

CF Obsidian

1- Figure

Pubblico Ministero P.M.

- Dirige le indagini preliminari col la [polizia giudiziaria](#)
- Nomina [consulenti tecnici](#) D'ufficio durante le indagini preliminari per ulteriori accertamenti.
- valuta l' esito delle indagini e decide se archiviare o rinviare a giudizio.
- Gestisce le indagini ed ha il potere di esercitare l'azione penale.
- iscrive le notizie di reato nel Registro Generale Notizie di reato.
- effettua la richiesta di [rinvio a giudizio](#) esercitando l' azione penale.
- Effettua la [citazione diretta a giudizio](#) con le seguenti accuse:
 - delitti puniti con la pena della reclusione non superiore al massimo di 4 anni.
 - violenza, minaccia o resistenza a pubblico ufficiale.
 - oltraggio a un magistrato in udienza aggravato.
 - violazione dei sigilli da parte del custode.
 - rissa aggravata senza gravi lesioni.
 - furto aggravato.
 - ricettazione.
- Al **termine delle indagini preliminari**, può presentare al [GIP](#) la [richiesta di archiviazione](#) nei seguenti casi:
 - gli elementi non sono idonei a sostenere l'accusa.
 - l' autore è rimasto ignoto.
 - il reato è estinto.
 - il fatto non è previsto dalla legge come reato.
 - il fatto sia particolarmente tenue.

Polizia Giudiziaria P.G.

- Svolge le [indagini preliminari](#) insieme al [PM](#).
 - Attività informativa: acquisisce la notizia di reato e la riporta al PM.
 - Attività investigativa: ricerca l' autore del reato.
 - Attività di prevenzione: impedisce che i reati vengano aggravati .
 - Attività assicurativa: individua e protegge le prove.
- Durante il [Procedimento penale](#) incarica il [Computer forenser](#) di svolgere determinate mansioni.

Indagato

è la persona alla quale vengono svolte delle indagini a seguito dell'iscrizione di un fatto a cui addebitato nel registro delle notizie di reato.

- l'indagato resta tale fino alla richiesta di rinvio a giudizio o di archiviazione.
- ha l'obbligo di farsi assistere da un difensore.
- Può difendersi producendo memorie e possono essere interrogati esclusivamente alla presenza del difensore.
- può avvalersi di consulenti tecnici.

Imputato

è la persona indagata nei confronti della quale è stata esercitata l'azione penale (rinvio a giudizio).

- l'imputato resta tale in ogni stato e grado del processo, fino a sentenza definitiva.
- la sua assenza in udienza non ne pregiudica il suo corso, che viene celebrato ugualmente.
- ha l'obbligo di farsi assistere da un difensore
- Può difendersi producendo memorie e possono essere interrogati esclusivamente alla presenza del difensore.
- può avvalersi di consulenti tecnici.

Parte offesa

- soggetto titolare del bene giuridico (patrimoniale, morale, personale) leso dall'autore di un reato.
- ha il diritto di querela in tutti i casi in cui il reato non debba procedersi d'ufficio o dietro richiesta o istanza.
- può presentare memorie, indicare elementi di prova, e nominare un difensore e consulenti tecnici.
- si deve fare una differenza fra esposto, denuncia e querela:
 - **Esposto**: segnalazione all'autorità giudiziaria di un fatto allo scopo di valutare se ricorrere ad un'ipotesi di reato.
 - **Denuncia**: è un atto con la quale si informa l'autorità Giudiziaria di una notizia di reato perseguibile d'ufficio.
 - **Querela**: è una dichiarazione della persona offesa con la quale si esprime la volontà di punire il colpevole di un reato subito, non perseguibile d'ufficio. può essere ritirata se non tratta di reati sessuali ai danni di minori.

Difensore

- Assistenza : resta un collaboratore di natura tecnica, diventando la bocca e l'orecchio giuridico del cliente.
- Rappresentanza: agisce in sostituzione dell' interessato nell' esercizio di diritti e facoltà.
- è nominato sia dalla parte offesa che dalla parte indagata.
- la sua presenza oltre ad essere un diritto , è condizione prima di legittimità e regolarità dello stesso procedimento penale
 - se non nominato da una delle 2 parti, ne viene nominato uno d'ufficio.
- può ottenere un accesso agli atti delle indagini preliminari
 - parziale a sostegno di una singola misura preventiva per poter gestire una eventuale opposizione.
 - completo solo a seguito dell'avviso di conclusione indagini (415bis c.p.p).

Giudice per le Indagini Preliminari GIP

- ha la funzione di garanzia dell' indagato nella fase delle indagini preliminari, decide se accogliere o meno le richieste del P.M su:
 - applicare misure cautelari.
 - autorizzare e convalidare l' uso di intercettazioni come mezzi di ricerca della prova.
- garanzia dell'azione penale
- accoglie o no la richiesta di archiviazione.
- non ha autonomia di iniziativa probatoria. provvede solo su richiesta della parte.
- è privo di un proprio fascicolo: Gli atti conosciuti sono quelli che il P.M presenta.

Giudice dell' udienza Preliminare GUP

- Interviene dopo l'esercizio dell' azione penale.
- Giudica la richiesta di rinvio a giudizio
 - esamina il fascicolo delle indagini preliminari e valuta le fonti delle prove raccolte.
 - ascolta le ragioni della difesa dell' imputato.
- il giudice potrà:
 - emettere decreto di rinvio a giudizio.
 - emettere sentenza di non luogo a procedere.

Giudice del dibattimento

- Presiede a tutta la fase dibattimentale e alle relative udienze.

- Può essere monocratica o collegiale.
- Per i reati più efferati è prevista una distinta composizione definita corte d' assise dove è presente anche la giuria popolare.
- Emette a sentenza.

Computer Forenser

- Nominato dalle autorità giudiziarie se richieste particolari competenze tecniche.
- a seconda di come e da chi è nominato, assume ruoli differenti:
 - **Ausiliario della PG:** nominato dalla polizia giudiziaria
 - **Consulente tecnico d'ufficio:** incaricato dal P.M durante le indagini preliminari per svolgere accertamenti.
 - **Consulente tecnico di parte:** incaricato da una delle parti coinvolte nel processo.
 - per assisterlo e presentare prove del reato subito (parte offesa).
 - Per controbattere a determinate operazioni tecniche compiute dalla parte accusatoria (indagato).
 - Perito del giudice: quando è il giudice a volere accertamenti tecnici o valutare quelle compiute dalle parti.
- impiega metodi e strumenti che garantiscono l'inalterabilità della prova anche se non dettagliatamente descritti dalla legge.
- è in grado di compiere accertamenti ripetibili e irripetibili
 - i secondi se compiuti comportano l'alterazione della fonte di prova e la ripetibilità della procedura non è più garantita.
 - compiuta se il dispositivo non è in buono stato oppure cambia autonomamente il proprio stato.
- compiuta se vi è l' esigenza di restituzione del reperto
 - dispositivi fondamentali per la normale attività di un azienda.

Consulente tecnico

D'ufficio

nominato dal P.M durante le indagini preliminari per ulteriori accertamenti.

Di parte

nominato da una delle 2 parti coinvolte nel procedimento

- per assisterlo a presentare prove tecniche del reato subito.
- per controbattere a determinare operazioni tecniche compiute dalla parte accusatoria.

Perito

- è nominato dal giudice nel caso siano richieste particolari competenze tecniche , nel caso di un incidente probatorio o di un udienza.
- può essere scelto dall' albo del tribunale oppure da soggetti non iscritti e individua in questi le competenze tecniche necessarie. esso viene avvisato degli obblighi e responsabilità che assume con il giuramento.

2- Procedimento penale e civile

![[Pasted image 20231129162754.png]]

Procedimento penale

Fase iniziale

le autorità giudiziarie ricevono una notizia di reato da parte di un'altra persona/soggetto, il P.M. iscrive la notizia sul Registro Generale Notizie di Reato.

Indagini preliminari

- Il P.M. e la polizia giudiziaria svolgono delle indagini per appurare o meno il reato
 - Possono avvalersi di 2 strumenti:
 - perquisizione: usato per verificare la presenza di una prova di reato
 - sequestro probatorio: usato a seguito di un riscontro positivo del primo, usato per tutelare la prova da alterazioni.
 - è usato anche in luogo di accertamento (253 c.p.p) quando non si dispongono immediatamente degli strumenti specifici o quando i tempi di accertamento possono essere lunghi.
 - le autorità che hanno disposto un sequestro provvederanno a sigillare il materiale e a custodirlo.

Accertamento tecnico (359 cpp)

- il P.M. può richiedere un accertamento tecnico, comportano specifiche conoscenze che esulano dalle competenze dall'organo inquirente.
- il PM può avvalersi/nominare un consulente tecnico.

Accertamento tecnico irripetibile (art 360 cpp)

- Se compiuti comportano l' alterazione della prova e la ripetibilità della procedura non è più garantibile.

- il P.M. esegue questa procedura avvisando preventivamente
 - l'Indagato e il suo Difensore.
 - la Parte offesa e il suo difensore.in modo da dare la possibilità a questi ultimi di assistere a tutta l'operazione del rispetto delle procedure.
- le parti possono nominare un proprio consulente tecnico.

Misure cautelari

- sono emessi dal giudice su richiesta del P.M. nel periodo intercorrente tra l'inizio del procedimento penale e l'emanazione della sentenza.
- Misure reali: impediscono la disposizione di determinati beni o cose.
- Misure personali: comportano una limitazione o privazione della libertà personale (coercitive), limitano temporaneamente l'esercizio di determinate facoltà o diritti (interdittive), emesse quando sussistono i seguenti rischi:
 - inquinamento delle prove.
 - fuga dell' indagato/imputato.
- reiterazione del reato.

Incidente probatorio

- può essere richiesta dalle 2 parti per anticipare la formazione di una prova durante le indagini preliminari.
- Richiesta dal GIP.
 - può nominare un proprio consulente tecnico nel caso servano particolari competenze tecniche: un perito.

Richiesta di archiviazione

- al termine delle indagini preliminari, il P.M. può presentare al GIP la richiesta di archiviazione nei seguenti casi:
 - gli elementi acquisiti nelle indagini non sono idonei a sostenere l'accusa.
 - l'autore del reato è ignoto.
 - il reato è estinto.
 - il fatto non è previsto dalla legge come reato.
 - il fatto sia particolarmente debole.
- la parte offesa può presentare una richiesta motivata di opposizione al GIP.

Rinvio a giudizio

- con questo atto il P.M. esercita l'azione penale.
- avviso all'indagato della conclusione delle indagini preliminari (415bis cpp).
- il P.M. indica il capo di imputazione all'indagato.

Citazione diretta a giudizio

- Esercitato dal P.M. quando si tratta di :
 - delitti con pena reclusione non superiore a 4 anni.
 - violenza minaccia o resistenza a pubblico ufficiale.
 - oltraggio ad un magistrato in udienza aggravato.
 - violazione dei sigilli da parte del custode.
 - rissa aggravata senza gravi lesioni.
 - lesioni personali stradali.
 - furto aggravato.
 - ricettazione.

Udienza Preliminare

- passaggio d fase procedimentale a processuale.
- l'indagato diventa imputato.
- il GIP viene sostituito dal GUP.
- l'imputato può richiedere al giudice di:
 - essere prosciolto .
 - rinunciare alla fase dibattimentale.

Fase dibattimentale

- Fase centrale del processo penale, si raccolgono e acquisiscono prove nel rispetto del contraddittorio delle parti
 - **Documentali**: scritti o altri documenti che rappresentano fatti, persone o cose attraverso foto, prove audiovisive.
 - **Esame testimoniale**: deposizione di un soggetto, sottoposto a giuramento, su fatti relativi al processo.
 - **La perizia**: si ricorre quando è necessario svolgere indagini o acquisire elementi o valutazioni che richiedono determinate competenze di tipo tecnico scientifico o artistico.

Sentenza

- proscioglimento:
 - Sentenza di non doversi procedere: manca una delle condizioni di procedibilità o sussista una causa estintiva del reato.
 - Assoluzione: il fatto non sussiste , l' imputato non lo ha commesso, il fatto non costituisce reato o è commesso da una persona non imputabile o punibile per altre ragioni, inoltre il giudice adotta sentenza di assoluzione quando sono insufficienti per la prova di colpevolezza dell'imputato.
 - Condanna: pronunciata quando l'imputato risulta colpevole del reato.

Procedimento Ordinario

Fase introduttiva: iscrizione a ruolo

- l'attore (instaura un giudizio) tramite l'avvocato espone i fatti che vengono posti a giudizio.
 - l'atto di citazione viene notificato alla controparte: il convenuto.

Fase istruttoria:

- vengono acquisite le prove dalle parti, tipicamente:
 - Testimoniali.
 - Consulenze tecniche di parte (C.T.P).
- il giudice può nominare il C.T.U.

Fase conclusiva:

- le parti devono chiarire definitivamente le proprie richieste, anche alla luce di quanto emerso nel corso del procedimento.

Fase decisoria:

- il giudice ha tutti gli elementi per pronunciarsi sulla controversia e può emettere la sentenza.

Procedimento con ricorso

Fase introduttiva

- il Ricorrente (che instaura il giudizio) tramite l'avvocato espone i fatti che vengono posti a giudizio direttamente al giudice.
- successivamente il giudice emette un decreto di fissazione dell'udienza.
- il ricorrente notifica l'udienza alla controparte: il resistente.
- le parti devono già esporre tutte le proprie difese e formulare le istanze istruttorie (rende più veloce il processo).

Fase conclusiva:

- le parti devono chiarire definitivamente le proprie richieste, anche alla luce di quanto emerso nel corso del procedimento.

Fase decisoria:

- il giudice ha tutti gli elementi per pronunciarsi sulla controversia e può emettere la sentenza

2.2- Reati informatici e normative

Definizione di reato informatico

- la definizione si è evoluta nel tempo
 - illecito che richiede conoscenze di informatica per la sua realizzazione.
 - illecito che comporta il coinvolgimento di un qualunque tipo di elaboratore.
 - illecito nel quale il computer interviene come strumento o come oggetto.
- essendo troppo ampie non riescono a definire bene il concetto.
- a livello internazionale si è rinunciato a dare una vera e propria definizione.
- si è preferito definire delle etichette di comportamenti collegati ai reati informatici.

1989 - Consiglio d' Europa NR (89) 9

Vengono elaborate 2 liste di abusi

Lista minima

- Condotte criminose che gli stati devono reprimere mediante sanzione penale
 - frode informatica.
 - falsi documenti informatici.
 - danneggiamento di dati e programmi.
 - sabotaggio informatico.
 - accesso non autorizzato ad un sistema informatico.
 - intercettazione illecita di comunicazioni informatiche.
 - riproduzione illecita di un programma protetto.
 - riproduzione illecita della topografia di un prodotto a semiconduttori.

Lista facoltativa

- Comportamenti ritenuti non eccessivamente offensivi, la repressione è a discrezione degli stati.
 - alterazione di dati o programmi (senza danni).
 - spionaggio informatico.
 - utilizzo illecito di un elaboratore.
 - utilizzo non autorizzato di un programma informatico.

Legge n 547 23-12-1993

- l'Italia recepisce le direttive del consiglio d'Europa nel 1989, introducendo nel codice penale di diverse figure di reato informatico:
 - collocazione in prossimità di figure di reato già esistenti, che sarebbero applicabili se il fatto non fosse commesso sfruttando la tecnologia informatica.

art. 392 c.p.

Esercizio arbitrario delle proprie ragioni con violenza sulle cose

- chiunque al fine di esercitare un preteso diritto, si porge in modo violento. Multe fino a 516 euro.
- diventa penale se la violenza porta al danneggiamento o alla trasformazione della cosa o ne è mutata la destinazione.
 - su sistemi informatici, un certo programma viene alterato modificato, cancellato in tutto o in parte o viene turbato il funzionamento.

art. 420 c.p.

Attentato a impianti di pubblica utilità

- Chiunque danneggi direttamente o distrugge impianti di pubblica utilità è punito, salvo reato aggravato, ad una reclusione da uno a 4 anni.

legge n.48 del 18-03-2008

- il reato ha la stessa validità su sistemi informatici di ente pubblico, ovvero file o programmi con dati in esso contenuti.
- nel caso si derivi una distruzione o un danneggiamento del sistema stesso, ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema, la pena è la reclusione da 3 a 8 anni.

art. 491 - bis c.p.

Documenti informatici

- se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente agli atti pubblici e le scritture private.

- come documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati ad elaborarli.

art. 615 - ter c.p.

Accesso abusivo a 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, punito con una reclusione fino a 3 anni.
- la pena è da uno a 5 anni
 1. il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso di poteri o violazione dei doveri inerenti alla funzione o al servizio, o da un un investigatore privato , abusando dei propri poteri.
 2. il colpevole usa la violenza su cose o persone, ovvero se palesemente armato.
 3. se dal fatto deriva la distruzione o il danneggiamento del sistema o l' interruzione totale o parziale del suo funzionamento, la distruzione o danneggiamento dei dati, informazioni o dei programmi in esso contenuti.
- se i fatti dei comma primo e secondo riguardino sistemi informatici di interesse militare o relativi all' ordine all' ordine pubblico, della sanità o della protezione civile. la pena è rispettivamente della reclusione da uno a cinque anni e da 3 a 8 anni.
- nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa : negli altri casi si procede d' ufficio.

art. 615 - quater c.p.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o multimediali

- chiunque al fine di lucro o di arrecare danni al prossimo, diffonda chiavi di accesso o mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, è punito con la reclusione sino ad un anno e con multa fino a 5164 euro.
- la pena è a reclusione da 1 a 2 anni e una multa da 5164/10329 euro e rincorre a circostanze di cui numeri 1-2 del quarto comma del 617quater.

art. 615 - quinquies c.p.(*)

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico

- chiunque diffonda un programma da lui creato con lo scopo o effetto il danneggiamento di un sistema informatico o telematico, dei dati o programmi un esso contenuti o pertinenti. è punito con la reclusione sino a 2 anni e con la multa fino a 10329 euro.

art. 616 c.p.

Violazione sottrazione e soppressione di corrispondenza

- chiunque prende condizione del contenuto di una corrispondenza chiusa a lui non diretta, quindi sottrae allo scopo di prenderne o farne da altri prender condizione , di una corrispondenza chiusa o aperta a lui non diretta, ovvero in tutto o in parte la distrugge o sopprime, è punito da una reclusione fino ad un anno e una multa da 30 a 516 euro.
- se il colpevole senza giusta causa rivela in tutto o in parte il contenuto della corrispondenza è punito se dal fatto la situazione non peggiora da una reclusione fino a 3 anni [618].
- il delitto è punibile a querela della persona offesa.
- agli effetti delle disposizioni di questa sezione la corrispondenza s'intende quella epistolare telegrafica o telefonica informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.

art. 617 - quater c.p.

intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

- chiunque fraudolentemente intercetta comunicazioni a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, punito con la reclusione da 6 mesi a 4 anni.
- salvo un grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo d' info al pubblico in tutto o in parte, il contenuto delle comunicazioni di cui primo comma.
- i delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
- si procede da reclusione d' ufficio e la pena è reclusione da uno a 5 anni se il fatto è commesso:

1. il danno è ad un sistema utilizzato dallo stato o altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità.
2. da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema.
3. da chi esercita anche abusivamente la professione di un investigatore privato.

art. 617 - quinquies c.p.

Installazione di attrezzature atte a intercettare impedire o interrompere comunicazioni informatiche o telematiche

- chiunque fuori dai casi consentiti, installa apparecchiature atte ad intercettare impedire o interrompere comunicazioni informatiche o telematiche, è punito con reclusione da 1 a 4 anni.
- la pena è da 1 a 5 anni secondo i casi del quarto comma dell' articolo 617-quater.

art. 617 - sexies c.p.

#Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche

- chiunque per procurare vantaggio o danno, forma falsamente o altera o sopprime in tutto o in parte, il contenuto anche occasionalmente intercettato di un sistema informatico o telematico, è punito qualora ne faccia uso o lasci ad altri l' utilizzo, da una pena da 1 a 4 anni.
- la pena è da 1 a 5 anni nei casi previsti dall' art. 617-quater.
- nel caso previsto dal primo comma il delitto è punibile a querela dalla persona offesa.

art. 621 c.p.

Rivelazione del contenuto di documenti segreti

- chiunque in possesso di contenuti che debbano rimanere segreti di cui atti o documenti li si rivelino a scopo di lucro proprio o altrui, è punito se dal fatto ne deriva documento con reclusione fino a 3 anni o con multa da 103 euro a 1032 euro.
- agli effetti della disposizione di cui promo comma è considerato documento anche qualunque supporto informatico contenente dati.

- punibile a querela della persona offesa.

art. 623 - bis c.p.

altre comunicazioni e conversazioni

- le disposizioni contenute nella seguente sezione relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni immagini o altri dati.

art. 635 - bis c.p.

danneggiamento di sistemi informatici e telematici

- chiunque distrugge deteriora o rende in tutto o in parte inservibili sistemi informatici o telematici altrui , è punito salvo che il fatto costituisca più grave reato da una reclusione da 6 mesi a 3 anni.
- se si ricorre a una o più circostanze del secondo comma dell' articolo 635, la pena è la reclusione da 1 a 4 anni.

art. 640 - ter c.p.

Frode informatica

- chiunque alterando il funzionamento di un sistema informatico intervenendo senza diritto con qualsiasi modalità di dati, procura a se o altri ingiusto profitto o altrui danno, è punito con la reclusione da 6 mesi a 3 anni e multa da 541 euro a 1032 euro.
- reclusione da 1 a 5 anni e multa da 600 a 3000 euro se si ricorre a una delle circostanze del numero 1. del secondo comma dell' articolo 640.
- il delitto è punibile a querela della persona offesa salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

art. 266 - bis c.p.p.

intercettazioni di comunicazioni informatiche o telematiche

1. nei procedimenti relativi ai reati nell' articolo 266, commessi mediante l' impiego di tecnologie informatiche o telematiche, è consentita l' intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi.

art. 268 - bis c.p.p.

esecuzione delle operazioni

0. 3-bis: quando si procede a intercettazioni di comunicazioni il pubblico ministero può disporre che le operazioni siano compiute mediante impianti appartenenti a privati.
1. i difensori delle parti mediante avviso , entro il termine fissato a norma dei commi 4 e 5 hanno facoltà di esaminare gli atti e ascoltare le registrazioni. scaduto il termine il giudice dispone l' acquisizione delle conversazioni o dei flussi di comunicazioni, procedendo anche d'ufficio allo stralcio delle informazioni e dei verbali di cui è vietata l' utilizzazione. PM e difensori hanno diritto di partecipare allo stralcio e sono avvisati almeno 24 ore prima.
2. il giudice dispone la trascrizione integrale delle registrazioni osservando le forme i modi e le garanzie previsti per l' espletamento delle perizie. sono inseriti nel fascicolo per il dibattimento.
3. i difensori possono estrarre una copia delle trascrizioni e far eseguire la trasposizione delle registrazioni su nastro magnetico. in caso di intercettazione dei flussi, i difensori possono chiedere copia di supporto idoneo dei flussi intercettati, ovvero la copia di stampa previsto dal comma 7.

2001 - Consiglio di Europa (Budapest)

- primo trattato internazionale sulle infrazioni penali commesse via internet e su reti informatiche.
 - violazione diritti d' autore.
 - frode informatica.
 - pornografia minorile.
 - violazioni della sicurezza di rete.
- vi sono una serie di misure e procedure adeguate, come la perquisizione dei sistemi e reti informatiche e intercettazione dei dati.
- l'obiettivo principale è perseguire una politica penale comune per i reati informatici, promuovendo una cooperazione globale a riguardo.

Legge n. 48 del 18-03-2008

- l' Italia recepisce le direttive del consiglio d' Europa del 2001
 - danneggiamento informatico
 - distinzione tra danneggiamento dell' integrità dei dati e il danneggiamento dell' integrità del sistema.

- differenziazione a seconda che l' oggetto della tutela abbia o meno rilevanza a fini pubblici.
- ridefinizione di documento informatico.
- gestione della scena del crimine informatica.

art. 491 - bis c.p.

Documenti informatici

- se alcuna della falsità previste riguarda un documento informatico pubblico avente efficacia probatoria si applicano disposizioni concernenti agli atti pubblici.

art. 495 - bis c.p.

Falsa dichiarazione o attestazione al certificatore di firma elettronica su 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. 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 o si mette a disposizione di altri apparecchiature, programmi o programmi informatici , è punito con la reclusione fino a 2 anni e con la multa fino a 10.329 euro.

art. 635 - bis c.p.

Danneggiamento di informazioni, dati e programmi informatici

- Salvo grande reato chiunque danneggi informazioni dati o programmi informatici altrui è punito a querela della persona offesa, con reclusione da 6 mesi a 3 anni.
- Se ricorre la circostanza di cui numero 1) del secondo comma dell' articolo 635 quindi che se il fatto è commesso con abuso della qualità dell' operatore di sistema, la pena è da 1 a 4 anni e si procede d'ufficio.

art. 635 - ter c.p.

Danneggiamento di info, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità

- salvo che il fatto costituisca più grave reato, chiunque danneggi un sistema informatico dello stato o da altro ente pubblico o ad essi pertinenti, la pena è la reclusione da 1 a 4 anni.
- se dall'atto si danneggia un sistema informatico di pubblica utilità è la reclusione da 3 a 8 anni.
- se ricorre la circostanza di cui al numero 1) del secondo comma dell' articolo 635 ovvero che il fatto sia compiuto con abuso della qualità di operatore del sistema, la pena è aumentata.

art. 635 - quater c.p.

Danneggiamento di sistemi informatici o telematici

- salvo grave reato , chiunque con le condotte dell' articolo 635-bis, attraverso la trasmissione di dati, etc...etc... atti a danneggiare sistemi informatici o telematici altrui è punito con la reclusione da 1 a 5 anni.
- se ricorre la circostanza di cui al numero 1) del secondo comma dell' articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

art. 635 - quinquies c.p.

danneggiamento di sistemi informatici o telematici di pubblica utilità

- se il fatto del 635-quater è diretto distruggere danneggiare o rendere inutilizzabili sistemi di pubblica utilità o ad ostacolarne il funzionamento, la pena è la reclusione da 1 lo 4 anni.
- se il fatto deriva danneggiamento del sistema informatico di pubblica utilità la pena è la reclusione da 3 a 8 anni.
- se ricorre la circostanza di cui al numero 1) del secondo comma dell' articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

art. 640 - quinquies c.p.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

- se il soggetto che presta servizi di certificazione di firma elettronica a scopo di lucro provocando danno altrui, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito da una reclusione fino a 3 anni e multa da 51 a 1032 euro.

art. 420 c.p.

attentato ad impianti di pubblica utilità

- chiunque commette un fatto che danneggia o distrugge impianti di pubblica utilità è punito salvo grave reato, con la reclusione da 1 a 4 anni.

art. 244 c.p.p.

casi e forme di ispezioni

1. delle persone, luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.
2. se il reato non ha lasciato tracce o effetti materiali o se sono scomparsi o sono stati cancellati o dispersi, l'autorità giudiziaria descrive curando anche di trovare il modo, tempo e cause delle eventuali modifiche, può disporre rilievi segnaletici descrittivi e fotografici e ogni altra operazione tecnica, anche relativamente a sistemi informatici, adottando misure tecniche necessarie ad assumere la conservazione dei dati originali e impedirne l'alterazione.

art. 247 c.p.p.

casi e forme delle perquisizioni

1. quando è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. quando è ritenuto che si trovi tali cose si trovino in un luogo determinato ovvero che si possa eseguire l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.
 - bis: quando è formato il motivo che i dati informatici o tracce pertinenti del reato si trovino in un sistema informatico, protetto da misure di sicurezza ne è disposta la perquisizione adottando metodi per non alterare il prodotto.

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

art. 248 c.p.p.

richiesta di consegna

1. se attraverso la perquisizione si cerca una cosa determinata, l'autorità giudiziaria può richiedere una consegna. se è presentata non vi è perquisizione salvo che si ritenga necessario.
2. per rintracciare cose a sequestro o per accettarne altre circostanze utili alle indagini, l'autorità giudiziaria o gli ufficiali di polizia giudiziaria da questa delegati possono analizzare sistemi informatici, in caso di rifiuto, vi è perquisizione.

art. 254 c.p.p.

Sequestro di corrispondenza

1. presso coloro che offrono servizi postali e simili è consentito procedere al sequestro di lettere pacchi valori telegrammi e altri oggetti di corrispondenza. anche se inoltrati tramite strumenti telematici che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o da lui diretti anche sotto nome diverso o per mezzo di persona diversa o che comunque possono avere relazioni di reato.
2. quando al sequestro procede un ufficiale di polizia giudiziaria, questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati senza aprirli o alterarli e senza prendere conoscenza del loro contenuto.
3. le carte e i documenti che non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati.

art. 254 - bis c.p.p.

Sequestro di dati informatici presso fornitori di servizi informatici telematici e di telecomunicazioni.

1. l'autorità giudiziaria quando dispone il sequestro dei dati informatici può stabilire per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su supporto adeguato, con procedura che assicuri la conformità dei dati a quelli immutabili. in questo

caso è comunque ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.

art. 256 c.p.p.

dovere di esibizione e segreti

1. le persone indicate negli articoli 200 e 201 devono consegnare immediatamente all' autorità giudiziaria che ne faccia richiesta gli atti e documenti nonché i dati le info e i programmi informatici anche mediante copia di essi su adeguato supporto salvo che dichiarino per iscritto che si tratti di segreto di Stato ovvero di segreto inerente al loro ufficio o professione.

art. 259 c.p.p.

Custodia delle cose sequestrate

1. le cose sequestrate sono affidate in custodia alla cancelleria o alla segreteria. quando non possibile o non opportuno, l' autorità giudiziaria dispone che la custodia avvenga in luogo diverso, determinandone il modo e nominando un un altro custode, idoneo a norma dell' articolo 120.
2. all' atto della consegna, il custode è avvertito dell' obbligo di conservare e di presentare le cose a ogni richiesta dell'autorità giudiziaria nonché delle pene previste dalla legge penale per chi trasgredisce i doveri di custodia. quando riguarda info e programmi informatici, il custode è avvertito dell' obbligo di impedirne l' alterazione o l' accesso da parte di terzi salva diverse disposizioni. può essere imposta una cauzione. dell' avvenuta consegna dell' avvertimento dato e della cauzione imposta è fatta menzione nel verbale. è ricevuta con separato verbale nella cancelleria o segreteria.

art. 260 c.p.p.

apposizione dei sigilli alle cose sequestrate deperibili e distruzione di cose sequestrate.

1. le cose sequestrate si assicurano col sigillo dell' ufficio giudiziario e con le sottoscrizioni dell' autorità giudiziaria e dell' ausiliario che la assiste. (anche di carattere informatico).
2. l' autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria di originali dei documenti, disponendo, quando alle cose, in conformità dell'

articolo 259. quando sono dati informatici la copia deve essere realizzata su supporti adeguati , mediante procedure che garantiscono la conformità della copia originale e la sua immodificabilità , può essere disposta in questi casi anche in luoghi diversi dalla cancelleria o dalla segreteria.

art. 352 c.p.p.

1. bis : nella flagranza del reato, ovvero nei casi di cui comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure adeguate , procedono alla perquisizione di sistemi informatici o telematici protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati informatici o tracce che possano essere cancellati o dispersi.

art. 353 c.p.p.

acquisizione plichi o di corrispondenza

1. quando vi è necessità di acquisire plichi sigillati o chiusi, l' ufficiale di polizia giudiziaria li trasmette intatti al pubblico ministero per l' eventuale sequestro.
2. se vi sono rischi di perdere il plico, l' ufficiale di polizia rende più celeri i controlli disponendo un apertura immediata.
3. si intende anche di plichi o documenti in forma elettronica per i quali è consentito il sequestro a norma dell' articolo 254, gli ufficiali di polizia giudiziaria, in caso di urgenza ordinano a chi è preposto al servizio postale, telematico telematico o di telecomunicazione di sospendere l' inoltrato. se entro 48 ore dall' ordine di polizia giudiziaria il pubblico ministero non dispone il sequestro, gli oggetti di corrispondenza sono inoltrati.

art. 354 c.p.p.

Accertamenti urgenti sui luoghi sulle cose e persone. sequestro

1. gli ufficiali di polizia giudiziaria curano le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga multato prima dell' intervento del pubblico ministero.
2. se vi è pericolo di alterazione o dispersione o si modifichino e il pubblico ministero non può intervenire tempestivamente. gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. in relazione ai sistemi informatici gli ufficiali di polizia giudiziaria adottano le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l' alterazione e l' accesso e provvedono ove

possibile alla loro immediata duplicazione su supporti adeguati mediante procedure che assicurino la conformità della copia originale e immodificabilità.

Ransomware

- nel caso si utilizzino ransomware, ovvero metodi che cifrano i dati cancellando perennemente gli originali proteggendoli con una chiave che si può dare solo sotto riscatto pena la cancellazione definitiva dei dati si incorrono ai seguenti reati:
 - accesso abusivo a sistema informatico.
 - danneggiamento di info dati e programmi informatici.
 - diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

2.3- Fasi del trattamento, identificazione e raccolta

La Computer forensics è l'insieme di metodologie scientificamente provate finalizzate alla ricostruzione di eventi ai fini probatori che coinvolgono direttamente o indirettamente un supporto digitale

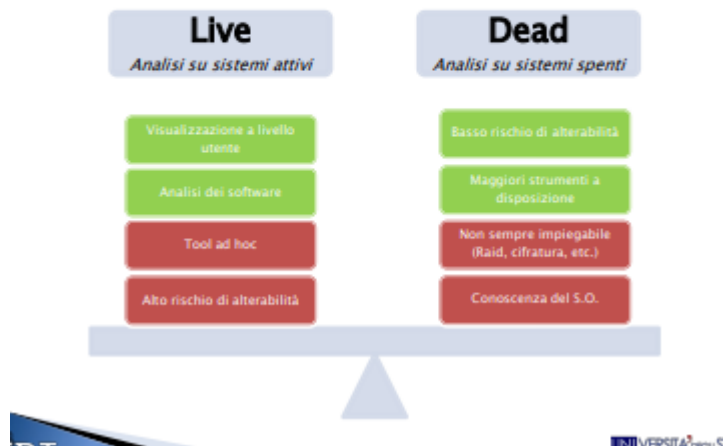
Identificazione

- ricerca della fonte di prova che può dare una svolta alle indagini, è volta ad individuare dove un dato è conservato..
- vanno identificati i seguenti dispositivi
 - computer / notebook.
 - cellulari e tablet.
 - memory card, pendrive, hdd esterni, cd/dvd.
 - fotocamere e videocamere.
 - server.
 - stampanti, fax, router.

[legge n48 del 18/03/2008 art. 247 cpp \(1bis\)](#)

Preview

Identificazione dell'evidence la «preview»



- consente di eseguire un'analisi di primo livello dei dispositivi allo scopo di trovare delle evidenze.
- si utilizzano *write blocker*.
- si rischia di alterare i contenuti con dispersione di una possibile prova.
- **Dead preview**
 - si esegue ad S.O. spento.
 - si usano write block: non altera il dispositivo analizzato.
 - hardware (si usano hardware specifici).
 - software: distro linux live.
 - PRO
 - non altera il dispositivo.
 - si possono usare diversi strumenti per l'analisi.
 - CONTRO
 - si deve conoscere bene il sistema e i software da analizzare.
 - non è sempre praticabile: sistemi embedded.
- **Live preview**
 - Si esegue ad S.O. acceso.
 - va documentata e verbalizzata.
 - PRO
 - si ha una visione d'ambiente su cui opera l'utente.
 - è veloce nell'analisi di software analizzati.
 - CONTRO
 - si altera il reperto.
 - gli strumenti sono adeguati al sistema.

Cambiamento di stato del dispositivo

Acceso → Spento

Spento → Acceso

- **Shutdown**

- Vanno valutate le seguenti criticità

- cifratura.
 - software in esecuzione.
 - Dump della RAM.

- **Metodi di shutdown**

- Scollegarlo dalla rete elettrica (unplug).
 - potrebbe compromettere il funzionamento del sistema.
 - Spegnimento tramite S.O.
 - Vengono eseguite su disco diverse operazioni (Aggiornamenti).

- **Accensione**

- vanno valutate se le informazioni che perderemo sono meno importanti dell' urgenza dell' accertamento
 - ultimo accesso al sistema.
 - esecuzione su disco di diverse operazioni.

Raccolta

Sequestro

- Dopo aver identificato i dispositivi o dati di interesse investigativo si procede al sequestro, di tipo
 - **Fisico:** Prendere fisicamente il supporto di interesse.
 - Si prende il supporto contenente i dati , posticipando le problematiche derivanti dall' acquisizione del dato.
 - Preoccuparsi solo di identificare e verbalizzare i reperti
 - catena di custodia.
 - Non è sempre fattibile
 - su sistemi che non possono essere fermati/spenti.
 - sistemi distribuiti su decine di rack.
 - **Logico:** si esegue una copia totale o parziale della memoria.
 - si esegue una copia forense.
 - si ha una garanzia di ripetibilità dei successivi accertamenti che verranno eseguiti sulla copia forense.

Catena di custodia

- Uno o più documenti in cui devono essere riportate tutte le info sul dispositivo che è stato sottoposto a sequestro
 - Luogo data e operatore che ha reperito e collezionato la fonte della prova.
 - Luogo data e operatore che ha gestito e/o esaminato la fonte di prova.
 - chi ha la responsabilità della custodia delle digital evidences.
 - metodo di conservazione del reperto.
 - eventuali trasferimenti di location dell' evidenza.

Copia forense

- Copia fisica
 - Copia bit a bit dell' intero supporto di memoria: dati di qualsiasi info sulla gestione dei dati.
- Clonazione: si ottiene un supporto pressoché identico all' originale
 - facilmente alterabile e si usa solo in casi particolari e va inserito nel proprio habitat per analizzarlo.
- La generazione di un file immagine ha come risultato un file rappresentabile il supporto originale
 - maneggevole.
 - può essere usato per creare un disco clone.

Copia Forense *gli strumenti*

- ▶ **Hardware:** duplicatori forensi
 - Certificati
 - Prestanti
 - Costosi
- ▶ **Software:** distro linux live forensi
 - Gratuiti
 - OpenSource
 - Versatili

Hash

- l' algoritmo restituisce una stringa di lunghezza fissa in esadecimali a partire da un flusso di dati di dimensione qualsiasi
 - la stringa è univoca per ogni file e ne è l' identificatore.
 - l'algoritmo non è invertibile, quindi non è possibile ricostruire il dato originale a partire dall' output.

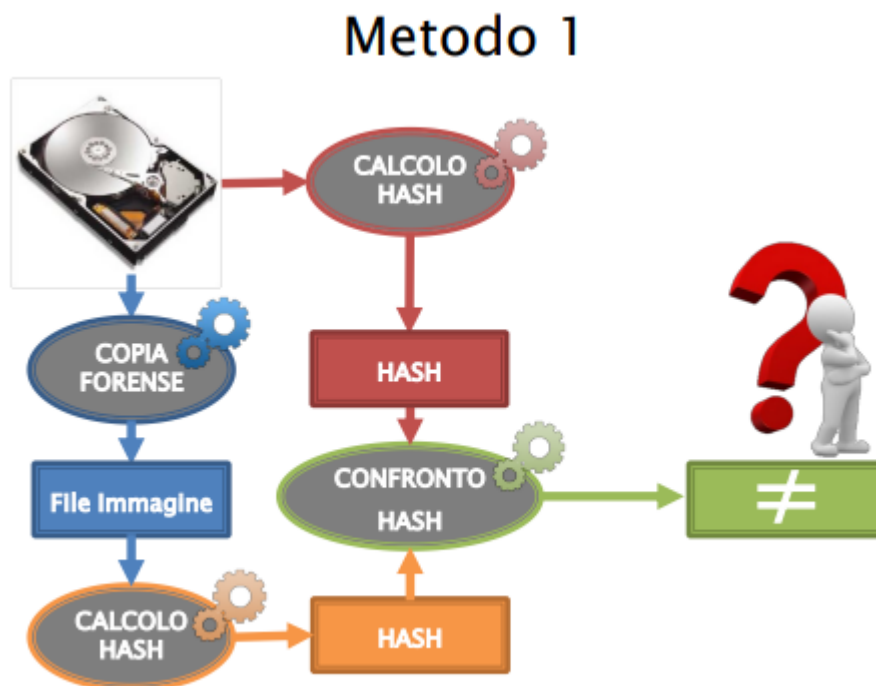
va ricordata la differenza tra accertamenti ripetibili ([359c.p.p.](#)) e irripetibili ([360c.p.p.](#)), il secondo tipo va compiuto:

- su memorie di massa non in buono stato.
- Live Acquisition: il sistema operativo del dispositivo va avviato per realizzare la copia forense.
- cloud.
- dispositivo di origine non disponibile nel tempo.
- Log file
 - file descrittivo con info sulla copia forense
 - strumenti impiegati: nome versione.
 - disco di origine: modello capacità S/N.
 - info dell' immagine forense: nr. di file, dimensioni.
 - altre info: data e ora, nr di settori saltati, etc.
 - **HASH:** MD5, SHA1, SH256, SHA512, etc.

Validazione

- Garantisce che la copia forense sia identica al dato originale.
- l'hash della copia forense coincide con l'hash del supporto originale.
- i dati della copia forense sono identici ai dati originali.

Evidence mutevole



Preservazione

- Garantisce che non vengano eseguite modifiche/alterazioni alla copia forense, se ciò avviene l'hash cambierà.

- l' hash della copia forense coincide con l' hash ricalcolato dalla medesima copia dopo la fase di analisi.
- i dati della copia forense varierebbe alla minima alterazione della copia forense.

Analisi

- Va eseguita su una copia.
- Riproducibilità.
- Stesso risultato ottenibile da diverse operazioni e strumenti di analisi.
- ricostruzione degli eventi passati mediante la lettura di dati digitali.

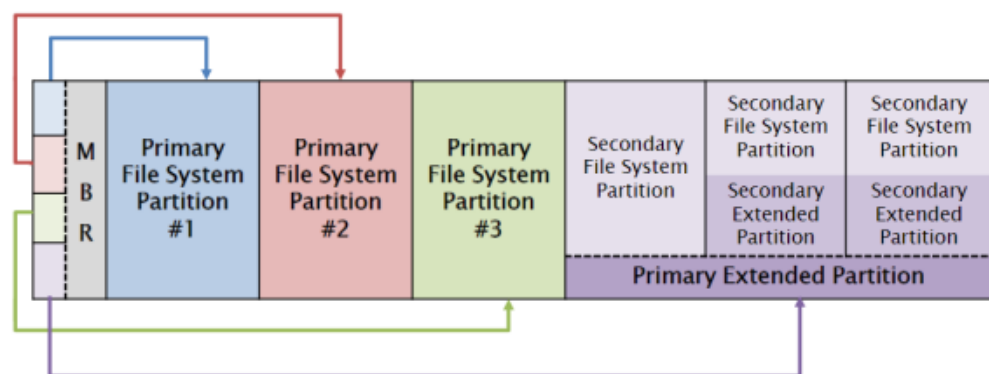


Volumi

- Volume system: gestisce i volumi per 2 obiettivi
 - unione di più volumi.
 - suddivisione del volume in partizioni.
- Volume: insieme di settori per memorizzare i dati.
- Partizione: insieme di settori consecutivi in un volume.
- indirizzamento dei settori
 - Physical address (LBA) : calcolato in base al primo settore del disco.
 - Logical disk Volume address: indirizzo del settore calcolato in base al primo settore del volume.
 - Logical volume partition address: l' indirizzo è calcolato in base al primo settore della partizione.
- **DOS partition**
 - è il sistema di partizione più comune.
 - MBR (Master boot record): primo settore
 - boot code.
 - partition table: max 4 entry
 - Starting CHS address.
 - Ending CHS address.

- Starting LBA address.
- number of sectors in a partition.
- type of partition.
- flags.
- signature : 0x55AA.
- Primary File system partition: contiene un file system.
- Primary extended partition: contiene altre partizioni.
 - Tabella della partizione.
 - Secondary file system partition
 - Tabella di partizione.
 - Secondary file system partition.
 - Secondary extended partition.
- il Boot code è situato nei primi 446byte del primo settore (MBR)
 - **Microsoft boot code**: processa la tabella di partizione e ricerca ed identifica quella c.d bootable tramite il Flag.
 - possibile incapsulamento di virus.
- il settore MBR viene allocato all'inizio del disk volume e di ogni extended partition.
 - EBR (extended boot record)
 - la parte riservata al boot code è inutilizzata.
 - la parte riservata alle altre 2 entry nella partition table è vuota.

ESEMPIO:



I volumi: DOS Partition

Partition Table: analisi



► File Immagine:

- Nr. 8 partizioni
- Dual Boot
- Architettura Little-Endian



► Strumenti:

- DD
- Editor Esadecimale (XDD)

- Apple partition Map
 - Apple partition (APM)
 - impiegato soprattutto dai vecchi sistemi basati su processori non Intel.
 - nessun limite massimo di partizioni.
 - gestisce volumi fino a 2TB.
 - partition map : secondo settore (512 byte)
 - ogni entry descrive una partizione.
 - la prima entry descrive la partition map.
- Guid partition table
 - Sistema di partizionamento utilizzato da Efi.
 - massimo 128 partizioni.
 - Volumi piu grandi di 2tb.
 - 5 aree/sezioni
 - protective MBR: Dos partition table (1^ settore).
 - GPT Header: definisce il layout delle aree.
 - Partition table: ogni entry descrive la partizione.
 - Partition area: locazione riservata alla partizione.
 - Backup area: copia di backup del GPT header e della partition table.

Relazione tecnica

- Base di partenza: quesito
- Descrizione degli strumenti Hardware e Software impiegati
- Descrizione delle azioni che hanno portato/non portato risultati
- **Scopo:** chiunque deve poter giungere alle medesime conclusioni

- Parte descrittiva :
 - dettagliata ed accurata.
 - Documentazione fotografica.
- Parte valutativa.
 - Motivazioni.
 - descrizione dell' iter logico.
 - Giuridicamente non è vincolante.
- Forma
 - Parte epigrafica.
 - Parte Descrittiva.
 - Parte Valutativa.
 - Parte Riassuntiva.
- Chiara ed intellegibile
 - impegno di grafici, illustrazioni, tabelle.

3- Comandi per la copia forense

Comando DD

è presente nella gran parte dei sistemi operativi UNIX like.

/dev

tutti i file al suo interno rappresentano dispositivi

- Character device : dispositivi di trasmissione e trasferimento
 - dsp[0]: dispositivo audio.
 - lp[0]: porta parallela.
- Block device : Dispositivi di memorizzazione e conservazione
 - hd[a]: hdd ide.
 - sd[a]: hdd scsi, memory stick, memory card, etc...

partiamo con un disco di destinazione:

```

Disk /dev/sdc: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x9a847d68

Device      Boot Start      End  Sectors  Size Id Type
/dev/sdc1           2048 16777215 16775168   8G  7 HPFS/NTFS/exFAT
  
```

Disco di
destinazione

il comando è il seguente:

```
dd if=/dev/sda of=/mnt/dest/dd_image/sda.dd bs=2048 conv=noerror, sync
```

Dove:

- **IF** = input file [sorgente /sda].
- **OF** = output file [file immagine sda.dd].
- **BS**= block size in byte, di default 512 [in questo caso 2048 byte].
- **CONV**= in base ai parametri
 - noerror= continua ad elaborare in caso di errore.
 - sync= sostituisce i blocchi non letti con NULS (sincronizza la dimensione della destinazione con la sorgente).
- Comandi avanzati
 - **SKIP**= [n] salta la lettura del n blocchi di memoria partendo dall' inizio.
 - **COUNT**= [n] l' elaborazione termina dopo aver letto n blocchi di memoria.
 - Di solito servono per acquisire una singola partizione o evitare

esempio di acquisizione di una sola partizione

```
dd if=/dev/sda of=/mnt/dest/dd_image/sda_p2.dd skip=2099199 count=6289408
```

```
$$\text{dd if=/dev/sda of=/mnt/dest/dd\_image/sda\_p2.dd} bs=1024  
skip=3000000 count=1000000}$$
```

Calcolare l'hash

- calcoliamo l' hash della sorgente sda e lo salviamo in un file sda_orig.hash.

```
md5sum /dev/sda > /mnt/dest/dd_image/sda_orig.hash  
cat /mnt/dest/dd_image/sda_origin.dd
```

- con lo stesso hash sda lo salviamo in un file sda_dd.hash.

```
md5sum /mnt/dest/dd_image/sda_orig.hash > /mnt/dest/dd_image/sda_dd.hash  
cat /mnt/dest/dd_image/sda_dd.hash
```

- Durante l' elaborazione di una copia.

```
dd if=/dev/sda bs=2048 | tee /mnt/dest/dd_image/sda.dd |  
md5sum < /mnt/dest/dd_image/sda.hash
```

- **TEE** = biforca/duplica lo stream (una si usa per il file immagine, l' altra vien trasmesso al comando successivo md5sum).

Comando DC3DD

Patch del comando DD

```
dc3dd if= /dev/sda of=/mnt/dest/dd_image/sda.000 ofsz=2G bufsz=2k hash=md5
```

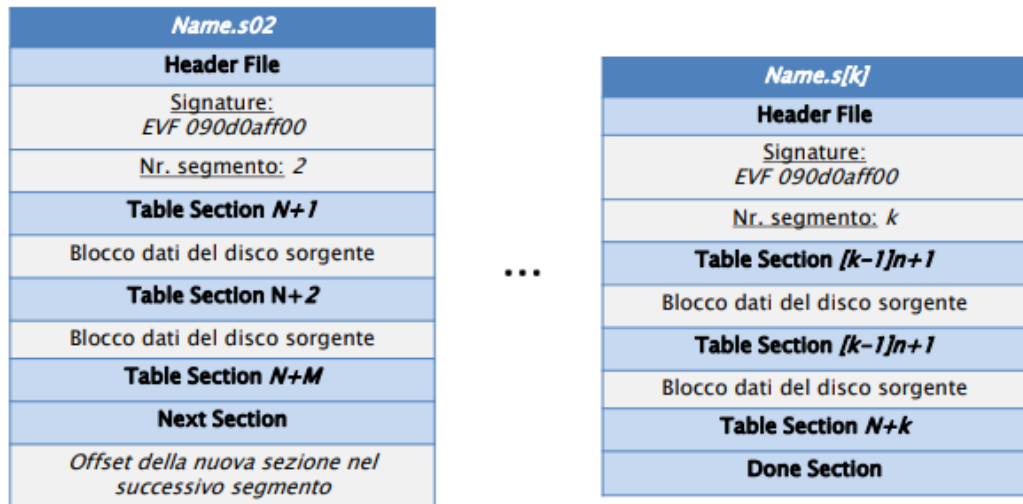
- **OFS**= output diviso in più file (in sda.000).
- **OFSZ**= dimensione massima dei file (2gb).
- **BUFSZ**= BS = blocksize in byte (512 default) (dimensione 2048byte).
- **HASH**= [MD5 | SHA1 | SHA256 | SHA512] calcola dell'[hash](#) indicato [**MD5** e **SHA256**].
- **LOG** = salva il report dell' elaborazione in un file [sda.log].
- **VERB**=ON indica di generare un report dettagliato (verbose).

4-Metodi per la copia forense

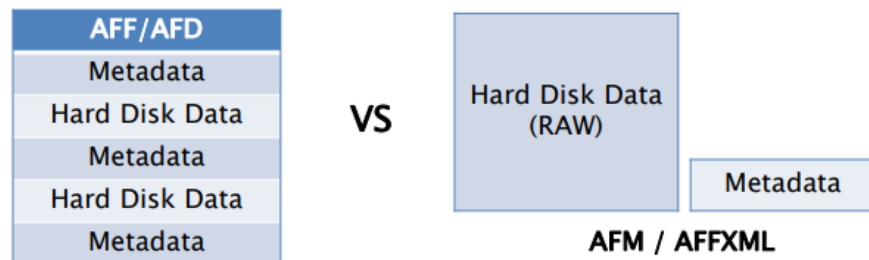
Disk image

- Supporti ottici
 - Formato ISO: più comune.
 - Formato .bin = Copia RAW.
 - Formato .cue = Metadati.
- Formato DD/RAW.
Formato semplice è un container dello stream
- Problematiche:
 - Non conserva metadati dell'evidence: modello, seriale dimensione, etc.
 - Non conserva hash calcolati.
 - Non esegue compressione.
 - Non può contenere più di un file/stream.
- Smart (EWF)
 - obiettivo: accesso veloce ad una parte dell' immagine.
 - Segmentazione: .s01 ; .s02 ; etc... etc...
 - ogni segmento è composto da:
 - headerfile: signature e numero di segmento.
 - una o più sezioni:
 - header section.
 - volume section.
 - table section.

- next/done sections.



- Encase L01 Logical (EWF)
 - acquisizione di file logici
 - segmentazione: .l01 ; l02 ; etcetc...
 - impiega 15 sezioni (+2 al formato E01)
 - Ltree section.
 - Ltypes section.
- Advanced Forensics format (AFF/AFF4)
 - ogni disco separato in 2 layer.
 - disk-rappresentation layer (metadato).
 - data-storage layer (dato).



Guymager



- ▶ Sviluppato da Guy Voncken
- ▶ Licenza: *Free OpenSource*
- ▶ Piattaforma: *O.S. Linux*
- ▶ Basato sulla libreria «libewf»

Clone

Disk Image

- Disk image
 - si sceglie il formato dell' immagine e la dimensione dei segmenti.
 - si inseriscono le informazioni di elaborazione.
 - il nome e destinazione del file immagine.
 - la scelta dell' HASH , il calcolo del dispositivo target dopo l' acquisizione e il calcolo del hash del file immagine.
 - durante l'elaborazione vengono visualizzate le statistiche sull' elaborazione e il riepilogo delle impostazioni , al termine viene visualizzata una spunta verde.
- è uno strumento per elaborare copie forensi.
- permette di scegliere tra i seguenti hash: MD5,SHA-1,SHA-256.
- esegue copie forensi solo di tipo "Full disk".

FTK imager



- ▶ Prodotto dalla AccessData
- ▶ Licenza: *Freeware*
- ▶ Piattaforma: *O.S. Microsoft Windows*

Lite Version

Install Version

- è uno strumento per elaborare copie forensi.

- può eseguire una copia della memoria volatile.
- File > Create disk image...
 - tipi di acquisizione
 - physical drive.
 - logical drive.
 - image file.
 - content of folder.
 - fenico device.

Physical Drive :

- Source drive selection: dispositivo a acquisire
 - Si sceglie il formato immagine.
 - Si inseriscono le informazioni del caso.
 - Definizione del file immagine
 - percorso e nome del file immagine.
 - dimensione dei segmenti dei file immagine.
 - livello di compressione del file immagine.
 - cifratura del file immagine.
 - **Add overflow location**: calcolo e verifica dell' [hash](#) del file immagine col dispositivo target e si decide se aggiungere ulteriore spazio di archiviazione per il file immagine (install version).
 - è possibile visionare il tempo rimanente l' elaborazione della copia forense.
 - è possibile generare un file CSV di tutti i file e cartelle presenti.
 - durante l'elaborazione:
 - dispositivo target.
 - file immagine.
 - indicazioni dello stato del processo.
 - info temporali sull' elaborazione.
 - vi è un processo di validazione del file immagine.
 - al termine dell' elaborazione si genera un file con le info riportate.

Apertura del file immagine.

- File > Add evidence item.

Logical Drive

- File > Create disk image.
- è possibile acquisire un supporto ottico.

Image file

- impiegato principalmente per convertire un file immagine da un formato ad un altro: Es.
E01 -> DD.

Contents of a Folder

- Acquisizione logica di file in una determinata cartella.

Custom Content image

- elaborazione di un immagine personalizzata
 - File -> add evidence item.
 - si visualizzano i file che sono stati selezionati.
 - wild card option
 - ? = qualunque carattere.
 - * = qualunque serie di caratteri.
 - | (pipe) = separatore di directory e file.
 - le distinzioni tra maiuscole e minuscole.
 - si può estendere la ricerca ricorsivamente alle sottocartelle.
 - la ricerca viene eseguita direttamente su tutte le evidence aggiunte e presenti nell' evidence tree.

dump memoria volatile

- File > Capture memory
 - percorso dove salvare il dump della memoria.
 - nome con il quale vogliamo salvare il dump.
 - si richiede di copiare anche il file di paging di windows.
 - il dump viene incapsulato in un file immagine AD1.

4.5-Analisi dei File system

File System

Dati Essenziali	Dati Non Essenziali
<ul style="list-style-type: none"> ▶ Dati che se modificati/alterati causano il malfunzionamento del sistema: • Indirizzamento del contenuto del file • Nome del File • Dimensione del file 	<ul style="list-style-type: none"> ▶ Informazioni accessorie • Dati temporali • Permessi utente
TRUSTED DATA	UNTRUSTED DATA

File system Category

- Solitamente posizionati nel primo settore.
- Essenziali: info sul layout dei dati.
- Analisi
 - info sulla generalizzazione del file system.
 - info sul layout.
 - controllo consistenza: Volume slack.
- Content category
 - Locazioni di memoria impiegate per la memorizzazione del contenuto dei file
 - Data unit: raggruppamento in più settori
 - stato: allocato e non.
 - logical file system address.
- Strategia del primo disponibile
 - si cerca una data unit libera ogni volta partendo dall' inizio.
- Prossimo disponibile
 - si cerca partendo dall' ultima locazione allocata.
- Più adatto
 - si cercano data unit libere in modo che possano contenere consecutivamente il file.

Analisi

- Data unit view: settori noti del file system.
- logical file system searching: ricerca di un contenuto specifico nei data unit.
- Data unit allocation status: ricerca nei data unit non referenziali in metadata category.
- Metadata category
 - descrivono i file presenti in content category
 - info temporali.
 - indirizzo delle data unit allocate per i file.
 - Analisi
 - ricerca di maggiori info su un file.
 - ricerca di file in base agli attributi descritti in questa categoria.
- **Logical file address :**
 - indirizzo di parte del file allocata nella data unit
 - è il contenuto nella data unit.
- **Slack space:**
 - parte non usata di una data unit allocata.
- **File recovery:**

- recupero dei file cancellati analizzando le entry in metadata category con lo stato non allocato.
- **Compressed file:**
 - memorizzare i dati in un formato compresso occupano meno data unit.
 - 3 livelli di compressione
 - soli dati all' interno del file.
 - di tutto il file.
 - eseguita nel file system : invisibile nel lato applicativo e utente.
- **File name category**
 - nome assegnato a ciascun file (indirizzo della struttura metadato).
- **File recovery**
 - recupero dei file cancellati ricercando i file name con lo stato non allocato
 - analisi della struttura metadati indirizzata.
- **Application category**
 - dati non essenziali al file system.
 - sono più efficienti se conservati nel file system.
 - spazio occupato, journaling.
 - **Journaling:**
 - conservazione delle modifiche effettuate e da effettuare sui metadati
 - evitare l' inconsistenza
 - completamento delle operazioni di modifica.
 - ripristino dei dati a prime delle modifiche (rollback).
 - Analisi
 - ricostruire eventi di un incidente recente.

FAT file system

FAT File System
File System Category

- ▶ **FSINFO (FAT32):** Reserved Area (BootSector)
 - Cluster liberi
 - Prossimo Cluster libero
- ▶ **Boot Sector:** primo settore (*Reserved Area*)
 - *Physical Layout (Essential Data):*
 - **Reserved Area:** settore 0
 - FAT12/16: Dimensione 1 Settore
 - FAT32: Dimensione variabile
 - **FAT Area:** dopo la «Reserved Area»
 - Dimensione: $\text{Size_FAT} \times \text{Nr_FAT}$
 - **Data Area:** dopo la «FAT Area»
 - Dimensione: $\text{tot_settori} - \text{Inizio Area}$
 - Dimensione Cluster
 - Root directory (FAT32)
 - Dimensione (FAT12/16)

FAT File System
File System Category

- ▶ **Boot Sector:** primo settore (*Reserved Area*)
 - *NON Essential Data:*
 - OEM Name: info strumento creazione del FS
 - Volume Serial Number: data di creazione (Microsoft)
 - File System Label: FAT, FAT12, FAT16, FAT32

- Analisi
 - Recuperare info sul layout.
 - Controllare possibili dati nascosti
 - bootcode.
 - settori in reserved areas

- FSINFO.
 - confronto tra boot sector ed il backup del boot sector.
- **Content category**
 - contenuto di file e directory.
 - Cluster: 2^x settori (max 32k)
 - primo: indirizzo 2.
 - solo in data area.
- **FAT**
 - identificare lo stato di allocazione dei cluster.
 - successivo cluster: cluster chain.
 - layout: boot sector.
 - entry di ugual dimensione: FAT12: 12 bit, FAT16, FAT32.
 - entry = cluster.
 - cluster non allocato: zero.
 - cluster allocato
 - prossimo.
 - eof.
 - cluster danneggiato.
- Indirizzamento
 - la prima entry è l' indirizzo 0.
 - indirizzo entry = indirizzo cluster.
 - 0 =info dei media.
 - 1= dirty status.
- **Metadata category**
 - info su file e directory
 - indirizzo del primo cluster.
 - parent directory
 - directory entry: 32k
 - file.
 - directory.
 - posizionata nella data area (cluster)
 - file name category.
 - nome file (8 chars) + estensione (3 chars).
 - > long file name directory.
 - info temporali (non essential)
 - data creazione (win).
 - nuovo file/copia => nuova data.
 - spostato/rinomino => copia data.
 - Data modifica (Win) : modifica del contenuto.

- Data accesso (Win): modifica anche visualizzando le proprietà.
- Mappare le strutture (metadata) con etichetta
 - filename.
- Directory entry: insieme ai metadata category
 - filename 11 chars.
 - long file name directory entry: +13 chars.

NT File system

NT File System

► New Technologies File System (NTFS)

- Microsoft 1993

► Ogni cosa è un file:

- **\$MFT**: Master File Table
- **\$MFTMirr**: backup della MFT
- **\$Boot**: boot sector
- **\$Volume**: informazioni del volume
- **\$Bitmap**: stato di allocazione dei cluster
- **\$AttrDef**: definizione degli attributi
- **\$BadClus**: elenco dei cluster danneggiati
- **\$Secure**: descrittore di sicurezza
- **\$130**: Index
- ...



• \$MFT

- Ogni file/directory ha almeno una entry (file record).
- 1024 byte (boot sector).
- entry [0] : \$MFT.
- Starter cluster (boot sector).

• Entry

- dim= 1024 byte.
 - header : 42 byte.
 - attributi: strutture dati.
- signature; <\File> / <\Baad>.
- Stato di allocazione: Attributo \$Bitmap nella entry [0] \$MFT.
- indirizzo sequenziale 48 bit (file number).
- numero sequenziale: 16 bit (contatore allocazione).

• File system metadata \$MFT file

- Contiene la master file table.
 - cluster iniziale : boot sector.

• Layout

- Win 7: cluster 786432.

- Entry[0] di MFT
 - \$DATA: cluster usati.
 - \$BITMAP: Stato di allocazione delle entry.
- File system metadata \$MFTMirr file
 - Backup della Master file table.
 - prime 4 entry: \$MFT, \$MFTMirr, \$LogFile, \$Volume.
 - Entry[1] di MFT.
 - layout
 - win 7 o superiore: dopo il boot sector (16 settore).
 - prima di win 7: a metà del file System.
- File system metadata \$Boot file
 - Boot sector
 - Dimensione dei cluster.
 - nr.settori del file system.
 - layout MFT
 - cluster iniziale.
 - dimensione entry.
 - Entry[7] di MFT.
 - Layout : primi 16 settori del file system
 - Signature : 0xAA55.
- File system metadata \$Volume File
 - Info sul volume
 - etichetta.
 - versione.
 - Entry [3] di MFT
 - \$Volume_name: nome in unicode del volume
 - id type: 96.
 - \$Volume_information:
 - versione di ntfs.
 - Dirty status.
 - \$DATA: 0 byte.
- ANALISI:
 - processare il primo settore del file system: Boot sector
 - Layout MFT.
 - Processare la MFT[0]
 - \$MFTMirr.
 - Processare \$volume.
 - Processare \$Attref.
 - processare le altre entry MFT.

- Content category
 - Contenuto degli attributi
 - residenti.
 - non residenti: Cluster esterni.
 - Cluster
 - Cluster[0] = settore[0] del file system
 - settore= Cluster x Settori_Cluster.
- File system metadata \$Bitmap File
 - Info sullo stato di allocazione del cluster
 - Bit[x] = Cluster[x].
 - 1= cluster x allocato.
 - 0= non allocato.
 - entry [6] MFT.
- File system metadata \$BadClus File
 - Traccia i cluster con settori danneggiati.
 - Entry[8] MFT
 - \$Data=\$bad.
 - flag=sparse.
 - size =file system .

NT File System

Content Category: Layout

- › **Diverso a seconda della versione NTFS**
- › **Zona MFT**
 - Settori consecutivi riservati per MFT:
 - 12,5% del File System
- › **Boot Sector:** primo settore
 - File System Metadata File dopo il Boot Sector

5-Crittografie

- Un protocollo o schema definisce le interazioni fra le parti per ottenere le proprietà di sicurezza desiderate.
- le parti sono le entità coinvolte nello schema.
- i protocolli si basano su una serie di protocolli più semplici detti primitive crittografiche
 - risolvono problemi facili.
 - possono essere usati per risolvere problemi più complessi.

le primitive crittografiche risolvono i seguenti problemi:

- CIFRATURA: cifrati simmetrici o asimmetrici o a chiave pubblica.
- Autenticazione ed integrità: funzioni hash e MAC.
- Firme digitali.
- Altro: generazione di numeri pseudo casuali, prove zero knowledge.
- Il cifrario simmetrico condivide la stessa chiave per la cifratura e la decifrazione
 - data encryption:
 - standard
 - des triplo, modalità di cifratura.
 - RC2, RC4, RC5, RC6.
 - Advanced encryption standard (AES).
 - Blowfish.
- Il cifrario asimmetrico impiega 2 chiavi differenti
 - una pubblica per la cifratura.
 - una privata per la decifrazione.
- La firma digitale consiste nell' apposizione di una firma ad un documento digitale
 - deve poter essere facilmente prodotta dal firmatario.
 - la firma è univoca , nessuno deve essere in grado di riprodurla
 - chiunque può facilmente verificarla.
 - Algoritmi
 - RSA.
 - Digital signature standard (DSS).

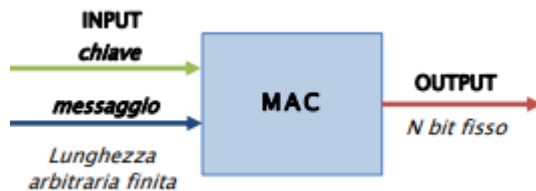
Funzione hash

il Valore hash è una rappresentazione non ambigua e non falsificabile del messaggio.

- impiego:
 - firma digitale.
 - integrità dei dati.
 - certificazione del tempo.
- Integrità:
 - ▶ Computo al **tempo T_0** il valore hash del **file M**: $H = h(M)$
 - ▶ Per controllare se il file è stato successivamente modificato:
 - al **tempo T_1** calcolo: $H' = h(M)$;
 - verifico se $H' = H$;

$h(M)$ è l'impronta digitale del file

- funzione message Authentication Code (MAC).



- impiego:
 - integrità dei dati.
 - autenticità dei dati: verificare il mittente.
- Proprietà di sicurezza
 - Confidenzialità: protezione da un soggetto estraneo.
 - Autenticazione: certezza di identificare l'interlocutore.
 - integrità: verificare che il messaggio non sia stato modificato durante la trasmissione.
 - solo chi è autorizzato può modificare l'attività di un sistema o le info trasmesse.
 - non-Ripudio: negare il disconoscimento del messaggio al mittente o al destinatario.
 - Anonimia: nascondere l'identità di chi ha compiuto un'azione nel contesto crittografico.

Proprietà di una funzione hash

- **One - way (pre-image resistant)**
 - dato un hash y , è computazionalmente difficile trovare M | $y=h(M)$.
- **Sicurezza debole (2nd pre image resistance)**
 - dato m è computazionalmente difficile trovare una variazione di M , M' | $h(M')$.
- **Sicurezza forte (Collision resistance)**
 - è computazionalmente difficile trovare 2 diversi messaggi con lo stesso valore hash.

Definizioni

- **One way Hash function (OWHF):**
 - verifica proprietà pre image e 2nd pre image resistance.
 - viene detta weak one-way hash function.
- **Collision resistant hash function (CRHF)**
 - verifica la proprietà di collision resistance.
 - viene detta strong one-way hash function.

Costruzione

Messaggi di lunghezza arbitraria sono trattati utilizzando hash con input fisso

- il messaggio viene diviso in k blocchi di lunghezza fissa.
- essi vengono trattati in modo seriale/iterato e parallelo.

MD4-MD5

md= Message Digest

Little-endian e Big-endian

Rappresentazione di parole da 32 bit

PAROLA W 32 bit			
B4	B3	B2	B1

▶ Little-endian

- il byte con indirizzo più basso è quello meno significativo
- valore parola: $W = 2^{24}B4 + 2^{16}B3 + 2^8B2 + 2^0B1$

▶ Big-endian

- il byte con indirizzo più basso è quello più significativo
- valore parola: $W = 2^0B4 + 2^8B3 + 2^{16}B2 + 2^{24}B1$

le operazioni sono efficienti su architetture 32 bit little-endian

- entrambe hanno come obiettivi:
 - una sicurezza forte.
 - una sicurezza diretta.
 - velocità di esecuzione.
 - semplicità e compattezza.
- Processano il messaggio in blocchi da 512 bit.
- i 2 metodi impiegano diverse operazioni sulle word in input x e y restituendo una nuova word:
- come funzione di compressione:
 - ogni round prende in input
 - blocco corrente di 512 bit = 16 word.
 - valore corrente del buffer, 4 word ABCD per 128 bit.
 - ogni round consiste in 16 operazioni.
 - [ABCD.k.s] [MD4]
 - [ABCD.k.s.i] [MD5]
 - l' output dell'ultima fase viene sommato all'input della prima fase
 - la somma avviene word a word

- l'output dell' L-esima frase è il digest a 128 bit

MD5/MD4: differenze

MD5	MD4
<ul style="list-style-type: none"> ▸ 4 round = 4 · 16 operazioni ▸ 4 funzioni logiche ▸ 64 costanti additive ▸ ogni passo aggiunge il risultato del passo precedente 	<ul style="list-style-type: none"> ▸ 3 round = 3 · 16 operazioni ▸ 3 funzioni logiche ▸ 2 costanti additive

SHA-1 vs MD4/MD5

- **Sicurezza forte**
 - maggiore in SHA-1, output 32 bit più lungo di MD4/5 (160 contro 128)
 - Attacco a compleanno 280 contro 264
- **Sicurezza contro l'analisi**
 - MD5 è soggetta ad alcuni attacchi
- **Velocità**
 - entrambi algoritmi molto veloci; SHA-1 ha più passi (80 contro 64) e il buffer ha 160 bit rispetto ai 128 bit di MD5
- **Semplicità e Compattezza**
 - semplice da descrivere e da implementare, nessun uso di tabelle e di complesse strutture dati

SHS-SHA-1, SHA-256, 512, 384

SHS= Secure Hash Standard

SHA= Secure Hash Algorithm

- operazioni efficienti su architetture a 32bit big-endian
- stessi principi di MD4/5 ma più sicuro

SHA processa blocchi da 512 bit (ogni blocco da 16 parole di 32 bit)

Espansione blocco ed iterazioni

- 4 round di 20 operazioni ciascuna (80)
- per ogni iterazione una parola $X[i]$ viene calcolata dal blocco input

Funzione Hash

SHA-256, SHA-512, SHA-384

- ▶ **Hash di SHA-1 è 160 bit**
 - Sicurezza contro attacco del compleanno 80 bit
- ▶ **Lunghezza chiavi AES: 128, 192, 256**
- ▶ **Proposti nuovi SHA (12 ottobre 2000)**
 - Lunghezza valore hash: 256, 512, 384 bit
 - Sicurezza attacco del compleanno 128, 256, 192 bit
- ▶ **Draft di Federal Information Processing Standard (FIPS), gennaio 2001**

SHA-256, SHA-512, SHA-384

Stessi principi di MD4, MD5, SHA-1

- ▶ **SHA-256**
 - Messaggio diviso in blocchi di 512 bit
 - Parole da 32 bit
- ▶ **SHA-512**
 - Messaggio diviso in blocchi di 1024 bit
 - Parole da 64 bit
- ▶ **SHA-384**
 - Valore hash = primi 384 bit di SHA-512, con costanti iniziali cambiate

6- Strumenti per l'Analisi

strumenti software

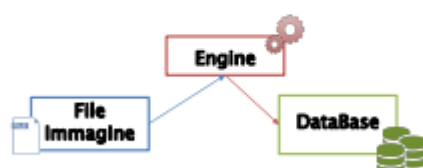
Toolkit	Tools Forensic Oriented	Tool Generici
▶ Supporto all'intera fase di analisi	▶ Esecuzione di un specifico task	▶ Non progettati per la C.F.
Es.: <ul style="list-style-type: none">• AccessData FTK• Autopsy• Encase Forensics• BlackLight• X-Ways Forensics• PassMark OS Forensics	Es.: <ul style="list-style-type: none">• Internet Evidence Finder• Amped Five• Log2Timeline	Es.: <ul style="list-style-type: none">• USBdeview• Diff-PDF• VMWare

Forensic ToolKit (FTK)

- ▶ Commerciale
- ▶ Microsoft Windows

Autopsy

- ▶ Free e OpenSource
- ▶ Multiplatforma



Multi-utente / Scalabile

Formati File Immagine

Forensic ToolKit (FTK)	Autopsy
<ul style="list-style-type: none">› Encase E01› Encase L01 Logical Image› Expert Witness› SnapBack› Safeback 2.0 and under› ICS› Linux DD› SMART› Ghost (forensic images only)› MSVHD (MS Virtual Hard Disk)› AccessData Logical Image (AD1)› Lx0, Lx01› DMG (Mac)› VMDK (VmWare Disk)	<ul style="list-style-type: none">› Encase E01› Raw (DD, BIN, IMG)› Virtual Disk (VMDK, VHD)

File System

Forensic ToolKit (FTK)	Autopsy
<ul style="list-style-type: none">› FAT› exFAT› NTFS› Ext2FS› Ext3FS› Ext4FS› APFS› HFS, HFS+› CDFS› ReiserFS 3› VxFS (Veritas File System)	<ul style="list-style-type: none">› FAT› ExFAT› NTFS› EXT2FS› EXT3FS› EXT4FS› APFS› HFS, HFS+› YAFFS2

Viste

- Albero : rappresentazione gerarchica dei file
 - File type
 - per estensione.
 - signature.
 - classificazione.
 - bad extension: estensione vs signature.
 - delete file: mancanti o cancellati.
 - known file : basato sull' hash.
 - ignorable file : come non di interesse.
 - notable file.
 - Artefatti:
 - metadati.
 - email archive.
 - system information.
 - user activity.
 - Navigazione web.
- Esistono delle viste specializzate
- image gallery: generazione e visualizzazione di thumbnail dei file grafici.
 - video gallery: elaborazione per l'estrazione e visualizzazione di frame dai video

- valore in % dei video.
- intervallo di tempo.
- social analyzer: relazioni/conessioni avvenute tra soggetti.
- Timeline : visualizzazione temporale dei file.
- File carving: recupero dei file non più residenti nel file system.
- Ricerche semi manuali:
 - Document content: info tramite espressioni regolari .
 - indexing: parole chiave.

Altri strumenti

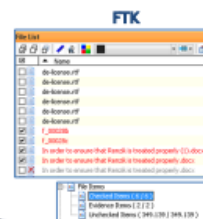


- ▶ Decrypt
- ▶ Malware Analysis
- ▶ Processing Image:
 - PhotoDNA
 - Riconoscimento Immagine/Viso
- ▶ Traduttore



Export/Report

- ▶ Esportare i file di interesse:
 - Etichette/Tag
 - Checkbox



FTK imager



- ▶ Prodotto dalla AccessData
- ▶ Licenza: *Freeware*
- ▶ Piattaforma: *O.S. Microsoft Windows*

Lite Version

Install Version

- è uno strumento per elaborare copie forensi.
- può eseguire una copia della memoria volatile.
- File > Create disk image...
 - tipi di acquisizione
 - physical drive.
 - logical drive.
 - image file.
 - content of folder.
 - fenico device.

Physical Drive :

- Source drive selection: dispositivo a acquisire
 - Si sceglie il formato immagine.
 - Si inseriscono le informazioni del caso.
 - Definizione del file immagine
 - percorso e nome del file immagine.
 - dimensione dei segmenti dei file immagine.
 - livello di compressione del file immagine.
 - cifratura del file immagine.
 - **Add overflow location**: calcolo e verifica dell' **hash** del file immagine col dispositivo target e si decide se aggiungere ulteriore spazio di archiviazione per il file immagine (install version).
 - è possibile visionare il tempo rimanente l' elaborazione della copia forense.
 - è possibile generare un file CSV di tutti i file e cartelle presenti.
 - durante l'elaborazione:
 - dispositivo target.
 - file immagine.
 - indicazioni dello stato del processo.
 - info temporali sull' elaborazione.
 - vi è un processo di validazione del file immagine.
 - al termine dell' elaborazione si genera un file con le info riportate.

Apertura del file immagine.

- File > Add evidence item.

Logical Drive

- File > Create disk image.
- è possibile acquisire un supporto ottico.

Image file

- impiegato principalmente per convertire un file immagine da un formato ad un altro: Es.
E01 -> DD.

Contents of a Folder

- Acquisizione logica di file in una determinata cartella.

Custom Content image

- elaborazione di un immagine personalizzata
 - File -> add evidence item.

- si visualizzano i file che sono stati selezionati.
- wild card option
 - ? = qualunque carattere.
 - * = qualunque serie di caratteri.
 - | (pipe) = separatore di directory e file.
 - le distinzioni tra maiuscole e minuscole.
 - si può estendere la ricerca ricorsivamente alle sottocartelle.
 - la ricerca viene eseguita direttamente su tutte le evidenze aggiunte e presenti nell' evidence tree.

dump memoria volatile

- File > Capture memory
 - percorso dove salvare il dump della memoria.
 - nome con il quale vogliamo salvare il dump.
 - si richiede di copiare anche il file di paging di windows.
 - il dump viene incapsulato in un file immagine AD1.

Autopsy

- Database in cui vengono memorizzate le info di casi precedentemente analizzati

Central repository

- conoscere se un file è già stato ricevuto.
 - evidenza automaticamente un file come di notevole interesse.
 - case db più leggero.
- Formati supportati

Disk Image:	Volume:	File System:
› Encase E01	› DOS	› FAT
› Raw (DD, BIN, IMG)	› GPR	› ExFAT
› Virtual Disk (VMDK, VHD)	› MAC	› NTFS
	› BSD	› EXT2FS
	› Solaris	› EXT3FS
		› EXT4FS
		› APFS
		› HFS, HFS+
		› YAFFS2

- **ingest modules:** Sono plug-in responsabili di analizzare i dati presenti all'interno del file immagine
 - hashing
 - identificazione del file type (bad extension).
 - user activity
 - analisi registri.
 - web activity.

- indexing.
- file carving.
- esegue i processi di analisi in background
 - i file vengono processati in base alla seguente priorità:
 - cartelle utenti.
 - program files e altre cartelle nella root.
 - cartella di windows.
 - spazio non allocato.
 - esecuzione parallela di più file immagine.
 - i risultati sono presenti nella sezione result.

- **Hash lookup**

1. calcola l' hash MD5 per ogni file.
2. li memorizza nel case DB.
3. ricerca gli hash calcolati all' interno della lista "known hash"
 1. as ignorable file (NSLR).
 2. as notable file.
 - ogni file ha 3 valori di known status.
 - unknown (default).
 - known (ignorable).
 - possono essere ignorati anche dagli altri moduli.
 - possono essere nascosti dalla views area.
 - possono essere nascosti dalla vista ad albero.
 - Velocizza notevolmente l'analisi.
 - notable (known bad).

- **ingest modules : file type**

- Determina la tipologia di file analizzando la signature
 - modo più accurato di definire un tipo di file.
- il file type viene conservato nel case DB
 - molti moduli dipendono da queste info.
 - basato su libreria **Tika** (open source)
 - catalogazione MIME type
 - application/zip.
 - audio/mpeg.
 - image/jpeg.
 - application/octet-stream.

- **ingest modules : file extension mismatch**

- per ogni file confronta l' estensione con la propria categoria
 - se non sono corrette viene etichettato.

- dipende dal modulo file type
l'obbiettivo è trovare il file che l'utente ha provato a nascondere.
- **ingest modules: exif parser**
 - estrae i metadati exif dal file jpeg , memorizzandoli nella sezione result
 - identifica la fotocamera.
 - timestamp dello scatto.
 - geolocalizzazione del luogo di scatto.
- **ingest modules: embedded file extractor**
 - estrae i file incapsulati in altri file
 - archivi file.
 - file grafici da documenti.
 - i file vengono salvati nel case folder
 - nella sezione tree view.
 - vengono etichettati se protetti da pass.
- **ingest modules : email parser**
 - ricerca e analizza archivi di posta
 - mbox, pst e eml file.
 - i risultati sono visualizzabili nella sezione e categoria email messages
 - gli allegati sono trattati come figli del messaggio.
 - sono raggruppati in threads.
 - è possibile analizzarli dettagliatamente attraverso la vista communications.
- **ingest modules : interesting files**
 - etichetta file e cartelle che si pensa essere interessanti
 - viene modificato il rinvenimento di tali oggetti
 - iphone backup.
 - VMware image.
 - bitcoin wallets.
 - cloude storage client.
- **ingest modules : encryption detection**
 - etichetta file e volumi che sono / potrebbero essere cifrati
 - documenti office e pdf e access DB protetti da password.
 - possibili file o volumi con cifratura basato su
 - high entropy.
 - dimensione: multiplo di 512 byte.
 - tipo di file: sconosciuto.
- **ingest modules : plaso**
 - Tool open source che esegue il parsing di file log e altri tipi di file per estrarre il timestamp
 - ne estrae di più possibili per elaborare la timeline.

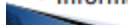
- come operazione è molto lunga.
- **ingest modules : Virtual machine extractor**
 - analizza le virtual machine presenti all'interno del reperto
 1. ricerca file VMDK e VHD.
 2. crea una copia locale.
 3. vengono inseriti in datasources.
- **ingest modules : data source integrity**
 - calcola l' hash del reperto
 - assicura l' integrità delle evidence.
 - 1. recupera l' hash dai metadati del disk image oppure da quelli inseriti dal c.f.
 - 2. calcola l' hash del disk image.
 - 3. invia un alert se la validazione fallisce.
- **ingest modules : recent activity**
 - estrae le attività recenti dell' utente
 - analisi dei web browser.
 - analisi dei registri
 - usb.
 - lista utenti.
 - programmi installati.
 - programmi eseguiti.
 - analisi del cestino.
 - i risultati vanno inseriti in extracted content.

Autopsy

Ingest Modules: Recent Activity

Analisi Registri

- ▶ **Analisi delle chiavi di registro mediante RegRipper:**
 - Tool OpenSource
 - Analizza il contenuto del registro e visualizza i risultati:
 - Non è un tool interattivo
- ▶ **Registri:** *System, Software, Security, SAM, NTUSER*
- ▶ **Produzione di artefatti:**
 - Dispositivi USB connessi
 - Programmi installati e eseguiti
 - Informazioni di sistema e dell'utente



Ingest Modules: Recent Activity

Recycle Bin

- Analisi del file cancellati ed ancora presenti nel «**cestino**»

- Cambio del filename:

- ≥ Windows 7: \$R+[random numbers/letters] (Es.:SR3F5245.di)
- < Windows 7: D+[drive letter] +[random numbers/letters] (Es.:DC8FXD2.doc)
- * se viene eliminata un'intera cartella solo il suo nome cambia.

- Analisi dei «file manifest» associati ai file:

- \$I+[newnamefile]
- Conserva l'originale *namefile* e *path*

- **ingest modules: keyword search**

- genera/aggiorna un text index
 - ricerca testuale.
- 1. si estrae ogni word da ogni file.
- 2. se la word non esiste viene aggiornata.
- 3. associa ogni word all' id del file.

- **uso di apache solr**

- indice memorizzato all' interno del case folder.
- contiene.
 - file name.
 - testo estratto dal contenuto file.
 - testo estratto dagli artefatti.

- **ingest modules keyword search**

- uso di apache **tika** per estrarre il contenuto dei file e dei metadati
 - per il file non riconosciuti o corrotti : string extractor
 - ricerca per byte.
 - uso di un proprio HTML text extractor
 - estrae anche i commenti e java script.
 - normalizzazione
 - ricerche case insensitive.
 - unicode.

- **ingest modules: correlation engine**

- ricerca dei file del caso all'interno del central repository
 - correlare il caso corrente con i casi passati.
 - evidenzia i file/item che erano stati etichettati come notable nei casi precedenti.
- aggiorna il central repository con i file del caso corrente
 - consente di correlare nuovi casi al caso corrente.
- central repository conserva:
 - valore.
 - caso.

- data source.
- file path.
- commento del CF.
- notable status.
- **ingest modules: photo rec carver**
 - recupero dei file cancellati mediante photo rec
 - open source tool.
 - data carving.
 - lavora su unallocated space.
 - i risultati sono nella vista ad albero \$carvedFile.
- **ingest modules: android analyzer**
 - analizza i dispositivi android
 - database di android e app di terze parti.
 - acquisizione fatta mediante altri strumenti.
 - estrae
 - registro chiamate.
 - contatti.
 - messaggistica.
 - browser.
 - geolocalizzazione.

Viste specializzate

- **Time Graphic interface**
 - consente di visualizzare graficamente le attività del sistema ordinate temporalmente
 - file time estratti dal file system.
 - web activity estratti dal recent activity.
 - exif.
 - plaso.
 - obbiettivo
 - quando è stato usato il sistema?
 - cosa è accaduto in un certo tempo?
 - cosa è accaduto prima e dopo certi eventi?
- **Image gallery**
 - Visualizza velocemente un insieme di immagini e video
 - materiale pedopornografico.
 - revenge porn.
 - documenti scansionati.
 - viene visualizzato il contenuto di una cartella alla volta

- priorità.
 - risultati positivi sull' hash.
 - numero di immagini/video.
- **Communication interface**
 - Visualizza i dati delle comunicazioni in modo differente
 - email parser.
 - android analyzer.
 - Orientato intorno agli account
 - vengono visualizzate tutte le attività associate.
 - visualizza le relazioni con altri account.
- **Geolocation**
 - Riepiloga tutti gli artefatti in cui sono state estratte le info sulle posizioni
 - exif parser.
- **Tagging**
 - Crea un riferimento ad un file/item di interesse
 - consente di commentarlo.
 - consente di etichettare solo una parte di una immagine.
 - sono associati all' esaminatore
 - conoscere chi li ha etichettati.
 - possono essere nascoste le etichette degli altri esaminatori.
 - obbiettivo
 - ritrovare facilmente il file di interesse.
 - evidenziarlo ed esportarlo nel report.
- **Reporting:**
 - Portable case
 - versione più piccola del caso originale
 - solo i file etichettati.
 - solo i file presenti nella categoria interesting item.
 - ha un proprio database SQLite.
 - i file sono esportati nel case folder.
- **Extensible**
 - Autopsy è costituito da moduli plug-in
 - datasource processor.
 - ingest module.
 - content viewer.
 - machine translation.
 - report module.
- gli utenti possono creare e pubblicare dei plug-in.
- utilizzano i linguaggi java e python.

- **Java module.**
 - Sono file con estensione .nbm.
 - possono contenere più moduli.
 - netbeans consente di auto aggiornarli e scaricarli.
 - Tools->plugins.
- **Python module**
 - sono cartelle che contengono file con estensione .py.
 - copia manuale delle cartelle nella directory.
 - possono essere solo ingest module e report module.

7- Sistemi Operativi

Windows

Analisi dei registri di sistema

- Configurazione dell'utente.
- Dispositivi USB.
- info temporali.
- strumenti
 - regedit.
 - win registry recovery (mitec).
 - registry viewer (Access data).

Thumbnails

miniature di immagini presenti nelle cartelle
per l' analisi di thumbnail non più presenti

- thumbs viewer.
- thumbcache viewer.

Shellbag

Personalizzazioni dell'utente delle visualizzazioni del contenuto delle cartelle.

- **Chiavi di registro**
 - HKEY_USERS\<USERID>\Software\Microsoft\Windows\Shell\
 - HKEY_USERS\<USERID>\Software\Microsoft\Windows\ShellNoRoam (Windows < Vista)
 - HKEY_USERS\<USERID>\Software\Classes\LocalSettings\Software\Microsoft\Windows\Shell\ (Windows ≥ Vista)

BagMRU: storico di tutte le cartelle visualizzate dall' utente.

Bags: impostazioni di visualizzazione delle cartelle contenute in bagMRU.

Analisi:

- si segue la lista delle cartelle presenti in MRUListex.
- si seleziona e visualizza il valore della chiave relativa.
- Si segue la sotto chiave della cartella.
- si visualizza la chiave MRUListex e si continua ricorsivamente la sua esplorazione.

Cosa si può ottenere:

- Bag Number: sottochiave bags che contiene le preferenze dell' utente.
- Registry key last write time : data del primo accesso o di ultima modifica dell'utente (nodeslot).
- Folder name: nome della cartella.

Tool: shellbagsview (nirsoft).

Application data

Impostazioni dei programmi utilizzati dall' utente e file temporanei.

```
► Windows XP:  
  • \Documents and Settings\[nome_utente]\  
    • Dati Applicazioni  
    • Impostazioni Locali  
► Windows ≥ Vista:  
  • \Users\[nome_utente]\AppData
```

Analisi :

Quadro complessivo dell' uso del computer da parte dell' utente

- Posta elettronica.
- Cache.
- Cronologia.
- Log.

- Configurazioni.



Microsoft Windows
Analisi

Vantaggi

- Diffuso
- Documentato
- Supportato

Svantaggi

- Pochi log
- Presenza di antivirus che possono compromettere una timeline
- Sistema commerciale

Linux

Configurazione

Netinfo (Db ad oggetti)

- Controlla diverse configurazioni del SO
 - Entry statiche di rete.
 - definizione di tutti gli utenti.

Gestione netinfo

/application/utility os x 10.4

/application/utility/utility directory os > 10.4

Configurazione server

- **Open Directory (Mac OS X Server 10.4)**
 - Servizio di directory
 - Gestione delle autenticazioni

Tool	Descrizione
dscl	Manipolazione e gestione dei servizi di directory
dsconfigd	manipolazione degli alberi LDAP
dsconfigd	manipolazione dei sistemi Active Directory
dseditgroup	gestione di gruppi di utenti
dsenableroot	abilita/disabilita l'utente root in OpenDirectory
dscacheutil	regola le cache relative a OpenDirectory
dsmemberutil	Gestisce i gruppi di appartenenza di un oggetto OpenDirectory
dsexport	esporta oggetti da un albero OpenDirectory
dsimport	importa oggetti in un albero OpenDirectory

Cifratura

File vault

- home directory (/users/[utente]).

File vault 2

- full disk encryption.

File swap

- Estensione memoria RAM
 - /private/var/vm/swapfile*.
- Congelamento della ram in fase di sospensione
 - /private/var/sleepimage.

Portachiavi

Accentrimento delle credenziali utente

- Tramite API.
- cifratura AES-128.

OS X \geq 10.9

- integrazione servizio apple iCloud.

Analisi

- Elevato numero di tecnologie proprietarie
- Strumenti
 - Blacklight: toolkit forense.
 - Macquisition: Tool di acquisizione forense.
 - Mac Forensics lab.
- Apple hdlutil: riga di comando
 - Apple dmg
 - Copia fulldisk.
 - copia logica.
- Home directory utente
 - gran parte dei file utente.
 - dati delle applicazioni.

Overview

- Distribuzioni basate su kernel GNU/linux.
- Linux Standard Base (LSB).
 - Standardizzazione delle diverse distribuzioni.
- Componenti
 - Kernel.

- Librerie di sistema.

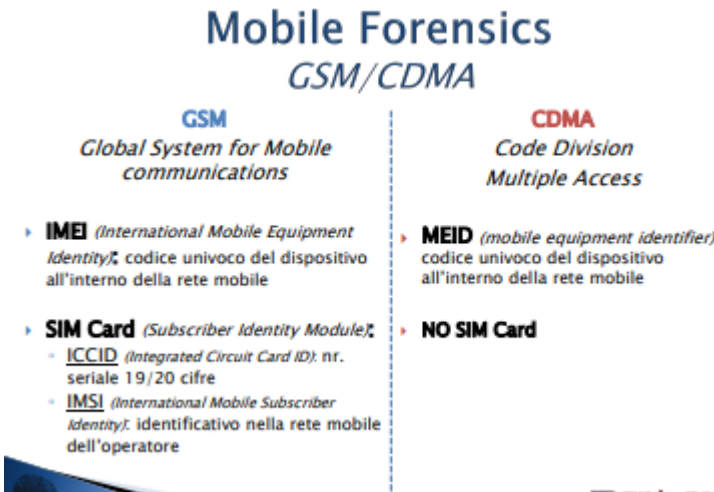
Distribuzioni commerciali

- Red hat enterprise
 - Defora.
 - Centos: versione libera senza supporto.
 - Scientific linux.
 - Suse Linux Enterprise
 - openSUSE.

Distribuzioni Gratuite

- Debian: free software foundation.
- Ubuntu.

Mobile



Mobile Forensics
GSM/CDMA

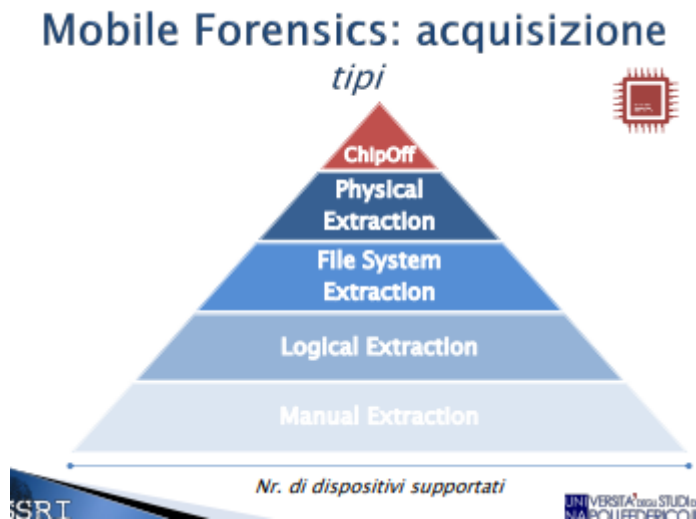
GSM	CDMA
<i>Global System for Mobile communications</i>	<i>Code Division Multiple Access</i>
<ul style="list-style-type: none"> ▶ IMEI (<i>International Mobile Equipment Identity</i>): codice univoco del dispositivo all'interno della rete mobile ▶ SIM Card (<i>Subscriber Identity Module</i>): <ul style="list-style-type: none"> ◦ ICCID (<i>Integrated Circuit Card ID</i>): nr. seriale 19/20 cifre ◦ IMSI (<i>International Mobile Subscriber Identity</i>): identificativo nella rete mobile dell'operatore 	<ul style="list-style-type: none"> ▶ MEID (<i>mobile equipment identifier</i>): codice univoco del dispositivo all'interno della rete mobile ▶ NO SIM Card

Raccolta

- Disabilitare le connessioni per evitare :
 - Remote Wipe.
 - Sovrascrittura di info presenti.
- Sbloccare il dispositivo
 - IOS
 - passcode a 4/6 o più cifre.
 - pass alfanumerica.
 - Face id / touch id.
 - Android os
 - Passcode da 4 o più cifre.
 - Pass alfanumerica.

- pattern.
- faceid/touch id.
- pass di avvio.
- Sim card
 - pass 4 cifre (pin) max 3 tentativi.
 - PUK 8 cifre max 10 tentativi.

Strumenti di acquisizione



SIM card

Struttura

- Master file (root).
- Dedicated file (directory).
- Elementary file.

Manual extraction

- repertazione fotografica del contenuto
 - Interagire con la gui.
- Svantaggi
 - Processo lungo.
 - Rischio di modifica/cancellazione dei dati.
- i limiti possono essere
 - Display non funzionante.
 - codice di sblocco.

Logical extraction

Estrazione tramite api del dispositivo

- limiti
 - Dipende dall' api
 - parziali.
 - solo alcune info.
 - solo alcuni dati.
 - Codice di sblocco.

File system extraction

Estrazione dei file tramite API del dispositivo.

Risultato

- L'output va processato per visualizzare i dati
 - sono contenuti in DB SQLite.
 - possibilità di vedere i dati cancellati (tramite entry db).
- Limiti
 - I risultati dipendono dai permessi con cui vengono fatte le richieste
 - Completo: tutta la struttura della live partition.
 - Parziale: Solo determinate porzioni.


Physical extraction

Copia bit a bit della memoria del dispositivo

- Boot loader
 - Bug del firmware/chipset.
- Agent: tool installato nell' SO
 - bug nel SO.
- Advanced ADB
 - bug nel SO.
- Risultato
 - Va processato per visualizzare i dati.
 - recupero dei file cancellati.
- Limiti
 - Produttore del dispositivo.
 - Chipset.
 - Versione del SO.
 - Patch di sicurezza.

Chip off

Estrazione fisica del chip da scheda madre

- 
- Distruzione del dispositivo.
 - limiti : dispositivo cifrato.