

```
root@hacklab:~/parte-01/lezione-10
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE I

LEZIONE 10

Digital Forensics e Incident Response

Acquisizione e analisi di evidenze su disco, memoria e rete, con un processo completo di incident response.

docente **Vincenzo Calabro**

fase Difesa e indagine: Digital Forensics e Incident Response

```
root@hacklab:~/lezione-10/agenda $
```

LEZIONE 10 / AGENDA

In questa lezione

// PERCORSO

- > Catena di custodia e ordine di volatilità
- > Acquisizione e imaging
- > Disk, memory e network forensics
- > Super-timeline e correlazione
- > Incident response secondo NIST

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

```
root@hacklab:~/lezione-10/obiettivi $
```

LEZIONE 10 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – principi e quadro giuridico della forensics
- > Applicare – acquisizione e analisi multi-sorgente
- > Analizzare – timeline, artefatti ed evidenze
- > Valutare – catena di custodia e ammissibilità
- > Creare – un processo IR (NIST) e un report difendibile

```
root@hacklab:~/lezione-10/inquadramento $
```

LEZIONE 10 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Quando un incidente accade, conta preservare le evidenze e ricostruire i fatti senza alterarli. La lezione unisce acquisizione forense, analisi su disco, memoria e rete, e il processo di incident response secondo NIST.

// PERCHE' CONTA

Acquisizione e analisi di evidenze su disco, memoria e rete, con un processo completo di incident response.

```
root@hacklab:~/lezione-10/mappa-insieme $
```

LEZIONE 10 / MAPPA // INSIEME

Mappa d'insieme del modulo

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

FONDAMENTI

- 01 Catena di custodia e volatilità
- 02 Imaging, write blocker e hash
- 03 Forensics su disco, memoria e rete
- 04 Super-timeline e IR NIST
- 05 Mobile, cloud, anti-forensics e IA

APPROFONDIMENTI

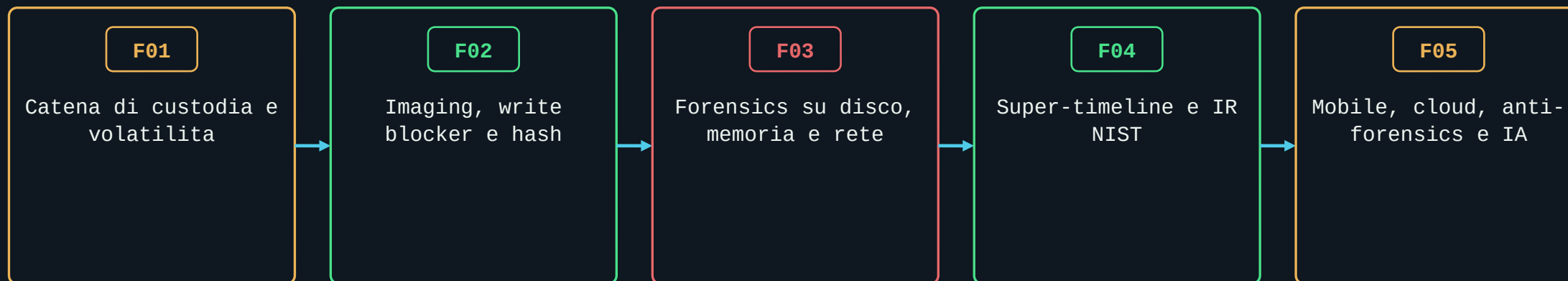
- 06 Integrità dei supporti
- 07 Artefatti di sistema Windows
- 08 Ricostruzione di C2 ed esfiltrazione
- 09 Fasi NIST dell'incident response
- 10 Limiti probatori e anti-forensics

```
root@hacklab:~/lezione-10/flusso-1 $
```

LEZIONE 10 / 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-10/concetto-1 $
```

LEZIONE 10 / CONCETTO 1/10

[Norme & metodo]

Catena di custodia e volatilità

// SPIEGAZIONE

La prova digitale vale in giudizio solo se integra e tracciabile: la catena di custodia documenta chi ha toccato cosa e quando. L'ordine di volatilità impone di acquisire prima ciò che svanisce, come RAM e connessioni, poi il disco; ISO/IEC 27037 ne fissa le buone pratiche.

// ESEMPIO

> Si acquisisce la RAM prima di spegnere, perché al riavvio i dati volatili spariscono.

```
root@hacklab:~/lezione-10/concetto-2 $
```

LEZIONE 10 / CONCETTO 2/10

[Difesa]

Imaging, write blocker e hash

// SPIEGAZIONE

L'acquisizione forense crea una copia bit a bit del supporto usando un write blocker che impedisce ogni scrittura sull'originale. L'hash calcolato prima e dopo prova che la copia è identica e che nulla è stato alterato.

// ESEMPIO

> Hash sorgente uguale ad hash copia conferma integrità; il write blocker protegge l'originale.

```
root@hacklab:~/lezione-10/concetto-3 $
```

LEZIONE 10 / CONCETTO 3/10

[Attacco/tecnica]

Forensics su disco, memoria e rete

// SPIEGAZIONE

L'analisi si articola su tre fronti: il disco con Autopsy e TSK per file e artefatti, la memoria con Volatility per processi e codice iniettato, la rete con Wireshark e Zeek per ricostruire comunicazioni ed esfiltrazioni.

// ESEMPIO

> Zeek trasforma un PCAP in log di connessioni, utile per ricostruire un canale C2.

```
root@hacklab:~/lezione-10/concetto-4 $
```

LEZIONE 10 / CONCETTO 4/10

[Difesa]

Super-timeline e IR NIST

// SPIEGAZIONE

La super-timeline con Plaso unisce timestamp da molte fonti in un'unica sequenza per ricostruire l'accaduto. L'incident response segue le fasi NIST SP 800-61: preparazione, rilevamento, contenimento, eradicazione, ripristino e lezioni apprese.

// ESEMPIO

> Una super-timeline correla l'apertura di un allegato con la successiva connessione C2.

```
root@hacklab:~/lezione-10/concetto-5 $
```

LEZIONE 10 / CONCETTO 5/10

[Norme & metodo]

Mobile, cloud, anti-forensics e IA

// SPIEGAZIONE

Dispositivi mobili, cloud e tecniche anti-forensics complicano l'indagine con cifratura, giurisdizioni e cancellazioni mirate. Nel triage di grandi volumi l'IA è di aiuto, ma i suoi output non hanno di per sé valore probatorio e vanno verificati.

// ESEMPIO

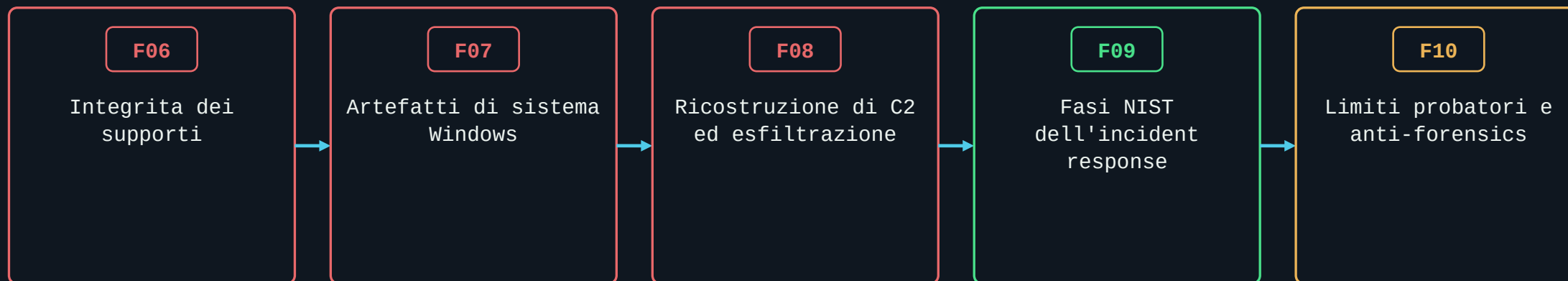
> L'IA segnala file sospetti in un'immagine; l'analista li valida prima di citarli in perizia.

```
root@hacklab:~/lezione-10/flusso-2 $
```

LEZIONE 10 / 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-10/concetto-6 $
```

LEZIONE 10 / CONCETTO 6/10

[Attacco/tecnica]

Integrità dei supporti

// SPIEGAZIONE

Ogni supporto acquisito va identificato, protetto da scrittura e verificato con hash a ogni passaggio. Una gestione rigorosa, con sigilli e registro, e ciò che rende la prova ammissibile e resistente alle contestazioni in dibattimento.

// ESEMPIO

> Hash SHA-256 registrato all'acquisizione e ricontrollato prima dell'analisi.

```
root@hacklab:~/lezione-10/concetto-7 $
```

LEZIONE 10 / CONCETTO 7/10

[Attacco/tecnica]

Artefatti di sistema Windows

// SPIEGAZIONE

Windows conserva tracce dell'attività: il registro, i file prefetch con i programmi eseguiti, gli shellbags con le cartelle visitate, la cronologia del browser. Questi artefatti ricostruiscono cosa è stato fatto, quando e da chi, anche senza i file originali.

// ESEMPIO

> Il prefetch mostra che un eseguibile malevolo è stato lanciato tre volte e quando.

```
root@hacklab:~/lezione-10/concetto-8 $
```

LEZIONE 10 / CONCETTO 8/10

[Attacco/tecnica]

Ricostruzione di C2 ed esfiltrazione

// SPIEGAZIONE

Dai log di rete si ricostruiscono i canali di comando e l'eventuale esfiltrazione di dati: domini contattati, volumi, orari. Zeek sintetizza il traffico in log analizzabili, dove un trasferimento anomalo verso l'esterno diventa evidente.

// ESEMPIO

> Un upload di centinaia di MB verso un host sconosciuto di notte segnala esfiltrazione.

```
root@hacklab:~/lezione-10/concetto-9 $
```

LEZIONE 10 / CONCETTO 9/10

[Difesa]

Fasi NIST dell'incident response

// SPIEGAZIONE

Dopo il rilevamento, il contenimento limita il danno isolando host e revocando credenziali, l'eradicazione rimuove la causa, il ripristino riporta i servizi in sicurezza. Chiudere con le lezioni apprese evita che l'incidente si ripeta.

// ESEMPIO

> Si isola l'host compromesso dalla rete prima di eradicare, per fermare la propagazione.

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

LEZIONE 10 / CONCETTO 10/10

[Norme & metodo]

Limiti probatori e anti-forensics

// SPIEGAZIONE

Anti-forensics come wiping e timestomping e ambienti cloud effimeri possono distruggere o rendere inaccessibili le prove. Un output IA, per quanto utile, non è di per sé prova: serve metodo documentato e verificabile perché regga nel contraddittorio.

// ESEMPIO

> Timestamp alterati col timestomping vanno riconosciuti e segnalati, non presi per buoni.

```
root@hacklab:~/lezione-10/strumenti $
```

LEZIONE 10 / STRUMENTI

Strumenti della lezione

// TOOLKIT

Autopsy

The Sleuth Kit

Volatility

FTK Imager

EnCase

Wireshark

Zeek

Plaso

// 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-10/lab-1 $
```

LEZIONE 10 / LABORATORIO 1

Laboratorio 1

\$ Acquisizione e analisi disco (FTK Imager + Autopsy)

// PROCEDURA

- [1]** Acquisisci con FTK Imager
- [2]** verifica l'hash
- [3]** analizza con Autopsy e documenta la custodia

[!] Verifica: Perché write blocker e verifica hash sono imprescindibili?

```
root@hacklab:~/lezione-10/lab-2 $
```

LEZIONE 10 / LABORATORIO 2

Laboratorio 2

\$ Memory & network forensics (Volatility + PCAP)

// PROCEDURA

[1] Analizza un dump con Volatility e correla un PCAP; costruisci la super-timeline

[!] Verifica: Perché l'ordine di volatilità guida l'acquisizione?

```
root@hacklab:~/lezione-10/lab-3 $
```

LEZIONE 10 / LABORATORIO 3

Laboratorio 3

\$ Incident response end-to-end (fasi NIST)

// PROCEDURA

[1] Esegui le fasi NIST su uno scenario e redigi il rapporto con lessons learned

[!] Verifica: Quali cautele per un output prodotto da un'IA in sede probatoria?

```
root@hacklab:~/lezione-10/caso-di-studio $
```

LEZIONE 10 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Risposta a un incidente ransomware reale (dinamiche di tipo Colonial Pipeline), dalla rilevazione alla post-mortem.

// 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-10/etica $
```

LEZIONE 10 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Dati personali e probatori: rigore nella catena di custodia, GDPR e coordinamento con l'autorità.

```
root@hacklab:~/lezione-10/ricapitolazione $
```

LEZIONE 10 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > Principi e quadro giuridico della forensics
- > Acquisizione e analisi multi-sorgente
- > Timeline, artefatti ed evidenze
- > Catena di custodia e ammissibilità
- > Un processo IR (NIST) e un report difendibile

```
root@hacklab:~/lezione-10/verifica $
```

LEZIONE 10 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Perché write blocker e verifica hash sono imprescindibili?
- ? Perché l'ordine di volatilità guida l'acquisizione?
- ? Quali cautele per un output prodotto da un'IA in sede probatoria?

// VALUTAZIONE

Report forense completo su caso simulato + quiz sul processo di IR.

// LETTURE

NIST SP 800-61 e 800-86; ISO/IEC 27037; doc. Volatility/Autopsy.

lezione 10 completata

\$ next

Digital Forensics e Incident Response

[!] 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



Inquadra il QR con la fotocamera
per aprire il sito.