DIGITAL FORENSICS

Peculiarità e Criticità riscontrate durante il Trattamento degli Elementi di Prova Digitali

INDAGINI ONLINE

About me

Ho studiato Ingegneria Informatica (La Sapienza) e Sicurezza Informatica (UniMi).

Mi sono «perfezionato» in Data Protection e Data Governance (UniMi), in Criminalità Informatica e Investigazioni Digitali (UniMi) e Big Data e Artificial Intelligence (UniMi).

Ho conseguito l'Advanced Cybersecurity Graduate Certificate alla Stanford University, il CERT Certification in Digital Forensics alla Carnegie Mellon University, l'European Certificate on Cybercrime and E-Evidence (ECCE) rilasciato dall'European Commission's Directorate General Justice, Freedom and Security.

Dal 1992 Referente Informatico e Funzionario alla Sicurezza c/o Ministero dell'Interno.

Dal 2004 Information Security Engineering: mi occupo della risoluzione delle problematiche connesse alla sicurezza delle informazioni ed alla tutela dei dati personali

Dal 2005 Consulente di Informatica Forense: esercito l'attività di consulenza tecnica in procedimenti giudiziari che hanno ad oggetto i reati informatici o che vengono attuati tramite l'information & communication technology

Dal 2017 Professore a contratto di Tecnologie per la Sicurezza Informatica c/o Università

Dal 2018 Trainer sulle tematiche della Cyber Security e Digital Forensics (Indagini Online)

Autore di alcuni articoli e saggi

INDAGINI ONLINE

Definizione: Digital Evidence

Definizione

La fonte di prova digitale o digital evidence è ***«qualsiasi informazione, con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale»***

Distinguiamo:

- La prova creata dall'uomo
- La prova creata autonomamente dal computer
- La prova creata sia dall'essere umano che dal computer

Caratteristiche

Le peculiarità che contraddistinguono la fonte di prova digitale, che non possono essere ignorate, consistono in:

- **Immaterialità**: la prova digitale è il contenuto e non il supporto su cui è memorizzata;
- **Dispersione**: la prova digitale può essere dislocata su più dispositivi molto distanti tra loro,
- **Promiscuità**: la prova digitale può trovarsi all'interno di dispositivi che contengono altre informazioni non attinenti all'indagine,
- **Congenita modificabilità**: la prova digitale è estremamente alterabile.

Digital Evidence: perché?

La maggior parte delle azioni umane sono svolte interagendo, direttamente o indirettamente, con gli strumenti dell'ICT.

Anche i reati hanno questa peculiarità? **SI**

Distinguiamo **i reati**:

- tipicamente informatici
- aventi ad oggetto gli strumenti dell'ICT
- perpetrati attraverso l'uso di strumenti dell'ICT
- che lasciano tracce sugli strumenti dell'ICT

e gli altri **illeciti**? **SI**

- procedimenti civili
- procedimenti aventi ad oggetto il diritto del lavoro
- procedimenti amministrativi
- procedimenti in materia tributaria

Digital Forensics: perché?

Il tema della prova è centrale all'interno del processo, costituendo il campo più critico entro il quale si dispiega l'attività degli operatori del diritto e che oggi non può prescindere dall'informatica, dalla **volatilità** e **fragilità** del **dato informatico**, dall'importanza della corretta acquisizione e gestione dei bit, dalla fonte di prova digitale.

La giurisprudenza, pertanto, incoraggia l'utilizzo delle tecniche di informatica forense, affinché siano estratti contenuti in copia dei dati presenti, cristallizzati in **copie forensi** consentendo la produzione di **elementi giudiziali certi**, in relazione ad **integrità** dei dati, **non manipolazione, riconducibilità all'autore** e **certezza temporale**, rendendo la copia forense prodotta **immodificabile** e tendenzialmente vincolante per il giudicante.

Scopo: Digital Forensics

Lo scopo dell'informatica forense si esplicita nelle seguenti prerogative: **identificare, conservare, acquisire, documentare e interpretare** i dati presenti su una memoria digitale.

L'ordinamento Italiano, dopo l'approvazione della Legge 48 del 2008 di ratifica della Convenzione sul Cybercrime di Budapest, **ha stabilito che**, nel processo penale, **tutte le attività probatorie che hanno ad oggetto le prove digitali devono essere disposte attraverso tecniche idonee ad assicurare la conservazione dei dati originali ed impedirne l'alterazione**.

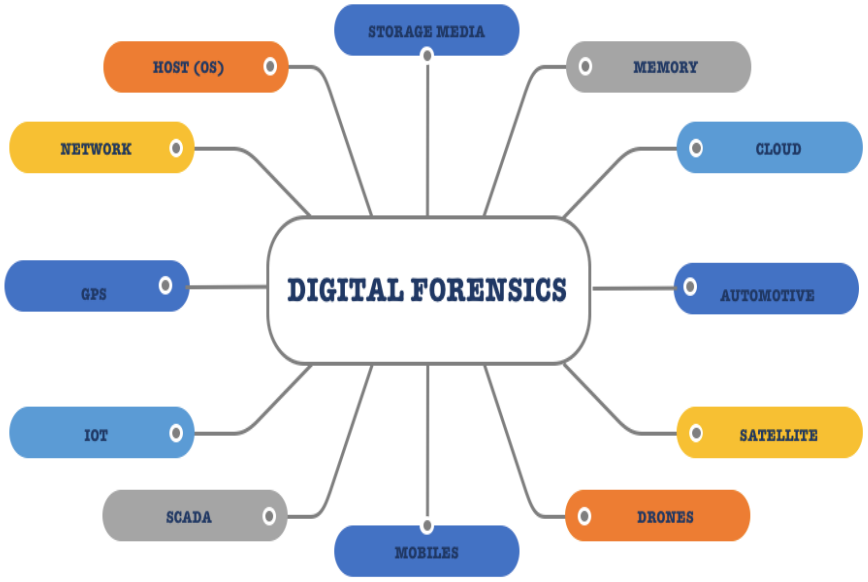
Pertanto, è necessario che anche **le metodologie utilizzate per il trattamento delle evidenze digitali abbiano la capacità di resistenza ad eventuali contestazioni e capacità di convincimento del giudice e delle parti processuali in ordine alla loro verificabilità, ripetibilità, riproducibilità e giustificabilità.**

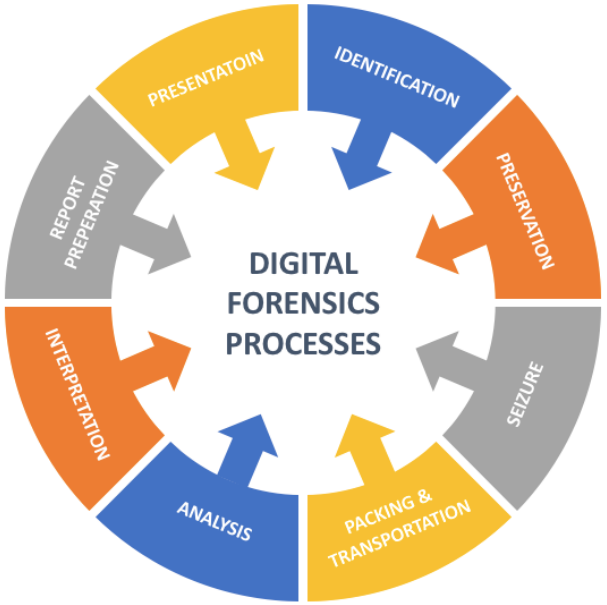
Per tale motivo è fortemente consigliato impiegare tecniche e standard ispirati al **metodo scientifico.**

Digital Forensics

Lo standard ISO/IEC 27037:2012 "**Guidelines for identification, collection, acquisition, and preservation of digital evidence**" fornisce delle linee guida relative alla gestione delle potenziali prove digitali, concentrandosi in particolar modo sulle fasi di identificazione, raccolta, acquisizione e preservazione.

Lo standard ISO/IEC 27042:2015 «**Guidelines for the analysis and interpretation of digital evidence**" fornisce una guida sull'analisi e l'interpretazione delle prove digitali in grado di affrontare le questioni di continuità, validità, riproducibilità e ripetibilità.





Identificazione

Tra le principali tipologie di media in grado di contenere dati, e quindi oggetto di interesse, possiamo annoverare:

- **Elaboratori** (disco interno, raid, supporti ssd, ecc.)
- **Storage esterni** (hd esterni, pen drive, schede di memoria)
- **Dispositivi ottici** (CD, DVD, BLU-RAY)
- **Supporti Legacy** (Floppy Disk, Nastri backup)
- **Dispositivi con memoria embedded** (macchine fotografiche, console, cellulari, sistemi di videosorveglianza, lettori multimediali, smart phone, smart watch, smart tv, ecc.)
- **Dispositivi per la trasmissione dei dati, dell'OT e dell'IOT, sensori o schede di controllo** (con o senza memoria)
- **Spazi di memoria condivisa o virtuali** (server remoti o cloud)

Acquisizione

Come prescrive la norma:

- Le copie eseguite devono essere **identiche** o il più possibile simili all'**originale** (in tal caso occorre giustificare la scelta)
- Durante la copia dell'origine, quest'ultima **non deve essere modificata** (integrità)
- Nel caso in cui non ci sia un metodo che consenta di evitare di alterare l'originale, la scelta va **giustificata** e **documentata**
- Le **procedure** devono essere attuate e **documentate** secondo metodologie e tecnologie riconosciute, in modo da poter essere **verificabili** dagli altri attori (verificabilità)
- Potrebbe essere necessario eseguire copie parziali della memoria del dispositivo, anche in questo caso la scelta deve essere **motivata** e **documentata**

Accertamento tecnico ripetibile o non ripetibile

«L'accertamento tecnico non è ripetibile quando riguarda persone, cose o luoghi il cui stato è soggetto a modificazione.»

In quali casi **l'accertamento tecnico digitale può modificare lo stato** delle evidenze digitali?

- Quando è possibile accedere al contenuto digitale solo previa accensione del dispositivo che lo contiene (memoria non rimovibile, utilizzo della crittografia, assenza di connettività)
- Se il dispositivo è in funzione e i dati non sono memorizzati su memoria permanente (memoria volatile, dati di sessione)
- Qualora non fosse possibile spegnere/scollegare/interrompere il funzionamento dell'apparato che contiene i dati digitali

Mobile Technology

New Challenges:

- Frammentazione del mercato
- Generazione di nuovi dispositivi
- Aggiornamenti continui dei sistemi operativi
- Passcode e cifratura
- Personalizzazioni utente
- Milioni di applicazioni
- Giga di dati
- Cloud
- …

Dati che possono essere memorizzati:

- Chiamate entrata, uscita, perse
- Contatti
- Calendario
- Messaggi di testo
- Email
- Messaggi istantanei o chat
- Web pages
- Audio / Foto / Video
- Transazioni / Logs di varie Apps

Sistemi di protezione

Sempre più frequentemente l'accesso alle informazioni, in particolar modo sui dispositivi portatili, è filtrato da sistemi di protezione (pin/password/autenticazione) per impedire l'accesso alle persone non autorizzate.

Non sempre è possibile bypassare tali meccanismi, in ogni caso:

- la rimozione degli stessi **modifica** lo stato del dispositivo,
- la loro forzatura può **compromettere** irrimediabilmente la **genuinità** del dato contenuto e/o il **funzionamento** del dispositivo che li contiene.

Crittografia

Molti dispositivi end-user (smartphone, laptop, ecc.) e/o le applicazioni (messaggistica, database, ecc.) utilizzano la crittografia per proteggere le informazioni da accessi abusivi.

Per copiare e analizzare i dispositivi cifrati spesso è necessario accenderli, ciò determina la **modifica** dello stato iniziale.

Inoltre, la crittografia non consente il recupero delle informazioni cancellate, perché la cancellazione riguarda anche la chiave con cui l'informazione è stata cifrata.

Captatore informatico

Il captatore informatico è un malware che costituisce, per le forze di polizia e per la magistratura (???), uno strumento in grado di bypassare i sistemi di cifratura dei sistemi e delle app.

Sono sistemi in grado di acquisire e/o intercettare le informazioni direttamente sul dispositivo acceso e in maniera silente.

Esso viene inoculato negli smartphone e nei personal computer e, in base alle norme in vigore, può attivare il microfono per ascoltare le conversazioni, geolocalizzare lo smartphone, attivare la telecamera e scattare le foto, leggere il contenuto della memoria all'insaputa dell'indagato (???).

L'installazione avviene attraverso l'uso di tecniche di hacking, per esempio:

- Invio per email o messaggio
- Installazione tramite download o aggiornamenti
- Tecniche di social engineering

Captatore informatico

Dopo l'installazione del captatore l'apparato ospite è:

- **Alterato**, perché subisce un aggiornamento e non può essere ripristinato allo stato iniziale
- **Vulnerabile**, perché il captatore abbassa i sistemi di sicurezza del dispositivo e blocca gli aggiornamenti di sicurezza
- **Compromesso**, non è facile rimuovere il captatore e può essere riutilizzato

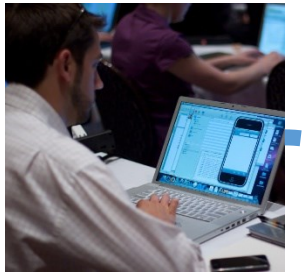
Il captatore viene inoculato all'interno del Target attraverso un exploit eseguito sul Target (bug di sistema, inoltro, upload, social engineering).

Il captatore è gestito da un Comand & Control da cui riceve i comandi.

Le informazioni sono catturate e inoltrate al server della Procura (???)

Per garantire la verifica e la riproducibilità è necessario un LOG che certifichi tutto il ciclo di vita, i comandi e le informazioni acquisite.

Captatore informatico



1. Installazione

2. Gestione

3. Memorizzazione

4. Consultazione

INDAGINI ONLINE

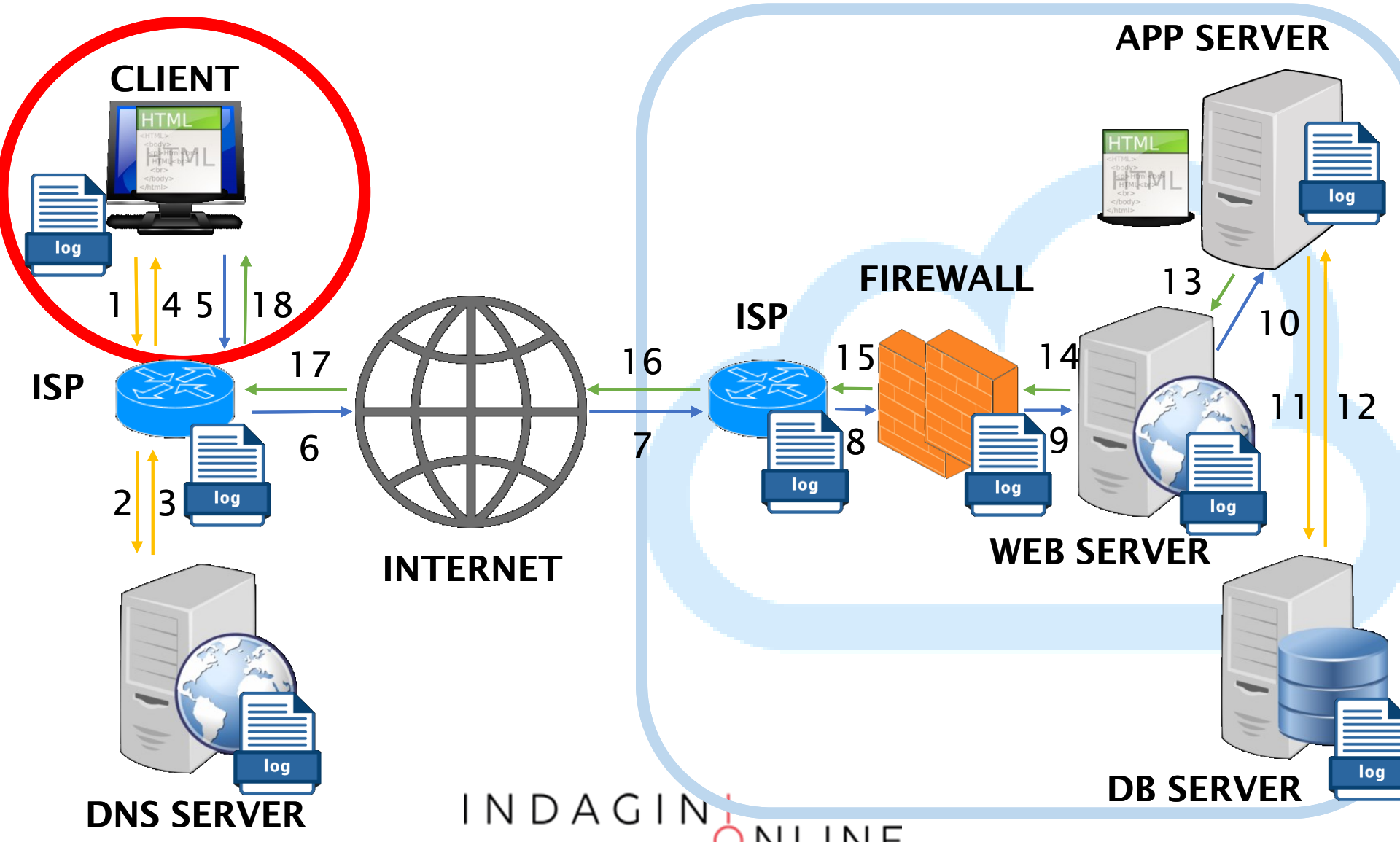
Acquisizione telematiche

Poiché molte attività si svolgono online, attraverso l'uso di servizi internet (web, email, e-commerce, social network, e-banking, messaggistica, audio e video chiamate, ecc.) occorre acquisire le informazioni attraverso la rete.

Ciò si rende necessario perché:

- Il dispositivo che contiene le informazioni è distante o non facilmente raggiungibile
- L'accesso alle memorie fisiche non è percorribile (rogatorie)
- Non è facile **individuare il luogo di memorizzazione** (cloud)
- È necessario acquisirle velocemente per criticità legate alla **volatilità o alterabilità** del dato (social media, email, ecc.)
- È un'ottima **alternativa per acquisire informazioni non reperibile sui dispositivi fisici** (backup smartphone, piattaforme di messaggistica, piattaforme di social network, email, spazi virtuali «iCloud» «Google Drive» «DropBox»

Web architecture



INDAGINE 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: caratteristiche

Poiché ogni copia coincide con l'originale, **l'analisi va eseguita sulla copia dei dati acquisiti e non sull'originale**

Caratteristiche dell'analisi

- Riproducibilità: ogni singola operazione deve produrre sempre lo stesso risultato (si intende risultato oggettivo, cioè i dati e non la loro valutazione)
- Metodologie: si può applicare la Regola delle «***5W***»
  - *WHO*? («Chi?»)
  - *WHAT*? («Che cosa?»)
  - *WHEN*? («Quando?»)
  - *WHERE*? («Dove?»)
  - *WHY*? («Perché?»)

Analisi: correlazione dei dati

- Che cosa è successo e come si è svolto?
  - Individuare i dati utili a ricostruire I fatti
  - Comunicazioni
  - Documenti
  - Log
  - Metadati (date, luoghi, coordinate…)
- Chi è coinvolto?
  - Comunicazioni
  - Metadati (date, utenti)
- Quando è accaduto?
  - Comunicazioni
  - Metadati (date, utenti)
- Da dove a dove?
  - Comunicazioni
  - Documenti
  - Log
  - Metadati (date, luoghi, coordinate…)
  - Tabulati telefonici
- Quante volte si è verificato?
  - Comunicazioni
  - Documenti
  - Log
  - Metadati (date…)
- C'era consapevolezza?
  - Comunicazioni
  - Cancellazione dati
  - Documenti
  - Log
  - Metadati (date…)
  - Navigazione web
  - Competenze utente

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
- Verifica dell'autore

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

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.

Report

Una consulenza tecnica forense dovrebbe esser strutturata:

- **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 (all. foto e video)**
- **Risultati**
  - **Risposte ai quesiti**
  - **Conclusioni**
  - *Elenco Allegati*

In sintesi

Il Consulente Tecnico, durante il suo operato, deve assicurare che siano rispettate SEI tipi di garanzie fondamentali:

1. **il dovere di conservare inalterato il dato informatico originale nella sua genuinità**
2. **il dovere di impedire l'alterazione successiva del dato originale**
3. **il dovere di formare una copia che assicuri la conformità del dato informatico acquisito rispetto a quello originale**
4. **il dovere di assicurare l'immodificabilità della copia del documento informatico**
5. **la garanzia delle installazioni di sigilli informatici sui documenti acquisiti**
6. **La riproducibilità e verificabilità del proprio operato**

Contatti

33 875 19 875
vincenzocalabro.it
Linkedin **vincenzocalabro**

INDAGINI ONLINE