La copia forense

- [ ] deve essere sempre eseguita con un write blocker
- [x] è una duplicazione dei dati eseguita in modo tale da garantire la ripetibilità della successiva operazione di analisi
- [x] è una qualunque copia di dati purché rispetti le caratteristiche di validazione e preservazione
- [x] una duplicazione dei dati eseguita in modo tale da garantire sempre la ripetibilità dell'operazione di copia
- [ ] deve essere sempre eseguita con tool forensi

La copia forense

- [ ] deve essere sempre eseguita con un write blocker
- [x] è una duplicazione dei dati eseguita in modo tale da garantire la ripetibilità della successiva operazione di analisi
- [x] è una qualunque copia di dati purché rispetti le caratteristiche di validazione e preservazione
- [x] una duplicazione dei dati eseguita in modo tale da garantire sempre la ripetibilità dell'operazione di copia
- [ ] deve essere sempre eseguita con tool forensi

il seguente comando: dd if=/mnt/sda.dd bs=2048 | tee /dev/sda | md5sum > /mnt/sda.hash

- [ ] produce una immagine divisa in parti da 2048MB
- [ ] il comando non è corretto
- [x] non produce una copia forense
- [x] esegue la copia della sorgente "sda"
- [x] esegue il calcolo dell'hash on-the-fly dell'immagine "sda.dd"

FTK Imager

- [x] è uno strumento per la produzione copie forensi
- [x] **non fa uso dell'hashing on-the-fly**
- [ ] non permette di segmentare/splittare il file immagine
- [ ] esegue copie forensi solo di tipo "full disk"
- [x] non permette la scelta del tipo di hash da calcolare

il formato DD/RAW:

- [x] non conserva nei metadati il calcolo dell'hash
- [ ] conserva i metadati del reperto sorgente
- [ ] permette la compressione
- [x] può contenere la copia logica di una cartella\directory
- [ ] è un formato della famiglia "Expert Witness Disk Image Format"

Nell'algoritmo di SHA-1 se il messaggio di input M è di 1024bit, dopo il padding avremo che M' sarà costituito da:

- [ ] 2 blocchi da 512bit
- [x] 64bit per la lunghezza del messaggio
- [x] un bit a "1" al 1025° bit
- [x] nessun bit di padding
- [ ] 1024bit

I Toolkit

- [x] processano\elaborano il contenuto disk image
- [ ] non permettono di ottenere diverse visualizzazioni dei dati
- [ ] non hanno ancora sviluppato una ricerca tramite hash
- [x] eseguono in maniera automatizzata tutta l'analisi
- [x] permettono di eseguire la classificazione bad extension confrontando l'estensione del file con la signature in esso presente

Autopsy

- [x] permette la selezione dei file di interesse solo tramite "tag"
- [ ] Il modulo "Encryption Detection" permette trovare e decifrare i file protetti
- [x] il modulo "Hash Lookup" permette di impostare sia una lista di "Ignorable File" e sia di "Notable File"
- [ ] il "file carving" viene eseguito su tutto il disk image
- [ ] non permette l'aggiunta di ulteriori moduli di analisi

Autopsy

- [ ] Il modulo "Exif Parser" dipende dal modulo "Embedded File Extractor"
- [ ] Pemette solo una configurazione "single user"
- [x] **Il modulo "Virtual Machine Extractor" permette di generare una macchina virtuale dalla copia forense**
- [ ] Il modulo che si preoccupa di estrarre informazioni dal cestino di sistema "RecycleBin Activity"
- [x] **Il modulo "Encryption Detection" permette di evidenziare possibili file protetti**

Partizionamento DOS

- [x] Il settore contenente l'MBR termina con una signature
- [ ] L'MBR è costituito da almeno quattro settori
- [x] rispetto al partizionamento GPT può contenere un numero di partizioni inferiore
- [ ] può contenere al massimo 4 secondary extended partition
- [ ] Il campo "Starting LBA Address", presente nella partition table, indica il settore iniziale della partizione

Nel File System

- [ ] le informazioni temporali sono definiti dati essenziali
- [x] In "Content Category" i dati sono organizzati in "Data Unit"
- [ ] il "File System Category" comprende le informazioni sull'indirizzo delle "Data Unit"
- [x] **In "Application Category" sono presenti i dati essenziali per alcune funzionalità del File System**
- [x] La strategia di allocazione del "primo disponibile" ricerca una "Data Unit" libera partendo dall'inizio del FileSystem

Nel FAT File System

- [x] Le data unit si chiamano cluster
- [x] Il layout è costituito da una Reserved Area, FAT Area, una Data Area e una Cluster Area
- [ ] Nel FAT12/16 la root directory ha dimensione dinamica
- [x] Lo stato di allocazione dei cluster è conservato nella strattura FAT
- [ ] I cluster inziano con indirizzo uno

Nel NT File System

- [ ] Ad esclusione delle strutture dati del FileSystem tutto il resto è gestito come file
- [x] Il File $BadClus ha un attributo $DATA della stessa dimensione del FileSystem
- [ ] La dimensione del cluster è indicato nella Tabella MFT
- [ ] Una Entry MFT può contenere solo un attributo di tipo $DATA
- [ ] L'attributo in una MFT Entry di tipo "non residente" indica che il file che descrive è stato cancellato

Nell'analisi dei Sistemi Operativi

- [ ] In un SO Windows il file SAM contiene sempre l'elenco di tutti gli account utente che possono avere accesso al sistema
- [x] **In SO Apple il FileVault offre la funzionalità di cifratura**
- [ ] In SO Windows i thumbnail del sistema sono sempre coerenti con i file residenti
- [ ] Il SO Windows è il sistema meno documentato
- [ ] Il PageFile.sys del SO Apple si trova nella root del disco

Nella Mobile Forensics

- [ ] La Manual Extraction è il metodo più veloce per eseguira una copia dei dati presenti
- [x] La Manual Extraction si esegue fotografando il contenuto del dispositivo
- [ ] La Physical Extraction può essere eseguita su quasi la totalità dei dispositivi

Per preservazione si intende che

- [x] l'hash della copia forense dovrebbe coincidere con quello calcolato dalla medesima copia dopo la fase di analisi
- [ ] la copia forense sarà immodificabile
- [x] l'hash della copia forense coinciderà con l'hash calcolato da una successiva copia forense
- [x] l'hash ricalcolato sulla copia forense varierebbe alla minima alterzione della copia stessa
- [ ] i dati della copia forense sono identici ai dati originali

Nel FAT File System

- [ ] Le data unit si chiamano settori
- [x] Le entry del FAT sono a dimensione variabile
- [x] Nel FAT32 la root directory ha dimensione dinamica
- [x] Lo stato di allocazione dei cluster è indicato con ZERO (non allocato) o con UNO (Allocato)
- [x] Le prime due entry del FAT non sono utilizzate per i cluster

Nel NT File System

- [ ] Le Entry MFT vengono pulite non appena viene settato a ZERO il flag in uso
- [x] Nel File $BitMap è indicato lo stato di allocazione di ciascun cluster
- [x] La dimensione del cluster è indicato nella Tabella MFT
- [ ] Una Entry MFT può contenere solo un attributo di tipo $DATA
- [ ] L'attributo in una MFT Entry di tipo "non residente" indica che il file che descrive è stato cancellato

L'indagato/imputato

- [ ] può rinunciare a nominare un difensore
- [x] **può farsi assistere da un consulente tecnico quando viene eseguito un accertamento tecnico**
- [ ] ha l'obbligo di presenziare in udienza
- [ ] L'indagato assume il ruolo di imputato dopo la sentenza di primo grado
- [x] può produrre memorie difensive nella fase delle indagini preliminari

il seguente comando: dd if=/dev/sda of=/mnt/sda.dd conv=noerror,sync

- [ ] è errato in quanto non è stato specificato il "blocksize"
- [x] è corretto
- [x] non è completo per eseguire la copia forense in quanto manca il calcolo dell'hash
- [ ] non è corretto poiché le opzioni "noerror" e "sync" non andrebbero combinate
- [ ] non è corretto per altri motivi

il formato DD/RAW:

- [x] non conserva il calcolo dell'hash
- [ ] conserva i metadati del reperto sorgente
- [ ] permette la compressione
- [ ] può contenere la copia logica di una cartella\directory
- [ ] è un formato della famiglia "Expert Witness Disk Image Format"

La c.d. "preview"

- [ ] permette di eseguire una analisi completa
- [ ] il suo uso è indicato nel codice di civile
- [x] Dovrebbe essere compiuto da tecnici specializzati poiché vi è rischio di alterazione della prova
- [x] è particolarmente utile ad individuare le fonti di prova
- [ ] può essere eseguito solo con l'ausilio di un writeblocker

Nel File System

- [x] I dati non essenziali possono non essere coerenti
- [x] In "Content Category" i dati sono organizzati in "Data Unit"
- [ ] il "Metadata Category" comprende le informazioni sul layout
- [ ] il "Logical Volume Address" è l'indirizzo di un settore calcolato basandosi sull'inizio del disco
- [x] lo "Slack Space" indica una "Data Unit" non più allocata

In Analisi, FTK Imager

- [ ] Riconosce tutti i tipi di File System
- [ ] permette di visionare\analizzare solo Disk Image
- [ ] Permette di visualizzare solo i file residenti
- [x] Può essere impiegato anche come strumento per la c.d. preview
- [x] Permette di esportare i file di interesse

L'algoritmo di Hash MD5

- [ ] processa il messaggio in blocchi di 1024bit
- [ ] è costituito da 3 round e 3 funzioni logiche
- [x] rispetto a MD4 fa uso di 62 costanti in più
- [x] l'output è un digest a 128bit
- [ ] il terzo round è composto da 48 operazioni

Guymager

- [ ] è uno strumento per la produzione di copie non di tipo forense
- [x] **non fa uso dell'hashing on-the-fly**
- [ ] non permette di segmentare/splittare il file immagine
- [ ] esegue copie forensi solo di tipo "full disk"
- [ ] non permette la scelta del tipo di hash da calcolare

il PM conferisce incarico ai sensi dell'art. 360 cpp

- [ ] Quando occorre agire in assoluta ugenza a causa della deperibilità del reperto
- [ ] Solo quando non vi è il rischio che l'elemento probatorio da analizzare possa venire alterato o distrutto in fase di accertamento
- [x] Indica al Consulente Tecnico che deve eseguire un accertamento tecnico non ripetibile
- [ ] chidendo autorizzazione al GIP (Giudice Indagini Preliminari)
- [x] Quando vuole dissequestrare il bene oggetto di accertamento tecnico

Partizionamento DOS

- [x] Il settore contenente l'MBR termina con una signature
- [ ] può conterene al massimo 8 partizioni
- [ ] Nelle entry della "Partition Table" è sempre indicato il tipo di partizione
- [x] La 'Partition Table' è costituita da quattro entry da 16byte
- [ ] Il campo "Starting LBA Address", presente nella "Partition Table", indica il cluster iniziale della partizione

I Toolkit

- [x] processano\elaborano il contenuto disk image
- [ ] non permettono di ottenere diverse visualizzazioni dei dati
- [x] permettono di eseguire una ricerca tramite hash
- [ ] eseguono in maniera automatizzata gran parte dell'analisi
- [ ] permettono di eseguire il "file carving" ricercando la signature del file

Nella Mobile Forensics

- [x] La Physical Extraction dipende solo dalla versione del SO e dai livelli di patch di sicurezza
- [x] Nella File System Extraction si ottengono i DB così come sono prensenti nel dispositivo
- [ ] La Manual Extraction può essere sempre impiegata
- [ ] Nella File System Extraction si ottiene sempre tutto il contenuto presente nel dispositivo
- [ ] La logical Extraction dipende dal chipset del dispositivo

Nell'analisi dei Sistemi Operativi

- [x] L'analisi dei thumbnail viene eseguita per avere informazioni sulle immagini non più presenti
- [ ] Il SO Windows registra molti più log di un SO Linux
- [ ] Lo Swapfile in un SO Windows è posizionato nel percorso /private/var/vm/
- [ ] Il PageFile.sys rappresenta un dump della RAM
- [ ] Il SO Windows è molto più rigido nella gestione della struttura del File System

Autopsy

- [x] Il "Central Repository" permette di rapportare il caso in esame con i precedenti casi già elaborati
- [ ] Pemette solo una configurazione "single user"
- [x] Il disk image viene processato tramite dei "Ingest Modules"
- [x] Il modulo che si preoccupa di estrarre informazioni dal cestino di sistema è "RecycleBin Activity"
- [ ] Il modulo "Encryption Detection" permette trovare e decifrare i file protetti

il PM conferisce incarico ai sensi dell'art. 360 cpp

- [x] Quando occorre agire in assoluta ugenza a causa della deperibilità del reperto
- [x] Quando sussiste il rischio che l'elemento probatorio da analizzare possa venire alterato o distrutto in fase di accertamento
- [ ] indica al Consulente Tecnico che deve eseguire un accertamento tecnico ripetibile
- [ ] Quando il PM vuole fornire la più ampia garanzia alle parti escludendo il rischio di successive eccezioni
- [x] Quando vuole dissequestrare il bene oggetto di accertamento tecnico

Quali caratteristiche sono proprie della Persona Offesa

- [x] In determinati casi può ritirare la querela
- [ ] è colui che assiste alla commisione di un reato
- [ ] Può prendere parte solo alla fase di giudizio
- [x] Può sporgere denuncia

Nella fase di identificazione, la preview...

- [x] è una fase in cui in alcuni casi vi è il rischio di alterare il reperto
- [ ] deve essere eseguita realizzando la copia forense
- [x] può essere eseguita su di un sistema accesso
- [ ] non devono essere accesi i dispositivi rinvenuti spenti
- [ ] non è particolarmente utile ad individuare le fonti di prova

Copia forense - validazione e preservazione - di Mario Gabriele Carofano

VALIDAZIONE: l'hash calcolato dalla copia originale e l'hash calcolato dalla copia forense sono uguali al termine dell'esecuzione della copia.

PRESERVAZIONE: dopo aver eseguito delle operazioni di analisi sulla copia forense, la proprietà di preservazione garantisce che l'hash rimanga sempre lo stesso (con il passare del tempo).

Comando 'dd': permette di eseguire la copia forense di un disco e salvarlo in un file immagine la cui estensione è .dd oppure utilizza un codice numerico che viene incrementato per ogni file restituito se la copia viene divisa in più file immagine (es. .00, .01, ...).

Parametri del comando 'dd':

IF: indica la directory del disco in input di cui eseguire la copia forense

OF: indica la directory nel quale andare a salvare la copia il file immagine della copia forense in output

BS: indica la dimensione dei blocchi di memoria (block size). Il valore di default è 512 byte.

CONV: permette di inserire dei parametri aggiuntivi al fine di personalizzare l'elaborazione

- noerror: l'elaborazione continua anche se viene riscontrato un errore in lettura
- sync: le dimensioni dei blocchi di memoria del disco originale e della copia forense devono sempre essere sincronizzati, quindi i blocchi di memoria non letti sono sostituiti con blocchi NULLs

SKIP: a partire dal primo blocco di memoria della sorgente, permette di saltare la lettura di un numero 'n' di blocchi di memoria

COUNT: il valore 'n' di questo parametro indica all'elaborazione il numero di blocchi da leggere nel disco sorgente (i comandi SKIP e COUNT sono utilizzati per partizionare i file immagine della copia forense).

SPLIT: al posto dei parametri SKIP e COUNT, è possibile utilizzare anche questo parametro per il partizionamento del file immagine in output

-D: utilizzando questo parametro, l'estensione di ogni singolo file che è parte della copia forense ha come estensione un numero che si incrementa

-B: utilizzando questo parametro seguito da un numero e una lettera (K, M, G, T, ...), viene indicata la dimensione massima di ogni singolo file in output

Verifica della proprietà di validazione:
Comando md5sum: permette di calcolare l'hash di un file in ingresso mediante l'algoritmo MD5. La sua sintassi prevede l'inserimento della directory sorgente nel quale di trova il file o disco di cui calcolare l'hash e, poi, l'inserimento della directory nel quale memorizzare l'output dell'algoritmo.

Metodo n.1: calcoliamo prima l'hash del disco sorgente, poi eseguiamo la copia forense di tale disco e, infine, calcoliamo l'hash della copia forense in output e verifichiamo che i due codici siano uguali.

Metodo n.2: dopo aver calcolato l'hash del disco sorgente, calcoliamo l'hash della copia forense durante la sua elaborazione utilizzando il comando TEE, che ha il compito di duplicare lo stream in output al comando dd in modo da poterlo utilizzare in due modi diversi (generazione del file immagine e calcolo dell'hash con md5sum).

Comando DC3DD: è una patch del comando dd che introduce alcuni miglioramenti sulla semantica dei parametri e permette l'applicazione dell'algoritmo di hashing direttamente nell'elaborazione della copia.

Parametri del comando DC3DD:
IF: è lo stesso parametro già visto nel comando DD

OFS: indica la directory del file immagine. Questo specifico parametro permette già durante l'elaborazione il partizionamento dell'output in più file di dimensione massima fissata

OFSZ: indica la dimensione massima di una parte del file immagine

BUFSZ: corrisponde al parametro BS già visto nel comando DD

HASH: indica quale algorimo di hashing deve essere

utilizzato (es. MD5, SHA256, SHA1, ...)

LOG: indica la directory di dove salvare un file di log (report) completo riguardante l'elaborazione della copia forense

VERB: assegnando a questo parametro il valore ON, si indica di voler ottenere un report molto più dettagliato dell'elaborazione (verbose)

REC: assegnando a questo parametro il valore OFF, si indica che l'elaborazione si interrompe in caso di errore di lettura di un blocco di memoria

HOFS: permette di calcolare l'hash per ogni singolo file immagine della copia forense generato dall'elaborazione

Computer Forensics

Accertamenti tecnici art 359 cpp: il PM può avere la necessità di svolgere accertamenti tecnici, che comportano specifiche conoscenze scientifiche, tecniche o artistiche, che esulano dalle competenze possedute dall'organo inquirente
Il PM può avvalersi/nominare un Consulente Tecnico

Accertamenti tecnici irripetibili art 360 cpp: Accertamenti che se compiuti comportano l'alterazione della prova e la ripetibilità della procedura non è più garantita; il PM esegue questa attività di accertamento avvisando previamente l'indagato e il suo difensore e la parte offesa 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, le parti hanno la facoltà di nominare un proprio Consulente Tecnico.

Incidente Probatorio: Viene richiesto per anticipare la formazione di una prova durante le indagini preliminari, il PM e il PG svolgono le indagini con perquisizioni e sequestro probatorio:
V Può essere richiesto dal PM
V Ha lo scopo di formare la prova
V Il GIP può nominare un suo consulente tecnico detto Perito
V Non velocizza il processo, semplicemente anticipa la formazione della prova

Procedimento Penale:
V Si realizza in due strutture: il tribunale e la Procura
V Si instaura con l'iscrizione della notizia di reato
V Si conclude con il giudicato penale
V Si instaura su iniziativa di una parte e anche d'ufficio

Procedimento Civile:
V Le parti in giudizio sono: l'attore ed il convenuto (procedimento ordinario)
V Si realizza in un'unica struttura: Il tribunale
V Le parti in giudizio sono: il ricorrente ed il resistente (procedimento con ricorso)
V Si instaura su iniziativa di una parte: l'attore o ricorrente
V Si instaura esclusivamente su iniziativa di una parte
V Le parti in giudizio possono nominare un consulente tecnico
V Il giudice può nominare un consulente tecnico detto Perito

GIP Giudice per le indagini preliminari:
V Non è l'unico interlocutore del Pubblico Ministero, anche la Polizia Giudiziaria
V Non Emette una sentenza
V Non può emettere sentenza di luogo a non procedere
V Provvede alle misure Cautelari
V Può non accogliere la richiesta di archiviazione

V Non ha autonomia di iniziativa probatoria, solo su richiesta di PM o indagato

GUP Giudice Udienza Preliminare:
V Interviene dopo l'esercizio dell'azione penale
V il GUP può emettere decreto di rinvio a giudizio dopo richiesta del PM di rinvio a giudizio
V il GUP può emettere sentenza di luogo a non procedere alla richiesta del PM di rinvio a giudizio

Il Pubblico Ministero conferisce l'incarico ai sensi dell'art 360 cpp:
V Quando sussiste il rischio che l'elemento probatorio da analizzare possa venire alterato o distrutto in fase di analisi/accertamento
V Indica al Consulente Tecnico che deve eseguire un accertamento NON ripetibile
V Quando il PM intende disporre il dissequestro del materiale sequestrato
V In caso di accertamenti non deve richiedere autorizzazione
V È l'organo con funziona requirente/inquirente

Chi può prendere parte agli accertamenti tecnici ripetibili ai sensi dell'art 359 cpp:
V Il consulente tecnico del PM (CTU), in quanto vige il segreto investigativo

Chi può prendere parte agli accertamenti tecnici non ripetibili ai sensi dell'art 360 cpp:
V Il difensore dell'indagato
V Il difensore dell'indagato accompagnato dal proprio consulente tecnico (CTP)
V il consulente tecnico di parte della persona offesa (CTP)
NOTA BENE: Si parla di indagato non imputato.

Quando si giunge al Giudicato Penale?
V Quando viene emessa la sentenza della Corte di Cassazione
V Quando sono decorsi i termini per proporre opposizione/impugnazione

Quali sono le caratteristiche proprie della Persona Offesa?
V Può nominare un difensore
V Può presentare memorie
V Può sporgere denuncia e fare esposti
V Può interloquire sia nella fase delle indagini preliminari che in quella di giudizio
V Può sporgere querela
V In determinati casi può ritirare la querela
V Può farsi assistere da un consulente tecnico

Esposto: segnalazione di un fatto allo scopo di far valutare se ricorre un'ipotesi di

reato
Denuncia: si dà notizia di reato perseguibile d'ufficio (può essere presentata da chiunque)
Querela: dichiarazione della persona offesa (Non perseguibile d'ufficio)(Può essere presentata solo da coloro che subiscono l'azione penalmente perseguibile)

L'intervento di un Computer Forenser può essere richiesto da:
V Il giudice dibattimentale in composizione monocratica
V Il Pubblico Ministero
V L'indagato
V La Polizia Giudiziaria
V La Parte offesa

La scelta degli strumenti tecnici e delle metodologie che il Computer Forenser deve impiegare nella corretta conduzione della propria opera è dettata da:
V La comunità scientifica

L'indagato/Imputato
La qualità di indagato si conserva fino alla richiesta di rinvio a giudizio o archiviazione
L'imputato è la persona indagata nei confronti della quale è stata esercitata l'azione penale

Entrambi hanno l'obbligo di farsi assistere da un difensore
Avvocato difensore: è nominato da entrambe le parti delle indagini preliminari/processo

V Ha l'obbligo di farsi assistere da un difensore
V Può farsi assistere da un consulente tecnico quando viene eseguito un accertamento tecnico
V Può produrre memorie difensive solo nella fase delle indagini preliminari
V Non ha l'obbligo di farsi assistere da un consulente tecnico quando viene eseguito un accertamento tecnico
V L'indagato assume il ruolo di imputato quando viene esercitata l'azione penale
V Non ha l'obbligo di presentarsi in udienza

Qual è l'ambito di applicazione della Computer Forensics?
V Qualsiasi reato dove possa esistere un sistema informatico coinvolto a questo titolo

La copia forense:
V È una qualunque copia di dati che rispetta le caratteristiche di preservazione e

validazione
V È una qualunque copia di dati eseguita in modo tale da garantire la ripetibilità delle successive operazioni di analisi
V È una duplicazione dei dati eseguita in modo tale da garantire sempre la ripetibilità delle successive operazioni di analisi
V Non è una duplicazione dei dati di interesse investigativo
V Non è una copia bit a bit dell'intero supporto
V Non deve essere eseguita con un write blocker
V Non deve essere sempre eseguita con tool forensi

Il Sequestro fisico:
Consiste nel prendere fisicamente il supporto
V Se il dispositivo è acceso bisogna preoccuparsi del problema dello shut down
V Non è sempre possibile eseguirlo

Il Sequestro Logico:
Consiste nell'eseguire una copia totale o parziale della memoria del dispositivo
V è sempre possibile eseguirlo
V Viene eseguito elaborando la c.d. copia forense
Quindi è una duplicazione dei dati di possibile interesse investigativo, garantisce la ripetibilità dei successivi accertamenti sulla copia stessa
V Se il dispositivo è acceso NON bisogna preoccuparsi del problema dello shut down perché per eseguire la copia il sistema deve essere già avviato

Nella fase di identificazione, la preview:
è un'analisi di primo livello delle memorie dei dispositivi per identificare elementi di interesse investigativo
V è una perquisizione informatica
V NON deve necessariamente essere eseguita realizzando la copia forense, posso anche semplicemente sfogliare il contenuto del reperto.
V Può essere eseguita su un sistema acceso
V è particolarmente utile ad individuare le fonti di prova
V è una fase in cui in alcuni casi vi è il rischio di alterare il reperto, soprattutto in caso di preview LIVE
V NON deve essere sempre eseguita su un sistema aperto
V Possono essere accesi dispositivi rinvenuti spenti, bisogna però considerare le informazioni che saranno perse

La Preview in un sistema acceso (LIVE):
Analisi del sistema attivo, più rapida, più rischiosa, può essere eseguita attraverso programmi di utility in lite mode, Tool ad hoc

V Rende veloce l'analisi dei software presenti nel sistema
V NON può essere eseguita con qualsiasi tool forensics oriented indipendentemente dal sistema da analizzare, bisogna usare tool compatibili con il S.O. del reperto
V NON può essere eseguita con una distro live forensics oriented (solo in caso di DEAD)
V NON è consigliabile usarla con un write blocker (da usare in caso di DEAD)

La Preview in un sistema spento (DEAD):
Analizza il S.O. morto, NON altera la prova attraverso l'uso di write blocker, Un alternativa al write blocker è la distro live forensics oriented
V Deve essere eseguita con un write blocker
V è meno rischiosa di un sistema acceso LIVE
V Se il sistema da analizzare è acceso bisogna analizzare se conviene spegnerlo
V Non può essere sempre eseguita (sistemi embedded come smartphone e router)
V Non velocizza l'analisi dei software presenti nel sistema (Quella è la LIVE)

Per Validazione si intende che:
V I dati della copia forense sono identici ai dati originali
V l'hash della copia forense coincide con l'hash calcolato dal supporto originale
V Non sempre l'hash della copia forense coinciderà con l'hash calcolato da una successiva copia forense (come succede in caso di riavvio con uno smartphone)

Per Preservazione si intende che:
V L'hash della copia forense coincide con l'hash calcolato dalla medesima copia dopo la fase di analisi
V L'hash ricalcolato sulla copia forense varierebbe alla minima alterazione della copia stessa

La c.d. Preview:
V Dovrebbe essere eseguita da tecnici specializzati poiché vi è il rischio di alterazione della prova
V è una fase in cui in alcuni casi vi è il rischio di alterare il reperto
V Può essere eseguita su di un sistema acceso
V Rende veloce l'analisi dei software del sistema
V è uno strumento di ricerca della prova permesso agli inquirenti in sede di perquisizione
V è particolarmente utile ad individuare le fonti di prova
V Il suo uso non è esplicitamente indicato nel Codice penale
V NON deve sempre essere eseguita realizzando la copia forense
V NON permette di eseguire un'analisi completa
V POSSONO essere accesi i dispositivi rinvenuti spenti

V NON è sempre necessario l'ausilio di un write blocker

In analisi, montare un file immagine:
V Implica che il sistema debba riconoscere il FileSystem presente
V è utile per analisi mirate
V è utile per impiegare strumenti non forensics oriented
V Permette l'esportazione del calcolo dell'hash dei file d'interesse
V Permette la visualizzazione immediata dei soli file residenti
V NON Permette la visualizzazione immediata dei file cancellati
V NON Permette di orrente una analisi completa

È un formato per disk image:
V DD
V ISO
V .bin/.cue
V Smart (.s01, .s02, …)

ENCASE L (logical) 01 Bitstream EWF
Acquisizione di tipo logica
15 sezioni
Si ottiene da un file E01 di tipo Disk Image

ENCASE E01 bitstream EWF
Formato basato su Smart
V Permette di conservare i metadati del reperto sorgente
V Permette la compressione (3 livelli: no, good, best)
V è un formato della famiglia Expert Witness Disk Image Format
V Può conservare il calcolo dell'hash
V Non può contenere la copia logia di una cartella/directory

ADVANCED FORENSICS FORMAT (AFF/AFF4)
Formato open, memorizzazione di disk image e relativi metadata associati
Disco separato in due layer:
-Disk-rappresentation layer (metadato)
-Data-storage layer (dato)

Il formato DD/RAW
V Non conserva nei metadati il calcolo dell'hash
V Non conserva alcun metadato del reperto sorgente
V Non permette la compressione
V Rappresenta la copia di un solo "file/steam"

V NON è un formato della famiglia Expert Witness Disk Image Format
V NON può contenere la copia logica di una cartella/directory

Il comando DD

V Esegue una copia bit a bit di un supporto di memoria generando un file immagine
V Permette di eseguire una copia di un solo file/steam
V Da solo non permette di produrre una copia forense (necessità di un write blocker)

Copia Forense: Comandi
dd
if: input file
of: output file
bs: block size in byte (default 512)
conv:
-"no error" continua ad elaborare nel caso di errore di lettura
-"sync" sostituisce i blocchi di memoria non letti nella destinazione con NULLs
skip = [n] salta la lettura del numero n di blocchi di memoria partendo dall'inizio
count = [n] indica all'elaboratore di terminare dopo aver letto il numero n di blocchi di memoria

I toolkit (GUYMAGER e FTK IMAGER)

V Permettono di eseguire la classificazione bad extension confrontando l'estensione del file con la signature in esso presente
V Facilitano il computer forenser nell'individuazione delle informazioni di interesse
V Permettono una ricerca tramite hash
V Eseguono una classificazione dei file
V Processano/elaborano il contenuto del disk image
V Permettono di eseguire il file carving (recupero da spazio non allocato) ricercando l'header ed il footer dei file conosciuti
V Permettono diverse tipologie di visualizzazioni

GuyMager

Tool opensource, si basa sulla libreria "libwf" ovvero AFF
Permette di fare solo una copia full disk elaborando una clonazione o disk image
Formato dell'immagine sarà DD/RAW o EWF(E01)
V Permette di produrre disk image nel formato E01
V è uno strumento per elaborare le copie forensi
V Fa uso dell'hashing on the fly
V Permette di segmentare/splittare il file immagine (è possibile selezionare la dimensione di split)
V Permette di scegliere tra i seguenti hash: MD5, SHA-1, SHA-256

V Esegue copie forensi solo di tipo “full disk”

FTK Imager

V è uno strumento per elaborare copie forensi
V Riconosce solo determinati tipi di FileSystem
V Permette di visionare il contenuto dei Disk Image
V Non permette la scelta del tipo di Hash da calcolare (Li calcola sempre e sono MD5 e SHA-1)
V Può eseguire una copia della memoria volatile
V Fa uso dell’hashing on the fly
V Permette di segmentare/splittare il file immagine
V Permette di esportare i file di interesse
V Permette di produrre disk image nel formato E01/RAW(DD)/SMART/AFF (Permette la scelta)
V Permette di avere informazioni su alcuni dei file cancellati
(File orphan, file cancellati che non hanno più la cartella che li conteneva)
V Può essere impiegato anche come strumento per la c.d. Preview

Algoritmo di Hash MD5

V Processa il messaggio in blocchi di 512 bit (ogni blocco è fatto da 16 parole di 32 bit)
V È costituito da 4 round e 4 funzioni logiche (MD4 è costituito da 3 round e 3 funzioni logiche)
V Fa uso di 64 costanti additive
V L’output è un digest a 128 bit
V Rispetto a MD4 fa uso di 62 costanti in più

SHS/SHA

Nell’algoritmo di SHA-1 se il messaggio di input M è di 968 bit, dopo il padding avremo che M’ sarà costituito da
V 3 blocchi da 512bit
V un bit “1” al 969 bit
V 1536bit
Nell’algoritmo MD5 se il messaggio di input M è di 1024, dopo il padding M’ sarà costituito da:
V Un bit “1” al 1025bit
V 448 bit di padding

Autopsy

V Permette l’aggiunta di ulteriori moduli di analisi

V Permette una configurazione “multiple user” (server) (single user SQlite)
V Permette la selezione dei file di interesse solo tramite “tag”
V Il “Central Repository” permette di rapportare il caso in esame con i precedenti casi già elaborati
V Il Disk Image viene processato tramite “Ingest Modules”
V Il modulo “Hash lookup” permette di impostare sia una lista di “ignorable file” e sia di “notable file”
V Il File Carving viene svolto tramite il tool “PhotoRec”
V Il modulo “PhotoRec” viene eseguito sullo spazio non allocato
V Il modulo che si preoccupa di estrarre informazioni dal cestino di sistema è “Recent Activity”
V Il modulo “Keyword Search” impiega “Apache Solr”
V Il modulo “Interesting Files” permette di evidenziare i file corrispondenti a determinate regole
V Il modulo “File Extension Mismatch” dipende dal modulo “File Type”
V Il modulo “Encryption Detection” permette di evidenziare possibili file protetti
V Il modulo Virtual Machine Extractor ricerca i file VMDK e VHD e li inserisce in “datasources”
V La sezione “Tags” contiene le annotazioni dell’utente
V Le informazioni dal registro di sistema vengono estratte tramite il tool “RegRipper”
V Il modulo “Exif Parse” estrae i metadati, exif dai file JPEG, memorizzandoli nella sezione Result
V Il modulo “Email Parser” ricerca ed analizza archivi di posta elettronica
V Il modulo “Plaso” elabora una timeline dell’evidence più specifica
V Il modulo “Data Source Integrity” Calcola e valida l’hash del reperto assicurano l’integrità del’’evidence
V Il modulo “Correlation Engine” è una ricerca più approfondita dei file del caso all’interno del “central repository” aggiornandola con i file del caso corrente
V Il modulo “Android Analyzer” analizza i dispositivi android ed estrae registro chiamate, contatti, messaggistica, browser, geolocation etc…

Partizione DOS (DOS PARTITION MBR)

V Contiene sempre un MBR
V Contiene un EBR se ha Secondary Extended Partition
V Può contenere al massimo 4 partizioni primarie
V Il settore contenente l’MBR termina con una signature
V Non ha limite al numero di partizioni che può contenere
V Rispetto al partizionamento GPT può contenere un numero di partizioni inferiore
V La Partition Table nell’EBR è costituita da 4 entry, di cui 2 sono vuote

V La Partition Table è costituita da quattro entry da 16 byte
V MBR è costituito da un settore da 512 byte
V Non contiene sempre una partizione EBR
V Non contiene sempre una MBR e un EBR
V l'EBR NON deve necessariamente contenere al massimo 1 entry

File System

I file system sono un sistema che permette la memorizzazione dei dati, organizzandoli gerarchicamente in file e directory in modo tale da ritrovarli in maniera rapida
-File system category
-Content category
-Metadata category
-File Name category
-Application category

Dati essenziali sono detti Trusted data e che se modificati/alterati causano un malfunzionamento del sistema:
indirizzamento del contenuto del file
nome del file
dimensione del file
Dati Non essenziali sono detti Untrusted Data e sono quindi informazioni accessorie:
dati temporali
permessi utente

Nel File System

V Le informazioni temporali sono dati non essenziali
V I dati non essenziali possono non essere coerenti
V Il FileSystem Category comprende le informazioni sul layout
V In Content Category i dati sono organizzati in data unit
V Il Metadata Category comprende le informazioni sull'indirizzo
V In Application Category sono presenti i dati NON essenziali per alcune funzionalità del FileSystem
V l'indirizzio della data unit dove è memorizzato un file è un dato essenziale
V lo Slack Space indica un settore non utilizzato di data unit allocata
V Il Physical Address (eseguito mediante Logical Block Address) è l'indirizzio del settore calcolato in base al primo settore del volume
V Logical Disk Volume Address è l'indirizzo del settore calcolato in base al primo settore del volume
V Logical Volume Address è l'indirizzo del settore calcolato in base al primo settore della partizione

V La strategia di allocazione del primo disponibile ricerca una data unit libera partendo dall'inizio del FileSystem
V la strategia di allocazione del prossimo disponibile ricerca una data unit libera partendo dall'ultima data unit allocata
V la strategia di allocazione del più adatto ricerca data unit consecutive libere per non frammentare il file da allocare

Nel FAT File system
V Il layout è costituito da:
-Reserved Area che include informazioni sul file system category
-FAT Area che contiene la primary structure del FAT e anche dei backup delle strutture, la sua dimensione è calcolata in base al numero e alla grandezza delle strutture FAT presenti
-Data Area che contiene i cluster da allocare per memorizzare i file e directory
V Le data unit si chiamano cluster
V Nel fat32 la root directory ha dimensione dinamica (valido solo per la FAT32)
V La dimensione delle entry del FAT dipendono dalla tipologia di FAT (Quindi hanno dimensione fissa in base al numero FAT12 = 12 bit)
V Le prime due entry del FAT non sono utilizzate per i cluster, la prima entry della tabella FAT inizia con indirizzo zero, Entry[0] = informazioni del media, Entry[1] = dirty status
V I cluster iniziano con indirizzo due
V lo stato di allocazione dei cluster è conservato nella struttura FAT
V La seconda entry del FAT indica se il FileSystem NON è stato smontato correttamente, oppure eventuali errori Hardware
V Lo stato di non allocazione dei cluster è indicato con ZERO all'interno della FAT
V Lo stato di non allocazione dei cluster è indicato con ZERO e quello di allocazione con l'indirizzo del prossimo cluster o con il marcatore End-Of-File
V La tipologia del FAT non è contenuta in nessun settore, bisogna calcolare i dati presenti nel boot sector
V il FSINFO è una strutta di dati NON essenziali per il FAT32

NEL NTFS
V Una entry MTFS può avere anche più di un attributo di tipo $DATA
V la signature BAAD serve per segnalare un ipotetico errore o corruzione dell'entry
V Lo stato di allocazione dell'entry è definito dall'attributo $BITMAP
V $Standard_information attribute esiste per ogni file e directory e contiene i metadati principali, nulla di questo attributo è essenziale
V $File_Name attribute contiene il riferimento al parent directory che lo contiene, e

permette in analisi di individuare tutto il percorso di una entry casuale
V $DATA attribute viene utilizzato per memorizzare qualsiasi forma di dati, se supera i 700 byte l'attributo diventa non residente
V Il contenuto di un attributo NON residente viene memorizzato in un cluster-run
V In ogni entry MFT di base vi è un attributo $Standard_Information
V In ogni entry MFT di base vi è un attributo di tipo $Attribute_List
V Ogni Entry MFT di base ha anche un attributo di tipo $File_Name
V Le entry MFT vengono pulite non appena il flag in uso viene settato
V La dimensione del cluster è indicata nel Boot Sector del $Boot File
V Nel File $BitMap è indicato lo stato di allocazione di ciascun cluster
V I Cluster danneggiati vengono indicati dal file $BadClus
V Ogni cosa è gestita come file
V Il file $BasClus ha un attributo $DATA della stessa dimensione del FileSystem
V Le informazioni temporali sul file sono contenuto solo all'interno dell'attributo $Standard_Information

Sistemi Operativi

Windows:
HKEY_CLASS_ROOT contiene due tipi di informazioni (dati che permettono di associare, dati di configurazione delle componenti)
HKEY_USERS contiene le impostazioni di tutti i profili utenti configuranti nel sistema (NTuser.dat), ogni sottoalbero di quest'albero descrive ciascun utente
HKEY_CURRENT_USER contiene il puntatore al profilo utente specifico presente in HKEY_USERS loggato nel sistema
HKEY_LOCAL_MACHINE contiene informazioni relative alla configurazione del pc come hardware, sistema operativo, bus, driver
HKEY_CURRENT_CONFIG contiene il puntatore alla corrente configurazione situata in HKEY_LOCAL_MACHINE

ShellBag

Preferenze utente nelle visualizzazione del contenuto delle cartelle
BagMRU: storico di tutte le cartelle visualizzate dall'utente
Bags: contiene solo le impostazioni di visualizzazione delle cartelle contenute in BagMRU(settate dall'utente)

File Swap

Pagefile.sys è un'estensione della memoria RAM
Pagefile.sys del SO Windows si trova nella root del disco
Hiberfil.sys è una copia della RAM quando viene mandato in ibernazione il sistema ed è un vero e proprio dump della RAM

V In SO Windows HKEY_USERS è una hive del registro di sistema che contiene le informazioni dell'utente
V Lo SwapFile o pagefile.sys in un SO Apple è posizionato nel percorso /private/var/vm
V Lo SwapFile in un SO Windows si trova nella root di Windows
V In un SO Windows la gran parte delle impostazioni del sistema e dell'utente sono memorizzate nel registro di sistema
V Il SO Windows è molto meno rigido nella gestione della struttura del FileSystem rispetto ad un SO Linux
V Linux registra molti più log di Windows
Il pagefile.sys rappresenta un'estensione della memoria RAM
V In SO Apple il FileValut offre la funzionalità di cifratura
V L'analisi dei thumbnail viene eseguita per avere informazioni sulle immagini non più presenti
V In Linux i file dell'utente si trovano esclusivamente nella propria home directory
V In un SO Windows i file dell'utente NON si trovano esclusivamente nella propria home directory
V In un SO Windows il file SAM contiene sempre l'elenco di tutti gli account utente che si sono loggati almeno una volta sul sistema
V In SO Windows i thumbnail del sistema NON sono sempre coerenti con i file residenti, potrebbero esserci thumbnail di file non più residenti

Nella Mobile Forensics:
Logical Extraction:
V Nella Logical Extraction NON bisogna preoccuparsi di decodificare i dati estratti
V Nella Logical Extraction i dati sono messi in strutture dati che dipendono dallo strumento di acquisizione
V La Logical Extraction dipende dall'API del dispositivo

Manual Extraction:
V La Manual Extraction si esegue fotografando il contenuto del dispositivo
V La Manual Extraction può essere eseguita su quasi la totalità dei dispositivi
V La Manual Extraction NON è il metodo più veloce per estrarre i dati
V La Manual Extraction NON può essere impiegata in caso di schermo rotto o codice di sblocco

FileSystem Extraction:
V Nella FileSystem Extraction si ottengono i DB così come sono presenti nel dispositivo
V Nella FileSystem Extraction si ottengono i contenuti presenti nel dispositivo a

seconda dei permessi
V Nella FileSystem Extraction bisogna decodificare l’output per visualizzare i dati

- COS'è L'INCIDENTE PROBATORIO?

ha lo scopo di anticipare la formazione della prova ma non di velocizzare il procedimento penale. può essere richiesto solo dal PM e dalle parti (offesa e indagata).
il GIP può nominare un proprio consulente, detto perito.

- IL PROCEDIMENTO PENALE

dove avviene? in due strutture, ovvero il tribunale e la procura.
ha lo scopo di accertare la verità nell'interesse dello stato e della collettività.
si instaura con l'iscrizione della notizia di reato.
si conclude con il giudicato penale.
prevede un grado di giudizio, in caso di impugnamento (una delle due parti non è contenta) c'è un secondo grado di giudizio (corte di appello) che può essere a sua volta impugnato e si procede al terzo grado (cassazione).
si fa partire d'ufficio se il reato coinvolge minori.

- IL PROCEDIMENTO CIVILE

le parti chiamate in giudizio sono l'attore e il convenuto, e il procedimento avviene in tribunale. le parti in giudizio sono: il ricorrente ed il resistente. si possono distinguere attore e convenuto (nel processo di cognizione di primo grado); appellante e appellato (nel grado di appello); ricorrente e resistente (nei procedimenti introdotti con ricorso); creditore procedente o pignorante o interveniente e debitore esecutato o intimato (nel processo esecutivo).
il procedimento civile ha lo scopo di verificare l'esistenza di un diritto reclamato da un privato cittadino nei confronti di un altro e stabilire quale dei due abbia ragione. si instaura esclusivamente su iniziativa di una parte. le parti in giudizio e il giudice possono nominare un consulente tecnico.

- IL GIP (GIUDICE PER LE INDAGINI PRELIMINARI)

è un interlocutore del pubblico ministero insieme alla polizia giudiziaria.
non può emettere sentenza, neanche di luogo a non procedere. provvede alle misure cautelari e può accogliere richieste di archiviazione. non ha autonomia, provvede solo su richiesta della parte. ha la funzione di garanzia dell'indagato nella fase delle indagini preliminari.

- IL GUP (GIUDICE DELL'UDIENZA PRELIMINARE)

Interviene dopo l'esercizio dell'azione penale;
Giudica la richiesta di rinvio a giudizio (celebrazione del processo)
Il giudice potrà:
• Emettere decreto di rinvio a giudizio;
• Emettere sentenza di non luogo a procedere.

- COMPUTER FORENSER

Deve garantire l'inalterabilità della prova nel caso vi possa essere (legge c.p. 360)

-PERITO
Caso in cui il CF sia nominato dal giudice stesso.

- COSA DICE LA LEGGE 360 cpp
Accertamenti che se compiuti comportano l'alterazione della prova e la ripetibilità della procedura non è più garantibile;
Il P.M. esegue questa attività di accertamento avvisando previamente l'indagato e il suo difensore e la parte offesa 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.
il PM conferisce incarico a questa legge quando:
sussiste il rischio che l'elemento probatorio da analizzare possa venire alterato distrutto in fase di analisi/accertamento.
il PM intende disporre il dissequestro del materiale sequestrato.

- QUAL è L'ORGANO GIUDIZIARIO CON FUNZIONE REQUIRENTE/INQUIRENTE?
il PM. è requirente dopo il rinvio a giudizio, è inquirente prima del rinvio a giudizio.

- CHI PUò PRENDERE PARTE AGLI ACCERTAMENTI TECNICI RIPETIBILI AI SENSI dell'art 359 cpp?
l'articolo 359 dice che: il PM può avere la necessità di svolgere accertamenti tecnici, che comportano specifiche conoscenze scientifiche, tecniche o artistiche, che esulano dalle competenze possedute dall'organo inquirente. il PM può avvalersi/nominare un consulente tecnico. vige il segreto investigativo quindi solo il CTU (il perito può prendere parte all'incidente probatorio).

- CHI PUò PRENDERE PARTE AGLI ACCERTAMENTI TECNICI NON RIPETIBILI AI SENSI DELL'ART 360 cpp?
il difensore dell'indagato, anche accompagnato dal proprio consulente tecnico CTP.
il difensore dell'inputato, accompagnato dal proprio consulente tecnico CTP.
il consulente tecnico di parte della persona offesa CTP.

- QUANDO SI GIUNGE AL GIUDICATO PENALE?
quando viene emessa la sentenza dalla Corte di Cassazione oppure quando sono decorsi i termini per proporre opposizione/impugnazione. l'imputato, prosciolto o condannato, non può essere nuovamente sottoposto a procedimento penale per il medesimo fatto storico. può essere impugnato ed andare al terzo grado (cassazione).

- QUALI SONO LE CARATTERISTICHE PROPRIE DELLE PERSONA OFFESA?
può sporgere denuncia e fare esposti. può interloquire sia nella fase delle indagini preliminari che in quella di giudizio. in determinati casi può ritirare la querela. può farsi assistere da un proprio consulente tecnico. è il soggeto titolare del bene giuridico leso dall'autore di un reato.

- DA CHI PUò ESSERE RICHESTO L'INTERVENTO DEL COMPUTER FORENSER?

dal giudice dibattimentale in composizione monocratica, dal pubblico ministero, dall'indagato, dalla polizia giudiziaria e dalla parte offesa.

- LE SCELTE DEGLI STRUMENTI E DELLE METODOLOGIE CHE IL CF DEVE IMPIEGARE NELLA CORRETTA CONDUZIONE DELLA PROPRIA OPERA è DETTATO DA:
la comunità scientifica internazionale.

- QUALI SONO LE DEFINIZIONI DI ESPOSTO, DENUNCIA E QUERELA?
esposto: segnalazione all'Autorità Giudiziaria di un fatto allo 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 (rimessa) se non si tratta di reati sessuali ai danni di minori (irrevocabile).

- L'INDAGATO E L'IMPUTATO DEVONO:
hanno l'obbligo di farsi assitere da un difensore.
può farsi assistere da un consulente quando viene eseguito un accertamento tecnico.
può produrre memorie difensive solo nella fase delle indagini preliminari.
non è vero che ha l'obbligo di presenziare in udienza.
ricordiamo che:
indagato: la persona nei cui confronti vengono svolte indagini a seguito dell'iscrizione di un fatto a lui addebitato nel registro delle notizie di reato.
imputato: la persona indagata nei confronti della quale è stata esercitata l'azione penale (rinvio a giudizio).

- QUAL è L'AMBITO DI APPLICAZIONE DELLA COMPUTER FORENSICS?
qualsiasi reato dove possa esistere un sistema informatico coinvolto a qualsiasi titolo.

-.-.-.-.-.-.-.-.-.-.-.-.-.-.-

- COS'è LA COPIA FORENSE?
è una qualunque copia di dati che rispetta le caratteristiche di preservazione e validazione, quindi una copia eseguita in modo tale da garantire la ripetibilità della successiva analisi.

- QUANDO SI PARLA DI SEQUESTRO FISICO?
def: sequestro di un qualunque sitema informatico fisico
inoltre: se il dispositivo è acceso bisogna preoccuparsi del problema dello shutdown

- QUANDO SI PARLA DI SEQUESTRO LOGICO?
def: si fa una copia -> si evita di portarsi fisicamente il dispositivo
è sempre possibile eseguirlo, viene eseguito elaborando la c.d. copia forense

- LA PREVIEW NELLA FASE DI IDENTIFICAZIONE:

è una perquisizione informatica.
può essere eseguita anche senza effettuare la copia forense, quindi semplicemente sfogliando il contenuto del reperto.
si può eseguire su un sistema acceso.
è una fase in cui in alcuni casi vi è il rischio di alterare il reperto, soprattutto in caso di preview LIVE.
posso essere accesi dispositivi rinvenuti spenti, ma bisogna valutare se le informazioni che perderemo (ultimo accesso, avvio di programmi allo startup ecc.)
sono meno importanti dell'urgenza dell'accertamento.

- LA PREVIEW IN UN SISTEMA ACCESO (LIVE):

può essere eseguita con una distro live forensics oriented, SOLO in caso di DEAD.
rende veloce l'analisi dei software presenti nel sistema.
bisogna usare tool compatibili con il S.O della macchina su cui stiamo facendo l'analisi.
è consigliabile eseguirlo con un write blocker in caso di DEAD.

- LA PREVIEW IN UN SISTEMA SPENTO (DEAD):

velocizza l'analisi dei software presenti nel sistema in caso di LIVE.
il sistema se è acceso può essere spento ma bisogna valutare: se è presente cifratura, informazioni sui software in esecuzione andranno perse, dump della RAM non più possibile.
non è detto che sia sempre eseguibile. in caso di sistemi embedded non è eseguibile (smartphone, router ...).
deve essere eseguita con un write blocker, sia fisico (tableau) che digitale (montare in sola lettura).
è meno rischioso della preview LIVE.

- COSA SI INTENDE PER VALIDAZIONE?

l'hash(una stringa esadecimale prodotta da un algoritmo che restituisce una stringa a lunghezza fissa di esadecimale a partire da un flusso di bit (dati) di dimensione qualsiasi. La stringa prodotta in output è univoca
per ogni file e ne è un identificatore. L'algoritmo non è invertibile, ossia non è possibile ricostruire il dato originale a partire dalla stringa che viene restituita in output) della copia forense coincide con l'hash calcolato dal supporto originale.
ci sono casi in cui l'hash della copia forense non coinciderà con l'hash da una successiva copia forense.
i dati della copia forense sono identici ai dati originali.

- COSA SI INTENDE CON PRESERVAZIONE?

l'hash della copia forense dovrebbe coincidere con l'hash calcolato dalla medesima copia dopo la fase di analisi.
l'hash ricalcolato sulla copia forense varierebbe alla minima alterazione della copia stessa.

- LA C.D. PREVIEW:

dovrebbe essere eseguita da tecnici specializzati poiché vi è il rischio di
alterazione della prova.

è una fase in cui in alcuni casi vi è il rischio di alterare il reperto.
può essere eseguita su di un sistema acceso.
rende veloce l'analisi dei software del sistema.
è uno strumento di ricerca della prova permesso agli inquirenti in sede di perquisizione.
è particolarmente utile ad individuare le fonti di prova.
il suo uso non è esplicitamente indicato nel Codice penale.

- MONTARE UN FILE IMMAGINE IN ANALISI:
implica che il sistema debba riconoscere il FileSystem presente.
permette la visualizzazione immediata dei soli file residenti.
è utile soprattutto per le analisi mirate.
è utile per impiegare strumenti non forensics oriented.

- QUALI SONO I FORMATI PER IL DISK IMAGE?
DD, ISO, bin/.cue, Smart s01,s02.

- FORMATO E01:
permette di conservare i metadati del reparto sorgente, permette la compressione.
è un formato della famiglia expert witness disk image format EWDIF.

- FORMATO DD/RAW:
non conserva (nei metadati) il calcolo dell'hash.
non conserva alcun metadato del reperto sorgente.
non permette la compressione.
rappresenta la copia di un solo file/stream.

- COMANDO DD?
da solo non permette di produrre una copia forense.
esegue una copia "bit a bit" di un supporto di memoria generando un file immagine.
permette di eseguire una copia di un solo file.

- dd if=/dev/sda of =/mnt/sdc.dd conv=noerror,sync
sto cambiando il nome del file di destinazione (sda -> sdc.dd).
non è completo per eseguire la copia forense in quanto manca il calcolo dell'hash.

- dd if=/mnt/sda.dd of =/dev/sda conv=noerror,sync
non è corretta.

- dd if=/mnt/sda.dd bs=2048|tee/dev/sda|md5sum>/mnt/sda.hash
esegue il calcolo dell'hash on-the-fly dell'immagine "sda.dd".
non produce una copia forense (non è corretto per eseguire una copia forense).

- dd if=/dev/sda bs = 2048|tee
mnt/dd_image/sda.dd|md5sum>mnt/dd_image/sda.hash
esegue la copia forense della sorgente "sda".

- TOOLKIT:

permettono di eseguire la classificazione bad extension confrontando l'estensione del file con la signature in esso presente.
facilitano il computer forenser nell'individuazione delle informazioni di interesse.
permettono una ricerca tramite hash.
eseguono una classificazione dei file.
processano/elaborano il contenuto del disk image.
permettono di eseguire il file carving ricercando l'header ed il footer dei file conosciuti.

- GUYMANAGER:
permette di produrre disk image nel formato E01.
è uno strumento per elaborare le copie forensi.
(NON?) fa uso dell'hashing on-the-fly.
permette di scegliere tra i seguenti hash: MD5, SHA-1, SHA-256.
esegue copie forensi solo di tipo "full disk".

- FTK IMAGER:
riconosce solo determinati tipi di FileSystem.
è uno strumento per elaborare copie forensi.
permette di visionare il contenuto dei Disk Image.
permette di avere informazioni su alcuni dei file cancellati.
permette di esportare i file di interesse.
permette di produrre disk image nel formato E01/Raw(dd)/SMART/AFF.
può essere impiegato anche come strumento per la c.d. preview.
fa uso dell'hashing on-the-fly.
permette di segmentare/splittare il file immagine.
non permette la scelta del tipo di hash da calcolare: li calcola sempre e sono MD5 e SHA-1.
può eseguire una copia della memoria volatile.

- ALGORITMO HASH MD5
processa il messaggio in blocchi di 512 bit ed è costituito da 4 round e 3 funzioni logiche.
fa uso di 64 costanti additive.
il suo output è un digest a 128bit (MD4/5 = 128 bit SHA-1 = 160bit)
rispetto a MD4 fa uso di 62 costanti in più.
fa 16 operazioni round.

-.-

- nell'algoritmo di SHA-1 se il messaggio di input M è di 968 bit, dopo il padding avremo che M' sarà costituito da:
3 blocchi da 512 bit, un bit "1" al 968" bit cioè 1536 bit.

- nell'algoritmo di SHA-1 se il messaggio di input M è di 1024bit, dopo il padding avremo che M' sarà costituito da:
1536 bit, 64 bit di lunghezza messaggio, un bit "1" al 1025'' bit

- COME CALCOLARE IL PADDING:
Supponiamo di avere un messaggio di 980 bit
Aggiungiamo 64 bit di lunghezza del messaggio (980+64=1044)
Abbiamo 1044 bit. Ora dobbiamo trovare il prossimo multiplo di 512 più grande di 1044

512x1=512 NO 512x2=1024 NO 512x3=1536 OK
Adesso per trovare i bit di padding dobbiamo semplicemente fare 1536-1044=492
Quindi abbiamo:
492 bit di padding
64 bit di lunghezza messaggio (SEMPRE)
3 blocchi da 512 bit (primo multiplo di 512 più grande di m+64)
981° bit=1
M'=1536 bit
IL PADDING è IDENTICO SIA PER SHA-1 CHE PER MD5

- AUTOPSY:

permette una configurazione "multiple user".
permette la selezione dei file di interesse solo tramite "tag"
la sezione "tags" contiene le annotazioni dell'utente.
il database "Central Repository" permette di rapportare il caso in esame con i precedenti casi già elaborati.
il Disk Image viene processato tramite dei "Ingest Modules".
il "file carving" viene svolto tramite il tool "PhotoRec".
il modulo "PhotoRec" viene eseguito sullo spazio non allocato.
il modulo "Keyword Search" impiega "Apache Solr".
il modulo "Interesting Files" permette di evidenziare i file corrispondenti a determinate regole. ex: tutti i file che terminano con .exe
il modulo "File Extention Mismatch" dipende dal modulo "File Type".
il modulo "Encryption Detection" permette di evidenziare possibili file protetti.
il modulo che si preoccupa di estrarre informazioni dal cestino di sistema è "RecentActivity".
il modulo che si preoccupa di estrarre informazioni dai browser è "RecentActivity".
il modulo "Hash lookup" permette di impostare sia una lista di "ignorable file" e sia di "notable file".
il modulo "Virtual Machine Extractor" ricerca i file VMDK e VHD e li inserisce in "datasources".

- NEL FILE SYSTEM:

le informazioni temporali sono dati non essenziali.
non essenziali = modificabili dall'utente e non compromettono il funzionamento del file system.
i dati non essenziali possono non essere coerenti.
dati essenziali = sempre coerenti.
il "FileSystem Category" comprende le informazioni sul layout.
in "Content Category" i dati sono organizzati in "data unit".
l'indirizzo della "data unit" dove è memorizzato un file è un dato essenziale.
il "Metadata category che contiene le informazionu sull' indirizzo delle "data unit".
in "Application Category" sono presenti i dati NON essenziali per alcune funzionalità del FileSystem.

il Phisical Address (LBA) è l'indirizzo del settore calcolato in base al primo settore del disco.
logical disk volume address è l'indirizzo del settore calcolato in base al primo settore del volume.
il Logical Volume Address è l'indirizzo del settore calcolato in base al primo settore della partizione.
lo "Slack Space" indica un settore non utilizzato di "data unit" allocata.
la strategia di allocazione del "primo disponibile" ricerca unaf "data unit" libera partendo dall'inizio del FileSystem.

- PARTIZIONAMENTO DOS:

contiene sempre un MBR.
rispetto al partizionamento GPT può contenere un numero di partizioni inferiore.
contiene un EBR se ha Secondary Extended Partition.
l'MBR contiene un primo (e unico) settore da 512 byte
può contenere al massimo 4 partizioni primarie (oltre all'MBR).
il settore contenente l'MBR termina con una signature.
non ha limite al numero di partizioni che può contenere.
rispetto al partizionamento GPT può contenere un numero di partizioni inferiore.
la "Partition Table" nell'EBR è costituita da 4 entry, di cui 2 sono vuote.
la "Partition Table" è costituita da quattro entry da 16 byte.

- NELL'NTFS (NT FILE SYSTEM):

una entry può avere anche più di un attributo di tipo $DATA.
il contenuto di un attributo NON residente viene memorizzato in un cluster-run.
in ogni entry MFT di base vi è un attributo $STANDARD_INFORMATION V.
in ogni entry MFT di base vi è un attributo di tipo $ATTRIBUTE_LIST,
ogni entry MFT di base ha anche un attributo di tipo $FILE_NAME.
le entry MFT vengono pulite non appena il flag "in uso" viene settato.
la dimensione dei cluster è indicato nel Boot sector del $Boot file.
nel file $BitMap è indicato lo stato di allocazione di ciascun cluster.
i cluster danneggiati vengono indicati dal file $BadClus.
nel file system tutto è gestito come un file.
lo stato di allocazione è indicato nel file $Bitmap.
il file $BadClus ha un attributo $DATA della stessa dimensione del FileSystem.
le informazioni temporali (opp. Flag/proprietario/security ID) sul file sono contenute solo all'interno dell'attributo $STANDARD_INFORMATION.

- IL FAT FILE SYSTEM:

le data unit si chiamano cluster.
il layout è costituito da: Reserved Area, FAT Area, Data Area.
nel FAT32 la root directory ha dimensione dinamica, solo in fat 32 la root directory ha dimensione variabile (Anche la reserved area in fat32 ha dimensione variabile).
la dimensione delle entry del FAT dipendono dalla tipologia di FAT, le entry del FAT sono a dimensione fissa e dipendono dal tipo di FAT (FAT12=12 bit ecc.)

le prime due entry del FAT non sono utilizzate per i cluster, le prime due entry sono utilizzate per: informazione del media e dirty status.
i cluster iniziano con indirizzo due.
la seconda entry del FAT indica se il file system NON è stato smontato correttamente [Google così dice] oppure segnala qualche errore hardware.
lo stato di allocazione dei cluster è conservato nella struttura FAT.
lo stato di non allocazione dei cluster è indicato con ZERO all' interno della FAT.
Lo stato di allocazione è indicato con ZERO (non allocato) mentre se è allocato contiene l'indirizzo del prossimo cluster oppure il marcatore End-Of-File (0xf..8) se è l'ultimo cluster.
per scoprire la tipologia bisogna calcolare i dati presenti nel boot sector poichè non è scritto da nessuna parte.
I dati contenuti in FSINFO Non sono essenziali, sono solo una guida per il S.O. e potrebbero non essere accurati.

- NELL'ANALISI DEI SISTEMI OPERATIVI:

in un SO windows la gran parte delle impostazioni del sistema e dell'utente sono memorizzate nel registro di sistema.
in un SO windows il file SAM contiene l'elenco di tutti gli account che si sono loggati almeno una volta su quella macchina (possono esserci account online che hanno l'accesso ma non l'hanno effettuato su quella determinata macchina).
il SO Windows è molto meno rigido nella gestione della struttura del FileSystem rispetto ad un SO Linux.
il SO Windows è molto flessibile nella gestione del file system.
Linux registra molti più log di windows.
in SO Windows potrebbero esserci thumbnail di file non più residenti.
il SO di Windows è il più documentato.
In SO Apple il FileValut offre la funzionalità di cifratura.
l'analisi dei thumbnail viene eseguita per avere informazioni sulle immagini non più presenti.
il pagefile.sys si trova nella root di windows.
lo Swapfile in un SO Apple è posizionato nel percorso /private/var/vm/.
in SO Windows HKEY_USERS è una hive del registro di sistema che contiene le impostazioni dell'utente.
in Linux i file dell'utente si trovano esclusivamente nella propria home directory.
il pagefile.sys del SO Windows si trova nella root del disco: è posizionato nel percorso /private/var/vm/
Il pagefile.sys rappresenta un estensione della memoria RAM.

- NELLA MOBILE FORENSICS:

i dati estratti tramite logical extraction sono già in chiaro.
nella logical extraction otteniamo i dati che sono messi in strutture dati che dipendono dallo strumento di acquisizione.
la logical extraction dipende dall'API del dispositivo.
nella Physical Extraction bisogna preoccuparsi di decodificare i dati estratti.
la Physical Extraction dipende dall versione del SO, dai livelli di patch di sicurezza, dal chipset e dal produttore del device.
la Physical Extraction dipende ANCHE dalla versione del SO e dai livelli di patch di sicurezza.

nella Physical Extraction si ottiene tutto il contenuto presente nel dispositivo.
la manual extraction può essere eseguita su quasi tutti i dispositivi.
la manual extraction è il metodo più lento per estrarre dati.
la Manual Extraction si esegue fotografando il contenuto del dispositivo.
la Manual Extraction può essere eseguita su quasi la totalità dei dispositivi.
non può essere eseguita in caso di schermo rotto o codice di sblocco.
nella FileSystem Extraction si può ottiene il contenuto presente nel dispositivo ma dipende dai permessi con cui vengono effettuate le richieste.
nella FileSystem Extraction bisogna decodificare l'output per visualizzare i dati contenuti.
nella FileSystem EXtraction si ottengono i DB così come sono presenti nel dispositivo.

PROCEDIMENTO PENALE E ATTORI DEL PROCEDIMENTO

L'incidente probatorio

V - può essere richiesto dal p.m.
F - viene richiesto SOLO dal p.m.
Può essere richiesto dalle parti (parte offesa e indagato)

V- ha lo scopo di formare la prova
F - viene richieste per velocizzare il procedimento
Ha lo scopo di ANTICIPARE la formazione della prova ma non velocizza il procedimento penale

F - il GIP può nominare un consulente tecnico di parte
Il GIP può nominare un proprio consulente detto Perito

F - nessuna delle altre risposte

Il Procedimento Penale

F - Si realizza in un'unica struttura: il tribunale
V - Si realizza in due strutture: il tribunale e la Procura
V - Si instaura con l'iscrizione della notizia di reato

F - prevede due gradi di giudizio
Prevede un grado di giudizio, in caso di impugnamento c'è un secondo grado di giudizio (corte di appello) che può essere a sua volta impugnato e si procede al terzo grado (Cassazione)

V - si conclude con il giudicato penale

F - si instaura esclusivamente su iniziativa di una parte

Si instaura anche d'ufficio (es. violenza su minore di 18 anni)

Il procedimento Civile

V - le parti in giudizio sono: l'attore ed il convenuto
V - Si realizza in un'unica struttura: il tribunale

V - Le parti in giudizio sono: il ricorrente ed il resistente
F - le parti in giudizio sono: l'imputato e la persona offesa
F - le parti in giudizio sono: l'indagato ed il ricorrente
Le parti in giudizio sono L'Attore ed il convenuto, Il ricorrente ed il resistente

F - ha lo scopo di accertare la verità nell'interesse dello stato e della collettività
No quello è il procedimento penale. il proc. Civile ha lo scopo di verificare l'esistenza di un diritto reclamato da un privato cittadino nei confronti di un altro e stabilire quale dei due abbia ragione

F - si instaura su iniziativa di una parte: il convenuto
Si instaura su iniziativa dell'Attore o ricorrente

V - si instaura su iniziativa di una parte: l'attore
V - Si instaura esclusivamente su iniziativa di una parte

V - le parti in giudizio possono nominare un consulente tecnico
F - Solo le parti in giudizio possono nominare un Consulente Tecnico

Anche il giudice può nominare un suo consulente (perito)

Il GIP Giudice per le indagini preliminari

F - è l'unico interlocutore del Pubblico Ministero
Anche la Polizia Giudiziaria è interlocutore del P.M.

F - emette una sentenza
V - non emette sentenza

F - può emettere sentenza di luogo a non procedere
V - provvede alle misure cautelari
V - può non accogliere la richiesta di archiviazione

F - ha autonomia di iniziativa probatoria

Non ha autonomia, provvede solo su richiesta della parte

Il PM conferisce incarico ai sensi dell'art. 360 c.p.p.

F - Quando occorre agire in assoluta urgenza a causa della deperibilità del reperto

V - Quando sussiste il rischio che l'elemento probatorio da analizzare possa venire alterato o distrutto in fase di analisi/accertamento

F - Solo quando non vi è il rischio che l'elemento probatorio da analizzare possa venire alterato o distrutto in fase di analisi/accertamento
In questo caso viene invocato il 359 c.p.p

F - indica al perito che deve eseguire un accertamento tecnico non ripetibile
Lo indica al consulente tecnico

F - indica al Consulente Tecnico che deve eseguire un accertamento tecnico ripetibile
V - indica al Consulente Tecnico che deve eseguire un accertamento tecnico NON ripetibile
V - Quando il PM intende disporre il dissequestro del materiale sequestrato

F - Chiedendo autorizzazione al GIP (Giudice Indagini Preliminari)
In caso di accertamento non deve chiedere autorizzazione (deve chiedere in caso si vogliano effettuare intercettazioni come mezzi di ricerca della prova)

F - Quando il PM vuole fornire la più ampia garanzia alle parti escludendo il rischio di successive eccezioni

L'Organo Giudiziario con funzione requirente/inquirente è

V - Il PM
F - Il GIP
F - La Polizia Giudiziaria
F - Il Consulente tecnico
F - Il Perito

Chi può prendere parte agli accertamenti tecnici ripetibili ai sensi dell'art 359 c.p.p.

F - L'indagato con il proprio difensore
F - la persona offesa
F - il consulente tecnico dell'indagato (CTP)
V - Il consulente tecnico del P.M. (CTU)
F - il Perito (F?)

Vige il segreto investigativo quindi solo il CTU (il perito può prendere parte all'incidente probatorio)

Chi può prendere parte agli accertamenti tecnici non ripetibili ai sensi dell'art 360 c.p.p.

F - il difensore dell'imputato
V - il difensore dell'indagato
F - l'imputato
F - il difensore dell'IMPUTATO accompagnato dal proprio consulente tecnico (CTP)
V - il difensore dell'INDAGATO accompagnato dal proprio consulente tecnico (CTP)
F - il perito del GIP
F - il perito del GUP
F - il Perito

V - il consulente tecnico di parte della persona offesa (CTP)
Fare attenzione a indagato e imputato con relativi difensori e consulenti (indagato si, imputato no) i consulenti si tranne i periti

Quando si giunge al Giudicato Penale?

F - Quando il giudice deposita la sentenza
V - Quando viene emessa la sentenza dalla Corte di Cassazione
F - Quando viene emessa la sentenza della Corte d'appello
Può essere impugnato ed andare al terzo grado (cassazione)

V - Quando sono decorsi i termini per proporre opposizione/impugnazione

Quali sono le caratteristiche proprie della Persona Offesa?

F - In alcuni casi può chiedere l'archiviazione del procedimento
V - Può sporgere denuncia e fare esposti
V - Può interloquire sia nella fase delle indagini preliminari che in quella di giudizio
F - Non può sporgere querela
V - può sporgere denuncia
F - è colui che assiste alla commissione di un reato
F - può prendere parte solo alla fase di giudizio
V - In determinati casi può ritirare la querela
V - Può farsi assistere da un proprio Consulente Tecnico
F - Non può farsi assistere da un proprio consulente tecnico

L'intervento di un Computer Forenser può essere richiesto da:

V - Il Giudice dibattimentale in composizione monocratica
V - Il pubblico Ministero
V - L'indagato
V - La Polizia Giudiziaria
V - La Parte Offesa

La scelta degli strumenti tecnici e delle metodologie che il Computer Forenser deve impiegare nella corretta conduzione della propria opera è dettato da:

F - Il Pubblico Ministero in fase di conferimento dell'incarico
F - Il Codice di Procedura Penale
V - La comunità scientifica internazionale
F - La legge 48/2008, Legge ratificata del Consiglio d'Europa di Budapest del 2001

Luca nota il suo vicino di casa costruire una mansarda. Egli può fare:

V - Un esposto
F - una denuncia
F - una querela
F - nessuna delle precedenti

Luca scopre che il suo vicino detiene materiale pedopornografico. Egli può fare:

F - Un esposto
V - una denuncia
F - una querela
F - nessuna delle precedenti

Luca scopre che il suo vicino di casa percuote la figlia minorenne. Egli può fare:

F - Un esposto
V - una denuncia
F - una querela
F - nessuna delle precedenti

L'indagato/imputato

V - ha l'obbligo di farsi assistere da un difensore
F - ha l'obbligo di farsi assistere da un consulente tecnico quando viene eseguito un accertamento tecnico
F - l'indagato assume il ruolo di imputato dopo la sentenza di primo grado
Lo assume quando viene esercitata l'azione penale (rinviato a giudizio)

V - può farsi assistere da un consulente quando viene eseguito un accertamento tecnico
F - l'indagato assume il ruolo di imputato dopo la sentenza di primo grado
V - può produrre memorie difensive solo nella fase delle indagini preliminari
F - ha l'obbligo di presenziare in udienza

FASI DEL TRATTAMENTO

Qual è l'ambito di applicazione della Computer Forensics

F - i soli reati che hanno come obbiettivo un sistema informatico
F - i soli reati che hanno come mezzo un sistema informatico
V - qualsiasi reato dove possa esistere un sistema informatico coinvolto a qualsiasi titolo
F - i reati informatici descritti dal Codice penale
F - i reati informatici descritti dal codice di procedura penale

La copia forense:

V - è una qualunque copia di dati che rispetta le caratteristiche di preservazione e validazione
V - è una qualunque copia dei dati eseguita in modo tale da garantire la ripetibilità della successiva operazione di analisi
F - è una duplicazione dei dati di interesse investigativo
F - è una copia "bit a bit" dell'intero supporto di memoria
F - è una duplicazione dei dati eseguita in modo da garantire sempre la ripetibilità dell'operazione di copia
V - è una duplicazione dei dati eseguita in modo tale da garantire sempre la ripetibilità della successiva operazione di analisi
F - deve essere sempre eseguita con un write blocker
F - deve essere sempre eseguita con tool forensi

Il sequestro fisico:

V - se il dispositivo è acceso bisogna preoccuparsi del problema dello shut down
F - è sempre possibile eseguirlo
non si può fare in caso di: Server di grosse dimensioni, rack ecc.

F - viene eseguito elaborando la c.d. copia forense

Quello è il sequestro logico

Il sequestro logico:

F - se il dispositivo è acceso bisogna preoccuparsi del problema dello shut down
No perché posso sempre effettuare una copia dei dati (sequestro logico) su un dispositivo già avviato

V - è sempre possibile eseguirlo
V - viene eseguito elaborando la c.d. copia forense

Nella fase di identificazione, la preview:

V - è una perquisizione informatica
F - deve essere eseguita realizzando la copia forense
Posso anche solo sfogliare il contenuto del reperto (cartelle, programmi, file ecc.)

V - può essere eseguita su un sistema acceso
F - non è particolarmente utile ad individuare le fonti di prova
V - è una fase in cui in alcuni casi vi è il rischio di alterare il reperto
Vero soprattutto in caso di preview LIVE

F - è una fase in cui non vi è alcun rischio di alterare il reperto
F - deve essere sempre eseguita su un sistema spento

F - non posso essere accesi dispositivi rinvenuti spenti

Bisogna valutare se le informazioni che perderemo (Ultimo accesso, avvio di programmi allo startup ecc.) sono meno importanti dell'urgenza dell'accertamento

La preview in un sistema acceso (LIVE)

F - può essere eseguita con una distro live forensics oriented
Solo in caso di DEAD

V - rende veloce l'analisi dei software presenti nel sistema
F - può essere eseguito con qualsiasi tool forensics oriented indipendentemente dal sistema da analizzare
Bisogna usare tool compatibili con il S.O della macchina su cui stiamo facendo l'analisi

F - è consigliabile eseguirla con un "write blocker"

In caso di DEAD si

La preview in un sistema spento (DEAD)

F - velocizza l'analisi dei software presenti nel sistema
In caso di LIVE si

F - il sistema da analizzare se è acceso, non deve essere spento
Può essere spento ma bisogna valutare: se è presente Cifratura, informazioni sui software in esecuzione andranno perse, Dump della RAM non più possibile

F - può essere sempre eseguita
In caso di sistemi embedded non può essere eseguita (Smartphone, router ecc.)

V - deve essere eseguita con un "write blocker"
Può essere usato un write blocker sia fisico (Tableau) che digitale (montare in sola lettura)

F - è più rischiosa di quella in un sistema acceso (LIVE)

È meno rischiosa

Per validazione si intende che:

V - l'hash della copia forense coincide con l'hash calcolato dal supporto originale

F - l'hash della copia forense coinciderà sempre con l'hash calcolato da una successiva copia forense
In caso di una particolare analisi (Es. smartphone che viene riavviato) gli hash delle successive copie potrebberò non essere uguali all' hash della prima copia forense

F - l'hash della copia forense coincide con l'hash calcolato dalla medesima copia dopo la fase di analisi
Questa è una proprietà della PRESERVAZIONE non della validazione

V - i dati della copia forense sono identici ai dati originali

Per preservazione si intende che:

V - l'hash della copia forense coincide con l'hash calcolato dalla medesima copia dopo la fase di analisi

F - l'hash della copia forense coincide con l'hash calcolato da una successiva copia forense
F - l'hash della copia forense coincide con l'hash calcolato dal supporto originale
Queste due proprietà valgono per la VALIDAZIONE non preservazione

F - la copia forense è inalterabile (**opp**. la copia forense sarà immodificabile)

F - i dati della copia forense sono identici ai dati originali
Proprietà della VALIDAZIONE

V - l'hash ricalcolato sulla copia forense varierebbe alla minima alterazione della copia stessa

La c.d. "preview"

F - può essere compiuto da qualsiasi agente della P.G. poiché ha un basso rischio di alterazione della prova
V - dovrebbe essere eseguita da tecnici specializzati poiché vi è il rischio di alterazione della prova

V - è una fase in cui in alcuni casi vi è il rischio di alterare il reperto
F - deve essere eseguita realizzando la copia forense

V - può essere eseguita su di un sistema acceso

F - permette di eseguire una analisi completa
F - non devono essere accesi i dispositivi rinvenuti spenti
V - rende veloce l'analisi dei software del sistema

V - è uno strumento di ricerca della prova permesso agli inquirenti in sede di perquisizione

F - non è particolarmente utile ad individuare le fonti di prova
V - è particolarmente utile ad individuare le fonti di prova
V - il suo uso non è esplicitamente indicato nel Codice penale
F - il suo uso è indicato nel Codice penale (**opp** Codice civile)
F - può essere eseguita solo con l'ausilio di un write blocker
F - deve essere eseguita impiegando obbligatoriamente un write blocker

DISK IMAGE

In analisi, montare un file immagine:

V - implica che il sistema debba riconoscere il FileSystem presente
F - non bisogna preoccuparsi di riconoscere il FileSystem presente

V - permette la visualizzazione immediata dei soli file residenti
F - permette l'immediata visualizzazione anche dei file cancellati

F - permette di ottenere una analisi completa

V - permette l'esportazione del calcolo dell'hash dei file di interesse

V - è utile soprattutto per le analisi mirate
V - è utile per impiegare strumenti non forensics oriented
F - non è utile per impiegare strumenti non forensics oriented

F - si ha la completa visione di tutto il contenuto presente
F - non vi è mai il rischio di alterare il file immagine

È un formato per "disk image"

F - Encase L01 (.L01, .L02, …)
V - DD
V - ISO
V - .bin/.cue
V - Smart (.s01, .s02, ..)

Il formato L01 contiene copie logiche

Il formato E01

F - non conserva il calcolo dell'hash (di nessun tipo)
V - permette di conservare i metadati del reperto sorgente
V - permette la compressione
F - non permette la compressione
V - è un formato della famiglia Expert Witness Disk Image Format

F - non è un formato della famiglia Expert Witness Disk Image Format
F - può contenere la copia logica di una cartella/directory

Il formato DD/RAW

F - conserva nell'header solo il calcolo dell'hash MD5
V - non conserva (nei metadati) il calcolo dell'hash
V - non conserva alcun metadato del reperto sorgente
F - conserva i metadati del reperto sorgente
V - non permette la compressione
F - permette la compressione
F - è un formato della famiglia "Expert Witness Disk Image Format"
F - può contenere la copia logica di una cartella/directory
V - rappresenta la copia di un solo "file/stream"

Il comando DD

F - da solo permette di produrre una copia forense
V - da solo non permette di produrre una copia forense

F - garantisce la non alterazione del disco originale
Viene garantito dai write blocker

V - esegue una copia "bit a bit" di un supporto di memoria generando un file immagine
V - permette di eseguire una copia di un solo file

F - permette di eseguire la copia di più file
Un solo file/stream

F - deve essere eseguito impiegando obbligatoriamente un write blocker

Il seguente comando: dd if=/dev/sda of =/mnt/sdc.dd conv=noerror,sync

F - è errato in quanto non è specificato il "blocksize"
il bs di default è 512 quindi può non essere specificato

V - è corretto
è corretto perché sto solo cambiando il nome del file di destinazione (sda->sdc.dd)

F - è completo per eseguire la copia forense
V - non è completo per eseguire la copia forense in quanto manca il calcolo dell'hash

F - non è corretto poiché le opzioni "noerror" e "sync" non andrebbero combinate
F - non è corretto per altri motivi

Il seguente comando: dd if=/mnt/sda.dd of =/dev/sda conv=noerror,sync

F - è errato in quanto non è specificato il "blocksize"
F - è corretto
F - non è completo, in quanto manca il calcolo dell'hash
F - non è corretto poichè le opzioni "noerror" e "sync" possono essere combinate
V - non è corretto per altri motivi

Il seguente comando: dd if=/mnt/sda.dd bs=2048|tee /dev/sda|md5sum>/mnt/sda.hash

F - produce una immagine divisa in 2048MB
F - il comando non è corretto
V - esegue il calcolo dell'hash on-the-fly dell'immagine "sda.dd"
F - esegue la copia della sorgente "sda"
V - non produce una copia forense (non è corretto per eseguire una copia forense)

Il seguente comando: dd if=/dev/sda bs = 2048|tee mnt/dd_image/sda.dd|md5sum>mnt/dd_image/sda.hash

F - non è corretto
V - è corretto
F - produce un file immagine segmentato/diviso in parti da massimo 2048MB
V - esegue la copia forense della sorgente "sda"
F - esegue il calcolo dell'hash on-the-fly dell'immagine "sda.dd"

TOOLKIT (GUYMAGER E FTK)

I Toolkit

V - permettono di eseguire la classificazione bad extension confrontando l'estensione del file con la signature in esso presente
V - facilitano il computer forenser nell'individuazione delle informazioni di interesse

F - permettono esclusivamente una visualizzazione gerarchica dei file
Oltre alla vista gerarchica (ad albero) c'è quella per file type e per signature

F - non hanno ancora sviluppato una ricerca tramite hash
V - permettono una ricerca tramite hash

F - eseguono in maniera automatizzata tutta (**opp.** gran parte) l'analisi
V - eseguono una classificazione dei file
V - processano/elaborano il contenuto del disk image
F - non eseguono una elaborazione del contenuto del disk image
F - non permettono di ottenere diverse visualizzazioni di dati
V - permettono di eseguire il file carving ricercando l'header ed il footer dei file conosciuti

GuyMager

V - permette di produrre disk image nel formato E01

V - è uno strumento per elaborare le copie forensi
F - è uno strumento per la produzione di copie NON forensi
V - fa uso dell'hashing on-the-fly
F - non fa uso dell'hashing on-the-fly
F - non permette di segmentare/splittare il file immagine
V - permette di scegliere tra i seguenti hash: MD5, SHA-1, SHA-256

F - non permette la scelta del tipo di hash da calcolare

A differenza di ftk imager, guymager permette di scegliere gli hash da calcolare

F - esegue copie forensi (anche) di tipo logico
V - esegue copie forensi solo di tipo "full disk"

A differenza di ftk imager esegue solo copie full disk

FTK Imager

V - è uno strumento per elaborare copie forensi

F - riconosce tutti i tipi di FileSystem
V - riconosce solo determinati tipi di FileSystem

F - permette di visionare/analizzare solo Disk Image
V - permette di visionare il contenuto dei Disk Image

F - permette di visualizzare solo i file residenti
V - permette di avere informazioni su alcuni dei file cancellati

V - permette di esportare i file di interesse
V - permette di produrre disk image nel formato E01/Raw(dd)/SMART/AFF
V - può essere impiegato anche come strumento per la c.d. preview
F - non può (deve) essere impiegato anche come strumento per la c.d. preview

F - non fa uso dell'hashing on-the-fly
V - fa uso dell'hashing on-the-fly

V - permette di segmentare/splittare il file immagine
F - non permette di segmentare/splittare il file immagine

F - esegue copie forensi solo di tipo "full disk"

F - permette di scegliere tra i seguenti hash: MD5, SHA-1, SHA-256
F - permette la scelta del tipo di hash da calcolare
V - non permette la scelta del tipo di hash da calcolare
Li calcola sempre e sono MD5 e SHA-1

V - può eseguire una copia della memoria volatile

HASH

L'algoritmo di Hash MD5

V - processa il messaggio in blocchi di 512bit
F - processa il messaggio in blocchi da 1024bit

F - è costituito da 4 round e 3 funzioni logiche
V - è costituito da 4 round e 4 funzioni logiche
F - è costituito da 3 round e 3 funzioni logiche
MD4 è costituito da 3 round e 3 funzioni logiche

V - fa uso di 64 costanti additive

F - l'output è un digest a 160bit
V - l'output è un digest a 128bit
MD4/5=128 bit SHA-1=160bit

V - rispetto a MD4 fa uso di 62 costanti in più
F - rispetto a MD4 fa uso di 2 costanti in più
MD5=64 costanti additive MD4=2 costanti additive

F - il terzo round è composto da 48 operazioni
F - il quarto round è composto da 48 operazioni

16 operazioni per round

Nell'algoritmo di SHA-1 se il messaggio di input M è di 968 bit, dopo il padding avremo che M' sarà costituito da:

V - 3 blocchi da 512 bit
F - 60 bit per la lunghezza del messaggio
V - un bit "1" al 969'' bit
F - nessun bit di padding
V - 1536 bit

Nell'algoritmo SHA-1 se il messaggio di input M è di 1024, dopo il padding M' sarà costituito da:

F - 2 blocchi da 512 bit

V - 64 bit di lunghezza messaggio
F - 60 bit di lunghezza del messaggio
V - un bit “1” al 1025’’ bit
F - nessun bit di padding
F - un bit “1” al 1048° bit
V - 1536 bit
F - 1024 bit

Nell’algoritmo MD5 se il messaggio di input M è di 1024, dopo il padding M’ sarà costituito da:

F - 4 blocchi da 512 bit
F - 60 bit di lunghezza messaggio
V - un bit “1” al 1025’’ bit

V - 448 bit di padding
F - 2048 bit

COME CALCOLARE IL PADDING:

Supponiamo di avere un messaggio di 980 bit

Aggiungiamo 64 bit di lunghezza del messaggio (980+64=1044)

Abbiamo 1044 bit. Ora dobbiamo trovare il prossimo multiplo di 512 più grande di 1044

512x1=512 NO 512x2=1024 NO 512x3=1536 OK

Adesso per trovare i bit di padding dobbiamo semplicemente fare 1536-1044=492

Quindi abbiamo:

492 bit di padding

64 bit di lunghezza messaggio (SEMPRE)

3 blocchi da 512 bit (primo multiplo di 512 più grande di m+64)

981º bit=1

M’=1536 bit

IL PADDING è IDENTICO SIA PER SHA-1 CHE PER MD5

AUTOPSY

Autopsy

F - non permette l’aggiunta di ulteriori moduli di analisi
F - permette solo una configurazione "single user"
V - permette una configurazione “multiple user”
F - permette la selezione dei file di interesse tramite "checkbox"

V - permette la selezione dei file di interesse solo tramite “tag”

F - La sezione “Result” contiene le annotazioni dell’utente
La sezione “Tags” contiene le annotazioni dell’utente

V - il “Central Repository” permette di rapportare il caso in esame con i precedenti casi già elaborati
V - il Disk Image viene processato tramite dei “Ingest Modules”

F - le informazioni dal registro di sistema vengono estratte tramite il tool "RegistryViewer"
Viene usato il tool RegRipper

F - il “file carving” viene eseguito su tutto il disk image
V - il “file carving” viene svolto tramite il tool “PhotoRec”
V - il modulo “PhotoRec” viene eseguito sullo spazio non allocato

V - il modulo “Keyword Search” impiega “Apache Solr”
V - il modulo “Interesting Files” permette di evidenziare i file corrispondenti a determinate regole
Es. tutti i file che terminano con .exe

V - Il modulo “File Extention Mismatch” dipende dal modulo “File Type”

V - il modulo “Encryption Detection” permette di evidenziare possibili file protetti
F - il modulo “Encryption Detection” permette di trovare e decifrare i file protetti
Li evidenzia solo, sta a noi poi trovare un modo per decifrarli

F - il modulo “Exif Parser” dipende dal modulo “Embedded File Extractor”

F - il modulo “Virtual Machine Extractor” permette di genere una macchina virtuale
dalla copia forense
Ricerca solo i file VMDK e VHD e li inserisce in “datasources”

F - il modulo che si preoccupa di estrarre informazioni dal cestino di sistema è "RecycleBin Activity"
V - il modulo che si preoccupa di estrarre informazioni dal cestino di sistema è “RecentActivity”
F - il modulo che si preoccupa di estrarre informazioni dai browser è “InternetActivity”/”BrowserActivity”
V - il modulo che si preoccupa di estrarre informazioni dai browser è “RecentActivity”

V - il modulo "Hash lookup" permette di impostare sia una lista di "ignorable file" e sia di
"notable file"
F - il modulo “Hash Lookup” permette solo di importare la lista di “ignorable file”

FILE SYSTEM

Nel File System

F - le informazioni temporali sono essenziali
V - le informazioni temporali sono dati non essenziali
Non essenziali=modificabili dall’utente e non compromettono il funzionamento del file system

F - i dati essenziali possono non essere coerenti
V - i dati non essenziali possono non essere coerenti
Dati essenziali=Sempre coerenti

F - il “Metadata Category” comprende le informazioni sul layout

F - il “Content Category” comprende le informazioni sul layout
V - il “FileSystem Category” comprende le informazioni sul layout

V - in "Content Category" i dati sono organizzati in "data unit"
F - in “Metadata Category” i dati sono organizzati in “data unit”

F - il "FileSystem Category" comprende le informazioni sull'indirizzo delle "data unit"
è il “Metadata category che contiene le informazionu sull’ indirizzo delle “data unit”

F - in “Application Category” sono presenti i dati essenziali per alcune funzionalità del FileSystem
Sono presenti i dati NON essenziali

V - l'indirizzo della "data unit" dove è memorizzato un file è un dato essenziale
F - l’indirizzo della “data unit” dove è memorizzato un file non è un dato essenziale

V - Phisical Address (LBA) è l’indirizzo del settore calcolato in base al primo settore del disco.
V - Logical Disk Volume Address è l’indirizzo del settore calcolato in base al primo settore del volume.
V - Logical Volume Address è l’indirizzo del settore calcolato in base al primo settore della partizione.
F - il “Logical Volume Address” è l’indirizzo di un settore basandosi sull’inizio del disco

F - lo “Slack Space” indica una “data unit” non più allocata
V - lo “Slack Space” indica un settore non utilizzato di “data unit” allocata

V - la strategia di allocazione del “primo disponibile” ricerca una “data unit” libera
partendo dall’inizio del FileSystem
F - la strategia di allocazione del "prossimo disponibile" ricerca una "data unit" libera
partendo dall'inizio del file system

I VOLUMI

Partizionamento DOS

V - contiene sempre un MBR

F - contiene sempre un EBR

F - contiene sempre un MBR e un EBR

F - contiene un MBR se ha Secondary Extended Partition
Contiene un EBR se ha Secondary Extended Partition

F - MBR è costituito da almeno quattro settori
primo settore da 512 byte (uno solo)

F - può contenere al massimo 8 partizioni

V - può contenere al massimo 4 partizioni primarie
F - può contenere al massimo 4 secondary extended partition
F - l'EBR può contenere al massimo 1 entry
V - il settore contenente l'MBR termina con una signature

V - non ha limite al numero di partizioni che può contenere
V - rispetto al partizionamento GPT può contenere un numero di partizioni inferiore

V - la "Partition Table" nell'EBR è costituita da 4 entry, di cui 2 sono vuote
V - la "Partition Table" è costituita da quattro entry da 16 byte
F - la "Partition Table" è costituita da massimo 8 entry
F - nella entry della "partition table" è (sempre) indicato il tipo di partizione
F - il campo "starting LBA address", presente nella "partition table", indica il cluster iniziale della partizione

Nel NTFS

F - una entry MFT può contenere solo un attributo di tipo $DATA

Una entry può avere anche più di un attributo di tipo $DATA

F - in una MFT entry, il contenuto di un attributo residente viene memorizzato in un cluster run
Il contenuto di un attributo NON residente viene memorizzato in un cluster-run

V - in ogni entry MFT di base vi è un attributo $STANDARD_INFORMATION
V - in ogni entry MFT di base vi è un attributo di tipo $ATTRIBUTE_LIST
ogni entry MFT di base ha anche un attributo di tipo $FILE_NAME

F - Le entry MFT vengono pulite non appena viene settato a ZERO il flag in uso
V - le entry MFT vengono pulite non appena il flag "in uso" viene settato

F - L'attributo in una MFT Entry di tipo "non residente" indica che il file che descrive è stato cancellato

F - La dimensione del cluster è indicato nella tabella MFT
La dimensione dei cluster è indicato nel Boot sector del $Boot file

V - Nel file $BitMap è indicato lo stato di allocazione di ciascun cluster
F - Il file $BitMap indica i cluster danneggiati
I cluster danneggiati vengono indicati dal file $BadClus

F - ad esclusione delle strutture del FileSystem tutto il resto è gestito come file
Ogni cosa è gestita come file

F - nel file $BadClus è indicato lo stato di allocazione di ciascun cluster
Lo stato di allocazione è indicato nel file $Bitmap

V - Il file $BadClus ha un attributo $DATA della stessa dimensione del FileSystem

V - Le informazioni temporali (**opp**. Flag/proprietario/security ID) sul file sono contenute solo all'interno dell'attributo $STANDARD_INFORMATION

Nel FAT file System

F - le data unit si chiamano settori
V - le data unit si chiamano cluster

F - il layout è costituito da una Reserved Area, FAT area, una Data Area e una Cluster Area
IL layout è costituito da: Reserved Area, FAT Area, Data Area

F - nel FAT12/16 la root directory ha dimensione dinamica
V - nel FAT32 la root directory ha dimensione dinamica
Solo in fat 32 la root directory ha dimensione variabile (Anche la reserved area in fat32 ha dimensione variabile)

F - le entry del FAT sono a dimensione variabile
V - la dimensione delle entry del FAT dipendono dalla tipologia di FAT
Le entry del FAT sono a dimensione fissa e dipendono dal tipo di FAT (FAT12=12 bit ecc.)

V - le prime due entry del FAT non sono utilizzate per i cluster
LE prime due entry sono utilizzate per: informazione del media e dirty status

F - i cluster iniziano con indirizzo uno
i cluster iniziano con indirizzo due

F - la seconda entry del FAT indica se il FileSystem è stato smontato correttamente
Indica se il file system NON è stato smontato correttamente [Google così dice] oppure segnala qualche errore hardware

V - lo stato di allocazione dei cluster è conservato nella struttura FAT

V - lo stato di non allocazione dei cluster è indicato con ZERO all' interno della FAT
F - lo stato di allocazione dei cluster è indicato con ZERO (non allocato) o con UNO (allocato)
Lo stato di allocazione è indicato con ZERO (non allocato) mentre se è allocato contiene l'indirizzo del prossimo cluster oppure il marcatore End-Of-File (0xf..8) se è l'ultimo cluster

F - nel boot sector è contenuta l'informazione sulla tipologia di FAT
Non è contenuta da nessuna parte, per scoprire la tipologia bisogna calcolare i dati presenti nel boot sector

F - il FSINFO è una struttura di dati fondamentale per il FAT32

I dati contenuti in FSINFO Non sono essenziali, sono solo una guida per il S.O. e potrebbero non essere accurati

SISTEMI OPERATIVI

Nell’analisi dei sistemi operativi

V - in un SO windows la gran parte delle impostazioni del sistema e dell'utente sono memorizzate nel registro di sistema

F - in un SO windows il file SAM contiene sempre l’elenco di tutti gli account utente che possono avere accesso al sistema
Contiene l’elenco di tutti gli account che si sono loggati almeno una volta su quella macchina (possono esserci account online che hanno l’accesso ma non l’hanno effettuato su quella determinata macchina)

V - il SO Windows è molto meno rigido nella gestione della struttura del FileSystem rispetto ad un SO Linux
F - il SO Windows è molto più rigido nella gestione della struttura del FileSystem
Windows è molto flessibile nella gestione del file system

F - il SO di Windows registra molti più log di un SO Linux
Linux registra molti più log di windows

F - in SO Windows i thumbnail del sistema sono sempre coerenti con i file residenti
Potrebbero esserci thumbnail di file non più residenti

F - SO Windows è il sistema meno documentato
Windows è il più documentato

V - In SO Apple il FileValut offre la funzionalità di cifratura
F - In SO Apple il FileValut contiene l’elenco degli utenti che hanno accesso al sistema

F - SO Apple è il sistema più documentato
V - l’analisi dei thumbnail viene eseguita per avere informazioni sulle immagini non più presenti

F - lo Swapfile in un SO Windows è posizionato nel percorso /private/var/vm/
il pagefile.sys si trova nella root di windows

V - lo Swapfile in un SO Apple è posizionato nel percorso /private/var/vm/
V- In SO Windows HKEY_USERS è una hive del registro di sistema che contiene le impostazioni dell’utente

F – In SO Linux i file dell’utente si trovano in giro per il sistema

In Linux i file dell’utente si trovano esclusivamente nella propria home directory

F - in un SO Windows i file dell'utente si trovano esclusivamente della propria home directory

V - il pagefile.sys del SO Windows si trova nella root del disco
F - il pagefile.sys del SO Apple si trova nella root del disco
è posizionato nel percorso /private/var/vm/

F - il pagefile.sys rappresenta un dump della memoria
F - il pagefile.sys rappresenta un dump della RAM

Il pagefile.sys rappresenta un estensione della memoria RAM

MOBILE FORENSICS

Nella mobile Forensics

F - Nella Logical Extraction bisogna preoccuparsi di decodificare i dati estratti
I dati estratti tramite logical extraction sono già in chiaro

F - Nella Logical Extraction otteniamo i dati così come sono all'interno del dispositivo
Otteniamo i dati che sono messi in strutture dati che dipendono dallo strumento di acquisizione

F - la Logical Extraction dipende dal chipset del dispositivo
Dipende dall'API del dispositivo

V - nella Physical Extraction bisogna preoccuparsi di decodificare i dati estratti

F - la Physical Extraction dipende SOLO dalla versione del SO e dai livelli di patch di sicurezza
Dipende anche dal chipset e dal produttore del device

V - la Physical Extraction dipende ANCHE dalla versione del SO e dai livelli di patch di sicurezza

V - nella Physical Extraction si ottiene tutto il contenuto presente nel dispositivo

F - La Physical Extraction può essere eseguita su quasi la totalità dei dispositivi
La manual extraction può essere eseguita su quasi tutti i dispositivi

F - La Manual Extraction è il metodo più veloce per eseguire una copia dei dati presenti
La manual extraction è il metodo più lento per estrarre dati

V - la Manual Extraction si esegue fotografando il contenuto del dispositivo

V - la Manual Extraction può essere eseguita su quasi la totalità dei dispositivi

F - la Manual Extraction può sempre essere impiegata
Non può essere eseguita in caso di schermo rotto o codice di sblocco

F - nella FileSystem Extraction si ottiene sempre tutto il contenuto presente nel dispositivo
Dipende dai permessi con cui vengono effettuate le richieste

F - nella FileSystem Extraction non bisogna preoccuparsi di decodificare i dati estratti

Bisogna decodificare l'output per visualizzare i dati contenuti

V - nella FileSystem EXtraction si ottengono i DB così come sono presenti nel dispositivo