DIIES Dipartimento di
INGEGNERIA
dell'INFORMAZIONE, delle INFRASTRUTTURE e dell'ENERGIA SOSTENIBILE

Corso di Tecnologie per la sicurezza informatica

Internet Forensics

Metodologie e Simulazioni di Indagine

Vincenzo Calabrò

Agenda

- Introduzione
  - Definizioni: Digital Evidence, Investigation, Forensics
  - Normativa di riferimento
  - Standard Internazionali
  - Esempi di acquisizione onsite + Esercitazione
- Acquisizione a distanza
  - Architettura dei Servizi Internet
  - Ispezione – Perquisizione – Acquisizione
  - Esempi di acquisizione a distanza + Esercitazione
- Presentazione dei risultati – Reporting
  - Esempio di Report + Esercitazione
- Conclusioni – Quesiti

Introduzione

Definizioni: Digital Evidence, Investigation, Forensics

Normativa di riferimento - Standard Internazionali

Definizione: Digital Evidence

SWGDE: *«qualsiasi informazione, con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale»*

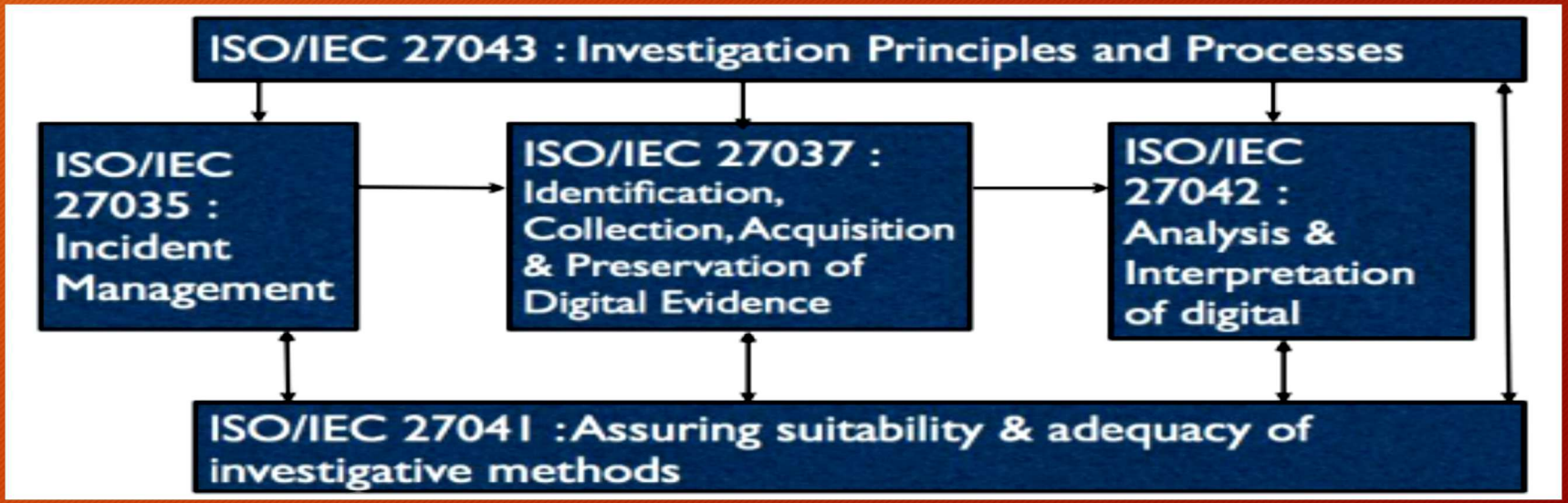
Eoghan Casey: *«qualsiasi dato digitale che possa stabilire se un crimine è stato commesso o che può fornire un collegamento tra il crimine e chi l'ha commesso»*

Distinguiamo:

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

Definizione: Digital Investigation

Eoghan Casey: *«un processo investigativo mediante il quale si utilizzano **tecniche informatiche per raccogliere indizi o fonti di prova** di varia natura, oppure quando l'informatica assume un ruolo di mero strumento facilitatore dell'investigatore stesso»*



Definizione: Digital Forensics

Luparia Ziccardi

«un processo teso alla manipolazione controllata e più in generale al trattamento di dati e/o informazioni digitali e/o sistemi informativi per finalità investigative e di giustizia, adottando procedure tecnico-organizzative tese a fornire ***adeguate garanzie in termini di integrità, autenticità e disponibilità*** *delle informazioni e dei dati in parola.»*

Tale disciplina, secondo alcuni una scienza chiamata anche informatica forense, non può limitare il proprio raggio d'azione alle sole indagini relative ai c.d. reati informatici , in quanto molti illeciti, così come le azioni della vita quotidiana, non hanno ad oggetto le tecnologie dell'informazione e della comunicazione, ma vi entrano in contatto e di conseguenza anche le indagini classiche si intersecano con questa scienza forense.

Normativa di riferimento

Codice Civile (c.p.) e Codice Procedura Civile (c.p.p.)

- Disponibilità delle prove: art. 115 c.p.c.
- Consulenza tecnica è regolata dagli artt. 61-64 e artt. 192-194 c.p.c.

Codice Penale (c.c.) e Codice di Procedura Penale (c.p.c.)

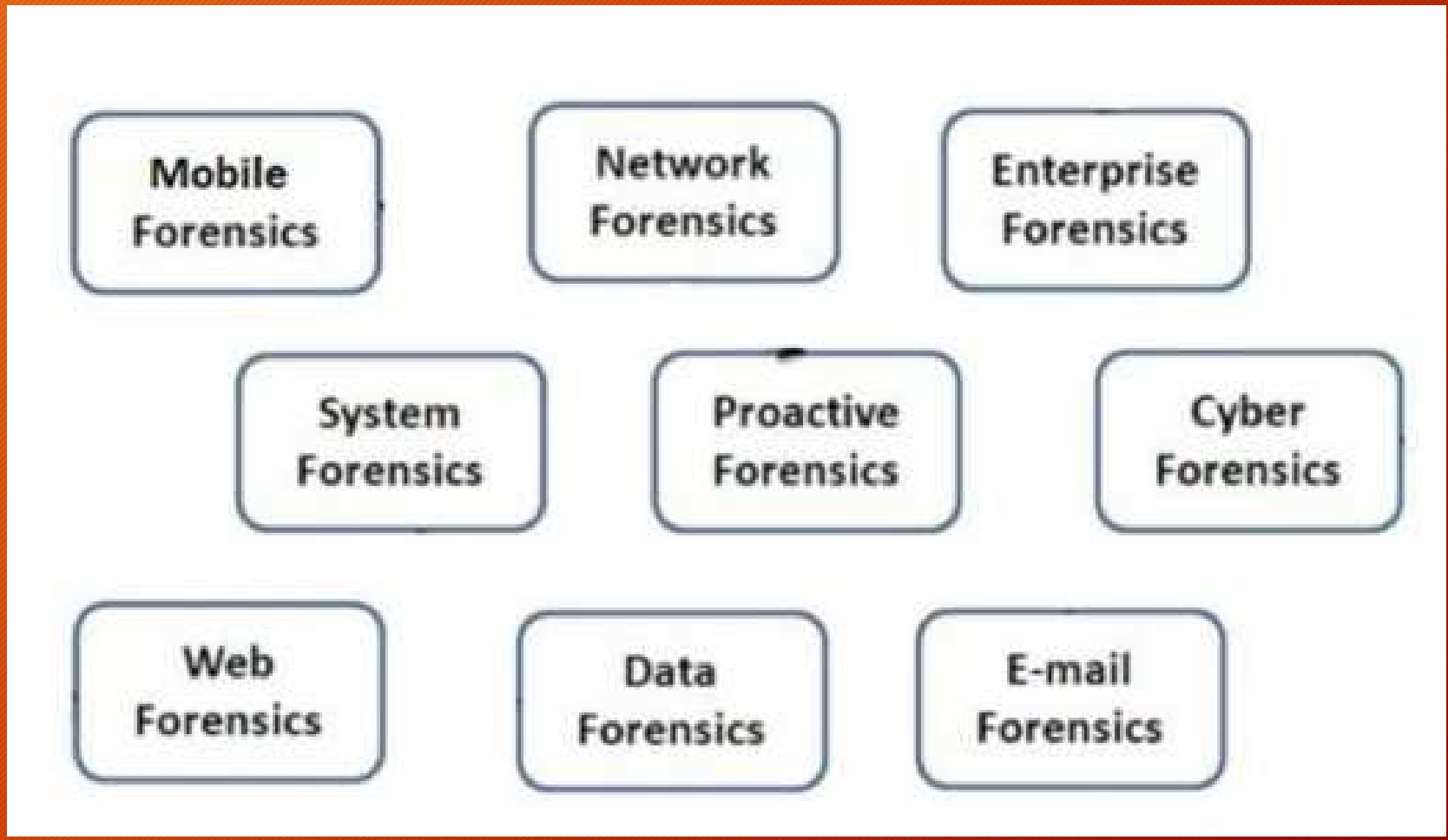
- Oggetto della prova: art. 187 c.p.p.
- Mezzi di prova: artt. 194 – 243 c.p.p.
  (la perizia e la consulenza tecnica, i documenti)
- Mezzi di ricerca della prova: artt. 244 – 271 c.p.p.
  (ispezioni, perquisizioni, sequestro, intercettazioni)
- Consulenti tecnici del pubblico ministero: art. 359 c.p.p.
- Accertamenti tecnici non ripetibili: art. 360 c.p.p.
- Accertamenti urgenti e sequestro: artt. 352-354 c.p.p.
- Incidente probatorio: art. 392 c.p.p.

Normativa di riferimento

In sintesi il Consulente Tecnico, durante il suo operato, deve assicurare cinque 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**

Digital Forensics



Standard Internazionali

La serie **ISO/IEC 27000 - Information security management systems** raggruppa un insieme di norme che hanno lo scopo di proteggere le informazioni che vengono mantenute ed elaborate da un'organizzazione. Tra queste troviamo:

- 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.

Standard Internazionali

La norma ISO stabilisce i requisiti della prova in formato digitale che sono di seguito riepilogati:

- **Pertinenza**: occorre dimostrare che il materiale è rilevante, cioè che contiene dati utili e che pertanto esiste una buona ragione per acquisirli
- **Affidabilità**: tutti i processi eseguiti devono essere ben documentati producendo un risultato riproducibile
- **Sufficienza**: occorre raccogliere tutto il materiale informatico necessario, valutando in base al caso e alle limitazioni di carattere giuridico
- **Verificabilità**: documentando tutte le attività svolte, un consulente tecnico informatico terzo deve essere in grado di verificare le attività svolte, valutando metodo scientifico, le tecniche e le procedure seguite
- **Giustificabilità**: bisogna essere in grado di dimostrare che le scelte adoperate erano le migliori possibili o le uniche possibili

Fasi della Digital Forensics

IDENTIFICATION

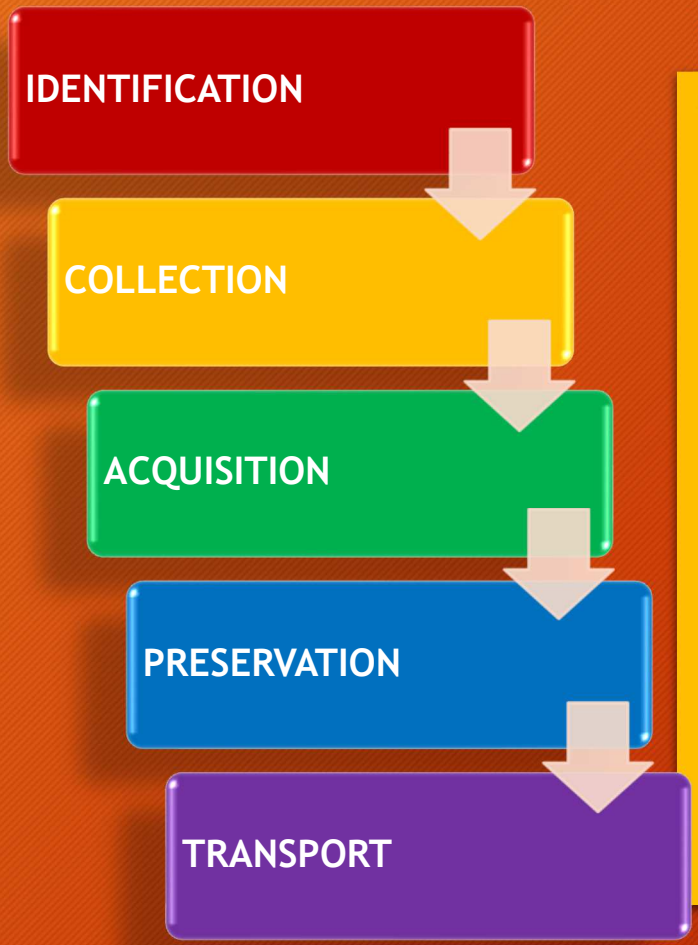
Il processo di identificazione implica la ricerca, l'individuazione e la documentazione delle potenziali prove digitali.

Il processo di identificazione dovrà individuare gli strumenti di archiviazione digitale e i device di elaborazione che possono contenere potenziali prove digitali.

Questo processo comprende anche un'attività di attribuzione della priorità nella raccolta delle prove basata sulla loro volatilità.

Inoltre, il processo dovrà accertare l'eventualità di potenziali prove digitali nascoste.

Fasi della Digital Forensics



COLLECTION

Una volta identificati i digital device che possono contenere potenziali prove digitali, si dovrà decidere se procedere alla raccolta/sequestro o all'acquisizione nel processo che segue.

La raccolta è un processo in cui i device che possono contenere potenziali prove digitali sono trasferiti dalla loro posizione originale ad un laboratorio.

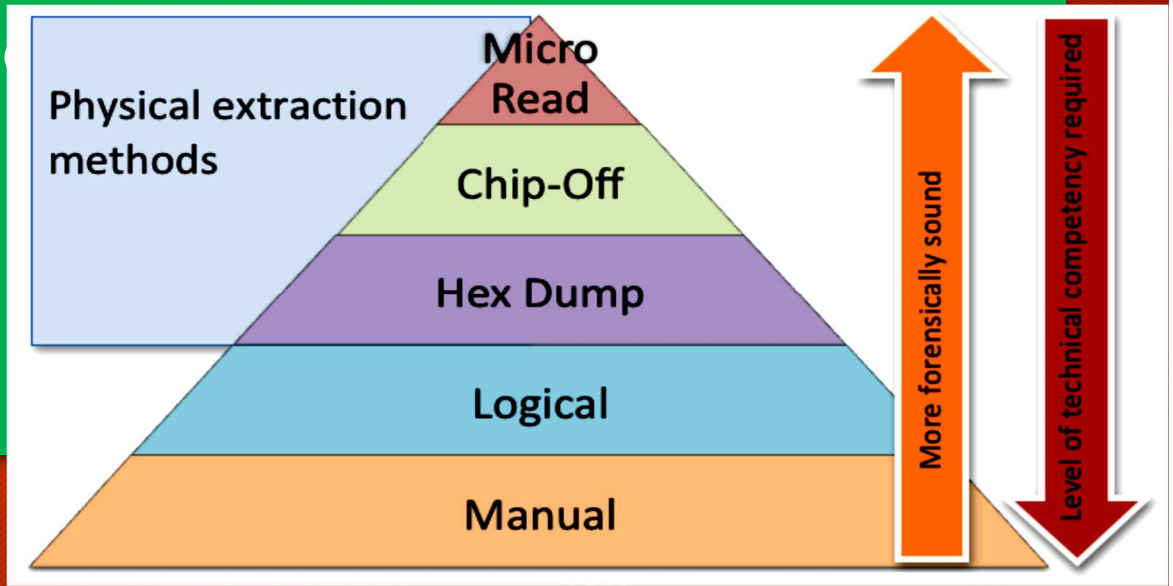
Questo processo include la documentazione dell'intero metodo, compreso l'imballaggio di questi device prioritario al trasporto.

Fasi della Digital Forensics

ACQUISITION

Il processo d acquisizione implica la produzione di una copia forense delle prove digitali e la documentazione dei metodi utilizzati e delle attività svolte.

Tipi



Fasi della Digital Forensics

PRESERVATION

La fase nella quale occorre proteggere la riservatezza e l'integrità dei supporti informatici e dei dati digitali raccolti e acquisiti.

Le potenziali prove digitali dovranno essere conservate per assicurare la loro utilità nelle indagini. È importante proteggere l'integrità delle prove. Il processo di conservazione implica la salvaguardia delle potenziali prove digitali e dei digital device che possono contenere potenziali prove digitali da manomissioni e alterazioni.

Fasi della Digital Forensics

TRANSPORT

La fase nella quale occorre adottare gli opportuni accorgimenti per la protezione di riservatezza supporto infor digitale.

È importante u catena di cust


Dettagli reperto informatico e catena di custodia

Caso: | © reperto:

Informazioni sulle evidenze

Dettagli macchina originaria

Produttore:
Modello:
Serial number:
Part number:
Note aggiuntive (schede, etichette, usernames, ecc...):

Dettagli reperto

Produttore:
Modello: | Dim. (GB):
Serial number:
Part number:
HASH: | MD5:
SHA1:
Note aggiuntive:

Reperto informatico originario presentato da

Nome e cognome:
Data e ora:
Luogo:
Note aggiuntive:

Catena di custodia

Data e ora	Ricevuto da	Descrizione
	Nome: Firma:	
	Nome: Firma:	
	Nome: Firma:	
	Nome: Firma:	
	Nome: Firma:	

Fasi della Digital Forensics

EXAMINATION

In questa fase sono esaminate le evidenze digitali per identificare ed estrarre tutto il contenuto digitale utile alla fase successiva di analisi.

Possono essere adoperate tecniche di data carving per tentare di recuperare le evidenze cancellate.

Fasi della Digital Forensics

ANALYSIS

Vengono analizzate tutte le evidenze digitali estratte per tentare di rispondere al quesito.

Le evidenze possono essere messe in correlazione tra loro per ricostruire un determinato evento.

In presenza di molti dati possono essere utilizzate le metodologie della big data analysis.

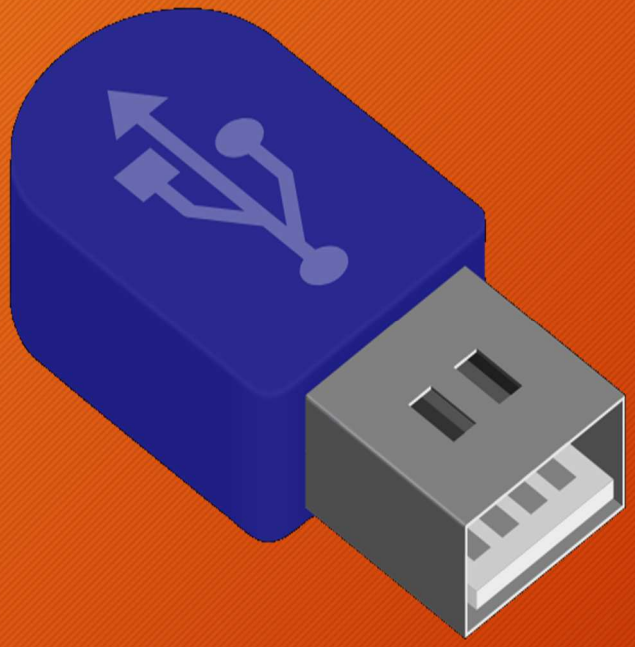
Fasi della Digital Forensics

REPORTING

L'obiettivo finale è quello di redigere un elaborato in cui descrivere:

- L'origine delle evidenze
- La metodologie utilizzata
- La tecnologie adoperata
- la procedura eseguita
- I risultati ottenuti oppure la risposta al quesito

Esercizio 1



Passi:

- Acquisire il contenuto di un memoria di massa
- Calcolare il codice hash
- Analizzare la copia

Tools:

- FTK Imager
- PhotoRec
- Autopsy

Acquisizione a distanza

Architettura dei Servizi Internet

Ispezione – Perquisizione – Acquisizione

Problema

La nascita del c.d. Web 2.0 ha favorito la proliferazione di diversi servizi Internet (**Newsgroup, Blog, Chat, Social network**), utilizzati per la diffusione delle informazioni, spesso non regolamentati e coperti dall'anonimato.

Ciò ha incrementato il numero di determinati reati quali:
la diffamazione, lo stalking (cyber-stalking), l'hate-speech, l'adescamento telematico (grooming), la pedopornografia, il reverge porn, il sextortion, il furto d'identità digitale, la sostituzione di persona, la violazione di copyright e l'utilizzo illecito di marchi, il furto dei dati, il phishing, le truffe online, l'accesso abusivo ad una banca dati, la violazione della privacy, il controllo a distanza illecito, l'assenza di tutela legale, ecc.

Inoltre, in base alle caratteristiche dei predetti servizi, le informazioni oggetto di reato possono essere volatili e, quindi, facilmente manipolabili o rimovibili.

La soluzione consiste nel realizzare una acquisizione forense e certificata del contenuto che si contesta, che diventerà evidenza o prova nel processo civile o penale, prima che possa scomparire.

Acquisizione di una pagina web

La stampa in PDF o su carta può essere utilizzata come prova?

Le stampe o gli screenshot difficilmente sono ammessi in un procedimento giudiziario come prova perchè non godono dell'**integrità** delle evidenze informatiche raccolte con strumentazione adeguata e metodi scientifici.

Anche la fotografia dello schermo del PC non ha pienamente valore probatorio, o meglio, può essere facilmente essere contestata dalla controparte, poiché per quanto possa avere una storicità temporale (l'ora esatta potrebbe essere contenuta nell'immagine, ovvero il sistema che l'ha generata si sincronizza automaticamente con l'ora esatta e salva le immagini in modo incrementale) ritrae qualcosa che può facilmente essere **artefatto** (lo schermo).

Acquisizione di una pagina web

La stampa in PDF o su carta può essere utilizzata come prova?

La stampa di un pagina web **certificata da un Notaio** o da un **Pubblico Ufficiale** è certamente un'alternativa migliore, ma può non essere sufficiente a identificare l'autore del reato, per esempio nel caso di un post diffamatorio pubblicato su un social network è necessario acquisire anche ulteriori dati come il codice identificativo univoco che permette di ritrovare il profilo o la pagina diffamatoria anche in caso di cambio del nome o dell'indirizzo.

Fatto salvo **il principio del libero convincimento del giudice** che gli consente di valutare la prova dando conto nella motivazione dei risultati acquisiti e dei criteri adottati (c.p.p. art. 192, comma I).

Acquisizione di una pagina web

Come procedere?

Iniziare a raccogliere le informazioni a latere:

- l'indirizzo del sito/servizio (whois)
- il proprietario del sito/servizio
- la tecnologia utilizzata per creare il sito/servizio
- l'autore dell'informazione (ID user)
- i dati identificativi dell'informazione (ID di un post, l'ora e la data)
- **La cronologia delle pagine che occorre acquisire per**
  - **rappresentare l'informazione d'interesse**
  - **dimostrare l'autore della pubblicazione e delle altre informazioni a latere**

OSINT

Acquisition type

La scelta della metodologia di acquisizione può dipendere da diversi fattori, tra cui:

- **Lo status** (acceso/spento/guasto/online/offline)
- **La posizione** (in presenza/a distanza/live/sequestrato)
- **La tecnologia** (mem. fisica/logica/mobile/web service/db)
- **Le misure di protezione** (pin/password/cifratura)
- **L'obiettivo** (incident response/uso giudiziario)
- **I vincoli legali** (giurisdizione/privacy/tutela del diritto d'autore e/o di altri diritti)

Target status

Acceso/Online

- Acquisizione Live
- Copie logiche dei dati
- Acquisizione Memoria RAM
- Chiavi di cifratura
- Connessioni di rete attive
- Copia supporti non rimovibili
- ….
- Successivamente, si spegne la macchina e si procede →

Spento/Offine

- Si possono rimuovere i supporti di memoria
- Si effettua la copia bit-a-bit
- È possibile fare il carving dei dati sullo spazio libero
- Il contenuto del dispositivo può essere cifrato … occorre procurarsi le chiavi e/o accendere il dispositivo

Target position

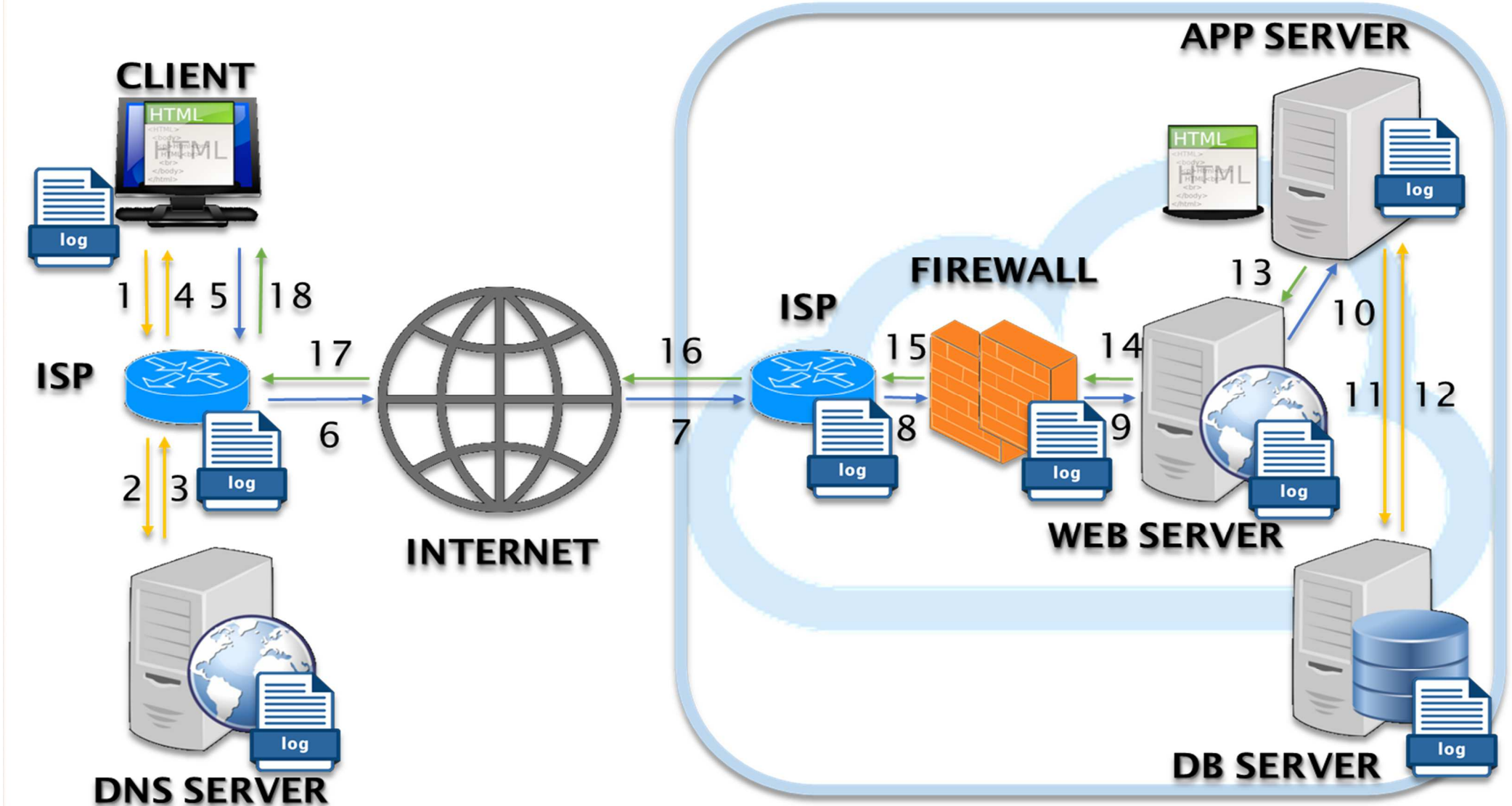
Presenza/On site

- È possibile effettuare la copia bit-a-bit dei dati
- Si possono verificare le connessioni e le sessioni utente
- Si può sequestrare tutto il materiale, oppure selezionare i dati di interesse

Distanza/Remote

- Spesso non è possibile effettuare una copia bit-a-bit della memoria
- Si può effettuare un'acquisizione logica
- Molto utile per fare una «preview» del target, oppure nei casi in cui è complicato intervenire sul provider *(es. giurisdizione, termini di contratto, rogatorie internazionali)*

Web architecture



Acquisizione classica

L'acquisizione forense delle evidenze digitali a fine di dimostrare l'esecuzione di un determinato reato, avvenuto attraverso la rete Internet, può prevedere la raccolta dei seguenti elementi:

- La copia forense dei servers (**anche parziale**)
- **I logs dei servers** (WEB, APP, DB)
- **I log del traffico dell'ISP** che ospita i server
- **I logs del traffico dell'ISP** da cui è stata effettuata la connessione
- **I logs dei DNS server**
- **I logs del traffico telefonico** (per risalire all'utenza telefonica)
- **La copia forense del client** con cui è stato eseguito il reato

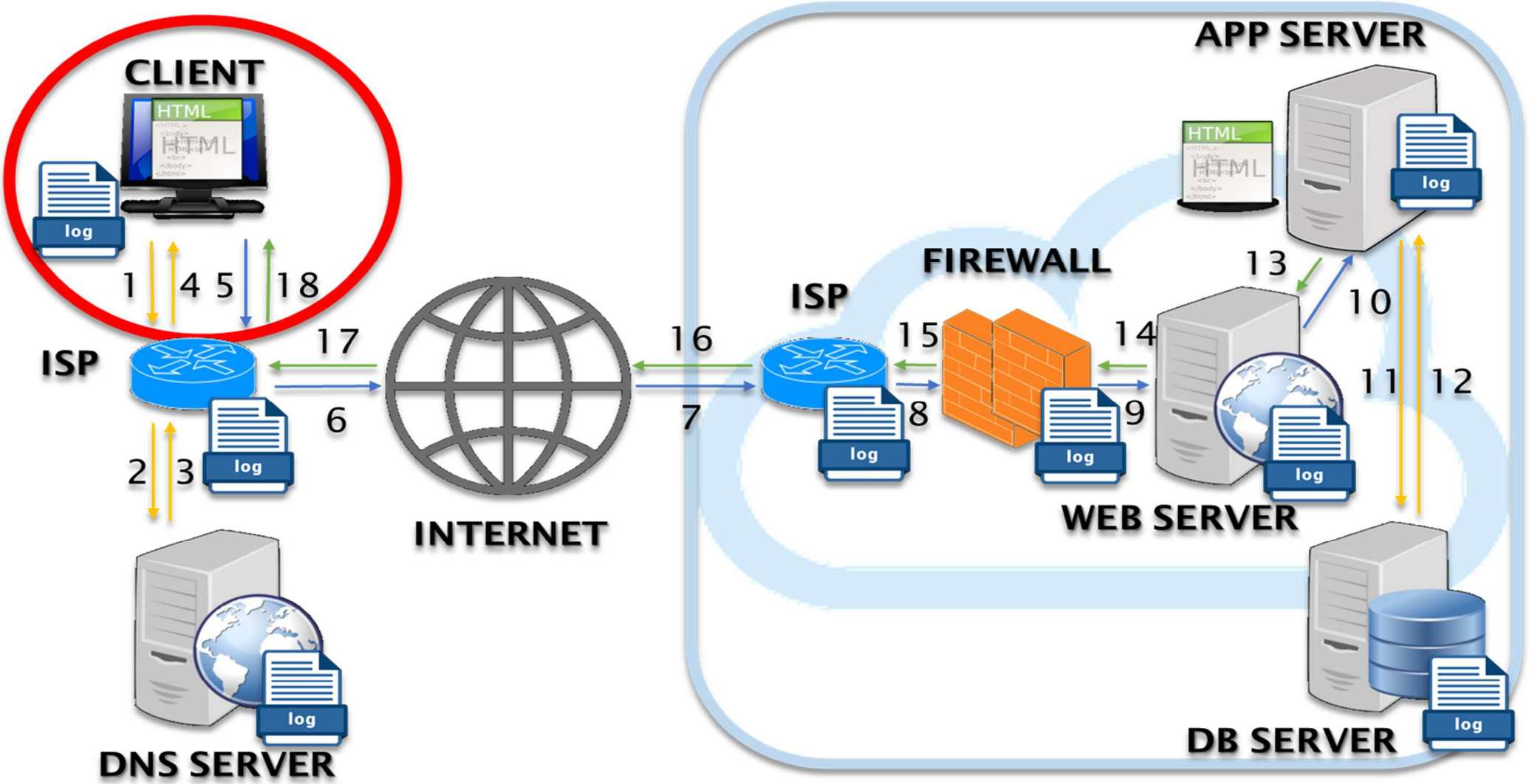
Acquisizione a distanza

L'acquisizione forense a distanza – attuata attraverso una connessione alla rete Internet – può essere eseguita per dimostrare l'esecuzione di un determinato reato, avvenuto attraverso la rete Internet, come:

- la diffamazione, lo stalking (cyber-stalking), l'hate-speech, l'adescamento telematico (grooming), la pedopornografia, il reverge porn, il sextortion, il furto d'identità digitale, la sostituzione di persona, la violazione di copyright e l'utilizzo illecito di marchi, il furto dei dati, il phishing, le truffe online, l'accesso abusivo ad una banca dati, la violazione della privacy, il controllo a distanza illecito, l'assenza di tutela legale, ecc.

È la tecnica utilizzata per realizzare una «preview» del dato e nei casi in cui non è possibile intervenire in presenza sui dispositivi su cui sono memorizzate le evidenze di interesse (p.e. per problemi di competenza territoriale, termini di contratto, rogatorie internazionali, ecc.)

Web architecture



Acquisizione di una pagina web

Alla luce delle **casistiche** *(pagina web, profilo sociale, mail, ecc.)*, del **contesto** *(evidenza principale o secondaria)* e della **volatilità del dato** possiamo distinguere tre modalità:

1. Acquisizione «**On-the-fly**» o «**Smart**»
2. Acquisizione «**Full**» o «**Rich**»
3. Acquisizione «**Paranoid**»

Gli elementi essenziali ed obbligatori, che rendono giuridicamente valida l'acquisizione, sono i seguenti:

- **Relazione dettagliata delle operazioni eseguite**
- **Firma digitale, con apposizione di una marca temporale, di tutti i contenuti digitali acquisiti**

Acquisizione «On-the-fly»

È la modalità più veloce per realizzare un'acquisizione di un contenuto web e può essere attuata con qualsiasi browser.

Passi:

- Creare un copia completa della pagina con il «Salva con nome» del browser
- Realizzare una seconda copia in formato PDF o Immagine (BMP,JPG,PNG)
- Realizzare una terza copia attraverso uno dei seguenti siti:
  - **https://www.hashbot.com (free/download/hash)**
  - **http://archive.is/ (free)**
  - **http://web.archive.org (free)**
  - **http://www.perma.cc (free)**
- Apporre la Firma digitale con Marca temporale a tutto il materiale scaricato
- Redigere una Relazione dettagliata dell'attività

Acquisizione «Full»

È la modalità completa per realizzare un'acquisizione di un contenuto web e può essere attuata con più livelli di dettaglio.

Registrare l'uscita audio/video della postazione:

- **OBS Studio** (obsproject.com free)
- **Icecream Screen Recorder** (icecreamapps.com free/pro)
- **Apowersoft** (apowersoft.it try/pro)

Registrare il traffico di rete generato:

- **Wireshark**
- **Microsoft Network Monitor**
- **Ethereal**

Catturare il contenuto web:

- **Firefox**
- **FAW**
- **Download dei file (anche attraverso l'uso di plug-in)**

Acquisizione «Full»

Passi:

1. Avviare la capture dell'audio/video
2. Avviare la capture del traffico di rete
3. Sincronizzare time
4. Controllare configurazione di rete / dns / proxy
5. Fare un tracert verso il target
6. Aprire il browser e navigare fino al target
7. Salvare la pagina in formato html e pdf (oltre al download di altri files)
   - Se necessario ritornare al punto 6
8. Chiudere la capture del traffico di rete
9. Chiudere la capture dell'audio/video
10. Apporre la Firma digitale con Marca temporale a tutto il materiale scaricato
11. Redigere una Relazione dettagliata dell'attività

Acquisizione «Paranoid»

È uguale alla modalità «Full», ma viene eseguita all'interno di una macchina virtuale «pulita».

- Dopo aver realizzato l'acquisizione, seguendo i passi citati in precedenza, si chiude la macchina virtuale e si aggiunge al materiale scaricato.
- Apporre la Firma digitale con Marca temporale a tutto il materiale scaricato
- Redigere una Relazione dettagliata dell'attività

Quadro normativo: ispezioni

La **Legge 48 del 18/3/20018** «*Ratifica ed esecuzione della Convenzione del Consiglio d´Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell´ordinamento interno*» ha introdotto alcune novità nel codice di procedura penale:

Art. 244 c.p.p. Ispezioni - Casi e forme delle ispezioni

1. L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.

2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. **L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione**.

Modus operandi: ispezione

È un mezzo di ricerca della prova disposto quando occorre accertare le tracce e gli altri effetti materiali del reato, ovvero descrivere lo stato dei luoghi.

Se dovessimo realizzare **un'ispezione** ci limiteremo ad un'osservazione del sistema attraverso la descrizione del suo status, anche con l'ausilio di immagini, e l'annotazione della eventuale presenza di software attivi, nonché periferiche e connessioni, con la conseguenza che all'attività di osservazione, **descritta nel verbale contestualmente redatto**, **non può seguire quindi alcuna forma di apprensione delle informazioni** eventualmente individuate all'interno del sistema: l'ispezione del sistema, infatti, rappresenta un'attività preliminare rispetto al contesto dell'indagine informatica, usualmente deputata all'estrazione di dati digitali, pur nelle forme della legal imaging generalmente condivisa.

Quadro normativo: perquisizione

Art. 247 c.p.p. Perquisizioni - Casi e forme delle perquisizioni

1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.

1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

2. La perquisizione è disposta con decreto motivato.

3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.

Modus operandi: perquisizione

La perquisizione è un Mezzo di ricerca della prova adottato nel processo penale qualora si ritenga che determinate cose pertinenti al reato afferiscano o si occultino.

Pertanto, assumono rilevanza **le modalità di perquisizione dell'elaboratore elettronico**, dettate dal comma 1-bis dell'art. 247 c.p.p., cui fa da pendant l'art. 352, comma 1-bis, c.p.p.

In tale ipotesi, oltre a redigere un dettagliato verbale, l'operatore dovrà acquisire le informazioni d'interesse «adottando le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

Presentazione dei risultati

Come creare un Report

Firma digitale e Marca temporale

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*
- **Acquisizione e/o Analisi**
  - *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*

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.**

Fine

vincenzo.calabro@unirc.it

linkedin.com/in/vincenzocalabro