

```
root@hacklab:~/parte-02/lezione-23
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE II

## LEZIONE 23

# Digital Forensics avanzata

Branche avanzate della forensics, anti-forensics e valore probatorio.

docente **Vincenzo Calabro**      fase Specializzazione avanzata: Digital Forensics avanzata

```
root@hacklab:~/lezione-23/agenda $
```

LEZIONE 23 / AGENDA

# In questa lezione

// PERCORSO

- > Mobile forensics
- > Cloud e container forensics
- > Anti-forensics
- > Threat hunting forense
- > Perizia e valore probatorio

metodo   obiettivi -> teoria -> strumenti -> laboratorio -> caso di studio -> etica -> verifica

```
root@hacklab:~/lezione-23/obiettivi $
```

LEZIONE 23 / OBIETTIVI

# Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – forensics avanzata (mobile, cloud, effimera)
- > Applicare – mobile e cloud forensics
- > Analizzare – scenari con tecniche di anti-forensics
- > Valutare – l'ammissibilità probatoria
- > Creare – una perizia forense difendibile

```
root@hacklab:~/lezione-23/inquadramento $
```

LEZIONE 23 / INQUADRAMENTO

# Inquadramento

// DI COSA PARLIAMO

Oltre il disco: mobile, cloud e anti-forensics richiedono tecniche e cautele probatorie avanzate. La lezione punta a evidenze solide e a una perizia difendibile in contraddittorio.

// PERCHE' CONTA

Branche avanzate della forensics, anti-forensics e valore probatorio.

```
root@hacklab:~/lezione-23/mappa-insieme $
```

LEZIONE 23 / MAPPA // INSIEME

# Mappa d'insieme del modulo

■ Attacco/tecnica   ■ Difesa   ■ Norme & metodo   ■ IA

## FONDAMENTI

- 01 Mobile forensics
- 02 Cloud forensics
- 03 Tecniche anti-forensics
- 04 Threat hunting forense
- 05 Perizia, testimonianza e IA

## APPROFONDIMENTI

- 06 Acquisizione e cifratura
- 07 Log, API e giurisdizione
- 08 Riconoscere l'anti-forensics
- 09 Correlazione multi-sorgente
- 10 Contraddittorio e limiti dell'IA

```
root@hacklab:~/lezione-23/flusso-1 $
```

LEZIONE 23 / FLUSSO // FONDAMENTI

## Sequenza di fasi – Fondamenti

■ Attacco/tecnica   ■ Difesa   ■ Norme & metodo   ■ IA



> Le fasi si susseguono: l'esito di ciascuna alimenta la successiva.

```
root@hacklab:~/lezione-23/concetto-1 $
```

LEZIONE 23 / CONCETTO 1/10

[ Attacco/tecnica ]

# Mobile forensics

## // SPIEGAZIONE

Sui dispositivi mobili l'acquisizione può essere logica, limitata ai dati applicativi, o fisica, sull'intera memoria, complicata dalla cifratura di default. Artefatti di localizzazione, app e comunicazioni ricostruiscono movimenti e attività dell'utente.

## // ESEMPIO

> L'acquisizione fisica recupera dati cancellati che quella logica non vedrebbe.

```
root@hacklab:~/lezione-23/concetto-2 $
```

LEZIONE 23 / CONCETTO 2/10

[ Attacco/tecnica ]

# Cloud forensics

## // SPIEGAZIONE

Nel cloud le prove sono log e dati accessibili via API, spesso distribuiti tra giurisdizioni diverse. I container effimeri spariscono alla terminazione: senza logging e snapshot preventivi, l'evidenza semplicemente non esiste piu.

## // ESEMPIO

> Un container compromesso viene distrutto: restano solo i log centralizzati, se attivati prima.

```
root@hacklab:~/lezione-23/concetto-3 $
```

LEZIONE 23 / CONCETTO 3/10

[ Attacco/tecnica ]

## Tecniche anti-forensics

### // SPIEGAZIONE

Chi vuole nascondere le tracce usa il wiping per cancellare in modo irreversibile, la steganografia per occultare dati dentro file innocui, il timestomping per alterare le date. Riconoscerle e documentarle è parte dell'analisi avanzata.

### // ESEMPIO

> Timestamp di sistema incoerenti tra loro rivelano un timestomping in atto.

```
root@hacklab:~/lezione-23/concetto-4 $
```

LEZIONE 23 / CONCETTO 4/10

[ Attacco/tecnica ]

## Threat hunting forense

### // SPIEGAZIONE

Il threat hunting forense cerca proattivamente tracce di compromissione correlando artefatti da più fonti: endpoint, rete, log. Invece di attendere un alert, si formulano ipotesi e si verificano sulle evidenze raccolte.

### // ESEMPIO

> Ipotesi 'persistenza via task pianificato' verificata incrociando registro e log di esecuzione.

```
root@hacklab:~/lezione-23/concetto-5 $
```

LEZIONE 23 / CONCETTO 5/10

[ Norme & metodo ]

## Perizia, testimonianza e IA

### // SPIEGAZIONE

Il forense può operare come CTU per il giudice o CTP per una parte, e sostenere le conclusioni in contraddittorio. L'IA può assistere l'analisi, ma i suoi output vanno spiegati e verificati: non hanno da soli valore probatorio.

### // ESEMPIO

> In perizia si spiega il metodo in modo che un non tecnico possa valutarne l'affidabilità.

```
root@hacklab:~/lezione-23/flusso-2 $
```

LEZIONE 23 / FLUSSO // APPROFONDIMENTI

## Sequenza di fasi – Approfondimenti

■ Attacco/tecnica   ■ Difesa   ■ Norme & metodo   ■ IA



> Le fasi si susseguono: l'esito di ciascuna alimenta la successiva.

```
root@hacklab:~/lezione-23/concetto-6 $
```

LEZIONE 23 / CONCETTO 6/10

[ Attacco/tecnica ]

## Acquisizione e cifratura

### // SPIEGAZIONE

La cifratura dei dispositivi moderni limita cosa e acquisibile: senza chiave o accesso sbloccato, l'acquisizione fisica puo restituire solo dati cifrati. Metodo, tempistica e stato del dispositivo determinano cosa si riesce a preservare.

### // ESEMPIO

> Un telefono acquisito da spento e cifrato restituisce molto meno di uno gia sbloccato.

```
root@hacklab:~/lezione-23/concetto-7 $
```

LEZIONE 23 / CONCETTO 7/10

[ Attacco/tecnica ]

## Log, API e giurisdizione

### // SPIEGAZIONE

Raccogliere prove nel cloud dipende dai log disponibili, dalle API del provider e dalle regole di giurisdizione su dove risiedono i dati. La cooperazione e i tempi legali diventano parte integrante dell'indagine.

### // ESEMPIO

> Dati ospitati all'estero richiedono procedure di cooperazione per essere acquisiti lecitamente.

```
root@hacklab:~/lezione-23/concetto-8 $
```

LEZIONE 23 / CONCETTO 8/10

[ Attacco/tecnica ]

## Riconoscere l'anti-forensics

### // SPIEGAZIONE

Spazi non allocati sospetti, file con entropia anomala, date incoerenti sono segnali di wiping, steganografia o timestomping. L'analista li documenta come tali: anche l'assenza o l'alterazione di dati e un'evidenza.

### // ESEMPIO

> Un'immagine con dati nascosti mostra dimensione ed entropia non spiegabili dal contenuto visibile.

```
root@hacklab:~/lezione-23/concetto-9 $
```

LEZIONE 23 / CONCETTO 9/10

[ Attacco/tecnica ]

## Correlazione multi-sorgente

### // SPIEGAZIONE

La forza dell'indagine avanzata è correlare fonti diverse, disco, memoria, rete, cloud e mobile, in un'unica narrazione coerente. Un singolo artefatto può essere ambiguo; più fonti concordi rendono la ricostruzione solida.

### // ESEMPIO

> L'orario di un login combacia tra log del server, artefatto dell'endpoint e traffico di rete.

```
root@hacklab:~/lezione-23/concetto-10 $
```

LEZIONE 23 / CONCETTO 10/10

[ Norme & metodo ]

## Contraddittorio e limiti dell'IA

### // SPIEGAZIONE

In giudizio le conclusioni vanno difese nel contraddittorio tra periti. Un risultato prodotto dall'IA va spiegato nel metodo e verificabile in modo indipendente: ciò che non è riproducibile e spiegabile difficilmente regge come prova.

### // ESEMPIO

> Un classificatore IA che segnala un file va validato con analisi manuale prima di citarlo.

```
root@hacklab:~/lezione-23/strumenti $
```

LEZIONE 23 / STRUMENTI

# Strumenti della lezione

// TOOLKIT

Autopsy

Cellebrite (tipo)

strumenti cloud

Volatility

Plaso

YARA

// NOTA OPERATIVA

> Ogni strumento si usa in ambiente virtualizzato e isolato, solo su bersagli di proprietà o autorizzati. Output e artefatti vanno protetti e, a fine ingaggio, gestiti o distrutti.

```
root@hacklab:~/lezione-23/lab-1 $
```

LEZIONE 23 / LABORATORIO 1

# Laboratorio 1

**\$ Mobile forensics (artefatti applicativi)**

**// PROCEDURA**

**[1]** Analizza un'immagine mobile e correla gli artefatti applicativi

**[ ! ]** Verifica: Come si preserva l'integrità con dispositivi cifrati?

```
root@hacklab:~/lezione-23/lab-2 $
```

LEZIONE 23 / LABORATORIO 2

## Laboratorio 2

**\$ Scenario anti-forensics (mini-perizia)**

**// PROCEDURA**

**[1]** Indaga uno scenario con tracce di anti-forensics e produci una mini-perizia

**[ ! ]** Verifica: Come si riconosce e documenta l'anti-forensics?

```
root@hacklab:~/lezione-23/caso-di-studio $
```

LEZIONE 23 / CASO DI STUDIO

# Caso di studio

## // SCENARIO

> Caso giudiziario anonimizzato in cui la forensics è stata decisiva, con le sfide di ammissibilità.

## // ANALISI RICHIESTA

- > Ricostruisci la dinamica dei fatti con metodo e tracciabilità
- > Individua errori, cause radice e punti di decisione critici
- > Proponi contromisure, controlli e lezioni apprese

```
root@hacklab:~/lezione-23/etica $
```

LEZIONE 23 / ETICA & DIRITTO

# Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta   scope definito   ambiente isolato   dati protetti   responsible disclosure

// SPECIFICO DELLA LEZIONE

[ ! ] Dati sensibili e probatori: rigore assoluto nella catena di custodia, GDPR e norme processuali.

```
root@hacklab:~/lezione-23/ricapitolazione $
```

LEZIONE 23 / RICAPITOLAZIONE

# Ricapitolazione

// PUNTI CHIAVE

- > Forensics avanzata (mobile, cloud, effimera)
- > Mobile e cloud forensics
- > Scenari con tecniche di anti-forensics
- > L'ammissibilità probatoria
- > Una perizia forense difendibile

```
root@hacklab:~/lezione-23/verifica $
```

LEZIONE 23 / AUTOVALUTAZIONE

# Autovalutazione

## // DOMANDE DI VERIFICA

- ? Come si preserva l'integrità con dispositivi cifrati?
- ? Come si riconosce e documenta l'anti-forensics?
- ? Cosa rende una perizia ammissibile in giudizio?

## // VALUTAZIONE

Perizia forense completa su caso complesso, con rubrica probatoria.

## // LETTURE

NIST SP 800-101 e 800-86; materiali su cloud forensics.

# lezione 23 completata

# \$ next

## Digital Forensics avanzata

[ ! ] Le competenze di questa lezione si impiegano esclusivamente in contesti legali, autorizzati e deontologicamente corretti, entro lo scope e con autorizzazione scritta.

root@hacklab:~# \_

```
root@hacklab:~/contatti $
```

CONTATTI / RISORSE

# Restiamo in contatto

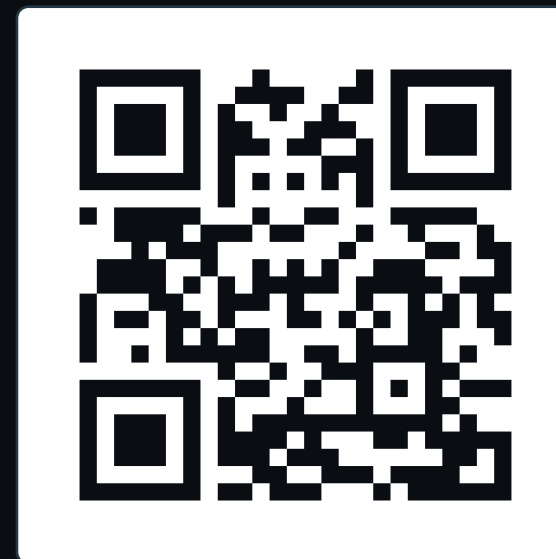


## Vincenzo Calabro

cyber security / digital forensics /  
docenza e divulgazione

// SCANSIONA O VISITA

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



Inquadra il QR con la fotocamera  
per aprire il sito.