DIGITAL FORENSICS

Acquisizione Forense di Evidenze da Memoria

INDAGINI ONLINE

AGENDA

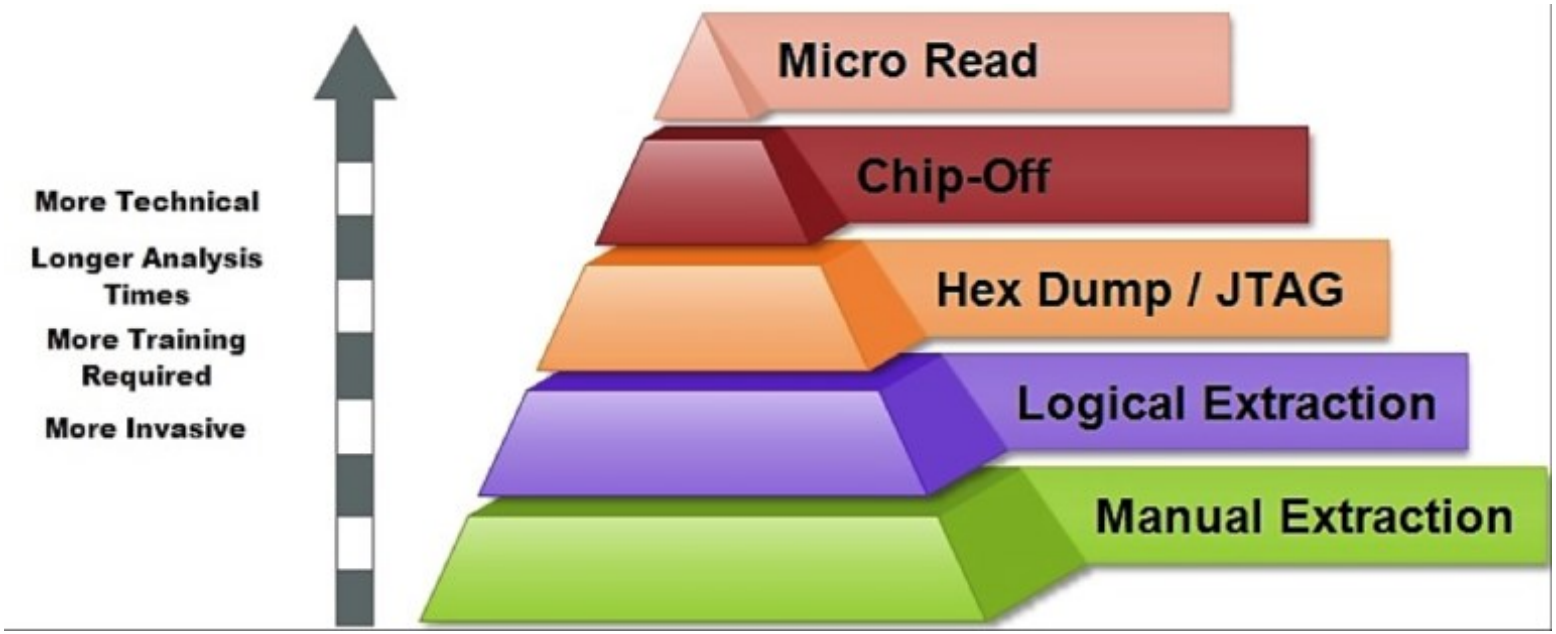
- Acquisizione e analisi forense
  - Identificazione
  - Raccolta
  - Acquisizione
  - Analisi
- Presentazione dei risultati – Reporting
  - Esempio di Report + Esercitazione
- Conclusioni – Quesiti

Acquisizione e analisi forense

INDAGINI ONLINE

Acquisizione: classificazione

Per acquisizione forense del supporto di memorizzazione si intende l'estrazione del contenuto memorizzato sotto forma di sequenza di bit memorizzati al suo interno.



La copia forense ideale è una copia bit a bit perché include: tutti i file, anche quelli cancellati, lo slack space e lo spazio libero.

Tipi di copia forense

Un dispositivo di memoria può essere copia in due modalità:

- Device to device
- Device to file

Nel secondo caso, quello più utilizzato, si può scegliere:

- Il formato: RAW (dd), EWF o AFF (compressi)
- Lo split su più file
- Livello di compressione
- La cifratura
- I metadati
- Calcolo degli hash
- È possibile memorizzare più copie sullo stesso device

Esempio

Acquisizione pendrive usb

INDAGINI ONLINE

Esercizio

Acquisizione memoria e calcolo impronta hash

INDAGINI ONLINE

Acquisizione: write blocker

Per dare garanzia del rispetto dei principi enunciati, tutte le operazioni eseguite in fase di acquisizione devono essere accuratamente documentate, meglio se si utilizzando dei dispositivi che registrano automaticamente quanto viene eseguito.

Se possibile è conveniente utilizzare dispositivi che impediscono l'alterazione del supporto di origine: c.d. write-blocker

Acquisizione live

Nel caso in cui ci dovesse capitare di trovare le apparecchiature in funzione oppure non è possibile spegnerle (macchine critiche), occorre effettuare l'acquisizione della ram e delle altre informazioni presenti all'interno della macchina.

In questo caso sono utilizzate le distribuzioni che consento di eseguire programmi presenti su altri dispositivi (DVD o Pendrive) senza intaccare la memoria di massa.

Lo stesso tipo di acquisizione può essere sfruttata su quelle macchine dove è complicato raggiungere la memoria, in questo caso il sistema può essere avviato direttamente dalla distribuzione in modalità Live.

Attività di preview o triage

Potrebbe essere necessario effettuare una preview del contenuto del sistema (per esempio durante un'ispezione) oppure acquisire solo alcune informazioni (perquisizione)

Oppure semplicemente occorre valutare se quel dispositivo è pertinente con l'obiettivo dell'attività oppure no.

Anche in questo caso si possono utilizzare le distribuzioni live.

È importante che qualsiasi attività posta in essere, anche se non comporta alcuna modifica dei dati, sia documentata in un apposito verbale di ispezione o perquisizione.

Acquisizione logica

In determinate condizioni, potrebbe essere necessario effettuare la copia logica, ovvero una copia parziale del contenuto del dispositivo.

Questa ipotesi si verifica principalmente nei dispositivi:

- Cifrati
- Server
- Mobile
- Condivisi o multifunzione

In pratica in quei dispositivi dove è necessario operare con il sistema operativo acceso oppure dove le informazioni di interesse sono circoscritte a determinati file.

Esempio

Triage e acquisizione logica

INDAGINI ONLINE

Acquisizione della RAM

La RAM (Random Access Memory) è una memoria di tipo volatile, che permette l'accesso diretto a qualunque indirizzo di memoria con lo stesso tempo di accesso.

Dopo lo spegnimento del dispositivo i dati vengono persi.

L'acquisizione della RAM si effettua a sistema acceso.

È utile acquisire la RAM quando:

- Si vuole recuperare le password o le informazioni presenti in memoria
- Per tenere traccia dei processi attivi ed analizzarli successivamente
- Per recuperare informazioni dai software che non lasciano tracce
- Nel caso di analisi di malware, rootkit o trojan

Acquisizione della RAM

- Eseguire il tool di acquisizione da dispositivo esterno (pendrive, DVD)
- Salvare il contenuto su dispositivo esterno per non intaccare i dischi locali
- Se la macchina da clonare è virtuale basta usare il comando «snapshot»

Software per acquisire e analizzare la RAM

- Volatility
- AccessData FTK Imager
- Windows Memory Reader
- Magnet RAM Capture

Verifica e apertura di un immagine forense

- È possibile verificare l'integrità di una copia forense ricalcolando l'hash sulla stessa immagine e confrontandolo con quello calcolato al momento della realizzazione della copia
- In base alla modalità con cui è stata eseguita la copia forense, (raw, split, ewf, aff, clone) ci sono diverse alternative per l'accesso in fase di analisi
- Il fine è quello di poter accedere al contenuto (filesystem, aree allocate e non) dell'immagine acquisita per poter eseguire le verifiche richieste
- Alcuni formati prevedono solo l'acceso in sola lettura

Esempio

Acquisizione RAM

Apertura di un'immagine forense, montaggio e analisi del file system

INDAGINI ONLINE

Analisi

L'analisi deve consentire:

- la ricostruzione degli eventi passati attraverso la lettura dei dati rinvenuti.
- L'estrazione dei dati e l'elaborazione per ricostruire le informazioni
- L'interpretazione delle informazioni per individuare gli elementi utili all'indagine
- La comprensione e correlazione dei dati, in modo da affinare le ricerche e poterne trarre le conclusioni

È sicuramente la fase più laboriosa di tutto il processo e richiede conoscenze multidisciplinari.

Analisi: strategie operative

- Ricerche
  - Autore
  - Intervallo di date
  - Tipo di file
  - Parola chiave
  - Per hash
  - Per thread (email)
- Recupero dati
  - Recupero dati cancellati, carving…
- Interpretazione dati
- Conversione tra formati
- Crack password
  - File tipicamente protetti
  - Tipologie di attacco
- Artefatti del sistema operativo

Recupero dei dati cancellati

Quando si cancella un file, i dati non sono immediatamente azzerati, ma soltanto derefenziati, ovvero viene cancellata la voce sul registro del file system che consente di richiamarlo.

I dati, di conseguenza, sono ancora sul supporto di memoria, ma lo spazio precedentemente occupato risulta deallocato (libero)

Anche i metadati potrebbero essere ancora presenti in maniera analoga sul File system (MFT)

Per il recupero dei file cancellati possono essere percorse due soluzioni alternative:

- Analisi dei metadati del file system
- File carving

Recupero dei dati cancellati

Recupero tramite analisi dei Metadati:

- Strettamente dipendente del File system
- Consente di ricostruire anche i file frammentati
- È possibile recuperare altre informazioni tra cui:
  - il nome del file
  - la data di creazione
  - la data di modifica
  - la data di ultimo accesso
  - il proprietario (dipende dal File system)
  - Permessi scrittura e lettura

Recupero dei dati cancellati

Recupero tramite File Carving:

- Se il dato è completamente dereferenziato, l'unico recupero possibile è tramite la scansione del Binary Large Object
- Vengono ricercate le intestazioni (header o magic number) identificative di specifici formati di file
- Si cerca di interpretare quello che segue come parte integrante del file (se esiste viene cercato anche il footer)
- Funziona bene nel caso in cui i file siano allocati su cluster contigui, ma non in caso di frammentazione
- Non recupera le informazioni come il nome originario del file e gli altri metadati del file system

Recupero dei dati cancellati

Il data carving è un processo di estrazione di un set di dati da un insieme di dati molto più ampio.

La tecnica del data carving è utilizzata solitamente durante le indagini di analisi forense per analizzare lo spazio non allocato.

Durante questo procedimento la struttura del file system viene ignorata.

I file sono individuati e catalogati in base all'header e al footer trovato

Distinguiamo

- Data carving base
  - L'header e footer dei file non sono sovrascritti
  - Il file non è frammentato
  - Il file non è compresso
  - Il file estratto è l'insieme di bit contenuti tra header e footer
- Data carving avanzato
  - I frammenti non sono sequenziali
  - I frammenti non sono ordinati
  - Mancano dei frammenti

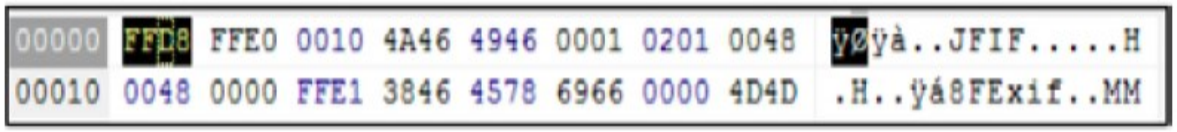


Figure 2. JPEG header.

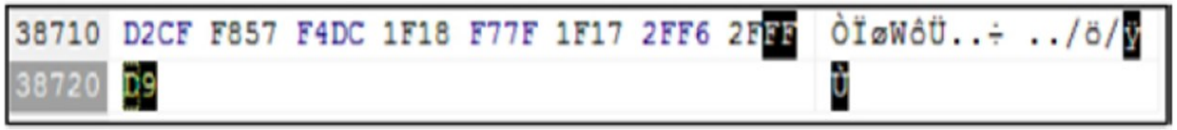


Figure 3. JPEG footer.

IN

Esempio

Analisi del file system per recupero dei file cancellati e data carving

INDAGINI ONLINE

Analisi dei metadati

I metadati sono dati riguardanti altri dati.

Spesso i metadati hanno un ruolo fondamentale nelle indagini digitali.

Possono fornire informazioni importanti riguardanti il documento stesso, l'autore e la data e ora di creazione e modifica.

Possono rilevare informazioni che si è tentato di oscurare, nascondere o cancellare

Possono essere utilizzati per correlare i documenti allo loro fonte

Esempi di metadati:

- File system
- Documenti (office, pdf, ecc.)
- Immagini (dati exif)
- Audio / Video
- Email
- Applicazioni

Esempio

Estrazione metadati

INDAGINI ONLINE

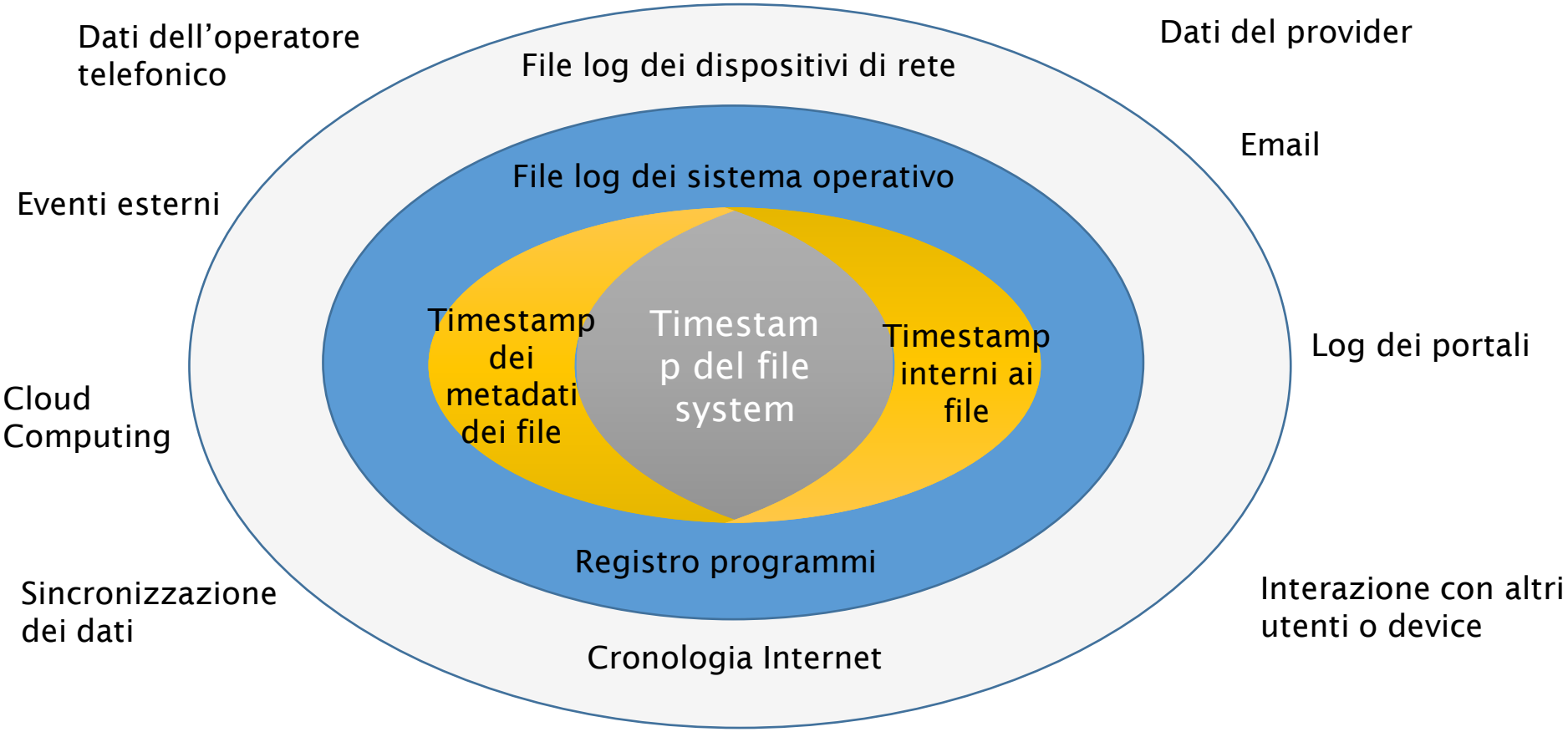
Analisi: Timeline

Spesso è necessario ricostruire la cronologia delle attività che hanno determinato lo stato del dispositivo con l'obiettivo di individuare gli elementi di prova che concorreranno a dimostrare o confutare dei fatti.

Occorre creare una linea temporale relativa agli eventi verificatesi e richiede l'integrazione delle varie informazioni temporali (timestamp) create dal sistema operativo, dal file system e dalle applicazioni utente.

- Metadata dei file (timestamp della creazione, ultimo accesso ed ultima modifica dei file)
- Esecuzione dei programmi (S.O. registra informazioni sull'esecuzione dei programmi)
  - File prefetch su Windows
  - Registro di Windows
  - File log di sistema ….
- Artefatti generati dai programmi ad ogni esecuzione
  - Elenco file aperti o salvati
  - File di cronologia di navigazione
  - File di log ….

Analisi: Supertimeline



INDAGINI ONLINE

Esempio

Ricostruzione timeline

INDAGINI ONLINE

Virtualizzazione delle immagini forensi

- Potrebbe essere necessario effettuare accertamenti direttamente sulla macchina accesa (p.e. per verificare il funzionamento di un programma o interrogare un database)
- La soluzione che consente di effettuare questo tipo di analisi, consiste nel creare una macchina virtuale a partire dalla copia forense, che deve essere obbligatoriamente bit a bit, e successivamente si esegue
- La macchina virtuale deve avere le schede di rete **disabilitate**
- Possono essere eseguiti programmi, in formato portable, per estrarre informazioni utili alle indagini
- Il vantaggio della macchina virtuale è legato soprattutto alla ripetibilità delle operazioni eseguite

Esempio

Esempio macchina virtuale

INDAGINI ONLINE

Valutazione

La valutazione è una fase necessaria per stabilire:

- Se il reperto informatico è stato
  - alterato
  - inquinato
  - contraffatto
- Se le procedure di acquisizione sono state legittime
- Se il reperto è
  - attendibile
  - integro
  - Autentico
- Il significato dei dati presenti sul supporto

Esempi di ricerche

- Ricerca per parole chiave
- Utilizzo delle periferiche usb
- Analisi dei documenti aperti e utilizzati
- Ricostruzione della navigazione in internet
- Manomissione delle prove
- Cronologia dei programmi
- Conferma di un alibi

Problematiche

- Dischi cifrati
- Memorie SSD
- Sistemi di sicurezza logica
- Sistemi embedded

Presentazione dei risultati

Come creare un Report

Firma digitale e Marca temporale

INDAGINI ONLINE

Presentazione

Dopo aver completato le fasi tecniche, occorre predisporre una sintesi dell'intero processo tramite l'esposizione, entro i limiti concordati, delle informazioni fattuali ricavate dalle prove e dall'insieme di esami ed analisi che hanno costituito l'indagine. Questo obiettivo si concretizza attraverso la redazione di un elaborato o report da cui sia possibile ricavare:

- l'origine delle fonti di prova digitale,
- la metodologia utilizzata per la gestione delle fonti di prova,
- la tecnologia adoperata per il trattamento delle fonti di prova,
- la procedura eseguita per giungere ai risultati conseguiti,
- i risultati ottenuti (anche sottoforma di allegati multimediali),
- la risposta al quesito.

Presentazione

Un metodo suggerito per la stesura della relazione finale consiste nello sviluppare e strutturare la presentazione seguendo lo stesso ordine delle fasi ISO descritte nei paragrafi precedenti.

La presentazione dei risultati è l'elemento con cui si valuta tutta l'attività svolta. Per cui, durante la stesura, è fortemente consigliato tener conto delle seguenti indicazioni:

- occorre essere semplici e chiari,
- i risultati devono essere esposti in una forma facilmente comprensibile a tutti,
- i destinatari non hanno di solito competenze informatiche,
- molto probabilmente la relazione sarà esaminata da un tecnico della controparte,
- non bisogna essere approssimativi o esprimere giudizi che non siano corroborati dai dati.

Report

Tipologia: La Perizia e la Consulenza tecnica

La perizia e la consulenza tecnica sono i due mezzi di prova attraverso i quali fa ingresso nel processo penale il sapere tecnico, scientifico e artistico.

Entrambe si sostanziano, alternativamente o cumulativamente, nello svolgimento di indagini, nell'acquisizione di dati o nell'effettuazione di valutazioni che richiedono per la loro natura particolari competenze tecniche, scientifiche o artistiche.

La perizia (artt. 220 e ss.c.p.p.) costituisce mezzo di prova "neutro" (essendone affidato l'espletamento ad un soggetto terzo, quindi imparziale, nominato dal giudice) ed essenzialmente discrezionale (essendo rimessa al giudice la valutazione sul requisito della sua "occorrenza"). Oltre che a richiesta di parte, può essere disposta anche d'ufficio.

La consulenza tecnica, invece, può esperirsi: nell'ambito di una perizia già disposta, concedendo alle parti facoltà di nominare propri consulenti che possono partecipare alle operazioni peritali al fine di realizzare il contraddittorio nella formazione della prova (art. 225 c.p.p.).

Report

Parti essenziali:

- **Premessa**
  - *Curriculum del consulente*
  - **Oggetto dell'Incarico**
  - **Quesiti formulati**
  - *Breve descrizioni dei Fatti*
- **Fasi dell'Attività**
  - *Documenti e/o Evidenze forniti ed analizzati*
  - *Metodologia applicata*
  - **Strumenti (hardware e software) utilizzati**
  - **Descrizione dettagliata delle operazioni eseguite (anche foto e video)**
- **Risultati**
  - **Risposte ai quesiti**
  - **Conclusioni**
  - *Elenco Allegati*

Esempio

Report di acquisizione

INDAGINI ONLINE

Firma digitale

La firma che consente di scambiare in rete documenti con piena validità legale.

CAD Art. 24. Firma digitale

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.
3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

Marca temporale

La Marca Temporale è un servizio che permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi. (cfr. Art. 20, comma 3 CAD)

Il servizio di Marcatura Temporale può essere utilizzato anche su file non firmati digitalmente, garantendone una collocazione temporale certa e legalmente valida.

Sui documenti informatici sui quali è stata apposta una Firma Digitale, **la Marca Temporale attesta il preciso momento in cui il documento è stato creato, trasmesso o archiviato**.

Contatti

info@vincenzocalabro.it

Linkedin vincenzocalabro

INDAGINI ONLINE