Esame di Computer Forensics

Test di autovalutazione apprendimento

*Campo obbligatorio

Indirizzo email *

Il tuo indirizzo email

In Analisi, montare un file immagine

- [ ] implica che il sistema debba riconoscere il File System presente
- [ ] non è utile per impiegare strumenti non forensic oriented
- [ ] si ha la completa visione di tutto il contenuto presente
- [ ] è utile soprattutto per analisi mirate
- [ ] non vi è mai il rischio di alterare il file immagine

Nel NT File System

- [ ] Una Entry MFT può contenere solo un attributo di tipo $DATA
- [ ] In ogni entry MFT di Base vi è un attributo di tipo $STANDARD_INFORMATION
- [ ] Ad esclusione delle strutture dati del FileSystem tutto il resto è gestito come file

- [ ] non vi è mai il rischio di alterare il file immagine

Nel NT File System

- [ ] Una Entry MFT può contenere solo un attributo di tipo $DATA
- [ ] In ogni entry MFT di Base vi è un attributo di tipo $STANDARD_INFORMATION
- [ ] Ad esclusione delle strutture dati del FileSystem tutto il resto è gestito come file
- [ ] Nel File $BadClus è indicato lo stato di allocazione di ciascun cluster
- [ ] In ogni entry MFT di Base vi è un attrubuto di tipo $ATTRIBUTE_LIST

Nel FAT File System

- [ ] Le data unit si chiamano settori
- [ ] Le entry del FAT sono a dimensione variabile
- [ ] La seconda entry del FAT indica se il FileSystem è stato "smontato" correttamente
- [ ] Lo stato di non allocazione dei cluster è indicato con ZERO all'interno della FAT
- [ ] Il FSINFO è una struttura dati fondamentale per il FAT32

il formato E01:

- [ ] non conserva il calcolo dell'hash

Guymager

- [ ] permette di produrre disk image nel formato E01
- [ ] non fa uso dell'hashing on-the-fly
- [ ] non permette di segmentare/splittare il file immagine
- [ ] esegue copie forensi di tipo logico
- [ ] non permette la scelta del tipo di hash da calcolare

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

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

Partizionamento DOS

- [ ] Contiene sempre un MBR
- [ ] Contiene sempre un EBR

il formato E01:

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

Nell'algoritmo di MD5 se il messaggio di input M è di 1024bit, dopo il padding avremo che M' sarà costituito da:

- [ ] 4 blocchi da 512bit
- [ ] 60bit per la lunghezza del messaggio
- [ ] un bit a "1" al 1025° bit
- [ ] 448 bit di padding
- [ ] 2048bit

Nell'analisi dei Sistemi Operativi

- [ ] In un SO Windows la granparte delle impostazioni del sistema e dell'utente sono memorizzate nel Registro di Sistema

Nell'analisi dei Sistemi Operativi

- [ ] In un SO Windows la granparte delle impostazioni del sistema e dell'utente sono memorizzate nel Registro di Sistema
- [ ] Il SO Windows registra molti più log di un SO Linux
- [ ] Lo Swapfile in un SO Windows è posizionato nel percorso /private/var/vm/
- [ ] In un SO Windows i file dell'utente si trovano esclusivamente nella propria home directory
- [ ] Il PageFile.sys rappresenta un dump della RAM

L'incidente Probatorio...

- [ ] può essere richiesto dal P.M.
- [ ] ha lo scopo di formare la prova
- [ ] viene richiesto per velocizzare il procedimento
- [ ] il GIP può nominare un consulente tecnico di parte
- [ ] nessuna delle altre risposte

Guymager

- [ ] permette di produrre disk image nel formato E01

I Toolkit

- [ ] permettono di eseguire la classificazione bad extension confrontando l'estensione del file con la signature in esso presente
- [ ] permettono esclusivamente una visualizzazione gerarchica dei file
- [ ] non hanno ancora sviluppato una ricerca tramite hash
- [ ] eseguono in maniera automatizzata tutta l'analisi
- [ ] permettono di eseguire il file carving ricercando l'header ed il footer dei file conosciuti

Autopsy

- [ ] permette la selezione dei file di interesse solo tramite "tag"
- [ ] Il modulo "Encryption Detection" permette trovare e decifrare i file protetti
- [ ] Il modulo "File Extension Mismatch" dipende dal modulo "File Type"
- [ ] il "file carving" viene eseguito su tutto il disk image
- [ ] non permette l'aggiunta di ulteriori moduli di analisi

Qual'è l'ambito di applicazione della computer forensics

- [ ] I soli reati che hanno come obiettivo un sistema informatico
- [ ] I soli reati che hanno come mezzo un sistema informatico
- [ ] Qualsiasi reato dove possa esistere un sistema informatico coinvolto a qualsiasi

- [ ] Le parti in giudizio possono nominare un Consulente Tecnico

Nella Mobile Forensics

- [ ] Nella Logical Extraction bisogna preoccuparsi di decodificare i dati estratti
- [ ] Nella Physical Extraction si ottiene tutto il contenuto presente nel dispositivo
- [ ] La Physical Extraction può essere eseguita su quasi la totalità dei dispositivi
- [ ] Nella File System Extraction si ottiene sempre tutto il contenuto presente nel dispositivo
- [ ] La logical Extraction dipende dal chipset del dispositivo

Autopsy

- [ ] permette la selezione dei file di interesse tramite "checkbox"
- [ ] le informazioni dal registro di sistema vengono estratte tramite il tool "RegistryViewer"
- [ ] il modulo "Hash Lookup" permette di impostare sia una lista di "Ignorable File" e sia di "Notable File"
- [ ] Il modulo che si preoccupa di estrarre informazioni dal cestino di sistema è "RecycleBin Activity"
- [ ] pemette solo una configurazione "single user"

Partizionamento DOS

- [ ] Contiene sempre un MBR
- [ ] Contiene sempre un EBR
- [ ] nella "Partition Table" è indicato il tipo di partizione
- [ ] può contenere al massimo 4 secondary extended partition
- [ ] Il campo "Starting LBA Address", presente nella "Partition Table", indica il cluster iniziale della partizione

Nel File System

- [ ] le informazioni temporali sono dati essenziali
- [ ] In "Content Category" i dati sono organizzati in "Data Unit"
- [ ] il "File System Category" comprende le informazioni sull'indirizzo delle "Data Unit"
- [ ] l'indirizzo della "Data Unit" dove è memorizzato un file è un dato essenziale
- [ ] La strategia di allocazione del "prossimo disponibile" ricerca una "Data Unit" libera partendo dall'inizio del FileSystem

I Toolkit

- [ ] permettono di eseguire la classificazione bad extension confrontando l'estensione del file con la signature in esso presente
- [ ] permettono esclusivamente una visualizzazione gerarchica dei file

- [ ] Il modulo che si preoccupa di estrarre informazioni dal cestino di sistema è "RecycleBin Activity"
- [ ] pemette solo una configurazione "single user"

La c.d. "preview"

- [ ] Può essere compiuto da qualisiasi agente della P.G. poiché ha un basso rischio di alterazione della prova
- [ ] è uno strumento di ricerca della prova permesso agli inquirenti in sede di perquisizione
- [ ] non è particolarmente utile ad individuare le fonti di prova
- [ ] il suo uso non è esplicitamente indicato nel codice di penale
- [ ] deve essere eseguita impiegando obbligatoriamente un write blocker

- [ ] il "file carving" viene eseguito su tutto il disk image
- [ ] non permette l'aggiunta di ulteriori moduli di analisi

Qual'è l'ambito di applicazione della computer forensics

- [ ] I soli reati che hanno come obiettivo un sistema informatico
- [ ] I soli reati che hanno come mezzo un sistema informatico
- [ ] Qualsiasi reato dove possa esistere un sistema informatico coinvolto a qualsiasi titolo
- [ ] I reati informatici descritti dal codice penale
- [ ] I reati informatici descritti dal codice di procedura penale

Il procedimento civile...

- [ ] Le parti in giudizio sono: l'attore ed il convenuto
- [ ] Le parti in giudizio sono: l'indagato ed il ricorrente
- [ ] Ha lo scopo di accertare la verità nell'interesse dello Stato e della collettività
- [ ] Si instaura esclusivamente su iniziativa di una parte: il convenuto
- [ ] Le parti in giudizio possono nominare un Consulente Tecnico

Nella Mobile Forensics