



La Scienza del Digitale: evoluzione evoluzione e riconoscimento della della figura dell'Informatico Forense

UN VIAGGIO NELLA DIGITAL FORENSICS E NELLE TECNICHE DI
INVESTIGAZIONE DIGITALE

10 giugno 2025 | Ore 9.15-16.30 | Sala convegni dell'Università degli Studi di
Brescia



Relatore: Prof. Ing. Michele Vitiello

Esperto di Ingegneria Informatica Forense

- 20 anni di esperienza e oltre 3.000 casi trattati
- Consulente per Procure, Tribunali, EPPO e Eurojust
- Docente della Scuola Superiore della Magistratura
- Professore in Informatica Forense presso UNINETTUNO
- Premiato con Investigation & Forensic Awards 2022
- Consigliere dell'Ordine degli Ingegneri della Provincia di Brescia
- Incarichi nazionali per l'Ingegneria Forense e l'Innovazione
- Ha contribuito a casi di rilievo nazionale (Pipitone, Alvarez, Mottarone, Bibbiano)
- Ospite in programmi TV/radio (Rai, Canale 5, ABC, CBC)
- Autore del libro: L'imputato è il tuo smartphone: Crimini, Investigazioni e Tecnologie al servizio della Giustizia

Chi è l'Informatico Forense: Evoluzione della Figura

1 Origini (Anni '80-'90)

Attività di recupero dati con approccio "hacker-style", focalizzata sul ripristino di informazioni cancellate.

2 Transizione

Professionalizzazione della disciplina con integrazione in ambito legale e di compliance aziendale.

3 Ruolo Odierno

Professionista certificato che gestisce incident response e investigazioni digitali con competenze tecniche e legali. Può ricoprire ruoli come CTU, CTPM e CTP per procedimenti giudiziari.

La digital forensics è nata come attività tecnica di recupero dati, ma si è rapidamente evoluta in una professione riconosciuta. Oggi, l'informatico forense **deve bilanciare competenze tecniche avanzate e trasversali con una solida conoscenza delle normative legali, legali, diventando una figura chiave nelle indagini penali, aziendali e di sicurezza informatica.**





Best Practices Generali



Catena di Custodia

Documentazione rigorosa di ogni passaggio, dalla raccolta all'analisi, per all'analisi, per garantire l'integrità delle prove digitali.



Documentazione Dettagliata

Logging completo di ogni operazione effettuata, specificando chi, come e quando ha eseguito ciascuna attività.



Ambiente Forense

Utilizzo di write-blocker per prevenire modifiche accidentali ai supporti originali durante l'acquisizione e utilizzo di strumentazione strumentazione riconosciuta dalla comunità scientifica.



Verifica e Validazione

Verifica dell'integrità tramite algoritmi hash.

Queste regole auree sono fondamentali per garantire l'**ammissibilità legale** delle prove digitali. La rigorosa aderenza a questi principi assicura dell'analisi forense dell'analisi forense siano **ripetibili** e **verificabili**, elementi essenziali in qualsiasi procedimento e contenzioso legale, soprattutto per i procedimenti penali.

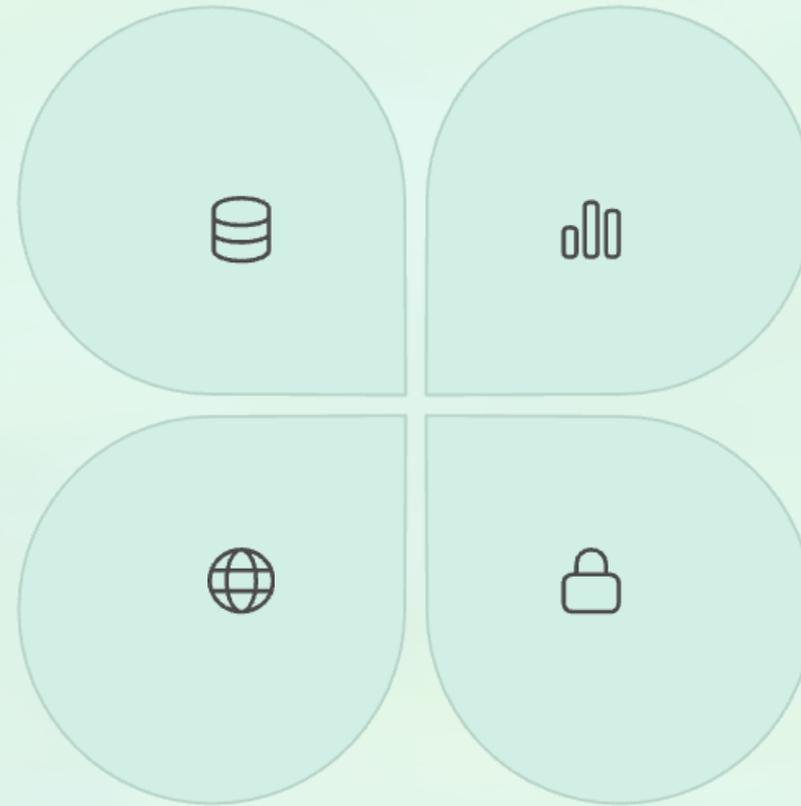
Problematiche Comuni

Molteplicità di File System

Necessità di competenze su NTFS, APFS, ext4 e altri file system per recuperare dati da diverse piattaforme.

Vincoli Giurisdizionali

Navigazione tra diverse normative nazionali e internazionali che influenzano la raccolta e l'utilizzo delle prove.



Volume Crescente di Dati

Gestione di **grandi moli di dati** che richiedono strumenti di analisi avanzati e tempi di elaborazione molto estesi.

Privacy e GDPR

Bilanciamento tra esigenze investigative e rispetto delle normative sulla protezione dei dati personali.

Ogni caso forense presenta **sfide uniche** che richiedono approcci personalizzati. La complessità aumenta quando si considerano i diversi sistemi operativi, l'enorme quantità di dati da analizzare e le restrizioni legali, **richiedendo una stretta collaborazione con collaborazioni con esperti legali, Forze dell'Ordine e membri dell'apparato giudiziario.**

Sfide nella Computer Forensics

Crittografia Avanzata

Superamento delle protezioni come BitLocker su Windows e FileVault su macOS, oltre alle sfide poste dai chip di sicurezza T2/M1/M2 di Apple.

Supporti Danneggiati

Recupero di dati da dispositivi fisicamente o logicamente compromessi che richiedono tecniche specializzate di data recovery (camera bianca/cambio parti e AceLaboratory PC3000).

Big Data Forensics

Analisi efficiente di dataset immensi attraverso tecniche di parallelizzazione e algoritmi ottimizzati per non bloccare l'indagine.

Le sfide tecniche nella computer forensics richiedono **competenze specializzate** e **strumenti all'avanguardia**. La **crittografia moderna** rappresenta uno degli ostacoli più significativi, specialmente con l'evoluzione dei sistemi di sicurezza hardware come quelli implementati nei dispositivi Apple più recenti.

Il recupero da supporti danneggiati spesso richiede l'intervento di **laboratori specializzati**, mentre l'analisi di grandi volumi di dati **richiede** **dati necessita di infrastrutture computazionalmente molto elevate** per ottenere risultati in **tempi ragionevoli**.

Tecniche di Decifrazione e Sblocco



Attacchi Brute-Force e Dizionario

Tentativi sistematici di decifrare password attraverso combinazioni di lettere/numeri/caratteri speciali o liste di password comuni/date nascita.



Exploit "Zero-Day" e Vulnerabilità Note

Utilizzo di falle di sicurezza non ancora corrette o già documentate per aggirare i sistemi di protezione.



Strumenti Hardware Specializzati

Impiego di dispositivi come Acelaboratory PC3000 per dischi e Ufed Inseyets o Magnet Graykey per dispositivi mobili che offrono capacità avanzate di recupero.



Coinvolgimento dell'Utilizzatore

Collaborazione con il proprietario del dispositivo per ottenere password o chiavi di ripristino, spesso la soluzione più veloce ed efficace.

Le tecniche di decrittazione variano in base al contesto e alle risorse disponibili. Gli attacchi **brute-force** e a **dizionario** possono richiedere **tempi molto lunghi** (variano molto in base al modello e al Sistema Operativo), mentre gli exploit sfruttano vulnerabilità specifiche, ma potrebbero non essere sempre disponibili.

Gli strumenti hardware professionali **offrono soluzioni potenti ma costose**, mentre la collaborazione dell'utente utilizzatore, ove disponibile, rappresenta spesso la via più rapida per accedere ai dati protetti.

Sfide nella Mobile Forensics

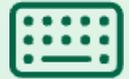


L'acquisizione di dati da smartphone presenta sfide uniche rispetto alla computer forensics tradizionale. La complessità deriva dalla **rapida evoluzione dei sistemi operativi mobile e dalle loro robuste misure di sicurezza**, progettate specificamente per proteggere i dati degli utenti.

degli utenti.

Ogni **tentativo di accesso può modificare lo stato del dispositivo**, rendendo essenziale la **descrizione di tutti i passaggi** ed eventualmente la presenza di testimoni qualificati che possano attestare la correttezza delle procedure seguite durante l'acquisizione forense.

Sfide nella Cloud Forensics



Accesso Dati e 2FA 2FA

Superamento delle barriere di **autenticazione a più fattori** e **gestione delle credenziali di accesso** ai servizi cloud.



Multi-tenancy

Isolamento delle prove relative a **specifici utenti** **utenti in ambienti condivisi** con altri tenant.



Catena di Custodia Custodia "Liquida" "Liquida"

Mantenimento dell'integrità delle prove in un ambiente virtuale e distribuito geograficamente.



Rischio di Cancellazione Remota

Prevenzione di tentativi di **eliminazione o modifica dei dati** tramite **comandi di remote wipe**.

La cloud forensics introduce **complessità uniche** legate alla **natura distribuita e virtuale dei dati**. L'accesso spesso richiede il **superamento di sistemi di autenticazione avanzati**, mentre la condivisione delle risorse tra più utenti complica **l'isolamento delle prove rilevanti**.

Particolare attenzione va posta al **rischio di cancellazione remota**, che potrebbe compromettere irrimediabilmente le prove digitali.

Strumenti e Costi in Digital Forensics

10-15K€

Costo Iniziale Suite Commerciali

Investimento base per Cellebrite, Magnet e altre soluzioni professionali

3-6K€

Costo Annuale Manutenzione

Aggiornamenti necessari per supportare nuovi dispositivi e sviluppare le capacità di analisi e recupero dati

100+

App e Servizi supportati con Plug-in

WhatsApp, Telegram, Signal e altre applicazioni popolari

Gli strumenti professionali per la digital forensics rappresentano un **investimento significativo, significativo**, giustificato dalla loro **capacità di estrarre dati da un'ampia gamma di dispositivi e dispositivi e applicazioni**. Le alternative open-source, sebbene economiche, presentano limitazioni sostanziali in termini di supporto e funzionalità.

I software commerciali offrono plug-in dedicati per le **applicazioni più diffuse**, mentre per **formati proprietari meno comuni è spesso necessario un lavoro di reverse engineering**, aumentando ulteriormente i costi e i tempi dell'analisi.



Il Valore e il Fascino dell'Informatica Forense

L'informatica forense non è solo una professione: è una missione con un **impatto diretto sulla giustizia e sulla sicurezza aziendale**. Ogni indagine rappresenta un puzzle tecnico unico che richiede pensiero analitico e competenze sempre aggiornate.



La professione premia chi combina **curiosità intellettuale, rigore metodologico e capacità di problem solving**. È un percorso che offre costanti **opportunità di specializzazione attraverso certificazioni riconosciute a livello internazionale**, con la soddisfazione incomparabile di contribuire a far emergere la **verità nei casi più complessi**.

Un Profilo Professionale Multidisciplinare

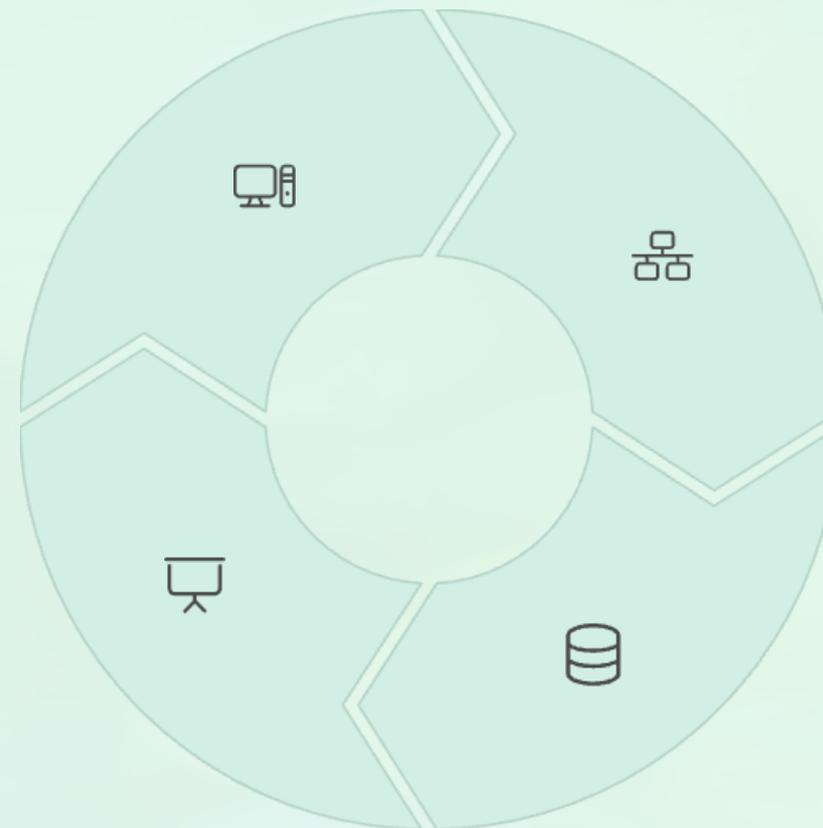
L'informatico forense deve **padroneggiare un vasto spettro di competenze tecniche trasversali**. La **versatilità** è essenziale per affrontare scenari investigativi sempre diversi, dai sistemi tradizionali alle nuove frontiere del cloud.

Sistemi e Dispositivi

Analisi di sistemi fissi, mobili e cloud con metodologie specifiche

Competenze avanzate

Conoscenze avanzate del mondo multimediale (immagini, video e audio) utili a certificare contenuti audio-visivi manipolati, oltre che per le comparazioni antropometriche



Reti, Telecomunicazioni e Trascrizioni

Intercettazione e analisi di traffico, protocolli e comunicazioni. Trascrizione intercettazioni telefoniche e ambientali

Recupero e Analisi Dati

Tecniche avanzate di data recovery e scripting per l'automazione delle fasi di analisi complesse

Oltre alle competenze puramente tecniche, un buon informatico forense deve sviluppare **eccellenti capacità di comunicazione** per spiegare **comunicazione** per spiegare concetti complessi a **pubblici non tecnici**, inclusi avvocati, giudici e dirigenti aziendali. La gestione efficace dei progetti investigativi richiede inoltre **disciplina metodologica e organizzativa**.

Stato dell'Arte e Tendenze Future

Automazione e Intelligenza Artificiale

Implementazione di sistemi automatizzati mediante IA per l'analisi, in special modo le operazioni più onerose e noiose, permettendo all'operatore di concentrarsi su concetti più complessi.

Live Forensics vs Snapshot

Evoluzione verso strumenti di live response che operano su sistemi in produzione, bilanciando la necessità di non interrompere i servizi con quella di raccogliere prove digitali affidabili.

Acquisizione e Analisi IoT

I dispositivi dell'Internet of Things (telecamere, frigoriferi, auto, smartwatch) generano dati e sono vulnerabili. La loro natura frammentata e i protocolli proprietari complicano la raccolta e l'analisi delle prove.

Deepfake

L'uso dell'IA per generare prove false (video, audio, immagini manipolate) complicherà la validazione delle evidenze digitali. Serviranno nuovi strumenti e competenze per distinguere reale da artefatto.

Il futuro dell'informatica forense sarà caratterizzato **dall'integrazione di tecnologie avanzate come l'intelligenza artificiale e il machine learning**, che permetteranno di **analizzare efficacemente volumi di dati sempre crescenti**.

Parallelamente, **l'informatica forense del futuro dovrà affrontare ambienti distribuiti e complessi** (cloud, container, IoT), **dati volatili e cifrati**, minacce sempre più avanzate, **prove manipolabili tramite IA e deepfake**, e crescenti difficoltà nell'acquisizione e analisi di dispositivi IoT e fonti eterogenee.

Perchè diventare Informatico Forense

Scegliere la professione dell'informatico forense significa entrare in un mondo affascinante, dove ogni dato può nascondere una prova nuova e stimolante, permettendo all'esperto di espandere i propri confini culturali.

È un ruolo che unisce **competenze tecniche**, **intuito investigativo** e **senso etico**, con l'obiettivo di proteggere persone, aziende e istituzioni da crimini digitali sempre più sofisticati e complessi.

In un'epoca in cui la sicurezza, la privacy e l'integrità delle informazioni sono fondamentali, **l'informatico forense è una figura chiave per la giustizia**: questa professione rappresenta una sfida continua, ma anche una missione appassionante e profondamente utile alla società.

Grazie per la partecipazione!

Prof. Ing. Michele Vitiello
Studio Ingegneria Informatica Forense
Via Cefalonia n.70, 25124 Brescia
info@michelevitiello.it www.michelevitiello.it

<https://shorturl.at/OPaF8>

Il tuo smartphone sa dove sei stato, con chi hai parlato, cosa hai scritto, cercato e fotografato. In un'indagine digitale, può essere testimone, prova e... colpevole.

In questo libro, il consulente informatico forense Michele Vitiello apre le porte del laboratorio investigativo dove dati, file, metadati e dispositivi mobili rivelano indizi che nessuno vorrebbe confessare alle Forze dell'Ordine.

Dai messaggi cancellati ai backup nascosti, dalle immagini alterate agli audio manipolati, ogni capitolo esplora il mondo affascinante — e inquietante — della Digital Forensics e delle discipline connesse. Proponendo strumenti, tecniche investigative e metodo scientifico per risolvere i casi giudiziari reali.



Michele Vitiello è un esperto nel campo dell'Ingegneria Informatica Forense, con una carriera come Prof. a.c. per l'Università Telematica Internazionale UNINETTUNO alla Facoltà di Giurisprudenza ed Economia e docente della Scuola Superiore per la Magistratura, Consulente Tecnico del PM per 62 Procure della Repubblica e Perito - CTU per 36 Tribunali, partecipando anche ad operazioni coordinate da Eurojust ed Europol, entrambi organismi chiave nell'ambito della cooperazione giudiziaria penale Europea.

Continua a contribuire nel settore, unendo competenza accademica e pratica per promuovere l'eccellenza nelle investigazioni informatiche e forensi, offrendo un supporto decisivo su oltre 3.000 casi trattati.

Noto al grande pubblico come opinionista nei programmi televisivi e radiofonici di cronaca nera sulle principali emittenti nazionali.



STUDIO INGEGNERIA INFORMATICA FORENSE

Prof. Michele Vitiello



MICHELE VITIELLO L'IMPUTATO È IL TUO SMARTPHONE

MICHELE VITIELLO

L'IMPUTATO
È IL TUO
SMARTPHONE

Crimini, Investigazioni e Tecnologie
al servizio della Giustizia