DIGITAL FORENSICS

Introduzione all'Informatica Forense

INDAGINI ONLINE

About me

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

Mi sono «perfezionato» in Data Protection e Data Governance (UniMi) e in Criminalità Informatica e Investigazioni Digitali (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

AGENDA

- Introduzione alla Digital Forensics
  - Definizioni: Digital Evidence, Investigation, Forensics
  - Normativa di riferimento
  - Standard Internazionali
  - Fasi della Digital Forensics
  - Conclusioni – Quesiti
- D.F. applicata alle memorie di massa
- D.F. applicata alle evidenze online
- D.F. applicata ai dispositivi mobile

Introduzione

Definizioni: Digital Evidence, Investigation, Forensics

Normativa di riferimento - Standard Internazionali

INDAGINI ONLINE

Digital Forensics: perché?

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

Anche i reati hanno questa peculiarità?

Distinguiamo:

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

E gli altri illeciti?

- Cause civili
- Cause lavoro
- Cause amministrativo
- Cause tributarie

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.

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 Evidence

A prescindere dalla definizione che vogliamo utilizzare, 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: valore probatorio

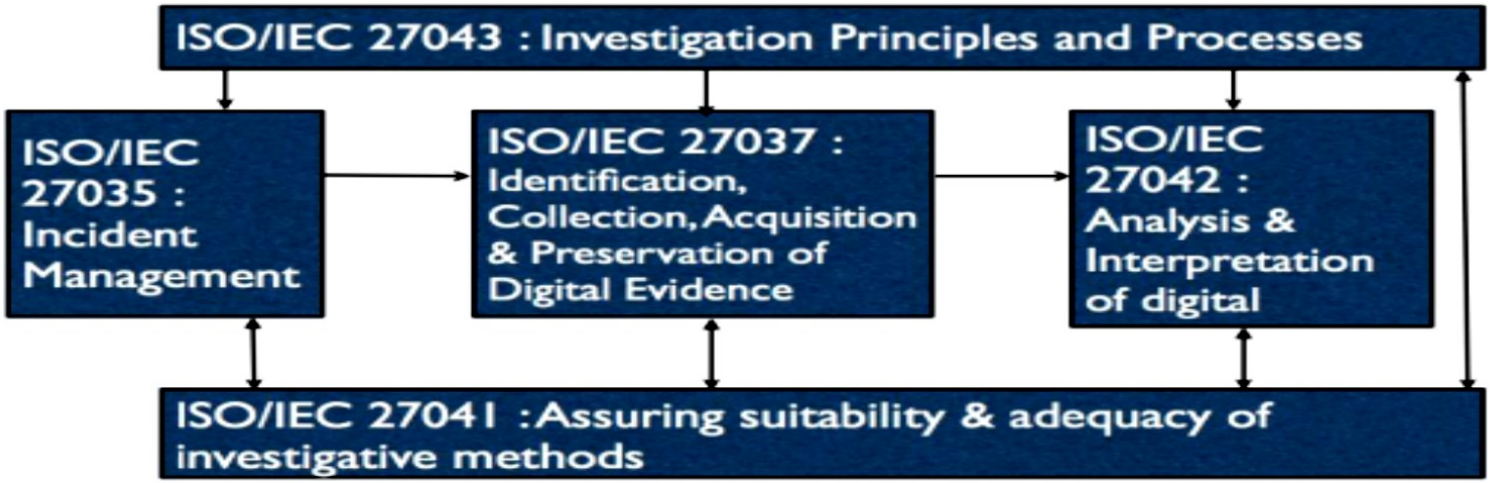
Il valore probatorio della prova informatica deve essere inteso come **la capacità di resistenza ad eventuali contestazioni e capacità di convincimento del giudice, delle parti processuali o di altri soggetti** in ordine alla **genuinità**, **non ripudiabilità**, **imputabilità** e **integrità** del dato stesso e dei fatti dallo stesso dimostrati.

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

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.

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.

A livello generale, si tratta di individuare le modalità e le tecnologie migliori per soddisfare i seguenti obiettivi:

- acquisire le prove **senza alterare o modificare** il sistema informatico su cui si trovano
- garantire che le prove acquisite siano **identiche** a quelle originarie
- analizzare i dati senza **alterarli**
- esplicitare il processo per renderlo **ripetibile**

Approccio: Digital Forensics

L'approccio, che consente di svolgere al meglio l'attività, riguarda quattro aspetti essenziali:

1. **un aspetto TECNICO.** Il primo problema da risolvere è quello dell'aggiornamento, in quanto la tecnologia muta rapidamente, aumentano le dimensioni dei sistemi di storage e i tools di analisi diventano spesso obsoleti o non sono in grado di gestire grandi quantità di dati.
2. **un aspetto PROCEDURALE**. L'analisi forense deve raccogliere tutto il materiale che potenzialmente possa contenere fonti di prova, e ciò vuol dire analizzare e vagliare tantissime informazioni a supporto delle investigazioni. Il problema, da un punto di vista squisitamente procedurale, è che sovente non esistono procedure, linee guida, protocolli standard o, se esistono, non vengono molto spesso applicati, conosciuti o standardizzati.
3. **un aspetto SOCIALE.** Le attività di forensics pongono seri problemi sociali, soprattutto con riferimento alla privacy dell'individuo e alla raccolta e all'analisi dei suoi dati.
4. **un aspetto LEGALE,** o giuridico che dir si voglia. Si possono utilizzare le tecnologie più avanzate esistenti, le tecniche più sofisticate, i sistemi più sperimentali sul mercato, ma se l'attività di indagine forense sui dati informatici non è conforme alle regole, soprattutto procedurali, dettate dalla legge, tutto ciò è assolutamente inutile.

Digital Forensics: metodo scientifico

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.

Linee guida e normative

RFC 2350 (06/1998): *"Expectations for Computer Security Incident Response"*

Convenzione di Budapest (11/2001) del Consiglio d'Europa sulla *criminalità informatica*

RFC 3227 (02/2002): "*Guidelines for Evidence Collection and Archiving*"

Legge 48/2008 (03/2008): "*Ratifica la Convezione di Budapest e modifica il C.P, il C.P.P., il D.lgs. 231/2001 e il cd. Codice della Privacy*"

ISO 27035 (09/2011-11/2016): "*Information security incident management*"

ISO 27037 (10/2012). "*Guidelines for identification, collection, acquisition and preservation of digital evidence*"

ISO 27041 (06/2015): "*Guidance on assuring suitability and adequacy of incident investigation methods*"

ISO 27042 (06/2015): "*Guidelines for analysis and interpretation of digital evidence*"

ISO 27043 (03/2015): "*Incident investigation principles and process*"

Normativa di riferimento nell'ambito giudiziario italiano

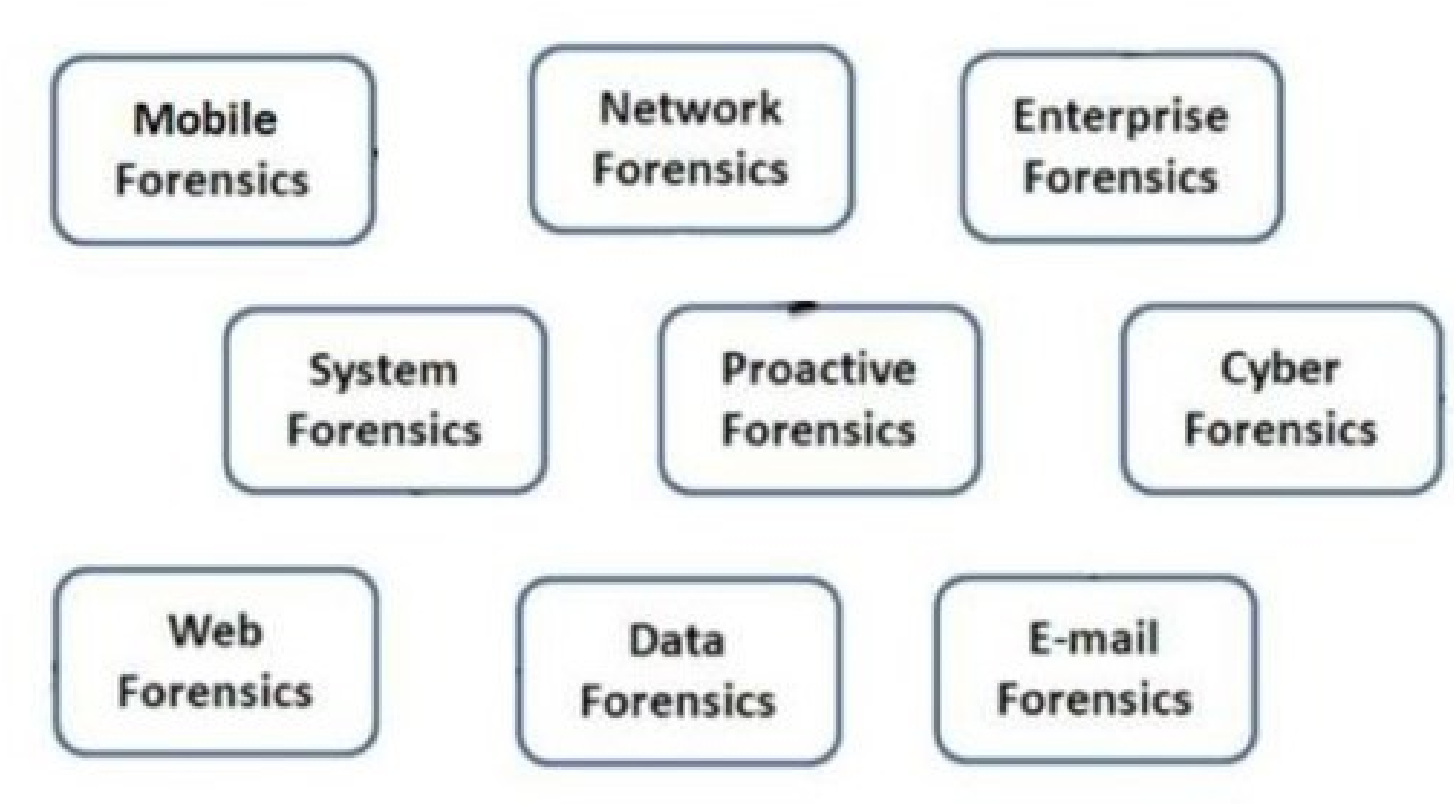
Codice Civile (c.c.) e Codice Procedura Civile (c.p.c.)

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

- 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.

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.

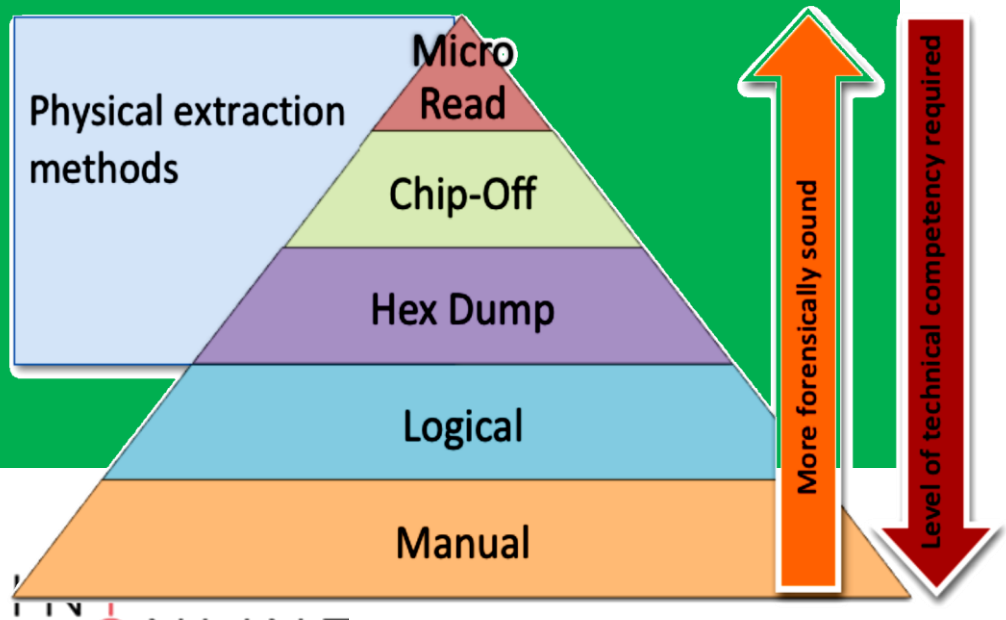
Questo processo include la documentazione dell'intero metodo, compreso l'imballaggio di questi device prioritario al trasporto.

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.

Occorre rispettare l'ordine di volatilità. Tipi di acquisizione:



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 e integrità del supporto informatico e del dato digitale.

È importante utilizzare la catena di custodia per documentare la storia degli accessi e degli spostamenti dei reperti originali e delle copie.


Dettagli reperto informatico e catena di custodia

Caso: ID reperto:

Informazioni sulle evidenze

Dettagli macchina originale

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

Dettagli reperto

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

Reperto informatico originale presentato da

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

Catena di custodia

Data e ora	Interfaccia		Descrizione
	Nome	Nome	
	Nome	Nome	
	Nome	Nome	
	Nome	Nome	
	Nome	Nome	

INDAGINI ONLINE

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.

E' possibile che il dato sia cifrato o protetto, pertanto è necessario utilizzare tecniche di hacking per ottenere il dato in chiaro.

Fasi della Digital Forensics

ANALYSIS

Solitamente è la fase più laboriosa.

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 metodologie di 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**

In sintesi

Il Consulente Tecnico, durante il suo operato, deve assicurare che siano rispettate 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**

Acquisizione e analisi forense

INDAGINI ONLINE

Problema

La trasformazione digitale di molteplici attività, che prima si sviluppavano attraverso lo scambio di documenti analogici, interessa anche i fenomeni criminali e, pertanto, è necessario che le tecniche di analisi forense si adeguino alle nuove tecnologie.

La Digital Forensics consiste nella raccolta ed analisi dei reperti che possono essere utilizzati al fine di documentare il fenomeno verificatosi e poter perseguire i responsabili.

Affinché le prove estrapolate dai reperti possano essere utilizzabili in sede processuale è bene adottare una serie di linee guida.

Queste linee guida hanno il compito di:

- Definire i requisiti del reperto digitale
- Stabilire le fasi da seguire e l'obiettivo che si vuole raggiungere
- Individuare le figure professionali che gestiranno le evidenze digitali

Requisiti del reperto digitale

Prova digitale

- Informazione o dato, memorizzato o trasmesso in formato binario, che può essere utilizzato come prova

Copia di prova digitale

- Copia di prova digitale che può essere prodotta per mantenere l'affidabilità della prova, includendo sia la prova digitale che la procedura di verifica

Dato volatile

- Dato facilmente soggetto a modifica. Una variazione può essere dovuta ad assenza di corrente o ad interventi di campi magnetici, a cambi di stato del sistema

Alterazione

- Modifica del valore di potenziali evidenze digitali e riduzione del valore probatorio

Distruzione di prova

- Modifica volontaria del valore di potenziali evidenze digitali

Requisiti del metodo forense

Pertinenza

- Serve per incolpare (o discolpare)
- Dimostrare che il materiale è rilevante, cioè che contiene dati utili e che pertanto esiste una buona ragione per acquisirli

Affidabilità

- Assicurarsi che la prova digitale sia genuina
- Tutti i processi eseguiti devono essere ben documentati e, se possibile, ripetibili. Il risultato dovrebbe essere riproducibile

Sufficienza

- Il Digital Evidence First Responder (DEFR) deve valutare quale materiale deve essere raccolto e le procedure idonee
- Il materiale può essere copiato o acquisito (sequestrato)
- Non è detto che sia sempre necessario acquisire una copia completa
- Valutare in base al caso (interessa la figura del DEFR)
- Può dipende dalla legislazione nazionale

Requisiti del metodo forense

Verificabilità

- Un terzo deve essere in grado di valutare le attività svolte dal DEFR e dal DES
  - Attuabile se esiste la documentazione delle azioni svolte
  - Valutare il metodo scientifico, le tecniche e le procedure seguite
- DEFR e DES devono essere in grado di giustificare le azioni svolte

Ripetibilità

- Le operazioni devono sempre essere ripetibili utilizzando le stesse procedure, lo stesso metodo, gli stessi strumenti, sotto le stesse condizioni

Riproducibilità

- Le operazioni possono essere ripetibili anche usando lo stesso metodo, gli strumenti diversi, sotto condizioni diverse

Giustificabilità

- Dimostrare che le scelte adoperate erano le migliori possibili

Figure professionali coinvolte

Vengono definite tre figure chiave, che si occupano e sono responsabili degli aspetti di gestione della prova digitale:

- il **DEFR o Digital Evidence First Responder** è un soggetto autorizzato, formato e qualificato ad agire per primo sulla scena di un incidente per eseguire attività di raccolta ed acquisizione delle prove avendone inoltre la responsabilità di corretta gestione
- il **DES o Digital Evidence Specialist** è un soggetto che ha le capacità di eseguire le stesse attività eseguite da un DEFR ed in più possiede conoscenze specialistiche ed è in grado di gestire una moltitudine di problematiche tecniche, ad esempio è in grado di portare a termine attività quali acquisizione di rete, di memoria RAM ed ha ampia conoscenza di sistemi operativi e/o Mainframe
- l'**Incident Response Specialist**, che normalmente è una figura professionale interna all'azienda che si occupa del primo intervento post incidente informatico.

Identificazione

La prova informatica si presenta in forma fisica e logica

- Device
- Rappresentazione dei dati

- Ricerca dei device che possono contenere dati rilevanti
  - Priorità ai dati volatili
  - Considerare dispositivi di difficile identificazione
    - Geografica: Es.: Cloud computing, SAN
    - Dimensioni Es.: miniSD
- Si considera computer un dispositivo digitale standalone che riceve, processa e memorizza dati e produce risultati
    - Non connesso in rete
    - Ci possono essere periferiche connesse
- Se il computer ha un'interfaccia di rete, anche se non è connesso in rete al momento dell'intervento, bisogna individuare gli eventuali sistemi con cui può aver comunicato

Identificazione

La scena del crimine può contenere diversi tipi di dispositivi di memorizzazione

- Hard disk, hard disk esterni, floppy disk
- Memorie flash, memory card, CD, DVD, Blu-ray

In fase di identificazione il DEFR deve:

- Documentare marca, tipo e numero di serie di ogni supporto individuato. Inoltre, se i supporti risultano danneggiati esternamente, deve documentare lo stato con l'ausilio di foto
- Identificare tutti i computer e il loro stato (acceso/spento), che deve rimanere inalterato:
  - stato acceso: documentare cosa è visibile sullo schermo (effettuando foto) e inserirlo a verbale
  - stato spento: non effettuare alcuna operazione sul dispositivo.
- Reperire i caricabatterie dei dispositivi alimentati a batteria, per evitare che possano scaricarsi
- Utilizzare un rilevatore di segnali wireless per verificare la presenza di dispositivi nascosti
- In determinate situazioni può essere molto utile prendere in considerazione anche evidenze non digitali, come ad esempio informazioni sui dispositivi fornite da personale impiegato in azienda (ad esempio: scopo di utilizzo del dispositivo, password per l'accesso, ecc. . .)

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.)

Raccolta (sequestro) o acquisizione?

Una volta terminata la fase di identificazione il DEFR, con gli strumenti in suo possesso, deve decidere se procedere con la raccolta o l'acquisizione.

Per prendere tale decisione vanno presi in considerazione alcuni fattori:

- volatilità della possibile evidenza
- esistenza di cifratura completa o parziale dei supporti (nel qual caso può essere utile effettuare l'acquisizione dei dati volatili in RAM)
- criticità del sistema (es. server che non può essere spento poiché critico per il business aziendale)
- requisiti legali
- carenza delle risorse necessarie (ad es. quantitativo di spazio necessario o disponibilità del personale).

Raccolta (sequestro) o acquisizione?

Dopo aver identificato i reperti e scelto se sequestrarli o acquisirli in loco occorre:

- Valutare cosa è pertinente e cosa è trascurabile
- Acquisire tutto quello che è necessario
- Assegnare un identificativo ad ogni reperto ed etichettarlo
- Compilare una scheda con le informazioni visibili (marca, modello, seriale, ubicazione, stato, condizioni, collegamenti)
- Stabilire un piano di acquisizione efficace e conforme agli obiettivi dell'indagine

Raccolta

Nel caso in cui si opti per il sequestro dei dispositivi, la modalità di esecuzione della stessa dipende dallo stato in cui si trova il sistema.

- Sistema trovato spento

  Nel caso in cui il sistema venga trovato spento, vanno prese in considerazione le seguenti attività:

  - assicurarsi che il dispositivo sia effettivamente spento e non in standby
  - rimuovere il cavo di alimentazione, staccando prima l'estremità connessa al dispositivo e poi quella a muro
  - disconnettere e assicurare tutti i cavi connessi al dispositivo ed etichettare le relative porte a cui sono connessi, così da ricostruire le connessioni in seguito
  - proteggere il tasto di accensione, onde evitare accensione casuale del dispositivo
  - mettere in sicurezza eventuali alloggiamenti per floppy disk, cd/dvd con del nastro per evitare apertura/espulsione del contenuto.

Raccolta

- Sistema trovato acceso

  Nel caso in cui il sistema venga trovato accesso, vanno prese in considerazione le seguenti attività:

  - acquisire i dati volatili del dispositivo prima di spegnerlo, così da poter avere a disposizione eventuali chiavi di cifratura residenti in memoria. Nel caso in cui si sospetti la presenza di meccanismi di cifratura conviene procedere in seguito con acquisizione logica
  - nel caso in cui si voglia lasciare il dispositivo acceso (ad esempio per presenza confermata di meccanismi di cifratura), bisogna prestare particolare cura durante il trasporto (raffreddamento, protezione da shock)
  - nel caso in cui si decida di spegnere il dispositivo, valutare se sia il caso di effettuarlo mediante regolare procedura di spegnimento o staccando il cavo di alimentazione (rimuovendo prima l'estremità attaccata al dispositivo e poi quella attaccata alla presa). Normalmente tale decisione dipende dalla configurazione del sistema
  - etichettare e staccare tutti i cavi dal sistema. Etichettare tutte le porte cosi che lo stato del sistema possa essere ricostruito in laboratorio
  - proteggere il tasto di accensione, onde evitare una accensione casuale del dispositivo
  - infine, nel caso tale dispositivo sia un notebook, acquisire i dati volatili prima di rimuovere batteria e successivamente il cavo di alimentazione. Mettere in sicurezza anche eventuali alloggiamenti per floppy disk, cd/dvd utilizzando del nastro.

Preservazione

Occorre garantire che sia preservata, con i dovuti accorgimenti, la confidenzialità, l'integrità e la disponibilità della potenziale prova.

L'evidenza, infatti, va preservata sia durante il trasporto che lo stoccaggio, che potrebbe superare il suo tempo di vita a seconda dei tempi di giustizia.

In caso di modifica accidentale o incidentale, deve essere giustificata e documentata con apposito verbale.

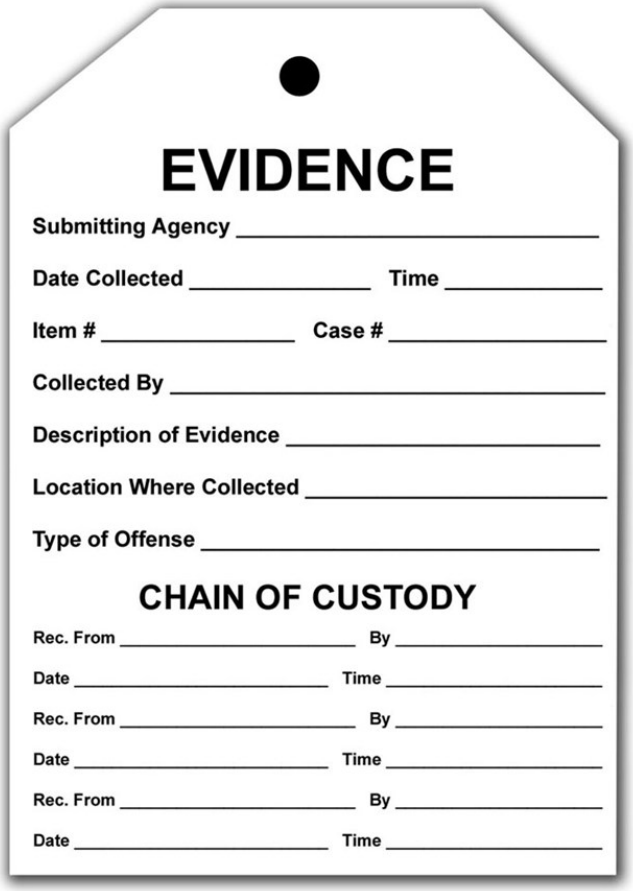
Per far ciò occorre:

- Etichettare tutto
- Verificare che le batterie siano opportunamente caricate (e ricaricare)
- Bloccare parti mobili
- Ridurre rischi in base alla natura del supporto
- Ridurre rischi dovuti al trasporto
- Preservare eventuali altri tracce
  - Es.: tracce biologiche
  - Utilizzare guanti puliti

Conservazione: catena di custodia

Data la fragilità dei dati e dei supporti che li contengono, questi ultimi devono essere protetti e sigillati per evitare modifiche o guasti e deve essere creata la Catena di Custodia.

- Documentare movimenti e interazioni con la fonte di prova digitale
- Storia del supporto a partire dalla fase di raccolta
- Formato cartaceo o digitale
- Deve contenere
  - Identificativo unico dell'evidenza
  - Quando, dove, chi e perché ha avuto accesso all'evidenza
  - Documentare e giustificare ogni alterazione inevitabile, con il nome del responsabile



Acquisizione forense

La copia forense è un duplicato fedele della memoria originale in ogni sua parte.

Le copie eseguite a basso livello sono dette bit stream image.

Possiamo distinguere alcuni tipi di acquisizioni:

- **Post mortem:** (dopo lo spegnimento) si scollega il dispositivo dal sistema di origine e lo si collega ad un postazione forense dotata di write blocker.
- **Live**: (direttamente sul sistema di origine) nel caso in cui non è possibile o è complicato scollegare i supporti di massa (dischi RAID o memoria saldate) la copia è effettuata sulla stessa macchina
- **Tramite rete**: è possibile trasferire la copia attraverso la rete

Acquisizione

Occorre stabilire e rispettare l'ordine di volatilità:

- Registri, Memoria Cache
- Memoria RAM
- Stato della rete (connessioni, socket in ascolto, applicazioni coinvolte, arp cache, routing table, dns cache, ecc.)
- Processi attivi
- Supporti di massa collegati (memorie interne: hd, pendrive)
- Log remoti
- Dispositivi rimovibili (memorie esterne: floppi, nastri)
- Supporti di backup (ottici e magnetici)

Acquisizione

- 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

Acquisizione forense

Nel caso in cui si opti per l'acquisizione dei dispositivi, sia on-site che in laboratorio, la modalità di esecuzione della stessa dipende, allo stesso modo della raccolta dallo stato in cui si trova il sistema.

- Sistema trovato acceso
  - Nel caso in cui il sistema venga trovato accesso, vanno prese in considerazione le seguenti attività:
  - acquisire tutti i dati volatili che verrebbero persi se il dispositivo venisse spento (es. RAM, processi in esecuzione, connessioni di rete, impostazioni di data ed ora). Per effettuare l'acquisizione è consigliabile riversare i dati copiati in un contenitore logico, calcolarne l'hash e documentarne il valore. Ove ciò non sia fattibile è possibile utilizzare un contenitore di tipo ZIP, calcolarne l'hash e documentarlo
  - iniziare il processo di copia forense dei dati non volatili utilizzando strumenti validati. La copia forense ottenuta va memorizzata in un dispositivo preparato per tale scopo (es. Formattato). Se la copia viene invece memorizzata in un contenitore logico bisogna assicurarsi che questa non possa essere corrotta o danneggiata. Al termine del processo di copia calcolare e annotare il valore di hash
  - utilizzare una sorgente affidabile per documentare data e ora e documentare accuratamente inizio e fine di oggi attività

Acquisizione forense

- Sistema trovato spento

  Nel caso in cui il sistema venga trovato spento, vanno prese in considerazione le seguenti attività:

  - assicurarsi che il sistema sia davvero spento
  - rimuovere il supporto di memoria dal dispositivo spento (se non già fatto), ed etichettarlo accuratamente (es. Produttore, modello, numero di serie)
  - eseguire la copia forense del supporto di memoria utilizzando un tool validato. Calcolarne il valore di hash al termine.

- Sistemi critici

  Un caso particolare nella fase di acquisizione si ha quando ci si trova davanti ad un sistema critico, per cui per svariate ragioni non è possibile procedere all'acquisizione completa dei dati contenuti all'interno del sistema. Alcuni esempi di tali sistemi sono data center, sistemi di sorveglianza o sistemi medici. In tali situazioni vi sono due sole possibili alternative di acquisizione:

  - acquisizione live (acquisizione totale della memoria RAM e di massa)
  - acquisizione parziale (solo determinate porzioni di memoria di interesse investigativo):
    - il sistema di cui si vogliono acquisire i dati ha una capacità di memoria notevolmente grande, contenendo quindi una mole notevole di dati (si pensi ai database server)
    - il sistema, a causa della sua criticità, non può essere spento
    - solo alcuni dati sono rilevanti all'interno del sistema
    - vi sono dei vincoli legali che consentono solo l'acquisizione di alcuni dati.

Algoritmi di hashing

Al termine della fase di acquisizione bisogna “sigillare” i dati acquisiti attraverso un sigillo digitale (solitamente un impronta hash con l’eventuale aggiunta dell’utilizzo di una firma digitale per associare l’operazione al DEFR) per dimostrare che la copia ottenuta sia inalterata ed identica all’originale.

L'algoritmo di hash (MD5, SHA-1) elabora una qualunque mole di bit e restituisce in output una stringa di bit di dimensione fissa.

L'output è detto digest.

- La stringa di output è univoca per ogni documento e ne è un identificatore
- L'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output (anche se in realtà per ogni digest esistono infiniti input che lo generano – cd. collisioni)

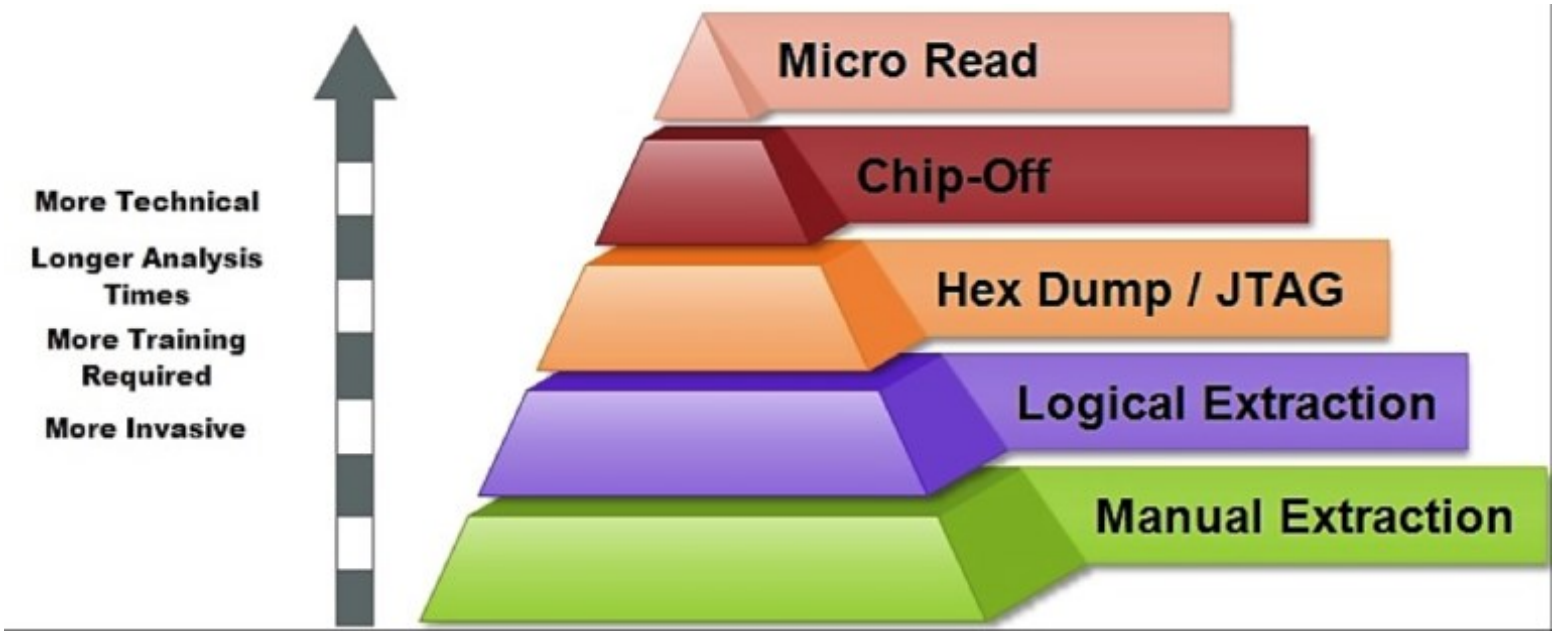
DPCM 8 febbraio 1999: «l'impronta di una sequenza di simboli binari è una sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione di hash»

Algoritmi di hashing

- L'algoritmo restituisce una stringa di numeri e lettere (detto digest) a partire da un qualsiasi flusso di bit di qualsiasi dimensione finita.
- La stringa di output dell'algoritmo è univoca per ogni documento identificato. Pertanto, l'algoritmo di hashing è utilizzato per la firma digitale.
- La lunghezza del digest varia a seconda degli algoritmo utilizzato
- L'algoritmo non è invertibile, cioè non si può ricavare la sequenza di bit in ingresso a partire dal digest.

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.

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.

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.

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

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

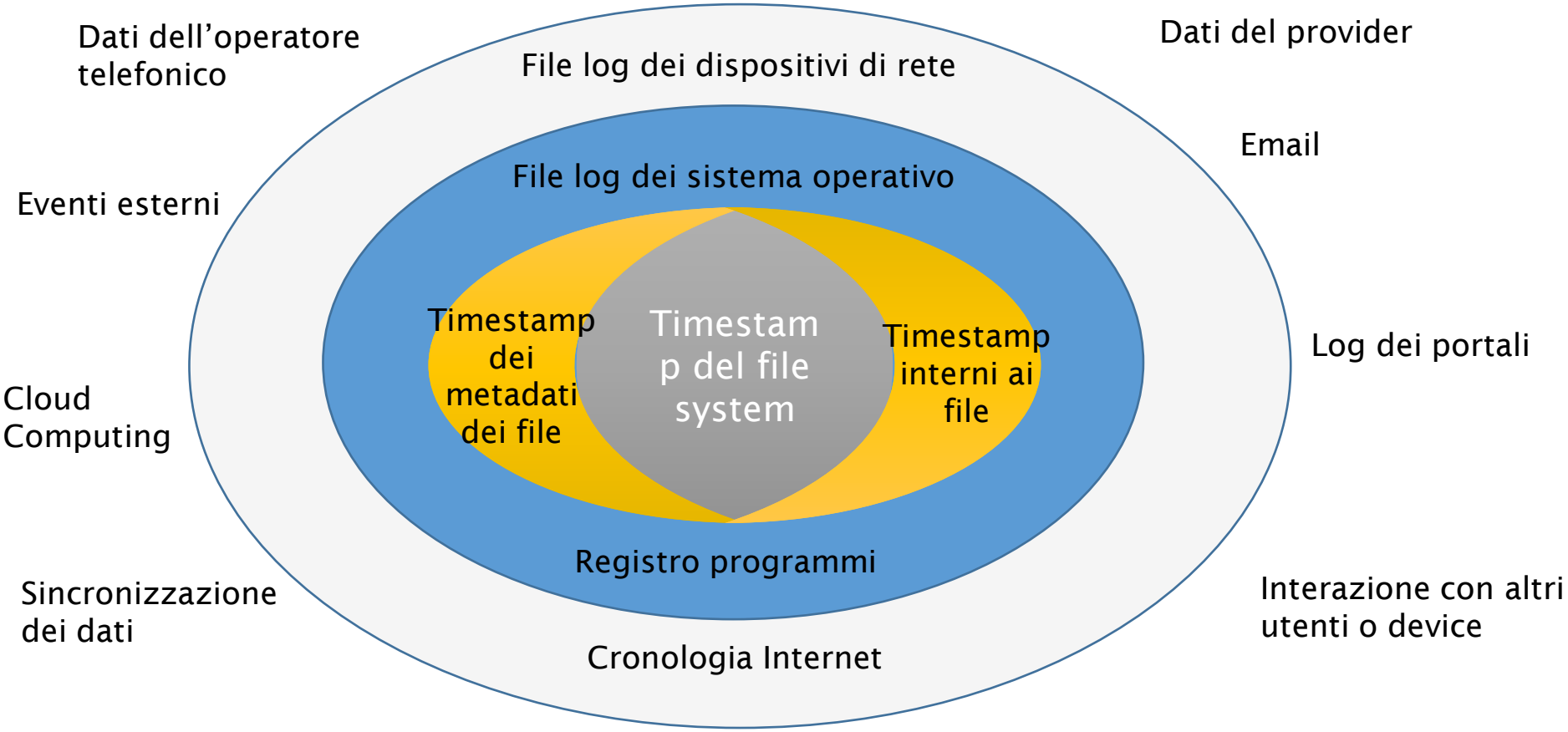
Analisi: Timeline

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

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
- Verifica dell'autore

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**.

Esercizio

Redazione di un report

INDAGINI ONLINE

Conclusioni

Note giuridiche

Quesiti

INDAGINI ONLINE

Quadro normativo: ispezioni

La **Legge 48 del 18/3/2008** *«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».

Contatti

info@vincenzocalabro.it

Linkedin vincenzocalabro

INDAGINI ONLINE