PROCEDIMENTO PENALE E ATTORI DEL PROCEDIMENTO

L’incidente probatorio

V - può essere richiesto dal p.m.
F - viene richiesto SOLO dal p.m.
V- ha lo scopo di formare la prova
F - viene richieste per velocizzare il procedimento
F - il GIP può nominare un consulente tecnico di parte
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
V - si conclude con il giudicato penale
F - si instaura esclusivamente su iniziativa di una parte

Il procedimento Civile

V - le parti in giudizio sono: l'attore ed il convenuto
V - Si realizza in un’unica struttura: il tribunale
F - 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
F - ha lo scopo di accertare la verità nell'interesse dello stato e della collettività
F - si instaura su iniziativa di una parte: il convenuto
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

Il GIP Giudice per le indagini preliminari

F - è l’unico interlocutore del Pubblico Ministero
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

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
F - indica al perito che deve eseguire un accertamento tecnico non ripetibile
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)
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?)

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

F - il difensore dell'imputato
F - il difensore dell'indagato (F?)
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
V - il consulente tecnico di parte della persona offesa (CTP)
F - il Perito

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

Il sequestro logico:

F - se il dispositivo è acceso bisogna preoccuparsi del problema dello shut down
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
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
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

La preview in un sistema acceso (LIVE)

F - può essere eseguita con una distro live forensics oriented
V - rende veloce l'analisi dei software presenti nel sistema
F - può essere eseguito con qualsiasi tool forensics oriented indipendentemente dal sistema da analizzare
F - è consigliabile eseguirla con un "write blocker"

La preview in un sistema spento (DEAD)

F - velocizza l'analisi dei software presenti nel sistema
F - il sistema da analizzare se è acceso, non deve essere spento
F - può essere sempre eseguita
V - deve essere eseguita con un "write blocker"
F - è più rischiosa di quella in un sistema acceso (LIVE)

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
F - l'hash della copia forense coincide con l'hash calcolato dalla medesima copia dopo la fase di analisi
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 (**validazione)**
F - l'hash della copia forense coincide con l'hash calcolato dal supporto originale (**validazione**)
F - la copia forense è inalterabile (**opp**. la copia forense sarà immodificabile)
F - i dati della copia forense sono identici ai dati originali
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 - 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
V - dovrebbe essere eseguita da tecnici specializzati poiché vi è il rischio di alterazione della prova
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
F - 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 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
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
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"
V - è corretto
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
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
F - esegue copie forensi (anche) di tipo logico
V - esegue copie forensi solo di topo "full disk"

FTK Imager

V - è uno strumento per elaborare copie forensi
F - riconosce tutti i tipi di FileSystem
V - riconosce solo determinati 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
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
V - fa uso di 64 costanti additive
F - l'output è un digest a 160bit
V - l'output è un digest a 128bit

V - rispetto a MD4 fa uso di 62 costanti in più
F - rispetto a MD4 fa uso di 2 costanti in più
V - il terzo round è composto da 48 operazioni (16 operazioni per round)
F - il quarto round è composto da 48 operazioni

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

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
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"
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

V - Il modulo “File Extention Dismatch” dipende dal modulo “File Type”
V - il modulo “Encryption Detenction” permette di evidenziare possibili file protetti
F - il modulo “Encryption Detenction” permette di trovare e decifrare i file protetti
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
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
F - i dati essenziali possono non essere coerenti
V - i dati non essenziali possono non essere coerenti
F - il “Content Category” comprende le informazioni sul layout
V - in "Content Category" i dati sono organizzati in "data unit"
F - il “Metadata Category” comprende le informazioni sul layout
F - in “Metadata Category” i dati sono organizzati in “data unit”
F - il "FileSystem Category" comprende le informazioni sull'indirizzo delle "data unit" (Quello è il Metadata)
V - il “FileSystem Category” comprende le informazioni sul layout
F - in “Application Category” sono presenti i dati essenziali per alcune funzionalità del FileSystem
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
F - MBR è costituito da almeno quattro settori
F - può contenere al massimo 8 porzioni
V - può contenere al massimo 4 partizioni primarie
F - può contenere al massimo 4 secondary extension 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", prensente nella "partition table", indica il cluster iniziale della partizione

Nel NTFS

F - una entry MFT può contenere solo un attributo di tipo $DATA
F - in una MFT entry, il contenuto di un attributo 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
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
V - Nel file $BitMap è indicato lo stato di allocazione di ciascun cluster
F - Il file $BitMap indica i cluster danneggiati
F - ad esclusione delle strutture del FileSystem tutto il resto è gestito come file
F - nel file $BadClus è indicato lo stato di allocazione di ciascun cluster
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
F - nel FAT12/16 la root directory ha dimensione dinamica
V - nel FAT32 la root directory ha dimensione dinamica
F - le entry del FAT sono a dimensione variabile
V - le prime due entry del FAT non sono utilizzate per i cluster
V - la dimensione delle entry del FAT dipendono dalla tipologia di FAT
F - i cluster iniziano con indirizzo uno
F - la seconda entry del FAT indica se il FileSystem è stato smontato correttamente
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)
F - nel boot sector è contenuta l'informazione sulla tipologia di FAT
F - il FSINFO è una struttura di dati fondamentale per il FAT32

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
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
F - il SO di Windows registra molti più log di un SO Linux
F - in SO Windows i thumbnail del sistema sono sempre coerenti con i file residenti
F - SO Windows è il sistema meno 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/
V - lo Swapfile in un SO Apple è posizionato nel percorso /private/var/vm/
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
F - il pagefile.sys rappresenta un dump della memoria
F - il pagefile.sys rappresenta un dump della RAM

MOBILE FORENSICS

Nella mobile Forensics

F - Nella Logical Extraction bisogna preoccuparsi di decodificare i dati estratti
F - Nella Logical Extraction otteniamo i dati così come sono all’interno del dispositivo
F - la Logical Extraction dipende dal chipset 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
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
F - La Manual Extraction è il metodo più veloce per eseguire una copia dei dati presenti
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
F - nella FileSystem Extraction si ottiene sempre tutto il contenuto presente nel dispositivo
F - nella FileSystem Extraction non bisogna preoccuparsi di decodificare i dati estratti
V - nella FileSystem EXtraction si ottengono i DB così come sono presenti nel dispositivo