APPUNTI DIGITAL FORENSICS – SAMUELE CUCUZZA

LEZ_0 DIGITAL FORENSICS 2023/2024

DIGITAL FORENSICS VS COMPUTER SECURITY

- Cyber Sicurezza: Mantenere sicuri dei sistemi ed evotare attacchi informatici
- **Digital Forensics**: Ha il compito di capire cos'è successo quando la cyber Sicurezza fallisce.

LEGGE N°48 DEL 18 MARZO 2008

Ha introdotto dei **principi fondati della computer forensics** all' interno del nostro ordinamento giuridico, legato alla gestione delle **digital evidence**

Il legislatore non ha indicato le modalità di esecuzione da applicare ma si è focalizato su due aspetti:

- Corretta procedura di copia dei dati utili alle indagini
- Integrità e non alterabilità in sede di acquisizione

FORENSIC SCIENCE

Applicazione pratica della scienza alle questioni giuridiche. Utilizza **metodi scientifici** per ottenere fatti probatori (da evidenze fisiche, analogiche o digitali)

DEFINIZIONE DI DIGITAL FORENSICS

Utilizzo di metodi scientificamente derivati e provati per la conservazione, raccolta, convalida, identificazione, analisi, interpretazione, documentazione e presentazione delle prove digitali derivate da fonti digitali, al fine di agevolare o promuovere la ricostruzione degli eventi ritenuti criminali, o per anticipare azioni non autorizzate che si dimostrano dannose per le operazioni pianificate

TECNICHE DI TRATTAMENTO DEI REPERTI INFORMATICI

INFORMATICA FORENSE
É la disciplina avente ad oggetto lo studiio delle attivitá di **individuazione**, **conservazione, protezione, estrazione, documentazione** ed ogni altra forma di trattamento ed interpretazione del dato digitale memorizzato su un supporto informatico, al fine di essere valutoato come prova nel processo.

DATO DIGITALE = OGGETTO DI INDAGINE

DATI
Entitá di base su cui operano i sistemi informatici
Law enforcer: Autoritá procedenti che per le loro indagini si avvalgono di tali dati, che una volta acquisiti o analizzati possono produrre prove, contribuendo al proseguimento delle indagini

TIPOLOGIE DI REATO
- **Reati tradizionali o comuni**: Computer come strumento
- **Reati relativi a contenuti**: Distribuzione di materiale illegale o illecito
- **Reati di danneggiamento**: Distribuzione di virus

DATI INFORMATICI
Puó rendersi necessario nei procedimenti aventi oggetto:
- Reati informatici
- Reati commessi con l'ausilio di strumenti informatici
- Dati aventi valori di prova o indizio per reati informatici
- Strumenti di archiviazione di dati rilevanti

LIMITI DELL'INFORMATICA FORENSE
- Estrema facilitá di alterazione dei reperti
- Facile creazione ad arte di elementi probatori
- Difficile riconducibilitá dei reperti ai veri autori
- Necessitá di trovare risconti (in maniera quasi paranoica)

DIGITAL FORENSICS
Tecniche e strategie basate sulla intangibile e volatile natura dei dati digitali.
Vengono utilizzate tecniche **scientifiche** e **analitiche** alle reti di computer, a dispositivi digitali e ai file per scoprire o recuperare **evidenze digitali** ammissibili nel procedimento penale

La raccolta dei dati a volte pu; portare a malfunzionamenti tecnici, danneggiamenti o contraffazioni.

Best pratices: Insieme dei processi e delle tecniche utilizzate dall'esperto forense

EVIDENZE DIGITALI
L'esame delle evidenze digitali puó richiedere molto tempo, il **tecnico** dev'essere **accurato** e **cauto** a **raccogliere gli elementi di prova**

Solitamente la **copia primitiva**, "originale", intatta viene clonata e restituita alle loro applicazioni.

DATA TYPE
Gli elementi di prova digitale comprendono:
- Contenuto di una trasmissione
- Attributi o metadati dell'attivitá di comunicazione
- Diritto alla privacy degli utenti della rete
- Gestione di una risorsa informatica

Ogni dato ha il suo trattamento giuridico differente rispetto ad altri dati

LE CINQUE FASI DELLA DIGITAL FORENSICS
- Identificazione
- Acquisizione
- Analisi
- Valutazione
- Presentazione

IDENTIFICAZIONE
Fase cruciale della Digital Forensics, **Rilevare cosa é effettivamente utile per l'indagine**
Elenco di strumenti utili per l'indagine:
- Sistemi informatici
- Sistemi di comunicazione
- Supporti di memorizzazione
- Supporti non digitali e informazioni

La maggior parte degli elementi presenti in una scena del crimine possono essere utilizzati dall'indagatore se ne ritiene opportuno

ACQUISIZIONE
Duplicare le informazioni in maniera fedele all'originale
Esso puó avvenire attraverso:
- Cloni
- Immagini bit-a-bit
- Immagini bit-a-bit compresse

Obiettivi:
- Acquisire il maggior numero di dati
- Rendere l'attività di acquisizione ripetibile
- Limitare i tempi di inattivitá di server "importanti"

L'acquisizione deve essere:
- Completa
- Accurata
- Incontaminata

La parte lesa hanno il diritto ad avere accesso e controllare la fase di acquisizione degli elementi da analizzare.

Imaging: Tecnica per ottenere dati forense, effettua una immagine bit-stream di un dispositivo di memorizzazione digitale, non modificando i dati dal dispositivo di memorizzazione "originale"

MODALITÁ OPERATIVE
Insieme di operazioni che permettono di produrre dati forense:

- Vengono generate piú copie
  - **Master**, Una
  - **Lavoro**, Molte
- Imaging, consente di restituire i dispositivi originali al proprietario che cosí puó continuare nel suo lavoro su quella risorsa
- Le immagini sono ampiamente accettate nei tribunali come rappresentazione dei dispositivi originali

Devono essere messe in atto delle procedure per verificare l'autenticitá e l'integrità dei dati dopo il processo di acquisizione e la generazione di successive copie.

FUNZIONI HASH
Funzione non iniettiva che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. Tale risultato viene chiamato **Digest**. Le funzioni hash inoltre permettono di non risalire al contenuto iniziale, anche se ultimamente per alcune funzioni has sono state trovate delle vulnerabilitá.
Proprietá delle funzioni Hash:

- Resistenza alla preimmagine: Una stringa non produce un hash uguale ad un dato hash
- Resistenza alla seconda preimmagine: Due stringhe non hanno hash uguale
- Resistenza alle collisioni: Una coppia di stringhe non possono dare lo stesso hash

MD5
Algoritmo crittograico di hashing che prende in input una stringa di lughezza arbitraria e ne produce un output di 128bit.

Caratteristiche:

- Codifica molto veloce
- Output con il quale non é possibile ottenere con due diverse stringhe in input uno stesso valore hash in output
  Problema: MD5 molte volte produce stringhe che collidono, output con lo stesso valore hash

SHA
Famiglia di cinque diverse funzioni crittografiche di hash.
I componenti di questa famiglia sono:

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Le ultime quattro varianti sono spesso indicate genericamente come SHA-2, per distinguerle dal primo.

- Il primo produce un digest di soli 160bit
- Gli altri produconon digest di lunghezza pari al numero indicato nella loro sigla

ANALISI
Mettere in evidenza i dati con contenuto informativo importante per l'indagine.
Tale processo deve essere **Documentato Dettagliatamente.**
L'analisi va eseguita su una copia, bit-a-bit, e deve essere **riproducibile**.

VALUTAZIONE
Interpretare i dati evidenziati in fase di analisi per sostenere le proprie tesi.
Nella valutazione bisogna sempre esplicitamente esporre i margini di sicurezza dei dati elaborati.

PRESENTAZIONE
Interpretare i dati evidenziati in fase di analisi per sostenere le proprie tesi.
Nella presentazione bisogna documentare:

- Cos'é stato fatto
- Come é stato fatto
- Cosa é emerso
- Che significato hanno i dati emersi

La presentazione deve essere adattata all'interlocutore.
Le conclusioni non possono essere diverse dalle conclusioni dell'analisi facendone cenno all'ultimo

DISPOSITIVI DI MEMORIZZAZIONE
La memorizzazione nei dispositivi digitali avviene a diversi livelli:

- Livello Fisico (Particelle magnetiche, incisioni laser)
- Livello Logico (Dispositivi, tracce e settori)

Le modalitá con cui un dispositivo gestisce i dati a livello logico ha implicazioni dirette su qualunque analisi forense.

I diversi file system utilizzano lo spazio sui dispositivi di memorizzazione in maniera dissimile l'uno dall'altro. Quindi **per ogni file system esistono tecniche d'analisi dei dati differenti**

CANCELLAZIONE DEI DATI
Forme di cancellazione dei dati:

- **Effettuata da un applicazione standard:** Rimuove solo **l'indirizzo dell'informazione** associata ad ogni blocco di dati. I dati restano fin quando non vengono sovrascritti.
- **Wiping:** Tramite un software di wiping é possibile **sovrascrivere/cancellare ogni dato** nel dispositivo di memorizzazione.

ES. Un software di wiping puó **impostare ogni bit del dispositivo di memorizzazione a 0** facendo si che i file del dispositivo vengano eliminati

SLACK SPACE
Area, compresa tra l'ultimo bit e la fine del settore, non utilizzata dal file che ha allocato lo spazio

INTRO IMAGE AND VIDEO FORENSICS

FORENSICS IMAGE/VIDEO ANALYSIS

É l'applicazione della scienza dell'immagine e del dominio della perizia per interpretare il contenuto di un'immagine o l'immagine stessa in questioni legali.

La Image/Video Forensics ha il compito di studiare le immagini e trarre conclusioni inerenti ad esse.

IMAGE/VIDEO FORENSICS IN PRATICE

Sul piano pratico le operazioni che vengono effettuate sono:

- **Enhancement**, Miglioramento dell'immagine/video
- **Restoration**, Restauro dell'immagine

Omografie: Trasformazioni opportune delle immagini

Per quanto riguarda il piano investigativo abbiamo due rame importanti che si legano alla Multimedia Forensics:

- **Source identification**, Identificazione della sorgente
- **Integrity/Authenticity**, Garantire l'integrità e l'autenticitá

AUTHENTICITY VS INTEGRITY

Concetto chiave: L'**Autenticitá** non é l'**Integritá**:

- **Autenticitá**: Accurata rappresentazione dell'evento originale
- **Integritá**: Informazione inalterata dalla cattura alla deposizione finale

CASO SPECIALE: FILE ORIGINALE

A volte per studiare un immagine il tecnico forense deve:

- **Recapture**: Ricatturare, Creare un falso e quindi scattare una foto con la fotocamera con la quale si crede che sia stata scattata la fotografia
- **Staging**: Creato ,Il file dell'immagine é autentico, ma il contenuto é stato modificato

In questi casi anche l'autenticitá della foto non implica l'autenticitá del contenuto

CAPIRE QUANDO É POSSIBILE OTTENERE QUALCOSA

Il successo di un miglioramento delle immagini dipende da due fattori:

- **Obiettivo principale**
- **Dettagli Tecnici Correlati**
  - Risoluzione dell'area d'interesse
  - Livello di compressione
  - Presenza della sfocatura/focus
  - Numero di frame disponibili
  - Rumore/Luminositá e contrasto

É importante capire quale difetti sono presenti in ordina da applicare i tool specifici.

ES. Se ho un immagine compressa e sfocata devo eseguire quest'ordine:

1. Algoritmo di **DeCompression** (Decomprimere l'immagine/video)
2. Algoritmo di **DeFocusing** (Rimozione del focus)

Nel 90% dei casi se un immagine é sfocata non si puó fare nulla.

MOTION-BLUR
Svocatura presente in un video/immagine causata dal movimento di un oggetto.
Il **motion-blur** puó essere risolto, estrapolando alcuni dettagli, solo se l'oggetto in questione si muove in una singola direzione

ES. Una macchina che prosegue in una **singola direzione**, se presenta **motion-blur** é possibile **estrapolare la sua targa** utilizzando una **sorta di media lungo il suo presunto spostamento**.
La **qualitá non é ottima** ma potrebbe risalire ad alcuni dettagli chiave per l'indagine
Puó essere risolto con un filtro Deconvolutivo, utilizzandolo nell'immagine sfocata.

SUPER RESOLUTION
Permette di migliorare la risoluzione dell'immagine.
Avviene nelle alte frequenze e permette di aumentare notevolmente la risoluzione dell'immagine.
A volte viene usato un dataset allenato con altri volti permette di elaborare degli algoritmi AI per ricostruire il volto.

CORREZIONE PROSPETTICA
I pixel vengono ridisegnati mediante un opportuna trasformazione geometrica.

L'AI É BANDITA , **PER ALCUNI**, nell'**AMBITO SCIENTIFICO** perché ritenuta non affidabile

IMPLICAZIONI IN AMBITO FORENSE
Il **dato digitale**, per sua natura, é molto sensibile a manipolazioni.
Possibili problematiche legate a quest'aspetto:

- Differenza tra Miglioramento e Manipolazione
- Quali elaborazioni sono ammissibili
- **Digital Forgery**

Principi generali delle indagini sulle immagini sono:

- **Preservazione dell'originale**, lavorando su copie
- **Acquisizione integra e non ripudiabile**
- **Utilizzo di copie di lavoro**
- **Documentazione e ripetibilitá**

Miglioramento del contrasto: Allontano i toni di grigi vicini in maniera tale che l'occhio percepisca maggiormente il contrasto tra essi.

PRINCIPI E LINEE GUIDA REDAZIONE

LA CONSULENZA TECNICA

PRINCIPI GENERALI (1)
Elementi essenziali:

- **Estremi del procedimento** (e ruoli)
- **Testo del quesito**
- **Premesse tecniche**
- **Dati di lavoro**
- **Metodologia di lavoro**

PRINCIPI GENERALI (2)
OBIETTIVO: Rispondere al quesito «Tecnico»

Elementi essenziali:

- **Analisi tecnica**: Analizzare il materiale trovato
- **Conclusioni**: Risultato delle analisi, a volte possiamo dare solo informazione e non risultati
- **Allegati tecnici**:
  - Documenti
  - Dati
  - Risultati Parziali
  - Hash degli allegati (Garantire integritá)
    - Per ogni allegato si genera un hash e inserito in relazione
    - Ogni hash viene inserito all'interno di un file excel e nella relazione viene inserito l'hash del file excel
- **Referenze bibliografiche alle «Best Pratice» di settore**

ALLEGATI DI UNA CONSULENZA TECNICA
Alcuni allegati fondamentali:

- **CV** del consulente tecnico
- **Contenuti digitali allegati**
  - CD, HD o memoria di massa compresi di hashcode
- **Copia in formato pdf della relazione**

FORMA DELLA CONSULENZA TECNICA
Forma, stile e linguaggio utilizzato devono essere adeguati agli «attori» coinvolti, senza cadere nel tecnicismo ma senza omettere dettagli importanti.
Devono essere ben evidenti le fasi di:

- Identificazione
- Acquisizione
- Conservazione
- Analisi
- Valutazione

La **presentazione** dei risultati é fondamentale

PRESENTAZIONE
É importante stirare un discorso che riassuma, pagina per pagina, la relazione.
La puntuale contraddizione fa fede a ció che viene detto in aula e la controparte potrebbe approfittarne.
Ogni cosa che accade in un processo viene trasritta e registrata.

Trucco del mestiere: Leggere le conclusioni in maniera tale da non scordare nula ed essere il piú preciso possibile.

Trucco del mestiere: Se la consulenza tecnica prevede delle figure queste devono essere citate nel dettaglio e talvolta mostrate in aula.

Una volta conclusa la presentazione il **CT** viene **interrogato** o dalla **controparte** o dal **giudice** e potrebbero cercare di metterlo in difficoltà.

La **relazione del CT** viene **esaminata** dal **tecnico** o **legale** della **controparte**:
- Essi potrebbero **contrapporsi** alle **conclusioni** dell'**analisi forense** sia dal punto di vista **tecnico** che **legale**

CARATTERISTICHE DELLA PRESENTAZIONE
La **presentazione** dovrebbe essere:
- **Semplice**
- **Chiara**
- **Completa**
- **Professionale**

Condivisibile perché **Completa, Professionale** e **Documentata**

ALTRI ASPETTI
Altri aspetti fondamentali della consulenza tecnica sono:
- **Tempistica**:
  - Concordata con il giudice
  - Con una scadenza prefissata senza possibilitàdi posticipazione
- **Retribuzione:**
  - A vacazione, tempo di periodo per il quale il CT lavora
    - Nel privato, la retribuzione viene concordata
    - Nel pubblico, grande problema, viene retribuito a ore, circa 5€/h

CONTENUTI DI UNA CONSULENZA TECNICA
La consulenza tecnica é composta da due parti:

- **Parte Epigrafica**
- **Parte Narrativa**

PARTE EPIGRAFICA
Vengono **indicati** gli **estremi del procedimento**, **i quesiti**, **riassunti sulle posizioni delle parti** relativamente a quegli **aspetti** che sono attinenti **all'oggetto della consulenza**.

PARTE NARRATIVA
Parte in cui deve essere riportato lo svolgimento delle operazioni peritali e riasunte eventuali osservazioni, obiezioni o istanze mosse dalle parti o dai rispettivi consulenti.
L'obbligo di inserire gli interventi della controparte é contemplato nell'**ART. 195 c.p.c**

ARTICOLO 195 c.p.c
Prevede che **nella relazione, il consulente, "inserisce anche le osservazioni e le istanze delle parti"**
Pur essendo obbligatorio peró la S.C ha comunque sancito che **la mancata indicazione** nella relazione **delle istanze delle parti e dei loro consulenti** o **l'omissa verbalizzazione delle operazioni peritali**, **non comportano la nullitá** della consulenza tecnica

PARTE DESCRITTIVA
In essa **il CT mette in rilievo** il **materiale** e la **documentazione utilizzata** ai fini della consulenza **esponendo i fatti sui qualli ha basato il proprio convincimento** e dunque **elaborato le risposte ai quesiti**.

PARTE VALUTATIVA
In questa parte della consulenza il **CT esprime il proprio giudizio**:

- **Ricostruendo** e **Motivando** la fattispecie che é stato chiamato ad accertare e valutare
- **Esponendo** in modo **Analiltico** il risultato della propria indagine

PARTE CONCLUSIVA
Si tratta della **Parte Finale** della consulenza nella quale il **CT Riassume** il **lavoro svolto**, **Fornendo risposte** specifiche e concise ai **quesiti**

DIRITTI E DOVERI DEL CT

PUNTI GENERALI
Quando un CT viene chiamato deve esporre e giurare di dire la veritá come testimone

ACCOMPAGNAMENTO COATTIVO
ART. 133 c.p.p
«Se il testimone, perito, la persona sottoposta all'esame del perito diversa dall'imputato, il consulente tecnico, l'interprete o custode di cose sequestrate regolarmente citati o convocati, omettono senza un leggittimo impedimento di comparire nel luogo, giorno e ora stabiliti, il giudice puó ordinare l'accompagnamento coattivo e puó altresí condannarli, con ordinanza, al pagamento di una somma da euro 51 a euro 516 a favore della cassa delle ammende nonché alle spese alle quali la mancata comparizione ha dato causa»
Quindi in sostanza **Obbliga la presenza di chiunque manchi all'appello in tribunale**

FALSA PERIZIA
ART 373 c.p.p.
«Il perito o l'interprete, che, nominato dall'autorità giudiziaria, dà parere o interpretazioni mendaci, o afferma fatti non conformi al vero, soggiace alle pene stabilite nel articolo 372 c.p. in merito alla falsa testimonianza»
Non si può dichiarare falsa perizia, ovvero falsa testimonianza

FRODE PROCESSUALE
ART 375 c.p.p
«Chiunque, nel corso di un procedimento civile o amministrativo, al fine di trarre in inganno il giudice in un atto d'ispezione o di esperimento giudiziale, ovvero il perito nella esecuzione di una perizia, immuta artificiosamente lo stato dei luoghi o delle cose o delle persone, è punito, qualora il fatto non sia preveduto come reato da una particolare disposizione di legge, con la reclusione da uno a cinque anni.»
Distruggere un reperto potrebbe portare a frode processuale. Avviene di più in fase di analisi.
La **frode proccessuale** si configura quando **qualcuno altera artificiosamente lo stato, luoghi, cose o persone** durante un **procedimento civile o amministrativo**, con l'intento di **ingannare un giudice o un perito.**

FRODE IN PROCESSO PENALE
ART 375 c.p.p
«Salvo che il fatto costituisca più grave reato, è punito con la reclusione da tre a otto anni il pubblico ufficiale o l'incaricato di pubblico servizio che, al fine di impedire, ostacolare o sviare un'indagine o un processo penale:
- **a) immuta artificiosamente il corpo del reato ovvero lo stato dei luoghi, delle cose o delle persone connessi al reato;**
- **b) richiesto dall'autorità giudiziaria o dalla polizia giudiziaria di fornire informazioni in un procedimento penale, afferma il falso o nega il vero, ovvero tace, in tutto o in parte, ciò che sa intorno ai fatti sui quali viene sentito.»**

La **frode in processo penale** si configura quando **qualcuno altera artificiosamente lo stato, luoghi, cose o persone** durante un **procedimento penale**, con l'intento di **ingannare un giudice o un perito.**

LA PERQUISIZIONE INFORMATICA TECNICHE, NORME E MODALITÀ OPERATIVE

LA PERQUISIZIONE INFORMATICA TECNICHE, NORME E MODALITÀ OPERATIVE

PERQUISIZIONE ART 247 c.p.p
Mezzo di ricerca della prova **a sorpresa** volto al ritraccio del corpo del reato o di cose pertinenti al reato che una volta rinvenute dovranno essere sottoposte a sequestro.

TIPOLOGIE DI PERQUISIZIONE
- **Personale**
- **Locale**

PERQUISIZIONE PERSONALE
Disposta quando vi é un fondato motivo di ritenere che **taluno occulti sulla persona il corpo del reato o cose pertinenti al reato**.
Cose pertinenti al reato: Cose che hanno la funzione di provare il reato

Modalitá di perquisizione:
- Consegna di una copia del decreto all'interessato con avviso della facoltá di farsi assistire da persona di fiducia. Nel rispetto della dignitá

PERQUISIZIONE LOCALE
Disposta quando vi é un fondato motivo che **il corpo del reato o cose pertinenti al reato si trovino in un determinato luogo** o che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso

Modalità di perquisizione:
- Consegna di una copia del decreto all'imputato e a chi abbia disponibilitá del luogo con l'avviso della facoltá di farsi rappresentare o assistere da persona di fiducia
- Il decreto puó specificare pure che le persone presenti in quel luogo siano perquisite

PERQUISIZIONE INFORMATICA
Approfondimento forense che viene sempre piú **richiesto dall'autorità giudiziaria**, é sempre piú **utilizata per individuare, acquisire e preservare le informazioni**. Ordinata dal magistrato per trovare il corpo del reato.
ES. Cyber Crime che fa uso di dati/informazioni illegali all'interno di una rete

Modalitá di lavoro:
- I consulenti isolano i sistemi dalla rete approfondendo ogni aspetto dei sistemi all'interno.

Componenti che effettuano la perquisizione informatica:
- Ufficiali di polizia giudiziaria
- Consulenti tecnici
- Ausiliari esperti della Digital Forensics

LEGGE N. 48 DEL 18 MARZO 2008 SULLA PERQUISIZIONE INFORMATICA
Rappresenta **le norme e le best pratices da seguire per l'acquisizione della fonte di prova**, in particolare del **dato informatico**, introducendo la **Digital Forensics** all'interno del nostro ordinamento, prevedendo imporanti aspetti legati quegli elementi di prova data la loro natura **fragile** e **volatile**.

Il legislatore in questa legge:
- **Non specifica le modalitá di esecuzione**
- Focalizza l'attezione su due concetti:
  - **Corretta procedura di copia dei dati**
  - **Integritá e non alterabilitá in sede di acquisizione**

STRUMENTI DEL MESTIERE
Il CTF (Consulente Tecnico Forese) deve essere pronto con la strumentazione opportuna, e soprattutto **deve essere pronto ad effettuare delle copie forense dei dati**.

Copia forense: Copia dei dati nel quale si garandisce l'integrità e l'identitá alle condizioni in cui si trovava al momento del prelievo consentendo successive verifiche o accertamenti tecnici

Possibile kit di strumenti del CTF:
- **Numerosi HardDisk**: **Di diverse dimensioni** preferibilmente, **per effettuare la duplice copia dei dati**
- **Duplicatori Forense**: Permettono di **effettuare copie forense di memorie** quali hard disk, pendrive USB e memorie di massa (ES. Lodicube, Tableau TD1, TD2u, TD3, ecc.)
- **Write blocker hardware e software**: Permettono di **bloccare in scrittura le memorie collegate** al pc
- **Distribuzioni linux**: Su pendrive USB da avviare in locale (ES. Kali, Caine, Deft e Parrot security)
- **Suite per acquisire dati da dispositivi mobile**: Permettono di acquisire dati dai dispositivi mobile o anche navigatori satellitari (ES. Cellebrite UFED e Oxygen Forensics)
- **Software per acquisire dati presenti su servizi cloud**: Permettono di acquisire dati presenti su servizi cloud (ES. Cellebrite UFED Cloud Analyzer, Axiom Cloud, Elcomsoft Phone Breaker)
- **Tool per effettuare il download delle email**: Permettono di scaricare le email (ES. Securecube Imap Downloader e Thunderbird Portable)
- **Suite di software portatili**: Permettono di facilitare le fasi di acquisizione (ES. FTK imager Portable, Hash My Files)
- **Kit di cacciaviti, pinsette e strumentazione**: Per smontare e rimontare dispositivi

ES. In una perquisizione in azienda le abitazioni dei singoli individui vengono perquisite all'alba tutte nello stesso orario per evitare che qualcuno possa iniziare le proprie attivitá

OPERAZIONI NECESSARIE PER UNA PERQUISIZIONE
La prima operazione svolta dalle autoritá é quella di **esibire il Decreto Di Perquisizione**, che autorizza le operazioni, nel frattempo viene data la possibilitá al perquisito di **Nominare un Avvocato o Consulente Tecnico di parte** o di farsi **Assistere da una persona di Fiducia.**

FASE OPERATIVA
Dopo le formalitá la perquisizione puó iniziare:

- Individuazione ed isolamento dei **sistemi informatici**
- Individuazione ed isolamento **di account online**
- Richiesta di **credenziali di accesso, codici di blocco, PIN e password** e cambio delle stesse
- Richiesta della presenza di **dati cifrati e relativa password di decifratura**
- Perquisizione di tutti i locali e **sequestro del materiale di interesse**

Una volta conclusa perquisizione in abitazione si prosegue con la perquisizione in azienda:

- **Isolano i locali** dell'azienda **allontanando il personale o collaboratori**
- Acquisire e **sequestrare i dispositivi informatici**
- Richiesta l'assistenza **di un tecnico interno** per agevolare il lavoro

Ogni singolo elemento **va isolato dalla rete attivando la modalità aereo.**
Durante le operazioni é necessario da parte dell'**indagato mantenere la calma, risultare disponibile e collaborare con le forze dell'ordine** per **diminuire i tempi ed evitare il sequestro dei supporti informatici**.

Una volta **acquisiti i dati ed effettuate le copie forense**, si stipula **il verbale** andando a **dettagliare le operazioni effettuate e i valori di HASH** che certificano l'attivitá forense.

RUOLO DEL CONSULENTE INFORMATICO FORENSE (CFT)
Routine tipica del CTF durante il processo di perquisizione:

- Luogo di intervento, solitamente **la polizia giudiziaria non comunica preventivamente l'indirizzo e il target esatto** al fine di **non compromettere l'operazione ed evitare inutili resbonsabilitá al CTF**
- Una volta riuniti gli attori, si effettua un **debrifing** (Veloce punto della situazione), **quantificando la mole di dati da acquisire e la tipologia di reato**
- **Accesso ai locali**, Le forze dell'ordine **mostrano il decreto**
- **Ricerca dei dati e delle evidenze di interesse**
- **Isolamento dei dispositivi informatici dalla rete**
- **Perquisizione effettiva dei supporti informatici**
- Assicurarsi che le **copie siano copie forense**

ISPEZIONI ART 244 c.p.p
Mezzo di ricerca delle prove, **non a sorpresa**, volto al ritraccio del corpo del reato o di cose pertinenti al reato che una volta rinvenute dovranno essere sottoposte a sequestro.
Se necessario, non obbligatorio, puó essere svolta con l'impiego di poteri coercitivi, polizia giudiziaria.

TIPOLOGIE DI ISPEZIONE
- **Personale**
- **Luoghi o Cose**

ISPEZIONE PERSONALE
Eseguita nel rispetto nella dignitá e del pudore, ha come oggetto il corpo di un essere umano vivente o parti di esso. Prima di procedere con l'ispezione é necessario che l'interessato sia avvenuto dalla facoltá di farsi assistere da una persona di fiducia

ISPEZIONE DI LUOGHI O COSE
Durante l'esecuzione l'imputato o la persona che ha la disponibilitá del luogo hanno diritto ad avere una copia del decreto che ha autorizzato l'atto. L'autoritá giudiziaria puó ordinare che taluno non si allontani.

ISPEZIONE INFORMATICA
Mezzo di ricerca della prova, **modalitá** con il quale **il soggetto competente ispeziona dei supporti informatici per consentire all'autoritá giudiziaria di verificare e acquisire direttamente o indirettamente le prove** in formato digitale necessarie **per procedere con l'indagine**.

REALIZZARE UN ISPEZIONE INFORMATICA
Effettuata **durante le indagini preliminali**, ad opera della **polizia o** dal **pubblico ministero**, oppure **durante il dibattimento** ad opera **del giudice**. Puó essere **ordinata dal pubblico ministero** con **decreto motivato la cui copia va consegnata solo nel caso di ispezione relativa a luoghi o cose**.

PASSAGGI CHIAVE PER UNA BUONA ISPEZIONE INFORMATICA
- Ispezione dei sistemi informatici, permettendo al soggetto di assistere all'ispezione
- Al termine dell'ispezione, stipulare un verbale nel quale vengono scritti nel dettaglio le attivitá svolte e le operazioni:
  - **Dettagli dei dispositivi ispezionati**, ES. Notebook, smarthphone ecc.
  - **Strumenti tecnici adottati per ecitare alterazioni**, ES. Write Blocker, modello ecc.
  - **Dettagli sulle operazioni svolte**, ES."Sono stati aperti i file immagini" ecc.
  - **Esito dell'ispezione informatica**, ES. "É emerso che …" ecc.

MODALITÁ DELL'ISPEZIONE INFORMATICA
- **Post/Mortem**: A sistema spento, collegando il supporto di memoria ad appositi strumenti che evitino le alterazioni
- **Live**: A sistema giá rivvenuto acceso all'atto dell'intervento della Polizia Giudiziaria, si opera riducendo al minimo le alterazioni

ALIBI INFORMATICO_DIGITALFORENSICS

ALIBI INFORMATICO

ALIBI
Rappresenta l' "**altro luogo**" in cui si trovava l'indiziato nello stesso arco temporale in cui veniva commesso un delitto.
Indica la **non presenza** dell'indiziato sul luogo del delitto quindi esclude la sua partecipazione.
Il soggetto, tramite il suo alibi, é costretto a dimostrare che al momento della commissione del reato si trovava in un luogo diverso rispetto al luogo del reato.

Alibi di ferro: Alibi talmente solido che il giudice deve emettere sentenza di assoluzione "per non aver commesso il reato". L'alibi di ferro permette all'imputato di assolvere ogni accusa al 100%

In un processo:
- Solo l'accusa deve dimostrare puntualmente tutti i suoi assunti percorsi **Oltre ogni ragionevole dubbio**
- Per la difesa é sufficiente che le stesse siano ragionevoli e coerenti e tali da impedire all'accusa il raggiungimento del cosí detto **punto di certezza.**

Luoghi dell'alibi:
- **Senso Letterale**
- **Senso Figuraivo**

Bisogna anche dimostrare una doppia proposizione:
- **Negativa**: In pratica il **non essere in quel luogo**
- **Positiva**: In pratica il **perché si é in altro luogo**

Ci possono essere delle evidenze digitali che dimostrano che quel soggetto si trovasse in un determinato luogo (ES. Il gps dei dispositivi mobili o dei navigatori satellitari)

Possibili luoghi per un alibi:
- **Luoghi Fisici**: Luoghi fisici, tangibili, dov'é avvenuto un delitto. ES. Scena di un omicidio
- **Luoghi Virtuali**: Luoghi interamente informatici dove avvengono degli illeciti. ES. Una rete o il web

Alibi come scelta difensiva:
- **Assenza di alibi non implica colpevolezza**
- **Fallimento dell'alibi**, l'alibi non viene riconosciuto come attendibile

FALSO ALIBI
Alibi costruito a doc per **ingannare chi sta effettuando l'indagine**, preordinato, mendace. Esso **provoca conseguenze se dimostrato**, soprattutto in fase di condanna (FALSA TESTIMONIANZA)

ESEMPI DI PROCEDUE OPERATIVE
Sono presenti due fasi:

- **Fase 1:** Dichiarazione di quanto ricorda l'indagato
- **Fase 2**: Ricerca di ulteriori informazioni a sostegno dell'alibi

Il processo si sposta nel dominio della **credibilitá** che riguarda come le persone accertano e valutano l'alibi:

- **Valutazione**: Svolta nella fase preliminare delle indagini da chiunque ne abbia necessitá
- **Finalizzazione:** Alibi rimesso al dibattito e alla decisione del giudice. **In questa fase si ricostruirá quanto studiato nelle fasi precedenti e si verificherá la consistenza dell'alibi.** Non tutti gli alibi arrivano a questa fase.

VERIFICA DI UN ALIBI
La **verifica di un alibi** avviene con uno schema da **otto domande**:

- **Cinque riguardano l'oggetto**
  - Chi?
  - Cosa?
  - Quando?
  - Dove?
  - Perché?
- **Tre riguardano il soggetto agente**
  - Quanto?
  - In che modo?
  - Con quali mezzi?

Un **CTF difficilmente riesce a dare risposta a tutte le domande**, ma tentare **aiuta a rappresentare un evidenza digitale in maniera completa.**

ALIBI INFORMATICO
Esistono due classi di aibi informatici:

- **Generati**: Durante, o **Contemporaneamente**, l'evento criminoso
- **Creati**: In un momento diverso, **Antecedente** o **Seguente**, dell'atto delittuoso

CONTEMPORANEITÁ
Le tracce informatiche sono prodotte nello stesso istante in cui si consuma il reato
Distinguiamo quattro specie:

- L'imputato **genera tracce informatiche sui dispositivi distanti dalla scena del crimine**
- Un **sistema informatizzato ha eseguito automaticamente azioni che producono tracce informatiche e simulano la presenza dell'imputato in un luogo diverso dalla scena del crimine**
- Una **terza persona**, o sistema automatizzato, **ha registrato tracce** che potrebbero giustificare **la presenza dell'imputato in luoghi diversi dalla scena del crimine**.
- **Un complice ha eseguito azioni per nome e per conto dell'imputato che producono tracce al di fuori della scena del crimine.**

Nell'ultima categoria possiamo distinguere altre due specie:

- L'imputato o chi per lui realizza una proca ex novo, facendo attenzione agli elementi caratterizzanti il tempo rivelino la contemporaneitá con l'azione crimine
- L'imputato o chi per lui riutilizza una traccia informatica giá esistente alterando gli elementi utili a dimostrare la correlazione temporale tra il momento della produzione e l'evento criminoso

IPOTESI DI FALSI ALIBI

A. L’imputato ha generato direttamente tracc informatiche a distanza
B. Un sistema automatizzato ha simulato un utilizzo in presenza
C. Un complice, persona o sistema automatizzato, ha registrato tracce informatiche
D. Un complice ha eseguito azioni per conto dell’indiziato
E. L’indiziato realizza una prova ex novo
F. L’indirizzato riutilizza una traccia informatica giá esistente

SITI WEB E POSTA ELETTRONICA – DIGITALFORENSICS2024

ACQUISIZIONE E TRATTAMENTO DATI INFORMATICI IN RETE

DIFFAMAZIONE IN RETE ART 595 COMMA 3° COD. PEN.
Offesa recata con mezzo della stampa o qualsiasi altro mezzo si pubblicitá verrá punita con reclusione dai sei mesi ai tre anni o alla multa non inferiore ai cinquecentosedici euro.
In sostanza Qualsiasi offesa recata nel web, o con ogni tipo di media, verrá punita con il carcere, da 6 mesi a 3 anni, o con una multa, non inferiore ai 516€

Fondamentili ipotesi di limiti a tutela della persona umana:
- **Limite dell'onore**
- **Limite della riservatezza**
- **Limite dell'identitá personale**
- **Limite della reputazione**

REQUISITI DEL REATO DI DIFFAMAZIONE
- **Assenza dell'offeso**: L'offeso dovrá essere assente, altrimenti entra in gioco il reato di ingiuria
- **Offesa all'altrui reputazione**: La persona diffamata non dev'essere indicata nominativamente ma **individuabile con certezza**. L'offeso puó essere individuato per **esclusione o in via deduttiva**
- **Comunicazione a piú persone**: Non sussisiste il reato di diffamazione nella lesione della reputazione comunicata ad una persona solamente. Ma il messaggio offensivo, su internet per esempio, puó essere scritto in un sito che tutti potrebbero visitare

DIFFAMAZIONE IN RETE
La Diffamazione via web o tramite piattaforma social é diventata una pratica diffusa.

DIFFAMAZIONE ATTRAVERSO SOCIAL
La diffamazione con **Facebook** come mezzo ha due generali ipotesi:
- **Pubblicazione su pagine personali**: Bisogna avere il consenso dell'offensore per poter accedere ai contenuti
- **Pubblicazione di post, commenti o altro**: Basterebbe pubblicare un post diffamatorio in una pagina pubblica per poter commettere il reato di diffamazione

PRESUPPOSTI PER LA DIFFAMAZIONE SOCIAL
I presupposti per la diffamazione con mezzo Facebook sono:
A. La precisa individualitá del destinatario delle manifestazioni ingiuriose
B. La comunicazione con piú persone alla luce del carattere pubblico dello spazio virtuale e la possibile sua incontrollata diffusione.
C. La coscienza e volontá di usare espressioni oggettivamente idonee a recare offesa al decoro, onore e reputazione del soggetto passivo.

PARERE DELLA CASSAZIONE SULLA DIFFAMAZIONE SOCIAL
La **Cassazione ha riconosciuto che il reato di diffamazione possa essere commesso a mezzo internet.** Configurando la propagazione del reato tramite **Facebook.**
Il **Legislatore si é interessato alla pubblicazione e alla diffusione di essa**, sia i gruppi che in bacheca

CERTIFICARE LA DIFFAMAZIONE SOCIAL
Fasi per la raccolta delle prove informatiche inerenti alla diffamazione:

- **Acquisizione delle prove informatiche**
- **Certificazione dell'integritá delle prove**
- **Stesura di una relazione tecnica**

Queste tre fasi **se effettuate nel modo corretto** possono permettere al **diffamato** di effettuare una **querela**

Una raccolta non corretta puó:

- **Evitare al diffamatore di essere identificato**
- **Permettere al diffamatore di cancellare le prove prima che si arrivi in fase di giudizio**
- **Consentire al diffamatore di attribuire ad altri l'azione di diffamazione**

PUNIBILITÁ DEL REATO DI DIFFAMAZIONE
La diffamazione in Rete é punibile a seguito di querela della parte offesa che diventa piú efficace **se riporta anche una consulenza tecnica dell'avvenuta diffamazione e l'acquisizione forense certificata del contenuto diffamatorio**, che diventerá **prova nel processo**.

La consulenza finalizzata a documentare tramite prove informatiche la diffamazione avvenuta in rete puó effettuata tramite **ricerche OSINT**. Spesso peró i gruppi o pagine diffamatorie vengono chiuse per complicare le indagini

Ricerche OSINT: Disciplina dell'intelligence che si occupa della ricerca, raccolta e analisi d'interesse tratte da fonti aperte e pubbliche, anche non indicizzate.

ACQUISIZIONE (ARTIGIANALE)
Le **Stampe** o **Screenshot difficilmente vengono ammesse in Tribunale come prova perché non garantiscono l'integritá**. Anche la fotografia allo schermo del PC non ha alcun valore come prova in tribunale data la sua **facile contestazione dalla controparte**

ACQUISIZIONE TRAMITE NOTAIO
La stampa della prova dell'avvenuta diffamazione certificata da un Notaio o da un Pubblico Ufficiale é certamente un'alternativa migliore ma puó non essere sufficiente a identificare il proprietario del media diffamatorio. Servirebbe estrapolare dal media l'identificativo del proprietario per rendere tutto ció piú concreto

TROVARE ID DI UN PROFILO FACEBOOK
Per trovare l'identificativo di un profilo o gruppo Facebook bisogna:

- **Copiare l'URL**
- **Andare sul sito "findmyfbid.com"**
- **Cliccare su "Find numeric ID"**

Una volta eseguite queste semplici istruzioni possiamo ricopiare o stampare il numero identificativo del profilo che permetterá di ritrovare il profilo anche in caso di cambio nome o URL.
La raccolta delle prove per uso legale in caso di diffamazione du Facebook con l'ID del profilo o della pagina é molto piú efficace.
Lo stesso procedimento puó essere fatto con i Post e i Commenti peró cliccando la data della pubblicazione.

OSINT
Attivitá di raccolta d'informazioni mediante la consultazione di fonti di pubblico accesso.
Si distingue dalla normale ricerca perché applica un processo di gestione delle informazioni con lo scopo di creare una specifica conoscenza in supporto di una specifica decisione di un individuo o gruppo.

FONTI DI OSINT
- **Mezzi di comunicazione**: Giornali, riviste, televisioni, radio e siti web
- **Dati Pubblici**: Rapporti dei governi, piani finanziari, dati demografici, dibattiti legislativi, conferenze stampa, discorsi, avvisi aeronautici e marittimi
- **Osservazioni Dirette**: Fotografie di piloti amatoriali, ascolto di conversazioni radio e osservazione di fotografie satellitari
- **Professionisti e Studiosi**: Conferenze, simposi, lezioni universitarie, associazioni professionali e pubblicazioni scientifiche

ACQUISIZIONE/CRISTALLIZZAZIONE PAGINE WEB
Per premunirsi delle prove digitali in caso di cancellazione é necessario iniziare la fase di **cristallizzazione** utilizzando il software gratuito **FAW (Forensics Acquisition of Websites).**
Oltre a FAW esistono ulteriori tool online che permettono di scaricare una **copia autentica** di pagine a patto che siano pubblici:
- **Perma.cc**
- **Archive.is**

ACQUISIZIONE: PROBLEMATICHE TECNICHE
L'acquisizione forense con cristallizzazione della prova online su internet per tutelare i propri diritti puó incluedere:
- **File robots.txt**
- **Certificati SSL**
- **Sitemap**
- **Metadati RSS**
- **Documenti presenti sul sito**
- **Filmato dell'acquisizione forense**
- **Eventuali codici di errore**
- **Indirizzi IP**
- **Record DN**
- **Dump del traffico di rete**
- **Chiavi SSL**

PERMA.CC
Caratteristiche di perma.cc:
- **Dieci acquisizioni gratuite al mese**
- **Possibilitá di acquisire una pagina creando una copia privata**

ARCHIVE.IS
Caratteristiche di archive.is:
- **Nessuna registrazione richiesta**
- **Qualunque cosa acquisita verrá pubblicata su internet**

Il problema piú grosso é che le pagine salvate non possono essere rese private e quindi rintracciabili sempre e da chiunque

FAW: FORENSICS ACQUISITION OF WEBSITES
Copia in maniera **Forense** pagine web con garanzie sull'**Originalitá del dato acquisito**

ISTRUZIONI BASE PER L'UTILIZZO
Dopo aver raggiunto la pagina web da copiare in modo forense:

- **Premere "Set Capture Area"**, Verrá bloccata la navigazione e i relativi controlli con possibilitá di regolare l'Altezza dell'area desiderata, chiamata **GOLDBOX**
- **Premere tasto "Acquire"**, Inizierá ad acquisire:
  - Pagina web
  - Headers
  - Codice HTML (di tutta la pagina)
  - Oggetti in pagina (se selezionati dal menú Configuration)
- **Si aprirá una cartella con tutti i file all'interno:**
  - **Acquisition.log**, File che contiene l'elenco delle operazioni eseguite da FAW
  - **Acquisition.txt**, File di testo che contiene i riferimenti dell'acquisizione
  - **Acquisition.xml**, File in formato .xml che contiene tutti i riferimenti per lo standard DFXML
  - **Checking.faw**, File che contiene un codice di controllo che permette di verificare se i file Acquisition.txt e Acquisition.xml non sono alterati
  - **Code.htm**, Codice HTML della pagina
  - **CodeFrame{nomeframe}.htm**, File che contengono il codice frame{nomeframe} se presente
  - **Headers.txt**, File di testo che contiene gli headers inviati al browser della pagina
  - **Hosts**, Copia del file hosts di Windows al memento dell'acquisizione della pagina
  - **image.png**, Immagine della pagina delimitata dalla **GoldBox**
  - **image{numero}.png**, Sono i file immagine con i ritafli dell'immagine completa della pagina web acquisita con aspect ratio 1,41, **adatte per stampa A4**
  - **SystemLogEvents.txt**, File in cui vengono registrati tutti glil eventi di windows avvenuti durante l'acquisizione della pagina Web
  - **screenCapture.wmv**, File video acquisito da VLC con la cattura dell'intero schermo del PC dall'inizio dell'acquisizione fino alla fine
  - **Wireshark_{macaddressnetworkinterface}.pcap**, file acquisito da WireShark con il traffico di rete avvenuto durante l'acquisizione della pagina web
  - **CartellaObjects**, Cartella che contiene tutti gli elementi della pagina web
- **Fasi finali**, Per rendere l'acquisizione della pagina web valida ai fini legali si puó:
  - Firmare digitalmente uno dei seguenti file con apposita **Marca Temporale**:
    - **Acquisition.txt**
    - **Acquisition.xml**

MARCA TEMPORALE
Tecniche per la **generazione, apposizione e verifica della validazione temporale dei documenti informatici**, mediante generazione e applicazione di una **Marca temporale**
Componenti della marca temporale:

- **Identificativo dell'emittente**
- **Numero di serie**
- **Algoritmo di sottoscrizione**
- **Identificativo del certificato relativo alla chiave di verifica**
- **Riferimento temporale della generazione**
- **Identificativo della funzione di hash utilizzata per generare la fingerprint**
- **Valore della fingerprint dell'evidenza informatica**

SOCIAL NETWORK E POSTA ELETTRONICA

SOCIAL NETWORK

Si identifica un servizio informatico online che permette la realizzazione di reti sociali virtuali.
Siti internet che consentono agli utenti di condividere contenuti testuali, immagini, video e audio tra loro.

ESEMPI DI SOCIAL NETWORK

- **Instagram**
- **Facebook**
- **X**
- **TikTok**

POSTA ELETTRONICA

Chiamato anche servizio **email** (Electronic Mail) consente ad ogni utente che abbia accesso ad un computer connesso ad internet di inviare messaggi ad un qualsiasi utente che disponga di un indirizzo di posta elettronica

SERVIZIO DI POSTA ELETTRONICA
Caratteristiche del servizio di posta elettronica:

- **Comunicazione Asincrona**, Messaggi recapitati in appositi server
- **Verifica dell'invio del messaggio**, Tramite server é possibile saperlo
- **Connessione internet**, Al solo fine di inviare o visualizzare messaggi
- **Velocitá d'utilizzo**, Servizio molto veloce

FORMATO DELL'INDIRIZZO DI POSTA ELETTRONICA
Forma di un indirizzo email:

- **utente@indirizzo**

@: Chiocciola, normalmente letto come "AT", identifica l'utente in maniera univoca all'interno del server che lo ospita.

SISTEMI DI POSTA ELETTRONICA
Ogni ISP permettono agli utenti di aprirsi una propria casella di posta elettronica.
La posta elettronica é consultabile:

- **WEBMAIL**, sito internet
- **Programma client**

Composti da altrettanti componenti:

- **Client**: Programmi che consentono la consultazione della posta elettronica
- **Server**: Spostamento dei messaggi dall'origine alla destinazione
- **SMTP**: Protocollo per l'invio e la ricezione delle email
- **POP3 e IMAP**: Ricezione e consultazione dei messaggi

SMTP TRAMITE TELNET
Servizio di posta elettronica senza accedere all'account di terzi.
Permetteva di creare una connessione con l'email server e scrivere direttamente i comandi relativi a mittente e destinatario e i parametri aggiuntivi per creare il corpo

DISTINZIONE TRA INVOLUCRO E CONTENUTO
Involucro: Incapsula il messaggio e contiene tutte le **informazioni necessarie per il trasporto dei messaggi** (indirizzi, prioritá e livello di protezione). **Viene utilizzato per l'instradamento dei messaggi**

Contenuto: **Messaggio all'interno dell'involucro**, composto da due parti:
- **Header**, Intestazione del messaggio
- **Corpo**, Contenuto effettivo del messaggio

PROTOCOLLI
Vari protocolli di intestazione:
- **To**: Indirizzi destinatari
- **Cc**: Indirizzi destinatari secondari
- **Bcc**: Indirizzi per le copie per conoscenza nascoste
- **From**: Persona che ha creato il messaggio
- **Sender**: Indirizzo di posta elettronica del mittente
- **Received**: Riga aggiunta da ogni agente di trasporto lungo il percorso
- **Return-Path**: Identificare un percorso di ritorno al mittente

STANDARD MIME
Permette di aggiungere alla psota elettronica qualsiasi documento

EMAIL: ANALISI FORENSE
L'esperto forense puó estrapolare informazioni chiave, per un indagine.
Molte volte le email sono fraudolente e possono contenere:
- **Pishing**
- **Malware**

Il mittente puó essere rintracciato dall'**header** ma non é sempre veritiera.

TOOLS: EMAIL TRACKER
Effettua un'operazione di analisi massiva delle mail.
Estrae gli header e fornisce informazioni, elenco di indirizzi e di server dov'e transitata la mail.

EMAIL: AUTENTICAZIONE MITTENTE
Problema comune: Identificare il mittente di una mail
Senza un sistema particolare non é possibile capirlo, anche avendo l'indirizzo.

DKIM
Stabilisce che i gestori di un determinato dominio **firmatario** abbiano applicato una **firma digitale** certificando il contenuto e le intestazioni del messaggio.
Se la firma risulta valida si puó dire che la mail é **certificata** dal dominio che ha apposto la firma.
DKIM garantisce solo che la mail é stata inviata dal dominio firmatario.

FAKE EMAIL
Per creare una email fake bisogna avere:
- **File di testo**
- **Specificare i campi d'interesse**
- **Salvarlo come .eml**

I client leggono questo file come una mail vera e propria

FAKE EMAIL: ANALISI
L’analisi identifica dei mittenti dei messaggi, destinatari, date e orari di invio.
In assenza del **DKIM** non possiamo certificare l’autenticitá dei messaggi ne tanto meno il reale invio degli stessi.
Non si puó stabilire che i file presenti siano autentici o inviati realmente ai destinatari indicati

ANONYMOUS EMAIL
Esistono sistemi che permettono di inviare email in totale anonimato
ES. anonymousemail.me

ANONYMOUS EMAIL: YOPMAIL
Nato per contrastare le email spam generando indirizzi email monouso.
Le email inviate alla casella di posta vengono eliminate in otto giorni

VALORE GIURIDICO DELLE MAIL
Un messaggio di posta elettronica puó essere usato come prova in un processo.
La normativa Italiana concede margine di manovra al giudice.
Il giudice puó considerare una mail come **prova**, ma esistono diverse varienti da prendere in considerazione

NORMATIVA L.N 59/199
Riconoscimento regolamentazione della validitá dei documenti formati o trasmessi con strumenti informatici.

L’email puó essere considerata nella **categoria dei cd. Documenti informatici**
Definita dall’**Art. 1, 1° comma, lett. P** come **rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti**

ORIENTAMENTI CONTRAPPOSTI
- **Non favorevole alla mail come prova**: Non si riesca da un punto di vista informatico a risalire ad una **Paterintá certa**
- **Favorevole alla mail come prova**: Valore effettivo come prova

ARTICOLO 2712 C.C
Le mail vengono giudicate come prove atipiche e possono essere usate come prova se il mittente non le disconosce

ARTICOLO 20 COMMA 1-BIS
L’email é un documento informatico sottoscritto con dirma elettronica semplice paragonabile con i documenti in forma scritta.

ARTICOLO 21 COMMA 1
Il documento informatico sul piano probatorio é liberamente valutabile in giudizio.

POSTA ELETTRONICA CERTIFICATA: PEC
Posta elettronica **non ripudiabile** che garantisce:

- **Integritá del messaggio**
- **Certificazione di invio**
- **Certificazione di consegnata**

La **PEC equivale alla,** forma digitale della **raccomandata con ricevuta di ritorno**
La PEC deve essere acquistata e i server hanno l'obbligo di conservare per 30 mesi tutto ció che si é inviato e ricevuto.
Per essere realmente fuzionale la PEC dovrebbe essere utilizzata sia dal mittente che dal destinatario

Vantaggi della PEC:

- **Mittente garantito**
- **Destinatario non ripubiabilitá**

CIRCOLARE 1 2018 GDF DIGITAL FORENSICS 2021

MANUALE OPERATIVO GDF 2018 (GUARDIA DI FINANZA)

MANUALE OPERATIVO
Questo documento specifica cose e come un tecnico forense deve agire nel suo lavoro, composto in Quattro Volumi.

VOLUMI DEL MANUALE

- **VOLUME I**:
  - **PARTE I**: Azione della GDF a contrasto dell'evasione e delle frodi fiscali
  - **PARTE II**: L'attivitá della polizia giudiziaria a contrasto dell'evasioni e frodi fiscali
- **VOLUME II**:
  - **PARTE III**: Esecuzione delle verifiche e dei controlli
  - **PARTE IV**: Valorizzazione delle informazioni acquisite nell'ambito delle attivitá investigative
- **VOLUME III**:
  - **PARTE V**: Principali metodologie di controllo
- **VOLUME IV**:
  - **PARTE VI**: Modulistica e documentazione di supporto

PRIMO VOLUME
Il primo volume individua per la prima volta anche la qualifica del **CDFDA**
CDFDA: Consulente Digital Forensics e Data Analysis, tecnico che agisce sul campo

SECONDO VOLUME
Il secondo volume dettaglia **le modalitá con il quale deve avvenire la ricerca e l'estrazione di documenti informatici nel corso dell'accesso** (copia bit-a-bit). **Fornisce le specifiche di cos'é una Copia Forense**

CASI DELLE ACQUISIZIONI

- **Acquisizione del dato in se**
- **Acquisizione del contenitore del dato**

ACQUISIZIONE DEL DATO
Permettono di cristallizzare l'evidenza acquisita

ACQUISIZIONE DEL CONTENUTO DEL DATO
Concetto di **Bitstream image** o **Copia forense**.

POSSIBILI MODIFICHE
Alla legge 48, la **copia forense** verrá un pó **limitata ai cesi indispensabili.**
Spesso si rischia di acquisire troppe informazioni anche quelle inutili al caso.

Attenzione principale alla parte in cui si cerca di far capire che **l'acquisizione é una parte importante e delicata della prassi di un tecnico forense**.

Nel caso di **Acquisizione d'immagini forense dei dispositivi** bisogna fare attenzione anche al **formato specifico** nel quale si fa la copia ed induce al tecnico a **non danneggiare in nessun modo i file,** nella **posta elettronica non bisogna limitarsi a stampare la mail ma bisogna anche salvare il file, garantire l'integrità**

CHAIN OF CUSTODY
Documento che accompagna l'evidenza, permette di verificare le operazioni svolte dai militari e di essere eventualmente replicate.

COMPONENTI DELLA CHAIN OF CUSTODY
- **Nominativi dei militari operanti**
- **Sede del contribuente e la data**
- **Nominativi del personale tecnico**
- **Evidenze Digitali acquisite**
- **Tipologie di evidenze digitali**
- **Impronta hash di ciascuna evidenza e la funzione di calcolo utilizzata**
- **Passaggi di consegna dell'evidenza digitale**
- **Luogo dove vengono custoditi le evidenze, digitali e non**

COSA CERCARE IN UN EVIDENZA
- **Back-up**
- **Artefatti**
- **Log applicativi**
- **Software personalizzati**

CLOUD
Luogo remoto dove vengono collezionati i file di un determinato soggetto sotto una compagnia di servizi cloud.
La parte della forense che si occupa di questa parte é molto delicata.

COME PROCEDERE
La procedura principale é **identificare la posizione del dato.**

IDENTIFICAZIONE DELLA POSIZIONE
Necessaria quando si dovesse procedere all'**acquisizione forense delle evidenze digitali** presenti nell'area remota

L'**indicazione** che fornisce il documento dulle **modalità di accesso al cloud** e **acquisizione forense** é piú di **rilevanza giuridica**, che tecnica

POSSIBILI CASI
Il verificato ha due scelte:
- **Collaborare**: Fornendo l'accesso ai dati, si procede **cristallizzando** l'evidenza spontaneamente consegnata dalla parte
- **Non collaborare**: Due modalità operative:
  - Utilizzo delle sue credenziali per accedere all'area remota
  - Utilizzo dei dispositivi del verificato per effettuare l'accesso all'area remota

CONSIGLIO UTILE
É buona prassi **registrare dei filmati che documentino l'acquisizione dei dati,** anche se giá effettuata in modo forense.

Se i dati contengono **dati sensibili di soggetti terzi** bisogna preventivamente **riflettere se cancellarli o meno**

INVESTIGARE SU IMMAGINI E VIDEO

INVESTIGARE SU IMMAGINI

IMAGE/VIDEO FORENSICS
Si occupa di analizzare immagini e video in maniera forense.
L'analisi di un immagine digitale **comprende** anche **dare contesto e spigazione di cosa accade nell'immagine**.

MULTIMEDIA FORENSICS
Analizza tutti i file multimediali in modo forense

PRICIPI FONDAMENTALI
- **Idenficazione della sorgente**
- **Verifica dell'integritá e delle interferenze**

Fornisce metodologie per identificare la sorgente e verificarne l'integrità
Tutto ció che abbiamo visto nella **Digital Forensics** si applica anche alla **Multimedia Forensics**

PROCEDURE DA ESEGUIRE
- **Preservare**, l'immagine originale
- **Documentare**, tutti i passi dell'elaborazione
- **Riproducibilitá**, delle azioni eseguite durante il processo documentato

ELEMENTI DELLE IMMAGINI
Alcuni elementi che possiamo notare nelle immagini sono:
- **Colore**: Colori che compongono l'immagine
- **Moviemnto**: Movimenti di oggetti
- **Profonditá**: La terza dimensione viene persa

Nelle Immagini potremmo avere pochissime evidenze
Un'immagine é una prova schiacciante rispetto ad un testo

TECNICHE DI HALFTONING
Tecniche per rappresentare i toni di grigio, composta da **cinque livelli di grigio.**
Sostituita con un tecnica da **quindici livelli di grigio**

AMPED FIVE E AMPED AUTHENTICATE
Amped Authenticate: Permette di verificare se un immagine è integra
Amped Five: Permette di analizzare immagini, migliorarle.

Entrambi i software vengono utilizzati perché forniscono User-Friendly semplice e consentono di effettuare il report finale, dove specifica ogni singolo passaggio effettuato in quel determinato file multimediale, fornisce anche l'hash del file stesso.

IMMAGINI DIGITALI
Funzione 2D f(x,y) che rappresenta una misura opportuna di una o piú caratteristiche (luminositá, colore, ecc.) di una data scena
Le comunicazione visuale é la forma piú immediata ed efficace di comunicazione.

DEFINIZIONE FORMALE
Un'immagine digitale monocromatica é una matrice I=f(x,y) di valori discreti di intensitá luminosa (livelli di grigio), costruita da M*N pixel, ciascuno dei quali ha valore appartenente all'intervallo [0,L-1], dove L sono i livelli possibili di intensitá (di grigio)
Le operazioni che possono essere fatte sulle immagini solo le stesse operazioni per le matrici matematiche.

PIXEL: Elemento dell'immagine

RISOLUZIONE SPAZIALE
Si riferisce al numero specifico di pixel di un immagine

COLORI
Esistono piú spazi di colori, uno dei piú famosi é **RGB**

COLORI RBG
Spazio di colori composto solamente da tre variabili**:**
- **R**: Rosso
- **G**: Verde
- **B**: Blue

Ogni colore che vediamo in un immagine é una combinazione di queste tre variabili

AGIRE SUL CONTRASTO
É possibile migliorare l'aspetto di un immagine attraverso l'utilizzo delle cosiddette look-up tables

MIGLIORAMENTO DEL CONTRASTO
L'immagine di output avrá un contrasto maggiore visto che i valori di grigio piú piccoli di m vengono resi piú scuri mentre quelli piú grandi vengono resi piú chiari

LUT: LOOK-UP TABLE
Permettono di implementare operazioni puntuali anche di tipo non banale sulle immagini

FILTRAGGI CONVOLUTIVI
Modificano i valori di Colore, trasparenza, ecc. di un pixel in base a un calcolo nell'intorno locale.
Si utilizzano le Kernel-Mask convolutive i cui valori (Pesi) definiscono il comportamento del filtro
ES. Sampling, Media Locale

INTORNO LOCALE
Area circostante di un singolo pixel. É possibile applicare una funzione che restituisca un valore in funzione del suo intorno
ES. Media 3x3

FILTRAGGIO SPAZIALE
Meccanismo simile alla convoluzione, esso é un intera famiglia di filtri
ES. Filtro di Smoothing

OPERATORI E MASCHERE
- **N-Box**: **Filtro di media**, calcola la media dei pixel all'interno di una finestra di dimensione NxN, **utilizzato per la sfocatura e il filtraggio del rumore**
- **N-Binomiale**: Simile al filtro media, **Utilizza un kernel binomiale anziché uno uniforme**. Utilizzato per la **sfocatura e la riduzione del rumore**
- **Sobel x,y**: **Rilevano i bordi in un immagine**. Fornisce una **Stima del Gradiente dell'immagine**
- **Laplaciano**: Calcola la seconda derivata dell'immagine, utilizzato per i cambio di concavitá nell'immagine
- **Edge Enhancing**: **Enfatizza i bordi dell'immagine**, Ottenuto tramite la **sottrazione dell'immagine con la stessa sfocata**
- **Shifting**: **Sposta l'intera immagine in una specifica direzione.** Utilizzato per **Allineare immagini o pre creare effetti di movimento**
- **Noise Reduction**: **Riduce il rumore nell'immagine,** Filtri come il **Filtro mediana o il Filtro Bilaterale**
- **Unsharm Masking**: **Tecnica di miglioramento dell'immagine che enfatizza i dettagli.** C

INTERPOLAZIONE
Operazione di ingrandimento di un immagine, Stima nuovi dati sulla base delle informazioni giá esistenti.
Problema: Puó creare artefatti o dettagli inesistenti nell'immagine originale o nella scena riprodotta

FORMATI DI UN IMMAGINE
Formati di immagini compresse e non:
- BMP
- GIF
- PNG
- JPEG
- Raw

La maggior parte delle immagini in circolazione é in **JPEG**

INVESTIGARE SU VIDEO DIGITALI

VIDEO DIGITALI
Sequenza di immagini statiche che vengono visualizzate in frequenza.

Un video puó essere inteso come:

- **Segnale Discreto**:
  - Come campionamento temporale della scena
  - Ad ogni istante del video é una **fotografia**
- **Sequenza Video**:
  - Succesione di istantanee
  - **Fotogrammi (Frame)**

ALGORITMI DI CODIFICA E DECODIFICA
Per poter lavorare con i video inanzitutto dobbiamo capire cosa sia uno standard video.
Standard Video: Come vengono visualizzati e memorizzati i video
Questi standard non riguradano solo la **codifica/decodifica** di un video ma anche dei **Protocolli** necessari al loro trasferimento.
Nonostante ci siano degli standard pubblici, nella pratica esistono tanti coder/encoder/decoder proprietari, ovvero degli **standard proprietari**.
Standard Proprietario: Standard ideato da chi produce un dispositivo di visualizzazione o memorizzazione che non é banalmente leggibile da qualsiasi dispositivo

RISOLUZIONE SPAZIALE
La risoluzione spaziale si riferisce al numero specifico di punnti di informazione di un’immagine.
Si riferisce al numero totale di pixel in quel frame/immagine.

RISOLUZIONE TEMPORALE
La risoluzione temporale si riferisce alla frequenza delle immagini, anche detta Frame Rate, ed é il numeor di immagini per unitá di tempo che vengono visualizzate.
In pratica si riferisce agli FPS, frame per secondo, che un video permette di visualizzare o nel quale viene acquisito.
Una sequenza di immagini si puó definire video se ha al piú 10 FPS.

STANDARD VIDEO

- **PAL**: 25 FPS
- **CINEMA**: 24 FPS
- **SECAM**: 25 FPS
- **NTSC**: 29,97 FPS

DIFFERENZA TRA FPS IN ACQUISIZIONE ED FPS DI CODIFICA
Scenario dove un dispositivo:

- **Acquisisce** a 10 FPS
- **Codifica** a 25 FPS

Cosa succede nella pratica in fase di **Codifica**:

- Avviene una **Duplicazione dei Frame**, vengono inseriti dei Frame clone uno dopo l'altro per rendere il video da 10 FPS un video a 25 FPS

Problemi per i CTF (Consulenti Tecnici Forensi):

- Nel calcolo sulle velocitá di determinati veicoli, se non teniamo conto dei frame duplicati potremo andare in contro a calcoli errati

Alcuni tool hanno la possibilitá di eliminare i frame Duplicati e identici, confrontando il frame precedente con il successivo pixel per pixel.

ASPECT RATIO
Rapporto tra le due dimenzioni dell'immagine, orizzontale e verticale
Indicato in diversi modi:

- **Frazione**: x:y o x/y
- **Risultato**: 1,3
- **Proporzione all'unitá**: 1,3:1

L'aspect ratio é diverso in base al campo di utilizzo
ES. il cinema avrá un aspect ratio diverso dalla televisione.

ASPECT RATIO 4:3
Formato standard televisivo, sempre meno frequente con l'avvento dei DVD e dei nuovi televisori digitali

ASPECT RATIO 16:9
Caratterizzati da diensioni orizzontali piú ampie del 4:3, con proporzioni panoramiche tipiche dello schermo Cinematografico. Esistono molte varianti di esso.

TECNICHE DI ADATTAMENTO DELLO ASPECT RATIO
Inserimento di barre laterali o superiori che permettono di adattare un video in formato 4:3 ad un dispositivo 16:9 e viceversa.
Nomenclature tecniche:

- **Latterbox**: 16:9 → 4:3
- **Pillarbox**: 4:3 → 16:9
- **Windowbox**: a:b → c:d
- **Pan&Scan**: 16:9 → 4:3
- **Tilt&Scan**: 4:3 → 16:9

LETTERBOX
Permette di visualizzare il 16:9 su schermi 4:3.
L'immagine viene scalata fino a farlo rientrare nello schermo con l'aggiunta di due bande nere orizzontali.

PILLARBOX E WINDOWBOX
Permettono di visualizzare il 4:3 su un dispositivo 16:9.
In particolare **WindowBox** permette di visualizzare un ipotetico a:b in un c:d con l'aggiunta di quattro bande nere in tutti i lati dell'immagine

PAN&SCAN E TILT&SCAN
Pan&Scan:
- Permette di vedere il 16:9 su schermi 4:3
- Immagine ritagliata a sinistra e a destra

Tilt&Scan:
- Permette di vedere il 4:3 su schermi 16:9
- Immagine ritagliata in alto e in basso

RISOLUZIONE MP MEGA PIXEL
Unitá di misura che equivale ad **un milione di pixel.** Non corrispondono esattamente ai pixel di un immagine.
Il numero di MP **non é** indice di qualitá delle macchine fotografiche. Influisce molto anche il potere risolutivo del sistema ottico.

Calcolo dei MP di un dispositivo:
(Risoluzione massima orizzontale * Risoluzione massima verticale)/1.000.000

Quando noi acquisiamo con un dispositivo acquisiamo solo una matrice e non le tre matrici RGB.
Un unico sensore cattura un pó dei colori che interpolati formano l'immagine.

Pochi dispositivi di acquisizione fotografica hanno tre sensori, e di solito sono quelle professionali

RISOLUZIONI DEI FORMATI VIDEO
Non siamo molto liberi sulla scelta della risoluzione video:
- **DVD**: 720x480
- **HDTV**: 1280x720
- **FULLHD**: 1920x1080
- **4K**: 3840x2160
- **8K**: 7680x4320
- **16K**: 15360x8640

RISOLUZIONI DEI FORMATI
Aspect Ratio 16:9 ha quattro tipi di Risoluzione:
- **Half Resolution**: 940x540 pixel
- **HD Ready**: 1280x720 pixel
- **1080i**: 1920x1080 pixel (Frame interlacciato)
- **Full HD**: 1920x1080 pixel

Frame Interlacciato: Tipologia di Frame nel mondo analogico, che permetteva di interlacciare due frame segnando prima le righe di un frame e poi le righe di un altro, tutto ció avveniva nei tempi t e t+1

INTERLACING

- Immagine divisa in parti pari o dispari.
- Si alternano i Field per metá tempo rispetto agli FPS
- Su un monitor si notano artefatti invece in un televisore no

SISTEMI DI SCANSIONE INTERLACCIAMENTO

Pro:

- **Paritá di larghezza di banda si puó dimezzare la banda del segnale**
  - Si raddoppia la frequenza di visualizzazione
- **Riduzione dello sfarfallio nei monitor CRT**

Contro:

- **Rinuncia a metá delle informazioni**
  - Possibile comparsa di artefatti dovuti a interpolazioni
  - Artefatti pesanti se sono presenti soggetti in rapido movimento

COMPRESSIONE VIDEO

CODEC video é un software composto da due parti:

- **Encoder**: Comprime la sequenza di immagini archiviandola in un file. Parte piú pesante
- **Decoder**: Decomprime la sequenza per poterla nuovamente visualizzare. Parte piú leggera

Queste due operazioni non sono sempre simmetriche.

Nelle immagini dal punto di vista delle operazioni e complessitá computazionale in Code e Decode sono simmetiche/identiche, trattasi di operazioni inverse

Nei video abbiamo un Encoder che effettua la maggior parte delle operazioni in una sequenza di immagini, come le operazioni di compressione, eliminazioni di frame duplicati, ecc.
In fase di Decoder prende ció che l'encoder ha processato e lo visualizza.

LOSSLESS/LOSSY

Anche le tecniche di compressione video possono essere suddivise in:

- **Lossless**: Compressione é un processo perfettamente reversivile che avviene senza perdita di informazioni
- **Lossy**: Compressione non é reversibile nelle quali il video compresso e quello decompresso non sono piú effettivamente identici in quanto al momento della compressione si sono perse delle informazioni, volutamente perdute ritenute sacrificabili.

VIDEO

Comprimere un video vuol dire comprimere un gruppo di **N-Fotogrammi**, in sostanza compressione delle immagini.

Operazione effettuabile nelle immagini/video:

- Lavorare nello spazio colore Luminanza/Crominanza:
  - Colori
  - Intensitá di grigi

Quando applivo la conversione video inizialmente la applico ad una matrice della luminanza e il restante nella parte della crominanza. Abbiamo meno informazioni rispetto alle immagini.

COMPRESSIONE DI UN VIDEO
Si sfruttano:
- Stesse idee di fonso della compressione delle immagini
- Ritondanza Spaziale e Temporale (Frame vicini si somigliano, [iú alti sono gli FPS piú si somigliano)

Sfruttando la **Ritondanza Spaziale**:
- Intraframe, mantengono per ogni fotogramma solo informazioni importanti, pixel vicini si somigliano e vengono codificati con meno bit

Sfruttando la **Ritondanza Temporale**:
- Intraframe nel tempo, Fotogrammi successivi sono simili, possiamo cambiare le informazioni che cambiano nel tempo

Sfruttanfo **Peculiaritá del sistema Visivo Umano**:
- L'occhio umano non percepisce le piccole differenze temporali.

A volte piccole strutture in movimento vengono compresse in modo forte.
A volte per un CTF é un problema perché se gli servissero quelle informazioni piccole, compresse fortemente, non avremo mai modo di averle perfette.

BLOCK MATCHING
Esplicita l'idea di rendere uniforme il moto di pixel vicini:
- Frame partizionato in blocchi non sovrapposti
- Un vettore di moto per ogni blocco

Ogni fotogramma viene suddiviso in blocchi, e si cerca di capire ogni blocco come si muove nel tempo.

FORMATI DI CODIFICA
Le strategie di codifica possono essere diverse.
Formato: Sorta di scatola che contiene il codec e lo integra con il sistema
Codec: Software che dice al computer con quali operazioni matematiche deve manipolare le immagini per comprimerle e quali eseguire per visualizzare quelle compresse.

Elenco dei principali formati:
- .avi
- .mpeg, .mpeg2, mpeg4
- .hdv

AMPED ha creato un tool per aprire i file del formato nei DVR.
Hanno aperto un fascicolo World Wide per la standardizzazione di tutti i formati video, Progetto fallito in partenza per colpa dei pochi contribuenti e dei molti standard proprietari.

MOTO ESTIMATION
L'encoder individua tra i fotogrammi adiacenti (in uno dei due, prima o dopo) il blocco piú simile (se non uguale).
Se una figura si sposta, possiamo applicare il moto e vedere se la stima (x,y) sia corretta o errata.
Si tratta di un **Algoritmo Veloce che approssima il moto con un approssimazione non precisissima** ma di grande aiuto.
L'immagine viene suddivisa in tanti blocchi e si controlla dove i blocchi interessati siano andati a finire nei fotogrammi adiacenti (uno dei due). Alla fine di questo algoritmo si viene a creare una Matrice degli errori.
Matrice degli errori: Matrice che evidenzia gli errori di questo algoritmo

FRAMES I/P/B NELLO STANDARD MPEG
- **I Frame**: Frame video completamente indipendenti
- **P Frame**: Si basa su un precedente frame. Dipendente da I
- **B Frame**: Costituito da informazioni ricavate sia da **I Frame** che **P Frame** (anche successivi) attraverso **Interpolazione.** Dipendente sia da I che da P

INTRAFRAMES (I-FRAMES)
Sono fotogrammi che vengono **codificati utilizzano le informazioni contenute nel fotogramma stesso** e non contengono nessun riferimento o informazione sui fotogrammi adiacenti
- Compressi da una singola immafine allo stesso modo di quando un'immagine viene salvata in formato JPEG
- Nessun tipo di Compressione Temporale
- Puó essere Generato da un encoder per creare un punto di accesso casuale
  - Consente ad un decoder di avviare la decodifica in maniera corretta
- Richiedono piú Bit per essere codificati
- Sono usati come riferimento per la decodifica di altre immagini
- Vengono inseriti dal CODEC ogni qualvolta c'é un cambiamento repentino tra due immagini successive

P-FRAMES
Sono fotogrammi che vengono **codificati utilizzando le informazioni acquisite in base al fotogramma che lo precede, sia di tipo I che di tipo P**
- Ogni macroblocco di 16x16 pixel di un P-Frame **puó essere codificato in modo indipendente** oppure **compensato**, bilanciato utilizzando informazioni del fotogramma precedente
- **Utilizzando le somiglianze tra fotogrammi successivi risultano essere piú piccoli dei corrispondenti I-Frame**

Esso puó contenere:
- dati del fotogramma
- Spostamenti rispetto al fotogramma da cui dipende
  - Contiene le informazioni della posizione (X', Y'), ovvero coordinate (X,Y) del fotogramma precedente al tempo t+1 (**Motion Estimation**)
- Una combinazione dei due
  - Svantaggio in fase di decodifica, é necessario ricostruire ciascun fotogramma P prima di poterlo visualizzare

B-FRAMES
Fotogrammi che vengono **decodificati richiedendo la precedente codifica di altri frames** prima di essere decodificato

- Sono di tipo Bidirezionale, fanno riferimento a ció che li segue e che li precede

Puó contenere:

- Dati del fotogramma
- Spostamenti rispetto al forogramma da cui dipende
- Una combinazione dei due

Caratteristiche:

- La ricerca del moto (Motion Estimation) é effettuata sui due fotogrammi, il successivo e il precedente, Codifica e decodifica piú complesse
- Inserire informazioni che si riferiscono ad un fotogramma successivo é possibile solo **alterando l'ordine in cui i fotogrammi vengono archiviati all'interno del file videok compresso**
- Richiedono meno bit per la codifica rispetto agli altri frame

PRINCIPALI PROBLEMATICHE DI IMMAGINI E VIDEO

- Compressione eccessiva (Sistemi vecchi o marine su hardware, lenti scarse, memorie ridotte)
  - Creazione di artefatti
- Sistemi a basso costo
- Ottiche e sensori di bassa qualitá
- Mancanza di luminante

ECCESSIVA COMPRESSIONE
Si vengono a formare **artefatti molto evidenti**.
Essi sono un problema perchàe potrebbero compromettere la qualità di un'immagine

BASSA CAPACITÁ DI ELABORAZIONE DEI SISTEMI
Algoritmi ci Codifica e Decodifica di bassa qualitá

- **Rumore e artifatti** visibili nell'immagine
- Esposizione di **bassa qualitá dell'immagine**, **mancanca di contrasto**
- Qualitá del colore bassa, **problemi del bilanciamento dei colori**

PICCOLA OTTICA E GRANDANGOLARE
Dimostrano un alta sensibilitá al rumore, come il **Sale e Pepe o Impulsivo**

DISTORSIONE GEOMETRICA

- Alto livello di **sfocatura**
- Alto livello di **distorsione**
- Alto livello di **vignetting**

Vignetting: Zone periferiche dell'immagine con luminositá piú bassa, si compensa con la manipolazione dell'immagine

MANCANZA DI FLASH E ESPOSIZIONE PROLUNGATA

- **Moving Blur**, Effetto movimento
- **Interferenze su lufi florescenti**

TOOL DELLA IMAGE FORENSICS
Tipologie di programmi ed esempi:

- **General Purpose**
  - Photoshop
- **High/level**
  - Matlab
  - OpenCV library
- **Forensics Software**

TOOLS UTILIZZABILI DA TUTTI
Visualizzatori:

- ACDSee
- Irfanview
- Faststone viewer
- Xniew

Editor:

- Adobe Photoshop
- The Gimp
- Paint Shop Pro
- **ImageJ**

SOFTWARE FORENSI

- Amped
- Ghiro
- dTective di Avid e Ocean System ClearID
- LucisPro
- Ikena reveal di MotionDSP
- Video Focus di Salient Stills
- Impress di Imix
- Video Investigator di Cognitech
- StarWitness di SignalScape
- CrimeVision di Imagine Products
- Adroit Photo Forensics
- Image Error Level analyzer
- JpegSnoop
- NFI PRNU Compare
- Image forensics Search System
- Videntifier

IMAGE/VIDEO FORENSICS SUL PRATICO

UTILIZZI PRATICI DELLA IMAGE FORENSICS
Scansioni di tomografia computerizzata (**TAC**), utilizzate in ambito sanitario, **vengono utilizzate per individuare pacchetti di droga nascoste nelle cavitá del corpo per contrabbando illegale**

CLASSIFICAZIONE DI INFORMAZIONI
Le informazioni di un immagine vengono classificate secondo certi criteri e permettono l'identificazione di diversi elementi fondamentali dell'immagine.
ES. Pastiglie, Impronte di scarpe, Proiettili, ecc.

BIOMETRIA
Confrontare e Riconoscere caratteristiche fisiologiche o comportamentali di un individuo.
ES. Impronte Digitali, Palmo della mano, Facce, Iride, Forma dell'orecchio, ecc.

FOTOGRAMMETRIA E RICOSTRUZIONE 3D
Valutazione di dimensioni in un scena tramite proporzioni con grandezze note.
ES. Analisi della dinamica di un elemento, Analisi di oggetti, luoghi, volti, ecc.

STRUCTURE SENSOR
Scanner che consiste in un piccolo sensore che appartiene alla categoria dello active scanner.
Sfrutta la luce strutturata a infrarossi al fine di creare una mappa 3D della scena o oggetto scansionato

3D FLOW ZEPHYR
Software operante nel campo della Computer Vision e dell'Imahe Processing.
Utilizza particolari aspetti della fotogrammeria per la ricostruzione in 3d della realtá osservata

IMAGE ENHANCEMENT/RESTORATION
Algoritmi di Miglioramento della qualitá e invertire il processo di degrado di un'immagine,
Permettono di recuperare un maggior numero di informazioni dall'analisi di un'immagine.

I problemi presenti possono essere in parte risolti con tecniche di image processing
Tipi di elaborazioni:

- Nel dominio dello S**pazio**
- Nel dominio della **Frequenza**
- Nel dominio del **Tempo** (informazioni provenienti da piú fotogrammi)

Per ogni problema possono essere applicate diverse tecniche con differenti prestazioni e costi computazionali

RIDUZIONE DEL RUMORE
Determinate operazioni permettono di risolvere il problema del rumore, a volte non del tutto.
Molte volte viene usato il **filtro mediano per risolvere la problematica rlativa ad alcuni rumori.**
Molte volte il **rumore** puó essere causato da **problematiche con i sistemi di acquisizione immagini**
ES. Piel Bruciati o **Sensore progettato in quel modo**.
Molte volte viene applicato automaticamente un piccolo filtro di mediana che permette di sistemare leggermente l'immagine da questi rumori.

FILTRO MEDIANO
Filtro che serve per rimuovere il rumore
Esso viene applicato in presenza dei rumori:
- **Sale e Pepe**
- **Impulsivo**

Come viene applicato il filtro:
- **Sostituisce il pixel con il rumore con quello della sua mediana**

RUMORE DA COMPRESSIONE
Problema che nella pratica é un misto tra il Blocking e Alta Frequenza Sparsa.
Si produce un alta frequenza con aggiunta di blocchi.
Alcuni algoritmi permettono di **aggiustare leggermente** il problema, migliorando la qualitá dell'immagine.
Di solito questo **Problema** viene Contrastato con due operazioni:
1. Applicazione di un algoritmo di **DeBlocking**
2. Applicazione del **Filtro Media**

EDGE DETECTION
Tecnica di rilevamento dei bordi di un'immagine.
L'obiettivo principale é quello di identificare curve in un'immagine digitale dove il cambiamento di luminosità avviene bruscamente o presenta discontinuitá.
Le **curve** di un immagine spesso **rappresentano i bordi** ai confini di un **oggetto.**
Il rilevamento dei bordi aiuta ad identificare gli oggetti presenti nell'immagine

METODI PER IL RILEVAMENTO DEI BORDI
- Rilevamento dei bordi di **Canny**: Metodo che utilizza un **algoritmo a piú fasi** per rilevare i bordi. Comprende:
  - **Riduzione del rumore**
  - **Calcolo del Gradiente**
  - **Soppressione del massimo locale**
  - **Tracciamento dei bordi**, tramite isteresi
- Operatore di **Sobel**: Utilizza il **Calcolo del Gradiente** sia nelle **direzioni orizontali che verticali.** Evidenzia i bordi **enfatizzando i cambiamenti di intensità**
- Operatore di **Scharr**: Simile a **Sobel** ma offre una **maggiore invarianza alla rotazione**. Utile per **rilevare i bordi a diverse orientazioni**
- Operatore di **Prewitt**: Altro metodo basato sul **Gradiente**

DECONVOLUZIONE
Tecnica di elaborazione delle immagini ad altá intensità di calcolo che viene utilizzata per**:**
- **Migliorare il contrasto**
- **Migliorare la risoluzione**

La tecnica della Deconvoluzione permette di trasformare un'immagine poco chiara in un'immagine piú intuitiva e chiara.

BLURRING
Sfocatura presente in un immagine, talvolta, **generata da un individuo o dalla scarsa capacitá di acquisizione del dispositivo di acquisizione.**
Esistono degli algoritmi, detti di DeBlurring, che permettono di ridurre la sfocatura di un immagine.
Questo problema, come il problema del motion blur, **puó essere risolto con l'utilizzo dei filtri convolutivi applicati all'immagine sfocata**

INTERLACCIAMENTO
Tecnica che raddoppia la frequenza dei fotogrammi percepita di un display video senza consumare ulteriore larghezza di banda.
In un video interlacciato, **due campi di un fotogramma video vengono acquisiti consecutivamente**:

- **Migliorando la percezione del movimento**
- **Riducendo lo sfarfallio**

DEINTERLACCIAMENTO
Processo che converte il mareriale sorgente, che contiene semi-immagini alternate, **in un'immagine completa alla volta.**
Il deinterlacciamento **puó indovinare il movimento di ogni oggetto nel video** e **applicare la correzione del movimento**.
Un video puó essere deinterlacciato utilizzando Software come:

- **AnyMP4 Video Converter Ultimate** (Windows e Mac), permette di:
  - **Migliorare la qualitá video**
  - **Correggere le Sorgenti interlacciate**
  - **Rimuovere gli artefatti frastagliati**

DEINTERLACCIAMENTO ADATTIVO
Tecnica piú sofisticata che processa solo le zone dell'immagine in rapido movimento riducento al minimo la perdita di risoluzione.
É possibile applicare un **processo di interpolazione tra i semiquadrati per ridurre la loro differenza temporale**.
Per deinterlacciare un video possiamo farlo con **VLC Media Player:**

- Attivare l'Opzione **Video > Deinterlaccia > Attivo**

Fatto ció **noteremo che ogni tipo di riga sfasata é sparita,** potrai infine salvare il video senza le fastidiose righe interlacciate.

FRAME INTEGRATION
Tecnica utilizzata per analizzare ed individuare manipolazione nei video digitali
Strumento prezioso per **identificare frodi nei video digitali** e **preservare l'integritá delle prove digitali** nelle indagini forense. Utilizzi pratici della Frame Integration:

- **Rilevamento e Localizzazione di frodi Inter-Frame**: Inserimento, cancellazione e la duplicazione di fotogrammi. Approccio:
  - **Basato su Caratteristiche di texture**
  - **Analizza le inconsistenze di correlazione tra gli istogrammi dei fotogrammi adiacenti**
- **SVM classifier**: Un classificatore SVM supervisionato viene addestrato per rilevare la manipolazione dei video con un accuratezza del 99%
- **Localizzazione dei fotogrammi manipolati**: Individuare la posizione dei fotogrammi manipolati nel video. Utilizzo **l'ineguaglianza di Chebyshev** per **evidenziare i fotogrammi forgiati in caso di attacchi di inserimento o cancellazione**

Data una sequenza di immagini che riprendono la stessa scena disturbate da rumore casuale a media nulla si puó fare la media fra pixel corrispondenti su diversi frame
Con un numero infito di fotogrammi il rumore dovrebbe annullarsi, ma anche con un numero piuttosto ridotto i risultati possono essere notevoli.
Per effettuare una **Frame Integration** é necessario che le **immagini rappresentino esattamente la stessa scena.**
Ipotesi **non sempre soddisfatta**, in quanto non sempre la telecamera é fissa o c'é qualche soggetto.

IMAGE REGISTRATION
Processo tramite cui vengono fatte sovrapporre due o piú immagini rappresentanti una scena presa in istanti differenti, da diversi punti di vista o con diversi sensori.
Processo atto ad allineare due immagini o particolari di esse.
Usata per allineare immagini spostate di una semplice traslazione per stabilizzare una ripresa mossa.

CORREZIONE PROSPETTICA
Processo che permette di rettificare l'effetto di prospettiva in un'immagine rendendo gli oggetti geometricamente corretti e allineati.
Particolarmente utile quando si fotografano edifici o oggetti con angolazioni sbagliate o distorsioni della lente.
ES. Fotografia alla targa di un automobile presa da un angolazione sbagliata.
Tecniche piú avanzate permettono di recuperare anche altri tipi di trasformazioni.

CENNI SULLA SUPER RESOLUTION PER I VIDEO
Si utilizzano le informazioni provenienti da diversi fotogrammi per ricostruire le informazioni perse nel processo di acquisizione
Scenario: Nel processo di acquisizione l'immagine reale é stata sottoposta a sottocampionamento e sfocatura.
Soluzione:

- **Prima parte:** Processo di registrazione (Frame Registration) con accuratezza superiore ai pixel
- **Seconda Parte:** Ricostruzione dei dati mancanti (ES. Interpolazione)

ZOOMING VS SUPER RESOLUTION
Lo Zooming puó creare artefatti nuovi dato l'utilizzo massiccio di interpolazione di nuove informazioni.
La Super Resolution permette di incrementare la risoluzione volta a recuperare l'informazione reale senza produrre artefatti.

MOTION DETECTION
Tecnica per riconoscere il movimento di soggetti o oggetti all'interno di una sequenza di frame.

TECNICHE ELEMENTARI
Consistono nel calcolare semplicemente quanto é diverso un fotogramma da quello precedente o da uno di riferimento.
Se tale differenza supera una certa soglia allora il sistema segnala una presunta presenza di moto.

SEPARAZIONE DEI COMPONENTI
Estrazione di diverse componenti di un immagine

TECNICHE

- **Color Deconvolution**: Isola le tonalitá desiderate
- **indipendent Component Analisys**: Separa due segnali sufficientemente scorrelati

ATTENZIONE AI BIAS COGNITIVI

Esistono vari tipi di Bias Cognitivi ai quali un consulente deve fare attenzione:

- **Expectation Bias**: Il consulente si aspetta di trovare qualcosa e quindi la trova. Analisi non distaccata dagli avvenimenti
- **Confirmation Bias**: Sapendo cosa sta cercando il consulente é portato a trovare e cercare ció che gli é stato chiesto trascurando altri importanti dettagli
- **Contextual Bias**: Il consulente si fa condizionare da informazioni che pregiudicano l'oggettivitá dei fatti

Uno dei bias cognitivi piú frequenti é la presenza dei volti nella scena

SOLUZIONE AI BIAS COGNITIVI

Per far fronte ai problemi inerenti ai Bias Cognitivi é possibile utilizzare delle **Strategie di Mitigazione:**

- Durante l'identificazione non fornire mai al consulente l'informazione di chi o cosa stiamo cercando, cosí da non ridurre l'oggettivitá delle analisi.
- Chiarire i ruoli nell'agenzia, avendo un leader del caso che assegna le analisi tecniche alle altre persone.
- Proseguire l'indagine con piú operatori, buona idea sia per la mitigazione del bias che per la riduzione degli errori

TRASFORMAZIONE PROIETTIVA

Concetto fondamentale nelle immagini digitali e nella grafica computerizzata.

Come si applica:

- **Proiezione prospettica**: Si utilizza quando si forma un'immagine tridimensionale a uno spazio bidimensionale. **Simula il comportamento di una fotocamera a foro stenopeico** (pinhole). **Responsabile della formazione di immagini realistiche con effetti di profonditá e prospettiva**
- **Distorsioni**: Le fotocamere possono avere distorsioni dovute alla lente o ad altri fattori e possono influenzare la qualitá dell'immagine e devono essere corrette durante la calibrazione della fotocamera. Le distorsioni possono essere:
  - **Radiali**: Effetto a botte o a cuscinetto
  - **Tangenziali**: Linee parallele ai bordi dell'immagine che curvano verso l'interno o verso l'esterno
- **Calibrazione**: Processo di **determinare i parametri intrinseci**, indispensabili per **convertire le coordinate 3D degli oggetti in coordinate 2D**, della fotocamera come:
  - **Lunghezza Focale**
  - **Punto Principale**
  - **Distorsioni**

La Trasformazione Prospettiva é ció che consente alle fotocamere di catturare il mondo tridimensionale in immagini bidimensionali.

TRASFORMAZIONE DI BASE

Utilizzate per mappare punti da uno spazio all'altro.

Ognuna di tali trasformazioni presenta delle caratteristiche peculiari ben distinguibili quando applicata ai punti di un oggetto rigido

COORDINATE OMOGENEE

Ad ogni R^n é possibile associare uno spazio di dimensione n+1 detto **spazio proiettivo**

Definizione di spazio proiettivo:

- $P^n = R^{n+1} - 0$

Nel caso del 2D:

- $x = (x,y) \in R^2 \rightarrow /x = (x_w, y_w, w) \in P^2$

/x é il **punto di coordinate omogenee**

Le coordinate omogenee sono utili in computer grafica e in compter vision in quanto **permettono di esprimere le trasformazioni di base in una forma matriciale standard**

Dato un punto in **coordinate cartesiane** (x,y) é possibile esprimerlo in **coordinate omogenee** (x_w, y_w, w) **scegliendo** $w \neq 0$ e ponendo:

$x_w = x*w$ e $y_w = y*w$.

ES. scegliendo w = 1 si ha:

- $(x,y) \rightarrow (x,y,1)$

É possibile ottenere un punto cartesiano da un punto in coordinate omogenee dividendo tutto per w:

- $(x_w, y_w, w) \rightarrow (x_w/w, y_w/w)$

FORMA MATRICIALE DELLE TRASFORMAZIONI DI BASE
Ogni trasformazione di base 2D puó essere espressa come il prodotto tra il vettore colonna delle coordinate omogenee del punto e un apposita matrice di trasformazione A [3x3]:

$$\begin{bmatrix} x_w \\ y_w \\ w \end{bmatrix} = A \begin{bmatrix} X \\ Y \\ 1 \end{bmatrix}$$

Dove (X,Y) é il punto da trasformare,
(x_w, y_w, w) é il punto trasformato in coordinate omogenee,
A é una matrice [3x3] che rappresenta la specifica trasformazione

MATRICI DI TRASFORMAZIONE
A ogni trasformazione di base é possibile associare una matrice T[3x3] costruita a partire dai suoi parametri:

- **Vettori di Traslazione**
- **Angoli di Rotazione**
- **ecc.**

TRASFORMAZIONE PROSPETTICA
Rappresenta come gli oggetti vengono proiettati da uno spazio tridimensionale a uno spazio bidimensionale.
La trasformazione prospettica é approssimata da una trasformazione proiettiva tra due punti appartenenti a piani diversi.
La **trasformazione proiettiva é determinata considerando il mapping tra un quadrilatero arbitrario nel piano dell'oggetto e un quadrilatero nel piano dell'immagine.**

MATRICE DI PROIEZIONE
La relazione tra i punti sul piano dell'oggetto $\{(x_i,y_i)\}^N_{i=1}$ e i punti sul piano dell'immagine $\{(x'_i,y'_i)\}^N_{i=1}$ é data da:

$$\hat{S} = TS = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{bmatrix} \begin{bmatrix} x_1 & \dots & x_N \\ y_1 & \dots & y_N \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} x'_1 & \dots & x'_N \\ y'_1 & \dots & y'_N \\ 1 & 1 & 1 \end{bmatrix}$$

Dove T é la matrice di trasformazione proiettiva
Si noti che i gradi di libertá della matrice sono otto:

- $a_{31}x + a_{32}y + a_{33} = 1$

DETERMINARE LA MATRICE DI PROIEZIONE
La corrispondenza tra i vertici dei quadrilateri ci dá una corrispondenza tra quattro punti (otto coordinate) che corrispondono agli otto gradi di libertá della trasformazione proiettiva.
La matrice T puó essere determinata risolvendo il sistema:

$$\hat{S} = TS$$

Note le matrici S e considerando il vincolo: $a_{31}x + a_{32}y + a_{33} = 1$

RICONOSCIMENTO ANTROPOMETRICO DA IMMAGINI DI VIDEO SORVEGLIANZA

RICONOSCIMENTO ANTROPOMETRICO DA IMMAGINI DI VIDEO SORVEGLIANZA

BIOMETRIA
Meccanismo per identificare soggetti umani tramite le loro caratteristiche uniche.
Elementi biometrici in una persona:

- **IRIDE**: Firma biometrica al 100%
- **DNA**: Firma biometrica al 98%,
- **Impronta Digitale**: Firma biometrica al 90%
- **Riconoscimento Facciale**: Volto unico con tante variabili, firma biometrica al 70%

Proprietá degli elementi biometrici di una persona:

- **Unicitá**: Ogni elemento é unico per ogni persona
- **Identificazione**: Problema relazionale 1 a N, Identificare che il campione sia presente in un certo dataset di popolazione N.
- **Verifica**: Relazione 1 a 1, una volta identificato si puó proseguire con la verifica

Per il **NIST** la percentuale di **errore** si aggira all'1%.

BIOMETRIA FORTE
Definita come:

- **Unica**
- **Possiede tecniche di verifica** con margine di errore basso e facilmente codificabili

BIOMETRIE FORTI

- **IRIDE**
- **DNA**
- **FINGERPRINT**

BIOMETRIE DEBOLI

- **RICONOSCIMENTO FACCIALE**
- **ALTEZZA**
- **ANALISI DELLA CAMMINATA (GAIT ANALISYS)**

PROBLEMI DI IDENTIFICAZIONE DELLA BIOMETRIA

- **Identificazione 1 a N**: Identificare che il campione sia presente in un certo dataset di popolazione N.
- **Precisione della FingerPrint**: La precisione puó diminuire se:
  - **Polpastrello non integro**
  - **Posizione errata del polpastrello** (Posizionato male nel dispositivo)
- **Precisione del dispositivo di acquisizione facciale**: Dipende dalla:
  - **Qualitá dell'immagine** (Nitida 70%, Oggetti ostruiscono il volto 40%, Sfocatura 20%)
  - **Occlusioni**:
  - **Luci**: Le luci in un immagine potrebbero distorcere il reale volto
  - **Posizione**: La posizione del volto é fondamentale ai fini di identificare il volto.
  - **Aging**: Invecchiamento della persona ritratta in foto
  - **Elementi del viso**: Forma degli occhi, naso, bocca, capelli
- **Riconoscimento dell'iride**: Difficile da acquisire
  - **Camere ad alta risoluzione**

MODALITÁ DI ACQUISIZIONE DEL DATO
Esistono quattro fasi che devono essere effettuate su un dato:

1. **Acquisizione**: Acquisizione del dato in se
2. **PreProcessing**: Pre processare il dato affinche sia possibile estrapolare caratteristiche
3. **Estrazione caratteristiche**: Estrazione delle caratteristiche del soggetto in questione
4. **Confronto**: Confronto a campione delle caratteristiche del soggetto con una lista di soggetti sospettati

ANALISI FISIONOMICA DEL VOLTO
Gli elementi morfologici si dividono in:

- **Fondamentali**: Devono essere il piú possibile indipendenti da variazioni ponderali e dall'erá del soggetto
- Non fondamentali: Potrebbero cambiare con il passar del tempo

ES. Forma Generale Del volto nella prospettiva frontale = Elemento di caratterizzazione

DIECI TIPI DI FISIONOMIA FACCIALE

1. **Ellittica**: Contorno a linea curva con **Uguale Larghezza in alto e in basso**
2. **Ovale**: Contorno piú **stretto verso il basso**
3. **Ovale invertita**: Contorno **maggiormente largo in basso**
4. **Rotonda**: Piuttosto **tonda** e **inscritta in un cerchio**
5. **Rettangolare**: Zigomi **molto sporgenti** e **uguale larghezza dei parietali e mandibola**
6. **Quadrata**: **Larghezza e altezza quasi uguali**
7. **Rombica**: Parietali **depressi,** mandibola **stretta** e zigomi **sporgenti**
8. **Trapezoidale**: A base **in basso** con parietali **relativamente poco sporgenti**, al contro zigomi e mandibola
9. **Trapezoide invertita**: **Inversa della precedente**
10. **Pentagonoide**: Parietali, zigomi e mandibola **della stessa larghezza**, con mento particolarmente **squadrato**

Elementi che potebbero causare problemi al riconoscimento della fisionomia facciale:

- **Barbe**
- **Baffi**
- **Parrucche**
- **Occhiali**

FORMA DELLA TESTA
Classificata tenendo in considerazione le tre parti costituenti:

- **Frontale**
- **Parietale**
- **Occipitale**

Forme di teste:

- **Di Fronte Curva**
- **Carenata**
- **Di Profilo Curva**
- **A Linea Spezzata**
- **Insellata**
- **Con Vertice Posteriore**
- **Con Vertice Anteriore**
- **Con Occipite Sporgente**
- **Ad Occipite Appiattito**

MORFOLOGIA DELL'ATTACCATURA DEI CAPELLI
Diverse tipologie di attaccatura dei capelli:

- Privi di **Trichion**:
  - **Curvilinea**
  - **Rettilinea**
- Con **Trichion**:
  - **Stretto**
  - **Largo (IO)**

Trichion: Punto specifico della fronte umana. **Intersezione in cui la linea dei capelli normali incontra la linea centrale della fronte**

PROFILO DEL VOLTO
Elemento morfologico di notevole valore e puó essere considerato**:**

- **Nella sua globalitá**: Interezza, cosí com'é
- **Dall'andamento del complesso**:
  - **Fronte-Naso**: Fronte e Naso
  - **Naso-Buccale**: Naso e Bocca

Tipologie di Profili:

- **Faccia Rettilinea**
- **Faccia Piramidale**
- **Faccia Semilunare**
- **Faccia Rientrante**

CLASSIFICAZIONE DEL PROFILO FRONTO-NASALE

- **Continuo**: Le **due rette della fronte e della piramide nasale non formano alcun angolo**, dando vita al **Naso Greco**
- **Parallelo**: I **due profili della fronte e del naso sono rettilinei**, ma **il primo sopravanza al secondo e i loro prolungamenti sono paralleli**
- **Spezzato**: L'**Angolo fronto-nasale é molto pronunciato**
- **Angoloso**: L'**Angolo fra la fronte e la piramide nasale é Infossato in una forte depressione**
- **Curvilineo**: La L**inea della fronte e quella del naso sono curvilinee**
- **Ondulato**: Il **Profilo della fronte é convello** e quello **del naso concavo e sono in continuazione senza formare angolo**

CLASSIFICAZIONE DEL PROFILO NASO-BUCCALE

- **Nasale**: La **Faccia sporge in corrispondenza del naso,** mentre **il mento é sfuggente**
- **Dentale Superiore**: Il **Labbro superiore sporge sul mento sfuggente**
- **Mandibolare**: il **Labbro inferiore sporge in avanti rispetto al superiore**
- **Totale**: **Naso e mentoniera sono protesi in avanti per cui la linea verticale che scende dalla parte inferiore della fronte raggiunge il mento tagliando in avanti tutte le altre parti**

PROFILO DELLA FRONTE

- **Concava**
- **Rettilinea**
- **Convessa**
- **Prominente**
- **Intermedia**
- **Sfuggente**

PADIGLIONE AURICOLARE

L'**Orecchio** puó essere considerato:

- **Grande**
- **Medio**
- **Piccolo**

Se si tiene conto della **Lunghezza** puó essere:

- **Lungo**
  - Molto Lungo
  - Medio Lungo
- **Corto**
  - Molto Corto
  - Medio Corto

Se si tiene conto della **Larghezza** puó essere:

- **Largo**
  - Molto Largo
  - Medio Largo
- **Stretto**
  - Molto Stretto
  - Medio Stretto

L'**Orecchio esterno** é costituito:

- **Padiglione Auricolare**
  - Molto variabile sia nella sua globalitá che negli elementi che lo compongono
- **Meato Acustico Esterno**

FORMA DELL'ORECCHIO

- **Ovale**
- **Triangolare**
- **Rettangolare**
- **Tondo**

DIREZIONE DELL'ORECCHIO

- **Obliqua Media**
- **Obliqua Accentuata**
- **Verticale**

TUBERCOLO DI DARWIN

Piccolo rilievo che si trova in corrispondenza dell'apice del padiglione, esso viene classificato in diverse forme:

- **Orecchio da Cercopiteco**: Il **Tubercolo si trova non sul margine dell'elice ma sul margine dell'orecchio stesso**, L'elice forma un netto gomito nel punto piú alto
- **Orechio a punta Aguzza**: IL **Tubercolo genera una punta aguzza**
- **Orecchio a punta Arrotondata**
- **Orecchio a punta Appiattita**
- **Orecchio con assenza di Punta**

FORMA DEL MENTO
Classificazione delle forme del mento:

- **Piatto**
- **Convesso**
- **Prominente**
- **Intermedio**
- **Sfuggente**
- **A Punta**
- **Quadrangolare**

MORFOLOGIE DELLA REGIONE NASO-BUCCALE
La regione Naso-Buccale é composta da:

- **Solco naso-labiale**
- **Solco naso-orale**
- **Angolo della bocca**
- **Rima buccale:** Linea sinuosa definita dalle labbra ravvicinate
- **Solco mento labbiale**
- **Labbro superiore**
- **Prolabio superiore**
- **Labbro inferiore**

SOPRACCIGLIA
Presentano colorazione che generalmente coincide con quello dei capelli.

CLASSIFICAZIONE DELLE SOPRACCIGLIA
Si controlla l'andamento delle **tre porzione:**

- **Testa**
- **Coda**
- **Corpo**

Le sopracciglia possono essere:

- **Curve**
- **Arcute**
- **Rette**
- **Ondulate**
- **Spezzate**
- **Orizzontali**
- **Oblique Interne**
- **Oblique Esterne**

SCALA DI COMPATIBILITÁ DEI DATI

- **TOTALE**: I dettagli trovati coincidono
- **COMPATIBILE**:
- **PARZIALMENTE COMPATIBILE**
- **NON COMPATIBILE**: I dettagli non coincidono con quelli del sospettato

CRITERI IDENTIFICATIVI

I criteri identificativi sono quattro:

- **Non Compatibilitá**
- **Compatibilitá Parziale**
- **Compatibilitá**
- **Compatibilitá Totale**

NON COMPATIBILITÁ

Nessuna delle caratteristiche in esame é oggettivamente compatibile oppure é presete almeno una caratteristica UNIVERSALE, UNICA e PERMANENTE che permette di escludere che due soggetti abbiano la stessa identitá

COMPATIBILITÁ PARZIALE

La scarsa definizione e/o visibilitá di almeno una delle due immagini a confronto non permette di rivelare particolari caratteri antropo-somatici che permettano di giungere ad un giudizio

COMPATIBILITÁ

Gli elementi presenti nei due individui o oggetti a confronto permettono di rilevare numerosi particolari o caratteri antropo-somatici simili in entrambi gli individui o oggetti. Non si puó giungere ad un giudizio certo

COMPATIBILITÁ TOTALE

I due individui o soggetti, ritratti nelle immagini a confronto, hanno tutti i particolari o caratteri antropo-somatici visibili simili, per forma e proporzioni.
Sono inoltre presenti alcuni elementi o particolaritá anatomiche singolari, contrassegnati, riscontrabili in entrambi gli individui o soggetti a confronto.

SISTEMA SARI

Database che contiene tutte le foto degli individui segnalati per un qualche motivo.
Non ha valore legale un matching fatto tramite AI per via della possibilità di eventuali falsi positivi è possibile utilizzare una comparazione 3D.

LIKELIHOOD

Verosomiglianza in percentuale tra due soggetti

ALTEZZA

Fattore discriminante, elemento biometrico debole, ma utile per alcune sue caratteristiche:

- **STATURA** (Altezza piena del soggetto)
- **ALTEZZA ACROMIALE** (Dallo sterno in giú)
- **ALTEZZA SOPRASTERNALE** (Dal centro del petto in giú)
- **ALTEZZA VITA** (Dalla vita in giú)
- **ALTEZZA STATILION** (Dalla minchia in giú)

L'altezza alla spalla valutata sulla popolazione italiana é scientificamente nota.
Da tali studi si evince che:

- **5% Altezza Coporea - Altezza Acromiale.**
- **50% Altezza Coporea – Altezza Acromiale.**
- **95% Altezza Corporea – Altezza Acromiale**

FATTORI DA CONSIDERARE

- **Prospettiva** dell'immagine**.**
- **Geometria** ed applicazione di un **preprocessing** per capire se é possibile calcolare l'altezza esatta.
- Il calcolo dell'altezza é possibile solo se é possibile tracciare dei riferimenti cartesiani sulla scena, anche nella migliore delle ipotesi ci possono essere errori
- Se la camera non cambia è possibile ritornare sulla scena un asta stadiometrica che permette di calcolare l'altezza sovrapponendo le immagini analizzate e quella scattata con l'asta.

TRADUZIONE LIKELIHOOD RANGE – RANKING VERBALE

	Likelihood Ratio	LLR	Verbal equivalent	
+5	> 10.000	> 4	Very strong evidence to support	Same-source hypotheses
+4	1000 – 10.000	3 – 4	Strong evidence to support	
+3	100 - 1000	2 – 3	Moderately strong evidence to support	
+2	10 - 100	1 – 2	Moderate evidence to support	
+1	2 – 10	0.3 – 1	Limited evidence to support	
0	1	0	***Inconclusive***	
-1	0.5 - 0.1	-0.3 to -1	Limited evidence to support	Different-Source hypotheses
-2	0.1 - 0.01	-1 to -2	Moderate evidence to support	
-3	0.01 - 0.001	-2 to -3	Moderately strong evidence to support	
-4	0.001 - 0.0001	-3 to -4	Strong evidence to support	
-5	< 0.0001	< -4	Very strong evidence to support	

In questa tabella sono presenti:

- **LR**: **Rapporto di probabilitá di somigliana di due soggetti**.
  - Valori Positivi: Ipotesi a favore della somiglianza
  - Valori Negativi: Ipotesi a sfavore della somiglianza
- **LLR**: **Logaritmo naturale del rapporto di probabilitá**. Valori come i precedenti
- **Equivalente Verbale**: **Descrizione verbale della forza dell'evidenza**

OSSERVAZIONE DELL’ALTEZZA DI UN SOGGETTO

- **Altezza stimata in fotogramma**: Margine di errore fino a 10+- centimetri
- La popolazione **Mondiale** in media é alta:
  - **Donne 160,2 cm**
  - **Uomo 173,7 cm**

STEGANOGRAFIA E STEGANALISI NELLE IMMAGINI IL LE AST SIGNIFICANT BIT

IMAGE/VIDEO FORENSICS STEGANOGRAFIA

WATERMARKING
Tecnologia grazie alla quale é possibile inserire opportune informazioni in un segnale,
In particolare su:

- Immagini
- Video

Obiettivi:

- **Segnalare l'Originalitá**
- **Titolare dei Diritti di Proprietá**

Un **WaterMark** deve essere visibile solo in certe condizioni.

WATERMARK SEMIFRAGILI
Tipologia di watermark, con determinate proprietá:

- **Piú Robusti alle Manipolazioni**
- **Piú Pesanti all'interno di un Immagine**

PROBLEMA DEL COPYRIGHT
Problema dei diritti d'autore, esso puó essere contrastato inserendo dei watermark all'inerno del file multimediale, anche se quest ultimi sono manipolabili e rimuovibili

COME AUTENTICARE UN'IMMAGINE

- **Ispezione Visuale**
- **Analisi dei File**: Formato dei file, Dati EXIF, Metodi di compressione. Se qualcuno ha modificato un immagine **risalvandola** la struttura cambia
- **Analisi Globale**: Statistiche sui pixel ed i dati compressi. Si valuta la **forma dell'istogramma**
- **Analisi Locale**: Si trovano inconsistenze nei pixel dell'immagine. AMPED AUTHENTICATE possiede filtri in grado di effettuare analisi locale

I **software non forniscono una risposta precisa** sull'effettiva **manipolazione** dell'immagine, forniscono solo degli **Indicatori** che aiutano a capire se sono state effettuate manipolazioni

STEGANOGRAFIA
Insieme di tecniche che consentono di nascondere messaggi, che devono essere interagibili solo al destinatario, inserendoli all'interno di un contesto del tutto estraneo, che funge da contenitore in grado di nascondere il contenuto ma la stessa esistenza della comunicazione, agli occhi di un eventuale osservatore.
Nascondere l'esistenza stessa del messaggio includendolo in un mezzo che potremmo definire neutrale e garantendo la segretezza della comunicazione.
Arte di comunicare senza essere osservati.

OBIETTIVO DELLA STEGANOGRAFIA
Nascondere l'esistenza stessa della comunicazione nascondendo il vero messaggio all'interno di un messaggio dal significato innocuo

STEGANOGRAFIA VS CRITTOGRAFIA

- **Crittografia**: Nascondere **il contenuto** del messaggio
- **Steganografia**: Nascondere **l'esistenza** del messaggio

A volte l'utilizzo di una sola delle due non é sufficiente quindi **le due tecniche vengono combinate**

STEGANOGRAFIA DIGITALE

La steganografia si é espansa fino ad utilizzare supporti digitali come:

- File Immagini
- File Audio/Video

Ma anche:

- File System
- Header Pacchetti TCP/IP

FORMALISMI

- **Cover**: Contenitore, **Immagine designata a contenere il messaggio**
- **Payload**: Carico, **Messaggio effettivo**
- **Stego-Image**: Immagine Stego, **Funzione steganografica che prende in input la cover e il payload**

$$\text{stego-image} = F\big(G(\text{cover}), H(\text{payload})\big)$$

- **G(cover)**: Funzione che elabora la **cover**
- **H(payload)**: Funzione che elabora il **payload** da inserire. ES. Funzione Crittografica

MODELLI STEGANOGRAFICI

Lo schema di base della steganografia contiene al suo interno due messaggi:

- **Messaggio Segreto**
- **Messaggio Contenitore**

In base all'origine del contenitore é possibile distinguere:

- **Steganografia Iniettiva**
- **Steganografia Generativa**

STEGANOGRAFIA INIETTIVA

Consente di inserire il messaggio segreto all'interno di un messaggio contenitore giá esistente modificandolo in modo tale che possa contenere il messaggio segreto.

PAYLOAD + COVER → STEGO-IMAGE

STEGANOGRAFIA GENERATIVA

Consente di generare, a partire dal messaggio segreto, un messaggio contenitore atto a nascondere nel migliore dei modi il messaggio segreto

PAYLOAD → PROCESSO GENERATIVO → COVER+PAYLOAD = STEGO-IMAGE

ULTERIORI CLASSIFICAZIONI

Classificazione delle tecniche steganografiche a livello pratico:

- **Steganografia Sostitutiva**
- **Steganografia Selettiva**
- **Steganografia Costruttiva**

STEGANOGRAFIA SOSTITUTIVA

Tecnica basata sull'osservazione che la maggior parte dei canali di comunicazione che trasmettono segnali che sono sempe accompagnati da qualche tipo di rumore.

Questo **Rumore** puó essere sostituito da un segnale (**messaggio segreto**) che é stato trasformato in modo tale che, a meno di conoscere la chiave segreta, é indistinguibile dal rumore vero e proprio.

Sostituisce i bit meno significativi dei file digitalizzati con i bit che costituiscono il messaggio segreto. Molto utilizzata nella pratica.

STEGANOGRAFIA SELETTIVA

Tecnica che mira a scegliere il supporto a seconda del messaggio da occultare. Viene effettuata una selezione dei supporti a disposizione o si usano semplici algoritmi per generarli, procedendo per tentativi finché non vengono rispettate particolari condizioni

Pregi e di questa tecnica:

- **Quasi impossibile da identificare**
- **Soluzione dispendiosa**
- **Tempo di reperimento o generazione del supporto alto**

Non viene realmente utilizzata nella pratica, ha un valore puramente teorico

STEGANOGRAFIA COSTRUTTIVA

Opera come la Steganografia Selettiva con una differenza che nel modificare il file contenitore si tiene conto di un modello di rumore, si tenta di sostituire il rumore presente con il messaggio segreto nel rispetto delle caratteristiche del rumore originale.

In questo modello il sistema steganografico deve adattarsi su un modello di rumore e adattare i parametri dei suoi algoritimi di codifica

Sembra la soluzione migliore, ma in realtá anch'esso non é esente da difetti

ANALISI

In qualsiasi applicazione di data-hiding (nascondere i dati) esistono tre requisiti in contrasto:

- **Invisibilitá** (steganografia)
- **Robustezza** (watermarking)
- **Capacitá** (etichettatura)

BIT PLANES

Un'immagine con una profonditá colore di N bit puó essere rappresentata da N piani di bit.

L'orgine va dai MSB (bit piú significativi) a LSB (bit meno significativi)

STEGANOGRAFIA NELLE IMMAGINI DIGITALI (DIMENSIONE DEL MESSAGGIO)

Supponendo di avere un'immagine **MxN**, essa puó contenere un **messaggio segreto lungo fino** a (**MxNx3)/8 byte.**

Un pixel puó contenere un messaggio segreto di 3bit

STEGANOGRAFIA LOSSY VS LOSSLESS

- **Lossy**: Compressione con perdita, non é possibile operare come sinora descritto. Se iniettassimo delle informazioni in un file bitmap (.bpm) e dopo applicassimo la compressione JPEG le informazioni andrebbero perse
- **Lossless**: Compressione senza perdita. Anche se effettuata la compressione JPEG le informazioni non andrebbero perse

STEGANOGRAFIA IN .GIF
Come iniettare un messaggio segreto in una GIF:

- **Decrementare il numero di colori ad un numero inferire a 256**, con un opportuno algoritmo che limita la perdita di qualitá
- **Convertire in GIF**, riempendo la palette con colori molto simili a quelli rimasti

STEGANOGRAFIA IN .JPG
Si opera ad un livello di rappresentazione intermedio. É possibile iniettare le informazioni nei **coefficienti di Fourier** ottenuti dalla prima fase di compressione

STEGANOGRAFIA IN BPCS
Possibilitá di scegliere regioni da modificare piuttosto che i bit meno significativi.
L'immagine viene divisa in blocchi 8x8 pixel e viene effettuato un test sulla complessitá dell'immagine. Se tale complessitá é minore di una determianata soglia allora un messaggio segreto puó essere nascosto in questo blocco senza alterare significatamente l'immagine

STEGANALISI
Tecniche di analisi per la rivelazione di messaggi nasconsti.
Possibili motivazioni dell'utilizzo della Steganalisi:

- **Contro-Spionaggio**
- **Anti-Terrorismo**
- **Controllo dell'opinione pubblica in reggimi Dittatoriali**
- **Raccolta Datti per motivazioni commerciali o fini illeciti**

Lo sviluppo di tecniche della steganalisi é indispensabile allo studio delle stesse tecniche della steganografia
Tecniche con l'obiettivo di individuare la presenza di un messaggio occultato attraverso l'uso di tecniche steganografiche.

FORMULAZIONE DELLA STEGANALISI
La steganalisi puó essere formulata come un **test sull'ipotesi che il mezzo contenga un messaggio segreto.**
Formalmente dato un insieme di osservazioni, o di loro funzioni dette **feature o statistiche** si formano due ipotesi:

- Il file non contiene un messaggio segreto
- Il file contiene un messaggio segreto

La decisione tra le due ipotesi viene presa in base ad un **criterio di ottimalitá**

ATTACCO
Tentativo di determinare la presenza di un messaggio segreto.
Distinzione di attacchi a seconda delle parti dell'equitazione:

- **stego-only-attack**: L'attaccante ha intercettato il frammento stego ed é in grado di analizzarlo
- **stego-attack**: Il mittente ha usato lo stesso cover ripetutamente per nascondere dati. L'attaccante possiede un frammento stego diverso ma originato dalla stessa cover.
- **cover-stego-attack**: L'attaccante ha intercettato il frammento stego e sa quale cover é stata usata per crearlo
- **cover-emb-stego-attack**: L'attacante ha tutto:
  - Frammento Stego-ImageCover Usato
  - Messaggio nascosto
- **manipulatig the stego data**: L'attaccante é in grado di manipolare i frammenti stego
- **manipulating the cover data**: L'attaccante puó manipolare la cover e intercettare il frammento stego

ATTACCHI VISUALI VS STATICI

- **Attacchi Visuali**: Sfruttano le capacitá dell'occhio umano per individuare artefatti introdotti da tecniche di steganografia
- **Attacchi Statici**: Effettuano test statici sui file steganografici

FASI ATTACCO VISUALE

- **Filtraggio del file** con un algoritmo di **filtering**, dipende dalla funzione usata per nascondere il messaggio
- Il risultato viene osservato per determinare se é stato nascosto un messaggio o meno

Operazione **lenta** se la **mole di immagini da analizzare é considerevole**.

FASI ATTACCO STATICO
L'informazione statica estratta da un'immagine piú nota ed utilizzata é sicuramente **l'istogramma** che rappresenta la distribuzione del colore nell'immagine stessa.
Grafo a basse dove:

- **Asse delle Ascisse**: Ci sono i valori di intensitá
- **Asse delle Ordinate**: Numero di pixel che hanno quel valore d'intensitá

IDEA DI ATTACCO STATICO
Confrontare la distribuzione di frequenza dei colori di un potenziale file steganografico con la distribuzione di frequenza

STEGANOGRADIA NELL'AUDIO DIGITALE .WAV
Sostituzione dei bit meno significativi allo scopo di steganografare il messaggio
ES. File WAV [44100Hz, 16bit] di un minuto
Dimensione file= 16bit x 44100Hz x 60sec x 2 = 84762000bit ~ 10366Kb
Spazio per file nasconsto utilizzando 2 bit meno significativi
84762000bit / 16bit x 2 = 10595250bit ~ 1293Kb
É possibile occultare qualsiasi cosa, anche un testo
Aggiunge rumore di fondo ai fini di aggiungere il messaggio segreto

ECHO DATA HIDING
Tecnica che evita l'inserimento di rumore di fondo per aggiungere il messaggio segreto all'interno di un audio

STEGANOGRADIA NELL'AUDIO DIGITALE .MP3

Non é possibile inserire il messaggio come nel caso dei file .wav, essendo file compressi in lossy.
Si inserisce il messaggio nella fase di Inner Loop.

INTRODUZIONE ALLA MOBILE FORENSICS

MOBILE FORENSICS

MOBILE FORENSICS
É la disciplica che si occupa delle attivitá d'indagine e consulenze/perizie informatiche su dispositivi cellulari come smartphone o telefoni, utilizzando le metodologie e le tecniche ereditate dalla digital forensics.
Punta ad **Acquisire queste informazioni nel modo meno intrusivo possibile,** preservando **l'integrità dei dati** e **riducendo alterazioni.**
Nella **Mobile Forensics** vengono effettuate tutte le **fasi** della **Digital Forensics**.

PRINCIPI DELLA MOBILE FORENSICS

- **Inalterabilitá dei dati**
- **IMEI**: Codice univoco associato ad ogni dispositivo

BEST PRATICE PER IL REPERIMENTO DEI DATI

- **Documentare le informazioni presenti sullo schermo**
- **Verificare data e ora del dispositivo, documentandola a mezzo foto**
- **Non navigare e non riaprire alcun messaggio**
- **Mantenerlo acceso e isolarlo dall'accesso alle eventuali comunicazioni**

DISPOSITIVI MOBILI
I dispositivi mobile sono composti da:

- **RAM**
- **Memoria Flash**
- **Memoria Esterna**
- **Schede Sim**
- **Sincronizzazione Cloud**

SFIDE DELLA MOBILE FORENSICS
La mobile forensics presenta diverse peculiaritá che rendono piú complessa l'acquisizione e l'analisi dei dati rispetto a quelli provenienti da PC

- **Varietá dell'hardware**: I dispositivi mobili differiscono in hardware, dimensioni, funzionalitá. ES. non é possibile estrarre la batteria in alcuni dispositivi
- **Varietá dei sistemi operativi**: Esistono molti sistemi operativi per dispositivi mobili e accessori smart
- **Funzionalitá di sicurezza presenti nei dispositivi mobili**: Le versioni piú recenti contengono misure di sicurezza che hanno lo scopo di proteggere i dati e la privacy
- **Alterazione dei dati**: I dati presenti nel dispositivo non devono essere alterati dall'analisi

ISOLAMENTO RADIO
É possibile isolare radiofonicamente i dispositivi mobili con diversi dispositivi o modalitá di utilizzo:

- **JAMMER**: Dispositivo che permette di disturbare totalmente le frequenza, comunicazioni wireless, in base alla sua potenza con sicurezza molto elevata. L'isolamento dura fino a quando non si scarica
- **FARADAY BAG**: Dispositivo portatile e flessibile che blocca i segnali wireless che cercano di raggiungere il dispositivo, il dispositivo viene inserito all'interno della bag. Tempo di utilizzo quasi infinito, sicurezza alta
- **AIRPLANE MODE**: Modalitá dei dispositivi elettronici, bloccano i segnali radio in ingresso con sicurezza bassa e dipende da come impostato

ACQUISIZIONE DEI DATI – ACQUISIZIONE FISICA
L'acquisizione **fisica** nei dispositivi mobili avviene:

- **Accedendo direttamente alla memoria flash e creando un'immagine bit-a-bit del suo contenuto**
- **Accedere fisicamente al chip della memoria estraendolo fisicamente dal dispositivo**

In questo modo avremo un'immagine completa di tutto il file system.
Questa operazione **non viene effettuata sempre** perché:

- In primo luogo:
  - **Dispendiosa in termini di tempo**
  - Potrebbe essere **Sovradimensionata rispetto allo scopo dell'acquisizione**
- In secondo luogo:
  - **Privilegi di root richiesti sul dispositivo.** Il **rooting** potrebbe essere un operazione **distruttiva** e **invasiva**

ACQUISIZIONE DEI DATI – ACQUISIZIONE LOGICA
L'acquisizione **logica** nei dispositivi mobili avviene:

- **Estraendo oggetti logici del dispositivo mobile**, file o directory attraverso un**'interazione con il sistema operativo**

Peculiaritá dell'acquisizione logica:

- **Facilitá d'utilizzo rispetto all'acquisizione fisica**
- **Non permette l'accesso a file cancellati o contenuti all'interno dello spazio non allocato**
- **Il sistema di sicurezza di Android non permette l'accesso alle directory di sistema**

ESTRAZIONE FILE SYSTEM E ADB BACKUP

- **Copia dei dati presenti sul dispositivo**
- **Non permettere recupero dei dati cancellati**
- **Estrazione Parziale**
- **Downgrade apk**

ACQUISIZIONE DEI DATI – ACQUISIZIONE MANUALE
L'acquisizione manuale nei dispositivi mobili avviene:

- **Interagendo con il dispositivo mobile attraverso l'interfaccia utente**

Metodo molto facile, ma introduce **il rischio di errore umano** che potrebbe portare alla **cancellazione dei dati.**

ACQUISIZIONE DEI DATI – ACQUISIZIONE DALLA RAM
L'acquisizione della RAM viene effettuata **raramente** in quanro per essere effettuata sono necessarie doti di un **accesso root al dispositivo,** che puó essere effettuata solo dopo il riavvio di un dispositivo, ma esso azzera i valori in RAM rendendo inultile l'acquisizione stessa dei dati.
In caso di **rooting giá effettuato** é possibile andare ad estrarre determinati dati in RAM, essi si limitano alla ricerca di stringhe

TECNICHE DI ACQUISIZIONE DATI SU SISTEMI ANDROID – ROOTING
I'analista forense ha necessitá di conoscere le **implicazioni di un dispositivo rooted** perché la prossibilitá di lavorare su un dispositivo con tali caratteristiche non é da escludere.

Utente Root: Utente amministratore che ha:
- Permessi per avviare o fermare i processi
- Modificare o cancellare qualsiasi file
- Modificare i privilegi degli altri utenti

Il Rooting del Dispositivo é l'operazione con la quale viene guadagnato l'accesso al dispositivo come utente root, allo scopo di eseguire azioni normalmente non permesse sul dispositivo
L'operazione di Rooting non é prevista dal produttore del dispositivo ma di solito si sfruttano delle vulnerabilitá del firmware per effettuarla

MODALITÀ PRATICHE ROOTING
- **Installazione ed esecuzione di un'app sul dispositivo**
- **Installazione di un software di recovery nella partizione di recovery**
- **Utilizzo di tool per PC che permettono il rooting del dispositivo connesso al PC via USB**

Esempio di tool per PC é KingoRoot.

Il rooting é un'operazione molto rischiosa per il dispositivo:
- Un rooting effettuato male potrebbe rendere inutilizzabile il dispositivo
- L'operazione invalida la garanzia del dispositivo

Un dispositivo rooted ha queste caratteristiche:
- **Esposto a malware o altri attacchi**
- **Alterazione dei dati del dispositivo da sottoporre ad analisi**

TECNICHE DI ACQUISIZIONE DATI SU ANDROID – ACQUISIZIONE BIT-BIT ADB
Android Debug Bridge **é un tool che fa parte degli android SDK tools, é uno strumento fodamentale per la Mobile Forensics in android in quanto permette la comunicazione via USB fra dispositivo mobile e un host computer.**
Ci permette di eseguire comandi di shell sul dispositivo

SDK: Insieme di tool rivolti agli sviluppatori che permette di costruire, testare ed effettuare il debug di app android

Per utilizzare questo **ADB** dobbiamo:
- **Abilitare la modalitá Sviluppatore**
- **Abilitare il Debugging USB**

Una volta avviato il **debugging USB** all'interno del dispositivo mobile verrá avviato il **demone ADB** il quale si occuperá della connessione usb con la workstation.
Due possibili strade per il demone:
- **Dispositivo non rooted**: Non permette l'acquisiziopne fisica dei dati né l'accesso ai dati interni delle applicazioni
- **Dispositivo rooted**: Inverso del precedente

Elementi presenti nella workStation:
- **Tool a riga di comando (abd)**: Una volta lanciato:
  - **Verificherá la presenza del demone ADB sulla workstation**
    - Se non é in esecuzione lo avvierá
    - il client comunica con il demone attraverso una connessione TCP nella porta 5037

ADB ci permette, come giá detto, di eseguire dei comandi shell nel dispositivo per:
- **Ottenere una shell di root**, se il dispositivo é rooted
- **Salvare l'immagine sulla workstation**
- **Acquisizione logica dei dati del dispositivo**

TECNICHE DI ACQUISIZIONE DATI SU ANDROID – TECNICA CHIP-OFF
Tecnica che consiste nella rimozione fisica dei chip di memoria dal device e nella conseguente acquisizione e analisi dei dati in essi contenuti.
Eseguita nei casi in cui sia l'unica o l'ultima risorsa disponibile, **the last technique standing.**
É possibile l'acquisizione dei dati anche se i dispositivi sono gravemente danneggiati, non funzionanti, protetti da password/pin o bloccati da altri meccanismi di sicurezza.
Si puó attuare sulla maggior parte dei device che montano memorie flash di tipo:
- **NAND**
- **NORMATIVA**

La procedura si effettua mediante:
- **Estrazione fisica dei chip,** de-saldatura a calore o prodotti chimici per i collanti
- **Pulizia e riparazione dei Chip**
- **Acquisizione dei raw data mediante copia Forense**
- **Analisi delle copie forense**

Questa metodologia necessita di una **Camera Bianca**
Poco utilizzata in italia per via dell'alto costo di intervento

TECNICHE DI ANALISI DATI SU MOBILE
Elenco di categorie di evidenze che possono essere estratte:

- **Elenco dei Contatti**
- **Registro delle chiamate**
- **SMS e MMS**
- **Cronologia della navigazione**
- **Foto e video**
- **Musica e documenti**
- **Agenda**
- **Posizioni**
- **Mappe**
- **Dati di social network**
- **Dati cancellati**

Queste evidenze contengono generalmente dei:

- **Timestamp di Creazione**
- **Timestamp di Modifica**
- **Timestamp di Accesso**

TECNICHE DI ANALISI DATI SU ANDROID – TOOLS A RIGA DI COMANDO
Le tecniche di analisi che possono essere utilizzate sono le stesse utilizzate nell'analisi forense di sistemi linux
ES. Sleuthkit é una collezione di tool Open Source per l'analisi forense di filesystem e dispositivi
Per le **evidenze** che possono essere estrattr dai dispositivi mobili c'é da considerare che spesso sono contenute all'interno di **database SQLite**
Caso dell'acquisizione fisica della flash memory:

- L'accesso a tale file non é cosí immediata.

AUTOPSY
Tool open source di analisi forense inizialmente nato come interfaccia grafica web based per il tool Sleuthkit ma diventato poi un tool standalone per sistemi Windows.
Autopsy é a conoscenza di dove **trovare le evidenze sui sistemi Android**, é possibile caricare un **immagine** derivante da **acquisizione fisica o logica** di un dispositivo.

TECNICHE DI ACQUISIZIONE DATI SU DISPOSITIVI IOS
Al fine di analizzare ed estrarre i contenuti della memoria é necessario conoscere come sono organizzati i dati al suo interno.
La **memorizzazione in IOS** avviene nella **memoria flash** in cui lo spazio é diviso nelle seguenti partizioni:

- **Partizione di Sistema**: Ospita i dati del **sistema operativo** e delle applicazioni native. Scarso interesse per gli operatori forensi, ma utile per vedere se é stato modificato il Sistema operativo
  - **Accesso sola Lettura**: Durante il normale funzionamento del Device
  - **Accesso Lettura e Scrittura**: Durante gli aggiornamenti di sistema
- **Partizione Dati**: Occupa il restante spazio della memoria e contiene i dati dell'utente durante il normale utilizzo del device.
  - **Contenuti Generativa**
  - **Scaricati**
  - **Sincronizzati**

MEMORIZZAZIONE DEI DATI
La memorizzazione dei **dati utenti** e delle **applicazioni** avviene con **modalitá diverse**:

- **Parte organizzata all'interno del filesystem**
- **Parte File Database SQLite**: Contenenti informazioni persolani

MECCANISMI DI PROTEZIONE E JAILBREAK
Meccanismi di sicurezza implementati su IOS per controllare l'accesso a funzionalitá e dati del dispositivo.

Tecniche di JailBreaking: Tecniche che permettono di disabilitare le protezioni "di jail" sfruttando alcune vulnerabilitá della piattaforma. **Vanno a sostituire**, temporaneamente o definitivamente, **il kernel originale con uno modificato e privo di protezioni**

ACQUISIZIONE DI UN DISPOSITIVO
Alcuni passi fondamentali per l'acquisizione dei dati quando si ha nelle mani un dispositivo acceso:

- **Attivare la modalitá aereo**
- **Collegarlo ad una sorgente elettrica**
- **Individuare lo specifico Modello, la versione del sistema operativo**
- **Prevenire che il dispositivo vada in blocco (**disabilitando l'auto-block**)**

Varie soluzioni e casistiche:

- **Dispositivo non protetto da nessun meccanismo di blocco**: Posssiamo accedere tranquillamente a tutti i contenuti
- **Dispositivo Bloccato**: Occorre sbloccarlo per accedere ai contenuti
  - **Dispositivo protetto da codice**: É possibile tentare di **Bypassare il blocco** tramite **brute force**
  - Se il **brute force** non puó essere effettuato:
    - **Ottenere il certificato di LockDown**: Se si ha un computer con il quale ci si é connessi al dispositivo, all'interno di questo é presente **il certificato di lockdown.** Tramite questo certificato **é possibile eseguire un backup o acquisizione attraverso Apple File Relay**
    - **Sfruttare le Vulnerabilitá del SO**: Se si conosce una vulnerabilitá della versione del Sistema Operativo in uso, é possibile sfruttarla

DISPOSITIVO IOS BLOCCATO

- **Il dispositivo é fino ad IOS 7 ed é disponibile un certificato di lockdown**
  - É possibile eseguire un applicazione basata su **Apple File Relay** utilizzando il lockdown
- **Il dispositivo é fino a IOS 7 e non é disponibile un certificato di lockdown**:
  - Si puó tentare soltanto una metodologia **Brute Force** per codici che permettono la risoluzione in tempi ragionevoli
- **Il dispositivo é fino ad IOS 8 ed é disponibile un certificato di lockdown**:
  - É possibile eseguire un'acquisizione tramite **Apple File Conduit**
- **Il dispositivo é fino ad IOS 8 e non é disponibile un certificato di lockdown**
  - Se il dispositivo é a 32bit é possibile utilizzare un servizio offerto **Cellebrite** per eseguire un acquisizione
- **Il dispositivo é uguale o successivo alla versione IOS 9**
  - Con gli strumenti e le tecniche note non é possibile effettuare nessun tipo di acquisizione

TECNICHE DI ACQUISIZIONE DATI SU IOS – DISPOSITIVO SBLOCCATO
Se si hanno le credenziali di accesso all'account iCloud é possibile effettuare un accesso online per ottenere:

- **Backup**
- **Calendario**
- **Contatti**
- **Foto**
- **Email**

É possibile effettuare **JailBreak** ed utilizzare strumenti come **Elcomsoft IOS Forensics Toolkit**.
Se il dispositivo ha giá il **jailbreak** é meglio, altimenti é bene eseguire la procedura come ultima alternativa

ANALISI DATI SU IOS
Elenco di software utilizzabili:

- Commerciali
  - **Cellbrite Physical Analyzer**
  - **MPE+**
  - **XRY**
  - **Oxygen**
- Open/Free/Trial
  - **iBackupbot**
  - **iPhone Backup Extractor**
  - **iExplorer**
  - **iPhone Backup Analyer**

DIGITAL FORGERY E NON SOLO

DIGITAL FORGERY

IDEA ALLA BASE DELLA MULTIMEDIA FORENSICS
La Multimedia Forensics si basa sull'idea che tracce intrinseche siano lasciate in un supporto digitale sia durante la fase di creazione che in qualsiasi altro procedimento successivo

OBIETTIVO DELLA MULTIMEDIA FORENSICS
Creare algoritmi per contrastare il forgering delle immagini

AMBITI DELLA MULTIMEDIA FORENSICS
- **Source Identification**: Identificazione della sorgente
  - Device Class Identification: Identificare che tipo di dispositivo ha elaborato il file
  - Model Identification: Identificazione del modello del dispositivo che ha elaborato il file
  - Camera Identification: Identificare quale fotocamera ha elaborato il file multimediale.
- **Integrity Detection**
  - Forgery Detection: Capire se l'immagine é stata manipolata
  - Forgery Location: Trovare in quale punto l'immagine é stata manipolata
- **Counter Forensics**

COS'É UN FORGERY
Un forgery é un'alterazione di un file multimediale. Un'immagine puó diventare un falso in base al contesto in cui viene utilizzato.
Un forgery é definito soprattutto dalla tipologia di utilizzo che noi ne facciamo.
- **Inteso come autenticitá e non integritá**, a volte si puó dire che un immagine con del forgery é autentica ma non integra.
- **Utilizzato per scopo di lucro**, Creare un immagine al solo scopo di ingannare il destinatario facendogli credere che sia reale per scopo di lucro

TIPOLOGIE DI FORGERY
Tre tipologie di forgery sono identificabili:
- **Immagine Creata**: Immagine creata con l'utilizzo di un software grafico o generata dall'Intelligenza Artificiale
- **Context Modified**: Contesto dell'immagine cambiato, falsificato per diversi fini.
- **Content Modified**: Contenuto dell'immagine alterato, con aggiunta, rimozione o modifica di elementi

DIFFERENZA TRA CONTESTO E CONTENUTO
- **Contenuto**: L'immagine viene manipolata a tal punto da sembrare un altra immagine a tal punto da cambiare anche significato
  - Gli oggetti dell'immagine vengono:
    - Rimossi
    - Aggiunti
    - Duplicati
  - Il miglior modo per manipolare degli oggetti nelle immagini é quello di utilizzare un software di editing
- **Contesto**: L'immagine non viene alterata totalmente ma viene solo decontestualizzata dal vero significato

Alterare le immagini non é una pratica nuova

WPP REPORT: L'INTEGRITÁ DI UN IMMAGINE
Per la prima volta viene definito ció che é realmente un'immagine alterata, ovvero, **un'immagine alterate é un'immagine alla quale sono stati aggiunti o sottratti digitalmente degli elementi**

Il ritocco in colori e intensitá luminosa potrebbe non essere considerata un alterazione dell'immagine.

ESTRATTO DEL RAPPORTO

1. **XMP Analysis**: Analisi dei metadati di un file immagine. Molti processi o applicazioni per la manipolazione delle immagini possono lasciare in esse dei metadati proprietari in modo da far capire che l'immagine é stata manipolata
2. **Error Level Analysis**: Metodo utilizzato per identificare le aree all'interno di un'immagine che presentano diversi livelli di compressione.
3. **Shadow Analysis**: Processo utilizzato per Identificare e analizzare le ompre presenti in una scena

Il rapporto della WPP ha messo in atto questi tre strumenti per determinare se l'immagine presentata nella competizione del 2012 fosse stata alterato o manipolata.

NEGATIVO VS SENSORE: DUE EPOCHE A CONFRONTO

- **Epoca Analogica**: L'immagine era considerata **prova d'evidenza attendibile.**
- **Epoca Digitae**: L'immagine é considerata **prova d'evidenza da verificare.**

La differenza discende dalle diverse tecniche di formazione dell'immagine tra i due tipi di apparati:

- **Fotocamere Analogiche**: La pellicola veniva **impressionata dalla luce proveniente dal sistema di lenti**, essa **costituiva una sorta di matrice dell'immagine** da cui si potevano estrarre quante **copie identiche** si desiderava
- **Fotocamere Digitali**: L'immagine semplicemente **transita**, prima di essere salvata in memoria. Al termine del processo di acquisizione questa viene salvata o cancellata. La **matrice originale dell'immagine non esiste piú**

ALTERAZIONE DELLE FOTOGRAFIE ANALOGICHE
Poteva avvenire in due modi:

- **Agendo Fisicamente sulle pellicola**: Asportandone delle parti o aggiungendone altre e poi sviluppando il negativo modificato
- **Duplicando il Negativo**: Con apposita strumentazione, applicando delle opportune maschere per nascondere o inderire i particolari voluti

Richiedeva una conoscenza specifica, abilitá e strumentazione adatta

TECNICHE DI RILEVAZIONE

- **Esamina del Negativo**
- **Esamina delle diverse carateristiche del negativo-copia**

FORENSICS IMAGE AUTHENTICATION

Intendiamo l’applicazione delle tecniche informatiche per capire se il contenuto di un’immagine é stato manipolato o rappresenta l’esatta riproduzione degli eventi reali in base a criteri ben definiti.

Questi criteri riguardano l’**interpretabilitá dei dati** e non semplici modifiche di formato che non alterano il significato o il contenuto dei dati.

DEFINIZIONE DI IMMAGINE AUTENTICA

Un’immagine realizzata contemporaneamente agli eventi visivi accaduti e in maniera coerente con il metodo di registrazione dichiarato dalla parte di chi ha prodotto l’immagine, priva di artefatti, modifiche, aggiunte, cancellazioni o modifiche inspiegabili.

FILE ORIGINALE

Per verificare che un’immagine é stata scattata con una determinata fotocamera bisogna:

- **Acquisire l’immagine che ipoteticamente ha scattato**
- **Procurarsi una fotocamera identica alla fotocamera dichiarata**
- **Scattare una foto**
- **Controllare i metadati e i parametri delle due foto**

Se nel confronto si evince che i parametri sono simili o uguali, allora l’immagine in questione é stata scattata da quella fotocamera

AMPED AUTHENTICATE permette di paragonare:

- **Print o Attributi delle foto**
- **Identifica i parametri mancanti o sfalsati**
- **Fornisce talvolta le informazioni del programma che si é utilizzato per la manipolazione del’immagine**

IDENTIFICARE L’AUTENTICITÁ

Studiare gli elementi caratterizzanti le immagini:

- **Luci**
- **Contrasto**
- **Ombre,** Direzione e Intensitá

TASSONOMIA DI MANIPOLAZIONI

- **Miglioramento** (NON FORGERY)
  - Equalizzazioni dell'istogramma
  - Modifiche del colore
  - Regolazione del contrasto
  - Filtraggio
  - ...
- **Modifiche Geometriche** (PUNTO DI MEZZO DALL'ESSERE FORGERY)
  - Rotazioni
  - Zoom
  - Ritaglio di parti dell'immagine
  - ...
- **Modifiche del Contenuto** (FORGERY VERO E PROPRIO)
  - Taglia e incolla
  - Copia e Incolla
  - Seam Carving
  - ...

Authenticate permette di identificare le aree clonate

COMBINAZIONI DELLE TASSONOMIE

La combinazione di queste tassonomie da vita a diversi tipi di **Elaborazioni**:

- **Innocua**: Miglioramento + Modifiche Geometriche
  - Ritenuta un elaborazione che non crea danno o falsi alibi
- **Maliziosa**: Modifiche Geometriche + Modifiche del Contenuto
  - Elaborazione al fine di creare danno o falsi alibi
  - Cambia la semantica dell'immagine:
    - **Aggiungono Informazioni**
    - **Rimuovono Informazioni** (Tecniche di Match Processing, Background tramite Interpolazione)

IMAGE FORENSICS

Tecniche per rivelare le anomalie nelle immagini.

Esistono diversi approcci:

- **Attivi**
  - **Watrermarking**: Aggiunta di watermark (impronte aggiunte ai dati, visibili o invisibili)
    - Usate per dimostrare la proprietá del file multimediale
  - **Cryptographic digital Signature**: Hash code
    - utilizzati per mantenere l'autenticitá e l'integritá dei dati
- **Passivi**
  - **Image Forensics**
    - **Steganalysis**: Nascondo dati all'interno dei file
    - **Tampering/Fogering Detection**: Comprendere se l'immagine presenta artefatti nel dominio spaziale e nel dominio delle frequenza
    - **Source Identification**
      - Computer Graphics
      - Scanner
      - Camera
        - Modello

IMAGE FORENSICS METHOD – WATERMARKING

Metodo attivo che permette di nascondere un segno (firma) o un messaggio in un'immagine che é stata creata.

Limitato alle:

- Fotocamere digitali appositamente attrezzate
- Non cosí robusto come metodo

La compressione JPEG potrebbe rimuovere queste informazioni

TIPOLOGIE DI WATERMARK

- **Visibili**
  - Immagine visibile, traslucida e quasi trasparente sovrapposta all'immagine principale
- **Invisibili**
  - Immagine sovrapposta all'immagine principale che non puó essere vista, ma puó essere rilevata tramite algoritmi

WATERMARK FRAGILI

Progettati per rilevare ogni possibile cambiamento nei valori dei pixel.

In molti casi il Watermark Fragile viene incorporato nel bit meno significativo (LSB).

Considerazioni:

- **Vantaggi**
  - Rilevano tutte le manipolazioni dell'immagine, sia maliziose che non
- **Svantaggi**
  - Sono troppo sensibili e possono dare falsi positivi

WATERMARK SEMI-FRAGILI
Watermark piú robusti, e meno sensibili alle modifiche dei pixel
Tecniche:

- **Dividere l’immagine in blocchi e utilizzare i bit di ciascuno per calcolare un rumore a spettro diffuso come il segnale che é combinato con i coefficienti DCT e inserito come filigrana**
- **Dividi l'immagine in blocchi, costruisci filigrana in DCT dominio dalla varianza unitaria pseudo-casuale a media zero in Numeri gaussiani, prendere la DCT inversa e inserirla in un'immagine**

IMAGE AUTHENTICATION
Esistono tre metodi per verificare l’autenticitá di un’immagine:

- **Visual Inspection**
- **File Analysis**
  - Formato del file e struttura
  - Matadati (EXIF)
  - Parametri di compressione (Tavole di quantizzazione)
- **Global Analysis**
  - Statistiche dei pixel e dati
- **Local Analysis**
  - Trovare inconsistenze tra i pixel dell’immagine

VISUAL INSPECTION
Possibilitá di trovare inconsistenze temporali o della scena

CAMERA-BASED
Agiamo a livello di file ed anche a livello di camera per capire il flusso di acquisizione di un’immagine
Lente → CFA → Sensore → Interpolazione → Post Processing → Immagine Digitale → Memorizzazione

IMAGE FORENSICS METHOD – PASSIVE
Utilizzano le alterazioni delle statistiche sottostanti prodotte dalla digital forgeries in un immagine
Elenco di metodi:

- **Physics Based**
- **Camera Based**
- **Pixel Based**
- **Geometric Based**
- **Format Based**

TIPI DI ANALISI – LIVELLO DI SCENA
Se avremo migliori risultati sull’unione, avremo meno risultati sulle manipolazioni (forgery)

- Pysics Based:
  - Lighting: Inconsistenze di luce, potrebbero rivelare tracce di manipolazione
- Geometry and perspectibe inconsistencies:
  - Principal Point Analysis
  - Shadows
  - Photogrammetry

LIGHT SOURCE
Nelle immagini le sorgenti di luce ci permettono di:

- **Vedere la luce che colpisce un oggetto**
- **Vedere la direzione della luce**

A volte grazie alle sorgenti luminose é possibile rivelare inconsistenze che permettono di rivelare se un'immagine é autentica o meno.
ES. Se voglio rilevare problematiche legate alla luce é possibile verificare gli occhi del soggetto inquadrato

SHADOW
La geometria delle Ombre puó essere analizzata con delle linee.
Le luci e le ombre spesso contengono le risposte per dire se un'immagine é reale o é stata elaborata.
La posizione di un ombra fornisce informazioni sulla luce circostante nella scena
Come verificare se un'ombra é veritiera:

- **Per ogni punto al di fuori dell'ombra, deve esserci una linea verso la fonte di luce che sia ostruita dall'oggetto stesso**

Nel caso delle ombre, le linee che collegano i punti di un oggetto e la loro ombra convergono su un'intersezione comune

REFLECTIONS
Fenomeno visivo che é suscettibile ad un'analisi lineare.
Una scena riflessa da uno specchio é spesso disorientante ma per la geometria é un semplice ragionamento.
Un oggetto riflesso in un vetro fotografato risulterá come se fosse una linea continua che entra dentro lo specchio alla stessa distanza che c'é tra oggetto e vetro
Nel caso delle riflessioni, le linee che collegano i punti di un oggetto e la loro riflessione convergono su un'intersezione comune

LENS FLARE
Rifleso luminoso causato dai raggi di luce che passano attraverso le lenti dell'obiettivo fotografico. Questo effetto si verifica quando la luce si riflette all'interno dell'obiettivo anziché colpirlo direttamente, **creando delle aree chiare o cerchi di luce nell'immagine**
Grazie ad esse possiamo avere un idea della posizione della sorgente di luce che colpisce la lente.

TIPOLOGIA DI ANALISI – A LIVELLO DI SEGNALE
Basato sulle caratteristiche statistiche dei valori dei pixel. Bisogna avere un'immagine di qualitá per poter utilizzare questo tipo di analisi
Due tipologie di analisi del segnale:

- **Clone Detection**
  - Blocchi di immagine clonati
  - Coppie simili di punti chiave
- **Resampling Detection**
  - Analisi per la scoperta della ridimensionamento, rotazione, splicing o cloning
- **Enhancement Detection**
  - Analisi per scoprire il miglioramento dell'immagine
- **Seam Carving Detection**
  - Scoprire se viene utilizzato un Algoritmo per il ridimensionamento intelligente
- **General Intrinsic Footprints**
- **Inconsistencies from acquisition and coding FingerPrint**
  - CFA, PRNU, DCT, ELA

DIGITAL FORGERY – CONCETTO DI PHOTOSHOPPING
Per Photoshopping si denota l'azione volta a falsificare digitalmente medicine, scene di guerra ed in generale immagini digitali di qualsiasi natura.

COPY-PASTE FORGERY
Basato sulla ricerca di blocchi che sembrano ripetersi nell'immagine.
Se il numero di elementi adiacenti ripetuti é piú alto di una euristica la regione risulta alterata

RESAMPLING
Al fine di generare una contraffazione avvincente di ricorre ad operazioni di:
- **Ridimensionamento**
- **Rotazioni**
- **Deformazioni di proporzioni**

Consiste nel ricampionare l'immagine di partenza in una nuova griglia di destinazione, generando in questo modo felle correlazioni periodiche nei dintorni dei pixel manomessi.

Come si procede se si hanno sospetti:
- **Prendere in input l'immagine**
- **Le coordinate utili ad inviduare l'area di ricerca**
- **Regione di cui si vogliono individuare i possibili cloni**
- **Range relativi alle posibili trasformazioni geometriche considerate**

L'area di ricerca individua l'area entro cui ricercare gli eventuali cloni della patch ad esclusione dela stessa patch

PROCEDERE IN CASI REALI
Possibili trasformazioni:
- **Rotazione**
- **Scala Lungo l'asse X**
- **Scala Lungo l'asse Y**
- **Crop sui 4 lati**
- **Flip Orizzontale**

METRICA DI SIMILARITÁ
Come metrica di similaritá si puó generalmente ritenere sufficiente ai nostri scopi la:
- **MAE**: Media delle differenze in valore assoluto tra la regione di input e il suo possibile clone

MAE: Valore numerivco tra 0 e 255, **misura quanto due regioni siano simili tra loro tenendo conto della differenza pixel per pixel delle regioni corrispondenti.** MAE pari a 0 indica che le due regioni sono uguali

CAMERA-BASED
Tecniche di digital forensics che basandosi su determinati artefatti introdotti dai vari stadi dell'elaborazione dell'immagine all'interno delle fotocamere, determinano un collegamento univoco tra fotocamera e immagine.

CHROMATIC ALBERRATION
É la rifrazione della luce in due dimensioni.
La luce policromatica entra nella lente ed emerfe con un angolo che dipende dalla lunghezza d'onda.

FORMAT BASED: JPEG
Regola fondamentale dell'indagine forense é ovviamente quella della conservazione dei dati originali.
La compressione lossy delle immagini JPEG puó essere considerata un nemico dell'analista forense
La perdita di dati sia utilizzata come ottimo strumento per l'individuazione delle manomissioni

STANDARD JPEG
Acroninmo di flusso di compressione dell'immagine di Byte

JFIF: Standard che definisce:
- **Registrazione del campione dei componenti**
- **Risoluzione e proporzioni**
- **Spazio di colore**

EXIF: Permette di integrare un ulteriore informazione al file

EXIF
Si tratta di una serie di informazioni che la tua fotocamera immagazzina al momento dello scatto.
Questi dati **offrono** una **panoramica sulla tua fotografia e sulle impostazioni utilizzate per ottenerla**.
EXIF agiunge alcuni tag di metadati come:
- **JPEG DCT**: Per i file di immagine compressi
- **TIFF**: Per i file immagine non compressi
- **RIFF WAV**: Per i file audio

Non é supportato in JPEG 2000, PNG o GIF
Oltre ai metadati lo standard specifica pure:
- **Dimendione dell'immagine**
- **Data e Tempo di acquisizione**
- **Caratteristiche sull'acquisizione:**
  - Tempo di esposizione
  - Bias di Esposizione
  - F-Number
  - Apertura
  - ISOLAMENTOLunghezza focale
  - Coordinate GPS
- **Thumbnail preview**

Controllare le informazioni EXIF puó dimostrare la possibilitá quasi certa di forgery

METADATI XMP
Standard dei metadati utilizzato dalle appicazioni Adobe.
I metasdati memorizzati in altri formati vengono sincronizzati e descritti con lo standard XMP in modo da poter essere visualizzati e gestiti piú facilmente

THUMBNAIL IN CASO DI FORGERY
In caso di forgery dell'immagine la **thumbnail EXIF resta sempre la stessa**

QUANTIZZAZIONE JPEG
Schema di compressione lossy permette di stabilire un grado di compressione dei dati.
I produttori delle fotocamere stabiliscono i diversi gradi di compressione selezionabili.
Le **differenze che fanno i vari produttori possono essere utilizzate per identificare la sorgente di un'immagine.**
Viene eseguita in blocchi 8x8 pixel

JPEG COME IDENTIFICAZIONE DELLA FOTOCAMERA SORGENTE
É possibile ottenere ulteriori informazioni dalla tabella di quantizzazione nell'header JPEG.
Problemi:

- Questi dati potrebbero non essere disponibili se l'immagine viene salvata in un formato differente o viene effettuata una ricompressione.
- Credibilitá delle informazioni scarsa, le informazioni possono essere facilmente rimpiazzate

COMPRESSIONE JPEG
Convertire un immagine a **JPEG** é un prosecco a sei passi:

- **Conversione da RGB a YcbCr**: Trasformazione dai dati raw RGB a YCbCr
- **Downsampling dei valori di crominanza**: Downsampling sui canali di crominanza
- **Suddivisione in blocchi 8x8**: Suddivisione dei canali in blocchi 8x8
- **Trasformata discreta del coseno DCT**: Applicata ai blocchi
- **Quantizzazione dei coefficienti DCT**: Coefficienti DCT quantizzati utilizzando tabelle fisse, perdita di dati
- **Compressione lossless**: Compressione senza perdita

Invertendo questo processo non si otterrá un'immagine identica all'originale per via della quantizzazione

FIRMA JPEG
Firma distintiva che puó essere utilizzata per collegare un'immagine a un tipo specifico di fotocamera.
In caso di discrepanza nell'immagine e quella della fotocamera utilizzata, vuol dire che l'immagine é stata risalvata dopo la registrazione iniziale.
Un'immagine risalvata non vuol dire che é stata alterata, ma potrebbe esserlo.

QUANTIZZAZIONE
Utilizzata per convertire un segnale continuo in uno spazio discreto.
Ogni immagine deve avere da una a quattro tabelle di quantizzazione, come stabilito dallo standard.
Viene applicata in blocchi 8x8 dell'immagine

$$B_{j,k} = round\left(\frac{G_{j,k}}{Q_{j,k}}\right)$$

G= Matrive dei coeffficienti DCT non quantizzati
Q= Matrice di quantizzazione
B= Matrice dei coefficienti DCT quantizzati

Una volta **stimata la tabella di quantizzazione** é possibile **ricostruire l'immagine originale** per identificare eventuali anomalie.
Si puó creare una **Mappa di errore** che viene utilizzata per **evidenziare le aree con caratteristiche diverse rispetto all'immagine originale** indicando le **parti manipolate**.

IDENTIFICAZIONE TRAMITE DCT

Ricerca concentrata sull'analisi delle correlazioni tra

- **Coefficienti di quanrizzazione** (QT)
- **Trasformata discreta del coseno** (DCT)

Tecniche per il rivelamento delle manipolazioni:

- **Misurazione degli artefatti di blocco**
- **Esposizione di manipolazioni digitali tramite JPEG Ghosts**, i fantasmi JPEG sono delle proprietá della compressione JPEG che non contengono informazioni rilevanti

MANUALE OPERATIVO

In caso di studio di un immagine bisogna seguire questi passaggi:

- **Proprietá del file**
- **Metadati** (EXIF, XMP, ecc.
- **Thumbnail**
- **Parametri di Codifica**
- **Vedere se tutto coicide con quello dichiarato** (Modello camera, risoluzione, tabelle di codifica)
- **Anomalie nei contenuti:**
  - Cut&Paste
  - Luce

DIGITAL CAMERA IDENTIFICATION: CAMERA BASED METHOD

IDENTIFICAZIONE DELLA CAMERA

Identificare il dispositivo é utile in tibunale per stabilire l'origine delle immagini presentate come prova.

I metodi forense che riescono a capire che due filmati provengono dallo stesso dispositivo possono far capire molte cose agli investigatori, come ad esempio, stabilire collegamenti tra diverse entitá o soggetti

L'identificazione della camera viene avviene tramite il suo FINGERPRINT, basato su:

- Pattern legato al rumore del sensore, a volte due modelli identici di camera hanno questo pattern simile, ma pur sempre diverso
- Dati derivati dal particolare formato (RAW, EXIF, codifica JPEG)

COLOR FILTER ARRAY

Griglia di filtri colorati posta all'interno del sensore che alterna tra**:**

- **Rosso**
- **Verde**
- **Blue**

Viene utilizzata dal sensore della camera per catturare l'immagine

Inoltre il **CFA** (Color Filter Array) é una griglia di disposizione periodica quindi é possibile individuare una **Firma Digitale** associata all'interpolazione del colore.

Demosaicing: Processso che permette di ricostruire le componenti mancanti per ogni pixel, **viene utilizzato per ottenere un immagine a colori**. Tramite l'interpolazione fornisce correlazoini statistiche specifiche tra sottoinsiemi di pixel nei tre canali di colore.

RUMORE

Fluttuazione casuale, non desiderata, dei valori dei pixel di un'immagine, Causata da diverse fonti di imperfezioni durante il processo di acquisizione dell'immagine.

Principali fonti di rumore:

- **Rumore del Fotone**
- **Rumore Termico**
- **Rumore di Lettura**
- **Rumore di Reset**
- **Rumore di Modello**
- **Rumore di Quantizzazione**

Ogni fotocamera ha un sensore con un **rumore univoco**, che consente di **identificare il sensore da cui proviene un'immagine** (mbare ripete sempre la stessa minchia sta materia)

Le **differenze tra sensori** sono dovute alle **minuzie nella loro costruzione e assemblaggio**, quindi é **improbabile che due camere generino lo stesso rumore**

Rumore a modello fisso FPN: Causato dalle correnti oscure, differenze pixel-to-pixel quando il CFA non é esposto alla luce

Rumore di non uniformitá della risposta alla luce PNRU é composto:

- **Non uniformitá dei pixel** (PNU): Dovuto alla sensibilitá dei pixel alla luce e dalle imperfezioni nella produzione del sensore
- **Difetto a bassa frequenza**: Quanto i pixel sono condizionati dai riflessi

ANTIFORENSICS

Scienza che riesce a capire se il PNRU é stato affiunto maliziosamente da un umano.

Il processo di falsificazione maliziosa di un'immagine coinvolge l'intenzionale rimozione del rumore a modello fisso per prevenire l'identificazione della fonte.

Se la **rimozione del PNRU non viene effettuata in modo corretto potrebbe generare artefatti che farebbero capire all'istante che l'immagine é stata alterata rispetto all'originale**

IMAGE AUTHENTICATION 2023/2024

IMAGE AUTHENTICATION

BEST PRATICE MANUAL: BPM

Regole che rappresentano le migliori pratiche da seguire per evitare errori durante l'esame e l'autenticazione delle immagini rilasciate dall'ENFSI.

Fornisce un quadro per le:

- **Procedure**
- **Principi di Qualitá**
- **Processi di Formazione**
- **Approcci all'Esame Forense**

L'autenticazione delle immagini mira a:

- **Fornire risultati affidabili**
- **Massimizzare la qualitá delle informazioni ottenute**
- **Produrre Prove Solide**

Esse non sono le uniche regole Best Pratices in ambito forense

DEFINIZIONI E TERMINI

Il BPM é composto da **quattordici sezioni**, ognuna dele quali é dedicata a una figuta specifica cooinvolta nel processo di autenticazione delle immagini.

L'EMSI regola il comportamento e le responsabilitá di ciascuna figura nel processo:

- **Case Leader**: Esaminatore capo del caso, responsabile:
  - Selezione
  - Proprietá dei Compiti
  - Assegnazione dei Compiti
  - Raccolta e Interpretazione dei risultati
- **Customer**: Persona, organizzazione, che richiede l'esecuzione dell'esame di autenticazione dell'immagine e che beneficia del rapporto forense
- **Examiner**: Persone indicate a condurre l'esame o gli esami di autenticazione dell'immagine
- **Terze Parti**: Intermediari che agiscono come inferfaccia tra il cliente e gli esaminatori, in grado di rivedere e redigere qualsiasi informazione fornita dal cliente che potrebbe influenzare gli esaminatore

ATTREZZATURA

Nei casi di autenticazione delle immagini l'hardware e il software devono essere:

- **Configurati**
- **Documentati**

Le attrezzature principali da considerare includono:

- **Computer**
- **Sistemi di Archiviazione**
- **Dispositivi Output,** display
- **Diverse categorie di strumenti software per analizzare**
  - Struttura dei file
  - Metadati
  - Contenuto Visivo
  - Analisi Globali e Locali

Le prestazioni e le capacitá degli strumenti dipendono molto dalla versione

STRUTTURE E CONDIZIONI AMBIENTALI
L'EMSI regola le condizioni ambientali dei laboratori informatici, con particolare attenzione alla:

- **Privacy**
- **Prevenzione dei BIAS che potrebbero influenzare l'addetto**
- **Condizioni di Illuminazione**
  - Quando si eseguono esami relativi all'ispezione visiva o si interpretano mappe di calore
- **Riservatezza del contenuto**
  - Cruciale per evitare problemi di pregiudizi

METODI
Necessario analizzare non solo i dati principali, ma anche i dati ausiliari.
ES. Nei video di sorveglianza anche l'orario é cruciale
Esistono **quattro aree di analisi**:

- **Analisi dei dati Ausiliari**: Metodi basati su **tutti i dati, tranne i pixel** dell'immagine
- **Analisi del Contenuto**: Metodi basati sui **dati pixel**
- **Strategia**: Indicazioni su come utilizzare questi metodi per eseguire attivitá di autenticazione
- **Peer Review**: Applicazione della peer review nel processo di autenticazione delle immagini, revisione alla pari dei contenuti scientifici

METADATI DEL FILESYSTEM
L'esame del FileSystem é importante perché contiene informazioni standard sui file archiviati, utili per la verifica e il confronto nell'autenticazione delle immagini.
Informazioni utili nel FileSystem:

- **Posizione del File**
- **Nome del File**
- **Valori Data/Ora**
- **Dimensione del File**
- **Flag di Funzionalitá del FileSystem**

Questi **valori** possono essere **modificati** da una normale **copia utente o estrazione.**
Importante verificare se i dati immagine siano stati ottenuti legalmente e se i metadati originali siano stati accuratamente conservati.

DATI CONTESTUALI RELATIVI ALL'ARCHIVIAZIONE O ALL'ELABORAZIONE
Oltre all'archiviazione basata su file system, esistono altre relazioni dirette tra un'immagine e il suo contenuto digitale.
Possono essere effettuati dei **controlli indiretti** sui dispositivi delle immagini su un computer:

- **Ricerca e revisione di immagini correlate**:
  - Immagini identiche in diverse posizioni, versioni meno elaborate che potrebbero essere originali o altre immagini che forniscono informazioni rilevanti
- **Ricerca di Software di Elaborazione delle immagini**:
  - Ed eventuali attivitá nei file di Registro e nelle directory temporanee, oltre alla ricerca nei recenti
- **Ricerca di Voci di Directory**
  - Vecchie, e non valide per trovare tracce di posizioni precedenti di un file e verificare la coerenza dell'utilizzo del blocco/cluster del file system

ANALISI DELLA STRUTTURA DEL FILESYSTEM
La maggior parte dei **file** é **strutturata** secondo **Formati Comuni**:

- **JFIF**
- **TIFF**
- **BMP**
- **PNG**
- **HEIF**

L'esaminatore deve considerare la versione del formato a cui un file potrebbe essere conforme e capire che **differnze nella struttura del file non implicano necessariamente manomissioni**.
Visualizzatori Esadecimali: Consente l'accesso ai dati grezzi e consente il controllo di eventuali interpretazioni effettuate da altri strumenti, Sostituite con **Strumenti semplificati**

ANALISI DEI METADATI INCORPORATI
I metadati descrivono parametri permanenti e variabili del dispositivo.

- Alcuni metadati sono necessari per la **decodifica e visualizzazione dell'immagine**
- Alcuni campi di metadati possono dipendere dall'inizializzazione da parte dell'utente come **nome del proprietario o data/ora**
- Molti metadati sono memorizzati in **strutture standardizzate e sono facilmente manipolabili**

Oltre all'immagine primaria i **dispositivi moderi** possono **memorizzare segmenti di dati aggiuntivi** come:

- **Miniature**
- **Immagini di Anteprima**
- **Brevi Video della scena**
- **Dati sulla Profonditá della scena**
- **Aree di Rilevamento Volti**

Questi dati possono essere **usati per confronti con l'immagine primaria e altri file di riferimento per verificare coerenze o incongruenze**

Gli elementi di **metadati aggiunti da strumenti di elaborazione delle immagini** possono essere distinti. ES Tabelle di quantizzazione di Abobe Photoshop
I **Metadati** possono contenere **collegamenti a file esterni.** ES. File di registro del software di elaborazione delle immagini

ANALISI DEL CONTENUTO VISIVO
Metodi che rilevano**:**

- **Caratteristiche visive**
- **Verificano se il contenuto di un'immagine puó essere una cattura di una scena reale**

Le immagini reali devono **rispettare vincoli fisici** come:

- **Dimensioni degli oggetti rigidi**
- **Regole dell'Ottica e della Geometria**

INCOERENZE OTTICHE
Le incoerenze ottiche possono essere dovute a tantissime cose:

- **Ombre**
- **Oggetti Trasparenti**
- **Oggetti Riflettenti**
- **Sfocature**

(Non parlo di ste cose perché é giá stato fatto nella parte di Digital Forgery)

ARTEFATTI
Distorsioni visibili, derivabili da vari fattori:

- **Proprietá della scena**
- **Distorsione Ottica**
- **Sfocatura**
- **Rumore**
- **Manipolazioni**
- **Sitesi dell'immagine** (ES. DeepFake)
- **Compressione con Perdita** (Causando blocchi, contorni e danneggiamenti)

Per **determinare** se un **artefatto** é dovuto al **normale processo di generazione dell'immagine o a manipolazioni** bisogna **paragonare l'artefatto con l'immagine di riferimento**

ANALISI GLOBALE
Si concentra sul rivelare le tracce di elaborazione applicate a un'immagine durante il suo ciclo di vita sfruttando il fatto che le manipolazioni possono lasciare segni all'interno dell'immagine stessa.
Consiste in una Descrizione compatta, singolo valore, grafico o statistiche aggregate, che devono essere interpretati dall'esaminatore.
Utile per orientare ulteriori analisi a livello locale.

ANALISI LOCALE
Si concentra sulla localizzazione delle aree manipolate all'interno di un'immagine
Esempi di manipolazioni locali includono:

- **Giunzione di immagini**
- **Clonazione**
- **Modifica di gruppi di pixel per cambiare**
  - Colore
  - Nitidezza
  - Dimensione
- **Sintetizzazione di Pixel**
- **Utilizzo di Impainting**
- **Utilizzo di Reti Neurali**

ANALISI DELLA FONTE
Il processo di classificazione del dispositivo sorgente delle immagini si suddivide in:

- **Tipologia Sorgente**
- **Marca**
- **Modello**
- **Software del Dispositivo**
- **Dispositivo Esemplare Specifico**

ANALISI DI INTEGRITÁ
Si verifica se un'immagine é originale e quali processi di elaborazione influenzano il risultato dell'analisi, considerando le fasi di:

- **Formazione**
- **Storia dell'immagine**

REVISIONE DEI REQUISITI DEL CLIENTE
Fondamentale prima di avviare un qualsiasi esame in laboratorio.
É essenziale:

- **Comprendere**
- **Concordare**

Lo scopo dell’esame con il Cliente
Si deve valutare cosa é:

- **Tecnicamente Fattibile**
- **Vantaggioso per le sue necessitá**

Questo processo puó includere diversi passaggi cruciali come:

- **Verificare la chiarezza dei requisiti del cliente**
- **Esaminare le Limitazioni di Costo**
- **Gestire Questioni di riservatezza**
- **Definire le Prioritá del Cliente**
- **Tradurre le Domande e Dichiarazioni del cliente on proposte**
- **Richiedere Informazioni aggiuntive**

VERIFICA PRELIMINARE DELLA PRESUNTA PROVENIENZA
La verifica preliminare della presunta provenienza delle immagini implica diverse considerazioni:

- **Valutare la provenienza dichiarata delle immagini**, inclusa la storia di come sono state ottenute dal sospettato
- Esaminare se **le informazioni** fornite dal Cliente **sono coerenti con le immagini ricevute** (ad esempio, confrontare se è stato inviato un originale o una semplice schermata).
- Se le **informazioni sulla provenienza sono incomplete o non fornite**, **contattare il Cliente** per risolvere eventuali discrepanze.
- Durante l'esame tecnico approfondito, se **non sono disponibili informazioni sufficienti sulla provenienza, il responsabile** del caso dovrebbe **cercare di determinarle** utilizzando metodi di analisi appropriati.
- Prestare **attenzione al ciclo di vita delle immagini**, dalle fasi precedenti al sequestro fino alla gestione e all'invio, per garantire l'integrità e l'accuratezza delle informazioni
- **Evitare modifiche non intenzionali o non dichiarate alle immagini** durante le varie fasi del ciclo di vita, come alterazioni dei metadati o ricompressioni non segnalate.

L'obiettivo è assicurare che le informazioni siano complete, accurate e affidabili durante tutto il processo di esame forense delle immagini.

PRIORITÁ E SEQUENZA DEGLI ESAMI
La priorità e la sequenza degli esami sono fondamentali nell'analisi forense delle immagini. Inizialmente, **si valuta il valore probatorio degli elementi disponibili** per **ottimizzare il rapporto costi/benefici**.
Le priorità dipendono:

- Dagli **elementi specifici da esaminare**
- Dalle **richieste formulate**
- Dalle **risorse disponibili** come gli esaminatori e gli strumenti tecnici.

Per quanto riguarda la **sequenza degli esami, non esiste una regola rigida applicabile a tutte le attività di autenticazione**. Tuttavia, di solito si segue un **approccio stratificato, procedendo dai test di base a quelli più complessi**, se necessario in fasi successive.
Le fasi includono:

- **Valutazioni iniziali**
- **Ricostruzione**
- **Varie analisi** come quella dei metadati, del contenuto visivo e approfondimenti del contesto digitale.

FUNZIONI DI ELABORAZIONE
Le funzioni di elaborazione delle immagini possono modificare le tracce all'interno di un'immagine, influenzate da vari fattori:

- **Acquisizione**: Caratteristiche dei dati dell'immagine come saturazione, risoluzione e modalità di ripresa.
- **Elaborazione interna alla fotocamera**: Implementazione dettagliata e parametri delle funzioni di elaborazione come impostazioni dei filtri e tecniche HDR.
- **Post-elaborazione**: Fasi successive di elaborazione come compressione, conversione e ridimensionamento applicate ai dati dell'immagine.

Nella **creazione di immagini** di riferimento, è **cruciale cercare di riprodurre l'intero ciclo di vita ipotizzato dell'immagine**, **includendo acquisizione, elaborazione interna alla fotocamera e post elaborazione**.
Tuttavia, è importante notare che ci sono **molteplici metodi per ottenere una determinata modifica**, il che rende **difficile determinare la catena esatta di elaborazione delle immagini in alcuni casi**.

PRESENTAZIONE DEI RISULTATI
Al termine dell'esame, i **risultati dell'autenticazione delle immagini possono essere presentati oralmente o per iscritto**, garantendo **onestà, integrità, obiettività e imparzialità**. I **rapporti scritti** indicano **fino a che punto si possono rispondere alle domande specifiche del caso**, **dettagliando** le **caratteristiche osservate** relative all'autenticazione dell'immagine. I dati di supporto devono essere conservati per garantire la ripetibilità dell'analisi.
Durante **la presentazione orale**, gli esperti dovrebbero **limitarsi** al loro **campo di competenza**, dichiarando i limiti e i rischi coinvolti se si risponde a domande al di fuori di esso.

FINE CORSO DF 2023/2024
SAMUELE CUCUZZA