

COMPUTER FORENSICS



DIE UNIVERSITÀ DI NAPOLI FEDERICO II

Esame di Computer Forensics

Test di autovalutazione apprendimento

*Campo obbligatorio

Email *

Il tuo indirizzo email

Autopsy

- Il modulo "Exif Parser" dipende dal modulo "Embedded File Extractor"
- Il modulo "PhotoRec Carver" permette all'utente di scegliere se eseguire il file carving anche sull'"unallocated space"
- 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 è "RecycleBin Activity"
- Il modulo "Embedded File Extractor" estrae i "File Archive"

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

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 del cluster è indicato con ZERO (non allocato) o con UNO (Allocato)
- Le prime due entry del FAT non sono utilizzate per i cluster

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

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

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 riccalcolato sulla copia forense varierebbe alla minima alterazione della copia stessa
- i dati della copia forense sono identici ai dati originali

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

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

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"

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

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" ricerchando la signature del file

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

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

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

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

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

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
- Indica al Consulente Tecnico che deve eseguire un accertamento tecnico non ripetibile
- chiedendo autorizzazione al GIP (Giudice Indagini Preliminari)
- Quando vuole disassegnare il bene oggetto di accertamento tecnico

Invia

Pagina 1 di 1

Questi contenuti non sono creati né avallati da Google. Segnalala una violazione - Termini di servizio - Norme sulla privacy.

Google Moduli

Chi può prendere parte agli accertamenti tecnici ripetibili ai sensi dell'art. 359 cpp?

- l'indagato con il proprio difensore
- la persona offesa
- il consulente tecnico dell'indagato (CTP)
- il consulente tecnico del P.M. (CTU)
- il Perito

Il procedimento civile...

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

Nella fase di identificazione, la preview...

- in alcuni casi c'è il rischio inevitabile di alterare il reperto
- deve essere eseguita realizzando la copia forense
- può essere eseguita su di un sistema acceso
- non devono essere accesi i dispositivi rinvenuti spenti
- non è particolarmente utile ad individuare le fonti di prova

E' errata, perché esiste la preview live(dove è possibile fare la preview live)

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

La risposta errata sarebbe stata corretta per la validazione, perché la preservazione garantisce che l'hash della sorgente non sia cambiato successivamente.

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 è corretto per eseguire una copia forense
- esegue la copia della sorgente "sda"
- esegue il calcolo dell'hash on-the-fly dell'immagine "sda.dd"

E' corretto, ma non è corretto per la copia forense, ed realizza l'hash on the fly siccome sta il TEE

FTK Imager

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

Fa uso dell'hash on the fly, e non è possibile escluderlo. E non permette il tipo di hash da calcolare(di default utilizza solo MD5 e SHA1)

il formato E01:

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

La copia logica di una cartella\directory viene fatta dal formato L01.

In Analisi, montare un file immagine

- implica che bisogna riconoscere il File System presente
- permette l'esportazione del calcolo dell'hash dei file di interesse
- si ha la completa visione di tutto il contenuto presente
- permette di ottenere una analisi completa
- non vi è il rischio di alterare il file immagine

Non si ha visione di tutto il contenuto esempio immagini compresse o archivi

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

Processano ed elaborano il contenuto del disk image(funzione principale)

Sono da aiuto ma non realizzano la gran parte dell'analisi

Permettono di eseguire il file carving su header e footer non su signature

Autopsy

- Il modulo "Keyword Search" impiega "Apache Solr"
- Il modulo "Hash Lookup" permette solo di importare la lista di "Notable File"
- Il modulo "Interesting Files" permette di evidenziare i file corrispondenti a determinate regole
- Il modulo che si preoccupa di estrarre informazioni dai browser è "Internet Activity"
- permette la selezione dei file di interesse tramite "checkbox"

E' possibile eseguire di evidenziare al forense determinati file interessanti.

Autopsy

- Il "file carving" viene svolto tramite il tool "PhotoRec"
- Il "file carving" viene svolto su tutto il disk image
- Il modulo che si preoccupa di estrarre informazioni dai browser è "Browser Activity"
- Il modulo "Hash Lookup" permette solo di importare la lista di "Ignorable File"
- Le informazioni dal registro di sistema vengono estratte tramite il tool "RegistryViewer"

Il file carving non viene fatto su tutto il disk image, ma solo sull'unlocated space

Partizionamento DOS

- Contiene sempre un MBR
- Contiene sempre un EBR
- non ha limite al numero di partizioni che può contenere
- può contenere al massimo 4 secondary extended partition
- l'EBR può contenere al massimo 1 entry

Non ha limite al numero di partizioni che può contenere, Il limite delle partizioni primarie è 4, poi quelle secondarie non ci sono limiti.

Nel FAT File System

- Ad ogni entry del FAT corrisponde un Cluster
- Il layout è costituita da una Reserved Area, FAT Area e una Data Area
- Nel FAT12/16 la root directory ha dimensione dinamica
- Lo stato di allocazione del cluster è conservato nella struttura FAT
- I cluster iniziano con indirizzo tre

Alle prime due entry del fat non corrispondono alcun cluster(contengono altre informazioni come il dirty status, che indicano se il file system è stato smontato correttamente oppure no)

Nel NT File System

- Una Entry MFT può contenere solo un attributo di tipo \$DATA
- Le Entry MFT vengono pulite non appena il flag "in uso" viene settato
- Ad esclusione delle strutture dati del FileSystem tutto il resto è gestito come file
- Il File \$BitMap indica i cluster danneggiati ↗
- In ogni entry MFT di Base vi è un attributo di tipo \$ATTRIBUTE_LIST

Le entry MFT vengono pulite solo quando il flag "in uso" viene settato

L'attribute_list si ha solo se il file viene descritto con più entry

Nell'analisi dei Sistemi Operativi

- In un SO Windows il file SAM contiene l'elenco di tutti gli account utente che possono avere accesso al sistema
- In SO Apple il FileVault contiene l'elenco degli utenti che ha accesso al sistema
- 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 Windows si trova nella root del disco

Nei sistemi windows tutti i file principali del suo funzionamento a livello file system si trovano nella root

Nella Mobile Forensics

- La Manual Extraction è il metodo più veloce per eseguire una copia dei dati presenti
 - Nella Physical Extraction bisogna preoccuparsi di decodificare i dati estratti
 - La Physical Extraction può essere eseguita su quasi la totalità dei dispositivi
 - La Logical Extraction otteniamo i dati così come sono all'interno del dispositivo
 - La Physical Extraction dipende solo dalla versione del SO e dai livelli di patch di sicurezza
-

Dire cosa cambia tra physical Extraction e logical extraction o file system extracion(Credo che sia domanda di teoria)

Nella physical extraction bisogna preoccuparsi di decodificare i dati estratti, perché ho un'estrazione di tutti i dati estratti del dispositivo così come sono, ad esempio DB vanno relazionati per vedere tutto il contenuto all'interno

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 SDATA
- 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 attributo 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 EO1:

- 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 gran parte delle impostazioni del sistema e dell'utente sono memorizzate nel Registro di Sistema

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
- 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"
- permette 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"
- permette solo una configurazione "single user"

La c.d. "preview"

- Può essere compiuto da qualsiasi 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

Chi può prendere parte agli accertamenti tecnici ripetibili ai sensi dell'art. 359 cpp?

- l'indagato con il proprio difensore
- la persona offesa
- il consulente tecnico dell'indagato (CTP)
- il consulente tecnico del P.M. (CTU)
- il Perito

Il procedimento civile...

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

Nella fase di identificazione, la preview...

- in alcuni casi c'è il rischio inevitabile di alterare il reperto
- deve essere eseguita realizzando la copia forense
- può essere eseguita su di un sistema acceso
- non devono essere accesi i dispositivi rinvenuti spenti
- non è particolarmente utile ad individuare le fonti di prova

E' errata, perché esiste la preview live(dove è possibile fare la preview live)

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

La risposta errata sarebbe stata corretta per la validazione, perché la preservazione garantisce che l'hash della sorgente non sia cambiato successivamente.

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 è corretto per eseguire una copia forense
- esegue la copia della sorgente "sda"
- esegue il calcolo dell'hash on-the-fly dell'immagine "sda.dd"

E' corretto, ma non è corretto per la copia forense, ed realizza l'hash on the fly siccome sta il TEE

FTK Imager

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

Fa uso dell'hash on the fly, e non è possibile escluderlo. E non permette il tipo di hash da calcolare(di default utilizza solo MD5 e SHA1)

il formato E01:

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

La copia logica di una cartella\directory viene fatta dal formato L01.

In Analisi, montare un file immagine

- implica che bisogna riconoscere il File System presente
- permette l'esportazione del calcolo dell'hash dei file di interesse
- si ha la completa visione di tutto il contenuto presente
- permette di ottenere una analisi completa
- non vi è il rischio di alterare il file immagine

Non si ha visione di tutto il contenuto esempio immagini compresse o archivi

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

Processano ed elaborano il contenuto del disk image(funzione principale)

Sono da aiuto ma non realizzano la gran parte dell'analisi

Permettono di eseguire il file carving su header e footer non su signature

Autopsy

- Il modulo "Keyword Search" impiega "Apache Solr"
- Il modulo "Hash Lookup" permette solo di importare la lista di "Notable File"
- Il modulo "Interesting Files" permette di evidenziare i file corrispondenti a determinate regole
- Il modulo che si preoccupa di estrarre informazioni dai browser è "Internet Activity"
- permette la selezione dei file di interesse tramite "checkbox"

E' possibile eseguire di evidenziare al forense determinati file interessanti.

Autopsy

- Il "file carving" viene svolto tramite il tool "PhotoRec"
- Il "file carving" viene svolto su tutto il disk image
- Il modulo che si preoccupa di estrarre informazioni dai browser è "Browser Activity"
- Il modulo "Hash Lookup" permette solo di importare la lista di "Ignorable File"
- Le informazioni dal registro di sistema vengono estratte tramite il tool "RegistryViewer"

Il file carving non viene fatto su tutto il disk image, ma solo sull'unlocated space

Partizionamento DOS

- Contiene sempre un MBR
- Contiene sempre un EBR
- non ha limite al numero di partizioni che può contenere
- può contenere al massimo 4 secondary extended partition
- l'EBR può contenere al massimo 1 entry

Non ha limite al numero di partizioni che può contenere, Il limite delle partizioni primarie è 4, poi quelle secondarie non ci sono limiti.

Nel FAT File System

- Ad ogni entry del FAT corrisponde un Cluster
- Il layout è costituita da una Reserved Area, FAT Area e una Data Area
- Nel FAT12/16 la root directory ha dimensione dinamica
- Lo stato di allocazione del cluster è conservato nella struttura FAT
- I cluster iniziano con indirizzo tre

Alle prime due entry del fat non corrispondono alcun cluster(contengono altre informazioni come il dirty status, che indicano se il file system è stato smontato correttamente oppure no)

Nel NT File System

- Una Entry MFT può contenere solo un attributo di tipo \$DATA
- Le Entry MFT vengono pulite non appena il flag "in uso" viene settato
- Ad esclusione delle strutture dati del FileSystem tutto il resto è gestito come file
- Il File \$BitMap indica i cluster danneggiati ↗
- In ogni entry MFT di Base vi è un attributo di tipo \$ATTRIBUTE_LIST

Le entry MFT vengono pulite solo quando il flag "in uso" viene settato

L'attribute_list si ha solo se il file viene descritto con più entry

Nell'analisi dei Sistemi Operativi

- In un SO Windows il file SAM contiene l'elenco di tutti gli account utente che possono avere accesso al sistema
- In SO Apple il FileVault contiene l'elenco degli utenti che ha accesso al sistema
- 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 Windows si trova nella root del disco

Nei sistemi windows tutti i file principali del suo funzionamento a livello file system si trovano nella root

Nella Mobile Forensics

- La Manual Extraction è il metodo più veloce per eseguire una copia dei dati presenti
 - Nella Physical Extraction bisogna preoccuparsi di decodificare i dati estratti
 - La Physical Extraction può essere eseguita su quasi la totalità dei dispositivi
 - La Logical Extraction otteniamo i dati così come sono all'interno del dispositivo
 - La Physical Extraction dipende solo dalla versione del SO e dai livelli di patch di sicurezza
-

Dire cosa cambia tra physical Extraction e logical extraction o file system extracion(Credo che sia domanda di teoria)

Nella physical extraction bisogna preoccuparsi di decodificare i dati estratti, perché ho un'estrazione di tutti i dati estratti del dispositivo così come sono, ad esempio DB vanno relazionati per vedere tutto il contenuto all'interno

Esame di Computer Forensics

28/07/2021

*Campo obbligatorio

Email *

Il tuo indirizzo email

- 1) vero ma può anche utilizzare Apache Tika per una string extractor per file e metadati, HTML extractor per commenti e javascript o la normalizzazione
- 2) no anche gli ignorabile
- 3) solo se sono interessanti
- 4) recent activity
- 5) tramite tagging

Autopsy

- Il modulo "Keyword Search" impiega "Apache Solr"
- il modulo "Hash Lookup" permette solo di importare la lista di "Notable File"
- Il modulo "Interesting Files" permette di evidenziare i file corrispondenti a determinate regole
- Il modulo che si preoccupa di estrarre informazioni dai browser è "Internet Activity"
- permette la selezione dei file di interesse tramite "checkbox"

L'algoritmo di Hash MD5

- processa il messaggio in blocchi di 512bit
- è costituito da 3 round e 4 funzioni logiche
- rispetto a MD4 fa uso di 2 costanti in più
- l'output è un digest a 128bit
- il terzo round è composto da 48 operazioni

MD5 divide il messaggio in blocchi da 512 bit, è composto da 4 round con 4 funzioni logiche ed ha 64 costanti additive (quindi 62 in più al MD4).
MD4/MD5 hanno un output di 128 bit (a differenza dello SHA1 che è di 160 bit).
Avendo 16 operazioni per round, allora il terzo round ne avrà 48 (16×3)

il formato E01:

- non conserva il calcolo dell'hash MD5
- permette di conservare i metadati del reperto sorgente
- non permette la compressione
- può contenere la copia logica di una cartella\directory
- è un formato della famiglia "Expert Witness Disk Image Format"

1) lo conserva per lo stesso motivo del pt2
 2) li conserva in quanto fa parte dell'EWF, l'unico a non conservarli è DD/RAW
 3) permette la compressione, infatti ha 3 livelli di compressione: no, good e best. Utilizza l'algoritmo di deflate.
 4) quello è l'Encase L01 Logical
 5) è basato sulla famiglia SMART che fa parte della famiglia Expert Witness Disk Image Format

Nella Mobile Forensics

- Con la Manual Extraction non vi è il rischio di alterare\modificare i dati
- Nella Logical Extraction non bisogna preoccuparsi di decodificare i dati estratti
- La Physical Extraction può essere eseguita su quasi la totalità dei dispositivi
- La Logical Extraction otteniamo i dati così come sono all'interno del dispositivo
- La Physical Extraction dipende solo dalla versione del SO e dai livelli di patch di sicurezza
 - 1) Con la Manual, proprio nei limiti viene detto che potrebbe andare ad alterare o modificare i dati
 - 2) No, i dati dipendono solo dalle API che li estraggono e non viene mai detto che debbano essere processati (diverso da Physical e File System)
 - 3) No (dal disegno a piramide), quelle cose da cui dipende o anche all'interno dei dispositivi cifrati
 - 4) No perché i risultati estratti dipendono sempre dalle API che si utilizzano per estrarre. Rischiano di essere incompleti o imparziali
 - 5) Non dipende SOLO dalla versione del SO e dai livelli di patch di sicurezza ma anche dal produttore del dispositivo e dal chipset

Nel File System

- I dati essenziali pos
- In "Metadata Category" i dati sono organizzati in "Data Unit"
- il "File System 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 un settore non utilizzato di una "Data Unit" allocata

- 1) Devono essere coerenti altrimenti c'è il malfunzionamento del dispositivo
- 2) E' nel content category?
- 3) Il File System Category contiene le informazioni generali sul file system che sono posizionate nel primo settore del volume. Queste non sono altro che i dati essenziali che vanno, dunque a fornire informazioni sul layout.
- 4) Nella domanda viene descritto il Physical Address mentre il Logical Volume Address è il primo settore del volume
- 5) Definizione

Autopsy

- Il modulo "Exif Parser" dipende dal modulo "Embedded File Extractor"
- il modulo "PhotoRec Carver" permette all'utente di scegliere se eseguire il file carving anche sull' "unallocated space"
- 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 è "RecycleBin Activity"
- Il modulo "Embedded File Extractor" estrae i "File Archive"
 - 1) Non sono collegati
 - 2) Lavora sull'unallocated space non su anche
 - 3) Analizza le VM ma non le va a generare
 - 4) Perchè estraendo i file contenuti in altri file ha senso

In Analisi, FTK Imager

- Riconosce solo determinati File System
- Permette di visionare il contenuto dei Disk Image
- Permette di visualizzare solo i file residenti
- Non deve essere impiegato come strumento per la c.d. preview
- Permette di visionare\analizzare solo Disk Image

- 1) vero, infatti nelle slides c'è una tabella, tra cui: NTFS, FAT12/16/32
- 2) si come dischi rigidi locali, unità di rete, floppy disk etc.
- 3) no anche quelli che sono stati eliminati dal cestino ma che non sono ancora stati sovrascritti
- 4) può essere impiegato per la c.d. preview
- 5) no anche file system e cd/dvd formats

FTK Imager

- 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 solo di tipo "full disk"
- non permette la scelta del tipo di hash da calcolare

- 1) E' uno dei formati supportati insieme a DD/RAW, SMART e AFF
- 2) Lo usa
- 3) Lo permette
- 4) esegue anche copie di tipo full disk ma può anche copiare file/cartelle che si trovano in determinati punti del file system di supporto
- 5) perchè ha di default lo SHA1 e MD5

- 1) contiene le credenziali di tutti gli utenti che hanno diritto all'autenticazione nel sistema ma non sempre solo se l'hash della password del file SAM e quella inviata dall'utente coincidono
 2) Windows ha pochi log
 3) non sempre, può succedere che in alcuni casi venga proposta la stessa miniatura per tutti i file residenti
 4) per esclusione
 5) No perché rappresenta l'estensione della RAM che si trova nella root del disco
- Nell'analisi dei Sistemi:

- In un SO Windows il file SAM contiene sempre l'elenco di tutti gli account utente che possono avere accesso al sistema
- Il SO Windows registra molti più log di un SO Linux
- In SO Windows i thumbnail del sistema sono sempre coerenti con i file residenti
- Il SO Apple è uno dei sistemi meno documentati
- Il PageFile.sys rappresenta un dump della RAM

Partizionamento DOS

- può contenere al massimo 4 partizioni primarie
- può contenere al massimo 8 partizioni
- può contenere delle secondary extended partition
- La "Partition Table" è costituita da massimo otto entry
- Contiene sempre un MBR ed un EBR

- 1) Vero
 2) Non viene detto da nessuna parte
 3) Dopo che sono state usate le primary extended partition possiamo trovare le secondary che possono avere le secondary extended partition
 4) No, sono 4
 5) Vera nel primo caso ma falsa per l'EBR che può anche non esserci

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 tutta l'analisi
- permettono di decifrare i file protetti mediante il "file carving"

- 1) è proprio la funzione principale dei toolkit
 2)
 3) Il Know file permette proprio di eseguire un analisi basandosi sull'hash
 4) sono di aiuto per l'analisi ma non la vanno a realizzare tutta
 5) Il file carving è il recupero dei file non più residenti nel file system quindi non ha proprio senso quello che sta scritto

Nel FAT File System

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

- 1) Si chiamano Cluster
- 2) Vero
- 3) no solo nel FAT 32 è di dimensione variabile, nel 12/16 ha dimensione un settore
- 4) e contiene anche la cluster chain ovvero i cluster successivi
- 5) Iniziano all'indirizzo 2 della data area

Nel NT File System

- Una Entry MFT può contenere solo un attributo di tipo \$DATA
- Le Entry MFT vengono pulite non appena il flag "in uso" viene settato
- La dimensione del cluster è indicato nella Tabella MFT
- Il File \$BitMap indica i cluster danneggiati
- Le informazioni temporali sul file sono contenute solo all'interno dell'attributo \$STANDARD_INFORMATION

- 1) No, può contenere anche gli ADS che sono ulteriori \$DATA
- 2) infatti vengono pulite solo quando il flag in uso viene settato
- 3) nella DATA AREA
- 4) indica lo stato di allocazione dei cluster
- 5) Indica lo stato di allocazione di un cluster insieme alla sicurezza, quota e proprietà

la preview in un sistema acceso (LIVE)

- può essere eseguita con una distro live forensic oriented
- rende veloce l'analisi dei software presenti nel sistema
- i tool forensic oriented devono essere compatibili con il sistema da analizzare
- deve essere eseguita con un write blocker
- non altera il reperto che si sta analizzando

- 1) si può utilizzare su una preview dead che appunto prevede l'utilizzo di vari strumenti per poter analizzare la memoria del dispositivo
- 2) Vero è tra i pro
- 3) Dato che gli strumenti che vengono utilizzati devono essere compatibili con il sistema credo valga uguale
- 4) La dead lo usa
- 5) Può alterarlo



Il GIP (Giudice per le Indagini Preliminari)

- è l'unico interlocutore del Pubblico Ministero
- non emette una sentenza
- può emettere sentenza di non luogo a procedere
- provvede sulle misure cautelari
- ha autonomia di iniziativa probatoria

- 1) dato che il PM collabora anche con il PG, il GIP non è l'unico interlocutore che ha
- 2) Vero, il GUP può emetterla
 - 3) No la emette il GUP insieme al decreto di rinvio a giudizio
 - 4) Vengono richieste al GIP da parte del PM, il GIP può decidere se applicarle o meno.
 - 5) No in quanto l'incidente probatorio deve essere richiesto da una delle due parti e non può essere eseguito in autonomia . La richiesta però viene effettuata al GIP

Quali caratteristiche sono proprie della Persona Offesa

- può sempre chiedere l'archiviazione del procedimento
- è sempre colui che assiste alla commissione di un reato
- Può prendere parte solo alla fase di giudizio
- Può sporgere querela
- Può farsi assistere da un proprio Consulente Tecnico

- 1) Non può sempre chiederlo perché l'archiviazione viene richiesta solo se non ci sono abbastanza prove o il reato non sussiste
- 2) Non è vero
 - 3) Può prendere parte anche alle indagini preliminari
 - 4) E' l'unico che la può sporgere almeno che non si tratta di reati sessuali sui minori/disabili
 - 5) Se necessario, si il CTP

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 soli reati informatici descritti dal codice penale
- I reati informatici descritti dal codice di procedura penale



il comando DD

- da solo permette di produrre una copia forense
- garantisce la non alterazione del disco sorgente
- permette di produrre una copia bit a bit di un supporto immagine
- permette di eseguire anche la copia di una specifica directory
- deve essere eseguito impiegando obbligatoriamente un write blocker

- 1) falso perché comunque servirebbe il calcolo dell'hash
- 2) potrebbe alterarlo in quanto è proprio nella natura del comando dd quello di poter alterare i dati
- 3) vero, ad esempio se utilizzo dd if=/dev/sr0 of=file.dd perchè sto effettuando una copia dei dati che risiedono nel dispositivo sr0 e ne vado a recuperare il file immagine .dd
- 4) si con dd if= inputfile
- 5) si può eseguire anche con un writeblocker ma non è obbligatorio

Pagina 1 di 1

Invia

Questi contenuti non sono creati né avallati da Google. [Segnala una violazione](#) - [Termini di servizio](#) - [Norme sulla privacy](#)

Google Moduli



COMPUTER FORENSICS



DIE UNIVERSITÀ degli STUDI di
NAPOLI FEDERICO II

Esame di Computer Forensics

28/07/2021

*Campo obbligatorio

Email *

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 preview in un sistema spento (DEAD)

- non può essere eseguita con una distro live forensic oriented
- velocizza l'analisi dei software presenti nel sistema
- il sistema da analizzare se è acceso, può essere spento
- in determinati casi si deve valutare il problema dello "shutdown"
- altera il reperto che si sta analizzando

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

- il difensore dell'indagato
- il difensore dell'imputato
- il consulente tecnico di parte della persona offesa (CTP)
- L'imputato
- il Perito del GUP

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

- Il Giudice solo in costituzione monocratica
- Solo dal Pubblico Ministero
- l'indagato solo per assistere agli accertamenti tecnici 360 cpp
- la Polizia Giudiziaria nominando un ausiliario di P.G
- la Parte Offesa

Nel FAT File System

- Ad ogni entry del FAT corrisponde un Cluster
- Il layout è costituita da una Reserved Area, FAT Area e una Data Area
- Nel FAT12/16 la root directory ha dimensione dinamica
- Lo stato di allocazione dei cluster è conservato nel Boot Sector
- I cluster iniziano con indirizzo due

Nel NT File System

- Le Entry MFT vengono pulite non appena viene resettato a ZERO il flag in uso
- Nel File BitMap è indicato lo stato di allocazione di ciascun cluster



NEI FILE QDQUAQAP È INDICATO IL STATO DI ALLOCAZIONE DI CIASCATI CLUSTER

- La dimensione del cluster è indicato nella Tabella MFT
- In una MFT Entry, il contenuto di un attributo esidente viene memorizzato in cluster run
- L'attributo in una MFT Entry di tipo "non residente" indica che il file che descrive è stato cancellato

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
- è corretto per eseguire una copia forense
- esegue la copia della sorgente "sda"
- esegue il calcolo dell'hash on-the-fly dell'immagine "sda.dd"

In Analisi, FTK Imager

- Riconosce tutti i tipi di File System
- Permette di visionare il contenuto dei Disk Image
- Permette di visualizzare solo i file residenti
- Può essere impiegato anche come strumento per la c.d. preview
- Non permette di esportare i file di interesse

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 di tipo logico
- permette la scelta del tipo di hash da calcolare

I Toolkit

- non eseguono una elaborazione del contenuto del disk image
- permettono esclusivamente una visualizzazione gerarchica dei file

- permettono esclusivamente una visualizzazione gerarchica dei file
- non hanno ancora sviluppato una ricerca tramite hash
- eseguono una classificazione dei file
- permettono di eseguire il "file carving" ricercando l'header ed il footer dei file conosciuti

Autopsy

- Il modulo "Keyword Search" impiega "Apache Solr"
- il modulo "Hash Lookup" permette solo di importare la lista di notable file
- il file carving viene eseguito esclusivamente sullo spazio non allocato
- Le informazioni dal registro di sistema vengono estratte tramite il tool "RegistryViewer"
- permette la selezione dei file di interesse tramite "checkbox"

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
- 60bit per la lunghezza del messaggio
- un bit a "1" al 1048° bit
- nessun bit di padding
- 1536bit

Nel File System

- I dati essenziali possono non essere coerenti
- il "Content Category" comprende le informazioni sul layout
- In "Content Category" i dati sono organizzati in "Data Unit"
- In "Application Category" sono presenti i dati essenziali per alcune funzionalità del File System
- lo "Slack Space" indica un settore non utilizzato di una "Data Unit" allocata

Nell'analisi dei Sistemi Operativi

- In un SO Linux i file dell'utente si trovano in giro per il sistema
- Il SO Windows è molto più rigido nella gestione della struttura del File System rispetto ad un SO Linux
- In SO Windows HKEY_USERS è una hive del registro di sistema che contiene le impostazioni dell'utente
- Il SO Apple è il sistema più documentato
- Il PageFile.sys del SO Apple si trova nella root del disco

il formato DD/RAW:

- conserva il calcolo dell'hash MD5
- conserva i metadati del reperto sorgente
- non permette la compressione
- non può contenere la copia logica di una cartella\directory
- è un formato della famiglia "Expert Witness Disk Image Format"

Partizionamento DOS

- può contenere al massimo 4 partizioni primarie
- Contiene sempre un EBR
- non ha limite al numero di partizioni che può contenere
- La "Partition Table" è costituita da massimo otto entry
- Contiene un MBR se ha secondary extended partition

Nella Mobile Forensics

- L'acquisizione della memoria del dispositivo deve essere eseguita prima di una possibile memory card in esso contenuta
- Nella File System Extraction bisogna preoccuparsi di decodificare i dati estratti
- 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

Autopsy

- Ulteriori "Ingest Modules" possono essere aggiunti solo dal produttore del software
- Pemette 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

Pagina 1 di 1

Invia

Questi contenuti non sono creati né avallati da Google. [Segnala una violazione](#) - [Termini di servizio](#) - [Norme sulla privacy](#)

Google Moduli

Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Your email

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
- Indica al Consulente Tecnico che deve eseguire un accertamento tecnico non ripetibile
- chiedendo autorizzazione al GIP (Giudice Indagini Preliminari)

Esame di Computer Forensics

Test di autovalutazione esperimento

Email *

Via e-mail

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

- l'ufficiale dell'indagine
- l'ufficiale dell'imputato
- il consulente tecnico di parte della persona offesa (CTP)
- imputato
- il Perito del GUP

Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Nome *

Il GIP (Giudizio per le Indagini Preliminari)

- è funzio interlocutore del Preliminary Interview
- non esiste una sentenza
- può esistere sentenze di non bellige a procedere
- privato nelle misure cautelari
- ha autoroma di indagine proattiva

Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Your email

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
- Indica al Consulente Tecnico che deve eseguire un accertamento tecnico non ripetibile
- chiedendo autorizzazione al GIP (Giudice Indagini Preliminari)

Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Your email

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

- Quando occorre agire in assoluta ugenza 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

Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Your email

Chi può prendere parte agli accertamenti tecnici ripetibili ai sensi dell'art. 359 cpp?

- l'indagato con il proprio difensore
- la persona offesa
- il consulente tecnico dell'indagato (CTP)
- il consulente tecnico del P.M. (CTU)
- il Perito

Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Your email

Il GIP (Giudice per le Indagini Preliminari)

- è l'unico interlocutore del Pubblico Ministero
- non emette una sentenza
- può emettere sentenza di non luogo a procedere
- provvede sulle misure cautelari
- ha autonomia di iniziativa probatoria

Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Your email

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

- Quando occorre agire in assoluta ugenza 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



Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Your email

Chi può prendere parte agli accertamenti tecnici ripetibili ai sensi dell'art. 359 cpp?

- l'indagato con il proprio difensore
- la persona offesa
- il consulente tecnico dell'indagato (CTP)
- il consulente tecnico del P.M. (CTU)
- il Perito



28.06.21 alle 15:52





Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Your email

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
- Indica al Consulente Tecnico che deve eseguire un accertamento tecnico non ripetibile
- chiedendo autorizzazione al GIP (Giudice Indagini Preliminarì)
-

Gianmichele
28.06.21 alle 15:57





Foto



Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Your email

Il Procedimento Penale

- Si realizza in un'unica struttura: il Tribunale
- si instaura con l'iscrizione della notizia di reato
- prevede due gradi di giudizio
- si conclude con il giudicato penale
- Si instaura esclusivamente su iniziativa di una parte

Mariaelena Ciccarelli
28.06.21 alle 4:00 PM





Foto



Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Your email

Il Procedimento Penale

- Si realizza in un'unica struttura: il Tribunale
- si instaura con l'iscrizione della notizia di reato
- prevede due gradi di giudizio
- si conclude con il giudicato penale
- Si instaura esclusivamente su iniziativa di una parte

Mariaelena Ciccarelli
28.06.21 alle 4:00 PM



Esame di Computer Forensics

Test di autovalutazione apprendimento

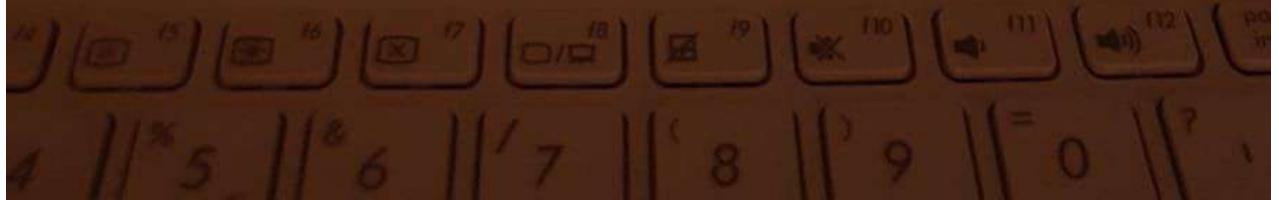
Email *

Your email

Chi può prendere parte agli accertamenti tecnici ripetibili ai sensi dell'art. 359 cpp?

- l'indagato con il proprio difensore
- la persona offesa
- il consulente tecnico dell'indagato (CTI)
- il consulente tecnico del P.M. (CTB)
- il Perito

//docs.google.com/forms/d/e/1FAIpQLSeQozjwR7krKIBWLm6DiV2C63BTfc3Lw4mPIMNNCXlwQ/closedform



Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Your email

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

- il difensore dell'imputato
- il difensore dell'indagato accompagnato dal proprio consulente tecnico (CTP)
- il consulente tecnico di parte della persona offesa (CTP)
- Il Perito del GIP
- il Perito del GUP

L'incidente Probatone...

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

Il Procedimento Penale

- Si realizza in un'unica struttura: il Tribunale
- si instaura con l'iscrizione della notizia di reato
- prevede due gradi di giudizio
- si conclude con il giudicato penale
- Si instaura esclusivamente su iniziativa di una parte

•

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

- Quando occorre agire in assoluta ugenza a causa della peribilità 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

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

- l'indagato con il proprio difensore
- la persona offesa
- il consulente tecnico dell'indagato (CTP)
- il consulente tecnico del P.M. (CTU)
- il Perito

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

- l'indagato con il proprio difensore
- la persona offesa
- il consulente tecnico dell'indagato (CTP)
- il consulente tecnico del P.M. (CTU)
- il Perito

Il GIP (Giudice per le Indagini Preliminari)

- è l'unico interlocutore del Pubblico Ministero
- non emette una sentenza
- può emettere sentenza di non luogo a procedere
- provvede sulle misure cautelari
- ha autonomia di iniziativa probatoria

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

- Il difensore dell'imputato
- Il difensore dell'indagato accompagnato dal proprio consulente tecnico (CTP)
- Il consulente tecnico di parte della persona offesa (CTP)
- Il Perito del GIP
- Il Perito del GUP

Il PM conferisce incarico ai sensi dell'art. 360 CPP

- Quando occorre agire in assoluta urgenza a causa della pericolosità del reperito
- 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
- chiedendo autorizzazione al GIP (Giudice Indagini Preliminari)

In Analisi, montare un file immagine

- non bisogna preoccuparsi di riconoscere il File System presente
- è utile per impiegare strumenti non forensic oriented
- permette l'immediata visualizzazione anche dei file cancellati
- permette di ottenere una analisi completa
- non vi è il rischio di alterare il file immagine

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

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

MyFederico! | Università Federico II | Posta :: Posta in Arrivo | Esame di Computer Forensics | (1) WhatsApp

docs.google.com/forms/d/e/1FAIpQLSeHY4Og4JTHGQQoijtIA_1SwL72ul8cD-2mo-ubnft1Mkh2g/viewform

Registri e didattica... Secondo Circolo Ac... WhatsApp Classroom YouTube Nuova scheda

Autopsy

- Il "file carving" viene svolto tramite il tool "PhotoRec"
- Il "file carving" viene svolto su tutto il disk image
- Il modulo che si preoccupa di estrarre informazioni dai browser è "Browser Activity"
- Il modulo "Hash Lookup" permette solo di importare la lista di "Ignorable File"
- Le informazioni dal registro di sistema vengono estratte tramite il tool "RegistryViewer"

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

Nell'analisi dei Sistemi Operativi

- In un SO Windows il file SAM contiene l'elenco di tutti gli account utente che possono avere accesso al sistema

Scrivi qui per eseguire la ricerca

17.02 28/06/2021

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

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

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**"

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
- Indica al Consulente Tecnico che deve eseguire un accertamento tecnico non ripetibile
- chiedendo autorizzazione al GIP (Giudice Indagini Preliminari)
- Quando vuole dissequestrare il bene oggetto di accertamento tecnico

MyFederico! | Università Federico II | Posta :: Posta in Arrivo | Esame di Computer Forensics | WhatsApp

docs.google.com/forms/d/e/1FAIpQLSeHY4Og4JTHGQQoijIjIA_1SwL72ul8cD-2mo-ubnft1Mkh2g/viewform

Registri e didattica... Secondo Circolo Ac... WhatsApp Classroom YouTube Nuova scheda

Nell'analisi dei Sistemi Operativi

- In un SO Windows il file SAM contiene l'elenco di tutti gli account utente che possono avere accesso al sistema
- In SO Apple il FileVault contiene l'elenco degli utenti che ha accesso al sistema
- 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 Windows si trova nella root del disco

In Analisi, montare un file immagine

- implica che bisogna riconoscere il File System presente
- permette l'esportazione del calcolo dell'hash dei file di interesse
- si ha la completa visione di tutto il contenuto presente
- permette di ottenere una analisi completa
- non vi è il rischio di alterare il file immagine

Nella Mobile Forensics

- La Manual Extraction è il metodo più veloce per eseguire una copia dei dati presenti
- Nella Physical Extraction bisogna preoccuparsi di decodificare i dati estratti

Scrivi qui per eseguire la ricerca

17.10 28/06/2021

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
- Nella Logical Extraction otteniamo i dati integralmente così come sono all'interno del dispositivo
- Nella File System Extraction non bisogna preoccuparsi di decodificare i dati estratti

FTK Imager

- 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 solo di tipo "full disk"
- non permette la scelta del tipo di hash da calcolare

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
- Non può farsi assistere da un proprio Consulente Tecnico

Partizionamento DOS

- può contenere al massimo 4 partizioni primarie
- può conterene al massimo 8 partizioni
- può contenere delle secondary extended partition
- La "Partition Table" è costituita da massimo otto entry
- Contiene sempre un MBR ed un EBR

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

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

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

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

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

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

In Analisi, montare un file immagine

- non bisogna preoccuparsi di riconoscere il File System presente
- è utile per impiegare strumenti non forensic oriented
- permette l'immediata visualizzazione anche dei file cancellati
- permette di ottenere una analisi completa
- non vi è il rischio di alterare il file immagine

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

In Analisi, FTK Imager

- Riconosce solo determinati File System
- Permette di visionare il contenuto dei Disk Image
- Permette di visualizzare solo i file residenti
- Non deve essere impiegato come strumento per la c.d. preview
- Permette di visionare\analizzare solo Disk Image

docs.google.com/forms/d/e/1FAIpQLSeQozjwR7krKibWLm6DjV2C63B... Aggiorna

bisogna preoccuparsi di redigere la catena di custodia

dove essere eseguito impiegando obbligatoriamente un write blocker

Autopsy

- La sezione "Result" contiene le annotazioni dell'utente
- Permette solo una configurazione "single user"
- Il modulo che si preoccupa di estrarre informazioni dal browser è "Browser Activity"
- Il modulo che si preoccupa di estrarre informazioni dal cestino di sistema è "Recent Activity"
- Il modulo "Encryption Detection" permette trovare e decifrare i file protetti

Nel File System

- I dati essenziali possono non essere coerenti
- Il "Content Category" comprende le informazioni sul layout
- In "Content Category" i dati sono organizzati in "Data Unit"
- In "Application Category" sono presenti i dati essenziali per alcune funzionalità del File System
- Lo "Slack Space" indica un settore non utilizzato di una "Data Unit" allocata

Il procedimento civile...

Corso Computer forense - Adobe Acrobat Reader DC (32-bit)

File Modifica Vista Elirma Finestra Aiuto

Home Strumenti Corso Com... Corso Com... mergeslide... ? Accedi

Domanda nr. 08

il comando DD

<input type="checkbox"/> da solo permette di produrre una copia forense	X
<input type="checkbox"/> garantisce la non alterazione del disco originale	X
<input checked="" type="checkbox"/> esegue una copia "bit a bit" di un supporto di memoria generando un file immagine	✓
<input checked="" type="checkbox"/> permette di eseguire una copia di un solo file	✓

Riunione in "ES280621 - Gr..." 44:40

Scrivi qui per eseguire la ricerca 33°C Soleggiato 17:19 28/06/2021

Screenshot of a Microsoft Edge browser window showing a Google Forms survey and a Microsoft Teams video conference.

Google Forms Survey:

- File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
- Indirizzi Cso C test cf.pdf appunti Corso Con Corso Con Posta Esci X
- https://docs.google.com/forms/d/e/1FAIpQLSe...
- Come iniziare
- il difensore dell'imputato
- il difensore dell'indagato accompagnato dal proprio consulente tecnico (CTP)
- il consulente tecnico di parte della persona offesa (CTP)
- Il Perito del GIP
- Il Perito del GUP

In Analisi, montare un file immagine

- non bisogna preoccuparsi di riconoscere il File System presente
- non è utile per impiegare strumenti non forensic oriented
- permette la visualizzazione immediata dei soli file residenti
- è utile soprattutto per analisi mirate
- non vi è il rischio di alterare il file immagine

Invia Pagina 1 di 1

Questi contenuti non sono creati né avallati da Google. Segnala una violazione - Termini di servizio - Norme sulla privacy

Google Moduli

Microsoft Teams Video Conference:

- Riunione in "ES280G21 - Gruppo (1)"
- 4/201
- PIETRO CHIARO (Professore ha avuto problemi a entrare, mi può riconoscere)
- FRANCESCO LA FRAZIA, FABRIZIO ZIFARELLI, LAURA SGAMMATO, ANTONIO D'ANTO, GIULIO POSSENTE, ROBERTO MAIELLO
- Chat della riunione
- 16:33 Inizio riunione Ultima lettura
- PIETRO CHIARO 16:45 Professore ha avuto problemi a entrare, mi può riconoscere

Scrivere un nuovo messaggio

Windows taskbar: 35°C Soleggiato, ITA, 17:20

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
- Nella Logical Extraction otteniamo i dati integralmente così come sono all'interno del dispositivo
- Nella File System Extraction non bisogna preoccuparsi di decodificare i dati estratti

Screenshot of a Windows desktop showing a Google Form, a PDF viewer, and a video conference window.

Google Form (Left):

- bisogna preoccuparsi di redigere la catena di custodia
- deve essere eseguito impiegando obbligatoriamente un write blocker

Autopsy:

- La sezione "Result" contiene le annotazioni dell'utente
- Permette solo una configurazione "single user"
- Il modulo che si preoccupa di estrarre informazioni dal browser è "Browser Activity"
- Il modulo che si preoccupa di estrarre informazioni dal cestino di sistema è "Recent Activity"
- Il modulo "Encryption Detection" permette trovare e decifrare i file protetti

Net File System:

- I dati essenziali possono non essere coerenti
- il "Content Category" comprende le informazioni sul layout
- In "Content Category" i dati sono organizzati in "Data Unit"
- In "Application Category" sono presenti i dati essenziali per alcune funzionalità del File System
- lo "Slack Space" indica un settore non utilizzato di una "Data Unit" allocata

Il procedimento civile...

PDF Viewer (Top Right):

Corso Computer forense - Adobe Acrobat Reader DC (32-bit)

Domanda nr. 08

SSRI

Riunione in "ES280621 - Gr..." 4440

il comando DD

- da solo permette di produrre una copia forense
- garantisce la non alterazione del disco originale
- esegue una copia "bit a bit" di un supporto di memoria generando un file immagine
- permette di eseguire una copia di un solo file

Scrivi qui per eseguire la ricerca

17.19 33°C Soleggiato 28/06/2021

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

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

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 "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

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"

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"

2 WhatsApp Posta :: Posta in Arrivo [CF] FS28 Esame di Computer Forensics +

docs.google.com/forms/d/e/1FAIpQLSeHY4Og4JTHGQQoi_ltlA_1SwL72ul8cD-2mo-ubnft1Mkh2g/viewform

App The Java™ Tutorials WhatsApp Segreteria OnLine ... Informatica-Unina Elenco di lettura

Partizionamento DOS

- Contiene sempre un MBR
- Contiene sempre un EBR
- non ha limite al numero di partizioni che può contenere
- può contenere al massimo 4 secondary extended partition
- l'EBR può contenere al massimo 1 entry

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
- 60bit per la lunghezza del messaggio
- un bit a '1' ai 1040° bit
- nessun bit di padding
- 1536bit

Riunione in "ES280621 - Gr..." 49:25



! 17:25 33°C 28/06/2021

MyFederico! | Università Federico II | Posta :: Posta in Arrivo | Esame di Computer Forensics | WhatsApp

docs.google.com/forms/d/e/1FAIpQLSeHY4Og4JTHGQQoijtIA_1SwL72ul8cD-2mo-ubnft1Mkh2g/viewform

Registri e didattica... Secondo Circolo Ac... WhatsApp Classroom YouTube Nuova scheda

Autopsy

- Il modulo "Keyword Search" impiega "Apache Solr"
- Il modulo "Hash Lookup" permette solo di importare la lista di "Notable File"
- Il modulo "Interesting Files" permette di evidenziare i file corrispondenti a determinate regole
- Il modulo che si preoccupa di estrarre informazioni dai browser è "Internet Activity"
- permette la selezione dei file di interesse tramite "checkbox"

Nella fase di identificazione, la preview...

- in alcuni casi c'è il rischio inevitabile di alterare il reperto
- deve essere eseguita realizzando la copia forense
- può essere eseguita su di un sistema acceso
- non devono essere accesi i dispositivi rinvenuti spenti
- non è particolarmente utile ad individuare le fonti di prova

il formato E01:

- non conserva il calcolo dell'hash

Scrivici qui per eseguire la ricerca

17.26 28/06/2021

Autopsy

- il "Central Repository" permette di rapportare il caso in esame con i precedenti casi già elaborati
- Pemette 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

In Analisi, montare un file immagine

- non bisogna preoccuparsi di riconoscere il File System presente
- non è utile per impiegare strumenti non forensic oriented
- permette la visualizzazione immediata dei soli file residenti
- è utile soprattutto per analisi mirate
- non vi è il rischio di alterare il file immagine

il formato E01:

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

la preview in un sistema spento (DEAD)

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

Il formato E01:

- non conserva il calcolo dell'hash

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 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

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 soli reati informatici descritti dal codice penale
- I reati informatici descritti dal codice di procedura penale

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

MyFederico! | Università Federico II | Posta :: Posta in Arrivo | Esame di Computer Forensics | (1) WhatsApp

docs.google.com/forms/d/e/1FAIpQLSeHY4Og4JTHGQQoijIJA_1SwL72ul8cD-2mo-ubnft1Mkh2g/viewform

Registri e didattica... Secondo Circolo Ac... WhatsApp Classroom YouTube Nuova scheda

esegue copie forensi solo di tipo "full disk"
 permette la scelta del tipo di hash da calcolare

Nel NT File System

Una Entry MFT può contenere solo un attributo di tipo \$DATA
 Le Entry MFT vengono pulite non appena il flag "in uso" viene settato
 Ad esclusione delle strutture dati del FileSystem tutto il resto è gestito come file
 Il File \$BitMap indica i cluster danneggiati
 In ogni entry MFT di Base vi è un attributo di tipo \$ATTRIBUTE_LIST

Nel File System

I dati essenziali possono non essere coerenti
 In "Metadata Category" i dati sono organizzati in "Data Unit"
 il "File System 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 un settore non utilizzato di una "Data Unit" allocata

Scrivi qui per eseguire la ricerca

17:30 28/06/2021

Il procedimento civile...

- Le parti in giudizio sono: l'imputato e la persona offesa
- 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
- Le parti in giudizio possono nominare un Consulente Tecnico

I Toolkit

- non eseguono una elaborazione del contenuto del disk image
- permettono esclusivamente una visualizzazione gerarchica dei file
- non hanno ancora sviluppato una ricerca tramite hash
- eseguono una classificazione dei file
- permettono di eseguire il "file carving" ricercando l'header ed il footer dei file conosciuti

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

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"

Partizionamento DOS

- Il settore contenente l'MBR termina con una signature
- L'MBR è costituito da almeno quattro settori
- La "Partition Table" nell'EBR è costituita da 4 entry, di cui 2 sono vuote.
- può contenere al massimo 4 secondary extended partition
- Il campo "Starting LBA Address", presente nella "Partition Table", indica il cluster iniziale della partizione

Nel FAT File System

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

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 inziano con indirizzo uno

MyFederico! | Università Federico II | Posta :: Posta in Arrivo | Esame di Computer Forensics | WhatsApp

docs.google.com/forms/d/e/1FAIpQLSeHY4Og4JTHGQQoijIjIA_1SwL72ul8cD-2mo-ubnft1Mkh2g/viewform

Registri e didattica... Secondo Circolo Ac... WhatsApp Classroom YouTube Nuova scheda

Partizionamento DOS

- Contiene sempre un MBR
- Contiene sempre un EBR
- non ha limite al numero di partizioni che può contenere
- può contenere al massimo 4 secondary extended partition
- l'EBR può contenere al massimo 1 entry

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 è corretto per eseguire una copia forense
- esegue la copia della sorgente "sda"
- esegue il calcolo dell'hash on-the-fly dell'immagine "sda.dd"

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

Scrivi qui per eseguire la ricerca

17:31 28/06/2021

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 attributo di tipo \$ATTRIBUTE_LIST

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 FAT File System

- Le data unit si chiamano settori
- La dimensione delle entry del FAT dipendono dalla tipologia di FAT
- Nel FAT32 la root directory ha dimensione dinamica
- Lo stato di allocazione dei cluster è indicato con ZERO (non allocato) o con UNO (Allocato)
- Nel boot sector è contenuta l'informazione sulla tipologia di FAT

Nel NT File System

L'algoritmo di Hash MD5

- processa il messaggio in blocchi di 512bit
- è costituito da 4 round e 4 funzioni logiche
- rispetto a MD4 fa uso di 2 costanti in più
- l'output è un digest a 160bit
- il quarto round è composto da 48 operazioni

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
- 60bit per la lunghezza del messaggio
- un bit a "1" al 1048° bit
- nessun bit di padding
- 1536bit

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

Nel NT File System

- Una Entry MFT può contenere solo un attributo di tipo \$DATA
- Le Entry MFT vengono pulite non appena il flag "in uso" viene settato
- La dimensione del cluster è indicato nella Tabella MFT
- Il File \$BitMap indica i cluster danneggiati
- Le informazioni temporali sul file sono contenute solo all'interno dell'attributo \$STANDARD_INFORMATION

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

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

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 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

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 acceso
- non devono essere accesi i dispositivi rinvenuti spenti
- non è particolarmente utile ad individuare le fonti di prova

MyFederico! | Università Federico II | Posta :: Posta in Arrivo | Esame di Computer Forensics | WhatsApp

docs.google.com/forms/d/e/1FAIpQLSeHY4Og4JTHGQQoijIjIA_1SwL72ul8cD-2mo-ubnft1Mkh2g/viewform

Registri e didattica... Secondo Circolo Ac... WhatsApp Classroom YouTube Nuova scheda

Il procedimento civile...

- Le parti in giudizio sono: l'imputato e la persona offesa
- 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
- Le parti in giudizio possono nominare un Consulente Tecnico

FTK Imager

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

Nel NT File System

- Una Entry MFT può contenere solo un attributo di tipo \$DATA
- Le Entry MFT vengono pulite non appena il flag "in uso" viene settato
- Ad esclusione delle strutture dati del FileSystem tutto il resto è gestito come file

Scrivi qui per eseguire la ricerca

17:33 28/06/2021

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

1 WhatsApp Posta :: Posta in Arrivo [CF] FS28 Esame di Computer Forensics +

docs.google.com/forms/d/e/1FAIpQLSeHY4Og4JTHGQQoi_ltlA_1SwL72ul8cD-2mo-ubnft1Mkh2g/viewform

App The Java™ Tutorials WhatsApp Segreteria OnLine ... Informatica-Unina Elenco di lettura

non permette la compressione

non può contenere la copia logica di una cartella\directory

non è un formato della famiglia "Expert Witness Disk Image Format"

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

Ad ogni entry del FAT corrisponde un Cluster

Il layout è costituita da una Reserved Area, FAT Area e una Data Area

Nel FAT16 il cluster minimo è di 16 byte

17:32 33°C 28/06/2021

La c.d. "preview"

- è uno strumento di ricerca della prova permesso agli inquirenti in sede di perquisizione
- rende veloce l'analisi dei software presenti nel sistema
- Può essere ^{compiuto} da qualsiasi agente della P.G. poiché ha un basso rischio di alterazione della prova
- non è particolarmente utile ad individuare le fonti di prova
- deve essere eseguita impiegando obbligatoriamente un write blocker

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

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"

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

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

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"
- 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

MyFederico! | Università Federico II | Posta :: Posta in Arrivo | Esame di Computer Forensics | WhatsApp

docs.google.com/forms/d/e/1FAIpQLSeHY4Og4JTHGQQoijtIA_1SwL72ul8cD-2mo-ubnft1Mkh2g/viewform

Registri e didattica... Secondo Circolo Ac... WhatsApp Classroom YouTube Nuova scheda

FTK Imager

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

Nel NT File System

- Una Entry MFT può contenere solo un attributo di tipo \$DATA
- Le Entry MFT vengono pulite non appena il flag "in uso" viene settato
- Ad esclusione delle strutture dati del FileSystem tutto il resto è gestito come file
- Il File \$Bitmap indica i cluster danneggiati
- In ogni entry MFT di Base vi è un attributo di tipo \$ATTRIBUTE_LIST

Nel File System

- I dati essenziali possono non essere coerenti

Scrivi qui per eseguire la ricerca

17:36 28/06/2021

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"

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
- Nella Logical Extraction otteniamo i dati integralmente così come sono all'interno del dispositivo
- Nella File System Extraction non bisogna preoccuparsi di decodificare i dati estratti

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

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"

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
- In una MFT Entry, il contenuto di un attributo esidente viene memorizzato in cluster run
- L'attributo in una MFT Entry di tipo "non residente" indica che il file che descrive è stato cancellato

Partizionamento DOS

- può contenere al massimo 4 partizioni primarie
- Contiene sempre un EBR
- non ha limite al numero di partizioni che può contenere
- La "Partition Table" è costituita da massimo otto entry
- Contiene un MBR se ha secondary extended partition

L'algoritmo di Hash MD5

- processa il messaggio in blocchi di 512bit
- è costituito da 4 round e 4 funzioni logiche
- rispetto a MD4 fa uso di 2 costanti in più
- l'output è un digest a 160bit
- il quarto round è composto da 48 operazioni

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 EO1:

- non conserva il calcolo dell'hash
- permette di conservare i metadati del reperto sorgente

mergeslideU.pdf - Adobe Acrobat Reader DC (32-bit)

File Modifica Vista Firma Finestra Aiuto

Home Strumenti Corso Com... Corso Com... mergeslide... Trova (1/192) hash Precedente Avanti

LA COPIA FORENSE

descrizione degli strumenti

- **Tableau T15 Forensic SATA:**
 - **Write Block:** strumento che impedisce qualsiasi scrittura, anche accidentale, sul supporto di origine
- **AccessData FTK Imager 2.5.3.14:** software forense utilizzato per la generazione della copia forese.
 - **Hash MD5 e SHA1:** Il software *certifica* digitalmente la copia forense calcolando l'hash del disco origine e della copia generata.
 - **File LOG:** riassumono l'attività di clonazione effettuata, con le indicazioni dei file generati e la verifica, conclusa con esito positivo, del calcolo degli algoritmi di Hash .

SSRI Università degli Studi di Napoli Federico II a.a. 2019-21

Scrivi qui per eseguire la ricerca 32°C Soleggiato 17:36 28/06/2021

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

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

MyFederico! | Università Federico II | Posta :: Posta in Arrivo | Esame di Computer Forensics | (1) WhatsApp

docs.google.com/forms/d/e/1FAIpQLSeHY4Og4JTHGQQoiJtIA_1SwL72ul8cD-2mo-ubnft1Mkh2g/viewform

Registri e didattica... Secondo Circolo Ac... WhatsApp Classroom YouTube Nuova scheda

esegue copie forensi solo di tipo "full disk"
 permette la scelta del tipo di hash da calcolare

Nel NT File System

Una Entry MFT può contenere solo un attributo di tipo \$DATA
 Le Entry MFT vengono pulite non appena il flag "in uso" viene settato
 Ad esclusione delle strutture dati del FileSystem tutto il resto è gestito come file
 Il File \$BitMap indica i cluster danneggiati
 In ogni entry MFT di Base vi è un attributo di tipo \$ATTRIBUTE_LIST

Nel File System

I dati essenziali possono non essere coerenti
 In "Metadata Category" i dati sono organizzati in "Data Unit"
 il "File System 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 un settore non utilizzato di una "Data Unit" allocata

Scrivi qui per eseguire la ricerca

17:38 28/06/2021

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

Nel FAT File System

- Le data unit si chiamano settori
- La dimensione delle entry del FAT dipendono dalla tipologia di FAT
- Nel FAT32 la root directory ha dimensione dinamica
- Lo stato di allocazione dei cluster è indicato con ZERO (non allocato) o con UNO (Allocato)
- Nel boot sector è contenuta l'informazione sulla tipologia di FAT

il formato E01:

- non conserva il calcolo dell'hash MD5
- permette di conservare i metadati del reperto sorgente
- non permette la compressione
- può contenere la copia logica di una cartella\directory
- è un formato della famiglia "Expert Witness Disk Image Format"

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

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

In Analisi, FTK Imager

- Riconosce tutti i tipi di File System
- Permette di visionare\analizzare solo Disk Image
- Permette di avere informazioni su alcuni dei file cancellati
- Non può essere impiegato anche come strumento per la c.d. preview
- Permette di esportare i file di interesse

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

MyFederico | Università Federico II | Posta :: Posta in Arrivo | Esame di Computer Forensics | (1) WhatsApp

docs.google.com/forms/d/e/1FAIpQLSeHY4Og4JTHGQQoijtIA_1SwL72ul8cD-2mo-ubnft1Mkh2g/viewform

Registri e didattica... Secondo Circolo Ac... WhatsApp Classroom YouTube Nuova scheda

Nel File System

- I dati essenziali possono non essere coerenti
- In "Metadata Category" i dati sono organizzati in "Data Unit"
- Il "File System 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 un settore non utilizzato di una "Data Unit" allocata

Chi può prendere parte agli accertamenti tecnici ripetibili ai sensi dell'art. 359 cpp?

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

Invia Pagina 1 di 1

Scrivi qui per eseguire la ricerca

17:41 28/06/2021

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"

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

- Quando occorre agire in assoluta ugenza 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

WhatsApp X 4 notifications X Esame di Computer Forensi X LorenzoMiraglia.pdf X Corso Computer Forensics X +

https://docs.google.com/forms/d/e/1FAIpQLSem_1VxEclJi9bragonjF0sr2W52RbwRdt0x_qSvqpu8j6w/viewform

Il hash della copia forense dovrebbe coincidere con quello calcolato dalla medesima copia dopo la fase di analisi

La copia forense sarà immodificabile

Il hash della copia forense coinciderà con l'hash calcolato da una successiva copia forense

Il hash ricalcolato sulla copia forense varierebbe alla minima alterazione della copia stessa

I dati della copia forense sono identici ai dati originali

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

Nell'analisi dei Sistemi Operativi

Scrivi qui per eseguire la ricerca

Corso Computer Forensics - Adobe Acrobat Reader DC (32-bit)

32°C Soleggiato 17:42 28/06/2021

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 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

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
- Nella Logical Extraction otteniamo i dati integralmente così come sono all'interno del dispositivo
- Nella File System Extraction non bisogna preoccuparsi di decodificare i dati estratti

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

1 WhatsApp Posta :: Posta in Arrivo [CF] FS28 Esame di Computer Forensics +

docs.google.com/forms/d/e/1FAIpQLSeHY4Og4JTHGQQoi_ltlA_1SwL72ul8cD-2mo-ubnft1Mkh2g/viewform

App The Java™ Tutorials WhatsApp Segreteria OnLine ... Informatica-Unina Elenco di lettura

Email *

FEZA5ZFUTL@studenti.unina.it

Il formato E01:

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

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

Windows 10 Taskbar: File Explorer, Edge, Netflix, Microsoft Store, Mail, Google Chrome, Microsoft Teams, OneDrive, Task View, Task Manager, System Tray showing 33°C, 17:43, 28/06/2021.

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 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

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

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
- Nella Logical Extraction otteniamo i dati integralmente così come sono all'interno del dispositivo
- Nella File System Extraction non bisogna preoccuparsi di decodificare i dati estratti

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
-

La c.d. "preview"

- è uno strumento di ricerca della prova permesso agli inquirenti in sede di perquisizione
- rende veloce l'analisi dei software presenti nel sistema
- Può essere compiuto da qualsiasi agente della P.G. poiché ha un basso rischio di alterazione della prova
- non è particolarmente utile ad individuare le fonti di prova
- deve essere eseguita impiegando obbligatoriamente un write blocker

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

In Analisi, FTK Imager

- Riconosce tutti i tipi di File System
- Permette di visionare il contenuto dei Disk Image
- Permette di visualizzare solo i file residenti
- Può essere impiegato anche come strumento per la c.d. preview
- Non permette di esportare i file di interesse

In Analisi, montare un file immagine

- non bisogna preoccuparsi di riconoscere il File System presente
- non è utile per impiegare strumenti non forensic oriented
- permette la visualizzazione immediata dei soli file residenti
- è utile soprattutto per analisi mirate
- non vi è il rischio di alterare il file immagine

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

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 gran parte delle impostazioni del sistema e dell'utente sono memorizzate nel Registro di Sistema

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

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"
- permette solo una configurazione "single user"

La c.d. "preview"

- Può essere compiuto da qualsiasi 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

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

Quale 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"
- permette solo una configurazione "single user"

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
- 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

- 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

- 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 attributo 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 EO1:

- non conserva il calcolo dell'hash

COMPUTER FORENSICS

TEST del 30-03-2022

NOME

COGNOME

MATRICOLA

01 - Chi può prendere parte agli accertamenti tecnici non ripetibili ai sensi dell'art.

360 c.p.p.?

- a) Il difensore dell'indagato
- b) Il difensore dell'imputato accompagnato dal proprio consulente tecnico (CTP)
- c) Il consulente tecnico di parte dell'indagato (CTP)
- d) Il Perito del GIP
- e) Il Perito del GUP

02 - Il procedimento civile...

- a) Le parti in giudizio sono: l'attore ed il convenuto
- b) Le parti in giudizio sono: l'indagato ed il ricorrente
- c) Ha lo scopo di accettare la verità nell'interesse dello Stato e della collettività
- d) Si instaura esclusivamente su iniziativa di una parte
- e) Solo le parti in giudizio possono nominare un Consulente Tecnico

03 - la preview in un sistema acceso (LIVE)

- a) Deve essere eseguita con un write blocker
- b) Velocizza l'analisi dei software presenti nel sistema
- c) Non è possibile eseguirla sui dispositivi rinvenuti "spenti"
- d) Deve essere svolta mediante l'uso di *distro live forensic oriented*
- e) È più rischiosa di quella in un sistema spento (*DEAD*)

04 - Per preservazione si intende che

- a) L'hash della copia forense dovrebbe coincidere con quello calcolato dalla medesima copia dopo la fase di analisi
- b) La copia forense sarà immodificabile
- c) L'hash della copia forense coinciderà con l'hash calcolato da una successiva copia forense
- d) L'hash ricalcolato sulla copia forense varierebbe alla minima alterazione della copia stessa
- e) I dati della copia forense sono identici ai dati originali

- c) Non è completo per eseguire la copia forense in quanto manca il calcolo
- d) In caso di un errore di lettura, la copia viene bloccata
- e) Non è corretto per altri motivi

06 - FTK Imager

- a) Permette di produrre *disk image* solo nel formato E01
- b) Fa uso del "hashing on-the-fly"
- c) Non permette di segmentare/splittare il file immagine
- d) Può eseguire copie forensi solo di tipo "full disk"
- e) Impiega esclusivamente il calcolo dell'hash MD5 e SHA1

07 - il formato *disk image* E01:

- a) Non conserva nei metadati il calcolo dell'hash
- b) Può conservare nell'header i metadati del reperto sorgente
- c) Non permette la compressione
- d) Può contenere la copia logica di una cartella\directory
- e) È un formato della famiglia "Expert Witness Disk Image Format"

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

- a) 1024bit
- b) 32bit per la lunghezza del messaggio
- c) Un bit a "1" al 1025° bit
- d) 3 blocchi da 512bit
- e) Nessun bit di padding

09 - In Analisi, montare un file immagine (*mount*)

- a) È utile poiché si può far a meno di riconoscere il File System presente
- b) È utile soprattutto per impiegare strumenti non *forensic oriented*
- c) Si ha la completa e veloce visione di tutto il contenuto presente
- d) Con il tool\comando "ewfmount" è possibile i disk image "E01"
- e) Non è possibile quando il file immagine è suddiviso in più parti

T2231012

15 - Nel FAT File System

- a) Il FSINFO conserva i dati essenziali per il File System
- b) Il layout del File System è descritto nel "MBR" — **NO**
- c) Le informazioni temporali sono conservative all'interno di "Directory Entries"
- d) Lo stato di allocazione di ciascun cluster è conservato nel FSINFO
- e) La FAT Area è organizzata in cluster

16 - Nel NT File System

- a) Una entry MFT può contenere un solo attributo di tipo \$DATA
- b) La entry MFT viene pulita appena il file corrispondente viene cancellato
- c) Le strutture dati del File System sono memorizzate in file
- d) Il file \$BitMap indica i cluster danneggiati
- e) In tutte le entry MFT vi è un attributo di tipo \$STANDARD_INFORMATION

17 - Nell'analisi dei Sistemi Operativi

- a) In un SO Windows all'interno del file SAM sono conservati tutti gli account utente che possono accedere al sistema
- b) Il SO Windows registra molti più log di un SO Linux
- c) In un SO Windows, l'analisi dei "thumbnail" generati dal sistema è utile per recuperare i file cancellati
- d) In un SO Windows, analizzando le "ShellBag" è possibile ricostruire la cronologia delle cartelle visualizzate dall'utente
- e) Il PageFile.sys rappresenta un dump della RAM

18 - Nella Mobile Forensics

- a) La *Manual Extraction* è il metodo più sicuro per non alterare\modificare i dati
- b) Nella *Logical Extraction* non bisogna preoccuparsi di *decodificare* i dati estratti
- c) La *Full File System Extraction* può essere eseguita su quasi la totalità dei dispositivi
- d) Con la *Logical Extraction* otteniamo integralmente i dati così come sono all'interno del dispositivo
- e) La *Physical Extraction* dipende solo dalla versione del SO e dai livelli di patch di sicurezza

I seguente comando: dd if=/dev/sda of=/mnt/sda.dd sync=512 conv=noerr
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
In caso di un errore di lettura, la copia viene bloccata
Non è corretto per altri motivi

mager
Permette di produrre disk image solo nel formato E01
uso del "hashing on-the-fly"
permette di segmentare/splittare il file immagine
eseguire copie forensi solo di tipo "full disk"
ege esclusivamente il calcolo dell'hash MD5 e SHA1

disk image E01:
conserva nei metadati il calcolo dell'hash
servare nell'header i metadati del reperto sorgente
mette la compressione
enere la copia logica di una cartella\directory
ato della famiglia "Expert Witness Disk Image Format"

di SHA-1 se il messaggio di input M è di 1024bit, dopo il padding
costituito da:

lunghezza del messaggio
1025° bit
2bit
padding

e un file immagine (mount)
uò far a meno di riconoscere il File System presente
per impiegare strumenti non forensic oriented
e veloce visione di tutto il contenuto presente
o "ewfmount" è possibile i disk image "E01"
ndo il file immagine è suddiviso in più parti

2 di 5

10 - I Toolkit

- a) Riconoscono la tipologia/formato dei file esclusivamente
- b) Permettono esclusivamente una visualizzazione gerarchica
- c) Possono identificare dei file di interesse mediante l'hash
- d) Eseguono una classificazione dei file analizzati
- e) Impiegano il c.d. "file carving" per identificare il formato

11 - In Autopsy

- a) Il modulo "Outlook Parser" permette di analizzare
- b) Il modulo "iOS Analyzer" permette di analizzare
- c) Apple
- d) Il modulo "Keyword Search" permette di svolgere
- e) parole chiavi
- f) Il "file carving" viene svolto tramite il tool "PhotoRec"
- g) non allocato
- h) La funzione "Extracted Content" si preoccupa

12 - In Autopsy

- a) Ulteriori "Ingest Modules" possono essere aggiuntivi
- b) Permette solo una configurazione "single user"
- c) Il disk image viene processato tramite dei moduli
- d) "RecycleBin Activity"
- e) Il registro di sistema del sistema operativo

13 - Partizionamento DOS

- a) Può contenere al massimo 2 partizioni
- b) La "Partition Table" è costituita da 4 partizioni
- c) Può contenere al massimo 8 partizioni
- d) La "Partition Table" è situata all'interno del file
- e) L'EBR è allocato all'inizio del "Disk Boot Record"

14 - Nel File System

- a) Il "Logical Volume Address" è l'indirizzo del volume
- b) In "Content Category" i dati sono organizzati
- c) In "Metadata Category" sono organizzate le informazioni temporali
- d) Le informazioni temporali sono organizzate
- e) Lo "Slack Space" indica una area di spazio libera