IL PROCESSO GIURISDIZIONALE E L'ATTIVITA' DI CONSULENZA

Processo giurisdizionale.
Cos'è la giurisdizione. Giurisdizione significa tradurre un fatto accaduto nella realtà in termini giuridici. Perché c'è l'esigenza di questa traduzione? Perché bisogna portarlo a processo. Si parla di un processo patologico della realtà, perché quando si svolge tutto nella liceità non c'è bisogno del processo. Ma quando lede il diritto di qualcuno si va a processo. Quando c'è questa incertezza, la storia passa a giudizio di un giudice che dirà chi ha ragione e chi ha torto. All'uomo della strada che accade qualcosa, ritiene che ha subito una lesione del suo diritto porta al giudice la conoscenza di quel fatto, il giudice traduce i fatti in termini giuridici.

Giurisdizione: processo giurisdizionale. Serie di fasi procedurali al termine del quale si stabilisce chi ha ragione e chi ha torto, oppure pareggio.
Il processo è un processo articolato, serie di attività che servono per far si che il giudice si possa convincere di ciò che è accaduto per poter decidere in maniera rispondente al sistema giuridico.

L'organizzazione dello Stato.
Basato sul vissuto della nostra nazione. Se si ripartisce il potere è più facile avere uno stato democratico, "separazione dei poteri".

Principio della "separazione dei poteri" (Locke, Montesqueiu).
Con la funzione legislativa lo stato pone le norme costitutive dell'ordinamento giuridico.
Con la funzione amministrativa lo Stato svolge un'attività' effettiva e concreta diretta al soddisfacimento dei suoi fini immediati (l'attività' di governo, i rapporti internazionale, la sicurezza pubblica, la tutela della salute, l'amministrazione finanziaria, il benessere economico, la difesa del territorio, la crescita culturale, …)
Con la funzione giurisdizionale lo Stato accerta la volontà' normativa da far valere in un caso concreto ed emette le sanzioni, assicurando così' la certezza del diritto e la reintegrazione dell'ordine giuridico violato.

Con la funzione legislativa lo Stato pone le leggi che tutti debbono osservare attraverso il legislatore. Il **parlamento**, attraverso la sua composizione, pone le leggi. Camera e Senato, svolgono la stessa funzione, ma formati da persone con requisiti diversi. Queste due camere svolgono la funzione legislativa, attraverso un procedimento che porta la proposta di legge in legge. Questo progetto di legge passa attraverso le camere che ne discutono, la modificano, la migliorano. Quel testo approvato da una camera passa all'altra camera che la discutono. Quando entrambe approvano, è pronta per essere promulgata al Capo dello Stato. La legge a quel punto deve essere osservato da colore che insistono nel territorio italiano, anche se ha un periodo di tempo che deve trascorrere perché tutti si possano mettere in regola (15 giorni o diversi mesi). Le legge è un atto pubblico, significa che appartiene a tutti noi, senza diritto d'autore. La sua divulgazione è un intervento strategico per lo Stato.

Il potere amministrativo. Cioè il potere esecutivo, svolto da un altro organo dello stato: il **governo**. Organo strettamente politico, formato da quella maggioranza che è stata eletta alle elezioni politiche a suffragio universale nel paese. Il governo svolge la funzione di

eseguire le norme che provengono dal parlamento. Il governo esegue le norme attraverso i ministeri che sono specifici per tutte le materie che lo stato intende coprire, per cui ritiene sia necessario intervenire.

C'è un terzo potere. Il terzo potere è il potere giudiziario, che serve per fare chiarezza dove c'è
incertezza. Il potere giurisdizionale, è svolto da un altro organo, la **magistratura**.

Il potere giudiziario.
Per accertare l'esistenza o la violazione di un diritto si aderisce il giudice.
Il processo, in Italia, prevede tre gradi di giurisdizione. Ciò significa, che lo stato Italiano, per garantire il cittadino prevede che quella questione possa essere valutata tre volte, da tre giudici
diversi, affinché si arrivi ad una soluzione che sia quanto più corrispondente alla verità. I tre gradi, non sono strettamente necessari. La sentenza si può concludere anche alla prima sentenza. Però se una delle parti non è concordo a ciò che ha stabilito il giudice, si andrà a secondo grado. Idem per la terza.
Per il primo grado, conoscono le cause il giudice di pace. Giudice non togato, ma onorario. Cause non troppo rilevanti. Per cose più importanti aderisce il tribunale. Che può essere in versione monocratica o collegiale. Non per forza una sola persona, ma più persone. Il tribunale può' avere anche un una composizione collegiale.
Quando le questioni sono di una certa gravità, il primo grado è svolto dalla Corte d'Assise. Quando invece la questione riguarda un potere pubblico o il potere amministrativo, il primo grado viene conosciuto da un tribunale speciale, il TAR (Tribunale Amministrativo Regionale).
Es. il ricorso degli Esami di Stato.
Il processo di primo grado, dopo una serie di passaggi dal codice di procedura civile o penale, arriva ad una conclusione. La conclusione è un atto emanato dal giudice, che si chiama sentenza. E' il dettato del giudice, la sua idea su quella questione. Quando però una parte non è soddisfatto della sentenza può ricorrere in appello, il secondo grado di giudizio. È una garanzia per il cittadino per arrivare alla verità.
Per il giudice di pace e il tribunale, si ricorre alla Corte d'Appello. Per la corte d'Assise si ricorre alla Corte d'Assise d'Appello. Per il TAR al Consiglio di Stato.
La sentenza si chiama merito.
In secondo grado, il procedimento è svolto ex-novo.
Perché si dice che questi due gradi si dicono di merito? Perché i giudici entrano nel merito dell'accaduto.
Il terzo grado, è svolto da un unico organo, La corte suprema di cassazione. Svolge un giudizio di legittimità. Ovvero, guarda alla corretta applicazione delle leggi durante i primi gradi di giudizio, cioè se i giudici hanno applicato correttamente le norme giuridiche. In caso contrario, rimanda ai giudici la corretta interpretazione che torna ad un altro giudice di merito, che decide secondo indicazione della Corte di Cassazione, che è vincolante, cioè dovrà procedere secondo quelle indicazioni.
Tribunale dei minori, giudica questioni che coinvolgono giovani che non hanno ancora compiuto la maggiore età, che al suo interno ha dei psicologi infantili che riescono a comprendere meglio la questione.

Tribunale militare, per persone coinvolte in ambito militare.
Commissione tributaria.
Corte Costituzionale. Per verificare che una legge non sia in contrasto con la costituzione, c'è un giudice formato da 15 elementi che verifica se il dettato di una norma è contrario alla costituzione.
Tribunale superiore e regionale per le acque pubbliche.
Per i conti dello stato conosce le cause la Corte dei Conti.

L'arbitrato.
Riguarda soltanto le cause di diritto civile. Prevede la possibilità di rivolgersi ad un collegio arbitrale o arbitro per il potere decisionale. Come un contratto. Per ragioni economiche o di tempo. La decisione dell'arbitro è una sentenza che assume il nome di **Lodo**. Ci sono delle garanzie in questo contratto di risoluzione delle controversie. Intanto, le parti vengono sentite, e che il lodo sia motivato, cioè che l'arbitro deciderà un suo giudizio che deve esprime in motivazione. Tipicamente l'arbitrato si usa per questioni che vanno al di fuori del territorio italiano.L'arbitrato per risolvere le questioni a distanza, ad esempio online, è l'Online Dispute Resolution. Il Lodo ha valore di sentenza di primo grado, cioè nello stato italiano, se una delle parti può essere ricorsa in appello. Ciò significa che è garantito il secondo e terzo grado anche per l'arbitrato.

Il procedimento giudiziario.
Il precedente è costituito da un atto singolo cui si uniforma, in presenza delle medesime circostanze, all'attività dell'organo che lo ha posto in essere o di un diverso organo. Il giudice è sottoposto soltanto alle leggi, il suo convincimento deve essere dettato esclusivamente dalle leggi, e non dalla giurisprudenza.
Il nostro ordinamento (Civil law, diritto fondamentalmente scritto a differenza del Common Law dove è il giudice che crea il diritto) non ha alcun valore vincolante. A differenza del Common Law che è vincolante per il futuro. Una volta che la questione è decisa ed è incontrovertibile, la sentenza diventa immutabile, forma giudicata. Non è possibile giudicare di nuovo su quella questione.

Il procedimento giurisdizionale.
Diviso in due tronconi. Civile ed amministrativo e penale.

Nel processo civile ed amministrativo.
C'è un attore e il convenuto. Dato che il giudizio è un processo molto tecnico, non ci si può presentare in giudizio da soli, ma debbo essere rappresentato da un tecnico del giudizio che si chiama avvocato difensore che dovranno affrontare non solo le norme di diritto sostanziale ma anche le regole di procedura penale.

Nel procedimento penale.
C'è il pubblico ministero (accusa) che rappresenta lo Stato che è stato violato. Ad esempio l'omicidio, reato grave. Lo Stato è ferito perché non ha garantito il diritto alla vita. Per questo

scende in campo lo stato. Il PM è un magistrato requirente (non giudicante). Dall'altro lato c'è
l'imputato (accusato), ad esempio che ha commesso l'omicidio. Imputato che per norma, è considerato innocente fino alla sentenza, che interviene in procedimento per difendersi. Interviene nel processo per cercare di limitare i danni. In questo caso, c'è anche una terza figura, la parte offesa, che ha subito il danno. Nel caso del PM, non c'è bisogno di un avvocato difensore essendo già un magistrato, nel suo caso si può fare aiutare dalla polizia giudiziaria nella ricerca delle prove. Può anche avvalersi di un consulente tecnico specifico del pubblico ministero. Specifica professionalità che lo aiuta a comprendere, cercare o produrre delle prove per suffragare la sua tesi. L'imputato, invece, come la parte civile, interviene le processo tramite un avvocato. La parte civile supporta l'accusa del PM, avendo lo stesso interesse.
In mezzo a tutti, c'è il giudice, terzo rispetto alla causa. Non deve avere né preconcetti né interessi all'interno del processo. Il gioco del processo è convincere il giudice.
Ausiliare del giudice: cancelliere (per la parte amministrativa) e l'ufficiale giudiziario che esegue la sentenza.Se né il cancelliere né l'ufficiale giudiziario conoscono, o anno conoscenze necessarie, nell'ambito portato dalle parti, il giudice può richiedere la consulenza o l'intervento del consulente tecnico d'ufficio di un ambito specifico. Il consulente tecnico d'ufficio può aiutare il giudice nell'interpretare quelle che le parti producono. Se il giudice produce un CTU, le parti possono chiamare il proprio consulente tecnico, che si chiama CTP.Verità che si raggiunge al processo. Probabile che non si arrivi alla verità assoluta, ma è una verità processuale. Si fa di tutto per arrivare alla verità assoluta, ma non è facile, magari perché mancano elementi o qualcuno è stato particolarmente bravo a nasconderlo. Alla fine del processo si arriva alla conclusione. Non si può stare in eterno a cercare la verità assoluta.
Il risultato del convincimento del giudice è determinato dall'analisi delle prove.
Il diritto ricerca certezze nel rispetto delle forme. Le forme all'interno del diritto assumono forme di sostanza. Se rispetto una forma ho creato una sostanza, se non la rispetto non ho niente in mano. Es. ipotesi di reato previsto dal codice penale: inquinamento di un corso d'acqua. L'ambiente non è solo un mezzo, ma un fine. Si protegge direttamente l'ambiente. Inquinare l'ambiente è reato. La prova è costituita dalle analisi sui prelievi dell'acqua per vedere se sono superati i limiti. Sia il PM, sia l'imputato, sia le parti civili, devono essere messi in condizioni di poter esercitare il proprio diritto di difesa. Presenza delle parti nei momenti più importanti del processo.

Consulenti CTU e CTP.
Il consulente tecnico è necessariamente una persona fisica (quindi non una società) che assume l'incarico di espletare un'attività tecnica al fine di redigere una perizia. Se il giudice affida l'incarico ad un perito, assume il nome di Consulente Tecnico d'Ufficio. Nel caso penale, si chiama Perito del Giudice.
Se la parte o il difensore affidano l'incarico ad un perito, questo prende il nome di CTP.
La consulenza, può essere richiesta per il compimento di singoli atti o per l'intero processo.
I professionisti possono essere iscritti all'albo del tribunale. Oppure non iscritti ma hanno fama. Di norma il CTU è iscritto all'albo. Quando un CTU è iscritto all'albo e viene scelto da un giudice, questi assume la veste di pubblico ufficiale e deve prestare giuramento.
Invece, nel caso del CTP, è un rapporto di tipo privatistico, non di risultato ma di mezzi,

ovvero il suo incarico è fornire il mezzo.

Nomina del CTP.
La nomina può avvenire a cura del legale o direttamente dalla parte.
Occorre individuare l'ambito entro il quale deve svolgersi l'incarico e stilare un preventivo per il compenso. L'incarico di CTP è personale, non può essere conferito ad associazioni professionali o società di professionisti. Può essere sostituito, ma i poteri del sostituto sono limitati rispetto al CTP.

CTPM nel processo penale.
Art. 359 c.p.p.Consulenti tecnici del pubblico ministero
1. Il pubblico ministero, quando procede ad accertamenti,rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di consulenti, che non possono rifiutare la loro opera(se sono iscritti negli albi).
2. Il consulente può essere autorizzato dal pubblico ministero ad assistere a singoli atti di indagine.

Responsabilità del consulente tecnico.
I consulenti tecnici d'ufficio e di parte hanno l'obbligo di rispettare i principi di correttezza e buona fede e di comportarsi in giudizio con lealtà e probità.

Attivita' del consulente tecnico.
Art 194 cpc.
Il CTP interviene nelle attività peritali del CTU e può presentare, per iscritto o a voce, osservazioni e istanze.

Sostituzione del CTU. Se il CTU non è imparziale, non è più terzo, allora si deve astenere con una giusta causa. E' bravo il CTP che riesce a convincere il giudice al di là del CTU.

Cause di nullità.
Inosservanza del principio di contraddittorio.
Indagini del CTU eccedono le richieste del giudice, si dice che va *ultra petita*.
Garantire le operazioni successive sul computer per consentire di fare operazioni esattamente come quando è stato sequestrato. Analisi che si fanno sulla copia. Per garantire la ripetibilità dell'azione. La prova è l'elemento chiave. Tutte le prove che possono dimostrare un fatto sono ammesse, a meno che non siano inutili. Ma non ci sono delle prove precostituite che possono essere espedite. Se non è manifestamente impedita non può essere vietata.
Le prove devono essere ricercate, proposte, ammesse, assunte e valutate secondo il libero convincimento del giudice. Ad eccezione della confessione, oppure l'atto pubblico. Il valore della prova sta nella prova stessa. Tranne se entra in gioco un giudizio di falsità (falsi in atti d'ufficio).

Atti invasivi su sistemi informatici e telematici.
LEGGE 18 marzo 2008, n. 48

Ratifica ed esegue la Convenzione del Consiglio d'Europa sulla criminalità informatica, siglata a Budapest il 23 novembre 2001.
Introduce alcune disposizioni correttive ed integrative al codice di procedura penale mediante le quali, sinteticamente, nei casi di intervento invasivo sui sistemi informatici e telematici …
- si dovranno adottare "misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione";- la copia dei dati deve avvenire con una procedura che assicuri la conformità dei dati copiati e la loro immodificabilità.

La prova.
La parte può avvalorare ciò che afferma con qualunque mezzo di prova, salvo che siano vietate dalla legge, manifestamente superflue o irrilevanti.Le prove devono essere ricercate, proposte, ammesse, assunte e valutate secondo il libero convincimento del giudice (salvo le prove legali). La **prova scientifica** consiste nell'applicazione di metodi scientifici nella ricerca delle evidenze a dimostrazione di un fatto, di un accadimento, di un risultato rilevante per l'economia del processo,ai fini della ricostruzione del fatto storico che si presume sia accaduto.
Il principio eziologico (nesso di causalità - se … allora …) regge l'efficacia della prova scientifica, in generale.
La prova scientifica è valida se ammette la verifica e se è assunta in contraddittorio.

CRIMINI INFORMATICI

Non c'è più un settore che non si appoggi a tecnologie dell'informazione e della comunicazione. Così come tutti i fenomeni sociali si sono trasposti all'interno dell'informatica, anche il fenomeno criminale interessa in misura sempre più maggiore i sistemi e le applicazioni informatiche. Ovviamente, parlando di crimini informatici ci riferiamo al diritto penale. Branca del diritti che si occupa di reprimere i fenomeni che ritiene maggiormente lesivi per l'interesse dello stato. Compromettendo l'ambiente si compromette anche la salute pubblica. Ci sono tanti reati che tradiscono la fede pubblica. Se esibisco in un processo, in un atto pubblico, e qualcuno [..] Ci sono crimini contro lo stato stesso, minacce all'integrità dello stato. Dunque, il penale, deve considerarsi all'interno del diritto un'estrema ratio.
Quando ci sono atti lesivi nei confronti del patrimonio, si attivano le norme di diritto penale.
Estrema ratio perché attraverso la parte sanzionatoria, di ledere, creare nel soggetto che subisce il procedimento penale un forte cambiamento (reclusione ovvero privare la libertà di un soggetto). Nel momento che lo stato ci impone questa sanzione, sono tutti atti che limitano la libertà individuale. Ovviamente non tutte le sanzioni penali comportano la reclusione. Alcune incidono sul patrimonio, tu hai sbagliato, vieni condannato e paghi. Quando l'illecito penale è più grave allora si paga con la reclusione. L'ergastolo è una pena reclusiva, "a vita", che non si estende oltre i trent'anni. La pena di morte è stata abolita da un po' di tempo, cosa che non è così in tutti i paesi.

Principi che governano il diritto penale nel nostro sistema giuridico.

Lo stato per controllare il potere lo ha diviso in tre parti. La divisione dei poteri in uno stato come il nostro che prima pone le norme giuridiche e poi le risposte. Il diritto ha come corollario il divieto di retroattività della legge penale. Non si può essere giudicati per un fatto avvenuto prima dell'avvenire della legge. Questo principio deriva dall'intuizione da Feuerback "null apoena sine lege". I giuristi, a proposito di questo punto, parlano di funzione general preventiva penale. Di queste norme esplicita quali sono le conseguenze del mancato rispetto delle stesse. Ovvero, so qual è la pena a cui vado in contro se commetto quel reato.
La nostra costituzione, cioè la nostra legge di riferimento, porta questo principio all'articolo 25 comma 2. Questo principio è stato anche trasposto nella convenzione europea per la salvaguardia dei diritti dell'uomo e della libertà.

Nozioni generali di diritto penale.
Illecito: comportamento antigiuridico
Reato: Fatto che dipende dall'operato dell'uomo, anche di natura omissiva, al quale l'ordinamento giuridico ricollega una sanzione penale
Responsabilità personale: la responsabilità penale muore con colui che ha commesso il reato.
Diritto di difesa: Tutti hanno diritto di difendersi, anche chi coloro che non hanno le possibilità economiche. E' un diritto inviolabile. Principio ripreso dalla nostra carta costituzionale.
Soggetto attivo e passivo. Soggetto attivo (agente) colui che agisce e soggetto passivo (chi subisce il reato). Nel caso di un omicidio subisce colui che muore ma anche la famiglia.
Procedimento di ufficio: se lo stato viene a conoscenza di un fatto di reato si attiva per portare in ordine ciò che è stato turbato dal reato. CI sono dei casi, dei reati meno gravi, dove è necessaria un'azione specifica ad esempio la querela, perché lo stato si attivi è necessario che venga esposta una querela da chi ha subito il reato. In quel caso lo stato si attiva solo se chi ha subito le lesioni espone querela nei confronti di chi ma commesso il reato.
Reati comuni o reati propri: reati comuni, che possono essere commessi da tutti. Ci sono altri reati che si dicono propri perché possono essere commessi solo da qualcuno che riveste una determinata qualifica. La corruzione, è un reato proprio. Un uomo comune non può commettere corruzione, un pubblico ufficiale può commettere reato di corruzione. Molti reati informatici, sono colpiti in maniera più grave se a commetterlo è l'amministratore di sistema. Se l'amministratore di sistema commette il reato tradisce il suo incarico che avrebbe dovuto proteggere il sistema. Concetto uguale al custode del museo, che ruba un oggetto del museo, non sarà giudicato alla stessa maniera di chi entra nel museo e ruba il pezzo. Il custode sarà giudicato in maniera diversa, più pesante. Si parla di **facilità di commettere il reato**. Il reato proprio riguarda una specifica categoria di persone.
La pena deve tendere alla rieducazione del condannato. Ci sono diverse fasi del procedimento penale. Prima del processo, l'uomo che si suppone abbia commesso il fatto di reato è detto **indagato**.
Quando il PM, ritiene di aver raccolto sufficienti prove per richiamarlo in giudizio, il soggetto sarà **imputato**. Fin quanto è imputato, lo Stato lo considera innocente. Fin quando non si ha la sentenza definitiva, anche quando la fatto è evidente.

Nozioni di teoria generale del reato.
Reati di pericolo. La sola messa in pericolo, comporta il reato. Non devo commettere e produrre il reato. La condotta criminosa comporta la semplice messa in pericolo o lesione potenziale del bene oggetto alla tutela personale. Esempio: detenzione di armi. Il solo fatto di avere l'arma mi rende punibile dallo stato tramite il reato di "detenzione illegale di armi". Se la detenzione avviene senza il rispetto delle regole è reato. Mettere in potenziale pericolo un bene dello stato. Sotto il profilo psicologico invece, si costituiscono i reati di colpa e di dolo.
Reato di colpa. L'agente con la sua condotta pur potendolo prevedere non ha voluto il verificarsi dell'evento dannoso che si verifica a casa di negligenza, imprudenza, imperizia, per inosservanza delle leggi, ordini o discipline. Es: guida con il cellulare. Lo stato chiama in giudizio chi conduceva il veicolo e sarà incolpato di *omicidio colposo*.
Reato di dolo. L'agente con la sua condotta criminosa ha preveduto e voluto il verificarsi dell'evento dannoso o pericolo a danno del bene protetto.

Crimini informatici
Crimini che sono commessi per mezzo dell'elaboratore elettronico e reati commessi a danno dell'elaboratore elettronico. Parte della dottrina che ritiene che ci sia una terza specie, in cui il sistema agente è proprio il sistema informatico, ad esempio in un'ottica dell'intelligenza artificiale.

Software
L'articolo 171/bis punisce con la reclusione e la multa:
- chi abusivamente duplica al fine di trarne profitto programmi per elaboratori protetti (SIAE)
- chi predispone o utilizza qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicativi a protezione di un programma.
- chi riproduce su supporti non contrassegnati SIAE il contenuto di una banca dati al fine di trarne profitto.
Il termine profitto comprende anche colui che, in termini personali, commette questo tipo di attività non spendendo quel denaro necessario, rientrando così nella ragione di profitto.
Altri reati, riportati su codice penale.

Art. 653-bis c.p. "Danneggiamento di informazioni, dati e programmi informatici"
"Chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione... "
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore di sistema la pena della reclusione si aggrava.

Art. 635-quater c.p. 'Danneggiamento di sistemi informatici o telematici'"
"Chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione"

Art. 635-ter c.p. ‘Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità’
“Chiunque commette un fatto diretto distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l’alterazione o la oppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni”

Domicilio informatico.
Il domicilio informatico è il figlio del domicilio fisico. La violazione di domicilio è reato. Il domicilio informatico è la trasposizione del domicilio. Se il computer è protetto da username e password è come se stesse violando i cancelli di casa mia. Se uno entra, commette reato. Se lascio aperto non è reato. Non si può entrare se qualcuno non ci consente di entrare.

Art. 615-ter c.p. ‘Accesso abusivo ad un sistema informatico o telematico’
“Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo è punito con la reclusione ...”

Art. 615-quater c.p. ‘Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici’
“Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all’accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione e con la multa”

Virus.
Art. 615-quinquies c.p. ‘Diffusione di apparecchiature,dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico’
“Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l’interruzione, totale o parziale, o l’alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329”

Reati di Social Engineering.
Per “social engineering” si intende lo studio dei comportamenti individuali, attraverso tecniche di persuasione psicologica non necessariamente con strumenti informatici,volte a ricavare dati personali, password o informazioni segrete altrui, al fine di commettere uno o più reati.
Muove dalla propensione delle persone a rispondere a domande dirette e impreviste o ad aiutare qualcuno che sembra in difficoltà.

Phishing.
Tecnica di commissione del reato: invio di messaggi immediati o di posta elettronica del tutto simili a quelli provenienti da società/enti reali e affidabili, per carpire informazioni riservate.

Frode informatica.
Art. 640-ter c.p.
Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione e con la multa [...] La pena è aumentata se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno d i uno o più soggetti [...]

Documenti informatici.
Art. 491-bis c.p. 'Documenti informatici'
"Se alcuna delle falsità... (in atti) riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni (reclusione) ... concernenti gli atti pubblici."

Falsità materiale: contraffazione o alterazione del documento.
Falsità ideologica: dichiarazione mendace.

Art. 495-bis c.p. 'Falsa dichiarazione' o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri'
"Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno"

Art. 640-quinquies 'Frode informatica del soggetto che presta servizi di certificazione di firma elettronica'
"Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro"

Corrispondenza informatica.
Art.617-quater c.p. 'Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche'
"Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione"
La stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni (intercettate)

Art. 617-quinquies c.p. ‘Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche’
“Chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni ... è punito con la reclusione”

Art. 617-sexies c.p. ‘Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche’
“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno,forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione”

Pedopornografia.
Art. 600-ter, 3°co. c.p.
“Chiunque,...con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico [,,,], ovvero distribuisce o divulga notizie o informazioni finalizzate all’adescamento o allo sfruttamento sessuale di minori degli anni diciotto è punito con la reclusione e con la multa...”

Chiunque [...] offre o cede ad altri,anche a titolo gratuito, il materiale pornografico di cui al primo comma ...la pena è aumentata ... ove il materiale sia di ingente quantità. Chiunque assiste a esibizioni o spettacoli pornografici in cui siano coinvolti minori di anni diciotto.

Ai fini di cui al presente articolo per pornografia minorile si intende ogni rappresentazione (anche virtuale), con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

Art. 600-quater
Chiunque ... consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, è punito con la reclusione e con la multa …
La pena è aumentata ove il materiale detenuto sia di ingente quantità.

LA CONSULENZA TECNICA

Principi generali.
Obiettivo: rispondere al quesito “tecnico”.
Elementi essenziali:
- Estremi del procedimento (e ruoli)
- Testo del quesito
- Premesse tecniche

- Dati di lavoro (acquisizione, provenienza)
- Metodologia di lavoro
- Analisi tecnica
- Conclusioni
- Allegati tecnici
- Referenze bibliografiche alle best practice di settore

Forma.
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**, e **valutazione**.
La presentazione è fondamentale.
La relazione di presentazione dei risultati deve essere redatta in forma comprensibile, perché i destinatari (giudici e avvocati) non hanno di solito conoscenze informatiche approfondite; di contro le loro conoscenze legali potrebbero consentir loro di sostenere la nullità, per vizio di forma, nella relazione finale dell'analisi forense.
Infatti la relazione dell'analista forense e' di solito esaminata dal tecnico e dal legale della controparte. Essi possono opporsi alle conclusioni dell'analisi forense sia dal punto di vista tecnico sia dal punto di vista legale.
In genere la presentazione dovrebbe essere:
- Semplice
- Chiara
- Completa
- Professionale

condivisibile, perché completa, professionale e documentata.

Contenuti.
Parte epigrafica.
Vanno indicati gli estremi del procedimento, e può essere utile per comodità di lettura riportarvi i quesiti, nonché riassumervi le posizioni delle parti relativamente a quegli aspetti che sono attinenti all'oggetto della consulenza.

Parte narrativa.
E' la parte in cui deve essere riportato lo svolgimento delle operazioni peritali (eventualmente anche allegando il verbale delle operazioni compiute) e riassunte le eventuali osservazioni, obiezioni o istanze mosse dalle parti o dai rispettivi consulenti. L'obbligo di inserire questi ultimi aspetti è contemplato direttamente dall'articolo 195 c.p.c. nel quale e' previsto che nella relazione il consulente "inserisce anche le osservazioni e le istanze delle parti". Pur essendo obbligatorio la S.C. ha comunque sancito che la mancata indicazione nella relazione delle istanze della parti e dei loro consulenti o l'omessa verbalizzazione delle operazioni peritali, non comportano la nullita' della Consulenza Tecnica.

Parte descrittiva.
In essa il consulente/perito mette in rilievo il materiale e la documentazione utilizzata ai fini della consulenza, esponendo i fatti sui quali ha basato il proprio convincimento e dunque elaborato le risposte ai quesiti.

Parte valutativa.
In questa parte della consulenza il consulente/perito esprime il proprio giudizio:
- ricostruendo e motivando la fattispecie che è stato chiamato ad accertare e valutare

- esponendo in modo analitico il risultato della propria indagine

Parte decretiva.
Si tratta della parte finale della consulenza, nella quale il consulente/perito riassume il lavoro svolto, fornendo risposte specifiche e concise ad ogni singolo quesito.

FORENSICS SCIENCE

La Forencics Science è l'applicazione di metodi tecnici e scientifici per il settore della giustizia, investigazione e scoperta di prove.

Storia della disciplina.
La prima nozione di Digital Forencics risale agli anni settanta ma è durante gli anni ottanta che si afferma nella ricerca di prove digitali. Negli anni novanta si afferma la Digital Forencics. Il primo workshop (Digital Forencics Research Workshop) si tenne in Utica (New York) nell'agosto del 2001, dove fu data la prima definizione di Digital Forencics Science come: "L'uso di metodi scientificamente provati al fine di preservare, collezionare, validare, identificare, analizzare, interpretare, documentare e presentare delle evidenze digitali derivate da risorse digitali con lo scopo di facilitare e favorire la ricostruzione di eventi criminali, o aiutare a prevenire azioni non autorizzate volte ad essere di disturbo".
Possiamo quindi riassumere, dando la definizione di Informatica Forense come la disciplina che studia le attività di individuazione, conservazione, protezione, estrazione, documentazione ed ogni altra forma di trattamento ed interpretazione del dato digitale memorizzato su supporto informatico, al fine di essere valutato come prova nel processo.

Il dato digitale.
I dati rappresentano le entità base su cui operano i sistemi informatici come applicazioni software, email, feed, il web, ecc.
Le autorità precedenti (law enforcer) nell'ambito delle loro attività d'indagine, si avvalgono sempre più di tali dati che, una volta correttamente acquisiti ed analizzati, possono assumere valore di prova contribuendo significativamente all'identificazione e persecuzione dell'autore del materiale dell'illecito.

Tipologie di reato.
Reati tradizionali o comuni che vedono il computer come strumento.
Reati relativi a contenuti come ad esempio la distribuzione di materiale illegale o illecito.
Reati di danneggiamento come la distribuzione di virus.

Dati informatici in ambito forense.
Il dato informatico gioca un ruolo importante nei procedimenti aventi come oggetto:
- Reato informatico
- Reato commesso con l'ausilio di strumenti informatici
- dati (o informazioni) aventi valore di prova o indizio per reati informatici e non
- strumenti (supporti) di archiviazione di reati rilevanti

Limiti dell'informatica forense.
Anche la disciplina dell'informatica forense, come tutte le altre discipline, ha dei limiti:
- Estrema facilità di alterazione dei reperti
- Facile creazione ad arte di elementi probatori
- Difficile riconducibilità dei reperti ai veri autori
- Necessità di trovare riscontri (in maniera quasi paranoica)

Competenze del tecnico.
Il consulente tecnico deve avere due importanti competenze. Una parte tecnica, quindi duplicazione di dati e analisi, ricostruzioni di timeline, archeologia informatica, reti e protocolli, redazione di rapporti tecnici solidi e una parte giuridica, con una terminologia adeguata, conoscenza delle norme e delle problematiche di giurisdizione.

Il problema centrale della materia, ha a che fare con il materiale utilizzato. Il materiale informatico è infatti di natura intangibile e volatile, specialmente in ambienti di rete o nella live forencics. È quindi necessario l'utilizzo di tecniche scientifiche e analitiche alle reti di computer, a dispositivi digitali e a file per scoprire o recuperare evidenze ammissibili nel procedimento penale.
La tecnologia rende il processo d'investigazione e raccolta dei dati a fini probatori estremamente vulnerabile per i diritti delle parti interessate (in particolare la difesa tecnica) e soggetto al rischi di malfunzionamenti tecnici, danneggiamenti o contraffazioni. L'insieme dei processi e delle tecniche utilizzate vengono definite "pratiche migliori (**best practices**).

Evidenze digitali.
L'aspetto caratteristico dei reperti virtuali delle evidenze è dato dalla volatilità, dalle infinite possibilità di riproduzione mediante procedure rapide e dalla necessaria interpretazione ai fine intellegibili. Le alterazioni possono intervenire per cause legate alle attività ordinarie del computer o da un uso incauto degli operatori: è difficile determinare quali siano i cambiamenti effettuati con la conseguente impossibilità di ristabilire la situazione ex-ante.
L'esame di evidenze digitali può richiedere molto tempo. Quindi chi effettua le indagini è di solito accurato e cauto quando raccoglie gli elementi di prova. Solitamente una **copia primitiva**, originale, intatta è prodotta per il successivo esame e i dispositivi sono restituiti alle loro applicazioni.

Tipi di dati.
Gli elementi di prova digitale comprendono:
- Il contenuto di una trasmissione
- Gli attributi o metadati dell'attività di comunicazione
- Il diritto alla privacy degli utenti delle reti
- La gestione di una risorsa informatica

La fonte di qualsiasi informazione digitale è data dalla sua rappresentazione attraverso la codifica binaria. Le leggi trattano i differenti tipi di dati forensi in maniera diversa. A ciò consegue un diverso regime giuridico di trattamento.
Altri tipi di dati (tmp file):
- Dati in memorie virtuali e file di swap
- History file dei browser
- History file in internet
- File temporanei nelle reti informatiche
- Link di collegamento
- File di log
- Metadati
- File di informazioni
- Web based emails

Obiettivi principali:
- Proteggere il sistema sospetto
- Scoperta di tutti i file

- Recupero di file cancellati
- Recupero di contenuti da file nascosti
- Accesso a file protetti o criptati
- Uso di steganalisi per l'identificazione di dati nascosti
- Analisi dei dati su spazi non allocati o di slack
- Fornire un'opinione sull'architettura di un sistema
- Fornire testimonianze o consultazioni di un esperto

Catena di custodia.
Quando si ha a che fare con un'evidenza informatica, bisogna seguire *the three C's of evidence:* ***care, control and chain of custody****.*
Procedure da seguire:
- Tenere un log dell'evidenza che registri quando questa è stata sequestrata e ricevuta e dove è stata locata
- Registrare le date degli elementi rilasciati a qualcuno
- Limitare l'accesso alle evidenze
- Collocare l'hard drive originale in una custodia delle evidenze
- Effettuare tutte le operazioni su una copia dell'originale e mai sull'originale

Le cinque fasi del reperto informatico.
- Identificazione: rivelare cosa è effettivamente utile per l'indagine. Quindi sistemi informatici, sistemi di comunicazione, supporti di memorizzazione esterna e supporti non digitali di informazione (documenti, post-it, password, modalità di accesso a sistemi complessi)
- Acquisizione: duplicare le informazioni in maniera fedele all'originale tramite clonazione, immagini bit-a-bit o immagini bit-a-bit compresse con l'obiettivo di acquisire il maggior numero di dati (possibilmente tutti), rendere l'attività di acquisizione ripetibile e limitare i tempi di inattività del servizio. L'acquisizione deve essere **completa, accurata e incontaminata**. Chi effettua le indagini deve poter ottenere i dati in modo completo con interferenze minime sui dati originali sotto esame. Tali dati possono essere stampati e copiati, anche se questo porta a variazioni nei metadati associati, con la possibilità di creare vulnerabilità. Pertanto la tecnica più utilizzata per ottenere dati forensi è quella dell'**imaging**. Un'**immagine bit-stream** di un dispositivo di memorizzazione digitale, ad es. hard disk o smart card, viene acquisita e creata in modo non invasivo includendovi le parti non occupate da dati interesse. Vengono generate più copie: una master e alcune di lavoro per tutte le parti processuali coinvolte. L'imaging consente di restituire i dispositivi originali al proprietario che così può 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 atte a verificare l'autenticità e l'integrità dei dati dopo il processo di acquisizione e la generazione di successive copie. A tal fine si utilizzano i digest ottenuti tramite apposite funzioni hash.

Funzioni Hash.
Il digest di un file (successione di bit) e' una stringa di simboli di lunghezza predefinita generata dall'applicazione di una funzione di hash sul file stesso,
DPCM 8 febbraio 1999: "L'impronta di una sequenza di simboli binari e' una sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione hash".
Non e' possibile risalire dal digest al testo originale.
Collisioni dello stesso valore del digest da due fonti diverse sono quindi pressoché impossibili.
Nel linguaggio tecnico, la funzione hash e' una funzione non iniettiva (quindi non invertibile)

che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. Esistono numerosi algoritmi che realizzano funzioni hash con particolari proprietà che dipendono dall'applicazione. Nelle applicazioni crittografiche si chiede, per esempio, che la funzione hash abbia le seguenti proprietà:
- Resistenza alla preimmagine: sia computazionalmente intrattabile la ricerca di una stringa di input che dia un hash uguale a un dato hash;
- resistenza alla seconda preimmagine: sia computazionalmente intrattabile la ricerca di una stringa in input che dia un hash uguale a quello di una data stringa;
- resistenza alle collisioni: sia computazionalmente intrattabile la ricerca di una coppia di stringhe in input che diano lo stesso hash.

MD5.
L'acronimo MD5 (Message Digest algorithm 5) indica un algoritmo crittografico di hashing realizzato da Ronald Rivest nel 1991, standardizzato con la RFC 1321.
Questo tipo di codifica prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 128 bit. La codifica avviene molto velocemente e l'output restituito e' tale per cui e' altamente improbabile ottenere con due diverse stringhe in input lo stesso valore di hash.
Ad oggi sono disponibili molte risorse online che hanno buone probabilità; di riuscire a decriptare parole comuni codificate.
Ad oggi, la disponibilità di algoritmi efficienti capaci di generare stringhe che collidono (ossia che producono in output lo stesso valore di hash) in un tempo ragionevole che reso MD5 sfavorito rispetto ad altri algoritmi di hashing, sebbene la sua diffusione sia a tutt'oggi molto estesa.

SHA (Secure Hash Algorithm)
Il termine SHA indica una famiglia di cinque diverse funzioni crittografiche di hash, sviluppate a partire del 1993 dalla NSA e pubblicate dal NIST come standard federale del governo USA.
Gli algoritmi della famiglia sono denominati SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. Le ultime quattro varianti sono spesso indicate generalmente come SHA-2, per distinguerle dal primo. Il primo produce un digest di soli 160 bit, mentre gli altri producono un digest di lunghezza di bit pari al numero indicato nella loro sigla.
SHA-1 e' il più diffuso algoritmo della famiglia SHA ed e' utilizzato in numerose applicazioni e protocolli. Rotto nel 2017.

Analisi.
Mettere in evidenza i dati con contenuto informativo importante per l'indagine sia a favore sia a sfavore. E' importante documentare il processo di analisi ed eseguirla su una copia bit a bit dell'originale e deve essere riproducibile.

Valutazione.
Interpretare I dati evidenziati in fase di analisi per sostenere le proprie tesi, sia a favore sia sfavore.

Presentazione.
Documentare cosa e come è stato fatto, cosa è emerso e cosa significano I dati emessi.
Adattare il registro all'interlocutore tecnico e giurista.

Dispositivi di memorizzazione.
La memorizzazione nei dispositivi digitali avviene a diversi livelli: a livello fisico, come le

particelle magnetiche e le incisioni create dal laser e a livello logico, in termini di partizioni, dispositivi tracce e settori.
Le modalità 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. Servono dunque tecniche di analisi diverse per esaminare I dati memorizzati da essi.
Nei diversi file system, i dati non sono necessariamente memorizzati in posizioni contigue ma sono frammentati in blocchi che sono logicamente associati tra loro tramite informazioni di indirizzamento.

Cancellazione di dati.
La cancellazione di dati sui supporti digitali può presentarsi in forme diverse:
Se effettuata da una applicazione standard rimuove solamente l'indirizzo dell'informazione associata a ogni blocco di dati, che logicamente connette I vari blocchi che costituiscono I contenuti dei file. I file che sono cancellati vengono rinominati in un'altra directory (es. Cestino, unused space).
I dati rimangono sul supporto, e sono recuperabili parzialmente, fintanto che non siano completamente sovrascritti da nuovi dati o cancellati tramite appositi strumenti (es. Software di wiping). La rappresentazione fisica residua dei dati cancellati viene detta permanenza dei dati, ed è una delle cause del problema della cosiddetta "viscosita'".

Slack space.
Area (compresa tra l'ultimo bit e la fine del settore) non utilizzata dal file che ha allocato lo spazio per l'ultimo.

IMAGE AND VIDEO FORENSICS

"Forencics Image (Video) analysis is the application of IMAGE SCIENCE and DOMAIN EXPERTISE to interpret the contest of an image or the image itself in legal maters" (SWGIT, FBI).

Autenticità e integrità.
Autenticità non significa integrità.
Definiamo autentica un'immagine che rappresenta accuratamente l'evento originale.
Definiamo integra un'informazione che non e' stata alterata dall'acquisizione fino alla disposizione.
Le operazioni come compressione e upload/download su piattaforme web mantengono la proprietà di autenticità ma non quella di integrità. Viceversa, le operazioni di ricattura di un'immagine falsa o lo staging mantengono l'integrità ma non l'autenticità.

File originali: casi speciali.
Ricattura: creare un'immagine falsa e successivamente fare una foto con una fotocamera con cui vogliamo far sembrare di aver scattato la foto.
Staging: il file dell'immagine è autentico, ma il contenuto è stato cambiato.
In entrambi I casi, l'autenticità dei file non implica l'autenticità dei contenuti.

Linee guida per l'autenticazione forense di immagini.
Analisi del file.
1) Analisi del formato;

2) Analisi dei metadati;
3) Analisi dei thumbnail e preview;
4) Analisi del formato JPEG
5) Analisi binaria;

Analisi globale dell'immagine:
1) Analisi dei coefficienti DCT;
2) Analisi della correzione dei pixel;
3) Analisi di luminosità e colori;

Identificazione del dispositivo:
1) Analisi globale del PRNU

Analisi locale dell'immagine:
1) ELA
2) Mappa DCT
3) Mappa di probabilità
4) Mappa del rumore
5) Analisi locale del PRNU
6) Analisi dei cloni

Analisi dettagliata della scena
1) Analisi dell'illuminazione
2) Analisi della geometria

Capire quando è possibile fare qualcosa.
Qual è la qualità minima per un video? La qualità minima non esiste.
Il successo del miglioramento dipende da molti fattori:
1) Obiettivo principale (il video e' stato catturato con una camera HD ma la targa che dobbiamo estrarre e' troppo lontana)
2) Dettagli tecnici rilevanti: Risoluzione dell'area di interesse. Livello di compressione. Presenze di sfocatura o messa a fuoco. Numero di frame disponibili. Rumore, luminosità e contrasto.
E' importante capire quali difetti sono presenti nell'immagine in modo da poter applicare in ordine gli strumenti adatti.

Fattibilita' del miglioramento.
Esempio dato un singolo fotogramma in cui si vede una targa composta da tre pixel bianchi non sara' mai possibile ottenere nulla.
Per quanto riguarda il miglioramento di targhe, che è senza dubbio una delle richieste più comuni, l'esperienza ci consente di affermare che se la risoluzione verticale della targa non e' almeno 12,15 pixel, non e' possibile ottenere alcun miglioramento significativo.

Da un video molto buio caratterizzato da un rumore elevato, spesso se si hanno a disposizione abbastanza fotogrammi e' possibile recuperare un dettaglio.
Se la ricostruzione e' adeguata e la compressione non eccessiva, anche con sfocature molto pesanti è possibile ottenere un'immagine nitida.

Correzione prospettica.
I pixel vengono "ridisegnati" mediante una opportuna trasformazione geometrica.

Implicazioni in ambito forense.
Il dato digitale è per sua natura molto sensibile a manipolazioni. Risulta semplice (ed economico) da manipolare.
Diverse problematiche in ambito investigativo/forense da gestire:
Che differenza c'è tra miglioramento e manipolazione dell'immagine? Quali elaborazioni sono ammissibili?
Digital Forgery: qual è l'originale? Qual è l'elaborato?

Valgono gli stessi principi della digital forensics per la trattazione dei reperti digitali:
1) Preservazione dell'originale
2) Acquisizione integra e non ripugnabile
3) Utilizzo di copie di lavoro
4) Documentazione e ripetibilità
In generale, ogni manipolazione tende ad evidenziare particolari presenti, non a cambiare I contenuti dell'immagine.
Le tecniche di Image (video) Forensics costituiscono sicuramente un ulteriore strumento di indagine a disposizione degli investigatori per poter estrarre ed inferire utili informazioni delle immagini (e del video) digitali anche nel caso di dispositivi mobili.
Per essere in grado di recuperare o di inferire delle evidenze di prova è comunque necessaria una adeguata competenza specifica che richiede uno studio sistematico dei fondamenti della teoria dell'elaborazione delle immagini e dei video digitali.
I software esistenti agevolano il lavoro degli investigatori ma non riescono per forza di cose ad automatizzare in maniera sistematica ed efficiente tali operazioni e richiedono l'ausilio di professionisti ed esperti.

LA PERQUISIZIONE INFORMATICA: TECNICHE, NORME E MODALITA' OPERATIVE

Perquisizione informatica.
Per scoprire la prova di un illecito, la perquisizione informatica è un approfondimento forense che viene sempre più richiesto dall'autorità giudiziaria, per la grande quantità di dati che si possono ottenere.
Il lavoro di consulenti e polizia giudiziaria inizia dall'isolare i sistemi dalla rete, procedendo ad approfondire ogni aspetto.
La perquisizione informatica e' sempre più utilizzata per individuare, acquisire e perseverare le informazioni.
All'interno delle memorie dei dispositivi vengono inviati, ricevuti e immagazzinati infatti dati essenziali per la vita quotidiana e lavorativa dell'uomo, utili in caso di indagini contro il cyber crime ma anche per reati non informatici.
Come viene spesso osservato, nella maggior parte dei casi, la prova dell'illecito e' sempre più abitualmente annidata nel dispositivo elettronico, anche tutte in quelle ipotesi in cui il sistema informatico non costituisce il destinatario dell'offesa né il mezzo attraverso il quale si è compiuto l'illecito.

La perquisizione consiste nell'attività di ricerca di determinati elementi che devono essere acquisiti al fine di renderli disponibili per l'Autorità Giudiziaria.
Viene deposta da un decreto del magistrato e nella maggior parte dei casi viene compiuta da ufficiali di Polizia Giudiziaria delegati, spesso accompagnati da Consulenti Tecnici e Ausiliari esperti della disciplina interessata. Nel nostro caso da uno o più consulenti in informatica forense.
L'atto di perquisizione personale o locale è normata dall'articolo n. 352 del c.p.p.
Mentre la legge n. 48 del 18 marzo 2008 rappresenta le norme e le best practices da seguire

per l'acquisizione della fonte di prova, in particolare del dato informatico, sancendo l'introduzione dei principi fondamentali della digital forensics all'interno del nostro ordinamento, prevedendo importanti aspetti legati alla gestione di quegli elementi di prova che, per loro natura, presentano caratteristiche di estrema volatilità e fragilità.
Seppur il legislatore si sia mossa cautamente nell'introdurre I nuovi principi per l'assunzione delle prove informatiche, non indicando cioè nel dettaglio le modalità dell'esecutorie da applicare nell'utilizzo di tali istituti, si e' comunque focalizzata l'attenzione su due basilari aspetti, sicuramente più vincolati al risultato finale che non al metodo da utilizzare, ovvero la corretta procedura di copia dei dati utili alle indagini e la loro integrità e non alterabilità in sede di acquisizione.

Gli strumenti del mestiere.
Il Consulente Informatico Forense deve presentarsi preparato all'appuntamento, e' opportuno che sia dotato di tutta l'attrezzatura necessaria ad effettuare copie forensi ed acquisizione in loco di dispositivi informatici e dati online. Un possibile kit di strumenti sono:
1) Numerosi hard disk di diverse dimensioni utilizzati per parallelizzare le acquisizioni di copie forensi da più dispositivi e per effettuare la duplice copia dei dati.
2) Duplicatori Forensi, come ad esempio il Ligicube Falcon e il Tableau TD1, TD2u, TD3, ecc per effettuare copie forensi di memorie quali hard disk, pendrive USB e memorie di massa.
3) Write blocker hardware e software per bloccare in scrittura le memorie collegate al PC.
4) Distribuzioni Linux su pendrive USB da avviare in locale come Kali Linux, Caine, Deft, ecc
5) Suite per acquisire dati da dispositivi mobili come smartphone, tablet o navigatori satellitari, come ad esempio Cellebrite UFED e Oxygen Forensics.
6) Software per acquisire dati presenti su servizi cloud di Google e iCloud ad esempio, come Cellebrite UFED Cloud Analyzer, Axiom Cloud e Elcomsoft Phone Breaker.
7) Tool per effettuare il download delle email, Securecube Imap Downloader e Thunderbird Portable sono tra I più utilizzati.
8) Suite di software portable per facilitare le fasi di acquisizione, come ad esempio FTK Imager Portable e Hash My Files.
9) Kit di cacciaviti, pinzette e strumentazione varia per smontare e rimontare dispositivi.

Quando si effettua una perquisizione in azienda, ad esempio, molto spesso la Polizia Giudiziaria e I consulenti in principio si recano presso l'abitazione dell'indagato alle prime ore dell'alba, prima che generalmente quest'ultimo esca per andare a lavoro o per andare a fare le proprie attività.
Se sono da effettuare perquisizioni in diversi obiettivi (vari indagati, diverse localita', abitazioni, proprieta' e pertinenze varie) le varie squadre dovranno sincronizzare gli accessi in modo da entrare su ciascun obiettivo contemporaneamente.

Le operazioni da effettuare.
La prima operazione svolta dall'autorità competente e' l'esibizione del **Decreto di Perquisizione** che autorizza le operazioni, in quanto prima di poter perquisire viene data la disponibilità di nominare un avvocato, un consulente tecnico di parte o di farsi assistere da una persona di fiducia.
L'autorita' giudiziaria puo' disporre che siano perquisite anche le persone presenti o sopraggiunte, quando ritiene che le stesse possano custodire o nascondere importanti fonti di prova.

Fase operativa.
Espletate le formalità può cominciare la fase operativa vera e propria:

1) individua
zione ed isolamento dei sistemi informatici (Pc, server, smartphone, tablet, ecc)
2) Individuazione ed isolamento di account online (email, file sharing, archiviazione online, ecc)
3) Richiesta di credenziali di accesso, codici di blocco, PIN e password e cambio delle stesse
4) Richiesta della presenza di dati cifrati e relativa password di decifratura
5) Perquisizione di tutti i locali e sequestro del materiale di interesse con descrizione dello stato e luogo in cui e' stato rinvenuto.

Una volta concluse le operazioni in abitazione queste ultime si trasferiscono in azienda.
Effettuato l'accesso ai locali vanno immediatamente isolati tutti I sistemi, facendo allontanare eventuali collaboratori e dipendenti dalle proprie postazioni di lavoro, al fine di quantificare il numero dei dispositivi da sequestrare o acquisire.
Subito va richiesta l'assistenza di un tecnico interno, se disponibile, per agevolare il lavoro e inquadrare immediatamente I componenti dell'infrastruttura informatica, specialmente per le aziende di grandi dimensioni. Ogni singolo elemento va isolato dalla rete, attivando la modalità aereo sui dispositivi e sui notebook, rimuovendo I cavi di rete dai pc fissi e dal server, ad esempio.
Durante le operazioni è necessario da parte dell'indagato mantenere la calma, risultare disponibili e collaborare con le forze dell'ordine al fine di concludere le operazioni nel minor tempo possibile ed evitare che avvenga il sequestro dei supporti informatici, la quale situazione porterebbe certamente ad un maggior disagio per i tempi di eventuale conferimento incarico per l'effettuazione della copia forense.
Una volta effettuate le operazioni di acquisizione a doppia copia di sicurezza va compilato assieme alla P.G. il verbale, andando a dettagliare tutte le operazioni tecniche effettuate inserendo anche I valori di hash che certificano le attività di copia forense effettuate.
Ovviamente al termine dei lavori tutti I componenti del sistema informatico, se non vengono sequestrati, vanno nuovamente resi disponibili e funzionanti, al fine di non recare danno interrompendo il processo lavorativo.

Il ruolo del Consulente Informatico Forense.
Viene di seguito proposto un esempio della giornata tipo che deve affrontare un Consulente Informatico Forense durante un processo di perquisizione:
1) Sveglia la mattina molto presto (partendo tante volte in piena notte) per raggiungere il luogo dell'intervento, solitamente la P.G. non comunica preventivamente l'indirizzo e il target esatto, al fine di non compromettere l'operazione ed evitare inutili responsabilità al CT.
2) Una volta riuniti tutti gli attori si cerca di fare un veloce punto della situazione, quantificando a grandi linee la mole di dati da acquisire e la tipologia di reato per cui si sta indagando.
3) Una volta terminata la fase preparatoria si effettua l'accesso ai locali, le forze dell'ordine mostrano il decreto e informano l'indagato delle operazioni che andranno effettuate.
Inizia quindi la fase di individuazione e ricerca delle evidenze di interesse, trattasi in questo caso esemplificativo di una smartphone Apple e un backup dello stesso salvato nell'area personale iCloud, un notebook con sistema operativo Windows 10, due pendrive USB, un account di posta elettronica Gmail e dei dati presenti sul server.
Subito vanno intercettati ed isolati ralle rete I dispositivi informatici.
Per quanto riguarda lo smartphone Apple, va richiesto il codice di sblocco, la presenza della cifratura iTunes e le credenziali per accedere all'account iCloud, la cui password deve essere immediatamente modificata.
Vanno poi individuate le credenziali dell'account Google, al fine di impedire l'accesso all'area

riservata.
Mediante procedura apposita si richiede il takeout, acquisendo oltre alle comunicazioni tutti I dati dell'universo Google, come cronologia delle ricerche web e Youtube, dati sul Drive, accessi, posizioni.
Sia per l'hard disk che per le pendrive USB va chiesto se I dati sono cifrati prima di acquisire l'intero contenuto della memoria mediante duplicatore forense, verificando quanto dichiarato.
Una volta avviato il processo va effettuata anche la copia forense dello smartphone Apple ed effettuato il download del backup iCloud.
Infine si potrà effettuare l'accesso al server. Individuati i dati di interesse che potranno essere acquisiti per esempio mediante il tool di acquisizione live FTK Image Portable.
Effettuare la copia forense dell'intero server sarebbe un incredibile spreco di tempo e risorse, operazione che prolungherebbe di molto le fasi operative, pertanto è sempre buona norma ragionare e consultarsi con la P.G. operante su quanto estrapolare.
Al termine del lavoro il consulente informatico Forense deve assicurarsi che le varie copie forensi siano integre e conformi alle originali, effettuare la doppia copia dei dati e restituire tutti I dispositivi funzionanti.
Infine va compilato il verbale di operazioni, letto e siglato da tutti I partecipanti, concludendo quindi l'operazione di perquisizione.

Ispezione informatica.
L'ispezione informatica è un mezzo di ricerca della prova, cioè una modalità con la quale il soggetto competente (la P.G., eventualmente avvalendosi di un ausiliario di P.G.) ispeziona dei supporti informatici per consentire all'Autorità Giudiziaria di verificare e acquisire direttamente o indirettamente le prove in formato digitale necessarie per procedere con l'indagine.
Da un punto di vista normativo, l'ispezione informatica e' disciplinata dall'articolo 244 del c.p.p. che, in maniera piu' ampia, regola le modalita' dell'ispezione.
Da un punto di vista operativo, l'ispezione informatica consiste nella ricerca di prove digitali all'interno di supporti informatici, quali ad esempio computer, tablet, smartphone ed ogni altro tipo di dispositivo digitale, utilizzando misure tecniche idonee ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.
L'ispezione informatica può essere ordinata dal Pubblico Ministero con decreto motivato la cui copia va consegnata all'interessato solo nel caso in cui l'ispezione e' relativa a luoghi o cose (ad esempio in caso di ispezioni su apparecchiature informatiche). L'ispezione informatica può' essere effettuata sia durante le indagini preliminari ad opera della P.G. (art. 354, 2 comma c.p.p.) o del Pubblico Ministero (art. 356 c.p.p.), sia durante il dibattimento ad opera del Giudice.
Nell'ispezione informatica, così' come in tutti I tipi di ispezione, il difensore dell'indagato, ha sempre e comunque il diritto di assistere e al preavviso per le ispezioni disposte dal giudice, tranne I casi di assoluta urgenza (art. 364 e 370 c.p.p.). Al termine dell'ispezione informatica va redatto un verbale nel quale vengono descritte nel dettaglio le operazioni e le attività' svolte, al cui interno devono essere presenti informazioni come:
- dettagli dei dispositivi ispezionati: tipo (ad esempio: notebook, smartphone, personal computer), serial number, marca, modello, ecc
- strumenti tecnici adottati per evitare alterazioni: ad esempio write blocker, marca, modello, versione
- dettagli delle operazioni svolte: ad esempio "sono stati aperti I file immagine" oppure "sono stati cercati I file per parola chiave con la tringa *fattura"…*
- esito dell'ispezione informatica: ad esempio "durante l'ispezione e' emerso che..."
Modalità' operative.
L'ispezione informatica può' avvenire in modalità':

- **post-mortem**, cioè' a sistema spento, collegando il supporto di memoria ad appositi strumenti che evito le alterazioni
- **live**, caso che si verifica solo quando il sistema e' gia' rinvenuto acceso all'atto dell'intervento della P.G. e si opera riducendo al minimo le alterazioni che però' sono inevitabili.

ALIBI INFORMATICO

Il ricorso sempre più' massiccio all'uso di strumenti elettronici, informatici e telematici per lo svolgimento di attività' lavorative e ricreative, ha determinato una enorme produzione di dati digitali.
Ci prefiggiamo l'obiettivo di illustrare in quali casi l'attività' informativa, svolta dall'indiziato, sia stata utile all'accertamento della verità' e I casi in cui, l'ausilio della tecnica, sia stato reso possibile precostituire un **alibi** ricorrendo a tecniche di antiforensics.
Il termine alibi deriva dal latino col significato di "altrove", "in altro luogo".
L'alibi rappresenta l'"altro luogo" in cui si trovava l'indiziato nello stesso arco temporale in cui veniva commesso un delitto.
Il termine, in ambito giudiziario, appare suscettibile di assurgere ad elemento di prova se corroborato da elementi di riscontro oggettivi capaci di dimostrare appunto che al momento in cui veniva commesso il reato, l'indiziato, nello stesso orario, si trovava in un luogo diverso.
Distinzione tra alibi e cause di giustificazione.
L'alibi, indica la "non presenza" dell'indiziato sul luogo del delitto che quindi esclude la sua partecipazione all'azione delittuosa.
Infatti, all'esito della celebrazione di un processo penale, il giudice, in presenza di alibi (di ferro) deve emettere sentenza di assoluzione nei confronti dell'imputato "per non aver commesso il fatto"; viceversa, se si trovasse a decidere il caso giudiziario di un soggetto che ha agito in presenza di una causa di giustificazione, dovrà' emettere sentenza di assoluzione "perché' il fatto non costituisce reato".

Aspetti generali.
Per "alibi" si intende generalmente una allegazione difensiva di circostanze di fatto prospettabili a difesa dell'imputato (o dell'indagato), che si pongono in oggetto contrasto con I fatti posti a base dell'ipotesi accusatoria.
E' volta a dimostrare che il soggetto indagato/imputato, al momento della commissione del reato si trovava in luogo diverso e lontano rispetto a quello ove il reato stesso sarebbe stato preparato o che, comunque, lo stesso non avrebbe potuto commettere quanto a lui contestato.
Trattasi di una prova o dimostrazione logico-fattuale controdeduttiva, rispetto alle tesi accusatorie, proposta dalla difesa al fine di minare elementi fondamentali della ricostruzione avversa e cioè' che si dice in un'ottica che, pur nella "parità'" fra accusa e difesa prevista nel nostro ordinamento processuale, vede comunque solo la prima tenuta a dimostrare puntualmente tutti I suoi assunti e percorsi "oltre ogni ragionevole dubbio".
Per la difesa e' sufficiente che le stesse siano ragionevoli e coerenti e tali da impedire all'accusa il raggiungimento di detto punto di certezza.
Il trovarsi "in altro luogo" infatti, può' e deve essere inteso sia in senso letterale che nel senso figurato di non essersi trovato in situazione tale da poter commettere il reato.
Doppia proposizione da dimostrare:
- **negativa** il "non essere nel luogo" e
- **positiva** "perche' si e' in altro luogo".
Il tutto legato dalla dimostrazione dell'impossibilità', per ragioni di spazio e di tempo, di trascendere dall'uno all'altro dei luoghi individuati al momento della commissione del fatto.

Su questi elementi interviene l'opera ricostruttiva dei consulenti, chiamati a coadiuvare I singoli soggetti del procedimento con le loro indagini.
E' ovvio che tali ragioni e tali percorsi mutino gravemente di significato allorquando la commissione del reato avvenga (e quindi la condotta si svolga) in tutto o in parte non in un ambito meramente "fisico", ma coinvolga ambiti "virtuali" per esempio il web. Oppure quando tracce ed elementi di prova attingano datti ambiti (ad esempio indagini su supporti o sistemi informatici, collegati o meno alla rete, volte alla dimostrazione dello svolgimento di "attività' informatica" in un certo luogo da parte di un certo soggetto).
I fatti, le condotte, gli eventi e le relative dimostrazioni, dirette, indirette e contrarie dovranno quindi tener conto del "luogo" ove si svolgono (o si sarebbero svolti) I fatti, sia per la loro ricostruzione, sia per la loro acquisizione processuale, sia, infine, per la loro valutazione.
Alibi come scelta difensiva:
- Assenza di alibi non implica colpevolezza
- Fallimento dell'alibi

Falso alibi.
Il rilievo della falsità' dell'alibi, come dimostrazione del fatto che lo stesso era stato artatamente preordinato o si e' dimostrato puramente mendace, può' essere (ma non deve, marcando una *regula iuris* in proposito) "posto in correlazione con altre circostanze di prova a carico e valutato come indizio, nel contesto delle competenze risultanze probatorie, se appaia finalizzato alla sottrazione del reo alla giustizia".

Esempio di procedure operative.
Fase 1: dichiarazione di quanto ricorda l'indagato.
Fase 2: ricerca di ulteriori informazioni a sostegno dell'alibi. Tale fase può' essere curata sia dello stesso indagato che dagli investigatori.
Il processo si sposta, successivamente, nel dominio della "**credibilità'**" che riguarda come le persone accertano e valutano l'alibi.
La valutazione è' svolta, come detto, nella fase preliminare delle indagini, da chiunque ne abbia necessità' (investigatori, parti offese, avvocati).
La finalizzazione nel caso in cui la valutazione sia stata costruita da chi ne abbia avuto interesse e quindi ora tale analisi e' rimessa al dibattimento e alla decisione del Giudice. In questa delicata fase si ricostruirà' quanto studiato nelle fasi precedenti e si verificherà' la consistenza dell'alibi all'interno di un più' ampio contesto investigativo.

Caso "Geri" (1999).
Alessandro Geri, ritenuto il "telefonista" delle Brigate Rosse coinvolte nell'omicidio del Prof. Massimo D'Antona, viene scagionato grazie ad una consulenza tecnica espletata su alcuni file presenti su un **floppy disk** acquisito dagli investigatori, che fornirono l'alibi già' nella prima fase delle indagini.
Nella memoria principale del dischetto I tecnici rinvennero e sottoposero ad esame una ventina di lavori; mentre nella memoria secondaria ne furono rinvenuti soltanto cinque. Il primo file risultava salvato alle **18.03** mentre l'ultimo alle **19.32**. La rivendicazione dell'attentato, da parte dei terroristi al Corriere della Sera, risultava essere avvenuta alle **19.04**. I magistrati requirenti, in possesso anche di altri elementi di prova utili a ricostruire l'attività' svolta dall'indagato in concomitanza con le fasi dell'agguato, hanno ritenuto **attendibile** l'alibi informatico sebbene I file recassero la data del 20 maggio 1990 anziche' la data del 20 maggio 1999, giorno in cui si erano verificati I gravi fatti si sangue.

Caso "Douglas Plude" (1999).
"Nella notte del 21 ottobre, poco prima della morte d Genell, entrambi I computer erano attivi

intorno alle 22:00. Il computer di Genell mostro' che l'utente aveva effettuato una ricerca online per informazioni sul Fioricet. Il computer di Plude mostro' l'uso di internet e l'uso di un programma per editing di immagini tra le 22:00 e le 22:30".
L'alibi fornito tendeva a dimostrare che la moglie, la sera stessa del decesso, aveva navigato sul suo notebook ed avevo aperto la pagina web dedicata a tale farmaco per verificare gli effetti mortali che derivano dall'assunzione di dosi massicce e quindi col chiaro intento di suicidarsi. Tutto cio' avveniva nello stesso momento in cui l'indiziato era impegnato ad editare foto sul prorpio portatile.
Ebbene il giudice non ha ritenuto degno di credibilita' l'alibi argomentando: che risultava visionata la sola pagina relativa al farmaco e non erano stase consulate le parti di essa che trattavano del dosaggio' che, tutto sommato, lo stesso indiziato avrebbe potuto usare entrambi I computer, visto che erano portatili e facilmente collocabili in prossimita' dell'operatore.

Strage di Duisburg/Faida di Locri (2006).
Viene causalmente ritrovata una cassetta, In cui l'inputato festeggia con I parenti il Natale.
La perizia di parte ne avvolora l'autenticita' enrando anche nel merito del filmato (trasmissione televisive, coincidenze sugli orari, ecc). Mentre, la perizia di accusa controbatte nel merito (luce, orari, ecc).
La perizia del giudice: "Effettuin I periti una perizia finalizzata a verificare l'integrita' del filmato girato con telecamera ad uso domestico il 25-12-XXXX, prodotto dalla difesa X, tenendo conto della CTP ing. X, dalla audizione dibattimentale di quest'ultimo, della memorai depositata, nonche' delle dichiarazioni rese in dibattimento di tutti I documenti allegati alla relazione del consulente e alla deposizione delle teste, esaminando il nastro origniale (riproducente il filmato) ed il DVD". Conlusione **falso alibi**.

Verifica di un alibi.
Cerchiamo di capire come si possa dimostrare la solidita', od eventualmente l'inconsistenza, di un alibi, nella fattispecie, informatico.
La verifica, che consiste nell'applicare il seguente schema di 8 domande:
- cinque riguardano l'oggetto: **chi, cosa, quando, dove, perche'**
- tre riguardano il sogetto agente: **quando, in che modo, con quali mezzi**

Difficilmente il consulente tecnico riuscira' a fornire una risposta a tutte le domande sufferite, ma tentare aiuta a rappresentare una evidenza digitale in maniera completa e consente, all'organo giudicante, di potersi determinare piu' facilmente circa l'eventuale ammissibilita' o meno della stessa.

Classificazione.
Se valutiamo la variabile tempo, possiamo distinguere due casi di alibi:
1) quelli generati durante, o contemporaneamente, l'evento criminoso;
2) quelli creati in un momento diverso, antecedente o seguente, dell'atto delittuoso.

Constemporaneita'.
Le tracce informatiche sono prodotte nello stesso istante in cui si consuma il reato.
Distinguiamo quattro fattispecie:
a) l'inputato ha genrato direttamente tracce informatiche su dispositivi distanti dalla scena del crimine;
b) un sistema informatizzato ha eseguito automaticamente azioni ed eventi pianificati che, producendo tracce informatiche, simulano la presenza e l'interazione dell'inputato in un luogo diverso dalla scena del crimine;
c) un terzo, persona fisica o sistema automatico, ha registrato tracce che potrebbero

giustificare la presenza dell'inputato in luoghi diversi dalle scena del crimine;
d) un terzo, un complice, ha eseguito azioni, per nome e per conto dell'inputato, che producono tracce informatiche su dispositivi distanti dalla scena del crimine

Nel caso di un falso alibi possiamo distinguere altre due fattispecie in aggiunta alle precedenti:
1) L'imputato (o chi per lui) realizza una prova ex novo, facendo attenzione che gli elementi caratterizzanti il tempo rilevino la contemporaneita' con l'azione criminale
2) L'inputato (o chi per lui) riutilizza una traccia informatica gia' esistente, alerando gli elementi utili a dimostrare la correlazione temporale tra il momento della produzione e l'evento criminoso.

Ipotesi.
A) L'imputato ha generato direttamente tracce informatiche a distanza.
B) Un sistema ha simulato un utilizzo in presenza
C) Un terzo, persona fisica o sistema automatizzato, ha registrato tracce informatiche
D) Un complice ha eseguito azioni per conto dell'indiziato
E) L'indiziato (o chi per lui) realizza una prova ex novo
F) L'indiziato (o chi per lui) riutilizza una traccia informatica già' esistente.

Esempio di finto alibi informatico.
1) Ci procuriamo una console KVM over IP
2) Assegnamo un indirizzo IP statico alla console per evitare che il DHCP server registri il MAC della stessa
3) Abilitiamo, sul router, il port per la connessione in entrata e la regola di inoltro specifica per la console
4) Configuriamo il servizio DNS dinamico (presente su tutti I router commerciali)
5) Colleghiamo la console al router
6) Scolleghiamo la tastiera, il mouse ed il video da pc e connettiamo la console KVM
7) Accendiamo il personal computer
8) Ci connettiamo, da un luogo a distanza, attraverso un browser web, utilizzando il nome mnemonico registrato, da un'altra postazione (o con un dispositivo mobile) ed utilizziamo alcune applicazioni presenti sul computer
9) Ritornati a casa, spegniamo il pc, scolleghiamo e occultismo la console KVM
10) Resettiamo il router ripristinando le impostazioni di default

Analisi.
Personal computer.
1) L'analisi del file di registro e del file system confermano l'utilizzo delle applicazioni e la creazione delle digital evidence che sono state esibite dall'imputato.
2) La time-line di accensione conferma gli orari di creazione e modifica del file
3) Viene rilevato traffico di rete
4) Il firewall è' abilitato con tutti I port chiusi
5) Non e' presente alcun software di gestione remota

Router.
1) È' impostato con I parametri di default, il firewall è' abilitato.
2) Dai file di log si rileva che e' stato riavviato in un momento successivo alla data e ora dell'alibi. Non vi sono tracce di collegamenti antecedenti alla data ed ora del riavvio.

Tabulati del traffico dati.

1) Si rileva traffico entrante, per gran parte, coincidente con quello presente sul pc.
2) Si rileva traffico uscente, proveniente da indirizzo IP afferenti ad alcuni ISP, non riscontrabile sul pc.

In presenza di queste evidenze non si potrà' affermare che l'alibi sia falso.

Altre tipologie.
- Connessione remota tramite software (Teamviewer su USB)
- Simulare, attraverso automatismi, l'utilizzo di un computer (linguaggi di scripting)
- Realizzare una prova ex novo, prima o dopo un determinato evento

Evidenze digitali automatismi "indesiderati".
Script che ha prodotto l'alibi digitali.
Tracce di esecuzione dello script:
- Registro di sistema
- Prefetch
- File memoria virtuale

Evidenze digitali sospette (potrebbero essere state utili per la costruzione di un automatismo)
- Esecuzione di programmi o comandi sospetti
- Presenza degli strumenti per la produzione dello script o per la sua esecuzione
- Tracce dell'attività' necessaria per la produzione dellos script.

Metodologia per la creazione di un automatismo per un generico sistema operativo.
- automatizzare l'alibi
- Analisi del rilevamente delle tracce
- Impostazione del sistema operativo per minimizzare le tracce
- Rendere indistinguibile l'esecuzione automatica da quella umana. Cancellare solo le "poche" tracce connesse all'esistenza dell'automatismo (dopo la sua esecuzione) che proverebbero che e' stato eseguito da uno script anziché' da un uomo
- Verificare se rimangono tracce digitali "indesiderate", nel caso ripetere il processo

Non e' necessario essere un hacker esperto per fare ciò'.
Automazione, cancellazione delle tracce indesiderate e cancellazione manuale o uso di supporto CD/DVD/USB sono operazioni facili. L'autocancellazione no.

Nel caso della computer forensics, il mutamento e l'evoluzione coinvolgono radicalmente non soltanto I tool e le metodiche necessarie per l'individuazione, repertamento ed analisi delle tracce digitali ma anche le componenti strutturali ed elettroniche degli stessi "fenomeni" oggetto delle analisi.
Risulta evidente la necessità di ricorrere, non solo ad un costante ammodernamento degli strumenti di forensic analysis, ma anche ad un aggiornamento delle stesse tecniche di analisi e delle conoscenze di base in materia (Ad esempio comportamento ed interazione dei programmi, etc).

ACQUISIZIONE E TRATTAMENTO DI DATI INFORMATICI IN RETE (SOCIAL, WEB, EMAIL)

Diffamazione in rete.
La sempre maggior diffusione di mezzi di comunicazione di massa, tra cui anche quelli

telematici, propongono il problema della individuazione del ruolo dell'informazione e dei limiti di liceità' della stessa, ove potenzialmente lesive dell'altrui reputazione.
A differenza di quanto avviene per I media tradizionali, in rete le notizie ed I commenti non sono, di norma, frutto dell'attività' di professionisti e non sono soggetti ad un regime di controlli professionali interni.
Ciò' spesso si traduce anche in una minore autorevolezza e credibilità' dei contenuti esposti.
I social network sono diventati l'ambiente virtuale dove ogni giorno milioni di persone interagiscono con gli altri, scambiandosi opinioni, foto, commenti e informazioni.
L'azione più' semplice di tutte, cioè' l'esprimere un proprio pensiero o una propria opinione, racchiude però' insidie e conseguenze, anche di natura penale, che a volte vengono ignorate.
Buon senso e la padronanza intrinseca del mezzo di comunicazione potrebbero aiutare.

Diffamazione.
L'articolo 595 comma terzo c.p.p. punisce ogni "**offesa recata col mezzo della stampa o qualsiasi altro mezzo di pubblicità'...**"; rientrano, quindi, nella previsione della norma anche altre forme di offesa come quelle realizzate attraverso internet o altri mezzi di comunicazione.
La pena è della reclusione da sei mesi a tre anni o della multa non inferiore a 516 euro.
La giurisprudenza ha costruito tre fondamentali ipotesi di limiti a tutela della persona umana: il limite dell'onore, della riservatezza, dell'identità personale.
Accanto a questi è il limite della reputazione.

Requisiti del Reato di Diffamazione.
1) Assenza dell'offeso (se è presente sussiste il reato di ingiuria).
2) Offesa all'altrui reputazione. La persona diffamata non deve essere necessariamente indicata nominativamente ma tuttavia deve essere individuabile agevolmente e con certezza. In sostanza è sufficiente che l'offeso possa essere individuata per esclusione, o in via deduttiva.
3) Comunicazione a più persone. Non sussiste quindi il reato di diffamazione nella lesione della reputazione comunicata ad una persona solamente, pur potendo essere ciò sufficiente per richiedere il risarcimento del danno in via civile. Con riguardo alla diffamazione a mezzo internet la sussistenza della comunicazione a più persone si presume nel momento stesso in cui il messaggio offensivo viene inserito su in sito internet che, per sua natura, e' destinato ad essere visitato da un numero indeterminato di persone in breve tempo.

La diffamazione via web o tramite piattaforma social e' diventata ormai una pratica diffusa.
Sindrome dell'abitacolo.
Cosa fare in caso di diffamazione via Facebook, ma anche su siti web, forum, o social network come Twitter, Linkedin, Google Plus o chat di gruppo su Facebook Messenger?
La diffamazione a mezzo Facebook, in particolare con riferimento a post diffamatori, può' verificarsi in due generali ipotesi:
1) la prima e' quella della pubblicazione su pagine personali, alle quali, per accedere, è' necessario il consenso del titolare, ove si ritiene la comunicazione non potenzialmente diffusa e pubblica, in quanto, attraverso Facebook si attua una conversazione virtuale privata con destinatari selezionati che hanno chiesto previamente il presunto offensore di poter accedere ai contenuti delle pagine dallo stesso gestite.
2) la seconda e' caratterizzata dalla pubblicazione di post, commenti o quant'altro du pagine nelle quali l'utente non sceglie direttamente I propri interlocutori.

Presupposto per la diffamazione a mezzo Facebook sono:

1) la precisa individualità' del destinatario delle manifestazioni ingiuriose
2) la comunicazione con più' persone alla luce del carattere pubblico dello spazio virtuale e la possibile sua incontrollata diffusione
3) la coscienza e volontà' di usare espressioni oggettivamente idonee a recare offesa al decoro, onore e reputazione del soggetto passivo.

La Cassazione ha espressamente riconosciuto la possibilità' che il reato di diffamazione possa essere commesso a mezzo internet, configurando la propagazione tramite Facebook un'ipotesi che integra quale aggravate quella di cui il terzo comma del menzionato articolo:
Il legislatore si e' interessato, pertanto, ad un'analisi della condotta protesa a postare un commento offensivo sulla bacheca, in rapporto alla pubblicazione e alla diffusione di essa, e cioè' volta a comunicare a terzi quale gruppo di persone apprezzabile dal punto di vista numerico (Cassazione Penale, sez. I, 28/04/2015, n 24431).

La certificazione di una presunta diffamazione via Facebook, su siti web o social network deve necessariamente includere la fase di acquisizione delle prove informatiche, certificazione dell'integrità' dei dati raccolti oltre che la stesura di una relazione tecnica che possa diventare Consulenza Tecnica di Parte da allegare a eventuale denuncia/querela per diffamazione.

Una raccolta delle prove per diffamazione non corretta può':
- 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 (ad esempio sostenendo la tesi del furto dell'account)

La diffamazione e l'offesa che avviene su in rete (anche in gruppi chiusi) e' punibile a seguito di querela della parte offesa che diventa più' efficace se riporta anche una Consulenza tecnica circa l'avvenuta diffamazione e l'acquisizione forense e certificata dal contenuto diffamatorio che si contesta, che diventerà' poi prova nel processo penale o civile in tribunale.
Prove che potrebbero anche scomparire prima di avere il tempo di sporgere querela, rischiando quindi che le evidenze digitali della diffamazione scompaiano e sia poi decisamente più' complesso ottenerle, se non tramite Rogatoria Internazionale (MLAT) in genere utilizzata in casi di rilevanza penale maggiore rispetto alla diffamazione, seppur a mezzo di stampa o a mezzo internet e Facebook.

La perizia/consulenza finalizzata a documentare tramite prove informatiche la diffamazione e l'offesa o l'ingiuria avvenuta in rete può' essere tramite indagini e ricerche OSINT alla ricerca e acquisizione dei dati relativi ai proprietari o agli utilizzatori dei profili, gruppi o pagine Facebook su cui vengono pubblicati I messaggi diffamatori.
Spesso I profili utilizzati per la diffamazione su Facebook o in generale a mezzo internet, ma anche le pagine o talvolta I gruppi, vengono chiusi dopo aver commesso il reato proprio per rendere più' complesse le indagini. Lo stesso tipo di cristallizzazione della prova e analisi forense e investigativa e' fattibile tecnicamente anche in caso di diffamazione su canali diversi, sempre a mezzo internet, come diffamazione su siti web, portali, forum, gruppi di discussione, post di blog, commenti a blog, tweet su Twitter, post e pagine su Linkedin o Instagram.

Acquisizione (artigianale).
La stampa in PDF o su carta può' essere utilizzata come prova?

La stampa o screenshot difficilmente vengono ammesse in Tribunale come prova perché' non godono dell'integrità' delle prove informatiche raccolte con strumentazione adeguata e metodi scientifici.
Anche la fotografia dello schermo del PC non ha pienamente valore legale o meglio, può' facilmente essere contestata dalla controparte, poiché' per quanto possa avere una storicità' temporale (I cellulari si sincronizzano automaticamente con l'ora esatta e salvano le immagini in tempo incrementale) ritrae qualcosa che può' facilmente essere artefatto (lo schermo).

Acquisizione tramite Notaio.
La stampa del profilo Facebook certificata da un Notaio o da un Pubblico Ufficiale e' certamente un'alternativa migliore ma può' non essere sufficiente ad identificare il proprietario del profilo o della pagina utilizzata per la diffamazione, poiché' è' necessario acquisire anche ulteriori dati come il codice identificativo univoco che permette di ritrovare il profilo o la pagina diffamatoria anche in caso di cambio del nome o dell'indirizzo.

Facebook: identificazione del profilo.
Per quanto sia importante, non e' sufficiente prendere nota del nome del profilo o della pagina, neanche copiando l'URL.
Per poter eseguire una consulenza informatica su un profilo, pagina o gruppo Facebook e' necessario, in realtà', identificare il codice **ID** che lo **identifica univocamente**.
Il nome del profilo infatti può' essere modificato dal proprietario, così' come l'indirizzo che compare nella barra delle URL del browser.
Per individuare il codice ID del profilo o della pagina da cui proviene la diffamazione, e' possibile utilizzare un sito come findmyfbid.com, incollando l'indirizzo del profilo o della pagina nel campo di testo e premendo il pulsante "Find numeric ID".
Si otterrà' un numero da copiare o stampare, per "congelare" l'identificativo univoco che permetterà' di ritrovare il profilo o pagina anche in caso di cambio di nome o URL e all'Autorità' Giudiziaria di richiedere a Facebook eventuali file di log o contenuti diffamatori.
La raccolta delle prove per uso legale in caso di diffamazione su Facebook, partendo dal codice ID del profilo o delle pagine, e' molto più' efficace.

Facebook: come trovare il riferimento univoco del post o del commento diffamatorio?
Identificado l'ID del proprietario del profilo da cui e' avvenuta la diffamazione o il Page ID della pagina che contiene il testo diffamatorio, si deve "congelare" anche il post o il commento stesso per utilizzarlo poi come prova informatica della diffamazione.
La data del post incriminato contiene un link all'indirizzo o URL che identifica il post stesso, che si aprirà' nel browser.
Es. www.facebook.com/nome.profilo/posts/10213357451991856
Per identificare un commento specifico per "congelarlo" come prova di una diffamazione, così' da poter poi redigere una consulenza tecnica che ne documenti in modo oggettivo il contenuto, andrà' fatta una cosa simile cliccando pero' una volta sulla data e ora sotto il commento stesso, dopo il link "Mi Piace".

Notifiche sui post diffamatori.
Per attivare le notifiche su un post diffamatorio di Facebook, cliccare sulla freccia con punta in basso posizionata in alto a destra nel post e poi sulla voce di menu' "Attiva le notifiche per questo post". Si riceveranno cose' email a ogni nuovo commento al post, che potranno essere utilizzate dal perito informatico per certificare o rintracciare I commenti anche nel caso in cui – come spesso accade – dovesse essere rimossi poco dopo la pubblicazione.
Ovviamente le email devono essere mantenute nella casella di posta e non cancellate, così'

da permettere successivamente un'analisi sulla posta elettronica che ne certifichi l'originalità' e la presenza sul server per un utilizzo in Tribunale.

OSINT.
La Open Source INTelligence, acronimo OSINT, e' l'attività' di raccolto di informazioni mediante la consultazione di fonti di pubblico accesso.
L'OSINT si distingue dalla 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.

OSINT fonti.
- Mezzi di comunicazione: riviste, giornali, televisione, radio e siti web.
- Dati pubblici: rapporti dei governi, piani finanziari, dati demografici, dibattiti legislativi, conferenze stampa, discorsi, avvisi aeronautici e marittimi
- Osservazioni diretta: fotografie di piloti amatoriali, ascolto di conversazioni radio e osservazione di fotografie satellitari. La diffusione di fotografia satellitari, spesso in alta risoluzione, sulla rete (ad esempio Google Earth) ha esteso la possibilità' di Open Source Intelligence anche per le aree che prima erano disponibili solo alle maggiori agenzie di spionaggio.
- Professionisti e studiosi: conferenze, simposi, lezioni universitarie, associazioni professionali e pubblicazioni scientifiche.
La maggior parte delle informazioni sono georeferenziate. Non tutti I dati open source sono testo senza struttura. Alcuni esempi di open source georeferenziati spaziali sono: copie materiali o digitali di mappe, atlanti, repertori biografici, progetti di porto, dat gravitazionali, aereonautici, nautici, geodetici, geo antropici, ambientali, di iconografia commerciale, lidar, iper e multi spettrali, foto aeree, di web services e mash-up, di database.

OSINT e Facebook.
Anche sulle piattaforme social e' possibile ricavare informazioni senza per forza far riferimento a software del settore.
Facebook e' una di quelle piattaforme che meglio si presta alla raccolta di informazioni.

Manipolazione URL.
Queste tecniche permettono di scoprire informazioni su persone, gusti, mi piace, recensioni, luoghi visitati e tutte quelle informazioni che non sono recuperabili dal profilo dell'utente stesso.
Il primo passo e' quello di cercafe il codice numerico dell'utente Facebook, per poterlo inserire in specifiche posizioni di una URL.
La URL che utilizzeremo sono così' composte:
- URL statica
- ID utente
- Termine di ricerca

| URL statica | ID utente | Variabile di ricerca |
https://www.facebook.com/search/000000/photo-liked

Non si tratta di bug o altro; le limitazioni alla privacy sono decise da ogni singolo utente che interagisce con la piattaforma.
Un profilo che utilizza tutti gli accorgimento di privacy possibili, interagendo con un altro utente che non le utilizza, deve "sottostare" alle impostazioni di quest'ultimo.
Nelle interazioni, chi ha il livello di privacy più' basso, decide la visibilità' o meno delle

informazioni.

Esistono siti che uniscono più' ricerche contemporaneamente. Ad esempio, All-io permette ricerche su Google, Twitter, Youtube e molti altri, mentre Qwant ha un opzione in base a ciò' che si vuole cercare.

Acquisizione/cristallizzazione pagine WEB.
Anche per premunirsi in caso di cancellazione e' comunque necessario iniziare al più' presto la fase di "cristallizzazione" utilizzando alcuni accorgimenti, come ad esempio il software gratuito FAW (Forensics Acquisition of Websites) che permette di acquisire in maniera forense pagine web o profili di social network con alcune garanzie sull'originalità' del dato acquisito.
Esistono poi servizi web che permettono di scaricare una copia autentica di pagine o post Facebook a patto che questi siano pubblici e non privati. Es. Perma.cc o Archive.is.

Acquisizione: problematiche tecniche.
L'acquisizione forense con cristallizzazione della prova online su internet per tutelare I propri diritti può' includere ad esempio anche I file robots.txt, I certificati SSL, le sitemap, I metadati RSS o dei documenti presenti sul sito, il filmato dell'acquisizione forense, eventuali codici di errore, indirizzi IP, record DNS, un dump del traffico di rete realizzato tra browser/client e il server web che ospita il sito, incluse le chiavi SSL necessarie poi per decriptare il traffico e verificarne la consistenza.

[DA COMPLETARE]

LA POSTA ELETTRONICA

Il servizio di posta elettronica.
Il servizio di posta elettronica, chiamato anche e-mail (electronic mail) consente a ogni utente che abbia accesso ad un computer e che possa connettersi ad Internet di inviare "messaggi" (testi, ma anche, più' in generale, "oggetti" memorizzati in formato elettronico, sotto forma di file, come programmi, immagini, suoni, ecc) ad un qualsiasi altro utente che disponga di un indirizzo di posta elettronica e che lavori su un qualsiasi altro computer, ovunque collocato, purché' raggiungibile tramite connessioni in rete.
I computer dei due corrispondenti non debbono essere contemporaneamente o permanentemente connessi alla rete. I messaggi infatti vengono recapitati su caselle di posta elettronica ospitate da appositi server (comunicazione asincrona).
L'utente che vuole verificare l'arrivo di messaggi a lui indirizzata potrà' contattare il server e solamente nell'intervallo in cui avviene la transazione tra computer dell'utente ed il server è' necessario che la connessione di rete sia attiva.
Un primo evidente vantaggio che l'utilizzo della posta elettronica comporta e' la velocità': anche tra I sistemi più' distanti tra loro, purché' in qualche modo comunicanti, I messaggi possono essere recapitati nel giro di poche ore (I piu' delle volte sono comunque sufficienti pochi minuti).
La disponibilità' di un indirizzo di email e' un prerequisito indispensabile per utilizzare il servizio di posta elettronica, dal momento che serve per individuare sulla rete mittenti e destinatari dei messaggi. Gli indirizzi di posta elettronica hanno la form: **utente@indirizzo**, dove la parte a sinistra dei **@**, detto anche "chiocciola" e normalmente letto come "at" (presso) identifica l'utente in maniera univoca all;interno del server che lo ospita. La parte di indirizzo a destra del simbolo @ identifica invece in maniera univoca, all'interno della rete internet, il sistema informatico presso il quale l'utente è' ospitato e corrisponde appunto al

“nome” del server, normalmente espresso come un insieme di parole (o più’ in generale di stringhe di caratteri alfanumerici) separate da punti.

Sistemi di posta elettronica.
Ogni ISP o altri fornitori di servizi online permettono agli utenti privati e di pubbliche imprese di aprirsi una propria casella di posta elettronica dove poter inviare e ricevere messaggi, anche allegati. La posta elettronica e’ consultabile:
- attraverso il sito web di riferimento (webmail)
- attraverso un programma client di posta elettronica che, settato opportunamente, scarica da internet la posta di uno o più’ account.
I sistemi di posta elettronica sono composti da due sottosistemi:
- agenti utente o client, ovvero programmi che consentono alle persone di leggere e inviare la posta elettronica (webmail o programmi client)
- server, si occupano dello spostamento dei messaggi dall’origine alla destinazione attraverso l’utilizzo di determinati protocolli.
I protocolli tipicamente impiegati per lo scambio di e-mail sono:
- **SMTP** (Simple Mail Transfer Protocol), usato per l’invio, la ricezione e l’inoltro dei messaggi tra server (nonché’ per il solo invio da parte del client)
- **POP3** (Post Office Protocol) e **IMAP** (Internet Message Access Protocol) usati invece per la ricezione e consultazione dei messaggi da parte degli utenti.

- MUA – Mail User Agent (Thunderbird, outlook) implementa il client o server SMTP
- MTA – Mail Transfer Agent (sendmail, qmail) risolve gli indirizzi usando I record MX nel NS.MTA contatta MTA attraverso SMTP
- MDA – Mail Delivery Agenti (procmail) Ricevuto l’MTA, fornisce l’email al MDA
- MRA – Mail Retrieval Agent (POP/IMAP client) MRA, usa IMAP/POP3/MAPI per ricevere dall’MDA. MUA presente le email all’utente
- NS – Name Server (DNS Server)

Senza accedere all'account di terzi e’ possibile stabilire una connessione con l’email server (ad esempio mediante telnet) e scrivere direttamente I comandi relativi a mittente e destinatario, ai parametri aggiuntivi e creare il corpo della mail.

Sistemi di posta elettronica.
Un aspetto importante nei sistemi di posta elettronica e’ la distinzione tra l’involucro e il suo contenuto.
L’involucro incapsula il messaggio e contiene tutte le informazioni necessarie per il trasporto dei messaggi: come l’indirizzo di destinazione, la priorita’ e il livello di protezione, che sono distinte dal messaggio stesso. Gli agenti di trasporto dei messaggi utilizzano l’involucro per l;instradamento e trasferire il messaggio al destinatario, così’ come gli uffici postali tradizionali utilizzano le buste.
Il messaggio all’interno dell’involucro consiste in due parti: l'intestazione (**header**) e il **corpo**. L’intestazione contiene le informazioni di controllo per gli agenti utente ed il corpo e’ dedicato interamente al destinatario umano.

Posta elettronica o Posta cartacea.
L’informazione trasmessa attraverso un messaggio di posta elettronica giunge normalmente al destinatario nella stessa forma in cui era sul computer “mittente” ma e’ suscettibile ad elaborazioni da parte del destinatario sul proprio computer (manipolazione, copiatura, “ritaglio”, completamento, ecc), senza passaggi intermedi.
Nel caso di un messaggio cartaceo invece, l’informazione non può’ essere alterata se non

attraverso una complicata procedura che prevede la riproduzione in formato elettronico del documento e l'elaborazione digitale del testo o delle immagini, ecc.

Protocolli.
Inizialmente il protocollo per la rappresentazione dei documenti di posta elettronica era definito nel documento **RFC 822** del 2982; in cui veniva specificato il formato per I messaggi di posta e ci si limitava ai messaggi esclusivamente di tipo testuale, senza alcun riferimento a messaggi di altro tipo (ad esempio multimediali).

- **To**: gli indirizzi di posta elettronica dei destinatari primari
- **Cc**: gli indirizzi di posta elettronica dei destinatari secondari
- **Bcc**: gli indirizzi di posta elettronica per le copie per conoscenza nascoste
- **From**: la persona che ha mandato il messaggio
- **Sender**: l'indirizzo di posta elettronica del mittente vero e proprio
- **Received**: la riga aggiunta da ogni agente di trasferimento lungo il percorso
- **Return-path**: può' essere utilizzato per identificare il percorso di ritorno al mittente.

L'affermarsi dei servizi di posta elettronica e la conseguente necessità' di far fronte alle limitazioni dettate de RFC 822, in cui viene descritto lo standard **MIME** (Multipurpose Internet Mail Extension). In particolare in RFC 1341 vengono specificati I meccanismi per definire il formato sia di messaggi testuali (ASCII e non) sia di messaggi multimediali (cioè' contenenti video, suono, immagini, ecc). Tale documento si concretizza con la definizione di cinque nuove intestazioni di messaggi:
- **MIME-version**: identifica la versione di MIME
- **Content-description**: stringa leggibile che comunica cosa contiene il messaggio
- **Content-Id**: identificatore univoco
- **Content-transfer-encoding**: indica come il corpo del messaggio e' stato preparato per la trasmissione
- **Content-type**: il tipo e il formato del documento

Email: Analisi Forense.
Webmail, accesso server (consenso, pwd, ecc).
Software di gestione di posta elettronica.
Nel secondo caso, in cui l'utente utilizza software di gestione di posta elettronica, tutto o parte dell'archivio di posta elettronica viene scaricato sul computer (o sul dispositivo) al momento della configurazione dell'account. Periodicamente il client di posta effettua controlli per verificare la presenza di nuovi messaggi in arrivo. In questo caso la Computer Forensic può' intervenire attraverso l'analisi sugli archivi, cercando di estrapolare la maggior parte dei dati possibile.
Una volta entrato in possesso dei file contenenti le e-mail, l'esperto forense puo' intraprendere la fase di analisi analizzando tutti I campi relativi all'intestazione al corpo del messaggio stesso.

Analisi e-mail: Intestazione/headers.
Identificazione mittente:
- Phishing
- Malware
- Ecc.

Analisi e-mail: estrazione headers.
I client di posta elettronica rendono disponibile questi tipo di informazione relativamente ad

ogni e-mail ricevuta. Le modalità' di accesso a tali dati dipendono dallo specifico client.

Headers.
Gli headers vanno letti dal basso verso l'alto. Partendo dalle informazioni principali, risalendo verso la cima della headers e' quindi possibile ricostruire tutto il percorso fatto dalla mail prima di giungere al destinatario.
Le righe che evidenziano questo percorso sono quelle che iniziano con la parola chiave **Received**. Tale elemento viene aggiunto da ciascun server SMTP che ha trattato il messaggio indicando tra le parentesi tonde e quadre gli indirizzi IP da cui e' stato ricevuto il messaggio ed ulteriori informazioni sulle locazioni geografiche del computer/server.
Dopo il blocco di informazioni contrassegnate dalla parola Received sono presenti altri campi:
- Subject: oggetto del messaggio.
- From: fornisce l'informazione della casella di posta del mittente.
- To: indica il destinatario.
- Cc: destinatari in copia carbone [per conoscenza]
- Bcc: destinatari in copia carbone nascosta.
- Date: data e ora al momento dell'invio.
- Message id: contiene un codice costruito dal primo server da cui il messaggio e' stato spedito, e che dovrebbe permettere di identificare univocamente il messaggio sui server attraversati.
- Importance o X-priority: priorità' del messaggio [da 1 a 3, alta-media-normale].
- X-Mailer: programma usato per inviare la mail (se so usa una webmail questo campo non e' presente)

Altra riga da tenere in considerazione e' quella preceduta dalla parola Mime.
Il Mime e' un protocollo definito per il trasferimento e l'interpretazione dei dati non codificati in ASCII. Il Mime si occupa anche del trasferimento di allegati in qualsiasi formato, ad esempio file audio, video e testo di qualsiasi formato.

Tools: Email Tracker.
Estrae automaticamente gli header, effettua diversi tipi di analisi, traccia attraverso gli IP negli headers il percorso fatto dalla mail, genere un report.

Autenticazione Mittente.
Dall'analisi degli header e' possibile ricostruire la storia e il percorso che una mail compie prima di arrivare a destinazione. La domanda che spesso ci si pone e' se tale tipo di analisi basti ad autenticare il mittente della mail inviata, ovvero se e' possibile in maniera univoca affermare che la casella di posta da cui e' partita la mail sia veramente stata utilizzata per l'invio della stessa.
In realtà' l'analisi dei campi finora descritti non può' fornire tale garanzia riguardo al mittente, a meno che non sia presente un ulteriore campo denominato **DKIM** (**Domain Key Identified Mail**).
Il campo DKIM-signature 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 può' quindi stabilire che la mail ricevuta sia **certificata** dal dominio che ha apposto la firma, permettendo al destinatario di verificare che il messaggio provenga dal dominio dalla quale dichiara di provenire.
La specifica DKIM garantisce solo che la mail e' stata inviata dal dominio firmatario.

Fake email.

Cosa occorre:
- editor di testo
- conoscere I campi dell'header
E' sufficiente inserire negli appositi campi I dati di interesse:
From, To, Cc, ecc.
Salvare il file di testo in formato .eml.

L'analisi identifica dei mittenti dei messaggi, destinatari, date e orari di invio.
L'assenza del campo DKIM non permette di certificare l'autenticità' dei messaggi ne' tanto meno il reale invio degli stessi.
In conclusione non è' possibile stabilire che I file presentati siano autentici e che siano realmente inviati ai destinatari indicati.

Anonymous email.
Le webmail consentono quasi sempre la registrazione senza una stretta verifica della veridicità' dei dati personali forniti. Tuttavia, questi servizi in generale possono non essere completamente anonimi, nel senso che il fornitore impegna coerentemente con la normativa italiana sul data retention, a tracciare gli IP di connessione alla casella.
Tali informazioni sono disponibili per le autorita' giudiziaria per un periodo normativo definito dalla norma in vigore.
Esiste tuttavia la possibilità' di utilizzare servizi webmail (a pagamento o gratuiti) dichiaratamente anonimi. Es. Anonymusmail.me.
Consente l'invio di email anonime. Nessuna attività' viene registrata. Servizio erogato tramite dominio registrato ad Alexandria (Virginia).

YOPmail.
Nasce per contrastare le mail spam generando indirizzi email monouso per le iscrizioni, domande di informazioni o di documentazioni su siti internet. Le mail inviate alla casella di posta vengono cancellati dopo 8 giorni.

Valore giuridico delle email.
Un semplice messaggio di posta elettronica ha un qualche valore legale? Lo si può' usare come prova in un vero processo. La normativa italiana lascia spazio all'interpretazione e concede margine di manovra al giudice, senza però' dare uno strumento certo e definitivo sul tema.
Quale valore hanno le email dal punto di vista giuridico?
Esse vengono utilizzate per una molteplicità' di scopi, sia in ambito privato sia in ambito pubblico, ma un email e' equiparabile a un documento sottoscritto o non ha alcun valore? Può' una semplice email trasformarsi in una vera e propria prova?
Ci si chiede che valenza abbia una dichiarazione contenuta in un messaggio di posta elettronica, se quest'ultimo sia suscettibile di assurgere a prova in un eventuale giudizio e, prima ancora, cosa debba intendersi giuridicamente per email.
I riferimenti normativi L. n. 59/199 (riconoscimento regolamentazione della validità' dei documenti formati e/o trasmessi con strumenti informatici), il Codice di Amministrazione Digitale (cd. CAD) di cui al G. Lgs. 82/2005 e successive modificazioni.
L'email può' essere ricondotta nella categoria dei cd. documenti informatici, in ragione alla definizione che di essi viene fornita all'art. 1, comma 1, lett. p) del suddetto Codice quale "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".
A tale riguardo occorre rilevare come siano rinvenibili due orientamenti contrapposti.
Da un lato, infatti, vi e' chi ritiene che l'email sia da considerarsi quale semplice documento informatico privo di firma, in considerazione della pressoché' assenza di garanzie che

consentano di attribuire allo stesso una paternità' certa, a nulla rilevando il dispositivo di riconoscimento tramite password per l'accesso alla posta elettronica, poiché' quest'ultimo sarebbe privo della necessaria connessione logica con I dati elettronici che costituiscono il messaggio.
Secondo tale orientamento, il valore probatorio dell'email sarebbe da rinvenirsi nell'articolo 2712 c.c. (così' come modificato ex art. 23-quater, CAD) alla stregua del quale le riproduzioni informatiche, "fanno piena prova dei fatti e delle cose rappresentate" solo se colui contro il quale sono prodotte non le contesta tempestivamente disconoscendo la conformità' ai fatti o alle cose medesime.

Art. 2712 c.c.
Le riproduzioni fotografiche, informatiche, o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti o delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità' ai fatti o alle cose medesime".

Secondo questo primo orientamento la mail vale come prova solo se il mittente non afferma il contrario. Se ciò' accade, il messaggio email non ha alcun valore legale – diviene ciò' che comunemente chiamiamo "carta straccia".
Secondo un differente ordinamento, invece, l'email e' da considerare, a tutti gli effetti, un documento informatico sottoscritto con firma elettronica semplice, come tale liberamente valutabile dal giudice sia in ordine all'idoneità, della medesima a soddisfare il requisito della forma scritta, sia per ciò' che concerne il suo valore probatorio, ai sensi degli articoli 20, comma 1-bis e 21 comma 1, D.lgs. 82/2005.

Art. 20 comma 1-bis
"*L'idoneità' del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità;, sicurezza, integrità' ed immodificabilità', fermo restando quanto disposto dall'articolo 21".*

Art. 21 comma 1
"*Il documento informatico, cui e' apposta una firma elettronica, sul piano probatorio e' liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualita', sicurezza, integrità' e immodificabilità'".*

Si potrebbe obiettare, tuttavia, che sebbene l'accesso alla casella di posta elettronica comporti l'autenticazione dell'utente, ossia l'inserimento di uno **user id** e relativa **password**, potrebbe accadere che tali informazioni siano state in precedenza memorizzate in modo tale da consentirne l'accesso immediato. In tale eventualità', quindi, la paternità' del documento inviato non corrisponderebbe al formale mittente del messaggio. Inoltre, sussiste la possibilità' che il messaggio di posta elettronica ricevuto venga modificato, pregiudicando l'integrità', o che un'email mai venuta ad esistenza sia addirittura creata ad arte in modo tale da risultare tra I messaggi di posta ricevuto (o inviati).
In sintesi: il giudice può' considerare una email come prova, ma esistono diverse varianti da prendere in considerazione. Per sua natura, il messaggio elettronico e' prono a modifiche che impediscono di considerarlo completamente attendibile.
E' certamente condivisibile la preoccupazione delineata in relazione alla limitata affidabilità' delle email tradizionale circa l'attribuzione di paternità' del messaggio trasmesso e l'integrità' di quest'ultimo, cionondimeno non puo' negarsi che si sia comunque in presenza di un documento elettronicamente firmato, seppure in forma non certificata.

Per tale motivo è' demandato al giudice il compito di valutare nel caso concreto se l'email prodotta in giudizio possa considerarsi attendibile, anche in relazione agli altri elementi probatori acquisiti.

Posta Elettronica Certificata (PEC).
La disciplina delle modalità' di erogazione e utilizzo del servizio di PEC e' detenuta nel DPR n. 68/2005 e nel DM 2 novembre 2005.
I soggetti del sistema PEC sono:
- il mittente, che si avvale del servizio per l'invio di documenti prodotti attraverso l'utilizzo di strumenti informatici.
- Il destinatario, al quale viene recapitato il messaggio.
- Il gestore, soggetto pubblico o privato, che fornisce il servizio di PEC.
- Il DigitPA, l'amministrazione che cura l'iscrizione dei gestori in un apposito elenco pubblico e che svolge attività' di vigilanza sul sistema.

Il mittente e il destinatario che intendono fruire del servizio di PEC si avvalgono dei gestori inclusi nell'elenco pubblico tenuto dal DigitPA (Art. 14, co. 1, DPR n.68).
I gestori devono possedere una serie di condizioni per poter essere accreditati presso tale elenco (art. 14, co. 3 e ss. DPR n.68), di carattere soggettivo (forma societaria, requisiti di onorabilità', ecc) e oggettivo (affidabilità' organizzativa e tecnica, personale adeguato, certificazione di qualità', polizza assicurativa, ecc).

Le principali caratteristiche della PEC sono:
- **Integrità' del messaggio**. L'utilizzo dei servizi di posta certificata avviene esclusivamente utilizzando protocolli sicuri, in modo da evitare qualsiasi manomissione del messaggio e degli eventuali allegati da parte di terzi. Infatti tutte le comunicazioni sono protette perché' crittografate e firmate digitalmente.
- **Certificazione dell'invio**. Quando si invia un messaggio da una casella PEC si riceve dal proprio provider di posta certificata una ricevuta di accettazione che attesta che la data e l'ora della spedizione ed I destinatari.
- **Certificati della consegna**. Il provider del destinatario invia al mittente la ricevuta di consegna. Anche in questo caso si tratta di un messaggio email che attesta la consegna con l'indicazione della data e ora e il contenuto contrassegnato.

La Posta Elettronica Certificata e' l'equivalente informatico della "classica" raccomandata con ricevuta di ritorno.
Si tratta sostanzialmente di un messaggio di posta elettronica di cui vengono fornite le ricevute, aventi valore legale, di avvenuta spedizione e di avvenuta o mancata consegna.
Per poter usufruire delle funzionalità' di PEC, non e' sufficiente una casella di posta normale, ma bisogna acquisire una casella (di PEC appunto) da un gestore di Posta Elettronica Certificata autorizzato.

Valore legale dell PEC.
Alla PEC e' riconosciuto pieno valore legale e le ricevute possono essere usate come prove dell'invio della ricezione ed anche del contenuto del messaggio inviato. Le principali informazioni riguardanti la trasmissione e la consegna vengono conservate per 30 mesi dal gestore e sono anch'esse opponibili a terzi,
Le ricevute hanno valore legale solo se sia il mittente che il destinatario comunicano tramite email PEC.
Il testo esplicativo redatto dal CNIPA e' esplicito in proposito:
"Da una casella di PEC e' possibile inviare un messaggio certificato a chiunque abbia una

casella di posta elettronica? Si, ma nel solo caso in cui il destinatario sia dotato di una casella di Posta Elettronica Certificata, sia l'invio che le recezione di un messaggio di PEC hanno valore legale".
Il mittente e' garantito (ricevuta come prova). Il destinatario ha degli obblighi (non ripudiabilità', ecc).

INVESTIGARE SU IMMAGINI E VIDEO

"L'analisi forense di immagini e video e' l'applicazione dell'Image Science e Domain Expertise per interpretare il contenuto di un'immagine o l'immagine stessa in ambito legale".

Digital Forensics.
Identificazione della sorgente e verifica dell'integrità'.
E' una tecnica dalla multimedia forensics che semplicemente si occupa di fornire un modo per testare l'autenticità' e la sorgente del sensore ottico. Non significa quindi analizzare la semantica degli oggetti digitali.

Procedura.
1) Preservare l'immagine originale.
2) Documentare tutti I passi dell'elaborazione
3) L'immagine elaborata deve essere esattamente riproducibile a partire da quella originale tramite il processo documentato.

Le immagini digitali.
Un'immagine e' una funzione 2D *f(x,y)* che rappresenta una misura opportuna di una o più' caratteristiche (luminosità', colore, ecc) di una data scena.
"Un'immagine vale più' di mille parole...".
La comunicazione visuale e' la forma più' immediata ed efficace di comunicazione.
Siamo circondati da immagini.
L'occhio interpreta l'immagine facendo si che il colore, il movimento e la profondità' diventino delle vere e proprie dimensioni aggiuntive rispetto all'informazione iniziale.
Le immagini digitali sono campionate per essere rappresentate da un numero infinito di campioni.
La prima fotografia non digitale risale al 1827. Il soggetto e' occasionale: un tetto visibile dalla finestra dell'autore, Joseph Nicéphore Niépce. La lastra litografica da lui preparata fu "esposta" per otto ore.

La prima applicazione di immagine digitale si ha nelle stampe dei quotidiani. Nel 1920 una immagine viene trasmessa via cavo tra New York e Londra al fine di comparire su un quotidiano. Il protocollo di trasmissione' specifico per l'immagine e il risultato e' stampato in halftoning da apposite stampanti.
La stampa in halftoning e' stata utilizzata per molti anni. Nel 1922 cambia il tipo di stampa e si possono ottenere fino a cinque livelli di grigio. Nel 1929 I livelli di grigio diventano 15.

La prima volta che l'immagine viene elaborata al computer e' nel 1964, quando un computer della NASA riceve ed elabora un'immagine della Luna e ne corregge alcune distorsioni ottiche.

A cosa serve elaborare le immagini? In medicina, per le forze dell'ordine, ecc.

Cos'e' un'immagine digitale?
Definizione: Un'immagine digitale monocromatica e' una matrice I = f(x,y) di valore discreti di intensità' luminosa (livello di grigio), costruita da M*N pixel, ciascuno dei quali ha un valore appartenente all'intervallo [0, L-1] essendo I livelli possibili di intensità' (o di grigio).
Su un'immagine si possono fare tutte le operazioni che si possono fare sulle matrici.

Risoluzione Spaziale.
La risoluzione spaziale si riferisce al numero specifico di punto di informazione di un'immagine.

I colori: Lo spazio RGB.
E' molto comune descrivere I colori riferendosi allo spazio di colore RGB. Lo spazio RGB e' basato sul fatto che ogni colore possa essere rappresentata da una "miscela" dei tre colori primari red, green blue. I vari contributi sono assunti indipendenti l'uno dall'altro (e quindi rappresentanti da direzioni perpendicolari tra loro). La retta che congiunge nero e bianco e' la retta dei grigi.

Agire sul contrasto.
E' possibile migliorare l'aspetto di una immagine attraverso l'utilizzo delle cosiddette look-up tables.

[CONTINUA]

VIDEO DIGITALI.

Cenni sulla storia del cinema.
La prima ripresa cinematografica e' ritenuta essere Roundhay Garden Scene, cortometraggio di 2 secondi, realizzato il 14 ottobre 1888 da Louis Le Prince.
Thomas Edison nel 1889 realizzò' una cinepresa destinata a scattare in rapida successione una serie di fotografie su una pellicola 35mm e una macchina da visione consentiva ad un solo spettatore per volta di osservare, tramite un visore, l'alternanza delle immagini impresse sulla pellicola.
La cinematografia intesa come proiezione in sala di una pellicola stampata e' invece nata il 28 dicembre 1895, grazie ad un'invenzione dei fratelli Louis e Auguste Lumière con un apparecchio da loro brevettato, chiamato cinematografo.

Video Digitali: fondamenti.

Un video digitale e' costituito da una sequenza di immagini statiche che vengono visualizzate in sequenza con una certa frequenza temporale.
Il video come segnale discreto e' inteso come il campionamento temporale della scena. Ad ogni istante la scena e' fotografata.
La sequenza video quindi e' una successione di istantanee, detti fotogrammi.
Per poter trasmettere o memorizzare dei file video e' necessario definire degli standard riguardanti sia gli algoritmi di codifica/decodifica dei flussi multimediali, sia I protocolli necessari al loro trasferimento e al loro controllo sulla rete.
5 proprietà' fondamentali dei video digitali:
- Risoluzione spaziale

- Risoluzione temporale
- Formati di codifica
- Encoder/Decoder (Codec)
- Motion Estimation

Risoluzione spaziale.
La risoluzione spaziale si riferisce al numero specifico di punti di informazione (pixel) di un'immagine.

Risoluzione temporale.
La frequenza delle immagini, anche chiamata frame rate, e' il numero di immagini per unità' di tempo che vengono visualizzate.

Gli standard PAL (Europa, Asia, Australia, ecc) e SECAM (Francia, Russia, parti dell'Africa) hanno 25fps mentre l'NTSC (USA, Canada, Giappone, ecc) ha 29.97 fps. La pellicola ha una registrazione ad un frame rate minore, 24 fps.
Per raggiungere l'illusione di un'immagine in movimento il frame rate minimo è' di circa 10 fotogrammi al secondo.

Aspect Ratio.
Rapporto larghezza/altezza dell'immagine, indicato in diversi modi:
- Frazione "x:y" o "x/y"
- Risultato "1,3"
- In proporzione all'unità' "1,3:1"
Rapporti differenti in base al campo di utilizzo: cinema, televisione, fotografia..

Aspect Ratio 4:3.
E' il formato standard televisivo. Con la nascita del DVD e dei nuovi formati e' sempre meno frequente.

Aspect Ratio Widescreen 16:9.
E' caratterizzato da dimensioni orizzontali più' ampie del 4:3, con le proporzioni panoramiche tipiche dello schermo cinematografico. Ne esistono varianti più' o meno allargate.

Tecniche di adattamento degli Aspect Ratio.
- Stretch (deforma l'immagine)
- Letterbox (16:9 → 4:3) Permette di visualizzare il widescreen (16:9) su schermi 4:3. L'immagine viene scalata fino a farlo rientrare nello schermo con l'aggiunta di due bande nere orizzontali sopra e sotto il video.
- Pillarbox (4:3 → 16:9) Permette di vedere il 4:3 su schermi 16:9, immagine scalata con aggiunta di bande nere
- Windowbox (a:b → c:d) aggiunta di quattro bande nere.
- Pan&Scan (16:9 → 4:3) Permette di vedere il 16:9 su schermi 4:3 ritagliando l'immagine a destra e a sinistra.
- Tilt&Scan (4:3 → 16:9) Immagine ritagliata in alto e in basso

Risoluzione MP "MegaPixel".
Unità' di misura che equivale a 1 milione di pixel.
Calcolo dei MP di un dispositivo: (Max_orizzontale * Max Verticale)/1000000. Il valore pubblicizzato e' spesso arrotondato.
Il numero di MP non e' un diretto indice di qualità' delle macchine fotografiche, influisce

anche il potere risolutivo del sistema ottico.

Risoluzione dei formati.
Aspect Ratio 16:9:
- Half resolution (540p) 960x540 pixel
- HD Ready (720p): 1280x720 pixel
- 1080i 1920x1080 pixel (interlacciato)
- Full HD (1080p) 1920x1080 pixel

Futuro.
- Super Hight Definition (SHD), detto 4K. Risoluzione 3840x2160 (4 volte FullHD)
- Ultra High Definition TeleVision (UHDTV) 7680x4320 (16 volte FullHD)

Interlacciamento.
Immagine divisa in field pari e dispari. Si alternano I field per meta' tempo rispetto ai fps del filmato. Su monitor si notano artefatti, sul televisore non accade.

Pro e contro.
A partita' di larghezza di banda si può' dimezzare la banda del segnale, analogamente, si raddoppia la frequenza di visualizzazione.
Si riduce lo "sfarfallio" dei monitor CRT. Per quanto riguarda I monitor dei PC invece lo "sfarfallio" lamentava (effetto flicker); la direzione attuale e' quella di prediligere il progressivo, a causa della alta qualità' video richiesta.
Rinunciando a metà' dell'informazione, però', si ha una possibile comparsa di artefatti dovuti a interpolazione se sono presenti strutture orizzontali (effetto twitter). Gli artefatti possono essere pesanti se sono presenti soggetti in rapido movimento.

La compressione video.
Un CoDec video (Coder/Decoder) e' un software composto da due parti: l'enCoder che comprime la sequenza di immagini (video) archiviando in un file e un Decoder necessario per decomprimere la sequenza e poterla nuovamente visualizzare.

Compressione Lossless/Lossy.
Anche le tecniche di compressione video possono essere suddivise in:
- **tecniche lossless**, dove la compressione e' un processo perfettamente reversibile che avviene senza perdita di informazione.
- **tecniche lossy**, dove la compressione non e' reversibile, nelle quali il video compresso e decompresso non sono perfettamente identici in quanto al momento della compressione sono state volutamente eliminate alcune informazioni ritenute "sacrificabili".

Un video e' costituito da una successione di immagini che si susseguono in rapida sequenza. Quindi quando si comprime un video, si stanno sostanzialmente comprimendo delle immagini.

Com'è' possibile comprimere un video?
Si utilizzano tecniche che sfruttano alcune caratteristiche intrinseche del video stesso, in combinazione con le caratteristiche del sistema visivo umano.
In particolare è' possibile comprimere un segnale video attaccando la ridondanza spaziale e temporale e le caratteristiche del sistema visivo umano.

E’ possibile comprimere un segnale video:
1) Rimuovendo la **ridondanza** (ripetitività’) statistica contenuta in un video e mantenendo solo le informazioni effettivamente utili; si cerca una rappresentazione “meno correlata” delle immagini, eliminando le “ripetizioni”. Si può’ dimostrare che pixel adiacenti, vicini, all’interno di una stessa immagini, presentano caratteristiche molto simili per quel che riguarda colore e luminosità’. La codifica intra-frames si occupa di rimuovere questa ripetitività’ altresì’ detta **ridondanza spaziale** all’interno dello stesso.
Esiste inoltre una netta correlazione non solo tra I pixel dello stesso fotogramma, ma anche tra I pixel di fotogrammi adiacenti. Un fotogramma e I due vicini (il successivo ed il precedente) risultano spesso pressoché’ identici (fanno eccezione le situazioni in cui si hanno cambi di scena). Questa **ridondanza temporale** tra fotogrammi vicini che ne sfrutta le loro minime differenze, viene trattata dalla codifica inter-frames.
2) Sfruttando alcune peculiarità’ del sistema visivo umano: la scarsa sensibilità’ dell’occhio alle alte frequenze video, soprattutto se si tratta di immagini in movimento.
E’ possibile “tagliare” alcune informazioni soprattutto relativamente alle alte frequenze di un’immagine senza introdurre artefatti Il sistema visivo umano non e’ infatti in grado di percepire le variazioni nei dettagli di figure molto frastagliate. E’ molto difficile rendersi conto di una perdita di dettaglio nelle fronde di alcuni alberi in movimento, molto più’ semplice invece notare anche la più’ piccola variazione di colore o luminosità’ nell’azzurro di un cielo limpido e sereno sullo sfondo di un video.

Compressione statica.
- Compressione dello spazio di colore: da RGB a YUV 4:1:1
- Blocking: l’immagine viene suddivisa in macroblocchi di 16x16 pixels
- DCT: Trasformata Discreta del coseno.
- Quantificazione
- Zig-Zag Scanning

Sostanzialmente si esegue una compressione in stile JPEG.

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.

Formati di codifica.
Il “formato” e’ una sorta di scatola che contiene il codec e lo integra con il sistema. Il codec e’ un software che indica al computer con quali operazioni matematiche deve manipolare le immagini per comprimerle e quali eseguire per visualizzare quelle compresse. I codec sono tantissimi al contrario dei formati.
Elenco dei principali formati: .avi, .mpeg, .mpeg2, .hdv, .mpeg4, .divx, .wmv, .mov, .flv, .3gp, ecc
Altri CodecVideo: Soresons Video, Quicktime, Real Video, Indeo Video, Cinepack, Mpeg2, Mpeg3, Mpeg3, H264, DIVX, XVID

Motion Estimation (ME).
L’encoder individua tra I fotogrammi adiacenti il blocco più’ simile (se non uguale). Dopodichè’ viene associato al blocco su cui e’ stata effettuata l’analisi, un vettore di moto, cioè’ una coppa di numeri tipo (x,y) = (-1,4) che individuano sul piano ipotetico rappresentato dal fotogramma, il vettore di spostamento, che indica verso ed entità’ dello spostamento del blocco passando dal fotogramma 1 al fotogramma 2.

Frames I/P/B.
Gli standard MPEG prevedono la classificazione dei frame in tre tipi: I, B, P.
- **I frame**: e' un frame video completamente indipendente
- **P frame**: (predictive frame) si basa un un precedente I frame.
- **B frame** (bi directional frame): e' costituiti da informazioni ricavate sia da I frame che da P frame (anche successivi) attraverso interpolazione.

Intra-Frames.
I fotogrammi di tipo I, chiamati anche Intra-Frames o Key-Frames (fotogrammi chiave), sono fotogrammi che vengono codificati utilizzando le informazioni contenute nel fotogramma stesso e non contengono nessun riferimento o informazione sui fotogrammi adiacenti. In pratica, sono compressi alla stregua di un'immagine singola, allo stesso modo di quando un'immagine viene salvata in formato JPEG. Nessun tipo di compressione temporale venga applicata a questi fotogrammi.
Può' essere generato da un encoder per creare un punto di accesso causale per consentire a un decodificatore di avviare la decodifica in maniera corretta, partendo da zero in quella posizione del video. In genere richiedono più' bit per essere codificati rispetto ad altri tipo di frame. Sono usati come riferimento per la decodifica di altre immagino. In genere I fotogrammi chiave vengono inseriti dei codec ogni qualvolta vi sia un repentino cambiamento tra due immagini successive.
Se inoltre viene specificato un intervallo massimo tra un fotogramma chiave ed il successivo il codec dovrà' necessariamente inserire un fotogramma chiave anche se non strettamente necessario.

P-Frames.
Il fotogramma P, (Predicted Freme) viene codificato utilizzando informazioni acquisite in base al fotogramma che lo precede, sia quello di tipo I o di tipo P. Ogni macroblocco di 16x16 pixels di un P-Frame può' essere codificato in modo indipendente (come nel caso del I-Frame) oppure può' essere compensato, cioe' bilanciato utilizzando informazioni del fotogramma precedente. Utilizzando le somiglianze tra fotogrammi successivi I fotogrammi P risultano essere più' piccoli del corrispondenti I-Frames.
Un P-Frame puo' contenere: dati del fotogramma, gli spostamenti (vettore di movimento) rispetto al fotogramma di cui dipende o una combinazione dei due. Un fotogramma di tipo P contiene informazioni della posizione (X',Y') nel fotogramma corrente in cui si e' spostato un blocco che aveva coordinate (X,Y) in quello precedente (Motion Estimation/Compression).
Lo svantaggio dell'utilizzo di questo tipo di fotogrammi si ha in fase di decodifica. E' infatti necessario "ricostruire" ciascun fotogramma P prima di poterlo visualizzare e per fare questo si deve sempre partire dal fotogramma P seguente l'ultimo fotogramma chiave.

B-Frames.
Il fotogramma B-Frame (Bidirectional Predicted, Bidirectional-dipendent Frames) richiede la precedente decodifica di altri frames prima di essere decodificato. Sostanzialmente I fotogrammi B sono di tipo Bidirezionale, nel senso che fanno riferimento sia a ciò' che li precede sia a quello che segue. Il fotogramma può' contenere: I dati del fotogramma, gli spostamenti (vettore di movimento) rispetto al fotogramma da cui dipende o una combinazione dei due.
Per I fotogrammi di tipo B la ricerca del moto e' effettuata non solo sul fotogramma precedente (come nel caso del P-Frame) ma anche nel successivo. La codifica ed anche la decodifica risultano quindi decisamente più' complesse. Sostanzialmente I fotogrammi sono di tipo bidirezionale nel senso che fanno riferimento sia a ciò' che li precede, sia a quello che segue. Inserire in un fotogramma informazioni che si riferiscono ad un fotogramma

successivo e' possibile solo alterando l'ordine in cui I fotogrammi vengono archiviati all'interno del file video compresso. In genere richiedono meno bit per la codifica rispetto agli I-Frame o al P-Frame.

Esempio.
Supponiamo di avere 4 fotogrammi da comprimere.
Il primo di questi sarà necessariamente un fotogramma chiave, mentre vogliamo che I successivi due siano B-Frames (che generalmente hanno una dimensione di ¼ del P-Frame corrispondente). L'ultimo deve essere necessariamente un P-Frame, in quanto I fotogrammi B necessitano dopo di loro qualcosa da cui essere derivati. In sequenza avremo: (1) I, (2) B, (3) B, (4) P. I fotogrammi verranno archiviati all'interno del filmato in questo modo: (1) I, (4) P, (2) B, (3) B. Dopo aver codificato l'I-Frame, l'encoder salta avanti di due fotogrammi e codifica quello che e' destinato ad essere il fotogramma P (ovvero il quarto) e lo codifica come se seguisse immediatamente l'I-Frame.
Questo processo genere una P-Frame di dimensioni superiori a quello che si avrebbe codificando come P-Frame il secondo fotogramma, in quanto generalmente vi saranno piu' cambiamenti (ovvero differenze) tra il primo fotogramma ed il quarto che non tra il primo e il secondo. Tuttavia, l'utilizzo dei due B-Frame porterà complessivamente ad una riduzione del numero di informazione (dimensioni) necessarie alla codifica.

PARTE 2

Disk forensics

Vedremo cosa c'è dietro un dispositivo, a basso livello del computer con l'utilizzo di strumenti software che ci aiutino in un'analisi forense.

Cosa succede quando avviamo il computer?

- Reset della CPU ad un livello di corrente basso
- Power-On Self Test (POST) l'elettronica si autodiagnostica
- BIOS consente di utilizzare tastiera, dischi, memoria centrale. L'elettronica inizia a capire come usare il sistema software
- BOOT si aggancia a delle parti di memoria su disco

Per bypassare la password del BIOS basta togliere la batteria o le batterie.
Nella fase di avvio di un componente elettronico sono più importanti le fasi di BIOS e BOOT.

Little Endian *e* ***Big Endian*** sono due tipologie differenti di ordinamento delle cifre di una codifica binaria. Nella prima la memorizzazione inizia dal byte meno significativo per finire con il più significativo; viceversa nella seconda.
Non bisogna confondere codifica con crittografia, nella prima si può passare da una tipologia ad un'altra senza alcun tipo di segreto da decifrare con una funzione.

Tutti i file iniziano con una intestazione o header, questa è la parte che interessa di più perché identifica il file.
EXIF area è la zona in cui nella codifica JPEG si può scrivere.
Come funziona un dispositivo di memorizzazione?
Un **Hard Drives** (disco fisso) può essere rappresentato con una disposizione a cerchio divisa in settori dove un giro è una traccia; all'interno di ognuna di queste tracce ci sono delle celle che vengono caricate automaticamente.

La componente **SMART** viene usata per registrare informazioni basilari sul controller come ad esempio quante volte il disco è stato girato, acceso e la sua temperatura interna attuale.
Queste informazioni che prevede lo stato di salute del disco aiutano a capire quando un disco probabilmente smetterà di funzionare correttamente.
SMART è particolarmente importante per gli SSD e per un'analisi forense dato che contiene informazioni come l'ultimo accesso.

La componente **SPECIAL TRACK** è la prima traccia sul disco ed è usata per immagazzinare informazioni sul driver coma la sua geometria, la posizione dei settori danneggiati e le tabelle di transizione.
Contrassegnando intenzionalmente la porzione del disco come danneggiata, un individuo può nascondere dati in queste aree dal sistema operativo.

La componente **HIDDEN PARTITION** è invisibile al sistema operativo. È facile da trovare usando strumenti che sono specificamente progettati per condurre ispezioni forensi.

Vi sono diverse famiglie per i file system come: FAT, NTFS, UFS…
FILES

- Quando un file occupa meno di un cluster altri file non utilizzeranno lo spazio aggiuntivo in quel cluster (slack space)
- Quando un file viene cancellato la sua voce nel file system viene aggiornata per indicare il suo stato di cancellamento ed i cluster precedentemente assegnati alla memorizzazione vengono deallocati e possono essere riusati per un nuovo file.
- I dati rimarranno sul disco fino a quando un nuovo file non li sovrascrive.

Un file system dà informazioni riguardo ad un certo file all'interno di una certa partizione si trova in una certa coordinata.
Mi dice inoltre quali cluster sono occupati, conoscendo lo spazio disponibile.

Il file inizia dal cluster, lo spazio che resta libero è lo slack space e in esso si possono nascondere informazioni e dati.
Esistono anche altri **metodi per nascondere dati**:

- Partizioni nascoste
- Cambiamento di nome
- File nascosti
- Flusso di dati alternativi
- Steganografia (nascondere informazioni all'interno di un'immagine)

Strumenti per l'analisi forense
Pro: operazioni automatiche, facili e veloci, comoda interfaccia grafica.
Contro: necessitano senso dell'uso e di cosa fanno esattamente questi strumenti, buon senso e consapevolezza. Inoltre si hanno diversi risultati con diversi strumenti

LOG Files
La prima cosa da fare per un'analisi forense è cercare il file di log, annotando ogni cosa nel registro di sistema.

La copia forense su una chiavetta USB è un'operazione ripetibile, mentre su un computer acceso è irripetibile. Nel dubbio bisogna agire sempre nel regime di non ripetibilità (es. con un cellulare)
Bisogna inoltre garantire di non poter scrivere sul dispositivo su cui si vuole fare la copia.

Il **Mount** è un comando dei sistemi operativi Unix che permette il monitoraggio di un file system ci consente di aprire il dispositivo ed analizzare la partizione del disco. È il punto di ingresso al file system.

Metodo di acquisizione di un dispositivo:

- Calcolare l'hash
- Fare una copia bit a bit
- Calcolare l'hash e confrontarla con la prima già effettuata

Il primo step dell'analisi dei dati è avere la rappresentazione della sequenza cronologica degli eventi, la **Timeline**. Vi è anche una **Super Timeline**.
In seguito vi la ricerca di un file o directory.

Il **file carving** è il processo di assemblaggio dei file del computer da frammenti in assenza di metadati del file system.

Strumenti per l'analisi dei dati

- DHash: effettua l'hash mentre crea la copia
- Guymager: effettua acquisizione e la gestione dei casi
- Catfish: serve ad individuare un determinato elemento
- FindWide: effettua ricerca nei contenuti di un file
- Hunchbacked: principalmente si occupa dell'implementazione

Autopsy è una piattaforma forense digitale che consente di fare quanto detto finora attraverso l'interfaccia grafica.

Analisi forense di sistemi Linux

La metodologia di analisi forense di un sistema GNU/Linux segue sostanzialmente gli standard e le best practices in uso nella digital forensics ma, per poter applicare correttamente tali metodologia, in particolare nelle fasi di **identificazione**, **acquisizione**, ed **analisi**, è necessario conoscere le caratteristiche, le potenzialità e le criticità dello specifico sistema.

Storia di Unix e Linux

All'inizio degli anni '70, il sistema operativo (OS) **Unix** - abbreviato da UNICS (Uni Placed Information and Computing Service) – evolve dalle ceneri di un progetto **AT&T Bell Labs** atto a fornire all'utente l'accesso simultaneo ai servizi di computer mainframe.
Unix crebbe di popolarità e dimostrò sul campo la sua **alta affidabilità**, iniziando a sostituire i sistemi operativi nativi su alcune comuni piattaforme mainframe.
La nuova versione del sistema, riscritta in linguaggio C, ne migliorò sensibilmente la portabilità e consentì l'emersione sul mercato di diverse versioni di Unix, comprese quelle

per microcomputer. Nei decenni successivi alcuni derivati di Unic, detti Unix-like, presero forma. E' il caso di ricordare **Mac OS** di Apple, **Sun Microsystem Solaris**, e **BSD**.
Gli sforzi per creare una versione liberamente disponibile di Unix iniziarono negli anni '80 con il progetto **GNU** (Gnu's Not Unix) General Public License (**GPL**), ma non riuscirono a produrre i risultati sperati.
Questo portò il programmatore finlandese **Linus Torvalds** ad affrontare lo sviluppo di un nuovo kernel Unix (il modulo di controllo centrale di un sistema operativo). Usando il sistema operativo educativo **Minix**, Torvald progettò con un successo un kernel affidabile nel 1991, rendendo il codice sorgente liberamente disponibile per il download pubblico e la manipolazione sotto licenza GNU GPL.
Il progetto fu poi chiamato Linux (una combinazione del nome di Torvalds "Linus", con "Unix").
La flessibilità e l'efficienza di Linux lo hanno conseguentemente portato all'adozione diffusa – da parte di industrie, aziende e singoli utilizzatori in tutti i continenti. Oggi il sistema è presente su smartphone, orologi, auto, elettrodomestici, installazioni militari e in svariati altri dispositivi. La maggior parte dei server attualmente presenti nella rete internet utilizzano Linux.
IBM lo scelse nel 2011 per realizzare **Sequoia**, il super computer che doveva essere il più potente mai creato.

GNU-Linux
Il 100% dei supercomputer attualmente esistenti usa GNU-Linux:
- esecuzione di carichi di lavoro ad elevato disponibilità all'interno di data center e ambienti cloud.
- modularità, che consente ad ogni singolo componente del sistema operativo Linux di essere sottoposto ad *audit*, monitorato e protetto
- dotazione di modelli e strumenti integrati, come SELinux, che aiutano a **bloccare**, **monitorare**, **segnalare** e **rimediare** in maniera più completa eventuali problematiche relative alla sicurezza.

Sistemi operativi Windows
La prima differenza con i sistemi operativi Windows è il **file system**.
Windows utilizza File System **NTFS**, **FAT** e **exFAT** o **FAT64**. **ReFS** (Resilient File System) è l'ultimo sviluppato da Microsoft introdotto con Windows 8 e ora disponibile per Windows 10.

L'architettura del File System differisce assolutamente dagli altri File System di Windows ed è principalmente organizzata in una forma B+-tree.

NTFS
NTFS è il più adoperato File System Windows: una sola struttura fissa, il **boot sector**. Le altre strutture di controllo sono predeterminabili essendo rappresentate da file.
La principale struttura è delineata dalla **MFT** (Master File Table), anch'essa costruita da file – fisicamente – ma logicamente strutturata come una sequenza lineare minore o uguale a 2^48 record di ampiezza da 1 a 4 Kbyte.

File System Linux

Linux impiega come regola generale il *mounting* dei dispositivi su *directory*, generalmente **/mnt** e **/media**.
L'organizzazione del file system di Linux è **gerarchica**. La sua struttura è ad albero con il livello più alto espresso dal simbolo "/" e denominato **directory root**.
Non esiste distinzione tra hardware e software (le periferiche hardware vengono rappresentate come dei ***file speciali*** e qualsiasi parte del sistema è figlia della directory radice.

Directory Linux
All'interno della directory di root è presente un insieme di directory comuni a tutte le distribuzioni Linux. Quello che segue è un elenco delle più comuni presenti nella root.
- /bin: applicazioni per la gestione del sistema
- **/boot**: kernel e file di configurazione necessari al processo di boot
- **/dev**: file dei devices
- **/etc**: file di configurazione, script di avvio, ecc
- **/home**: directory home degli utenti locali
- /**lib**: librerie di sistema
- **/media**: dispositivi rimovibili (media) montati (caricati) come CD, fotocamere, ecc
- **/mnt**: punto di montaggio per media esterni
- **/opt**: contiene applicazioni aggiuntive ed opzionali
- **/proc**: contiene un file system virtuale. Viene creato dal kernel dinamicamente, istante per istante, in memoria e non sul disco. Al suo interno sono contenute informazioni relative al sistema
- **/root**: home directory per l'utente root
- **/sbin**: contiene programmi di sistema eseguibili solo dall'amministratore del sistema
- **/sys**: file di sistema
- **/tmp**: file temporanei
- **/usr**: file ed applicazioni che per la maggior parte disponibili a tutti gli utenti e non indispensabili per il sistema
- **/var**: parte variabile dei programmi. Contiene log, mail, database, ecc

Tutti i file di un sistema Linux hanno **permessi** che abilitano o meno gli utenti alla **visualizzazione**, **modifica** o **esecuzione**. Il super utente root ha l'abilità di accedere ad ogni file di sistema.
Ogni file possiede delle restrizioni di accesso, restrizioni sull'utente ed è associato con un proprietario/gruppo.

Analisi su sistemi Linux
Un ausilio importante per l'analisi di un sistema Linux proviene dalla compressione del processo di avvio. Infatti, la conoscenza dei file coinvolti in detto processo potrebbe aiutare l'esaminatore forense a determinare, ad esempio, la versione del sistema operativo in esecuzione e la data di installazione.
Inoltre, ciò consente di puntare la ricerca delle evidenze in caso di modifica fraudolenta di alcuni aspetti del processo di avvio che, data la sua natura di sistema aperto, un utente dotata di privilegi sufficienti, potrebbe aver modificato.

Cenni su processo di avvio di Linux
Il primo passo del processo di avvio di Linux è l'esecuzione del **boot loader**, che individua e carica il kernel.
Il kernel è il cuore del sistema operativo ed è generalmente presente nella directory /boot.
Successivamente viene montato in memoria **initrd** (Initial RamDisk).
Il File System temporaneo initrd contiene i driver di dispositivi, i moduli del File System, i moduli del volume logico e altri elementi richiesti per l'avvio ma non presenti nel kernel.
Terminata la cosiddetta fase di **bootstrap**, il kernel procede ad inizializzare l'hardware del sistema e ad avviare il processo **/sbin/init** che porterà il sistema in uno stato operativo.
Due sono le filosofie che organizzano il funzionamento di init: **System V** e **BSD**.

System V
Nel metodo System V, il processo init, legge il file **/etc/inittab** per determinare l'impostazione predefinita del **runlevel**.
Un runlevel è un numero che identifica il set di script che una macchina eseguirà per un dato stato. Ad esempio, nella maggior parte delle distribuzioni Linux, *runlevel 3* fornirà un pieno ambiente di console multiutente, mentre *runlevel 5* produrrà un ambiente grafico.
Da notare che ogni voce di una directory di runlevel è in realtà un collegamente software ad uno script in **/etc/init.d/**, che verrà avviato o interrotto a seconda del nome del collegamento: il nome che inizia con "**S**" indica l'ordine di avvio, mentre quelli che iniziano con "**K**" ne indicano l'ordine di interruzione del servizio.

System BSD
Nel metodo BSD, invece, a ogni *runlevel* corrisponde uno script (solitamente chiamato ***/etc/rc.d/rc.X***), che ha il compito di avviare tutti i processi necessari a portare il sistema nel runlevel richiesto.

Filesystem Linux
Esaminiamo la peculiarità del File System di Linux, ovvero il meccanismo con il quale i file vengono immagazzinati ed organizzati su un dispositivo di archiviazione.

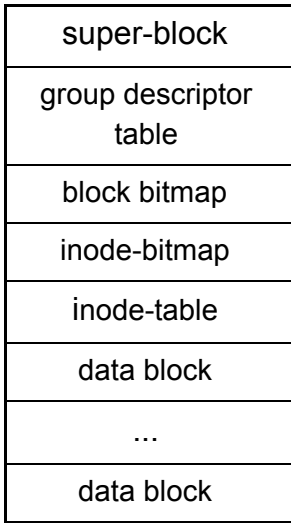
Vengono utilizzati principalmente due tipologie **Ext3** e **Ext4**.
Ext3 è retrocompatibile con il file system Ext2 da cui deriva con l'aggiunta del **journaling** che permette di eseguire modifiche ai file adoperando il concetto di transazione, preservando in questo modo l'integrità dei dati. Genericamente un file di Linux consiste in uno o più blocchi di dati contenenti qualsiasi tipo di informazioni (una directory è un particolare tipo di file).
Ad ogni file è associato un **inode**; inoltre gli inode vengono identificati tramite un numero chiamato **inumber**; con un inumber è possibile identificare univocamente un file all'interno del File System.

Inode
Poiché un inode ha una dimensione limitata e ha lo spazio solo per un piccolo numero di puntatori diretti ai blocchi di dati, i blocchi successivi sono referenziati in modo indiretto.
L'accesso indiretto ai blocchi di dati è realizzato attraverso alcuni puntatori in ogni inode.

Un file richiede più blocchi di quelli che possono essere indirizzati dai puntatori diretti, viene allocato un blocco che non fa parte del file, ma viene usato per contenere puntatori diretti ai blocchi successivi del file (indirizzamento indiretto singolo).
Se il file è particolarmente grande, un blocco pieno di puntatori diretti può non bastare, in questo caso sarà necessario usare uno o due livelli di indirizzamento (indirizzamento indiretto doppio o triplo).
Un puntatore indiretto doppio di inode punta a un blocco che contiene puntatori indiretti singoli, ciascuno dei quali punta ai blocchi contenenti puntatori diretti. Così il sistema operativo può seguire una catena fino a 4 di questi puntatori per accedere ai blocchi di file molto grande.
Vi sono grandi differenze tra File System Ext2 e Ext3.
Su Ext3 il recupero dei dati è decisamente arduo e, in alcuni casi, addirittura impossibile; per garantire l'integrità dei dati dopo un malfunzionamento, il sistema azzera tutti i puntatori agli inode, che vanno irrimediabilmente persi una volta che il file è in stato non allocato.
Il contenuto del file originale sarà ancora presente nei blocchi di dati non allocati dal File System, almeno fino a quando tali blocchi non saranno riutilizzati, ma non esiste una "mappa" per ricostruire quei blocchi di dati nel file originale.

File carving
I metodi tradizionali per il recupero dei file si basano su strumenti di **file carving** quali **Scalpel** e **Foremost**. Questi strumenti, impegnandosi sull'allocazione consecutiva dei blocchi di dati che comportano un file, consentono, adoperando una *signature* – che normalmente identifica un particolare tipo di file – il recupero della maggior parte o di tutto il file, raccogliendo via via i blocchi successivi.
Se il formato del file include anche una signature di fine file, lo strumento sarà in grado di interrompere la raccolta dei blocchi appartenenti al file in esame.
Pur tuttavia, vi sono alcuni problemi derivanti dall'utilizzo di detta tecnica durante il recupero dei dati dai sistemi Linux.
1. Data l'intrinseca struttura del sistema operativo, orientata ampiamente al testo, molti artefatti Linux mancano di signature valide.
2. Ext3, come già evidenziato, utilizza i blocchi indiretti nel mezzo del contenuto del file per memorizzare i metadati. Questi *blocchi indiretti* – che Foremost ignorerà semplicemente sia come blocco che come contenuto – vengono utilizzati per archiviare i puntatori di riferimento ai blocchi di dati quando un file diventa troppo grande e non può essere più rappresentato dal numero relativamente piccolo di puntatori di riferimento all'inode; ciò potrebbe causare il danneggiamento del file qualora vengano estratti assieme ai blocchi di dati che lo compongono.
3. Il tentativo di recuperare un file raccogliendo blocchi consecutivi si interromperà quando verrà individuata una frammentazione del file su più aree del disco.

File System Ext
In generale, il layout Ext, si basa su blocchi sequenziali di 1024, 2048 o 4096 byte numerati e raggruppati, a loro volta, a gruppi.
Ogni catena di blocchi contiene metadati che documentano la sua struttura interna.
La disposizione generale di tutte le catene di blocchi è la seguente:



Il **superblocco** contiene molti metadati essenziali del File System, come ad esempio il **numero** e la dimensione dei blocchi, il **numero di inode** e i **blocchi riservati**.
La **group descriptor table** contiene le informazioni per ogni catena di blocchi nel File System e la **block bitmap** memorizza lo **stato libero/utilizzato di ciascun blocco**.
Allo stesso modo, la **inode-bitmap** memorizza lo stato **libero/utilizzato** di ogni inode nella tabella degli inode.
Il resto della catena di blocchi è costituito da dati consecutivi che vengono utilizzati per memorizzare i dati.
In tutti i File System Ext, quasi tutti i metadati di file/directory, come ad esempio *timestamp*, diritti di accesso, riferimenti a blocchi di dati, sono memorizzati nell'inode del file (i nomi del file, ad esempio, non lo sono, sebbene non siano sempre considerati come metadati).
Gli indoe sono numerati, a partire dall'inode numero 1 e memorizzati nella tabella degli inode della rispettiva catena di blocchi.
Con la Ext3, per motivi di compatibilità con le versioni precedenti, sono state implementate solo poche modifiche alla struttura inode.

File System Ext4
Il layout generale di Ext4 è molto simile a Ext3 anche se ha subito alcune modifiche.
Una caratteristica, ad esempio, introdotta in Ext4 è il concetto dei cosiddetti **Flex Group**. I Flex group combinano più gruppi di blocchi in un unico gruppo di blocchi logici. Solo il primo gruppo di blocchi contiene le *bitmap* di blocco e *inode*, nonché le tabelle di *inode* di tutti i gruppi di bocchi.
E ancora:
- Spazio degli indirizzi a 48 bit
- Utilizzo di estensione (Extend) invece di catene di blocchi indiretti
- Timestamp a 64 bit con precisione al nanosecondo
- Data e ora di creazione del file

Il recupero dei dati, anche con detta versione del File System, è particolarmente ardua.
Pur utilizzando una tecnologia diversa da Ext3 basata su Extent, cioè un gruppo di blocchi contigui invece del mapping del blocchi indiretti, non cambia la gestione dei puntatori che vengono comunque azzerati dopo la cancellazione di un file.

Logical Volume Manager
Oltre a ciò vi è un'ulteriore complicazione dovuta all'organizzazione dei File System di Linux in blocchi logici tramite la tecnologia **LVM** (Logical Volume Manager).

Linux vs Windows
Ma cosa c'è di realmente diverso in Linux rispetto a Windows, molto più conosciuto?
- Non vi è alcun registro
- È necessario raccogliere le informazioni da fonti diverse e sparse
- La struttura del File System è diversa
- Non vi sono date di creazione file alla versione del File System nota come Ext4
- I metadati importanti vengono azzerati con la cancellazione dei file
- I file/dati sono per lo più composti da semplice testo
- Ottimo per la ricerca di stringhe e l'interpretazione dei dati
- Accesso complesso al File System data la presenza di Encryption, RAID, LVM
- Molteplici partizioni, anche nascoste, da montare

Linux usa il kernel come un singolo grande processo eseguito interamente in un unico spazio di indirizzamento, rappresentato da un singolo file binario. Tutti i servizi del kernel vengono eseguiti nello spazio di indirizzamento dedicato ed è il kernel stesso a richiamare direttamente le sue funzioni.

Windows utilizza invece programmi e sottosistemi in modalità utente e quindi limitati in termini di risorse di sistema a cui si ha accesso, al contrario della modalità kernel che ha, invece, accesso illimitato alla memoria di sistema e ai dispositivi esterni.

Quindi, dove cercare? Cosa analizzare? Quali artefatti tenere in considerazione?
L'analisi forense di un sistema GNU/Linux pu essere davvero ardua e rappresentare una vera sfida per un esperto di Digital Forensics.
Da un lato il sistema fornisce una grande quantità di informazioni rispetto ad un sistema Windows, dall'altro, la sua prerogativa di sistema aperto consente all'utente con privilegi di amministratore, la compilazione del kernel includendo tutto le patch che desidera, trasformando l'analisi in un incubo.

Analisi forense di un sistema GNU/Linux
È consigliato quindi, prima di intraprendere l'analisi del sistema, porsi alcune semplici domande:
1. Quando è stato installato il sistema operativo Linux?
2. Quale distribuzione Linux è installata?
3. L'orologio e la time zone della macchina erano corretti?
4. Qual era l'indirizzo IP della macchina al tempo dell'accadimento?
5. Chi era connesso alla macchina in corrispondenza della date e ora segnalate?
6. Sono stati riscontrati accessi al server Web del cliente identificati in base alla date e ora segnalate?
7. Vi è un cronologia dei comandi digitati?

Va tenuto in debita considerazione che, la fase più importante dell'analisi del caso in oggetto, è costituita proprio dai dati da acquisire e soprattutto dalla profonda conoscenza delle strutture utili al reperimento delle evidenze rilevanti.
Nel caso di **dati volatili**, si ha davvero una sola possibilità di acquisirli correttamente; E' necessario quindi documentare attentamente tutte le operazioni sin dalla fase di acquisizione forense.

Di seguito verranno fornite le risposte alle domande sopra elencate:
1. La **data di installazione** del sistema operativo può essere estrapolata dal file **/root/install.log** oppure dai ***file.key*** contenuti nella directory ***/etc/ssh***
2. La **versione del sistema operativo e le informazioni sulla release** sono identificate dal contenuto del file ***/etc/os-release***
3. Le informazioni sul **fuso orario della macchina** sono identificate dal contenuto del file ***/etc/localtime*** adoperando l'output del comando **zdump**. Per ulteriore conferma è possibile ricercare il file nella directory ***/usr/share/zoneinfo***
4. L'**indirizzo IP della macchina** è identificato dal contenuto del file ***/etc/hosts*** per gli indirizzi statici e dal contenuto del file ***/etc/dhcp/dhclient.conf***, ***/var/lib/dhclient/dhclient.leases***, ***/var/run/dhclient.pid***, per gli indirizzi dinamici (DHCP)
5. I dettagli delle **attività di accesso degli utenti** sono identificati dal contenuto dei file ***/var/log/wtmp*** e ***/var/log/auth.log***
6. [DA COMPLETARE]
7. Il riepilogo dei **dipositivi di archiviazione USB collegati** è identificato dal contenuto del file ***/var/log/syslog***. Le voci relative ai file recentemente utilizzati sono stati evidenziati dal contenuto di ***/home/[username]/.local/share/recently-used.xbel***
8. La **cronologia dei comandi digitati** è rilevata dal contenuto del file ***/home/[username]/.bash_history***. Non è possibile rilevare i timestamp di esecuzione, dato che non è prevista di default. Va comunque tenuto in debito conto che la stessa cronologia può essere modificato o rimossa dall'utente. Nel caso di utilizzo di **sudo**, la cronologia può essere rinvenuta in ***/var/log/auth.log*** e ***/var/log/sudo.log***

Questi semplici quesiti consentono un iniziale approccio all'analisi forense del sistema Linux, avvalendosi successivamente dei molteplici strumenti a supporto delle indagini.
La vera sfida che questi strumenti devono superare riguarda la necessità di non modificare o danneggiare, neanche minimamente o temporaneamente, nessuna delle periferiche che possono contenere dati sensibili.

Distribuzioni forensi di Linux
Caine, DeFT, TSURUGI, Paladin, Raptor, SIFT, Kali, Parrot e BlackBox

Possono essere suddivisi in quattro macro-categorie:
- **Tool di acquisizione**: consentono l'acquisizione delle evidenze digitali da una macchina
- **Tool di analisi**: consentono l'analisi delle evidenze ottenute in fase di acquisizione, a loro volta si suddividono in **tool di analisi di basso livello** e **tool di analisi di alto livello**. Fra i tool di analisi di alto livello è possibile individuare, inoltre, le seguenti categorie:
    - Tool di *cracking*: consentono il recupero, a partire da un'evidenza cifrata, dell'evidenza originale e/o la password utilizzata per la cifratura

- Tool integrati: supportano il consulente informatico forense nella ricerca, estrazione e stesura degli elaborati peritali, consentendogli il riporto, in modo dettagliato, delle informazioni rilevanti trovate

Per l'analisi di ciò che è avvenuto sul sistema in esame sono essenziali due strumenti:
1. The **Sleuth Kit** basato su "The Coroner's Toolkit"
2. **log2timeline/Plaso**

Sleuth Kit e Autopsy
The **Sleuth Kit** e la sua estensione grafica **Autopsy** è ormai consolidato da anni e permette di eseguire la timeline del sistema basata sui metadati temporali del File System che, a mezzo dell'opzione ***daily summary*** consente anche la costruzione di un grafico (istogramma) contenente l'attività rilevata sul sistema durante ogni giorno e ad ogni ora del periodo selezionato.

Autopsy ha funziona molto avanzate di gestione dei file e di analisi degli stessi – inclusi i file cancellati – permettendo la visione degli stessi in diverse modalità, l'estrazioni di immagini, l'analisi delle estensioni e del loro cambiamento.

Log2Timeline
Con la nuova versione di **Plaso** è uno strumento che permette l'estensione della timeline generata tramite **TSK** (The Sleuth Kit) aggiungendo attività ricavate dai metadati o da informazioni interne ai file, quali ad esempio dati **exfi**, di **registro**, **eventi di sistema**, **log di antivirus**, **journaling NTFS**, **storia della navigazione internet**, etc., consentendo un'agevole analisi degli accadimenti molto più precisa e puntuale.

Bulk Extractor
E' un software open source sviluppato da Simson L. Garfinkel, professore e ricercatore californiano. Il software consente l'estrazione di mail, artefatti Facebook, indirizzi e domini web, numeri di telefono, carte di credito, prefetch, indirizzi IP e molto altro ancora.
Tramite accesso sequenziale a livello di settore, Bulk Extractor è in grado di estrarre da dischi, immagini forensi o directory di file, informazioni utili per gli investigatori senza la necessità di dover accedere al file system sottostante. Oltre al rilevamento delle informazioni direttamente disponibili sul disco durante il "parsing", Bulk Extractor è in grado di rilevare, decomporre e processare ricorsivamente i dati contenuti all'interno di archivi complessi con svariati algoritmi.
Il software consente quindi accesso alle analisi dei contenuti dei vari file zip/rar presenti nelle aree allocate e non allocate del sistema.
Anche per questo aspetto, se non opportunamente configurati, diversi tool commerciali rischiano di trascurare informazioni rilevanti non parsificando gli archivi.
Il software produce delle **Feature Files**, ovvero dei file suddivisi per tipologia di dati estratti e contenenti le informazioni trovate.

Testdisk, Photorec, Scalpel, Foremost
Infine, per quanto riguarda il recupero di dati cancellati su sistemi Linux, ricordiamo Testdisk/Photorec, Scalpel e Foremost.

- **Testdisk** permette di ricostruire partizioni danneggiate di qualsiasi tipo, indispensabile per la ricostruzione di supporti danneggiati
- **Photorec** consente il recupero dei file cancellati dalle aree di memoria non allocate. Il recupero utilizza la cosiddetta tecnica di ***carving***, basata su firme dei file
- **Foremost** è il più famoso tool di carving su Linux, in grado di lavorare su file immagine (dd, Ewf, ecc) oppure direttamente sul dispositivo. Gli *header* e i *footer* dei file da ricercare possono essere specificati nei file di configurazione o attraverso parametri della riga di comando. Una volta in esecuzione crea nella directory di output un file denominato ***audit.txt*** ed una serie di sub directory nominate con il tipo di file ritrovato (doc, jpg, tiff, ecc)
- **Scalpel** è stato riscritto a partire da Foremost onde consentire un miglioramento di performance e riduzione dell'utilizzo di memoria. Nel caso di Scalpel, i file da identificare devono essere specificati nel file di configurazione ***/etc/scalpel/scalpel.conf***.

CAINE
CAINE (Computer Aided Investigative Environment) è una distribuzione live GNU/Linux italiana, basata su Ubuntu, creata come progetto Digital Forensics.
Offre un ambiente forense completo, organizzato per integrare gli strumenti software esistenti come moduli software e per fornire un'interfaccia grafica friendly. Il principale obiettivo di CAINE è quello di dare un ambiente di supporto alle investigazioni digitali.
La novità di CAINE 9.0 è che tutti i dispositivi sono (inizialmente) in modalità **read-only**. Questo nuovo metodo di blocco della scrittura assicura che tutti i dischi vengano effettivamente preservati dalle operazioni di scrittura accidentale.

Tools
- **Stegdetect** ottimo tool steganografico per scoprire le informazioni nascoste nelle immagini
- **Ophcrack** per l'exploit delle password
- **Fundl** per recuperare tutti i files cancellati in un hard disk
- **AIR** (Automated Image Restore) utility avanzata per la creazione di immagini di supporti di memoria
- **Exif** un software che permette di estrarre i metadati EXIF dalle fotografie digitali
- **DvdDisaster** recupero di dati da supporti ottici danneggiati
- **Wipe** software per cancellare file in modo che non siano più recuperabili
- **Fundl** software per il recupero rapido dei dati cancellati
- **Stegbreak** estrazione dei dati nascosti in file JPG mediante steganografia
- **GtkHash** calcolo dell'hash dei un file mediante diversi algoritmi

Steganografia

La circolazione e la condivisione delle informazioni ha, nella nostra epoca basata sulla comunicazione, un'importanza cruciale. Spesso però c'è il **desiderio** o la **necessità** di mantenere queste comunicazione **riservate**, in modo che nessuno, tranne il legittimo destinatario, possa acquisire informazioni ritenute sensibili.

L'approccio più utilizzato per rendere private la conversazione è quello di rendere il

messaggio **incomprensibile** a chi non è a conoscenza delle tecniche necessarie a renderlo nuovamente leggibile.
La cosiddetta rivoluzione digitale ha portato anche nel settore delle segretezza (o sicurezza) delle informazioni nuovi paradigmi di implementazione di teorie e tecniche già note.
La sicurezza che si occupa di questo problema è la **crittografia**, il cui obiettivo principale è quello di **garantire la segretezza attraverso la codifica del messaggio**.
Il messaggio è visibile, ma è **codificato** mediante appositi algoritmi di cifratura che lo rendono incomprensibile a chi non è a conoscenza dei relativi **sistemi di decodifica**.

Il **watermarking** (letteralmente *filigranatura*) invece è la tecnologia grazie alla quale è possibile inserire opportune informazioni in un segnale, in particolare su file multimediali quali immagini e video, magari per segnalarne l'originalità o il titolare dei diritti di proprietà.
Un watermark, proprio come le filigrane delle banconote, deve essere visibile solo in certe condizioni – per esempio dopo l'applicazione di opportuni algoritmi.

La **steganografia** nasconde l'esistenza stessa del messaggio, includendo in un mezzo che potremmo definire "neutrale" e garantendo quindi la segretezza della comunicazione.
Il termine steganografia deriva dai vocaboli greci *sèganos* (nascosto) e *gràfein* (scrivere).

Insieme di tecniche che consentono di nascondere messaggi, che **devono essere esseri intelligibili al solo destinatario**, inserendoli all'interno di un contesto del tutto estraneo, che funge da **contenitore**, il grado non tanto di nascondere il contenuto ma la stessa esistenza della comunicazione, agli occhi di un eventuale osservatore.

La steganografia è la scienza (arte) di comunicare senza essere osservati.

A differenza della crittografia, dove l'avversario sa dell'esistenza della comunicazione, l'obiettivo della steganografia è nascondere l'esistenza stessa della comunicazione nascondendo il vero messaggio all'interno di un messaggio dal significato innocuo.

Steganalisi
Tecniche di analisi per la rilevazione di messaggi nascosti (anche senza decifrare).
Possibili motivazioni possono essere: **controspionaggio**, anti terrorismo, controllo dell'opinione pubblica in regimi totalitari, raccolta di dati (anche sensibili) per motivazioni commerciali per fini illeciti.
Indipendentemente dalle motivazioni lo sviluppo di tecniche di steganalisi è indispensabile allo studio delle stesse tecniche di steganografia.

Steganografia vs Crittografia
In certi scenari l'esistenza stessa di un messaggio cifrato può destare sospetti e non essere ammessa.
Nella steganografia l'esistenza stessa di una comunicazione nascosta rimane segreta.
Importante non confondere la crittografia con la steganografia in quanto:
Crittografia: ha lo scopo di nascondere il **contenuto** di un messaggio.
Steganografia: ha lo scopo di nascondere l'**esistenza** di un messaggio.
In molte situazioni l'uso della sola crittografia o della sola steganografia non è sufficiente

quindi le due tecniche vengono combinate.

Il problema dei prigionieri
Ai giorni nostri lo studio di questa materia nella letteratura scientifica si deve a Simmons che nel 1983 formulò il **problema dei prigionieri**.
In questo conteso **Alice** e **Bob** sono in prigione e devono escogitare un piano per fuggire. Tutti i loro messaggi vengono scambiati tramite un guardiano. Se quest'ultimo scopre che essi si scambiano messaggi segreti metterà uno di loro in isolamento ed il piano fallirà. Quindi essi devono trovare un metodo per nascondere il loro testo in un testo apparentemente innocuo.

Steganografia digitale
L'avvento dell'era digitale e della rete internet ha permesso lo sviluppo di tecniche per la steganografia consentendo l'utilizzo dei seguenti supporti digitali: file di immagini e file audio/video. Ma anche: file system (steganografici) e header pacchetti TCP/IP.

Formalismi
Ci riferiremo all'immagine designata a contenere il messaggio con il nome di immagine **cover** o **contenitore**. Quando il messaggio, detto payload (letteralmente carico), viene inserito nella cover image, chiameremo il risultato **stego-image** o **immagine stego**. Quindi, in termini matematici, si avrà:

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

dove
F è la funzione steganografica, che prende in input un'immagine cover ed un messaggio e restituisce l'immagine stego.
G è una funzione che elabora l'immagine cover
H è la funzione che elabora il messaggio da inserire, ad esempio una funzione crittografica.

Modelli steganografici
Lo schema di base della steganografia presuppone l'esistenza di due messaggi: messaggio **segreto** e messaggio **contenitore**. In base all'origine del contenitore è possibile distinguere: steganografia **iniettiva** e steganografia **generativa**.

Steganografia iniettiva
La steganografia iniettiva è la più utilizzata e consente di inserire il messaggio segreto all'interno di un messaggio contenitore già esistente modificandolo in modo tale sia da contenere il messaggio segreto, sia da risultare, al livello al quale viene percepito dai sensi umani, praticamente indistinguibile dall'originale.

Steganografia generativa
La stenografia generativa consente di generare, a partire dal messaggio segreto, un messaggio contenitore atto a nascondere nel migliore dei modi quel messaggio segreto.

Un'altra classificazione

Oltre alla classificazione precedente, di carattere prettamente concettuale, ne esiste un'altra che caratterizza le tecniche steganografiche a livello pratico:
- Steganografia **sostitutiva**
- Steganografia **selettiva**
- Steganografia **costruttiva**

Steganografia sostitutiva
E' la tecnica steganografica più diffusa, tanto che spesso quando si parla di steganografia ci si riferisce implicitamente a quella di questo tipo.
Tale tecnica si basa sull'osservazione che la maggior parte dei canali di comunicazione (linee telefoniche, trasmissioni radio, ecc) trasmettono segnali che sono sempre accompagnati da qualche tipo di **rumore**.
Questo rumore può essere sostituito da un segnale (il messaggio segreto) che è stato trasformato in modo tale che, a meno di conoscere una chiave segreta, è **indistinguibile** dal rumore vero e proprio, e quindi può essere trasmesso senza destare sospetti.
La tecnica impiegata è concettualmente molto semplice, consiste nel **sostituire i bit meno significativi** (LSB) dei file digitalizzati con i **bit che costituiscono il messaggio segreto**.
Quello che succede quindi è che il file contenitore risultante, dopo un'iniezione steganografica, si presenta in tutto e per tutto simile all'originale, con differenze difficilmente percepibili e quindi, a meno di confronti approfonditi con il file originale (non effettuabili ad occhio nudo) è difficile dire se le eventuali perdite di qualità siano da imputare al rumore od alla presenza di un messaggio segreto.

Steganografia selettiva
Ha un valore puramente teorico e non viene realmente utilizzata nella pratica. Ne fanno parte le tecniche che mirano 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.
Un esempio di tecnica selettiva è quella di impostare una **funzione hash** che controlli la parità dei bit del file uguali ad 1 dispari, e il valore 0 se ne contiene un numero pari.
A questo punto, volendo codificare il bit 0, acquisendo il file binario si controlla se il numero di bit uguali ad 1 sia pari, in caso affermativo si è trovato un file adatto a contenere l'informazione codificata, altrimenti si procede con la acquisire un altro file digitale.

Questa tecnica ha il pregio di risultare praticamente impossibile da identificare, in quanto il supporto, nonostante contenga effettivamente un messaggio segreto, non risulta assolutamente modificato.

Purtroppo ha il difetto di rivelarsi una soluzione alquanto dispendiosa in termini di tempo e insoddisfacente dal punto di vista dell'esiguo quantitativo di dati segreti che permette di celare. Infatti, dovendo aumentare il numero di bit da nascondere, aumenta anche il tempo per il reperimento o la generazione del supporto, il quale è costretto a soddisfare più vincoli contemporaneamente.

Steganografia costruttiva
Opera più o meno come la steganografia sostitutiva, con la differenza che nel modificare il

file contenitore si tiene conto di un **modello di rumore**, nel caso che si tenta di sostituire il rumore presente con il messaggio segreto nel rispetto delle caratteristiche statistiche del rumore originale.

Secondo questa concezione, un buon sistema steganografico dovrebbe basarsi su un modello del rumore e adattare i parametri dei suoi algoritmi di codifica in modo tale che il falso rumore contenente il messaggio segreto sia il più possibile conforme al modello di partenza. Questo approccio sembra la soluzione migliore, ma in realtà anch'esso non è esente da difetti.

Innanzitutti non è facile costruire un modello accurato del rumore. La costruzione di un modello del genere richiede grossi sforzi ed è probabile che qualcuno, in grado di disporre di maggior tempo e di risorse migliori, riesca a costruire un modello più accurato riuscendo ancora a distinguere tra il rumore originale e un sostituto.
Inoltre, se il modello del rumore utilizzato dal metodo steganografico dovesse cadere nelle mani del “nemico” egli lo potrebbe analizzare per cercarne possibili difetti e quindi utilizzare proprio il modello dello stesso per controllare che un messaggio sia conforme ad esso. Così, il modello, oltre ad essere parte integrante del sistema steganografico, fornirebbe involontariamente uno strumento di attacco estremamente efficace proprio contro lo stesso sistema.

Analisi
In una qualsiasi applicazione di **data-hiding** si devono fare i conti con tre requisiti in contrasto tra loro: **invisibilità**, **capacità**, **robustezza**.

Invisibilità percettiva
La tecnica di steganografia iniettiva su immagini sicuramente più diffusa anche grazie alla sua relativa facilità di implementazione è quella che si basa sulla modifica del bit meno significativo (LSB)

RGB
E’ molto comune descrivere i colori allo spazio di colore RGB (red, green, blue). Lo spazio RGB è basato sul fatto che ogni colore possa essere rappresentato da una “miscela” dei tre colori primari red, green e blue. I vari contributi sono assunti indipendenti l’uno dall’altro (e quindi rappresentati da direzioni perpendicolari tra loro). La retta che congiunge nero e bianco è la retta dei grigi.
RGB è molto usato nelle videocamere e nei monitor dato che risulta essere lo spazio colore più semplice per registrare e visualizzare immagini digitali a colori.

Bit-planes
Un’immagine con una profondità di colore di **N bit** può essere rappresentata da **N piani di bit** (bit-planes), ciascuno dei quali può essere vista come una singola immagine binaria. In particolare si può indurre un ordine che varia dal MSB fino al LSB.

Steganografia nelle immagini digitali (.bmp)

Supponiamo di voler utilizzare come contenitore un file di tipo **bitmap** con una profondità di colore a 24 bit, quindi una matrice MxN di pixel codificata in modalità RGB. Quindi per esempio un file bitmap a 24 bit di dimensione 640x480 occuperà uno spazio di 640x480x3=921600 byte.

Una possibile operazione di steganografia sostitutiva su questi file consiste nel sostituire i bit meno significativi dei singoli byte (LSB).
Se ad esempio avessimo un pixel codificato nel seguente modo:

11100001 00000100 00010111

E volessimo modificare: **110**, il pixel diventa:

1110000<u>1</u> 0000010<u>1</u> 0001011<u>0</u>

Queste semplici operazioni fanno si che le variazioni di colore siano praticamente impercettibili ad occhio nudo.

Steganografia nelle immagini digitali (dimensione del messaggio)
Quindi dato che sono un pixel può contenere un'informazione segreta di 3 bit, un'immagine di dimensione MxN può contenere un messaggio segreto lungo fino a **(MxNx3)/8 byte**.

Steganografia nelle immagini digitali (.gif)
Il formato GIF è un formato molto utilizzato per i siti web perché è poco ingombrante. Si basa su una palette di 256 colori. Un file GIF è una **sequenza di puntatori alla palette** (uno per ogni pixel).
Per iniettare un messaggio segreto in un file GIF, acquisita l'immagine, bisogna:
1) Decrementare il numero di colori ad un numero inferiore a 256 con un opportuno algoritmo che limita la perdita di qualità
2) Convertire in GIF riempiendo la palette con colori molto simili a quelli rimasti

Dopo un'operazione di questo tipo ogni pixel potrà essere rappresentato alternativamente con il colore originale o con il relativo colore simile aggiunto.

Quindi in presenza di alternative possiamo nascondere un'informazione. Ad esempio, se per rappresentare il pixel **p(i,j)** si hanno due alternative **C1** e **c2**, si potrà nascondere un bit, associando il valore 0 a C1 ed il valore 1 a C2. Il numero di bit rappresentabili aumenta di uno al raddoppio dei colori sostituiti.

La soluzione esposta è senz'altro molto ingegnosa, ma presenta il problema che è molto semplice scrivere un programma che analizzi la palette ed individui sottoinsiemi di colori simili e quindi la probabile presenza di un messaggio steganografato.
In effetti, questo tipo di attacco è stato portato a termine con pieno successo da diversi staganalisti, tanto che alcuni di loro hanno sostenuto che il formato GIF non fosse adatto alla steganografia. In realtà esiste un altro modo per steganografare con GIF che si basa sulla seguente osservazione: un'immagine GIF può essere rappresentata in 256! modi diversi. La palette di una GIF si compone di 256 colori. Tuttavia non è importante l'ordine in cui i colori compaiono nella palette e quindi i 256 colori di una palette possono essere permutati in 256| modi, ciò vuol dire che una stessa immagine GIF può essere rappresentata in 256! modi diversi, a patto di cambiare opportunamente la sequenza dei puntatori.

La teoria dell'informazione afferma e dimostra che l'informazione è una quantità misurabile, ed è direttamente proporzionale al numero di simboli dell'alfabeto del linguaggio che viene usato per comunicare. Nel nostro caso, pertanto opportunamente la palette, si potranno avere **256! rappresentazioni** – cioè simboli – alternative della stessa immagine, per un totale di **log(256!) = 1683 bit** (circa 200 byte) disponibili per la codifica di un messaggio nascosto, indipendentemente dalla dimensione dell'immagine.

Steganografia nelle immagini digitali (Lossless vs Lossy)
I formati considerati fino ad adesso sono tutti formati Lossless (senza perdita), nel caso si dovessero considerare i formati Lossy (con perdita) non è possibile operare con sinora descritto. In particolare, se accettassimo delle informazioni in un file e dopo lo convertiremo ad esempio, in JPEG, le informazioni andrebbero inevitabilmente perse.
La compressione JPEG, infatti, ha la tendenza a preservare le caratteristiche visive dell'immagine piuttosto che l'esatta informazioni contenuta nella sequenza di pixel, di conseguenza sarebbe impossibile risalire al file bitmap originario.

Steganografia nelle immagini digitali (.jpg)
In questi casi si opera ad un **livello di rappresentazione intermedio**. Per poter utilizzare anche le immagini JPEG come contenitori, è possibile intiettare le informazioni nei coefficienti di Fourier ottenuti dalla prima fase di compressione. Le tecniche steganografiche solitamente vengono applicate dopo la fase di quantizzazione e sono caratterizzate dall'eseguire un'alterazione dei coefficienti DCT al fine di occultare informazioni segrete. Bisogna innanzitutto tenere presente che la modifica di un singolo coefficiente DCT in un blocco ha effetto su tutti e 64 pixel dell'immagine appartenenti ad esso. Inoltre, la scelta di quali coefficienti modificare deve essere ponderata in funzione del tipo di protezione necessaria:
- Coeff. Alte frequenze: **+ invisibilità – robustezza**
- Coeff. Basse frequenze: **+ robustezza – invisibilità**
- Coeff. Medie frequenze: **invisibilità = robustezza (solitamente)**

La principale modalità di occultamento prevede la modifica del bit meno significativo (LSB) dei coefficienti DCT per inserirvi i bit del messaggio segreto.

Un'altra procedura alquanto efficace sfrutta e pilota l'operazione di arrotondamento all'intero dei coefficienti DCT, nella **fase di quantizzazione**, per occultare informazione. L'inserimento dei dati segreti viene attuato scegliendo opportunamente di arrotondare i coefficienti all'intero superiore o inferiore.
In un sistema più complesso, invece, l'occultamento dei biti del file segreto viene codificato nella differenza relativa tra i coefficienti che corrispondono a locazioni di uguale valore nella tabella di quantizzazione. Se tale differenza non eguaglia il bit da nascondere allora i coefficienti vengono scambiati tra loro.

Steganografia nelle immagini digitali (BPCS)
Invece di considerare sempre e solo i bit meno significativi come i bit da sostituire, è possibile analizzare l'immagine e scegliere delle regioni nelle quali effettuare una modifica non significa alterare in modo significativo l'immagine nel complesso. Una tecnica che

effettua questo lavoro è al BPCS Steganography sviluppara da Eiji Kawaguchi nel 1997.
Per determinare tali regioni sostituibili, l'immagine viene divisa in blocchi, per ogni blocco di 8x8 pixel viene effettuato un test che determina la complessità dell'immagine contenuta in questo blocco. Se tale complessità è minore di una determinata soglia (parametro variabile dipendente dall'immagine) allora un messaggio segreto (eventualmente cifrato) può essere nascosto in questo blocco senza alterare significativamente l'immagine.
Un'immagine **P** costruita da pixel ad **n-bit** può essere decomposta in un insieme di n immagini binarie. Per esempio, se l'immagine è un'immagine n**-bit gray**, la possiamo descrivere come: **P = (P1, P2,…, Pn)**. Un'immagine **RGB P**, invece, può essere vista come: **P = (PR1, PR2,…, PRN ; PG1, PG2,…,PG3 ; PB1, PB2,…, PBN)**, dove **PR1**, **PG1**, **PB1** è la **bit-plane più significativa** (immagine formata dai bit più o meno significativi di tutti i pixel dell'immagine) e **PRN**, **PGN**, **PBN** è la **bit-plane meno significativa**. Analizzando ogni singola bit-plane, quello che accade molto di frequente è che più ci si allontana dalla bit-plane più significativa, è più aumenta la complessità (intesa come confusione dell'immagine) della bit-plane stessa.
Ogni bit-plane può essere segmentata in regioni **shape-informative** (forma informativa, cioè parti dell'immagine che sono significative sotto il punto di vista visivo) e **noise-looking** (disturbo visivo, cioè poco rilevanti dal punto di vista visivo). Le regioni semplici (cioè ben distinguibili visivamente) sono delle shape-informative e pertanto non possono essere modificate, quelle complesse, invece, rappresentano della noise-looging che possono essere rimpiazzate senza deteriorare la qualità dell'immagine nel complesso.

Cenni sulla steganografia su file video
Un file video è un file multimediale in senso stretto. Infatti esso contiene il video (cioè una sequenza di immagini), audio (sia dialoghi che musica) e testo (sottotitoli, titoli di testa e di coda, scritte in sovraimpressione). Inoltre i file video vengono compressi a causa delle grandi dimensioni, utilizzando numerosi sistemi di codifica/decodifica (CODEC).

Sfruttando la poliedricità dei file video, è possibile inserire messaggi nascosti all'interno di una qualunque delle sue parti (flusso di immagini statiche, audio, testi), utilizzando gli efficienti algoritmi già noti per ciascuna parte. L'uso dei file video come cover consente di avere più bit a disposizione per il messaggio nascosto, e rende più complicato l'attacco; infatti il messaggio potrebbe essere nascosto in uno qualunque tra gli elementi del video, o addirittura suddiviso tra di essi.

Steganalisi
Le tecniche che si prefiggono di individuare la presenza di un messaggio occultato attraverso l'uso di tecniche steganografiche rientrano sotto il nome di steganalisi. L'obiettivo almeno in prima istanza non è quello di individuare e decodificare il contenuto del messaggio segreto, ma semplicemente determinare se un mezzo contiene un messaggio oppure no.

Pertanto la steganalisi può essere formulata come un test sull'ipotesi che il mezzo contenga un messaggio segreto.

Formalmente, dato un insieme di osservazioni $\mathbf{Y = \{y_1, y_2, \ldots, Y_n\}}$ o di loro funzione dette

feature o **statistiche** si formulano due ipotesi alternative: il fine non contiene un messaggio segreto oppure il file contiene un messaggio segreto. La decisione tra le due ipotesi viene presa in base ad un **criterio di ottimalità**.

Attacchi
Il tentativo di determinare la presenza di un messaggio segreto è detto attacco. Ripetendo l'equazione 1, è possibile distinguere gli attacchi a seconda delle parti dell'equazione note all'analista.
Si avrà quindi:
- **stego-only-attack**: l'attaccante ha intercettato il frammento stego ed è in grado di analizzare. E' il più importante tipo di attacco contro il sistema steganografico perché è quello che occorre più di frequente nella pratica.
- **stego-attack**: il mittente ha usato lo stesso cover ripetutamente per nascondere i dati. L'attaccante possiede un frammento stego diverso ma originato dallo stesso cover. In ognuno di questi frammenti stego è nascosto un diverso messaggio segreto.
- **cover-stego-attack**: l'attaccante ha intercettato il frammento stego e sa quale cover è stato usato per crearlo. Ciò fornisce abbastanza informazioni all'attaccante per poter risalire al messaggio segreto.
- **cover-emb-stego-attack**: l'attaccante ha "tutto": ha intercettato il frammento stego, conosce il cover usato e il messaggio segreto nel frammento stego.
- **manipulating the stego data**: l'attaccante è in grado di manipolare i frammenti stego. Il che significa che l'attaccante può togliere il messaggio segreto dal frammento stego (inibendo la comunicazione segreta).
- **manipulating the cover data**: l'attaccante può manipolare il cover e intercettare il frammento stego. Questo può significare che con un processo più o meno complesso l'attaccante può risalire al messaggio nascosto.

Attacchi visuali e statistici
E' possibile effettuare degli attacchi alle immagini digitali con lo scopo di rilevare la presenza di attacchi segreti:
Attacchi visuali: che sono in correlazione con le capacità visive umane. Si sfruttano cioè le capacità visive umane. Si sfruttano cioè le capacità dell'occhio umano per individuare artefatti introdotti da tecniche steganografiche.
Attacchi statistici: che effettuano test statistici sui file steganografati.

Attacchi visuali
Il file steganografato viene filtrato con un algoritmo di filtering dipendente dalla funzione utilizzata per nascondere il messaggio. L'immagine filtrata viene osservata per determinare se è stato nascosto un messaggio o meno.

L'operazione risulta lenta se la mole di immagini da analizzare è considerevole. Gli algoritmi di filtering effettuano un'operazione sull'immagine steganografata, facendo risaltare

visivamente i biti che contengono il messaggio nascosto.

Attacchi statistici
L'informazione statistica estratta da un'immagine più nota ed utilizzata, è sicuramente l'istogramma che rappresenta la distribuzione del colore nell'immagine stessa. Si tratta di un semplice grafico a barre, in cui sull'asse delle ascisse ci sono valori di intensità del colore e sull'asse delle ordinate il numero di pixel che hanno quel valore di intensità. Si può quindi immaginare di utilizzare queste informazioni per definire un modello statistico della distribuzione dei valori attesi di intensità in una immagine stego. Confrontando i valori dell'immagine candidata con il modello statistico teorico, si riesce ad ottenere la probabilità che nell'immagine sia presente un messaggio nascosto.

L'idea dell'attacco statistico è controllare la distribuzione di frequenza dei colori di un potenziale file steganografato con la distribuzione di frequenza teoricamente attesa per un file steganografato. Se la funzione utilizzata è la sovrascrittura del bit meno significativo, il valore del pixel diventa uguale a tutti gli altri pixel il cui valore differisce solo per il bit meno significativo. Se il bit da sovrascrivere (cioè il messaggio nascosto) sono equamente distribuiti, le frequenze nell'istogramma relative al valore originale e al valore con il LSB sovrascritto diventeranno uguali.

Steganografia nell'audio digitale (.wav)
Un file **WAV** mono, campionato a **44100 Hz** a **16 bit**, per esempio, indica che un file è stato costruito ottenendo 44100 stringhe di 16 bit al secondo nella fase di digitalizzazione del suono, ossia è stata generata una stringa di 16 but ogni 1/44100 di secondo. Nel caso di un wav stereo, le stringhe di 16 bit ottenute sono due, una per il canale destro e una per il sinistro. Anche in questo caso si possono sostituire i bit meno significativi allo scopo di steganografare un messaggio.

Un punto debole della tecnica LSB sui file audio è rappresentato dal fatto di introdurre solitamente un fastidioso rumore di fondo, avvertibile all'orecchio umano. Inoltre le considerazioni fatte per la tecnica LSB applicate alle immagini valgono anche per i file audio, con la sola differenza che invece di operare in piani di pixel si agisce sui campioni dell'onda.

Echo Data Hiding
L'approccio visto in precedenza modifica il file aggiungendo un forte rumore di fondo (noise) facilmente avvertibile. L'echo data hiding è una tecnica che evita questo inconveniente. Se il suono originale e la sua eco sono divisi da una spazio di tempo piccolo abbastanza, l'orecchio umano non riesce a distinguere i due suoni. I dati vengono codificati in questi eco rappresentando gli 0 e gli 1 come due offsets differenti di eco.

Steganografia nell'audio digitale (.mp3)
Anche nel caso dei file audio compressi lossy, come il formato MP3, non è possibile iniettare il messaggio segreto operando come nel caso del file WAV. In questo caso si inserisce il messaggio segreto nella fase di inner loop.

Steganografia e Indagini

La potenza della steganografia sta nel fatto che **non c'è nessuna cifratura visibile ad un primo controllo**, contrariamente a quanto avviene per le tecniche crittografiche; quindi la presenza di eventuali messaggi segreti che potrebbero essere utilizzati come evidenze va scovata caso per caso. La molteplicità di tecniche esistenti, e le grandi differenze che sussistono tra loro, rendono praticamente impossibile determinare la presenza di un messaggio nascosto, a meno di non avere indizi supplementari che l'analista può interpretare, supponendo la presenza o da ulteriori informazioni a corredo ottenute mediante metodi di investigazione tradizionale.

Digital Forgery

La Multimedia Forensics è basata sull'idea che le tracce intrinseche (come le impronte digitali) sono lasciate da un media digitale sia durante la fase di creazione che nei processi successivi.

Ad esempio, nell'immagine di Bin Laden, la barba e la bocca sono molto sfocati e con una risoluzione molto bassa, mentre i capelli sono più definiti, con risoluzione e contrasto maggiori. Poi al centro della fronte c'è una macchia chiara, che più che un riflesso sembra una pennellata. Identico riflesso del flash sull'orecchio sinistro.

Cos'è una Forgery?
1) Uso di software grafici
2) Modifica del contesto

Metodi di forgery detection:
1) Lo standard JPEG
2) Informazioni presenti in EXIF (analisi dei thumbnails)

JPEG DCT Techiniques
1) Misurare le inconsistenze dei blocchi artefatti
2) Digital Forgeries dai JPEG Ghosts

Il termine contraffatto è soggettivo. Un'immagine può diventare contraffatta in base al contesto in cui è usata. Un immagine alterata per divertimento o qualcuno che ha scattato una brutta foto, ma l'ha alterata per migliorare il suo aspetto non può essere considerato un contraffatta nonostante è stato alterata la sua forma originale.
L'altra parte della contraffazione è quella usata per trarne guadagno e prestigio. Questi creano un'immagine con lo scopo di ingannare l'osservatore nel credere che l'immagine sia vera al fine di trarne guadagno e fama.
Possiamo distinguere due tipi di contraffazione:
1) Un'immagine che è creata usando un software grafico
2) Un'immagine dove il contesto è stato alterato

Creare un immagine alterandone il contesto è un altro metodo. Ingannare l'osservatore nel fargli credere che l'oggetto nell'immagine è qualcos'altro da ciò che veramente è.
Gli oggetti possono essere rimossi o aggiunti, per esempio una persona può essere aggiunta o rimossa. Il modo più semplice è tagliare un oggetto da un'immagine e inserirla in un'altra immagine – i software di editing di immagini rendono l'operazione semplice.
Manipolando il contenuto di un'immagine il messaggio può cambiare drasticamente significato. Un esempio è che questa immagine alterata potrebbe essere usata per influenzare gli eventi.

Alterare le immagini non è una cosa nuova, bensì dai primi giorni della fotografia. I concetti si sono spostati al mondo digitale grazie alle fotocamere digitali e la disponibilità dei software di editing di immagine.

Il semplice uso dei software di manipolazione delle immagini, che non richiede nessuna abilità speciale, rende la manipolazione delle immagini facile da eseguire.

WPP Report: The integrity of the Image (nov 2014)
Le pratiche correnti e gli standard accettati, in relazione alla manipolazione delle immagini nel fotogiornalismo e nei documentari fotografici.

Le organizzazione proibiscono l'alterazione delle immagini dietro la tradizionale tecnica di camera oscura.

Ciò implica – in primis – le alterazioni delle immagini – dove alterazione significa l'aggiunta o la sottrazione digitale di elementi è proibita.

- Il divieto sull'alterazione è spesso tradotto in termini di non inganno per il lettore.
- L'unica alterazione genericamente permessa è il ritocco o l'uso di tool di clonazione che eliminano la polvere nei sensori delle camere o graffi sui negativi o stampe.
- Alcune organizzazioni di media permettono la sfocature delle faccie o altre forme di identificazione (es targhe), dove questa è ritenuta necessaria dalla legge o dal giudice dell'organizzazione
- Qualsiasi immagini sono alterato per scopi illustrativi devono essere citate e/o sottotitolate come "photo-illustrations" o in termini simili.
- Gli aggiustamenti fatti dai software di elaborazione di immagini (cropping, toning, color adjustment, ecc) sono accettate finché sono ritenuti "minor/normal/subtle/moderate", mentre "excessive use" non è accettato.
- Questi "minor/normal/..." aggiustamenti sono regolarmente giustificati dal termine "pratiche tradizionali di camera oscura", o non per violare il "veracità emozionale" di un'immagine, e sono considerati necessari per rendere pulito e accurato la riproduzione.

Esperti a confronto.
Sono stati contattati degli "esperti" forensi che hanno stabilito che: sì la foto è ritoccata, in quanto a luce e colori, così da renderla più forte, ma sostanzialmente **non si tratta di un'immagine composta** (confronto con raw). Il **ritocco di colori e intensità luminosa** è un

discorso a parte, ricade nelle scelte della giuria del WPP sull'accettare o meno una foto in stile Instagram.

Estratto del rapporto:
1) **XMP Analysis**. L'analisi XMP riflette una comprensione incompleta dei metadati di Photoshop e parafrasa anche i contenuti in un modo ingannevole. I blocchi di riferimento dei metadati indicano semplicemente che il file è stato aggiustato nel modulo Adobe Photoshop Camera Raw in più occasioni prima di essere aperto con Photoshop e salvato come JPEG. Infatti, questi metadati non tengono traccia se sono composti da più file.
2) **Error Level Analysis**. L'analisi forense della compressione del JPEG effettuata tramite ELA (error level analysis) non fornisce un quantitativo di affidabilità dell'analisi della foto manipolata. Questa analisi spesso identifica erroneamente foto autentiche come alterate e fallisce l'identificazione di immagini alterate, e quindi non è un tool affidabile per la forensics.
3) **Shadow Analysis**. L'analisi delle ombre è imperfetta nella sua logica e conclusione. E' vero che il vincolo lineare che connette due punti su un oggetto con il suo corrispondente punto nell'ombra dovrebbe essere l'intersezione di un singolo punto (supponendo la presenza di un singolo punto di luce). Il punto di intersezione di questi punti, tuttavia, non può essere usato per la molteplicità (dei punti di luce) nella scena. Il punto di intersezione è semplicemente l'intersezione è semplicemente la proiezione della sorgente di luce nel piano dell'immagine. Questa punto proiettato può essere ovunque nell'immagine (incluso dietro il piano del terreno) in base a dove il fotografo è orientato rispetto al sole.

Negativo vs Sensore: due epoche a confronto.
Nel vecchio mondo della fotografia analogica, un'immagine, era in genere, considerata una prova d'evidenza attendibile. Allo stato attuale non esiste tecniche automatiche "perfette" che permettono l'esatta individuazione di manomissioni delle immagini digitali. Per questo motivo le fotografie digitali non sono, in genere, attendibili ai fini di provare l'evidenza, se non con dovuto accorgimenti formali e procedurali.

In epoca pre-digitale, possiamo afermare che molto raramente veniva messa in dubbio la veridicità di una immagine. Era comunque abituide, allorquando era necessario coredare una fascicolo di indagine di alcune fotografie, dopositare anche i negativi delle stesse. Prassi voleva che questa accortezza fosse sufficiente per mettersi al ripao da contestazioni in merito all'originalità della fonte di prova. Inoltre, poter fornire l'intero rullino da cui erano state estratte le immagini, impedica di omettere qualche scatto "scomodo", dato che la pellicola li contrassegnava in ordine cronologico.

L'odierna diffidenza discende dalle diverse tecniche di formazione dell'immagine tra i due tipi di apparati.
Nelle fotocamere analogiche la pellicola veniva impressionata dalla luce proveniente dal sistema di lenti, dopodiché essa costituiva una sorta di "matrice" dell'immagine, da cui si potevano estrarre quante copie si desiderava, tutte (a parte lievi variazioni cromatiche determinate dai dosaggio dei reagenti per lo sviluppo, ma uguali in due operazioni distinte) identiche all'originale.
Nel sensore delle fotocamere digitali (che in senso lato sostituisce la pellicola) l'immagine semplicemente transita prima di essere salvata nella memoria (dopo essere stata fra l'altro

elaborata). Al termine del processo di acquisizione questa viene salvata ma può essere anche subito cancellata e non soddisfa il gusto dell'operatore. La "matrice originale" di un'immagine in un certo senso non esiste più.

In realtà, anche i negativi potevano essere alterati, sia gendo fisicamente sulla pellicola, asportando delle parti o aggiungendone altre e poi sviluppando il negativo modificato, oppure duplicando il negativo con apposita strumentazione, applicando delle opportune maschere per nascondere od inserire i particolari voluti.
Alcune tecniche per la rilevazione prevedevano l'esaminazione del negativo modificato per notare i ritocchi, ed esamina delle diverse caratteristiche (grana, spessore) del negativo-copia, di solito mai del tutto identici a quelli dei rullini delle fotocamere.

Queste presunte modifiche sulle fotografie analogiche non erano alla portate dell'utente generico, ma richiedevano conoscenze specifiche, abilità e strumentazione adatta.

Nel mondo digitale invece l'autenticità e quindi la validità di un'immagine o di un video presenta una "sfida" più comune. Non vi sono segni su un negativo, o spessore di pellicole da controllare, ma dati e tracce digitali, statistiche da interpretare in modo non sempre univoco e con una certa dose di incertezza.

Forensics Image Authentication
L'applicazione della scienza dell'immagine e gli esperti di dominio per discernere se l'immagine o il video in questione è una rappresentazione accurata del dato originale tramite alcuni criteri ben definiti. Questi criteri spesso coinvolgono le interpretabilità del dato, e non un semplice cambio di formato che non alterano il significato o il contesto del dato.

File originale.
L'immagine è coerente con quella creata dalla specifica fotocamera?

Principio usato per determinare se e un file di un'immagine digitale è stato creato dallo stesso processo e un'altra immagine, per esempio la stessa camera digitale.

Perché vogliamo il file originale?
File originale implica immagine originale. I software di immagini spesso alterano la struttura del file. Un file che non è originale può suscitare dubbi riguardo l'autenticità del contenuto dell'immagine.

Image Forensics
Approccio attivo: watermarking facile, firma digitale crittografata.
Approccio passivo: image forensics, steganalisi, Tampering/Forgery detection, identificazione della sorgente

Metodi di image forensics: watermarking.
Nascondere un marchio o un messaggio in un'immagine quando essa è creata.
Svantaggi: limitata alla specifica camera digitale fornita, non così robusto.

Watermarks fragili.
I watermarks fragili sono progettati per individuare ogni possibile cambiamento dei valori dei pixel. Ci sono molte tecniche, ma in molti casi, il watermark è inserito nel last significant bit dell'immagine.

Pro: raccoglie tutte le manipolazioni dell'immagine (maligne e non)
Contro: troppo sensibile.

Watermarks semi-fragili.
Sono robusti, in una certa misura, e sono poco sensibili alla modifica dei pixel.
1) Viene suddivisa l'immagine in blocchi e vengono utilizzati i bit da ogni blocco per calcolare uno spettro di propagazione del rumore come segnale che p combinato con i coefficienti DCT e inserita come watermark.
2) L'immagine viene suddivisa in blocchi, viene costruito il watermark nel dominio della DCT da una distribuzione gaussiana a media nulla di numeri pseudo-random, si prende l'inverso della DCT e la si inserisce nell'immagine.
Vantaggi: meno sensibile del watermark fragile

Self-Embedding
Le immagini manomesse perdono informazione. Le tecniche precedenti individuano e localizzano aree di interesse soltanto quando l'autenticazione viene rimossa. Il self-embedding consente la manomissione e il recupero delle informazioni perse. Il concetto generale è che l'immagine è inserita in se stessa in forma criptata.
Vantaggi: buona per ripristinare i dati originali
Svantaggi: la manomissione dell'immagine può rimuovere blocchi dell'immagine originale rendendo il ripristino impossibile.

Digital Cameras with Watermarking Capabilities.
Il watermark si basa su una chiave segreta, block ID e contenuto. L'immagine è divisa in blocchi e ogni blocco con watermark usa una frequenza basato su uno spettro di propagazione che incorpora la chiave segreta, il block ID e il contenuto del blocco.

Come autenticare un'immagine?
- Ispezione visuale
- Analisi del file: formato del file, metadati (EXIF), parametri di compressione (tabelle di quantizzazione)
- Analisi globale: statistiche sui pixel e dai compressi
- Analisi locale: Trovare inconsistenze sulle statistiche dei pixel nell'immagine

Ispezione Visuale
Caso di studio: il file è originale, ma la rappresentazione del contenuto no (caso estremo). Inconsistenza temporale, anacronismo, inconsistenza della scena.

Tipi di analisi: livello delle scena
Usa le caratteristiche della scena, non dei pixel dell'immagine e potrebbe funzionare bene

anche sulle foto digitali.
Difficile da dimostrare: molte falsificazioni contengono leggeri errori non visibili dall'occhio umano ma rilevabili da una corretta analisi.
Difficile da automatizzare: richiede molta esperienza.

Risultati migliori sullo splicing, meno successo sulle alterazioni nascoste.
Basata sulla fisica della luce.
Inconsistenza geometrica a prospettica: punto principale dell'analisi, ombre e fotogrammetria.

Tipi di analisi: livello del segnale
Basato caratteristiche statistiche dei valori di pixel, richiede un'immagine di buona qualità.
Clone detection: blocchi di immagini clonati, coppie simili di punti chiave.
Individuazione del ricampionamento: ritaglio, rotazione, ma anche tagli o cloni.
Individuazione del contrasto: algoritmi specifici (mediana, equalizzazione dell'istogramma, aggiustamento del colore).

È possibile utilizzare tecniche per la detection automatica di eventuali manipolazioni "maliziose" delle immagini digitali? E' stato coniato il termine **photoshopping** per denominare l'azione volta a falsificare digitalmente medicine, scene di guerra, ed in generale immagini digitali di qualsiasi natura ("Photoshop Forensics", Cynthia Baron 2008)

Copy-Paste Forgery
La contraffazione Copy-Paste si basa principalmente sulla ricerca di blocchi che sembrano ripetersi nell'immagine. Se l'ammontare di blocchi adiacenti ripetuti è maggiore di una certa soglia euristica la regione è probabilmente alterata.

Come procedere in reali casi…
Se si hanno dei sospetti sulle aree clonate è sufficiente prendere in input l'immagine, le coordinate utili ad individuare una data area di ricerca e la regione (o patch) di cui si vogliono individuare i possibili cloni oltre che i range relativi alle possibili trasformazioni geometriche considerate. L'area di ricerca individua l'area entro cui ricercare gli eventuali cloni della patch ad esclusione della stessa patch (qualora fosse essa stessa inclusa nella zona di ricerca). I parametri relativi alle trasformazioni specificano invece i valori da utilizzare per ciascuna trasformazione geometrica considerata.
Mediante analisi visiva ed utilizzando apposite procedure di ispezione virtuali ci si può concentrare, caso per caso, sulle trasformazioni più pertinenti, limitando anche il relativo range di ricerca. Il crop sui 4 lati viene utilizzato in tutti i casi e ha lo scopo di compensare possibili errori commessi dall'utente durante la defnizione della patch da ricercare. Il crop permette dunque di aumentare o ridurre le dimensioni della patch quando i bordi di quest'ultima non si riescono a fornire in maniera precisa.

Metrica di similarità
Come metrica di similarità si può in genre ritenere sufficiente ai nostri scopi la media delle differenze in valore assoluto, in gergo MAE (Mean Absolute Error), tra la regione di input e il

suo possibile “clone”. Questo valore numerico (che varia tra 0 e 255) misura quanto due regioni siano tra loro simili, tenendo conto della differenza pixel per pixel delle regioni corrispondenti. Un valore di MAE pari a zero indica la perfetta corrispondenza: le due regioni sono uguali.

Valori prossimi allo zero o comunque molto piccoli indicano un'alta probabilità che le due regioni siano copia l’una dell’altra.

Camera based
Le scanalature impresse dalle canne delle pistole sui proiettili collegano, con un certo gradi di confidenza, una pallottola ad una ben determinata arma da fuoco. Sfruttando la stessa filosofia, sono state sviluppate delle 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.

Abberrazioni cromatiche
La rifrazione della luce in due dimensioni. La luce policromatica entra nelle lenti e fuoriesce con un angolo che dipende dalla lunghezza d’onda. Di conseguenza, differenti lunghezze d’onda della luce, saranno immaginate a punti differenti.

Sul formato: JPEG
La prima regola fondamentale dell’indagine forense è ovviamente quella della conservazione dei dati originali. Per questo motivo la compressione lossy delle immagini JPEG può essere considerata il peggior nemico dell’analista forense.
Il caso vuole che proprio questa caratteristica di “perdita di dati” sia utilizzata come ottimo strumento per l’individuazione delle manomissioni.

La quantizzazione
La maggior parte della macchine fotografiche digitali memorizzano gli scatti in formato JPEG. Questo schema di compressione lossy permette di stabilire, in qualche modo, un “grado” di compressione dei dati. Di solito, sono i produttori di fotocamere a stabilire i differenti gradi di compressione selezionabili, in funzione a statistiche che bilancino qualità e dimensioni finali dei files. Queste differenze possono essere utilizzate per identificare la sorgente (modello di fotocamera, produttore) di un'immagine.

Lo standard JPEG
JPEG sta per un compressione di immagini.
JFIF (JPEG File Interchange Format) sta per uno standard che definisce: risoluzione e proporzioni, spazio di colore, ecc
ExIF permette di integrare ulteriori informazioni nel file.

Exif: alcuni dettagli
Exchangeable Image file format (Exif) è uno standard che specifica il formato per immagini, suoni e tag ausiliari usati da camere digitali (inclusi gli smartphone), scanner e altri sistemi di cattura di immagini e suoni da camere digitali.
L’uso specifico che segue i formati di file esistenti con l’aggiunta di specifici tag di metadati.

JPEG DCT per i file di immagini compresse, **TIFF** per i file di immagini non compressi e **RIFF WAV** per i file audio. Non è supportato in JPEG 2000, PNG e GIF.

Exif: informazioni

ExIF permette di integrare ulteriori informazioni in un file. Le informazioni tipicamente contenute in uno standard Exif sono: dimensione dell'immagine, data e ora di acquisizione, caratteristiche dell'acquisizione (tempo di esposizione, ISO, apertura focale, GPS, ecc), thumbnail preview (piccola immagine che dovrebbe essere uguale all'immagine originale). Controllare le informazioni contenute nell'Exif dimostra la possibilità di individuare subito possibili contraffazioni. In effetti, se il costruttore è conosciuto, i dati contenuti nell'Exif devono combaciare.

I metadati XMP

L'Extendible Metadata Platform (XMP) è lo standard di metadati utilizzato dalle applicazioni Adobe. I metadati memorizzati in altri formati, ad esempio Exif, IPTC, GPS, TIFF, vengono sincronizzati e descritti con lo standard XMP in modo da poter essere visualizzati e gestiti più facilmente. Ad esempio, le regolazioni apportate alle immagini con Adobe Camera Raw vengono memorizzate come metadati XMP. Lo standard XMP è basato su XML.

Thumbnail

La maggior parte delle fotocamere memorizza negli Exif data un thumbnail (in JPEG) dell'intera immagine ad utilizzare per preview veloci. Che succede in caso di forgery (malizioso o meno)?

E' possibile estrarre i thumbnail attraverso semplici Exif tools. Questi tool permettono di identificare dati che non sono stati rimossi da utenti inesperti.

Inoltre, l'analisi dell'Exif permette di estrarre (se presente) una ulteriore dettagliata preview dell'immagine che è posta alla fine del file JPEG ed è presente solo nelle fotocamere di fascia alta. Questa preview è molto più dettagliata e permette anche di identificare le persone.

Identificazione della camera sorgente

Al massimo ovvio e semplice livello, uno dovrebbe ispezionare il **File Elettronico** stesso e guardare per indizi negli headers o in altre informazioni aggiuntive o associate. Per esempio, l'header EXIF contiene informazioni sul tipo di camera digitale e le condizioni sotto il quale l'immagine è stata catturata (esposizione, data e ora, ecc). È **fondamentale** evidenziare che i metadati possono essere manipolati.

Exif per camere rubate

Molte camere salvano l'informazione del numero seriale nei dati dell'EXIF di tutte le foto che scattano.

JPEG: la quantizzazione

La maggior parte delle macchine fotografiche digitali memorizzano gli scatti in formato JPEG. Questo schema di compressione lossy permette di stabilire, in qualche modo, un "grado" di compressione dei dati. Di solito, sono i produttori di fotocamere a stabilire i differenti "gradi" di compressione selezionabili, in funzione a statistiche che bilanciano

qualità e dimensioni finali dei files. Queste differenze possono essere utilizzate per identificare la sorgente (modello di fotocamera, produttore) di un'immagine.
Informazioni aggiuntive possono essere ottenute dalla tabella di quantizzazione nell'header del JPEG. Questi dati, tuttavia, possono non essere disponibili se le immagini è riservata in un differente formato o ricompressa. Un altro problema è la credibilità delle informazioni che possono essere facilmente sostituite.

JPEG Compression
Convertire un'immagine in JPEG è un processo a 6 passi:
1) L'immagine è convertita da raw RGB a YcbCr
2) Un sottocampionamento è eseguito sul canale della crominanza
3) I canali sono splittati in blocchi 8x8
4) Viene applicata la DCT
5) I coefficienti DCF sono quantizzati (lossy) usando le tabelle fisse
6) Infine una codifica entropica (lossless) è applicata e l'immagine è detta compressa in JPEG

Quantizzazione
La quantizzazione è spesso usata per convertire un segnale continuo in uno spazio discreto.

Tabelli di quantizzazione
Lo standard fissa che ogni immagine deve avere da una a quattro tabelle di quantizzazione. Le tabelle di quantizzazione più comunemente usate sono state pubblicata da IJG (independent JPEG Group) nel 1998. Queste tabelle possono essere scalate per un fattore di qualità Q. Il fattore di qualità permette al dispositivo che crea l'immagine di scegliere tra valore: **più grandi** (alta qualità dell'immagine) o **più piccoli** (bassa qualità dell'immagine).
Una tabella di quantizzazione differente può essere classificata in due categorie:
- **Standard Tables**: Immagini che usano versioni scalate delle tabelle pubblicate dallo standard IJG.
- **Extended Tables**: alcune delle tabelle standard ma hanno tre tabelle invece di due. La terza tabella è un duplicato della seconda.
- **Custom Fixed Tables**: immagini che contengono una tabella non IJG che non dipende dall'immagine da processare (Adobe Photoshop)
- **Custom Adaptive Tables**: Queste immagini non sono conformi allo standard IJG. In aggiunta, possono cambiare, o in parte o per intero, tra immagini create dallo stesso dispositivo che usa le stesse impostazioni. Queste possono anche avere costanti nelle tabelle; valori che non cambiano indipendentemente dal settaggio di qualità dell'immagine da processare.

Tabelle di quantizzazione per la balistica
Considerare solo le tabelle di quantizzazione non è sufficiente per determinare le differenze tra camere sorgenti, ma è utile per identificare chiaramente le immagini alterate.

Identificazione di alterazione attraverso DCT
L'attività di ricerca in questa area è iniziata attraverso l'analisi delle correlazioni tra tabelle di quantizzazione e coefficienti DCT. Due tecniche di investigazione riguardano due aspetti:

individuazione delle alterazioni misurando le inconsistenze tra blocchi artefatti e scoprire alterazioni digitali a partire dai JPEG Ghost.

Misurare le inconsistenze di blocchi artefatti
Come i produttori tipicamente usano differenti tabelle di quantizzazione per bilanciare il rapporto di compressione e qualità dell'immagine, gli artefatti dei blocchi introdotti nelle immagini possono essere differenti. Quando creiamo un'alterazione, il risultato dell'immagine manomessa può ereditare differenti tipi di artefatti di compressione da differenti sorgenti. Queste inconsistenze, se individuate, possono essere usate per verificare l'integrità di un'immagine.

Identificazione della camera digitale

Fingerprint basato su pattern legato al rumore del sensore, dati derivati dal particolare formato (raw, EXIF, codifica JPEG, ecc), alibi?

L'identificazione affidabile di un dispositivo usato per acquisire una particolare immagine digitale è utile in particolare in tribunale per stabilire l'origine di un immagine presentata come prova. Il metodo di forensics capace di determinare che due clip vengono dalla stessa videocamera o che due versioni di transcoder su un filmato hanno la stessa sorgente comune sarà ovviamente d'aiuto per gli investigatori per tracciare connessioni tra differenti entità o soggetti e possono diventare un componente di prova nel perseguire gli imputati.

CFA Color Filter Array
La maggior parte della macchine fotografiche è equipaggiata con un singolo sensore che cattura le immagini attraverso un CFA (filtro a griglia di colori). La pluralità dei filtri CFA è composta da una griglia che alterna i tre colori rosso, verde e blu, posizionata direttamente sul sensore. Poiché, con questo sistema, è possibile catturare solo un canale per pixel, per ottenere un'immagine a colore occorre ricostruire le due componenti mancanti per ogni singolo pixel (demosaicing). Trascurando la metodologia utilizzata al fine di ricreare i tre piani di colore, l'interpolazione, in genere, introduce specifiche correlazioni statistiche tra sottoinsiemi di pixel, in ognuno dei tre canali. Poiché il filtro CFA è una griglia con una tessitura periodica, queste correlazioni avranno un andamento periodico. Sfruttando questa periodicità è possibile individuare un tipo di firma digitale associata all'interpolazione del colore.

Approcci esistenti.
Analisi dei difetti dei pixel. Questo metodo rappresenta un affidabile strumento per l'identificazione della camera anche da immagini compresse lossy (JPEG). Alcune camere non contengono nessun difetto o sono eliminati in post produzione dagli algoritmi.

Ogni banda di colore dell'immagine, mostra dei tratti e degli schemi definiti a prescindere dal contenuto dell'immagine stessa che dipendono da: CFA, algoritmo di demosaicing, elaborazione/trasformazione del colore. Per individuare le differenze che risultano essere presenti fra immagini catturate con fotocamere differente occorre estrarre 34 caratteristiche da ogni immagine, divise in due grandi gruppi:
- Misure relative al colore

- Misure relative alla qualità dell'immagine
La classificazione avviene tramite una classificazione SVM.

Il sensore non riporta in output solo il segnale pure ma anche varie componenti di rumore. Il modello di rumore del sensore può essere usato come caratteristica rappresentativa della camera.

Rumore
Durante tutto il processo di acquisizione ed elaborazione, l'immagine può essere affetta da rumore o imperfezioni di diversa natura. Il rumore nelle immagini digitali si evidenzia in prevalenza come un certa granulosità o puntinatura monocromatica (luminance noise) e/o come puntini o macchioline colorate (chroma noise) evidenti soprattutto nelle aree uniformi come il cielo, o in aree scure con poco dettaglio. L'effetto è molto simile a quello delle immagini da pellicola ad alta sensibilità.
Il rumore delle immagini è un random, indesiderato, oscillazione del valore del pixel nell'immagine. Ci sono numerose sorgenti di imperfezioni e rumore che entrano dentro vari stadi del processo di acquisizione dell'immagine.

Le sorgenti principali di rumore sono:
- **Photon Shot Noise**: si verifica quando un numero finito di fotoni è più piccolo abbastanza da dare vita ad una fluttuazione visibile in una misurazione
- **Dark Current (Thermal Noise)**: questo tipo di rumore esiste anche quando il sensore non è esposto ad nessuna luce incidente, e aumenta all'aumentare della temperatura del sensore.
- **Readout noise (Bias Noise)**: questo rumore è generato durante la lettura dei valori del sensore e non dipende delle condizioni di ripresa.
- **Reset noise**: succede quando si resetta un pixel, dovuto ad un residuo di carica. Il pixel non si resetta esattamente a zero.
- **Pattern noise**: un componente deterministico che resta approssimativamente lo stesso se più foto sono scattate dalla stessa scena
- **Quantization noise**: analogo al convertitore digitale in ogni colonna introduce rumore a causa del processo di quantizzazione.

Image noise
Quando il sensore acquisisce una scena, anche nelle migliori condizioni di illuminazione, l'immagine digitale mostrerà comunque piccole variazioni di intensità tra i singoli pixel, a causa delle numerose fonti di rumore che intervengono nel processo di formazione dell'immagine. Come precedentemente accennato, il rumore è composto da una componente casuale che dipende dal photon shot noise, rumore termico, ecc e una componente fissa, dovuta al pattern noise, che lascia una traccia pressoché identica su tutte le immagini acquisite con lo stesso sensore.
In particolare, ogni fotocamera digitale possiede un sensore lievemente differente dalle altre dello stesso modello, per via di un "disturbo" univoco e riconoscibile, ciò permette di identificare il sensore a partire dalle immagini, sfruttando la stessa idea che ci consente di distinguere le tracce univoche lasciate dalle canne delle armi da fuoco sui proiettili.
Il disturbo generato nelle immagini è legato sia al sensore in sé, che alle minuzie nella

costruzione e nell'assemblaggio di ogni dispositivo. Questo assicura una differenza tra singoli dispositivi sufficiente a rendere improbabile la presenza di due camere che generino il medesimo disturbo, proprio come avviene per le impronte digitali.

Identificazione del sensore usando il pattern noise
Tra le differenti cause di disturbo presentate, il pattern noise differisce dalle per le sue **proprietà deterministiche**, così può essere usato come identificazione della camera.
Pattern noise consiste in due componenti principali che sono:
- Fixed Pattern Noise (FPN)
- Photo Response Non-Uniformity Noise (PRNU)

Il componente principale del FPN è a causa delle corrente oscura che si riferisce alla differenza pixel-a-pixel quando il sensor array non è esposto alla luce.
PRNU è composto da:
- Pixel non-uniformity (PNU), che è definito come la sensibilità del pixel alla luce ed è la causa primaria di imperfezione nel processo di produzione del sensore
- Low frequency defect, dovuto alla rifrazione della luce sulle particelle di polvere e alle superfici ottiche e alle impostazione dello zoom.

PNU associato al sensore può essere usato per identificare la sorgente nel seguente modo: Estrarre il pattern di riferimento usando un algoritmo di riduzione del rumore da un set di immagini catturate con la stessa camera. Il pattern di riferimento deve essere mediato per eliminare il componente casuale del rumore. Determinare se un'immagine data è catturata da una camera digitale verificando che il pattern di rumore estratto dall'immagine individuale è correlata con il pattern di riferimento della camera digitale. Una decisione è presa basandosi comparando la correlazione statistica misurata ad una predeterminata soglia di decisione.

Occorre calcolare un valore di correlazione fra il rumore estratto dall'immagine in esame e le impronte digitali calcolare. I valori ottenuti vengono confrontati tra loro e con un valore di soglia per stabilire da quale fotocamera è stata acquisita l'immagine.

Questi metodo produce buoni risultati, ed è abbastanza affidabile usando anche immagini con un differente livello di compressione JPEG, immagini processate usando operatori puntuali come ad esempio aggiustamenti di luminosità/contrasto o correzione di gamma e immagini acquisite da due camere dello stesso brand e modello.

La procedura appena descritta è la più semplice e nota. Recentemente sono state proposte diverse migliorie e piccole varianti che rendono l'algoritmo di identificazione ancora più affidabile. Alcuni autori hanno presentato delle tecniche attraverso le quali è stato possibile migliorare la stime del reference pattern, che fanno uso di piccoli training set e utilizzano

particolari procedure di classificazione.

Operazioni di post-processing applicate ai reference pattern stimati, inoltre, possono ridurre la correlazione tra reference pattern di fotocamere della stessa marca e modello, riducendo quindi ulteriormente il numero di errori della procedura.

Contraffazione e processi maliziosi
Rimuovere intenzionalmente il pattern noise da un'immagine per prevenire l'identificazione.
Il modo più facile per prevenire una semplice identificazione del pattern di riferimento è applicare una leggera rotazione, possibilmente combinata con altri processi che potrebbero includere resizing, cropping e filtering.
Estrarre il rumore e copiarlo in un'altra immagine per far in modo che l'immagine sembri scattata con una particolare camera. Questo tipo di processo malizioso è molto difficile: richiede di rimuovere il pattern noise da un'immagine che vogliamo controllare e aggiungere il pattern noise di riferimento di un'altra camera, evitando di creare artefatti visibili.

AntiForensics
Fortunatamente l'eliminazione del pattern noise, o la sovrapposizione dello stesso su un'immagine, sono operazioni abbastanza complicate, soprattutto per un non esperto. Se l'alterazione non è ben fatta, infatti, si potrebbe rischiare di aggiungere artefatti che potrebbero far risaltare il tentativo di manomissione, e comunque di non riuscire ad ingannare l'algoritmo di identificazione.
D'altra parte, purtroppo, operazioni molto elementari sull'immagine, come un crop o una rotazione potrebbero rendere l'immagine irriconoscibile.

Casi di studio

Ricostruzione dinamica
Oltre all'ovvio "miglioramento visuale" dei dati, all'analista è spesso richiesto di dare supporto alla ricostruzione delle dinamiche che hanno portato all'evento criminoso.
Situazioni complesse di difficile rappresentazione.
Determinazione dei "punti fermi (o certi)" della ricostruzione dinamica in termini di tempi e spostamenti e luoghi:
Obiettivo: fornire ipotesi sulle dinamiche dei fatti analizzati, affiancate da un'analisi di plausibilità su basi analitiche/statistiche.

Esperimenti e simulazioni
Quando? E' necessario ricostruire o comprendere meglio un evento o una dinamica
Cosa serve? E' necessario siano presenti uno o più "dati certi". Per dato certo si intende un dato sicuro, inconfutabile scientificamente misurabile tramite tecniche ripetibili (posizione di un cadavere, orario di passaggio da una telecamera di sorveglianza)
Come? Tramite tecniche informatiche è possibile ricostruire un evento fissando le grandezze note o dati certi e facendo variare - tramite simulazioni le grandezze incognite.

Esperimenti.

Quando? I dati certi sono tanti e le grandezze incognite sono poche. Inoltre il dato certo è replicabile in un ambiente “controllato”
Come? Viene eseguito un esperimento giudiziale in ambiente controllato.

Simulazioni
Quando? I dati certi sono pochi e le grandezze incognite sono tante. Pertanto non è possibile replicare tutte le possibilità in un ambiente “controllato”.
Come? Attraverso un tool create (tante) simulazioni diverse al variare di tutte le combinazioni di grandezze incognite.

E’ così possibile dimostrare **scientificamente** che alcuni scenari possono essere **realistici** ed è anche possibile valutare analiticamente tutte le **probabilità**.

La fase di acquisizione
Quando si intendono acquisire evidenze che potrebbero essere contenute all’interno d un sistema di videosorveglianza, si devono seguire prescrizioni di carattere generale, facendo poi attenzione a prelevare i dati rilevanti che caratterizzano ogni specifico ambito applicativo e implementazione tecnologica.

Criteri di carattere generale
L’acquisizione risulta essere una delle fasi più delicate della Digital Forensics; è dunque necessario attenersi a linee guida che permettono la corretta acquisizione senza alcuna possibilità di invadere la prova.
Modalità di acquisizione:

- **LIVE**, in tutti quei casi in cui il sistema di videosorveglianza non può essere sequestrato per svariati motivi.
- **POST-MORTEM**, i dati possono essere acquisiti in un secondo momento.

La prima operazione da fare in entrambi i casi:
Riportare con precisione marca, modello, numero seriale ma anche versione del software e firmware per ognuno dei componenti individuati.

Il problema del formato del file video
Spesso i filmati dei sistemi di sorveglianza sono codificati in formati cosiddetti proprietari. Ciò significa che il file video è incapsulato in una sorta di “scatola nera” digitale, in cui chi si trova ad operare sa molto poco.
Problema: il contenuto video è visibile con i player forniti direttamente dal gestore del sistema di sorveglianza È dunque necessario convertire i filmati in formato adeguato per poterli elaborare.
Cosa occorre: conoscenza del software fornito dal produttore del sistema e possibilità di ricorrere a tecniche di engineering per capire la struttura del sistema.
Vista la varietà di sistemi nel mercato questo passo è complesso e richiede tempo per essere svolto in maniera corretta. L’obiettivo è quello di non introdurre perdite di qualità del filmato.

Dove trovare i dati
I dati importanti non sono le “informazioni visive”, ma anche le **informazioni accessorie**.

E’ necessario dunque cercare i dati oltre che nel video anche nei seguenti accessori:

- Telecamere: all’interno del supporto di memorizzazione estraibile (cassetta, VHS, cassetta DV o miniDV, memoria SD, HD) o nei files di log dell’apparato.
- DVR: nell’hard disk dell’apparato su cui vengono registrati i filmati e nel file di log
- Apparati client: eventuali salvataggi di immagini fatte da un operatore sul sistema cliente e nel files di log.
- Server di registrazione: negli hard disk, nelle impostazioni di configurazioni e nei files di log
- Switch o ponti wireless (es WIFI): nelle eventuali impostazioni di configurazioni e nei files di log

Operazioni di acquisizione live

5 procedure da seguire in modo corretto, pena la perdita o l’alterazione di informazioni:

1) Prescrizioni generali di “live video forensics”
2) Assicurazione della timeline
3) Consultazione del sistema di videosorveglianza
4) Raccolta dei dati rilevanti live
5) Spegnimento del sistema

Prescrizioni generali di “live video forensics”

1) Documentare su documento cartaceo ogni operazioni eseguita
2) Attivare un videoregistratore esterno sulle postazioni clienti delle quali eventualmente si opera, utilizzando una videocamera posta alla spalle dell’operatore
3) Qualora fosse possibile attivare una registrazione interna caricando sulla postazione client dalla quale si opera un programma tipo CamStudio
4) Individuare tutti i dispositivi funzionanti connessi al sistema, postazioni client, telecamere connesse via rete, server di archiviazione e più in generale tutti i componenti del sistema dotati di indirizzo di rete
5) Utilizzare analizzatori di rete come Wireshark per individuare tutti gli apparati connessi in rete

Assicurazione della timeline

1) Rilevare il System Clock del BIOS di ogni componente del sistema (data, ore, minuti, secondi) annotando con precisione lo scostamento con l’ora reale. La determinazione dello scostamento tra l’ora realtà e quella impressa sulle immagini del sistema di videosorveglianza è certamente un “atto irripetibile”
2) Verificare la presenza di un NTP server di sincronizzazione
3) Salvare il layout delle impostazione client individuate attraverso salvataggio di screenshot
4) Salvare il “field of view” di ogni telecamera e fotografarla. Effettuare questa

operazione nel momento del reperimento è importante poiché successivamente l'inquadratura potrebbe essere spostata
5) Analizzare gli apparati di rete presenti, salvando la configurazione

Accertamenti live: "Consultazione" del sistema di videosorveglianza

1) Creare un sistema dedicato per le ricerche o documentare con quale operatore si stanno eseguendo le ricerche.
2) Salvare i filmati di interesse, facendo attenzione a mantenere il filmato nel formato originale nel quale è archiviato sul sistema.
3) Qualore il sistema ne sia dotato, esportare i file associando un watermark.
4) Calcolare immediatamente il numero di hash dei file salvati
5) Qualora il sistema lo permetta, inserire un "bookmark" sui files di interesse, in mood
6) che questi non vengano sovrascritti, trascorso il tempo di "retention" programmato.

Raccolta dei dati rilevanti "live"

Individuare, attraverso lo studio dei manuali o la consultazione del produttore, quali dati sono presenti nella memoria "volatile" in senso stretto (RAM) e quali si possono classificare come dati temporanei. Tra questi quali possono essere di interesse per procedere, se necessario, alla loro acquisizione.

a. Registrazioni temporanee o di backup su scheda SD a bordo camera o a bordo encoder
b. Registrazioni su supporti di "failover"
c. Spezzoni di registrazioni esportate presenti su una delle macchine client
d. Log del sistema di videosorveglianza
e. I "registri del sistema"

Spegnimento del sistema

Qualora il sistema di video sorveglianza dovesse essere sequestrato, una domanda classica è se sia più opportuno eseguire uno spegnimento fisico della macchina attraverso un'operazione di shutdown, oppure se sia opportuno procedere alla rimozione dell'alimentazione.

Primo caso : il rischio è quelli di attivare script non conosciuti e potenzialmente distruttivi la cui esecuzione può essere stata decisa in fase di pre intervento

Secondo caso: è possibile causare danni irreparabili ai dati archiviati

Non è quindi possibile dare una risposta univoca al quesito di cui sopra, se non consigliare una attenta valutazione caso per caso, in relazione alla tipologia dell'impianto. In generale si dovrebbero propendere per uno spegnimento di tipo fisico: la maggiore salvaguardia deriva da una buona acquisizione realizzata nell fase "live"

Acquisizione: Digital Video Recorder

I dati di contesto e i dati rilevanti da prelevare in fase di acquisizione del reperto possono cambiare in relazione alla specifica implementazione tecnologia utilizzata. informazioni essenziali da reperire:

- Nome del reale costruttore
- Presenza di file di log
- Manuali utenti
- Software di esportazione di filmati

Network Video Recorder

La principale preoccupazione quando si devono realizzare acquisizioni su NVR, è quello di individuare tutti i “terminali della rete” nei quali potrebbero essere presenti informazioni utili da acquisire.

Di cosa bisogna tener conto:

- le informazioni possono essere distribuiti su server diversi
- A volte sono presenti server di backup, detti failover archiver, di cui bisogna tener conto
- Le informazioni di accesso possono essere, a loro volta, mantenute su server dedicati, detti server directory.

Risulta evidente che non sia sufficiente fare una copia di un server archiver per avere la certezza di aver acquisito tutte le registrazioni ma anche i dati di contesto ad esempio contenuti nel server di directory.

Secure Digital

SD possono essere trovate sia a bordo di telecamere, sia a bordo di encore. Prima di rimuovere la SD della telecamera, o dell'onere, è assolutamente opportuno accedere in modalità logica al suo contenuto e salvarlo tramite il client del sistema di videosorveglianza.

Di cosa bisogna tener conto:

- La SD potrebbe essere formattata in un formato proprietario. Risulta quindi opportuno sequestrare anche la telecamera o l’encoder.
- Dopo aver effettuato la copia forense dell’SD, questa potrà essere utilizzata all’interno dell’encoder o dalla telecamera connessa in rete, per valutare il contenuto.

La fase di analisi

Dopo la fase di acquisizione è necessario effettuare un’analisi sui dati e metadati relativi a un’immagine digitale. E’ noto infatti che ogni dispositivo di acquisizione e ogni elaborazione sulle immagini introduce una propria caratteristica di riconoscimento. E’ necessario saper distinguere tra **originalità del file** e **originalità del suo contenuto informativo**.

Valutazione di genuinità

Possibili approcci:

- Stimare in fase di decodifica il vettore di moto adatto in origine dall’encoder, oppure individuare alcune caratteristiche di ogni fotogramma (ad esempio la presenza o meno di artefatti di blocking, o le impronte date dalla fase di quantizzazione dell’immagine)
- Sfruttare la correlazione temporale dei residui di rumore di ogni singolo frame. In particolare ogni frame è diviso in blocchi e viene calcolata la correlazione fra i residui

di rumore di due blocchi temporalmente attigui (cioè blocchi nella stessa posizione di due frames adiacenti)
- Sfruttare il fatto che la trasmissione di un video attraverso un canale, nonostante vengano prese le opportune precauzioni, è sempre affetta da rumore. Ciò lascia tracce caratteristiche, che possono essere sfruttate per esempio in termini di pacchetti persi, nel contenuto video ricostruito.

Oltre al dato visivo i metadati

Si definisce metadato in un contesto di videosorveglianza “qualsiasi informazioni o dato secondario associato alla immagini in un sistema CCTV”. Questi dati ulteriori possono essere memorizzati in vario modo: embedded nel filmato stesso oppure associati ad esso in un unico file, che si può definire container.

I metadati sono sempre esistiti in un sistema di videosorveglianza, ma diventano sempre più importanti e attuali con l’evoluzione dei sistemi stessi. I sistemi attuali più evoluti, soprattutto di tipo NVR, permettono di creare veri e propri contenitori di informazione, container, strutturati secondo un database, che permettono di associare a filmanti metadati di ogni genere.

Operazioni da svolgere per il miglioramento dell’immagine/video

Il flusso di lavoro può essere riassunto come segue:

- Acquisizione e conversione del filmato
- Selezioni dei fotogrammi di interesse
- Deinterlacciamento
- Correzione degli artefatti da compressione
- Correzione dei disturbi analogici
- Riduzione del rumore
- Definizione dei dettagli
- Correzione della sfocatura e miglioramento dei dettagli
- Correzioni geometriche
- Regolazione di intensità e colori
- Stabilizzazione
- Integrazioni di più fotogrammi
- Altre elaborazioni

Riconoscimento antropometrico da immagini di videosorveglianza

Analisi fotometrica

Gli elementi morfologici fondamentali devono essere il più possibile indipendenti da variazioni ponderali e dall’età del soggetto, quando sia concluso il periodo

dell’accrescimento.
La forma generale del volto nella prospettiva frontale, per esempio, è uno degli elementi di caratterizzazione.

La forma della testa è classificata tenendo in considerazioni le tre parti costituenti: **frontale**, **parietale** e **occipitale**.

Il profilo del volto costituisce l’elemento morfologico di notevole valore, è può essere considerato nella sua globalità oppure dell’andamento del complesso fronte-naso e di quello naso-buccale.

L’orecchio esterno è costituito dal **padiglione auricolare** e dal **meato acustico esterno**. Le variazioni del padiglione sono molto numerose e interessano sia il padiglione nella sua globalità sia le parti che lo costituiscono. Considerandolo in toto l’orecchio può essere **grande**, **medio**, **piccolo**. Se si tiene conto della larghezza e della lunghezza sarà: **molto largo, largo, medio, stretto e molto stretto, molto lungo, lungo, medio, corto e molto corto.**

Tubercolo di Darwin.
Nel punto che corrisponde all’apice del padiglione di trova molto frequente mento un piccolo rilievo detto tubercolo di Darwin che viene classificato in diverse forme:

- **Orecchio da cercopiteco**: il tubercolo si trova non sul margine dell’elice ma sul margine dell’orecchio stesso, per cui l’elice forma un netto gomito nel punto più alto.
- **Orecchio a punta aguzza**: il tubercolo genera una punta aguzza
- **Orecchio a punta arrotondata**
- **Orecchio a punta appiattita**
- **Orecchio con assenza della punta**

Forma del mento.
La classificazione avviene distinguendo, a seconda delle dimensioni di altezza e larghezza, in alto, medio, basso e in largo, medio e stretto.

Sopracciglia.
Presentano colorazione che generalmente coincide con quello dei capelli. L’andamento delle tre porzioni che le costituiscono e cioè testa, corpo e coda, permettono la classificazione.

Criteri identificativi
Non compatibile: nessuna delle caratteristiche in esame è oggettivamente compatibile oppure è presente almeno una caratteristica **universale**, **unica** e **permanente** che permette di escludere che due soggetti hanno la stessa identità.

Compatibilità parziale (o affinità): la scarsa definizione e/o visibilità di almeno una delle due immagini a confronto non permette di rilevare particolari o caratteri antropo-somatici che permettano di giungere ad un giudizio positivo di comparazione; vi si riscontrano comunque alcuni particolari simili in entrambi gli individui o oggetti a confronto.

Compatibilità: gli elementi nei due individue o oggetti a confronto permettono di rilevare numerosi particolari o caratteri antropo-somatici simili in entrambi gli individui o oggetti. non è possibile comunque, vista la deinizione di almeno una delle immagini a confronto, evidenziare particolari o contrassegni (nei, cicatrici, rughe caratteristiche, ecc) nei due individue o oggetti messi a confronto che porterebbero ad un giudizio di **incompatibilità** o di **compatibilità totale**.

Compatibilità totale: i due individui o oggetti, ritratti nelle immagini a confronto, hanno tutti i particolari o caratteri antropo-somatici visibili simile, per forma e proporzioni. Sono inoltre presenti alcuni elementi o particolarità anatomiche singolari, contrassegni, riscontrabili in entrambi gli individui o soggetti a confronto.

Il sistema SARI
Basato su nuovi e potenti meccanismi di IA. Matching automatico su DB con milioni di volti.

Audio (Forensics): la fonetica forense

Riconoscimento biometrico
Con il termine riconoscimento biometrico si fa riferimento alla tecniche automatiche per riconoscimento dell'identità di un individuo basata su uso di **caratteristiche fisiologiche** o **comportamentali** distintive.

La modalità del riconoscimento può essere in termini di:

1. **Verifica (autenticazione)**: si dichiare l'identità. Confronto uno a uno al fine di determinare se l'identità dichiarata dell'utente è vera o no.
2. **Identificazione**: l'utente non dichiare l'identità. Confronto uno a molti al fine di stabilire l'identità dell'individuo.

Errori nei sistemi biometrici

- **False Match** (nel riconoscimento positivo chiamato spesso **false acceptance** o **falsa attribuzione**) misurazioni biometriche di persone diverse vengono erroneamente considerate come appartenenti alla stessa persona.
- **False Non-Match** (nel riconoscimento positivo chiamato spesso **false rejection** o **falsa esclusione**) misurazione biometriche della stessa persona vengono erroneamente attribuite a persone diverse.

Attendibilità degli indici biometrici

- Impronte vocali (voce naturale Hi-Fi) FE 1%, FA 0,1%
- Impronte vocali (segnale telefonico) FE 3%, FA 0,4%

- Impronte digitali FE 0.5%, FA 0,001%
- Firma FE 0,2%, FA 0,6%
- Retina FE 2,8%, FA 0%

Natura del suono
Segnale di pressione - generato da una sorgente di vibrazione - che si propaga in un **mezzo elastico** (aria, acqua) fino ad un apparato sensoriale (orecchio). Durante la propagazione si modifica - per assorbimento, riflessione, diffusione, ecc - e si carica di "indizi" spaziali.

Nel vuoto assoluto i suoni **non possono** propagarsi e quindi non si sentono i rumori.

Come accennato la natura del suono è di tipo **ondulatorio**: si tratta di onde meccaniche che trasportano energia lontano dalla sorgente sonora. Viene quindi trasportato un segnale, cioè una variazione continua di qualche parametro legato all'ambiente in cui avviene la propagazione. Il segnale sonoro è un'**onda longitudinale** poiché la sorgente sonora vibra nella stessa direzione di propagazione del suono.

Suono e percezione
La natura percettiva del suono è stata spiegata solo in parte. Alla fine dell'elaborazione effettuata dal nostro apparato è possibile percepire: musica, linguaggio, rumore.
Il segnale sonoro: caratteristiche
Innanzitutto distinguiamo le tre caratteristiche fondamentali di ogni suono **altezza, intensità** e **timbro**. Poiché si tratta di **grandezze percettive** per misurare in modo esatto sono stati messi a punto altrettanti parametri di tipo fisico.
La **vibrazione** responsabile del suono può essere rappresentata come un'**onda sinusoidale**. E' possibile quindi mettere in relazione diretta i parametri percettivi con i relativi parametri fisici dell'onda:

Parametro Percettivo	Parametro fisico	Rappresenta
Altezza	Frequenza	Tonalità audio
Intensità	Ampiezza	Volume
Timbro	Spettro	Tipologia di strumento

Distinguiamo poi: **dominio del tempo** ovvero come varia la pressione sonora nel tempo in corrispondenza di un determinato punto di ascolto e il **dominio della frequenza** ovvero da quante e quali componenti elementari (toni) è composto il segnale sonoro.

Suoni elementari: toni
Ampiezza (**A**) espressa in decibel **dB**;
Periodo (**T**) espresso in secondi;
Frequenza (**f**) numero di cicli (onde) al secondo, espressa in Hertz **Hz**.

La frequenza

La frequenza si può definire come il numero di onde completate in un secondo. La frequenza è il parametro che distingue tra loro le note musicali. A frequenze minori corrispondono i bassi (20-500 Hz) e in maniera crescente si hanno i toni medi (500-8000 Hz) e poi gli alti (8000-20000 Hz).

Le caratteristiche frequenziali inducono una differenziazione dei suoni in suoni **puri e complessi**. Un suono pure (detto anche tono) è costituito da una sola frequenza ed è quindi descritto da **un'onda sinusoidale semplice**. Un suono complesso consiste invece di **più frequenze sommate in un'onda dall'andamento articolato**; in un singolo periodo possono essere comprese più alternanze di compressioni e rarefazioni intermedie; l'ascolto rivela il timbro caratteristico di una sorgente.
In generale, in natura i suoni sono di tipo complesso, e lo specifico andamento deriva da metodo di produzione del suono da parte della sorgente.

Frequenza e note musicali
IL suono sono segnali che hanno frequenze comprese all'incirca tra i 20 e 20000 Hertz. tali limiti derivano direttamente dal nostro sistema uditivo, Oltre tali valori si hanno gli infrasuoni e gli **ultrasuoni**.
Un suono complesso qualsiasi contiene molte frequenze. Affinché in un suono si possa individuare una frequenza speciale, che caratterizza la sensazione globale di gravità/acutezza trasmessa dal suono occorre che il segnale sia periodico. I suoni prodotti da strumenti musicali, hanno delle fasi di periodicità significative e per essi ha senso parlare della sensazione di altezza.

Digitalizzazione del suono

I microfoni producono **rappresentazioni analogiche del segnale audio**. Questo è infatti rappresentato da un valore di tensione il cui andamenti nel tempo riflette le oscillazioni di pressione nell'aria. Nel caso di dischi di vinile o nel campo magnetico la curva continua nel tempo delle variazioni di ampiezza viene rappresentata da una curva continua nel tempo delle variazioni di tensione elettriche ed è memorizzata nei solchi del disco o nel campo magnetico del nastro.
Per poter rappresentare il suono in un sistema digitale bisogna prima convertirlo in un flusso di numeri rappresentati in **forma binaria**. Una rappresentazione digitale assegna dei numeri.

Campionamento
E' la **discretizzazione** del segnale analogico nel tempo.
La conversione del suono da formato analogico a digitale avviene per mezzo di una scheda di acquisizione o **digitalizzazione** che campioni il valore della forma d'onda ad intervalli regolari.

Quantizzazione
E' la discretizzazione dell'ampiezza. L'ampiezza di ogni campione, dovendo essere rappresentata digitalmente (cioè con una codifica binaria) non può assumere infiniti valori. Ogni singolo campione di ampiezza (tensione elettrica) viene quindi assegnato ad uno dei valori numerici che sono consentiti dalla codifica digitale (si commettono errori di

quantizzazione). La conversione analogico-digitale richiede pertanto un processo di **discretizzazione sia nel tempo** (campionamento) che in **ampiezza** (quantizzazione). E' necessario quindi specificare due parametri relativi: quanto spesso campionare il segnale nel tempo (**frequenza di campionamento**) e quanti valori rappresentare per ogni campione (**precisione di quantizzazione**).

Precisione di quantizzazione
Con qualsiasi rappresentazione analogia una parte del segnale impiegato per rappresentare la grandezza è dovuta al **rumore**. Un poco rumore che tutti sperimentiamo è quello causato **dall'impressione magnetica sul nastro e viceversa** della lettura del segnale registrato; tale rumore viene percepito come un fruscio dal nostro orecchio.

Per la riduzione del rumore sono stati sviluppati vari metodi: il noto sistema della **Dolby**, ad esempio, enfatizza in registrazione alcune regioni dello spettro nelle quali il rumore è maggiormente percepibile; in riproduzione, le stesse regioni vengono de-enfatizzate, con il risultato di riportare al libelli corretti i rapporti fra le frequenze nel segnale e attenuare nel contempo il rumore.

Per stimare l'ammontare di rumore introdotto da un sistema analogico si utilizza il **signal-to-noise ratio** (**SNR**), cioè il rapporto tra la massima ampiezza utile del segnale e l'ampiezza del rumore presente (statico o bianco) sovrapposto al segnale. Viene anche definito come rapporto tra la potenza del segnale e quella del rumore. A valori alti di SNR, che si misura in db corrisponde una migliore qualità del suono.

I CD Audio hanno un valore tecnico di SNR ratio di circa 96 dB. Valori inferiori a 70 dB indica un rumore di fondo udibile. Ridurre la quantizzazione a 8-bit, riducendo del 50% la quantità di dati farebbe diminuire la qualità di un CD audio di circa 50 dB, producendo una quantità simile a quella della radio AM.

Dinamica
Molto semplicemente rappresenta la capacità di **graduare** in modo nitido **l'intensità del suono** (nel contesto complessivo) riproducendo nel giusto rapporto i picchi di intensità, i suoni di basso livello, e tutti i suoni la cui intensità è compresa tra i due estremi. Ad una maggiore profondità di bit corrisponde la possibilità di registrare e/o riprodurre una maggiore dinamica. La **gamma dinamica** è il rapporto tra l'ampiezza massima e l'ampiezza minima presenti nel segnale.

Teorema di Nyquist
Per avere una **digitalizzazione senza perdita** di informazione è necessario campionare con un frequenza almeno il **doppio della massima frequenza** che compare nello spettro della forma d'onda da acquisire. Il tasso di campionamento **fc** deve essere almeno il doppio della frequenza massima **fmax** presente nel segnale: **fx >= 2fmax**.

Se l'orecchio è in grado di captare suoni, fino a 20000 Hz, occorre campionare ad almeno 40000 Hz. In realtà la frequenza di campionamento standard attuale è pari a 41100 Hz per almeno due ragioni:

- Il valore 20000 Hz è un valore medio. Fissando una frequenza di campionamento standard leggermente superiore ci si assicura la massima fedeltà
- Nei primi anni ‘70 i supporti magnetici utilizzati impedivano di oltrepassare questo limite.

Al di sopra di tale soglia si ha il ***sovracampionamento*** che può portare solitamente ad uno spreco di banda.
Al di sotto si ha il ***sottocampionamento*** che spesso genera disturbi e distorsioni quali ad esempio l’**aliasing**.

Aliasing
È importante notare che ciò che avviene nella digitalizzazione rispetta il teorema del campionamento in senso inverso. Stabilito un tasso di campionamento SR, occorre eliminare dal segnale tutte le frequenze che siano maggiori di SR/2. Per fare ciò si una un **filtro passa basso** in quanto fa passare solo frequenza sotto una certa soglia ed è detto **antialiasing**, in quanto evita il problema dell'aliasing.

Memoria in Kb del file audio
Lo spazio di memoria occupato da un file si calcola con la seguente formula:

spazio = (fc * D * Nbc * Nc) / (8*1024)

dove:

- **fc**: tasso di campionamento (campioni al secondo)
- **D**: durata in secondi
- **Nbc**: numero di bit usati per rappresentare ciascun campione
- **Nc**: numero di canali (1 mono, 2 stereo)

Formati audio digitale
I formati del file audio sono stati sviluppati per standardizzare la riproduzione e la distribuzione di dati audio nei sistemi digitali. I parametri che determinano i dati audio sono tre:

- **sampling rate**, misurato in campioni/sec (Hz) per canale
- **lunghezze e tipo di codifica della parola binaria**, ovvero il numero di bit per campione
- **numero di canali**

I formati si dividono in due tipi:

- **con intestazione** (header), auto descriventi
- **senza intestazione** (header less o raw)

L’intestazione contiene la **definizione della codifica usata** per i dati audio e la **descrizione del brano e dati di copyright**. L’intestazione inizia spesso con una parola chiave, e prosegue poi con i dati della codifica.

Caratteristiche del segnale vocale

- Voce naturale 20-10000 Hz
- Segnale telefonico: banda standardizzata ITU-T:
    - **Narrowband** (20-4000Hz, qualità telefonica)
    - **Wideband** (20-7000, qualità videoconferenza)
- Media nulla, distribuzione uniforme
- Segnale non stazionario con correlazione a breve e lungo termine
- Struttura "**on-off**" nel tempo con il 40% di attività vocale e circa il 60% di pause e silenzio.
- **Suoni vocalizzati, non vocalizzati e misti**

Struttura ON-OFF di una conversazione
- Utilizzo di un **codec CBR + VAD** (source driven)
- Codifica **CBR** dei tratti ON (Talkspurt)
- Trasmissione periodica dei **SID** nei tratti di OFF (silenzio o rumore ambientale)
- Sintesi dei **tratti di OFF in Rx tramite un CFG**
- Prestazioni dipendono dal rumore ambientale

Compressione/Decompressione del segnale vocale
- bit rate **rb = fc * b**
- La frequenza di campionamento **fc** (NB o WB) e la risoluzione **b** determinano la qualità del segnale originale non compresso
- Fattore di compressione = input bit rate / output_bit rate

Standard ITU-T G.711 Log PCM
- Banda telefonica 0-4 kHz
- Frequenza di campionamento **fc = 8kHz**
- Distribuzione non uniforme
- Compressione della dinamica
- Bitrate: **rb = b * fc = b * 8 kHz**
- 12 bit lineari/campione -> 8 bit logaritmi/campione
- 96 kbit/sec (b = 12) -> 64 kbit/sec (b = 8)
- Qualità **MOS 4.3**
- Standard per l'accesso base ISDN

La frequenza fondamentale
La frequenza fondamentale o **pitch** è l'inverso del periodo di vibrazione delle corde vocali durante l'emissione di un suono vocalizzato

Le formati
Sono le frequenze delle spettro vocale in cui è la massima energia. Sono rappresentative delle **caratteristiche fisiche del tratto vocale**. Si estraggono tramite l'analisi **LPC o CEPSTRUM**

La voce
La voce è un suono complesso perché è dato dalla combinazione di tre effetti:
1) La vibrazione delle corde vocali (genere la frequenza fondamentale)
2) Il rumore prodotto nella fonazione

3) Il transito attraverso il tratto vocalico (genere le frequenze formanti)