

La copia forense

- ☐ deve essere sempre eseguita con un write blocker
- ☒ è una duplicazione dei dati eseguita in modo tale da garantire la ripetibilità della successiva operazione di analisi
- ☒ è una qualunque copia di dati purché rispetti le caratteristiche di validazione e preservazione
- ☒ 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
- ☒ è una duplicazione dei dati eseguita in modo tale da garantire la ripetibilità della successiva operazione di analisi
- ☒ è una qualunque copia di dati purché rispetti le caratteristiche di validazione e preservazione
- ☒ 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
- ☒ non produce una copia forense
- ☒ esegue la copia della sorgente "sda"
- ☒ esegue il calcolo dell'hash on-the-fly dell'immagine "sda.dd"

FTK Imager

- ☒ è uno strumento per la produzione copie forensi
- ☒ 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 formato DD/Raw:

- ☒ non conserva nei metadati 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"



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
- ☒ 64bit per la lunghezza del messaggio
- ☒ un bit a "1" al 1025° bit
- ☒ nessun bit di padding
- ☐ 1024bit



I Toolkit

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

Autopsy

- ☒ permette la selezione dei file di interesse solo tramite "tag"
 - ☐ Il modulo "Encryption Detection" permette trovare e decifrare i file protetti
 - ☒ 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"
- ☐ Permette solo una configurazione "single user" 
- ☒ 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"
- ☒ Il modulo "Encryption Detection" permette di evidenziare possibili file protetti

Partizionamento DOS

- ☒ Il settore contenente l'MBR termina con una signature
- ☐ L'MBR è costituito da almeno quattro settori
- ☒ 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
- ☒ In "Content Category" i dati sono organizzati in "Data Unit"
- ☐ il "File System Category" comprende le informazioni sull'indirizzo delle "Data Unit"
- ☒ In "Application Category" sono presenti i dati essenziali per alcune funzionalità del File System
- ☒ La strategia di allocazione del "primo disponibile" ricerca una "Data Unit" libera partendo dall'inizio del FileSystem



Nel FAT File System

- ☒ Le data unit si chiamano cluster
- ☒ 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
- ☒ Lo stato di allocazione dei cluster è conservato nella struttura FAT
- ☐ I cluster iniziano con indirizzo uno

Nel NT File System

- ☐ Ad esclusione delle strutture dati del FileSystem tutto il resto è gestito come file
- ☒ 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
- ☒ 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 eseguire una copia dei dati presenti
- ☒ 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

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

Nel FAT File System

- ☐ Le data unit si chiamano settori
- ☒ Le entry del FAT sono a dimensione variabile
- ☒ Nel FAT32 la root directory ha dimensione dinamica
- ☒ Lo stato di allocazione dei cluster è indicato con ZERO (non allocato) o con UNO (Allocato)
- ☒ 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
- ☒ Nel File \$Bitmap è indicato lo stato di allocazione di ciascun cluster
- ☒ 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
- ☒ 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
- ☒ 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"
- ☒ è corretto
- ☒ 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:

- ☒ 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
- ☒ Dovrebbe essere compiuto da tecnici specializzati poiché vi è rischio di alterazione della prova
- ☒ è particolarmente utile ad individuare le fonti di prova
- ☐ può essere eseguito solo con l'ausilio di un writeblocker



Nel File System

- ☒ I dati non essenziali possono non essere coerenti
- ☒ 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
- ☒ 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
- ☒ Può essere impiegato anche come strumento per la c.d. preview
- ☒ 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
- ☒ rispetto a MD4 fa uso di 62 costanti in più
- ☒ 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
- ☒ 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 urgenza 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
- ☒ Indica al Consulente Tecnico che deve eseguire un accertamento tecnico non ripetibile
- ☐ chidendo autorizzazione al GIP (Giudice Indagini Preliminari)
- ☒ Quando vuole dissequestrare il bene oggetto di accertamento tecnico



Partizionamento DOS

- ☒ Il settore contenente l'MBR termina con una signature
- ☐ può contenere al massimo 8 partizioni
- ☐ Nelle entry della "Partition Table" è sempre indicato il tipo di partizione
- ☒ 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



- ☒ processano\elaborano il contenuto disk image
- ☐ non permettono di ottenere diverse visualizzazioni dei dati
- ☒ 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

- ☒ La Physical Extraction dipende solo dalla versione del SO e dai livelli di patch di sicurezza
- ☒ Nella File System Extraction si ottengono i DB così come sono presenti 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

- ☒ 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

- ☒ Il "Central Repository" permette di rapportare il caso in esame con i precedenti casi già elaborati
- ☐ Permette solo una configurazione "single user"
- ☒ Il disk image viene processato tramite dei "Ingest Modules"
- ☒ 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



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



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



Quando vuole dissequestrare il bene oggetto di accertamento tecnico



Quali caratteristiche sono proprie della Persona Offesa



In determinati casi può ritirare la querela



è colui che assiste alla commissione di un reato



Può prendere parte solo alla fase di giudizio



Può sporgere denuncia

Nella fase di identificazione, la preview...

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