Appunti

Lezione 1 - Introduzione

Cos è la Computer Forensics?

> L'insieme di metodologie scientificamente provate finalizzate alla ricostruzione di eventi ai fini probatori che coinvolgono direttamente o indirettamente un supporto digitale.

Nasce come naturale conseguenza delle attività presso gli Uffici Giudiziari e dalla presa di coscienza del problema della "gestione" di un reperto digitale.

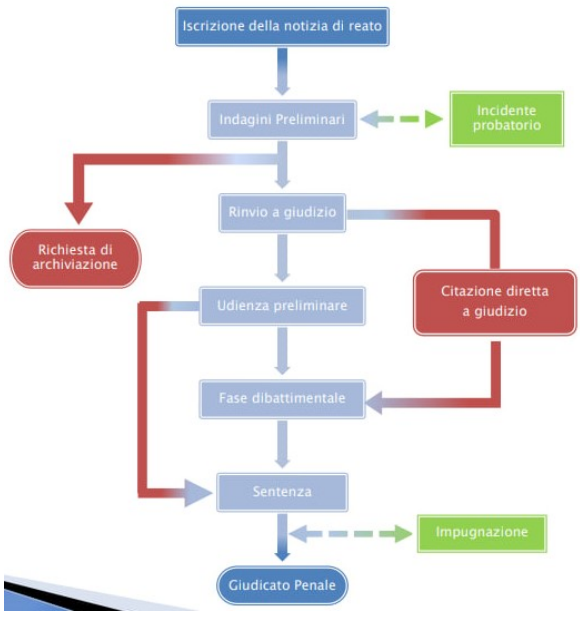
Un **digital forenser** può agire come Consulente Tecnico, per le forze dell'ordine o come impiegato in un Cyber Security Office.

Metodologie

- Identificazione
- Raccolta
- Validazione
- Preservazione
- Analisi
- Interpretazione
- Documentazione
- Presentazione

Lezione 2 - Procedimento Penale e Civile

Procedimento Penale



1. Iscrizione alla notizia di reato
2. Indagini preliminari
    a. (Facoltativo) - Incidente Probatorio
    b. (Alternativo) - Richiesta di approvazione
3. Rinvio a giudizio
    a. (Alternativo) - Citazione diretta a giudizio
4. Udienza preliminare
5. Fase dibattimentale
6. Sentenza
    a. (Facoltativo) - Impugnazione
7. Giudicato Penale

FASE INIZIALE

Quando le autorità giudiziarie ricevono una notizia di reato da parte di un'altra autorità o da un soggetto (persona offesa o testimone), il Pubblico Ministero (P.M.) iscrive tale notizia su un apposito registro: Registro Generale Notizie di Reato (R.G.N.R.).

Il P.M. e la Polizia Giudiziaria (PG) svolgono le indagini ritenute necessarie per poter verificare l'attendibilità della notizia di reato, cercando le prove e stabilendo se vi siano o meno i presupposti utili per poter esercitare un'azione penale.

INDAGINI PRELIMINARI

- Il PM e la PG svolgeranno le indagini per appurare che il reato iscritto sussista.
- Possono fare uso di due strumenti giuridici:
  - Perquisizione → verificare la presenza di una prova di reato
  - Sequestro probatorio → solitamente usato a seguito di un riscontro positivo della perquisizione per tutelare la prova da possibili alterazioni, o quando è necessario l'uso di strumenti specifici che non si dispongono nell'immediatezza

ACCERTAMENTO TECNICO

Il PM può avere la necessità di svolgere accertamenti tecnici che comportano specifiche conoscenze e tecniche. Per questo può avvalersi di un Consulente tecnico. Gli accertamenti possono essere **irripetibili:**

- Irripetibile → se compiuto causa l'alterazione della prova e la ripetibilità della procedura non è garantita. Viene eseguita previo avviso dell'indagato e della parte offesa.

MISURE CAUTELARI

Sono provvedimenti emessi su richiesta del PM nel periodo che intercorre tra l'inizio del procedimento penale e l'emanazione della sentenza.

- Reali → impediscono la disposizione di determinati beni o cose
- Personali → comportano una limitazione o privazione della libertà personale (coercertive), limitano temporaneamente l'esercizio di alcune facoltà o diritti (interdittive)

INCIDENTE PROBATORIO

Può essere richiesto dal Giudice per le Indagini Preliminari (GIP) o dal PM e ha la funzione di anticipare l'acquisizione e la formazione di una prova durante le indagini.

Il processo normalmente vorrebbe che la prova venga assunta davanti al giudice nel corso del dibattimento. Nel caso dell'incidente probatorio, quindi, si anticipa una parte del dibattimento nel periodo delle indagini preliminari. Può essere richiesto nei casi in cui debba essere disposta una perizia particolarmente complessa che comporterebbe la sospensione del procedimento per un periodo molto lungo, o quando deve essere fatta una perizia su un luogo o una persona che sono destinati ad avere dei mutamenti nel corso del tempo (accertamento irripetibile).

RICHIESTA DI ARCHIVIAZIONE

Al termine delle indagini preliminari, il PM 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 rimasto ignoto
- il reato è estinto
- il fatto non è previsto dalla legge come reato
- Il fatto sia particolarmente tenue

La parte offesa può presentare una richiesta motivata di opposizione al GIP.

RINVIO A GIUDIZIO

La richiesta di rinvio al giudizio è l'atto con cui il PM esercita l'azione penale. Si avvisa l'indagato della conclusione delle indagini preliminari, che ha 20 giorni per depositare atti e memorie, chiedere ulteriori indagini o di essere sottoposto a interrogatorio.

CITAZIONE DIRETTA A GIUDIZIO

E' esercitata dal Pubblico Ministero quando si tratta di:

- delitti puniti con la pena della reclusione non superiore nel massimo a quattro anni;
- violenza, minaccia o resistenza a un pubblico ufficiale;
- oltraggio a un magistrato in udienza aggravato;
- violazione di sigilli da parte del custode;
- rissa aggravata senza gravi lesioni;
- lesioni personali stradali;
- furto aggravato;
- ricettazione;

UDIENZA PRELIMINARE

Segna il passaggio dalla fase procedimentale a quella processuale, dove l'indagato si trasforma in imputato. Il GIP viene sostituito dal Giudice dell'Udienza Preliminare (GUP).

L'imputato può chiedere al giudice di essere prosciolto o rinunciare alla fase dibattimentale.

FASE DIBATTIMENTALE

Rappresenta la fase centrale del processo penale, nella quale si procede alla raccolta e acquisizione delle prove nel rispetto del contraddittorio delle parti. Le prove possono essere:

- Documentali → scritti o documenti che rappresentano fatti, cose, persone o cose attraverso la fotografia, cinematografia o altro mezzo
- Esame testimoniale → Deposizione di un soggetto, sottoposto al vincolo di giuramento, sui fatti rilevanti per il processo
- Perizia → Mezzo di prova al quale si ricorre quando è necessario svolgere indagini o acquisire elementi o valutazioni che richiedono determinate competenze tecniche

SENTENZA

La fase dibattimentale può terminare in due modalità:

- Proscioglimento:
  - Sentenza di non doversi procedere → manca una delle condizioni di procedibilità o sussiste una causa estintiva del reato
  - Sentenza di assoluzione → Quando il fatto non sussiste, l'imputato non lo ha commesso, il fatto non costituisce reato, il reato è stato commesso da persona non imputabile.
- Condanna → Pronunciata quando l'imputato risulta colpevole

IMPUGNAZIONE

Strumento attraverso il quale la parte processuale, nei cui confronti sia stato emesso un provvedimento giudiziario svantaggioso ne rimette il controllo a un giudice diverso:

- Secondo grado di giudizio → Corte d'appello. Può ribaltare le sentenze emesse in primo grado
- Terzo grado di giudizio → Corte di cassazione. Si ritiene che il processo sia illegittimo

GIUDICATO PENALE

La sentenza non è più impugnabile e la decisione non è modificabile. L'imputato non potrà essere sottoposto a procedimento penale per lo stesso fatto storico.

Procedimento civile

PROCEDIMENTO ORDINARIO

- Fase introduttiva → iscrizione a ruolo
  - L’attore (che instaura un giudizio) tramite l’avvocato espone i fatti che vengono posti a giudizio, notificato alla controparte (il convenuto)
- Fase istruttoria → Vengono acquisite in giudizio le prove richieste dalle parti, solitamente testimoniali o consulenze tecniche di parte (CTP). Il giudice può nominare un consulente tecnico d’ufficio (CTU)

PROCEDIMENTO CON RICORSO

- Fase introduttiva
  - Il ricorrente (instaura il giudizio) tramite l’avvocato espone i fatti posti a giudizio direttamente al Giudice (domanda con ricorso)
  - Il Giudice emette un decreto di fissazione dell’udienza
  - Il ricorrente notifica l’udienza alla controparte (il resistente)
  - Le parti devono esporre tutte le proprie difese e formulare le istanze istruttorie

Le leggi che hanno portato la maggiore evoluzione sono la legge 547 del 1993 e la legge 48 del 2008.

Procedimento Penale

- Diritto Penale.
- Si realizza in due strutture diverse: Procura e Tribunale.
- Ha lo scopo di accertare la verità nell’interesse dello Stato e della collettività.
- Si instaura anche d’ufficio.
- Il giudice non si pone una sanzione di indifferenza ma persegue uno scopo ben preciso: accertare la verità.

Procedimento Civile

- Diritto Privato.
- Si realizza solo in Tribunale
- Ha lo scopo di verificare l’esistenza di un diritto reclamato da un privato cittadino nei confronti di un altro e quale, tra le due parti in causa, ha ragione.
- Si instaura esclusivamente su iniziativa di una parte: l'attore
- il giudice si attiene solo alle prove presentate dalle parti, ponendosi in una posizione di equidistanza e imparzialità (principio dispositivo);

Lezione 3 - Gli attori del procedimento penale

Gli attori

- Pubblico Ministero (PM)
  - Organo dell’amministrazione giudiziaria dello Stato designato per garantire il rispetto della legge per valutare le azioni penali di un individuo. Rappresenta la pubblica accusa ed è titolare delle indagini
  - Dirige le indagini preliminari avvalendosi della polizia giudiziaria. Trova le prove d’accusa nei confronti di coloro che commettono reati
  - Nomina consulenti tecnici
  - Valuta l’esito delle indagini e decide se archiviare o rinviare a giudizio
  - Esercita l’azione penale, formando il capo di imputazione e sostiene in giudizio la tesi accusatoria
- Polizia Giudiziaria (PG)
  - Forze di polizia che collaborano con il PM nelle attività di indagine
  - Attività formativa → acquisisce la notizia di reato e la riporta al PM

    - Attività investigativa → ricerca dell'autore del reato
    - Attività di prevenzione → impedisce che i reati vengano portati a conseguenze peggiori
    - Attività assicurativa → individua e protegge le fonti di prova
- Parte Offesa (PO)
    - Soggetto titolare del bene giuridico leso dall'autore di un reato
    - Ha diritto di querela in tutti i casi in cui per il reato non debba procedersi d'ufficio o dietro richiesta di istanza
    - Può presentare memorie, indicare elementi di prova e nominare un difensore e consulenti tecnici
- Indagato/Imputato → Hanno l'obbligo di farsi assistere da un difensore
    - Indagato → Persona nei cui confronti vengono svolte delle indagini a seguito dell'iscrizione di un fatto a lui addebitato nel registro delle notizie di reato. Si conserva fino alla richiesta di rinvio a giudizio o di archiviazione
    - Imputato → Persona indagata nei confronti della quale è stata esercitata l'azione penale. Si conserva in ogni stato e grado del processo
- Avvocato Difensore → Ricopre un ruolo di assistenza, diventando bocca e orecchio giuridico del cliente, e un ruolo di rappresentanza, agendo in sostituzione dell'interessato nell'esercizio di diritti e facoltà. La sua presenza è un diritto e condizione prima di legittimità e regolarità dello stesso procedimento penale
- Giudice dell'Indagine Preliminare (GIP)
    - Ha funzione di garanzia dell'indagato durante le indagini preliminari. Può decidere se accogliere le richieste del PM su misure cautelari e autorizzare l'uso delle intercettazioni come mezzi di prova.
    - Ha funzione di garanzia dell'azione penale, accogliendo o no la richiesta di archiviazione
    - Non ha autonomia di iniziativa probatoria, provvede esclusivamente su richiesta della parte ed è privo di un proprio fascicolo (gli atti conosciuti sono quelli che il PM decide di allegare alle istanze che presenta)
- Giudice dell'Udienza Preliminare (GUP)
    - Interviene dopo l'esercizio nell'azione penale
    - Giudica la richiesta del rinvio a giudizio
    - Può emettere il decreto di rinvio o la sentenza di non procedere
- Giudice del Dibattimento (Monocratico o Collegiale)
    - Presiede a tutta la fase dibattimentale e alle relative udienze
    - Può essere singolo o collegiale
    - Per i reati più efferati è prevista una distinta composizione definita Corte d'Assise, dove è presente anche la Giuria popolare
    - Emette la sentenza

Struttura organizzativa

- Uffici magistratura inquirente
    - Procure della Repubblica
    - Procure Generali c/o corti di appello
    - Procure Generale c/o Suprema corte di cassazione
- Uffici magistratura giudicante
    - Tribunali ordinari
    - Tribunali per minorenni
    - Tribunali militari

    - Corte d’appello
    - Suprema corte di cassazione

Gli uffici della procura sono organizzati in gruppi di lavoro (sezioni) specializzati nella trattazione di specifici reati.

Esposto, denuncia e querela

- Esposto → Segnalazione all’autorità giudiziaria di un fatto alla scopo di far valutare se ricorre un’ipotesi di reato
- Denuncia → Atto con il quale si informa l’autorità giudiziaria di una notizia di reato perseguibile d’ufficio
- Querela → Dichiarazione della persona offesa con la quale si esprime la volontà di punire il colpevole per un reato subito, non perseguibile d’ufficio. Può essere ritirata se non si tratta di reati sessuali ai danni di minori

Il Computer Forenser nel procedimento penale

INDAGINI PRELIMINARI

Se sono richieste particolari competenze tecniche può essere nominato dall’autorità giudiziaria un consulente tecnico

Deve impiegare metodi e strumenti che garantiscono l’inalterabilità della prova, anche se non dettagliatamente descritti dalla legge

ACCERTAMENTO IRRIPETIBILE

Sono accertamenti che se compiuti portano a un’alterazione della fonte della prova e la ripetibilità della procedura non è più garantita (es: dispositivo non in buono stato)

Il PM esegue questa attività avvisando previamente l’indagato e il suo difensore, in modo da dare la possibilità a questi ultimi di assistere a tutta l’operazione a garanzia del rispetto delle procedure. L’indagato può farsi assistere da un proprio consulente tecnico (CTP)

PERITO

In caso di incidente probatorio o di un’udienza, in cui sono richieste particolari competenze tecniche, il giudice può nominare un consulente tecnico detto Perito.

Può essere scelto dall’albro del tribunale o da soggetti non iscritti.

RIEPILOGO

IL CF a seconda da chi e da quando viene incaricato assume ruoli diversi all’interno del procedimento:

- Ausiliario di PG
- Consulente Tecnico d’Ufficio (CTU)
- Consulente Tecnico di Parte (CTP)
- Perito del Giudice

Lezione 4 - Genesi del diritto informatico

IL REATO

Un reato è quell’illecita azione od omissione, teso a ledere un bene tutelato giuridicamente e a cui viene sottoposta una pena:

- Illecita → Contraria all’ordinamento giuridico
- Azione:
    - Doloso (consapevolezza di volontà)
    - Preterintenzionale (più danni di quanto voluto)
    - Colposo (manca la volontà di reato ma si verifica lo stesso l’evento)
- Omissione → Non impedire un evento che si ha l’obbligo di impedire

- Pena → Sanzione predisposta per la violazione di un precetto penale

REATO INFORMATICO

A livello internazionale si è riunciato a dare una vera e propria definizione di reato informatico. Si è preferito concordare una tipologia di comportamenti ai quali dare l'etichetta di reati informatici.

Vengono elaborate due liste di abusi:

- Lista minima → Condotte criminose che gli stati devono reprimere mediante una sanzione penale (frode informatica, falso di documenti informatici, sabotaggio, accesso non autorizzato, intercettazione non autorizzata di comunicazioni, etc.)
- Lista Facoltativa → Comportamenti ritenuti non eccessivamente offensivi la cui repressone è stata rimandata alla valutazione dei singoli stati (alterazione di dati, spionaggio, utilizzazione non autorizzata di elaboratori o programmi, etc.)

Lezione 6 - Fasi del trattamento - Identificazione e raccolta

Identificazione

La fase di identificazione dell'evidence consiste nel ricercare la fonte di prova che può dare una svolta alle indagini. La prima fase è volta a individuare dove un dato è conservato.

Vanno identificati tutti i dispositivi che possono contenere dati rilevanti (computer, cellulari, pen drive, fotocamere, server, stampanti). L'articolo 247 del c.p.p. stabilisce che quando vi è fondato modivo di ritenere che dati o informazioni si trovino in un sistema informatico ne è disposta la perquisizione con misure dirette a conservare i dati originali senza alterazioni.

FASE DI PREVIEW

Consente di eseguire un'analisi di primo livello delle memorie dei dispositivi utilizzando un "write blocker", anche se si rischia di alterare i contenuti e di conseguenza disperdere un'eventuale prova

- Preview DEAD → Analisi eseguita con il S.O. spento utilizzando un write blocker (hardware)
  - PRO → Non altera il dispositivo e consente di usare diversi strumenti di analisi
  - CONTRO → Buona conoscenza del sistema e dei software e non sempre praticabile (sistemi embedded)
- Preview LIVE → Analisi impiegata usando il S.O. presente sul dispositivo da documentare e verbalizzare
  - PRO → Si ha una visione dell'ambiente in cui si opera ed è veloce nell'analisi dei software installati
  - CONTRO → Alterazione del reperto e necessità di strumenti adatti al sistema

CAMBIAMENTI DI STATO DEL DISPOSITIVO

- Shutdown
  - Prima di eseguirlo vanno valutate alcune criticità:
    - Cifratura
    - Software in esecuzione
    - Dump della RAM
  - Come spegnere il dispositivo
    - Scollegarlo → potrebbe compromettere il funzionamento (Server, Raid, etc.)
- Accensione → Valutare se le informazioni che perderemo sono meno importanti dell'urgenza dell'accertamento:
  - Ultimo accesso al sistema
  - Esecuzione sul disco di diverse operazioni

Raccolta

IL SEQUESTRO

Dopo aver identificato i dispositivi o i dati di possibile interesse investigativo si procede con il sequestro fisico o logico:

- Fisico → Prendere il supporto contenente i dati, posticipando le problematiche derivanti dall'acquisizione del dato. Non è sempre fattibile (Es: dispositivi che non possono essere spenti o sistemi distribuiti sui rack)
- Logico → Duplicazione dei dati di interesse investigativo (generazione della copia forense)

Catena di Custodia → Uno o più documenti in cui devono essere riportati tutte le informazioni sul dispositivo sequestrato. Contiene:

- Luogo, data e operatore che ha reperito
- Luogo, data e operatore che ha gestito la fonte di prova
- Chi ha la resposabilità della custiodia delle digital evidence
- Metodo di conservazione del reperto
- Eventuali trasferimenti

COPIA FORENSE

La copia forense è una duplicazione dei dati di interesse investigativo, volta a fornire garanzia di ripetibilità dei successivi accertamenti che verranno eseguiti su tale copia.

- Acquisizione fisica → Copia bit a bit dell'intero supporto di memoria: dati e qualsiasi informazione sulla gestione dei dati
  - Clonazione → Creazione di un supporto identico all'originale (facilmente alterabile e usato solo in casi particolari)
  - File immagine → File che rappresenta il supporto originale (maneggevole e può essere utilizzato per generare un disco clone)
- Strumenti Hardware (duplicatori forensi - certificati, pesanti e costosi) e software (distro linux live forensi - gratuiti, open source e versatili)

Lezione 7 - Fasi del trattamento - Validazione e preservazione

Hashing

L'algoritmo di hashing restituisce una stringa a lunghezza fissa di esadecimali a partire da un flusso di bit di dimensione qualsiasi. La stringa è univoca per ogni file e ne è un identificatore.

L'algoritmo non è invertibile.

Validazione

La validazione garantisce che la copia eseguita è identica al dato originale: una volta clonato il disco con un file immagine si esegue un calcolo di hashing sia sul disco originale che sul file immagine per assicurarsi che i due codici di hash siano uguali.

ACCERTAMENTI RIPETIBILI

Si ha con memorie di massa in buono stato e sempre disponibili quando, eseguendo N copie forensi, ognuna delle copie restituisce lo stesso valore di hash

ACCERTAMENTI IRRIPETIBILI

- Si ha con memorie di massa non in buono stato
- Live Acquisition: il sistema operativo del dispositivo deve essere avviato per poter realizzare la copia forense

- Cloud (acquisizione remota)
- Dispositivo di origine non disponibile nel tempo

Preservazione

Sistema che garantisce che non vengano eseguite modifiche/alterazioni alla copia forense, se ciò avviene l'hash cambierà

FILE LOG

File descrittivo in cui sono presenti le informazioni sulla copia forense realizzata:

- Informazioni sullo strumento impiegato
- Informazioni del disco di origine
- Informazioni dell'immagine forense
- Altre informazioni (data, ora, settori, etc.)

Comandi della copia forense

COMANDO DD

Comando presente in tutti i sistemi operativi linux.

- /dev → Tutti i file al suo interno rappresentano dispositivi:
  - Character device (dispositivi che trasmettono dati)
  - Block device (dispositivi che memorizzano dati)

Comando di copia:

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

- if → Input file
- of → output file
- bs → block size in byte (default 512)
- conv → esegue l'elaborazione in base ai parametri indicati
  - noerror → continua l'elaborazione in caso di errore di lettura
  - sync → sostituisce i blocchi di memoria non letti nella destinazione con NULLs

Comandi avanzati:

- skip → salta la lettura di un numero n di blocchi di memoria partendo dall'inizio
- count → indica all'elaborazione di terminare dopo aver letto il numero n di blocchi di memoria
- split
  - -d → indica di appendere al nome del file un contatore decimale
  - -b → [n/n(K/M/G/T/P/E/Z/Y)] specifica la dimensione massima di ciascuna parte

Divisione del file immagine:

```
dd if /dev/sda bs=2048 | split -d -b 2G - mnt/dest/dd_image/sda
```

METODI DI CALCOLO DELL'HASH

- Metodo 1:

Calcoliamo l'hash del dispositivo sorgente e lo memorizziamo in un file

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

Se l’immagine è divisa in più file si adopera il CAT:

```
cat /mnt/dest/dd_image/sda.* | nd5sum /mnt/dest/dd_image/sda_merge.hash
```

- Metodo 2:

Calcoliamo l’hash durante l’elaborazione della copia:

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

COMANDO DC3DD

Patch del comando DD

```
dC3DD if=/dev/sda ofs=/mnt/dest/dd_image/sda.000 ofsz=2G bufsz=2k hash=md5 hash=sha256 log=/mnt/dest/dd_image/sda.log verb=on
```

- ofs → output diviso in più file
- ofsz → dimensione massima di ogni file
- bufsz → block size in byte
- hash → calcolo dell’hash indicato
- log → salva il report dell’elaborazione in un file
- verb → indica di generare un report dettagliato (verbose)

Comandi avanzati:

- rec=off → interrompe l’elaborazione in caso di un errore di lettura di un blocco di memoria
- hofs → l’output viene diviso in più file e per ciascuno di essi viene calcolato l’hash

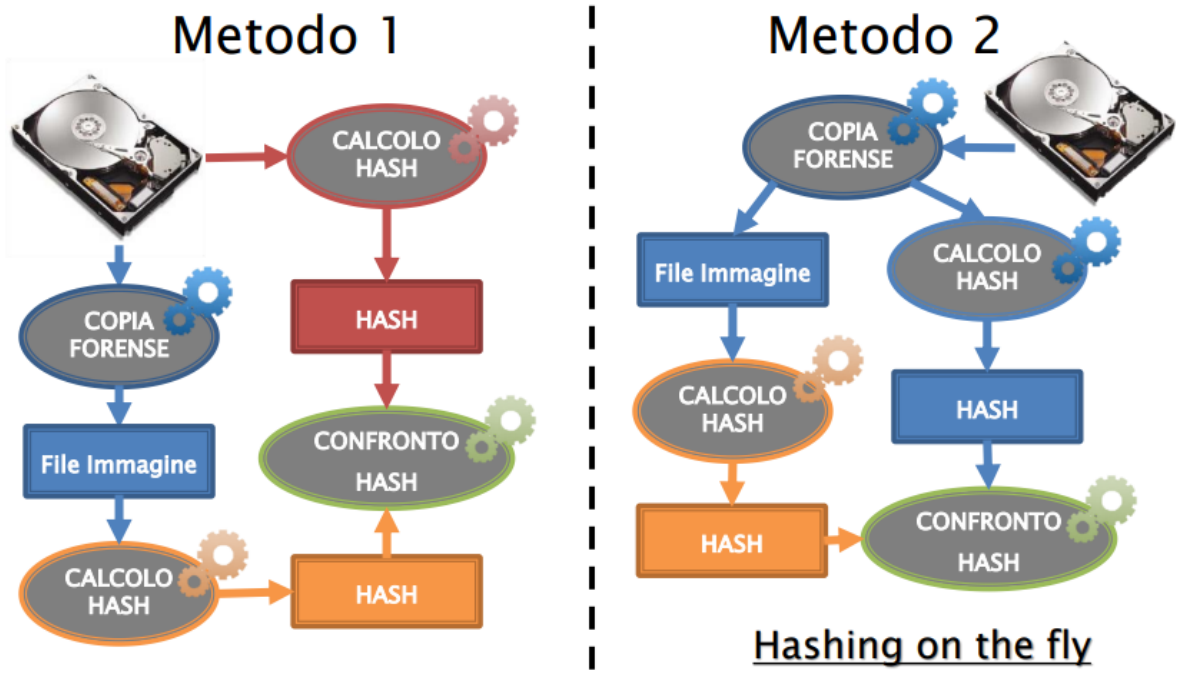
---

Lezione 8 - Raccolta e validazione - Disk Image e Tool

Calcolo dell’hash

Il calcolo dell’hash può avvenire in due modi:

1. Hashing “classico” → Metodo attraverso il quale il calcolo dell’hash viene effettuato prima e dopo la copia per la verifica (hash → copia → hash di verifica)
2. Hashing “on the fly” → Metodo attraverso il quale il calcolo dell’hash avviene allo stesso momento della copia forense



EVIDENCE MUTEVOLE

L'evidence prodotta viene definita mutevole. Infatti ci si può trovare in una situazione in cui l'hashing pre e post copia forense siano diverse se si usa il metodo classico, al contrario se si utilizza l'hashing on the fly.

Copia Forense

La copia forense avviene attraverso l'acquisizione fisica delle informazioni, ovvero una copia bit a bit dell'intero supporto di memoria, dei dati e di qualsiasi informazione sulla gestione dei dati (tabella partizioni MBR, etc.). La copia forense viene salvata in un file immagine (Disk Image)

Formati dei Disk Image

FORMATO DD/RAW

Formato molto 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

EXPERT WITNESS DISK IMAGE FORMAT (EWF)

File Immagine composto in sezioni. Fa utilizzo di un algoritmo di deflate per la compressione e salva l'immagine in modo segmentato. Della famiglia EWF fanno parte molti altri formati.

SMART (Famiglia EWF)

Ha come obiettivo un accesso veloce a una parte dell'immagine
e ogni segmento è composto da:

- Header File (Signature e nr. di segmento)
- Una o più sezioni (4 tipi):
  - Header

- Volume
- Table
- Next/Done

Name.s01
Header File
Signature: *EVF 090d0aff00*
Nr. segmento: *1*
Header Section
Informazioni sull'acquisizione
Volume Section
Informazioni sulla geometria del disco
Table Section *1*
Blocco dati del disco sorgente
Table Section *2*
Blocco dati del disco sorgente
Table Section *N*
Next Section
Offset della nuova sezione nel successivo segmento

ENCASE E01 BITSTREAM (Famiglia EWF)

Basato sul formato SMART e implementa una segmentazione dell'immagine. Esegue la compressione in tre livelli (no, good, best) e impiega 13 sezioni (+ 9 rispetto allo smart):

- Header2
- Disk
- Sectors
- Table2
- Data
- Errors2
- Sessione
- Hash
- Digest

ENCASE L01 LOGICAL (Famiglia EWF)

Implementa un'acquisizione dei file logici e utilizza la segmentazione dell'immagine. Impiega 15 sezioni (+ 2 rispetto al formato E01):

- Ltree
- Ltypes

ADVANCED FORENSICS FORMAT (AFF/AFF4)

Formato open ed estensibile, creato prima dell'implementazione opensource di "libewf".

Ogni disco viene separato in due layer:

- Disk-representation layer → Metadato
- Data-storage layer → Dato

Tool di acquisizione

Guymager

Tool per la piattaforma Linux basato sulla libreria open source "libewf" (clone + disk image).

SETTAGGIO DELL'ELABORAZIONE

- Scelta del formato dell'immagine e della dimensione dei segmenti
- Scelta dell'HASH

- Calcolo dell’hash del dispositivo target dopo l’acquisizione e del file immagine

Al termine dell’elaborazione viene generato un file .info con tutte le informazioni relative all’acquisizione

COSE DA RICORDARE

- Permette di produrre disk image nel formato E01
- Fa uso dell’hashing on the fly
- Permette di scegliere tra gli hash: MD5, SHA-1, SHA-256
- Esegue copie forensi solo di tipo “full disk”

FTK Imager

Strumento analogo a Guymager ma per piattaforma Windows con licenza Freeware.

Permette diversi tipi di acquisizioni:

- Phisical drive
- Logical drive → Impiegato principalmente per la conversione dei file immagine
- Image file
- Content of folder → Acquisizione logica di un file in una determinata cartella
- Fernico device
- Dump della memoria volatile → Richiede un percorso dove salvare il dump, il nome del file, se si vuole copiare anche il file di paging di windows e se incapsulare il file in un’immagine AD1

PHISICAL DRIVE

Permette la scelta del formato di immagine (Raw/dd, SMART, E01, AFF) e di definire diverse informazioni di quest’ultimo: percorso e nome, dimensioni dei segmenti, livello di compressione e cifratura del file.

COSE DA RICORDARE

- Riconosce solo determinati tipi di file system
- Permette di visionare il contenuto dei disk image
- Permette di avere informazioni su alcuni dei file cancellati
- Permette di esportare file di interesse
- Può essere utilizzato come strumento per la c.d. preview
- Fa uso dell’hashing on the fly
- Permette di segmentare il file immagine
- Non permette la scelta del tipo di hash
- Può eseguire una copia della memoria volatile

L9 - Protocolli di hashing (Pt. 1)

Crittografia

La crittografia è un processo che si utilizza per rendere oscuro ciò che si scrive e si vuole comunicare. La scienza che si occupa della comunicazione in forma sicura è detta Crittologia.

CRITTOGRAFIA VS CRITTOANALISI

- Crittografia → Studio e applicazione dei principi e delle tecnice per rendere l’informazione intelligibile a tutti tranne che al destinatario
- Crittoanalisi → Scienza e arte di risolvere i crittosistemi per recuperare l’informazione nascosta

PROTOCOLLI

Un protocollo, o schema, definisce le interazioni fra le parti (entità coinvolte) per ottenere le proprietà di sicurezza desiderate (segretezza, autenticità)

I protocolli si basano su una serie di protocolli più semplici detti primitive crittografiche, che risolvono problemi facili e possono essere usate per risolvere problemi più complessi usando come fonti dei Costrutti e dei problemi matematici

Le primitive risolvono i seguenti problemi:

- Cifratura → Cifrari simmetrici o asimmetrici o a chiave pubblica
- Autenticazione e Integrità → Funzioni HASH e MAC
- Fime digitali
- Altro → Generazione di numeri, prove zero-knowledge, etc.

Le primitive crittografiche

CIFRARIO SIMMETRICO

La crittografia simmetrica viene anche definita crittografia a chiave privata o crittografia a chiave segreta e prevede che **tutti gli** utenti coinvolti nella comunicazione si scambino la singola chiave di lettura per cifrare e decodificare i dati.

I principali algoritmi utilizzati nella crittografia simmetrica sono DES (Data Encryption Standard), 3DES (Triple DES) e AES (Advanced Encryption Standard). Altri algoritmi usati: RC2, RC4, RC5, RC6 e Blowfish

CIFRARIO ASIMMETRICO

La crittografia asimmetrica, nota anche come crittografia a coppia di chiavi, crittografia a chiave pubblica/privata o semplicemente crittografia a chiave pubblica, è un tipo di crittografia in cui, come si può dedurre dal nome, ad ogni attore coinvolto nella comunicazione è associata una coppia di chiavi:

- Chiave pubblica → Deve essere distribuita
- Chiave privata → Personale e segreta

Il meccanismo si basa sul fatto che se con una delle due chiavi si cifra un messaggio, allora quest'ultimo sarà decifrato solo con l'altra.

FIRMA DIGITALE

Apposizione di una firma a un documento digitale, che deve essere facilmente prodotta dal legittimo firmatario. Nessun utente deve poter produrre la firma di altri e chiunque deve poter facilmente verificare una firma.

Utilizza algoritmi quali RSA e DSS.

FUNZIONE DI HASH

Il valore hash h(M) è una rappresentazione non ambigua e non falsificabile del "messaggio M". Impiegato nella firma digitale, per mantenere l'integrità dei dati e per la certificazione nel tempo.

- Integrità → Computo al tempo T_0 il valore di hash del file M: $H = h(M)$. Per controllare se il file è stato successivamente modificato calcolo al tempo T_1 l'hash: $H' = h(M)$ e verifico se $H = H'$. Diciamo che $h(M)$ è **l'impronta digitale** del file.

FUNZIONE MESSAGE AUTHENTICATION CODE (MAC)

In crittografia, un message authentication code (MAC) è un piccolo blocco di dati utilizzato per garantire l'autenticazione e l'integrità di un messaggio digitale. Viene generato secondo un meccanismo di crittografia simmetrica: un algoritmo MAC accetta in ingresso una chiave segreta e un messaggio di lunghezza arbitraria da autenticare, e restituisce un MAC (anche chiamato *tag*). In ricezione, il destinatario opera in maniera identica sul messaggio pervenuto in chiaro, ricalcolando il MAC con lo stesso algoritmo e la stessa chiave. Se i due MAC coincidono, si ha l'autenticazione e l'integrità del messaggio inviato.

PROPRIETÀ DI SICUREZZA

- Confidenzialità → Protezione del dato da un soggetto estraneo (sistema di cifratura)
- Autenticazione → Certezza di identificare l'interlocutore

- Integrità → Verificare che il messaggio non è stato modificato durante la trasmissione. Solo chi è autorizzato può modificare l'attività di un sistema o le informazioni trasmesse.
- Non-ripudio → Negare il disconoscimento del messaggio al mittente o al destinatario. Risulta impossibile negare l'occorrenza di una determinata azione.
- Anonimia → Nascondere l'identità di chi ha compiuto una determinata azione nel contesto crittografico (gradi di anonimia)

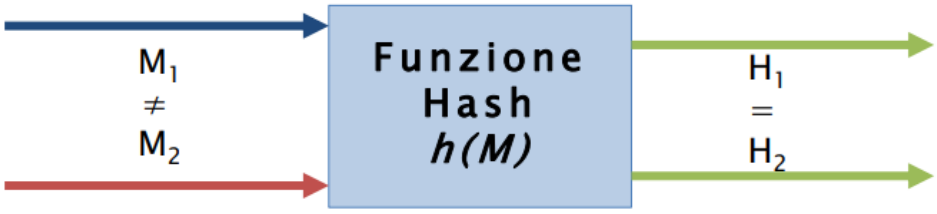
Hashing

COLLISIONE

In crittografia, una **collisione hash** è una situazione in cui due input diversi producono lo stesso output tramite una funzione hash:

$$h : \Sigma^* \to \Sigma^n$$
$$h(m_1) = h(m_2)$$

Potenzialmente, la maggior parte delle funzioni hash danno luogo a collisioni, ma con una buona funzione hash esse avvengono molto raramente.



PROPRIETÀ

- One-Way (pre-image resistant) → Dato un hash y, è computazionalmente difficile trovare $M|y = h(M)$.
- Sicurezza debole (2nd pre-image resistance) → Dato un hash y, è computazionalmente difficile trovare una variazione di M, $M'|h(M) = h(M')$.
- Sicurezza forte (collision resistance) → Computazionalmente difficile trovare 2 diversi messaggi con lo stesso valore di hash.

DEFINIZIONI

- One-Way Hash Function (OWHF) → Verifica le proprietà pre-image e 2nd pre-image resistant, e viene detta "weak one-way hash function"
- Collision Resistant Hash Function (CRHF) → Verifica la proprietà di collision resistance e viene detta "strong one-way hash function"

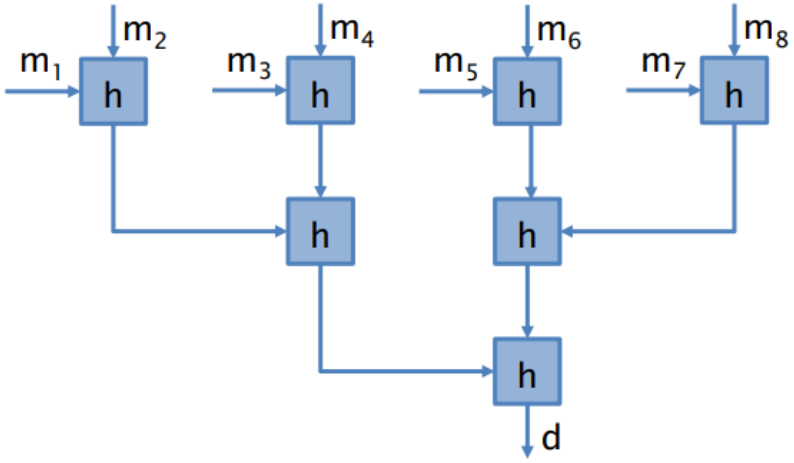
COSTRUZIONE

Messaggi di lunghezza arbitraria sono trattati usando hash con input fisso:

- Il messaggio di input M viene diviso in k-blocchi di lunghezza fissa.
- I blocchi vengono trattati in modo seriale o parallelo.

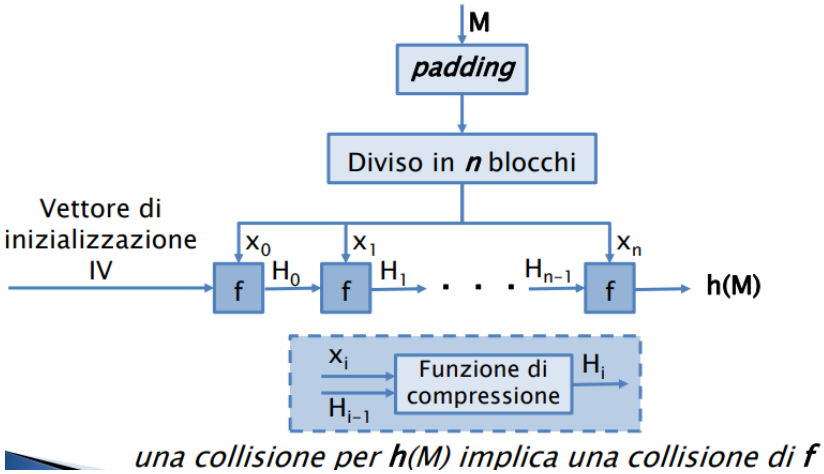
Modello di Hashing parallelo

Modello resistente alle collisioni solo se lo è la funzione di hashing iniziale.



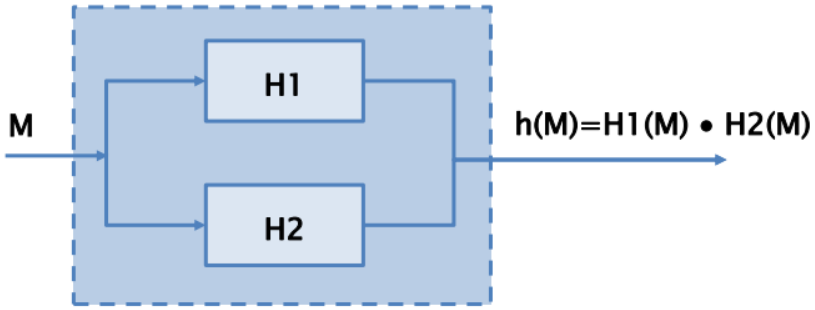
Modello di Hashing seriale

Introduce il concetto di **padding** → Una collisione $h(M)$ implica una collisione della funzione di compressione.



Modello di Hashing a Cascata

Il valore è dato dal prodotto di due funzioni hash: una collisione per h(M) significa trovare una collisione sia per H1 che per H2.



L10 - Protocolli di hashing (Pt. 2)

Funzione MD4/MD5

- MD → Message Digest

Sono operzioni efficienti su architetture 32 bit little-endian

LITTLE ENDIAN

Il byte con indirizzo più basso è quello meno significativo

BIG ENDIAN

Il byte con indirizzo più basso è quello più significativo

OBIETTIVI

- Sicurezza forte → Computazionalmente difficile trovare 2 messaggi con lo stesso hash
- Sicurezza diretta → Non basata su problemi teorici difficili computazionalmente
- Velocità → Algoritmo adatto per implementazioni software molto veloci
- Semplicità e compattezza → Semplice da descrivere e da implementare, senza nessun uso di tabelle e complesse strutture dati

CARATTERISTICHE

- Processa il messaggio in blocchi di 512 bit (ogni blocco avrà 16 parole di 32 bit)
- M' sarà costituito da:
  - Messaggio originario M
  - Bit di padding (p)
  - Bit di rappresentazione della lunghezza (b → max 2^{64})

$$M' = M\ 100...0\ b$$
$$p|(p + M)mod_{512} = 448 \iff 512 - [(M + b)mod_{512}]$$

- M' consta di un numero di bit multiplo di 512, ovvero di un numero L blocchi di 512 bit (ovvero di N parole con N multiplo di 16) → L=N/16 blocchi di 512 bit

OPERAZIONI

Impiegano diverse operazioni sulle word in input X e Y restituendo una nuova word:

- $X \wedge Y$ → and bit a bit
- $X \vee Y$ → or bit a bit
- $X \oplus Y$ → xor bit a bit
- $\neg X$ → complemento bit a bit
- $X + Y$ → somma intera modulo 2^{32}
- $X << s$ → shift circolare a sinistra di s bit

FUNZIONI

Funzioni definite su parole di 32 bit (utilizzo di 4 round e 4 funzioni logiche)

- round 1: $F(X,Y,Z) = (X \wedge Y) \vee ((\neg X) \wedge Z)$
- round 2: $G(X,Y,Z) = (X \wedge Z) \vee ((Y \wedge (\neg Z))$
- round 2: $G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge Z) \vee (X \wedge Y)$
- round 3: $H(X,Y,Z) = X \oplus Y \oplus Z$
- round 4: $I(X,Y,Z) = Y \oplus (X \vee (\neg Z))$

COMPRESSIONE

TRE round [MD4] - QUATTRO round [MD5]

- 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 di 16 operazioni
    - MD4 → $t = (A + W(B, C, D) + X[j] + y[j])) << s[j]$
        - X[j] è predefinito e reperibile nell'algoritmo
        - s[j] indica lo shift ciclico
        - y[j] è la costante additiva relativa al round corrente
        - W è la funzione del round (F,G,H)
    - MD5 → $A \leftarrow B + ((A + W(B, C, D) + X[k] + T[i])) << s$
        - K è l'indice della parola
        - s indica lo shift ciclico
        - i è l'indice dell'iterazione
        - W è la funzione del round (F,G,H,I)
        - X[k] ← M'[16i+k] è la k-esima word di 32 bit nell'i-esimo blocco
        - T[i] è l'i-esimo elemento della tabella di 64 valori
- L'input dell'ultima fase viene sommato all'input della prima fase (word a word)
- L'output della L-esima fase è il digest a 128 bit

MD5

- 4 round = 4*16 operazioni (64)
    - 4 funzioni logiche
- 64 costanti additive
- ogni passo aggiunge il risultato del passo precedente

MD4

- 3 round = 3*16 operazioni
- 3 funioni logiche
- 2 costanti additive

Funzione SHS/SHA

- SHS → Secure Hash Standard
- SHA → Secure Hash Algorithm

Implementano gli stessi principi di MD4 e MD5 ma sono più sicuri.

SHA-1 VS MD4/MD5

- Sicurezza maggiore in SHA-1, otuput di 32 bit più lungo rispetto a MD4/5 (160 contro 128)
- SHA-1 è più sicuro contro l'analisi
- Entrambi molto veloci ma SHA-1 ha 80 passi contro 64 di MD e il buffer ha 160 bit rispetto ai 128 bit di MD5
- Entrambi sono semplici e compatti da scrivere, senza l'utilizzo di tabelle o complesse strutture dati

Sono state successivamente proposte altre funzioni di SHA (256, 512, 384):

- 256 → Messaggio diviso in blocchi di 512 bit (parole da 32 bit)
- 512 → Messaggio diviso in blocchi di 1024 bit (parole da 64 bit)
- 384 → Valore di hash = primi 384 bit di SHA-512 con costanti iniziali cambiate

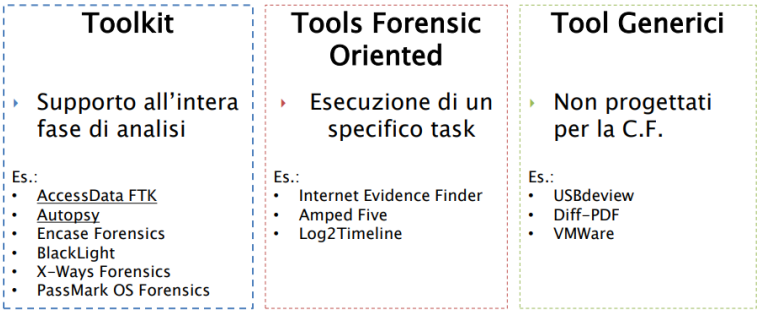
ALTRE FUNZIONI DI HASH

- Snefru
- N-hash

- HAVAL
- FFT-hash I
- FFT-hash II
- RIPEMD-160

L12 - L’Analisi - Gli strumenti

La fase di analisi va eseguita su una copia forense e ha come obiettivo la ricostruzione di eventi passati mediante la lettura di dati digitali. Bisogna garantire la riproducibilità del risultato, ovvero uno stesso risultato deve essere ottenibile da diverse operazioni/strumenti di analisi.



MONTARE UN FILE IMMAGINE

1. Analizziamo il file immagine per trovare dispositivi e partizioni:

```
fdisk -l /mnt/dest/dd_image/sda.dd

Device                      Boot    Start    End    Sectors Size Id  Type
/mnt/dest/dd_image/sda.ddp1 2048    2099199 2097152 1G      b    W95 FAT32
/mnt/dest/dd_image/sda.ddp2 2099200 8388607 6289408 3G      b    W95 FAT32
```

Questo file immagine rappresenta una memoria con due partizioni p1 e p2.

2. Montiamo la partizione p2:

```
mount -o ro,loop,offset=1074790400 /mnt/dest/dd_image/sda.dd /mnt/sda_dd
```

- ro → read-only
- loop → crea un virtual block device da un file (character device)
- offset=byte → punto di inizio della partizione da montare (start*512)

PRO

- Veloce per operazioni semplici
- Utiliizzo di tool non forensics oriented

CONTRO

- Farraginoso
- Solo file residenti
- Riconoscimento del FileSystem dell’immagine demandata al nostro SO

MERGING DELL’IMMAGINE SEGMENTATA

- DD\RAW → comando “affuse” → affuse /mnt/dest/dd_image/sda.000 /mnt/sda_fuse
- EWF → comando ewfmount → ewfmount /mnt/dest/e01_image/sda.E01 /mnt/sda_fuse

I Toolkit

FORENSICS TOOLKIT (FTK)

- Commerciale
- Windows

Formati file immagine

- Encase E01/E01 Logical Image
- Expert Witness
- Snapback
- Safeback 2.0
- ICS
- Linux DD
- SMART
- Ghost (forensics image)
- MSVHD
- AccessData Logical Image (AD1)
- Lx0, Lx01
- DMG
- VMDK

File System

- FAT, exFAT
- NTFS
- Ext2FS, Ext3FS, Ext4FS
- APFS
- HFS, HFS+
- CDFS
- ReiserFS 3
- VXFS

AUTOPSY

- Free e Open Source
- Multipiattaforma

Formati file immagine

- Encase E01
- RAW (DD, BIN, IMG)
- Visrtual Disk (VMDK, VHD)

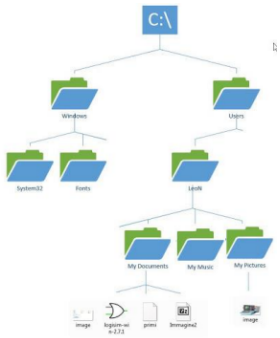
File System

- FAT
- ExFAT
- NTFS
- Ext2FS, Ext3FS, Ext4FS
- APFS
- HFS, HFS+
- YAFFS

Le viste

ALBERO

Rappresentazione gerarchica dei file



FILE TYPE

- Catalogazione → Analisi dei file per:
  - Estensione
  - Signature (magic number) → Sequenza di bit posta in un punto ben preciso del file (offset) per definire il formato in cui i dati sono memorizzati
- Classificazione → I file vengono analizzati e arricchiti di alcuni attributi (bad extension o delete file)

KNOWN FILE

- Riconoscimento del file basato sull'HASH
- **IGNORABLE FILE** → File riconosciuti come di non interesse
- **NOTABLE FILE** → File riconosciuti come di notevole interesse

ARTEFATTI

- Analisi del contenuto del file → Estrazione ed elaborazione di informazioni persenti in uno o più file
- Metadati → Dati strutturati contenenti informazioni aggiuntive sul file
- E-Mail Archive → Analisi degli archivi email (visualizzazione ed estrazione degli allegati)
- System Information
- Estrazione delle informazioni dell'ambiente di lavoro
- User Activity → Analisi delle attività eseguite dall'utente (File registro, log, etc.)
- Navigazione WEB → Analisi dei file dei browser web (history, cookies, cache, download, etc.)

Viste specializzate

- **IMAGE GALLERY** → Processo di elaborazione per l'estrazione e la visualizzazione frame dai video
- **SOCIAL ANALYZER** → Visualizzazione delle relazioni/connessioni avvenute tra i diversi soggetti (email)
- **TIMELINE** → **V**isualizzazione temporale del file

Altri strumenti

- **FILE CARVING** → Recupero dei file non più residenti nel file system
- **RICERCHE SEMI MANUALI**
  - Ricerca tramite attributi
  - Document content → Estrazione di determinate informazioni mediante regular expression
  - Indexing → Ricerche di determinate parole chiave
- Altro (Decrypt, Malware analysis, processing image, traduttore)

L14 - L'Analisi - Autopsy (Pt. 1)

Programma che permette una doppia configurazione:

- Single user
- Multi user

CONFIGURAZIONE

- Central repository → Database nel quale vengono memorizzate le informazioni di casi precedentemente analizzati:
  - Conoscere se un file è già stato rinvenuto
  - Evidenziare automaticamente un file come di notevole interesse
  - Case DB più leggerp

DISK IMAGE

- Encase E01
- Raw (DD, BIN, IMG)
- Virtual Disk (VMDK, VHD)

VOLUME

- DOS
- GPR
- MAC
- BSD
- Solaris

FILE SYSTEM

- FAT, ExFAT
- NTFS
- EXT2/3/4FS
- APFS
- HFS, HFS+
- YAFFS2

Ingest Modules

Sono plugin responsabili di analizzare i dati presenti all'interno del file immagine:

- Hashing
- Identificazione del file type
- User activity
- Indexing
- File carving

Sono installati tramite Ingest Manager, che esegue i processi di analisi in background:

- 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 visualizzabili nella sezione "result"

HASH LOOKUP

1. Calcola l'hash MD5 per ogni file
2. Memorizza gli hash nel Case DB
3. Ricerca gli hash calcolati all'interno di una lista di "known hash"

Ogni file nel caso ha tre valori di status:

- Unknown (default)
- Known (ignorable) → Possono essere ignorati anche dagli altri moduli, nascosti dall'area "views" e nascosti dalla vista ad albero
- Notable (known bad/bad file)

FILE TYPE

Determina la tipologia del file analizzando la signature → ES: 0xffd8 = JPEG.

Il file type viene conservato nel case DB (siccome molti moduli dipendeono da queste informazioni) ed è basato sulla libreria open source Tika.

FILE EXTENSION MISMATCH

Per ciascun file confronta l'estensione con la propria categoria: se le informazioni non sono coerenti viene etichettato. Dipende dal modulo File Type e ha come obiettivo trovare i file che l'utente ha provato a nascondere.

EXIF PARSER

Modulo che estrae i metadati Exif (Exchangeable Image File Data) dai file JPEG memorizzandoli nella sezione “Result”:

- Identificazione della fotocmera
- Identificazione del timestamp dello scatto
- Geolocalizzazione del luogo dello scatto

EMBEDDED FILE EXTRACTOR

Estrae i file incapsulati in altri file (zip, rar, pdf, etc.). I file estratti vengono salvati nel Case Folder, sono visionabili nella tree view e vengono etichettati se protetti da password.

EMAIL PARSER

Ricerca ed analizza archivi di posta (Mbox, PST, EML). I risultati sono visualizzabili nella sezione “result” nella categoria “Email messages” raggruppati in thread (gli allegati sono trattati come figli del messaggio). Possono anche essere analizzati dettagliatamente attraverso la vista “Comunications”

INTERESTING FILES

Etichetta file e cartelle che si pensa essere “interessanti”.

ENCRYPTION DETECTION

Etichetta file e volumi che sono/potrebbero essere cifrati (Documenti office, PDF, Access DB protetti da password). Possono essere file o volumi con cifratura basata su:

- High entropy
- Dimensione multipla di 512 byte
- Tipo di file sconosciuto

PLASO

Tool open source che esegue il parsing di file log e altri tipi di file per estrarre i timestamp. Estrae quanti più timestamp possibili per la generazione di una timeline (operazione molto lunga)

VIRTUAL MACHINE EXTRACTOR

Analizza le virtual machine presenti all’interno del reperto:

1. Ricerca file VMDH e VHD
2. Crea una copia locale
3. Vengono inseriti in datasource

DATA SOURCE INTEGRITY

Calcola e valida l’hash del repero, assicurando l’integrità dell’evidence:

1. Recupera l’hash dei metadati del disk image o da quelli inseriti dal CF
2. Calcola l’hash del disk image
3. Invia un alert se la validazione fallisce

L15 - L’Analisi - Autopsy (Pt. 2)

Altri ingest modules

RECENT ACTIVITY

Estrae le attività recenti dell’utente e inserisce i risultati in “Extracted Content”:

- Analisi dei web browser (history, cookies, download) → I risultati dei differenti browserr vengono uniti
- Analisi dei registri (dispositivi usb, lista utenti, programmi installati/eseguiti)

    - Analisi delle chiavi di registro mediante RegRipper (analizza il contenuto del registro e visualizza i risultati)
    - Registri → System, software, security, SAM, NTUSER
    - Produzione di artefatti (Dispositivi usb connessi, programmi installati ed eseguiti e informazioni di sistema e dell'utente)
- Analisi del Cestino (Recycle Bin) → Analisi di file cancellati ma ancora nel cestino:
    - Cambio del filename
    - Analisi dei file manifest associati ai file
    - Porta come risultato un "delete file" nella vista ad albero

KEYWORD SEARCH

- Genera/aggiorna un "text index":
    - Si estrae ogni word da ogni file
    - Se la word non esiste viene aggiunta
    - Associa la word all'ID del file
- Utilizzo di Apache Solr:
    - Indice memorizzato all'interno del case folder che contiene file name, testo estratto dal file e testo estratto dagli artefatti
- Uso di Apache Tika per estrarre il contenuto dei file e dei metadati (string extractor per i file non riconosciuti o corrotti)
- Uso di un proprio HTML TEXT EXTRACTOR
- Normalizzazione → Ricerche case sensitive in unicode

CORRELATION ENGINE

Ricerca dei file del caso all'interno del central repository per correlare il caso corrente con i casi passati. Aggiorna il central repository con i file del caso corrente e consente di correlare nuovi casi al caso corrente.

Nella central repository viene conservato:

- Valore
- Caso
- Data Source
- File Path
- Commendo del CF
- Notable Status

PHOTOREC CARVER

Recupero dei file cancellati mediante PhotoREC, un tool open source per effettuare data carving lavorando su unallocated space. I risultati sono visibili nella vista ad albero ($CarvedFiles).

ANDROID ANALYZER

Analizza i dispositivi android ed estrae:

- Registro chiamate
- Contatti
- Messagistica
- Browser
- Geolocalizzazione

Viste specializzate

TIMELINE GRAPHIC INTERFACE

Consente di visualizzare graficamente le attività del sistema ordinate temporalmente e ha come obiettivo lo scoprire quanto è stato usanto il sistema, cosa è successo in un certo tempo e cose è accaduto prima e dopo certi eventi.

IMAGE GALLERY

Consente di visualizzare velocemente un insieme di immagini e video mostrando il contenuto di una sola cartella alla volta, dando priorità al numero di risultati positivi sull'hash e al numero di immagini/video.

COMMUNICATION INTERFACE

Visualizza i dati delle comunicazioni in modo differente orientato intorno agli account:

- Vengono visualizzate tutte le attività associate
- Vengono visualizzate le relazioni con gli altri account

GEOLOCATION

Rieptiloga tutti gli artefatti in cui sono stati estratte le informazioni sulle posizioni

Tag e Report

TAGGING

Serve a creare un riferimento a un file di interesse e consente di comentarlo e di etichettare solo una parte di una immagine. Sono associati all'esaminatore per conoscere chi li ha etichettati e possono essere nascoste le etichette degli altri esaminatori.

Ha come obiettivo il ritrovare facilmente i file di interesse per evidenziarli ed esportarli nei report.

I commenti consentono di annotare il motivo di interesse di un file, verrano visualizzati nei report e possono essere salvati nel central repository.

REPORTING

Processo di generazione di un report per esportare e condividere i risultati dell'analisi, salvato nella sezione "reports". Può essere salvato come HTML report visualizzabile nel web.

Una versione più piccola del caso originale è detta "portable case". Contiene solo i file etichettati e i file presenti nella categoria "interesting item". Ha un proprio DB SQLite e i suoi file sono esportati nel case folder.

L16 - L'Analisi - I volumi

VOLUME SYSTEM

Si preoccupa di gestire i volumi (insiemi di settori per memorizzare dati) per raggiungere due obiettivi:

1. Unione di più volumi in uno solo
2. Suddivisione del volume in partizioni → Insiemi di settori consecutivi in un volume

INDIRIZZAMENTO DEI SETTORI

- Phisical address (LBA) → Indirizzo del settore è calcolato in base al primo settore del disco
- Logical Disk Volume Address → L'indirizzo del settore è calcolato in base al primo settore del volume
- Logical Volume Partition Address → L'indirizzo del settore è calcolato in base al primo settore della partizione

DOS Partition

Sistema di partizione più comune. Composto da:

- MBR (Master Boot Record) → Primo settore, allocato all'inizio del disk volume e di ogni extended partition, che contiene:

    - Boot Code → Situato nei primi 446 byte del primo settore
    - Partition table
    - Signature
    - EBR → Extended Boot Record (512 byte)
- Primary File System Partition → Parizione primaria che contiene un file system
- Primary Extended Partition → Partizione primaria che contiene altre partizioni
    - Tabella di partizione
    - Secondary File System Partition: partizione secondaria che contiene un file system (partizione logica)
    - Secondary Extended Partition

Apple Partition Map

Sistema impiegato soprattutto dai vecchi sistemi basati su processori non Intel, che non ha limite massimo di partizioni e gestisce volumi fino a 2TB.

La partition map è presente nel secondo settore (512 byte). Ogni entry descrive una partizione e la prima entry descrive la partition map.

Guid Partition Table

Sistema di partizionamento utilizzato da EFi con un massimo di 128 partizioni e volumi più grandi di 2TB. Composto da 4 sezioni:

- Protective MBR
- GPT Header (layout delle aree)
- Partition table (ogni entry descrive la partizione)
- Backup area (copia di backup del GPT header e della partition table)

L17 - L’Analisi - I File System (Pt. 1)

Il file system è un sistema che permette la memorizzazione dei dati organizzandoli gerarchicamente in file e directory, in modo tale da ritrovarli velocemente.

DATI ESSENZIALI

- Dati che se modificati causano il malfunzionamento del sistema (trusted data)

DATI NON ESSENZIALI

- Informazioni accessorie (untrusted data):
    - Dati temporali
    - Permessi utente

FILE SYSTEM CATEGORY

Contiene le informazioni generali sul file system, solitamente posizionati nel primo settore e contengono essenziali informazioni sul layout dei dati.

Dall’analisi ricaviamo informazioni sulla generazione del FS, informazioni sul layout e possiamo controllare la consistenza (volume slack → Parte non usata di una data unit allocata)

CONTENT CATEGORY

Sono locazioni di memoria impiegate per la memorizzazione del contenuto dei file:

- Data Unit → Raggruppamento di più settori

Utilizza diverse strategie di allocazione:

- Primo disponibile → Si cerca una data unit libera ogni volta partendo dall’inizio del file system

- Prossimo disponibile → Si cerca una data unit libera partendo dall'ultima locazione allocata
- Più adatto → Si cercano data unit libere che possano contenere consecutivamente il file

Attraverso l'analisi del content category troviamo:

- Data unit view → Ricerca di settori noti del FS
- Logical file system searching → Ricerca la presenza di un contenuto specifico nei data unit
- Data unit allocation status → Ricerca nei data unit non allocati
- Consistency check → Ricerca di data unit non referenziati in metadata category

METADATA CATEGORY

Descrivono i file presenti in "content category" dando informazioni temporali e indirizzo delle data unit allocate per il file.

Con l'analisi ricerchiamo maggiori informazioni sui file e ricerchiamo i file stessi in base agli attributi descritti dalla categoria (es: file creati dopo una data x).

- Logical file address → Indirizzo di parte del file allocata nella data unit (contenuto nella data unit)
- 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 che occupa meno data unit. Ci sono 3 livelli di compressione:

- Soli dati nel file
- Tutto il file (creazione di un nuovo file)
- Compressione eseguita dal file system (invisibile lato utente)

FILE NAME CATEGORY

Rappresenta il nome associato a ciascun file.

- File recovery → Recupero dei file cancellati ricercando i file name con lo stato non allocato

APPLICATION CATEGORY

Dati non essenziali al file system ma sono più efficienti se conservati in quest'ultimo.

- Journaling → Conservazione delle modifiche da effettuare ed effettuate sui metadati per evitare l'inconsistenza.

L18 - L'Analisi - File System (Pt .2)

FAT File System

Un tipo particolare di file system che non contiene un'application category e le cui data unit sono chiamate "cluster" al posto di "settori".

FILE SYSTEM CATEGORY

- FSINFO (fat32) → Area di cluster liberi riservata al boot sector
- Boot sector → Primo settore:
  - Reserved area → Settore 0 → In Fat12 ha dimensione di 1 settore. In Fat32 ha dimensione variabile
  - FAT Area → Successiva all'area riservata → Dimensione di Nr.FAT * SizeFAT
  - Data Area → Dopo la FAT Area

Tra i dati non essenziali nel boot sector abbiamo il nome di OEM, il seriale del volume e il Label del file system (fat, fat12, fat16, fat32).

Attraverso l'analisi del file system category possiamo:

- Recuperare informazioni sul layout
- Controllare possibili dati nascosti
- Confrontare il boot sector e il suo backup

CONTENT CATEGORY

Mantiene il contenuto di file e directory. I cluster sono rappresentati da 2^x settori (max 32 kb)

FAT

Inditifica lo stato di allocazione dei cluster ed è successivo al cluster del file (cluster chain). Ogni entry è di uguale dimensione ed è a indirzzamento diretto:

- Prima entry → indirizzo 0
- Indirizzo entry = Indirizzo cluster (es: entry[10] = cluster[10])
  - Entry[0] → Informazione del media
  - Entry[1] → Dirty status
  - Entry[n] → Cluster[n]

In ogni entry è quindi presente un'area FAT che identifica lo status e le posizioni dei cluster contenuti in una "data area".

Come calcoliamo il settore dato il cluster?

$$\text{Settore} = (\text{cluster\_address} - 2) * \text{n\_settori\_cluster} + \text{settore\_cluster\_2}$$

ESEMPIO: $(75 - 2) * 2 + \text{settore\_cluster\_2}$, dove:

$$\text{settore\_cluster\_2} = \text{dim\_ReservedArea} + \text{dim\_FatArea}$$

Sapendo che dim_ReservedArea = 38 e dim_FatArea = 1594 avremo:

$$(75 - 2) * 2 + 1632 = 1778$$

METADATA CATEGORY

Mantiene informazioni su file e directory con l'indirizzo del primo cluster. Fa uso di una Parent directory:

- Directory entry → 32 kb (file, directory)
- Posizionata nella Data Area (Cluster)
- File name category → Nome file (8 caratteri) + Estensione (3 caratteri)

Come informazioni non essenziali mantiene le informazioni temporali:

- Data di creazione
- Data di modifica
- Data di accesso

FILE NAME CATEGORY

Serve a mappare i metadati con un'etichetta (filename).

L19 - L'Analisi - I File System (Pt. 3)

NT File System

Il New Technology File System (NTFS) è un file system all'interno del quale ogni cosa è rappresentata da un file:

- $MFT → Master File Table

- $MFTMirr → Backup della MFT
- $Boot → Boot sector
- $Volume → Informazioni di volume
- $Bitmap → Stato di allocazione dei cluster
- $AttDef → Definizione degli attributi
- $BadClus → Eleneco dei cluster danneggiati
- $Secure → Descrittore di sicurezza
- $130 → Index

MASTER FILE TABLE

Contiene informazioni sul file e directory: ogni file ha almeno una entry (File Record) di 1024 byte.

Il boot sector è contenuto nel cluster iniziale della MFT.

Una entry MFT ha:

- Dimensione → 1024 byte
  - Header: 42 byte
  - Attributi: strutture dati
- Signature → File/BAD
- Stato di allocazione → Attributo $BITMAP nella entry[0] $MFT
- Indirizzo sequenziale → 48bit (File Number)
- Numero Sequenziale → 16 bit (contatore allocazione)

Le prime 12 entry MFT costituiscono il **FILE SYSTEM METADATA.** Sono, quindi, file contenenti dati per l'amministrazione del FS.

ATTRIBUTI

Ogni attributo contiene:

- Header → Descrive l'attributo
  - ID → Identificatore univoco nell'entry (16 bit)
  - Type ID → Identificatore tipo attributo
  - OFFSet → Attribute content
- Attribute content:
  - Residente → Posizionato nella stessa entry
  - Non residente → Posizionato in cluster esterni (Cluster Run)

Quando una entry riesce a contenere/descrivere tutti gli attributi per uno specifico file è detta "Base MFT Entry" costituita da:

- $STANDARD_INFORMATION
- $ATTRIBUTE_LIST
- $FILE_NAME
- $[ID3]

FILE SYSTEM METADATA

Spazio che contiene il boot sector (cluster iniziale). Nella Entry[0] di MFT sono presenti i cluster usati ($DATA) e lo stato di allocazione delle entry ($BITMAP).

- MFTMirr File → Copia di backup della MFT dove le prime 4 entry sono:

    - $MFT, $MFTMirr, $LogFile, $Volume
    - Contenuto nella Entry[1] di MFT
- Boot File → Contenuto nel boot sector:
    - Dimensione del cluster
    - Nr. di settori del FS
    - Presente nella Entry[7] di MFT
- Volume File → Contiene le informazioni sul volume (etichetta e versione). Presente nella Entry[3] di MFT:
    - $VOLUME_NAME → Nome in UNICode del volume
    - $VOLUME_INFORMATION → Versione di NTFS e dirty status
    - $DATA → 0 Byte
- AttrDef File → Definisce gli attributi (nomi, type ID) ed è contenuto nella Entry[4] di MFT.

Attraverso l'analisi del file system category possiamo:

1. Processare il primo settore del File System: Boot sector
2. Processare la MFT[0]
3. Processare $AttrDef
4. Processare le altre entry MFT

CONTENT CATEGORY

Ha all'interno il contenuto degli attributi (residenti e non residente)

- $Bitmap File → Contiene informazioni sullo stato di allocazione dei cluster:
    - Bit[x] = Cluster[x]:
        - Bit[x]=1 → Cluster x allocato
        - Bit[x]=0 → Cluster x non allocato
    - Contenuto nella Entry[6] di MFT
- $BadClus → Traccia i cluster con settori danneggiati. Contenuto nella Entry8] di MFT.
    - $DATA = $Bad

Il Layout della content category è diverso a seconda della versione NTFS:

- Zona MFT → Settori consecutivi riservati per MFT
- Boot Sector → Primo settore

L20 - L'Analisi - I File System (Pt. 4)

PICCOLO RECAP

- NTFS Gestisce tutto con i file
- Nella MFT sono presenti le prime 12 Entry.
- Entry MFT contiene:
    - Header MFT → 42 Byte
    - Attributi → Header, Content (residente e non residente: cluster run)
- File System Category → File System Metadata File:
    - $MFTMirr

    - $BootFile
    - $Volume
    - $AttrDef
- Content Category:
    - Attributo $Data
    - FS Metadata File → $BitMap e $BadClus

METADATA CATEGORY

I metadati sono reperibili dagli attributi:

- $STANDARD_INFORMATION → Esiste per ogni file e directory e contiene i metadati principali tra cui:
    - Informazioni temporali → Quattro valori temporali (timestamp)
        - Data di creazione
        - Data di ultima modifica
        - Data di ultima modifica MFT (modifica dei metadati)
        - Data di ultimo accesso
    - Proprietà
    - Sicurezza e quota
- $FILE_NAME → Ogni file e directory ha almeno un attributo di questo tipo. Ha dimensione di 66 Byte + la lunghezza del nome e fa riferimento alla Parent Directory.
- $DATA → Impiegato per memorizzare qualsiasi forma di dati (non ha formato e valori definiti). La dimensione è ≥ 0 Byte (o > 700 Byte se non residente)
- $ATTRIBUTE_LIST → Lista degli attributi nella entry. Si ha quando un file necessita di più entry per gli attributi. Il tipo di attributo è contenuto nella posizione della entry che lo contiene.
- $SECURITY_DESCRIPTOR → Descrive i criteri di controllo dell'accesso che devono essere applicati a un file o una directory
- $SECURE File → Descrive i criteri di controllo dell'accesso che devono essere applicati a un file o una directory. Contenuto nella Entry[9] di MFT con due indici e un attributo.

Sono presenti anche degli algoritmi di allocazione:

- Allocazione delle entry MFT:
    - Primo disponibile (dalla entry 24)
    - Allocato>Non allocato → Cambio della flag "in uso"
    - Non allocato>allocato → Pulizia della entry
- Allocazione degli attributi:
    - Riduzione dell'ultimo attributo
    - Crescita dell'attributo: residente>non residente

L'aggiornamento delle informazioni temporali ha effetto su:

- $FILE_NAME → Aggiornamento, creazione, spostamento del file
- $STANDARD_INFORMATION:
    - Data di creazione → Creazione di nuovo file o copia
    - Data ultima modifica → Variazione di DATA, INDEX_ROOT o INDEX_ALLOCATION
    - Data di ultima modifica MFT → Modifica degli attributi

- Data di accesso → Viene fatto accesso alla entry

Analizzando la metadata category è possibile:

- Individuare una entry MFT (tramite il boot sector)
- Elaborare il contenuto della entry:
  - STANDARD_INFORMATION
  - DATA → Non residente: processare la RUNLIST
  - FILE_NAME
  - Elaborazione delle possibili entry secondarie → ATTRIBUTE_LIST

FILE NAME CATEGORY

Mette in correlazioni i nomi (indici) ed è una raccolta di strutture dati ordinate per chiave.

Ha una struttura B-TREE con i nodi:

- $INDEX_ROOT → Radice dell'albero
- $INDEX_ALLOCATION → Indici utilizzati

Nella Root Directory (contenuta nella entry[5] di MFT con nome ".") risiedono tutti i file system metadata file.

APPLICATION CATEGORY

- Disk Quotas ($QUOTA) → Da supporto alle quote di spazio sul disco (limitare lo spazio allocato a un utente) ed è contenuto nel registro di windows.
- Logging ($LogFile) → Consente di mantenere il File System in uno stato di consistenza. Contenuto nella Entry[2] di MFT

L'analisi dell'application category consente di recuperare i file eliminati:

- File eliminato dall'index directory
- Recupero entry MFT → Attributo FILE_NAME (parent directory)
- Controllare la presenza di ulteriori $DATA

L21 - L'Analisi - I Sistemi Operativi

Microsoft Windows

UTENTI

- Account locali → Accesso al singolo sistema con autenticazione locale.
- Account di dominio → Accesso a tutti i sistemi attestati con autenticazione tramite Domain Controller
- Account online → Accesso a tutti i sitemi attestati con autenticazione tramite account Microsoft

REGISTRO DI SISTEMA

Contiene le impostazioni del SO e dei programmi installati.

Ha una struttura ad albero con 5 sotto-alberi principali (hive):

- HKEY_CLASSES_ROOT → Associazione: estensione file - applicazione
- HKEY_USERS → Impostazioni di tutti i profili utente configurati nel sistema
- HKEY_CURRENT_USER → Puntatore al profilo utente presente in HKEY_USERS loggato nel sistema
- HKEY_LOCAL_MACHINE → Configurazione del computer
- HKEY_CURRENT_CONFIG → Puntatore alla corrente configurazione situata in "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current"

Ogni nodo dell'albero è rappresentato da una chiave (coppia di valori) e delle sottochiavi

Analizzando il registro di sistema con strumenti come RegEdit è possibile risalire a:

- Configurazioni dell'utente
- Dispositivi USB
- Informazioni temporali

THUMBNAILS

Sono miniature delle immagini presenti nell cartelle, e possono essere analizzate anche per immagini non più presenti (thumbs viewer, thumbcache viewer).

SHELLBAG

Sono personalizzazioni utente della visualizzazione del contenuto delle cartelle:

- BagMRU → Storico di tutte le cartelle visualizzate dall'utente
- Bags → Impostazioni di visualizzazione delle cartelle contenute in BagMRU

Per analizzare la ShellBag:

1. Si segue la lista delle cartelle presenti in MRUListex e si seleziona il valore della chiave relativa
2. Si esegue la sottochiave della cartella → Si visualizza la chiave MRUListex e si continua ricorsivamente la sua esplorazione

Le informazioni ottenibili sono:

- Bag Number → Sottochiave Bags che contiene le preferenze dell'utente (Nodeslot)
- Registry key last write time → Data primo accesso o ultima modifica della cartella
- Folder name → Nome della cartella

APPLICATION DATA

Contiene le impostazioni dei programmi utilizzati dall'utente e file temporanei. Attraverso l'analisi è possibile avere un quadro complessivo dell'utilizzo del computer da parte di un utente:

- Posta elettronica
- Cache
- Cronologia
- Log
- Configurazioni

FILE SWAP

Estensione della RAM nel PageFile.sys. Il file Hiberfil.sys congela la ROM in fase di sospensione/ibernazione

L'analisi ha vantaggi e svantaggi:

VANTAGGI

- Diffuso
- Documentato
- Supportato

SVANTAGGI

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

MacOS

CONFIGURAZIONE

- NetInfo (DB a oggetti) → Controlla diverse configurazoni del SO:
  - Entry statiche di rete

    - Definizione di tutti gli utenti
- Open Directory → Servizio di directory che getisce le autenticazioni
- Cifratura:
    - FileVaul → Cifratura della home directory
    - FileVault 2 → Full disk encryption
- File Swap → Estensione della RAM. Il congelamento della RAM in fase di sospensione è salvato in un file “sleepimage”
- Portachiavi → Accentramento delle credenziali utente. Accesso tramite API con cifratura AES-128

Dato l’elevato numero di tecnologie proprietare l’analisi deve essere svolta utilizzando un sistema OSXm attraverso strumenti come:

- Blacklight → Toolkit forense
- MacQuisition → Tool di acquisizione forense
- Apple hdiutil → Tool da riga di comando

La gran parte dei file da analizzare sono nella Home Directory Utente.

Linux

I sistemi operativi Linux sono distribuzioni basate su kernel GNU/Linux con componenti:

- Kernel
- Librerie di sistema
- Tool di base

SISTEMA

- Multiente e Multitasking
- Struttura rigida del file system
- Sistema di permessi di file e directory (l’utente root non ha limi di permessi):
    - r: permesso di lettura
    - w: permesso di scrittura
    - x: permesso di esecuzione (file) o di accesso (directory)

LOG

- Syslog → Sistema di gestione dei log
- Posizione dei log: /var/log
    - Messages → Eventi relativi alla macchina
    - wtmp → Registrazione degli accessi
- Logfinder → Ricerca di tutti i file log

CONFIGURAZIONI

- Posizione → /etc (configurazione di default) o file nascosti nella home directory utente (configurazioni personalizzate):
    - Inittab → File di configurazione del boot
    - Passwd → Elenco degli utenti
    - Shadow → Password degli utenti

HOME DIRECTORY

- Tipi di utente:
  - Root → Amministratore di sistema
  - Utente comune
- Directory disponibili all’utente
  - /usr/local/bin: file dei programmi utilizzabili dall'utente
  - /tmp: file temporanei
  - /home/[nome_utente]: directory principale dell'utente
    - Dati dell'utente: la maggior parte dei file creati e gestiti dall'utente
    - Shell history: lista dei comandi impiegati dall'utente
    - Cache
    - File di configurazione: configurazioni personalizzate di programmi

/VAR

Contiene i dati che cambiano durante la normale esecuzione del sistema (specifico per ogni sistema).

ANALISI

L’analisi di Linux va eseguita sulle cartelle /home, /etc e /var. L’analisi live controlla:

- inittab → Controlla tutti i servizi eseguiti in fase di boot
- Autenticazione → Verifica la configurazione PAM, kerbero e openLDAP
- /etc/fstab → Verifica il montaggio del File System all’avvio

---

L22 - Mobile Forensics

OVERVIEW

Vanno considerati i seguenti fattori:

- Presenza di memorie diverse (interno o esterna)
- Presenza di SIM CARD
- Presenza di un IMEI/MEID

GSM

Global System for Mobile communications

- IMEI → Codice univoco del dispositivo all’interno della rete mobile
- SIM Card → Subscriber Identity Module
  - ICCID → Nr. seriale
  - IMSI - Identificativo nella rete

CDMA

Code Division Multiple Access

- MEID → Codice univoco del dispositivo all’interno di una rete mobile
- No SIM Card

Le Fasi

RACCOLTA

Le fasi della raccolta sono le seguenti:

1. Disabilitare tutte le connessioni per evitare Remote Wipe e sovrascrittura di informazioni presenti:
   a. Modalità aereo
   b. Faraday Bag

2. Sbloccare il dispositivo
    a. iOS → Max 10 tentativi → PassCode a 6 cifre (default)
    b. Android → PassCode ≥ 4 cifre
    c. Applicazioni di sicurezza
    d. SIM Card → PassCode (4 cifre) o PUK (8 cifre)
3. Spegnere il dispositivo

ACQUISIZIONE

- Strumenti → Cellebrite UFED
- Acquisizione della memory card (la prima cosa da acquisire)
- SIM Card → SIM, Micro SIM, Nano SIM
    - Acquisizione di Rubrica, SMS, identificativi
    - Strutturata in Master File, Dedicated File, Elementary File

TIPI DI ACQUISIZIONE

- Manual Extraction → Repertazione fotografica del contenuto
    - Svantaggi → Processo lungo con rischio di modifica o cancellazione dei dati e visualizzazione limitata delle informazioni
    - Limiti → Display non funzionante e codice di sblocco
- Logical Extraction → Estrazione dei dati tramite API del dispositivo
    - Limiti → I risultati dipendono dall'API e sono solo parziali
- File System Extraction → Estrazione dei file tramite API del dispositivo
    - Risultato → L'output va processato per visualizzare i dati contenuti in DB SQLite
    - Limiti → I risultati dipendono dai permessi con cui vengono fatte le richieste (completo o parziale)
- Physical Extraction → Copia bit a bit della memoria del dispositivo
    - Boot loader → Codice immesso nella fase di avvio del dispositivo per avvia l'estrazione dati
    - Agent → Tool installato nel SO
    - Advanced ADB → Android Debug Bridge
    - Risultato → L'output va processato per visualizzare i dati contenuti recuperando anche i file cancellati (carving)
    - Limiti → Produttore del dispositivo, chipset, versione del SO e patch di sicurezza
- Chip Off → Estrazione fisica del chip dalla scheda madre
    - Limiti → Dispositivo cifrato

ANALISI

Sistemi operativi:

- OS Android → Migliaia di produttori e modelli con kernel open source
- Apple iOS → Pochi modelli con kernel closed source

Le applicazioni estendono le funzionalità del SO e rappresentano le principali interazioni con l'utente.

Lo strumento principale utilizzato per l'analisi è UFED Physical Analyzer, con l'aggiunta di alcun plugin.

L23 - La Fase Finale

Le fasi finali dell'analisi forense sono:

- Interpretazione
- Documentazione
- Presentazione

LA PROVA DIGITALE

- PRO → Duplicazione
- CONTRO → Facilmente Corruttibile

ACCERTAMENTI

- Ripetibile → Agire in modo da non alterare la prova, documentando ogni azione compiuta su di essa e ponendo la controparte in condizione di replicare quanto fatto

RELAZIONE TECNICA

Ha come base di partenza il quesito e deve descrivere gli strumenti hardware e software impiegati, delle azioni che hanno portato e non portato risolutati e ha come scopo quello che chiunque deve poter giungere alle medesime conclusioni.

ESEMPIO: Indagine pedopornografica

1. Ricerca di immagini residenti
2. Ricerca di immagini in archivi compressi e posta elettronica
3. Ricerca di programmi P2P
4. Ricerca di file cancellati
5. Ricerca di periferiche di archiviazione
6. Analisi steganografica

Descrizione dettagliata di hardware e software impiegato:

- Parte descrittiva → Dettagliata e accurata (documentazione fotografica)
- Parte valutativa → Motivazioni, descrizione dell’iter logico e giuridicamente non vincolante

La forma deve essere chiara e intelligibile e divisa in 4 parti:

- Parte epigrafica → indicazione degli estremi del PP, PM, Giudice, descrizione dell’incarico, parti presenti a un accertamento, etc.
- Parte descrittiva → Illustrazione degli accertamenti e o ricostruzioni compiuti
- Parte valutativa → Risposta ai quesiti con motivazione esaustiva delle conclusioni
- Parte riassuntiva → Esposizione sintetica della risposta a ogni quesito