

MODULO 10

Mobile, cloud e multimedia forensics

Il metodo forense oltre il disco: dispositivi mobili, log degli ambienti cloud e contenuti multimediali, con l'AI come strumento d'indagine e come origine dei contenuti sintetici da esaminare.

iOS / Android

M365 / AWS / Azure

DEEPFAKE / C2PA

Abstract e obiettivi formativi

Abstract

Il modulo estende il metodo forense ai dispositivi mobili (acquisizione logica, file system e fisica su iOS/Android), agli ambienti cloud (Unified Audit Log di M365, AWS CloudTrail, Entra ID) e ai contenuti multimediali: autenticazione delle immagini, rilevamento di deepfake e standard di provenienza C2PA, con i relativi limiti probatori.

Obiettivi formativi (Bloom)

- **Applicare:** pianificare un'acquisizione mobile proporzionata al caso
- **Analizzare:** condurre un'indagine su log cloud (M365, AWS, Azure)
- **Valutare:** applicare criticamente strumenti di deepfake detection e autenticazione multimediale

Traccia core

01 02 07

Detection & Response

03 04 05 06

o

Digital Forensics

08 09 10 11

o

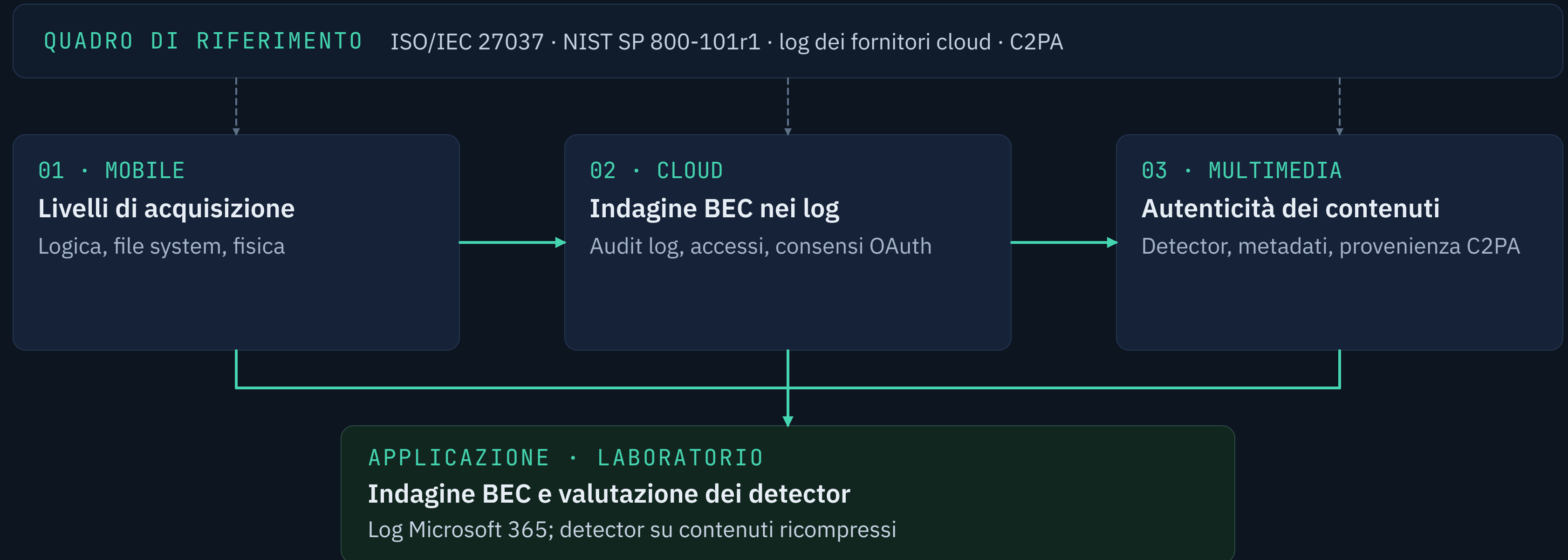
Sicurezza dell'AI

06 12 13 14

Traccia core

15 16

Il metodo forense oltre il disco



Livelli di acquisizione e proporzionalità

LOGICA

Dati esposti dalle API del sistema: contatti, messaggi, media. Minima invasività, copertura parziale

FILE SYSTEM

Struttura completa accessibile: database delle app, artefatti di messaggistica, geolocalizzazione

FISICA

Copia bit a bit, spazio non allocato incluso. Cifratura e secure enclave la rendono spesso impraticabile; quando è possibile richiede lo sfruttamento di vulnerabilità, da documentare

La scelta del livello dipende dal caso e dalla base giuridica: è proporzionata l'acquisizione sufficiente agli scopi dell'indagine con la minore invasività. Gli artefatti delle app di messaggistica, cioè database SQLite, allegati e metadati, sono spesso la fonte più rilevante.

Indagine BEC nei log del cloud

Le fonti

- **M365 Unified Audit Log:** accessi, regole di inoltramento, accessi alle caselle di posta
- **Entra ID sign-in log:** provenienza geografica, dispositivi, MFA
- **AWS CloudTrail / Azure Activity Log:** chiamate API, creazione di risorse e chiavi
- **Consensi OAuth:** possono mantenere l'accesso anche dopo il cambio della password; vanno revocati insieme alle sessioni dell'utente

Differenze di metodo

- Al posto del supporto si acquisisce l'**esportazione dei log**, con hash e verbale di estrazione
- Periodi di conservazione limitati: la tempestività è parte della custodia
- Il fornitore è un soggetto terzo: contratti e giurisdizione determinano l'accesso ai dati
- L'AI aiuta a correlare migliaia di eventi di accesso in pattern leggibili

Autenticità dei contenuti e AI generativa

Strumenti d'analisi

- Analisi classica: metadati, ELA, incoerenze di compressione e illuminazione
- Detector ML per volti, voci e video sintetici
- **C2PA**: provenienza firmata crittograficamente; attesta origine e modifiche dichiarate, non la veridicità della scena

Limiti probatori

- Tassi d'errore non trascurabili, più alti sui generatori assenti dai dati di addestramento
- Prestazioni ridotte su contenuti ricompresi da social network e app di messaggistica
- L'esito del detector va valutato insieme a metadati, contesto e testimonianze

Recupero e verifica dei dati



Livelli di acquisizione dei dispositivi mobili

Nei dispositivi mobili l'immagine completa della memoria è un'eccezione: cifratura per file attiva per impostazione predefinita, secure enclave, bootloader bloccati. I tre livelli di acquisizione hanno completezza e invasività crescenti. L'acquisizione **logica** raccoglie ciò che il sistema espone tramite backup e API, come contatti, messaggi e foto. Copiando l'albero dei file accessibile, l'acquisizione del **file system** include anche i database delle app, con i record cancellati ancora presenti negli spazi liberi e nei file WAL. L'acquisizione fisica, che produce l'immagine della memoria flash, è oggi raramente possibile senza sfruttare vulnerabilità. La scelta è un compromesso documentato tra completezza, rischio di alterazione e base giuridica: ai livelli più profondi lo strumento interviene di più sul dispositivo.

Esempio

Un'estrazione limitata ai dati esposti dalle API restituisce i soli messaggi visibili nell'app; con l'accesso al file system si possono recuperare dal database SQLite della chat i record contrassegnati come eliminati e non ancora sovrascritti. La differenza tra un messaggio mai esistito e un messaggio cancellato può essere rilevante per il procedimento.

Cautele

Il dispositivo acceso va isolato dalla rete, con la modalità aereo o un contenitore schermato, per evitare cancellazioni da remoto. Ogni interazione con lo schermo può modificare lo stato del dispositivo e va verbalizzata. Le funzioni di estrazione assistita dall'AI degli strumenti commerciali pongono gli stessi problemi di spiegabilità discussi nel Modulo 8.

Evidenze negli ambienti cloud

Negli ambienti cloud l'investigatore non ha accesso fisico ai supporti. Le evidenze si trovano negli snapshot delle istanze, nei metadati dei servizi e nei **log del fornitore**, che registrano attività amministrative, accessi e chiamate API. Sono spesso replicate in giurisdizioni diverse e soggette a **conservazione limitata**, scaduta la quale i dati non esportati vengono cancellati. L'acquisizione richiede quindi tempestività: esportazione immediata dei log rilevanti con hash e verbale, documentazione delle configurazioni, richiesta formale di conservazione al fornitore. La catena di custodia riguarda soprattutto i processi: chi ha esportato, con quale account, con quali filtri, e come si dimostra la completezza dell'esportazione.

Scenario didattico

Si supponga un tenant Microsoft 365 compromesso con uno schema BEC: lo Unified Audit Log mostra accessi dall'estero, la creazione di una regola di posta che inoltra le fatture a un indirizzo esterno e il consenso a un'applicazione OAuth malevola. Con una conservazione di 180 giorni, un giudizio civile successivo potrà basarsi sull'esportazione certificata nei primi giorni dell'indagine.

Nota normativa

Per i dati conservati all'estero rilevano i trattati di assistenza giudiziaria, il CLOUD Act statunitense (2018) e la disciplina europea e-Evidence (Reg. (UE) 2023/1543 e Dir. (UE) 2023/1544). Il contratto con il fornitore determina quali dati il cliente può ottenere e in quali tempi.

Autenticazione dei contenuti e deepfake

Accanto alla domanda tradizionale sul ritocco di una foto si pone quella sull'esistenza stessa dell'evento rappresentato. Il rilevamento dei deepfake cerca le incoerenze lasciate dai generatori: illuminazione e riflessi negli occhi, anomalie nello spettro delle frequenze, artefatti di fusione e, nei video, dinamiche fisiologiche innaturali. Ogni nuova generazione di modelli riduce però gli artefatti della precedente, e i detector perdono accuratezza sui contenuti ricompresi dalle piattaforme. Per questo si stanno diffondendo i sistemi di **provenienza**: lo standard C2PA (Content Credentials) firma crittograficamente l'origine del file e le modifiche registrate, e sposta la verifica sulla storia documentata del contenuto.

Caso documentato

Nel 2019, secondo quanto riferito dall'assicuratore Euler Hermes, l'amministratore delegato della controllata britannica di un gruppo energetico autorizzò un bonifico di circa 220.000 euro dopo una telefonata in cui una voce sintetica imitava il vertice della capogruppo tedesca. Quando esiste una registrazione, l'analisi combina spettrogramma e metadati del file con il contesto: tabulati, canale di arrivo, verifiche con le persone coinvolte.

Cautele

I detector forniscono probabilità, da dichiarare con i tassi di errore (Modulo 8) e da confrontare con metadati, provenienza, testimonianze e tabulati. Esiste anche il **liar's dividend**: un contenuto autentico può essere contestato come falso.

Recupero di dati da database SQLite

Gran parte dei dati di interesse su un dispositivo mobile, come messaggi, chiamate, cronologie e posizioni, è conservata in database **SQLite**, nei quali i record cancellati non vengono rimossi subito. Un record eliminato finisce in spazio libero, cioè nei blocchi liberi delle pagine o nelle pagine della freelist, e resta leggibile finché non viene sovrascritto. Il **WAL** (write-ahead log) contiene le pagine modificate dalle transazioni recenti, mentre fino al checkpoint il file principale conserva le versioni precedenti. Anche i file di journal possono conservare copie di pagine anteriori alle modifiche. In relazione si distingue il dato presente nelle tabelle dal dato recuperato da spazio non allocato, perché affidabilità e contestabilità sono diverse.

Scenario didattico

Nell'ipotesi che l'indagato cancelli una conversazione la sera del fatto e che il telefono venga sequestrato acceso poche ore dopo, prima del checkpoint, il file principale del database conserva le pagine precedenti alla cancellazione, con i messaggi e i relativi timestamp, mentre il WAL contiene le pagine aggiornate. Anche la cancellazione, se collocabile nel tempo grazie ad altri artefatti, diventa un elemento di valutazione.

Ruolo dell'AI

Ogni app usa uno schema proprio, che cambia tra una versione e l'altra: un LLM può aiutare a interpretare schemi non documentati e a scrivere le query di estrazione. Il recupero da spazio non allocato resta affidato a strumenti dedicati e validati, e ogni risultato si verifica manualmente prima di entrare in relazione.

Indagini su container e Kubernetes

I container mettono in discussione un presupposto dell'analisi forense: che il sistema compromesso esista ancora quando l'indagine comincia. Un pod può restare attivo pochi minuti e, quando viene ricreato, riparte dallo stato dell'immagine: le modifiche dell'attaccante che non risiedono su volumi persistenti vanno perse. Le evidenze vanno quindi raccolte mentre il pod è attivo, con il checkpoint del container, la copia del layer scrivibile o lo snapshot del nodo, oppure devono essere già state esportate per scelta progettuale: log applicativi e **audit log** di Kubernetes inviati fuori dal cluster in tempo reale. L'indagine si basa sul confronto tra il container e la sua immagine, perché ogni differenza corrisponde ad attività svolta durante l'esecuzione, e sulla ricostruzione delle operazioni dai log centralizzati e dall'audit del control plane.

Scenario didattico

Si consideri un cryptominer attivo in un cluster, con il pod coinvolto già ricreato tre volte e quindi privo dello stato originale. L'audit log di Kubernetes mostra che il deployment è stato creato con le credenziali di un service account della pipeline CI, e il confronto tra l'immagine e il file system di un pod ancora attivo rivela il binario scaricato all'avvio.

Metodo

Nei sistemi effimeri la **forensic readiness** è un requisito di progetto: i dati non esportati in tempo reale possono non essere più disponibili dopo l'incidente. Lo stesso principio vale per gli ambienti cloud (approfondimento 2) e per i sistemi di AI (Modulo 14), in cui la registrazione degli eventi va progettata prima della messa in esercizio.

Metadati e geolocalizzazione dei contenuti

Un file multimediale contiene più informazioni di quelle visibili. I dati **EXIF** di una foto possono includere coordinate GPS, data, modello della fotocamera e direzione dello scatto, e i documenti Office registrano autore, data di creazione e numero di revisione. I metadati si modificano con facilità e vanno confermati da altre fonti; le piattaforme social li rimuovono spesso al caricamento, per cui la copia prelevata dal dispositivo ha più valore di quella scaricata da una piattaforma. In assenza di metadati si ricorre alla geolocalizzazione dal contenuto, che esamina ombre, vegetazione, cartelli e profilo degli edifici. Questa tecnica di verifica OSINT è oggi supportata da modelli di visione che propongono luoghi candidati da confrontare con fonti indipendenti.

Scenario didattico

Un alibi si fonda su una foto che sarebbe stata scattata in montagna alle 17:40 del giorno X. Le coordinate EXIF sono coerenti, ma l'ombra indica un sole troppo alto per quell'orario; il modello digitale del terreno e le effemeridi solari collocano lo scatto intorno a mezzogiorno. Resta da stabilire se l'orario nei metadati sia stato alterato o derivi da un errore dell'orologio del dispositivo.

Cautele

La geolocalizzazione assistita dall'AI produce ipotesi: ogni luogo candidato va verificato su immagini satellitari, fotografie d'archivio delle strade e fonti locali. Gli stessi strumenti possono servire a localizzare persone senza il loro consenso, con implicazioni trattate nel Modulo 15.

Indagine BEC e valutazione dei detector

Parte A • Caso BEC simulato

1. Analisi dei log M365: accessi anomali per geografia e orario
2. Individuazione delle regole di inoltramento e dei consensi OAuth malevoli
3. Cronologia della compromissione con esportazione verbalizzata dei log

Parte B • Deepfake detection

1. Valutazione di un set di immagini e audio, autentici e sintetici, con detector open source
2. Misura dei falsi positivi/negativi, anche dopo ricompressione
3. Discussione: cosa scrivereste in relazione?

Lecture e autovalutazione

Lecture obbligatorie

- NIST SP 800-101r1, *Guidelines on Mobile Device Forensics*
- Documentazione Microsoft sulle indagini nello Unified Audit Log
- Farid, *Photo Forensics*; specifica C2PA

Domande di autovalutazione

1. Quali vincoli giuridici limitano l'acquisizione dei dati di uno smartphone, e quali si aggiungono se si sfruttano vulnerabilità?
2. Quali log cloud documentano la compromissione di un account?
3. Perché l'esito di un deepfake detector non costituisce da solo una prova?
4. Che cosa attesta la provenienza C2PA e che cosa non può attestare?
5. Come cambia la catena di custodia per evidenze acquisite da cloud?

FINE DELLA LEZIONE • MODULO 10

Grazie

Mobile, cloud e multimedia 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