cache del processore, poi tabelle di routing, cache ARP, tabella dei processi, statistiche del kernel e memoria. Seguono i file system temporanei, il disco e i log remoti, quindi la configurazione fisica e la topologia di rete e, per ultimi, i supporti d'archivio come le copie di backup. Acquisire nell'ordine sbagliato distrugge le evidenze più fragili, perché ogni azione sul sistema acceso consuma memoria e sovrascrive tracce. Da qui la scelta del primo intervento: acquisire i dati volatili a sistema acceso (**live forensics**) e poi il disco, accettando una perturbazione documentata, oppure spegnere subito, perdendo il contenuto volatile; anche la modalità di spegnimento incide sulle tracce.

Scenario didattico

Un ransomware è in esecuzione su un server. In memoria possono trovarsi la chiave di cifratura in uso, le connessioni verso il server di comando e il processo malevolo. Se l'host viene spento senza acquisire la RAM, il disco resta integro ma chiave e connessioni vanno perse; con BitLocker attivo lo spegnimento può impedire anche l'accesso al disco senza la chiave di ripristino.

Metodo

La scelta va fatta prima, nel playbook di primo intervento: quando procedere con l'acquisizione live (cifratura del disco attiva, malware residente in memoria) e quando spegnere (cancellazione distruttiva in corso). Ogni azione sul sistema acceso va annotata con l'orario, perché modifica ciò che si sta acquisendo.

Artefatti di esecuzione e di attività in Windows

Il sistema operativo registra molte tracce dell'attività. In NTFS la **MFT** contiene un record per ogni file con i relativi timestamp, che sopravvive alla cancellazione finché non viene riutilizzato; il journal USN annota creazioni, modifiche e rinomine dei file del volume. Il registro di Windows conserva i dispositivi USB collegati, le reti usate e i programmi eseguiti o presenti nel sistema (UserAssist, Amcache, ShimCache). I file di Prefetch indicano quali eseguibili sono stati avviati, quante volte e quando, e le shellbag registrano le cartelle visualizzate, anche su supporti poi rimossi. Nessun artefatto da solo prova una ricostruzione, perché ciascuno ha eccezioni e condizioni di validità, e il valore probatorio sta nella concordanza di fonti indipendenti.

Scenario didattico

Si sospetta che un dipendente in uscita abbia copiato dati. Il registro mostra una chiavetta USB non dichiarata collegata in una certa data, e le shellbag indicano l'apertura della cartella «Clienti_2025» su quel volume. Negli stessi minuti Prefetch documenta l'esecuzione di uno strumento di archiviazione, mentre il journal USN del disco interno registra la creazione di un archivio compresso, poi cancellato.

Ruolo dell'AI

L'estrazione e la normalizzazione degli artefatti sono operazioni meccaniche, svolte da strumenti come Plaso (Modulo 9). Un LLM può aiutare a interpretare artefatti poco comuni e a suggerire dove cercare; il significato probatorio di un timestamp e le sue eccezioni note restano materia di valutazione dell'esperto.

Tecniche anti-forensi e loro tracce

Chi prevede un'indagine può ostacolarla con la cancellazione sicura (wiping) di file o dello spazio libero, l'alterazione dei timestamp (timestomping), la cancellazione dei log, i contenitori cifrati, l'uso esclusivo della memoria. Queste tecniche lasciano a loro volta tracce. L'esecuzione di uno strumento di wiping può comparire in Prefetch, e Amcache ne attesta almeno la presenza. Il timestomping produce incoerenze tra gli attributi **\$STANDARD_INFORMATION** e **\$FILE_NAME** della MFT. Su un disco magnetico uno spazio libero interamente azzerato è statisticamente anomalo, mentre sulle unità SSD con TRIM attivo è frequente anche senza wiping. Anche la cancellazione del registro Security di Windows lascia un evento (ID 1102), e un'assenza selettiva di dati, documentata con rigore, va riportata come fatto.

Scenario didattico

Un file decisivo risulta creato due anni prima dei fatti. Nella MFT, però, il timestamp di **\$FILE_NAME** riporta una data diversa. Il journal USN registra la creazione effettiva e, pochi minuti dopo, la modifica dei timestamp (motivo **BASIC_INFO_CHANGE**), mentre Prefetch documenta negli stessi minuti l'esecuzione dello strumento di manipolazione, e l'alterazione così accertata si riporta nella relazione come fatto autonomo.

Cautele

Le conclusioni non devono andare oltre ciò che le evidenze sostengono. «Lo spazio libero è stato sovrascritto con uno strumento compatibile con X in data Y» è un'affermazione verificabile; «ha distrutto le prove del reato» è una conclusione che spetta ad altri.

Consulenti tecnici e accertamenti non ripetibili

Nel processo penale l'esperto interviene come perito nominato dal giudice, come consulente tecnico del pubblico ministero (art. 359 c.p.p.) o come consulente tecnico di parte; nel processo civile come consulente tecnico d'ufficio (CTU) o di parte (CTP). Sul piano processuale si distingue tra accertamento **ripetibile**, come l'analisi su una copia forense verificata con l'hash, e accertamento **non ripetibile**, che riguarda un oggetto il cui stato è soggetto a modificazione, anche per effetto dell'accertamento stesso, come l'acquisizione da un sistema acceso. Per gli accertamenti non ripetibili disposti dal pubblico ministero l'art. 360 c.p.p. prevede l'avviso alla persona sottoposta alle indagini, alla persona offesa e ai difensori, che possono nominare consulenti tecnici e assistere; se il pubblico ministero procede nonostante la riserva di incidente probatorio e senza urgenza, i risultati non sono utilizzabili nel dibattimento.

Scenario didattico

Uno smartphone acceso con cifratura attiva va acquisito subito e l'estrazione ne modifica lo stato. È un accertamento non ripetibile, da svolgere con le garanzie dell'art. 360 c.p.p., verbale dettagliato, strumenti e versioni documentati e, se possibile, videoregistrazione, mentre le analisi successive sulla copia estratta, verificata con l'hash, sono ripetibili.

Ruolo dell'AI

Un'analisi con strumenti di AI su copia forense è riproducibile solo se modello, versione e parametri sono fissati e documentati e la variabilità degli output è controllata (Modulo 8). Con uno strumento cloud aggiornato automaticamente l'accertamento resta ripetibile sulla copia, ma il risultato non si riproduce, e per questo sono preferibili strumenti locali e versionati.

Ricostruzione dell'attività da un'immagine disco

Svolgimento (FTK Imager, Autopsy, The Sleuth Kit)

1. Acquisizione dell'immagine disco didattica con FTK Imager e verifica degli hash calcolati all'acquisizione; calcolo dello SHA-256 dei dati acquisiti con uno strumento documentato (per esempio `ewfverify -d sha256` per le immagini E01)
2. Compilazione del modulo di catena di custodia, passo per passo
3. Analisi in Autopsy: prefetch, registro, shellbag, file cancellati
4. Ricostruzione dell'attività utente in una timeline motivata

Consegna

- Modulo di custodia completo e coerente
- Timeline dell'attività con artefatti a supporto
- Mini-relazione: metodo, strumenti, hash

Lecture e autovalutazione

Lecture obbligatorie

- ISO/IEC 27037:2012
- Carrier, *File System Forensic Analysis* (capitoli su NTFS)
- ISO/IEC 27042:2015 e 27043:2015; L. 48/2008

Domande di autovalutazione

1. Quali requisiti deve soddisfare la catena di custodia?
2. Perché l'hash si calcola all'acquisizione e si verifica dopo l'analisi?
3. Che differenza c'è tra acquisizione fisica e logica?
4. Quali artefatti di Windows attestano l'esecuzione di un programma?
5. Cosa comporta la distinzione tra accertamenti ripetibili e non ripetibili?

FINE DELLA LEZIONE • MODULO 07

Grazie

Fondamenti di Digital Forensics • Corso «Incident Response potenziata dall'AI»

Domande e materiali: ricevimento del docente. Profilo e contatti:
vincenzocalabro.it



Vincenzo Calabrò

CYBER SECURITY • DIGITAL FORENSICS



VINCENZOCALABRO.IT