

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

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

Esame di Computer Forensics

Test di autovalutazione apprendimento

Email *

Your email

Il GIP (Giudice per le Indagini Preliminari)

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

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

Foto

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



Foto

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)
-

Gianmichele
28.06.21 alle 15:57





Foto



Esame di Computer Forensics

Test di autovalutazione apprendimento

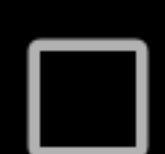
Email *

Your email

Il Procedimento Penale

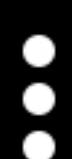
- Si realizza in un'unica struttura: il Tribunale
- si instaura con l'iscrizione della notizia di reato
- prevede due gradi di giudizio
- si conclude con il giudicato penale
- Si instaura esclusivamente su iniziativa di una parte

Mariaelena Ciccarelli
28.06.21 alle 4:00 PM





Foto



Esame di Computer Forensics

Test di autovalutazione apprendimento

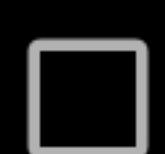
Email *

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?

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

//docs.google.com/forms/d/e/1FAIpQLSeQozjwR7krKiBWLM6DiV2C63BTlc3Lw4mPIMNNC

XiwxQ/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 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

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 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

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

- 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 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

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

- Quando occorre agire in assoluta urgenza e causa delle peribilità 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)

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

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



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

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

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 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

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

Trienn... C.so C... test cf.pdf appunti C... Corso Con... Corso Con... Posta Esa...

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

47:01

Altri segnalibri

Chat della riunione

16:33 Inizio riunione

Ultima lettura

PIETRO CHIARO 16:45 Professore ho avuto problemi a entrare, mi può riconoscere

Scrivi un nuovo messaggio

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

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"

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" al 1048° bit
- nessun bit di padding
- 1536bit



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



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

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

- 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

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



Registri e didattica...



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



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

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

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



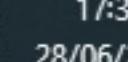
- non permette la compressione
- non può contenere la copia logica di una cartella\directory
- non è un formato della famiglia "Expert Witness Disk Image Format"

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 FAT16/32 le nostre dimensioni dimensione dimensione



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

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
- In "Metadato Catalogo" i dati sono organizzati in "Data Unit"

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

(17) WhatsApp | MyFederico | Posta :: Post | Esame di C | + | - | X

docs.google.com/forms/d/e/1FAIpQLSeQozjwR7krKiBWLm6DiV2C63B... Aggiorna :

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 E01:

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

Scrivi qui per eseguire la ricerca

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

Efile Modifica Vista Firma Finestra Aiuto

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

1066 / 1095 60,9% ...

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 Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
a.a. 2020/21

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

- 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



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

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

- 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

< > C : VPN 🔒 https://docs.google.com/forms/d/e/1FAIpQLSem_1VxEcUi9bragorjF0sr2W52RbwwRdt0x_qSvqpu8j6w/viewform

TP 🌐 ⚡ ⏪ ⏴ ⏵ ⏷

- 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

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

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

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

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

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"

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

- 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 E01:

- non conserva il calcolo dell'hash