

MODULO 12 • AGOSTO 2026

# Laboratorio Integrato e Casi di Studio

L'indagine completa su sette casi di studio:  
dalla scena alla relazione peritale difesa in sede d'esame

NIST CFReDS • Digital Corpora • Enron • dataset sintetici

Corso di Laurea Magistrale in Sicurezza Informatica

# Ciascun gruppo conduce un'indagine completa

## FASE 1 • INCARICO

Il gruppo riceve quesito, reperti (dataset pubblici o sintetici) e vincoli di tempo: le condizioni di un incarico reale, inclusa l'ambiguità del quesito.

## FASE 2 • INDAGINE

Pipeline integrata sul caso della specializzazione scelta: metodologia classica e strumenti AI, con replica manuale su campione e log completo delle operazioni.

## FASE 3 • RESTITUZIONE

Relazione peritale completa, peer review incrociata tra gruppi e discussione orale con controesame del docente.

**Regole del laboratorio:** dataset esclusivamente pubblici e sintetici (NIST CFReDS, Digital Corpora, Enron); nessun dato reale su servizi AI esterni; ogni uso di AI dichiarato e validato; catena di custodia simulata ma formalmente completa.

# Il percorso del laboratorio integrato



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

# Il calendario operativo del laboratorio

| Sessione | Attività                                                                                                   | Esito atteso                            |
|----------|------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| 1        | Assegnazione dei casi, lettura delle schede, pianificazione dell'indagine e divisione dei ruoli nel gruppo | Piano d'indagine approvato dal docente  |
| 2        | Acquisizioni e analisi secondo la traccia core; avvio delle pipeline AI                                    | Reperti lavorati, log avviati           |
| 3        | Analisi AI-assistita, replica manuale in cieco su campione, consolidamento degli esiti                     | Protocollo di validazione completato    |
| 4        | Redazione della relazione, peer review incrociata tra gruppi, revisione finale                             | Relazione consegnata + scheda di review |

Il laboratorio simula le scadenze di un'indagine reale. La sessione 1 obbliga a pianificare prima di toccare i reperti; la peer review della sessione 4 anticipa il controesame che il docente condurrà in sede d'esame.

# Dalla kill chain alla rete di identità

| Caso                                  | Quesito e metodologia                                                                                          | Moduli mobilitati e ruolo dell'AI                                                    |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| 1 · Ransomware aziendale              | Ricostruire la kill chain da immagine disco e memory dump; Volatility, Plaso/Timesketch; relazione d'incidente | M2–M5, M8: triage AI-assistito dei log, validato in cieco                            |
| 2 · Deepfake vocale (caso Arup, 2024) | Frode da 25 M\$ via videoconferenza contraffatta: analisi di autenticità e protocollo anti-frode               | M10: detection multilivello; M11: valore probatorio del giudizio                     |
| 3 · Mobile in sede penale             | Messaggistica, geolocalizzazione, attribuzione del dispositivo; discussione del precedente Apple–FBI           | M6, M9: correlazione NLP delle conversazioni, con rimando ai reperti                 |
| 4 · Silk Road                         | Attribuzione di identità online tramite OSINT e correlazione di tracce testuali                                | M9: che cosa cambierebbe oggi con entity resolution AI, e con quali rischi di errore |

I casi storici (2 e 4) si studiano su fonti pubbliche e si **rigiocano** su dataset sintetici predisposti, così che l'esercizio si svolga su dati di laboratorio.

# Ransomware: la traccia dell'indagine attesa

1. **Accesso iniziale:** dai log VPN e di posta, il vettore (credenziali compromesse o allegato); dalla timeline, il primo host toccato
2. **Esecuzione e persistenza:** dal memory dump (Volatility), il processo malevolo e il suo avvio; dal registry e dai task, il meccanismo di persistenza
3. **Movimento laterale:** dagli event log correlati, la sequenza host-per-host, con il triage AI dei log a prioritizzare e la replica in cieco a validare
4. **Esfiltrazione e cifratura:** dai flussi di rete, l'eventuale uscita dei dati prima della cifratura; dalla super-timeline, l'ora zero
5. **Relazione:** kill chain ricostruita, ogni anello con le sue evidenze, limiti dichiarati

## Le domande del committente

- Da dove sono entrati, e quando?
- Che cosa hanno toccato, e che cosa hanno portato via?
- Sono ancora dentro?
- Che cosa dobbiamo notificare, e a chi?

La relazione è buona se risponde a queste quattro, nell'ordine in cui le farebbe un consiglio di amministrazione.

# Dal corpus Enron alla scena del crimine algoritmica

| Caso                                   | Quesito e metodologia                                                                          | Moduli mobilitati e ruolo dell'AI                                       |
|----------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| 5 · Email forensics (corpus Enron)     | Topic modeling, grafo relazionale, comunicazioni anomale su dataset pubblico consolidato       | M9: pipeline NLP completa con validazione manuale su campione           |
| 6 · Prova fabbricata con AI generativa | Stabilire se immagini e documenti prodotti «in giudizio» siano autentici o sintetici           | M10: metadati, ELA, detector, provenance C2PA, con i limiti di ciascuno |
| 7 · Compromissione di un sistema LLM   | Prompt injection ed esfiltrazione da un chatbot aziendale simulato: ricostruzione dell'attacco | M10: forensics sull'AI; M5: log di inferenza come fonte di rete         |

Nei casi 1–5 l'AI è uno strumento d'indagine, nei casi 6–7 ne è l'oggetto: la sequenza segue lo sviluppo del corso.

# Caso 6: la prova sospetta di fabbricazione

In un procedimento civile una parte produce lo screenshot di una conversazione, che l'altra disconosce integralmente. Quesito: **la conversazione è autentica, fabbricata o non determinabile?**

Il percorso atteso: (1) **gerarchia delle fonti**: lo screenshot è il gradino più basso; si chiedono dispositivi e database originali delle app (modulo 6); (2) **analisi dell'immagine**: metadati, tracce di fotomontaggio o generazione (modulo 10); (3) **riscontri esterni**: tabulati, backup, log del provider (moduli 5-6); (4) **formulazione**: tre ipotesi esplicite, pesate sull'evidenza, senza oltrepassare i dati.

Il materiale è sintetico e predisposto dal docente; a seconda della variante, la conversazione è autentica, fabbricata o indeterminabile.

## CRITERI DI VALUTAZIONE

Se i dispositivi originali non sono disponibili e mancano riscontri, la risposta «non determinabile» è un esito **professionalmente corretto**.

La valutazione premia la qualità del percorso e l'onestà della conclusione; è penalizzato il gruppo che afferma una fabbricazione non sostenuta dal materiale.

# Ogni caso contiene errori da non commettere

I dataset dei casi sono costruiti con insidie deliberate, una per famiglia di errore vista nel corso. Alcuni esempi del repertorio (variano per gruppo):

- Un file **timestompato** che la sola lettura di \$SI daterebbe male (modulo 3)
- Una **falsa pista**: un processo dal nome sospetto ma legittimo, che punisce l'attribuzione frettolosa (modulo 4)
- Un'**anomalia benigna** nei log (la manutenzione notturna) che il triage AI segnala e la validazione deve riclassificare (modulo 8)
- Un documento del fascicolo **generato con AI**, da intercettare in autenticazione (modulo 10)
- Dati di **terzi estranei** nel corpus, che non devono comparire in relazione (modulo 11)

## Come vengono valutate

Si premia chi trova la trappola e, in misura quasi pari, chi **vi cade e se ne accorge** durante la peer review: il corso vuole formare l'abitudine alla revisione.

L'unico esito davvero penalizzato è difendere l'errore in sede orale, perché l'arroccamento è un difetto di metodo.

# Criticare una relazione altrui

## Dove guardare

Catena di custodia e hash **verificabili**; metodo dichiarato e ripetibile; versioni degli strumenti; salti logici fra dato e conclusione; alternative non considerate; limiti taciuti (calibrazione, dominio di validazione, drift).

## Come scrivere la critica

La critica riguarda il metodo, senza attacchi personali. Ogni rilievo è **specifico e verificabile**: pagina, passaggio, motivo, che cosa sarebbe servito. Dare atto delle parti corrette rafforza i rilievi.

## L'errore da evitare

La critica totale e indiscriminata: i rilievi fondati si perdono fra quelli generici e il giudice percepisce il consulente come **schierato**.

**IN AULA** • Ogni gruppo riceve la relazione di un altro gruppo, su un caso diverso dal proprio, e ne redige una memoria critica di due pagine. Fare da revisori e sapere di essere letti da pari aiuta a evitare conclusioni eccessive.

# Il deliverable che riassume il corso

## Struttura obbligatoria

1. Incarico e quesito; qualifiche del gruppo
2. Reperti e catena di custodia
3. Metodologia: strumenti, versioni, standard di riferimento
4. Uso dell'AI: le cinque voci del modulo 11, per ogni strumento
5. Accertamenti e risultati, con rimando puntuale ai reperti
6. Valutazioni conclusive: certezze, probabilità, limiti
7. Allegati: log, hash, protocolli di validazione

## Rubrica di valutazione

- Correttezza metodologica · 30%
- Tracciabilità delle affermazioni · 25%
- Uso e validazione dell'AI · 20%
- Chiarezza espositiva per un lettore non tecnico · 15%
- Consapevolezza dei limiti · 10%

La rubrica è consegnata con l'incarico, così i criteri sono noti in anticipo.

# Il controesame d'esame: struttura e criteri

La discussione finale simula l'esame del consulente in udienza, in tre fasi: **esposizione** (10 minuti: il candidato presenta metodo e conclusioni a un «giudice» non tecnico, puntando alla chiarezza senza semplificazioni scorrette); **controesame** (15 minuti: un docente nel ruolo del consulente avversario attacca i punti deboli della relazione depositata); **quesito a sorpresa** (5 minuti: un elemento nuovo, «e se emergesse che...?», per valutare il ragionamento in tempo reale).

I criteri premiano la condotta professionale: **distinguere ciò che si sa da ciò che si inferisce**, ammettere i limiti prima che emergano dalle domande, correggersi quando serve, rinunciare alle tesi insostenibili. Le cinque voci sull'uso dell'AI richieste nella relazione sono sempre oggetto di domanda.

## ESEMPIO • LA DOMANDA TIPO

«Lei scrive che il triage AI ha selezionato 240 conversazioni rilevanti. Come fa a sapere che cosa c'era in quelle che ha scartato?»

Vale il massimo chi dichiara il recall stimato dello strumento sul set di validazione, il campionamento di controllo effettuato sugli scarti e il residuo di incertezza che rimane. Una risposta generica («lo strumento è molto affidabile») comporta invece la bocciatura.

# Valutazione finale e sviluppi futuri

## Composizione del voto

- **40%** • Prova scritta sui moduli della traccia core e delle due specializzazioni
- **40%** • Progetto di laboratorio (relazione peritale)
- **20%** • Discussione orale con controesame

## Sviluppi futuri

- Forensics dei sistemi agentici: azioni autonome da ricostruire
- La prova generata da AI nel processo
- Standardizzazione internazionale (SWGDE, ENFSI) sull'AI forense

## Il profilo in uscita

Un perito che padroneggia il metodo forense classico e impiega l'AI solo dove metriche e motivazioni ne giustificano l'uso.

Il metodo insegnato non dipende dagli strumenti: documentare, preservare, validare, rispondere del proprio operato.



# Grazie per l'attenzione

**Vincenzo Calabrò**

Domande, materiali del corso e contatti  
sul sito del docente



[vincenzocalabro.it](https://vincenzocalabro.it)