Cancellazione sicura e cenni alla digital forensics

Indice

- Richiami sul File System
- Cancellazione Sicura in Hard Disk Magnetici
- Cancellazione Sicura in SSD
- Digital Forensics

Introduzione

- La cancellazione di un file può non essere sufficiente a eliminare le informazioni in esso contenute
- Bisogna distinguere tra hard disk magnetici e unità SSD o flash
- La cancellazione sicura e le tracce presenti nell'hard disk sono legati alla digital forensics, di cui daremo un breve cenno

Richiami sul File System

- I sistemi operativi suddividono i file in *blocchi logici* di dimensione fissa
- I blocchi vengono memorizzati su un supporto fisico e indicizzati attraverso opportune strutture dati (es., FAT, i-node, MTF, etc.)
- Ogni blocco, sul supporto fisico, contiene quindi una *porzione* del file
- Il meccanismo fisico che consente la memorizzazione dei bit dipende dal tipo di supporto fisico.

Richiami sul File System

- Anche l'operazione di cancellazione, per i SO moderni, dipende dal tipo di supporto
- In ogni SO, in ogni caso, la cancellazione deve comportare l'aggiornamento della struttura dati usata per l'indicizzazione e il relativo aggiornamento del contenuto della directory che includeva il file.
- Cosa succede ai blocchi? Dipende dal supporto.

Hard Disk Magnetico (organizzazione)

- Vengono sfruttate le proprietà di un materiale ferromagnetico di magnetizzarsi permanentemente se immerso in un campo magnetico
- Tipicamente vi sono uno o più dischi multistrato con uno strato finale ferromagnetico
- Sulla superfice vi sono areole microscopiche che possono essere magnetizzate dalla testina di scrittura (per induzione elettromagnetica), memorizzando in questo modo un bit 1, o smagnetizzate, memorizzando così uno 0
- La testina di lettura effettua la trasduzione inversa, rilevando pertanto le informazioni memorizzate
- Attraverso suddivisione in tracce e settori, si costituiscono i blocchi su disco, dove sono mappati i blocchi logici dei file.

Hard Disk Magnetico (cancellazione)

- La cancellazione del SO (**riferendoci alla rimozione dal cestino**), nel caso di HD magnetici, non sovrascrive il contenuto dei blocchi fisici (è aggiornata soltanto la struttura dati di indicizzazione e la directory che include il file)
- Tutto il contenuto del file è presente sull'hard disk subito dopo che il file è stato rimosso

Hard Disk Magnetico (recupero)

- Attraverso utility di forensics è possibile pertanto recuperare il file interamente se i blocchi non sono stati riscritti
- L'uso dei blocchi del disco è determinato dalle politiche di allocazione del SO e dalle eventuali operazioni di deframmentazione effettuate dall'utente
- Se un blocco è riscritto perché allocato a un altro file o sovrascritto in caso di deframmentazione l'informazione in esso memorizzata è persa
- Tuttavia, senza specifiche funzioni di cancellazione sicura (wiping) o supportate dal SO o offerte da specifiche APP, non si può controllare la riscrittura dei blocchi, neppure con una formattazione del disco di alto livello.

Numero di riscritture

- Dal punto di vista fisico, in linea di principio, l'areola del disco sottoposta a scrittura, a causa del fenomeno dell'isteresi magnetica, potrebbe conservare memoria di più di una scrittura
- Tuttavia le perturbazioni di potenziale che potrebbero far risalire a precedenti scritture non è rilevabile via controller del disco.
- Di conseguenza, una semplice riscrittura del blocco, di per sé elimina le informazioni in esso contenuto rispetto all'uso di comuni utility di recupero dati. Esiste però la possibilità teorica di recuperare informazioni precedenti attraverso accesso fisico al disco.
- La precedente considerazione motiva il fatto che le funzioni di *wiping* permettono diverse riscritture con pattern di bit pseudo-casuali (basati cioè su PRNG), che sono pertanto suggerite in caso di elevata sicurezza.

Wiping e altre tecniche

- Vi sono diversi SW per il wiping (es. Eraser, Freeraser, Hardwipe, Black and Secure, Dban's Boot and Nuke, CCLeaner, Dp Sheddrer etc.)
- Esistono anche comandi di SO, come Sdelete in Windows 10 (command-line utility di Windows)
- Questi SW permettono di definire il numero di riscritture e il PRNG usato per i pattern di bit
- Bisogna tener conto del fatto che le sovrascritture usurano il disco e impiegano tempo
- Misure alternative (non selettive sui file): formattazione a basso livello, degaussing, distruzione fisica dei supporti

Indicazioni del Garante della Privacy(1)

- **Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008**
- Secondo il garante «*in caso di reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti, adottati nel rispetto delle normative di settore, devono consentire l'effettiva cancellazione dei dati o garantire la loro non intelligibilità*»

Indicazioni del Garante della Privacy(2)

- Il Garante indica l'utilizzo di programmi di cancellazione sicura"*che provvedono, una volta che l'utente abbia eliminato dei file da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati*".
- Riguardo Il numero di riscritture la nota del garante osserva che: *varia da sette a trentacinque e incide proporzionalmente sui tempi di applicazione delle procedure, che su dischi rigidi ad alta capacità (oltre i 100 gigabyte) possono impiegare diverse ore o alcuni giorni), a secondo della velocità del computer utilizzato.*

Garante: Altre misure applicabili

- **Formattazione** "a basso livello" dell'hard disk "*attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità*".
- **Demagnetizzazione** (degaussing) *dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, floppy-disk, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software (che richiedono l´accessibilità del dispositivo da parte del sistema a cui è interconnesso).*
- **Smaltimento di rifiuti elettrici ed elettronici**
  In caso di smaltimento di rifiuti elettrici ed elettronici, l´effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche può anche risultare da procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di dati personali.

Supporti SSD

- Per questi supporti la cancellazione nativa, se il Sistema Operativo supporta il TRIM, comporta un azzeramento del contenuto dei blocchi
- Il Wiping risulta quindi inappropriato, anche perché deteriora le celle SSD
- Tuttavia è da considerare che il TRIMMING marca le celle come non-allocate, e quindi, il firmware dell'SSD restituisce 0x00 per queste celle, senza controllare il contenuto effettivo
- Strumenti di forensics capaci di interfacciarsi direttamente con il firmware possono pertanto leggere il contenuto delle celle
- Pertanto, per gli SSD l'unica cancellazione sicura è la distruzione del dispositivo, perché le politiche di scrittura preferiscono celle fresche per evitare di deteriorare le celle con le riscritture, quindi, vista la capacità elevata media dei dispositivi la riscrittura è improbabile.

Digital Forensics

Consiste nella raccolta ed analisi dei reperti che possono essere utilizzati al fine di documentare il fenomeno verificatosi e poter perseguire i responsabili.

Affinchè le prove estrapolate dai reperti possano essere utilizzabili in sede processuale è bene adottare una serie di linee guida.

Queste hanno il compito di:

- Definire i requisiti del reperto digitale
- Stabilire le fasi da seguire e l'obiettivo che si vuole raggiungere
- Individuare le figure professionali che gestiranno le evidenze digitali

Requisiti del reperto digitale

- Prova digitale
  - Informazione o dato, memorizzato o trasmesso in formato binario, che può essere utilizzato come prova
- Copia di prova digitale
  - Copia di prova digitale che può essere prodotta per mantenere l'affidabilità della prova, includendo sia la prova digitale che la procedura di verifica
- Dato volatile
  - Dato facilmente soggetto a modifica. Una variazione può essere dovuta ad assenza di corrente o ad interventi di campi magnetici, a cambi di stato del sistema
- Alterazione
  - Modifica del valore di potenziali evidenze digitali e riduzione del valore probatorio
- Distruzione di prova
  - Modifica volontaria del valore di potenziali evidenze digitali

Requisiti del metodo forense

- Pertinenza
  - Serve per incolpare (o discolpare)
  - Dimostrare che il materiale è rilevante, cioè che contiene dati utili e che pertanto esiste una buona ragione per acquisirli
- Affidabilità
  - Assicurarsi che la prova digitale sia genuina
  - Tutti i processi eseguiti devono essere ben documentati e, se possibile, ripetibili. Il risultato dovrebbe essere riproducibile
- Sufficienza
  - Il DEFR (Digital Evidence First Responsder) deve valutare quale materiale deve essere raccolto e le procedure idonee
  - Il materiale può essere copiato o acquisito (sequestrato)
  - Non è detto che sia sempre necessario acquisire una copia completa
  - Valutare in base al caso (interessa la figura del DEFR)
  - Può dipende dalla legislazione nazionale

Requisiti del metodo forense

- Verificabilità
  - Un terzo deve essere in grado di valutare le attività svolte dal DEFR e dal DES (Digital Evidence Specialist)
    - Attuabile se esiste la documentazione delle azioni svolte
    - Valutare il metodo scientifico, le tecniche e le procedure seguite
  - DEFR e DES devono essere in grado di giustificare le azioni svolte
- Ripetibilità
  - Le operazioni devono sempre essere ripetibili utilizzando le stesse procedure, lo stesso metodo, gli stessi strumenti, sotto le stesse condizioni
- Riproducibilità
  - Le operazioni possono essere ripetibili anche usando lo stesso metodo, gli strumenti diversi, sotto condizioni diverse
- Giustificabilità
  - Dimostrare che le scelte adoperate erano le migliori possibili

Fasi

Lo standard di riferimento (ISO/IEC 27037) indica le fasi che consento la raccolta delle evidenze:

- **Identificazione**
- **Raccolta**
- **Acquisizione**
- **Conservazione**

Mentre la ISO/IEC 27042 si concentra sull'analisi delle evidenze:

- **Analisi**
- **Interpretazione**

L'obiettivo finale consiste nella **Presentazione** dei risultati raggiunti.

Identificazione

- La prova informatica si presenta in forma fisica e logica
  - Device
  - Rappresentazione dei dati
- Ricerca dei device che possono contenere dati rilevanti
  - Priorità ai dati volatili
  - Considerare dispositivi di difficile identificazione
    - Geografica: Es.: Cloud computing, SAN
    - Dimensioni Es.: miniSD

➢ Si considera computer un dispositivo digitale standalone che riceve, processa e memorizza dati e produce risultati
  - Non connesso in rete
  - Ci possono essere periferiche connesse

➢ Se il computer ha un'interfaccia di rete, anche se non è connesso in rete al momento dell'intervento, bisogna individuare gli eventuali sistemi con cui può aver comunicato

Raccolta

- **Sistema spento**

  Nel caso in cui si operi su un sistema spento, vanno prese in considerazione le seguenti attività:

  - assicurarsi che il dispositivo sia effettivamente spento e non in standby
  - rimuovere il cavo di alimentazione, staccando prima l'estremità connessa al dispositivo e poi quella a muro
  - disconnettere e assicurare tutti i cavi connessi al dispositivo ed etichettare le relative porte a cui sono connessi, così da ricostruire le connessioni in seguito
  - proteggere il tasto di accensione, onde evitare accensione casuale del dispositivo
  - mettere in sicurezza eventuali alloggiamenti per floppy disk, cd/dvd con del nastro per evitare apertura/espulsione del contenuto.

Raccolta

- **Sistema acceso**

  Nel caso in cui si operi su un sistema accesso, vanno prese in considerazione le seguenti attività:

  - acquisire i dati volatili del dispositivo prima di spegnerlo, così da poter avere a disposizione eventuali chiavi di crifratura residenti in memoria. Nel caso in cui si sospetti la presenza di meccanismi di cifratura conviene procedere in seguito con acquisizione logica
  - nel caso in cui si voglia lasciare il dispositivo acceso (ad esempio per presenza confermata di meccanismi di cifratura), bisogna prestare particolare cura durante il trasporto (raffreddamento, protezione da shock)
  - nel caso in cui si decida di spegnere il dispositivo, valutare se sia il caso di effettuarlo mediante regolare procedura di spegnimento o staccando il cavo di alimentazione (rimuovendo prima l'estremità attaccata al dispositivo e poi quella attaccata alla presa). Normalmente tale decisione dipende dalla configurazione del sistema
  - etichettare e staccare tutti i cavi dal sistema. Etichettare tutte le porte cosi che lo stato del sistema possa essere ricostruito in laboratorio
  - proteggere il tasto di accensione, onde evitare una accensione casuale del dispositivo
  - infine, nel caso tale dispositivo sia un notebook, acquisire i dati volatili prima di rimuovere batteria e successivamente il cavo di alimentazione. Mettere in sicurezza anche eventuali alloggiamenti per floppy disk, cd/dvd utilizzando del nastro.

Acquisizione

- **Sistema trovato acceso**

  Nel caso in cui il sistema venga trovato accesso, vanno prese in considerazione le seguenti attività:

  - acquisire tutti i dati volatili che verrebbero persi se il dispositivo venisse spento (es. RAM, processi in esecuzione, connessioni di rete, impostazioni di data ed ora). Per effettuare l'acquisizione è consigliabile riversare i dati copiati in un contenitore logico, calcolarne l'hash e documentarne il valore. Ove ciò non sia fattibile è possibile utilizzare un contenitore di tipo ZIP, calcolarne l'hash e documentarlo
  - iniziare il processo di copia forense dei dati non volatili utilizzando strumenti validati. La copia forense ottenuta va memorizzata in un dispositivo preparato per tale scopo (es. Formattato). Se la copia viene invece memorizzata in un contenitore logico bisogna assicurarsi che questa non possa essere corrotta o danneggiata. Al termine del processo di copia calcolare e annotare il valore di hash
  - utilizzare una sorgente affidabile per documentare data e ora e documentare accuratamente inizio e fine di oggi attività

Acquisizione

- **Sistema trovato spento**

  Nel caso in cui il sistema venga trovato spento, vanno prese in considerazione le seguenti attività:
  • assicurarsi che il sistema sia davvero spento
  • rimuovere il supporto di memoria dal dispositivo spento (se non già fatto), ed etichettarlo accuratamente (es. Produttore, modello, numero di serie)
  • eseguire la copia forense del supporto di memoria utilizzando un tool validato. Calcolarne il valore di hash al termine.

- **Sistemi critici**

  Un caso particolare nella fase di acquisizione si ha quando ci si trova davanti ad un sistema critico, per cui per svariate ragioni non è possibile procedere all'acquisizione completa dei dati contenuti all'interno del sistema. Alcuni esempi di tali sistemi sono data center, sistemi di sorveglianza o sistemi medici. In tali situazioni vi sono due sole possibili alternative di acquisizione:

  • acquisizione live (acquisizione totale della memoria RAM e di massa)

  • acquisizione parziale (solo determinate porzioni di memoria di interesse investigativo)

Acquisizione: write blocker

Per dare garanzia del rispetto dei principi enunciati, tutte le operazioni eseguite in fase di acquisizione devono essere accuratamente documentate, meglio se si utilizzando dei dispositivi che registrano automaticamente quanto viene eseguito.

Se possibile è conveniente utilizzare anche dei dispositivi che impediscono l'alterazione del supporto di origine: c.d. write-blocker

Acquisizione: impronta hash

- Al termine della fase di acquisizione bisogna “sigillare” i dati acquisiti attraverso un sigillo digitale (solitamente un impronta hash con l’eventuale aggiunta dell’utilizzo di una firma digitale per associare l’operazione al DEFR) per dimostrare che la copia ottenuta sia identica all’originale.

Conservazione

L’evidenza, infatti, va preservata sia durante il trasporto (se effettuato) che lo stoccaggio, che potrebbe superare il suo tempo di vita a seconda dei tempi del procedimento

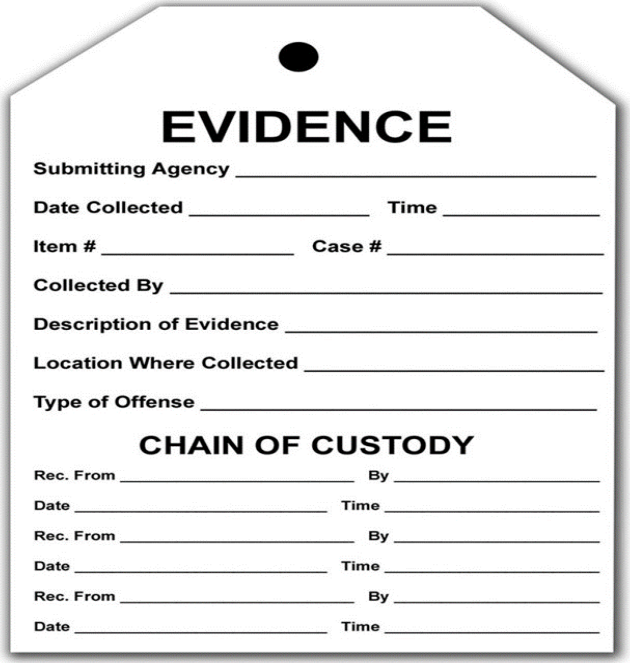
Per far ciò occorre:

- Etichettare tutto
- Verificare che le batterie siano opportunamente caricate (e ricaricare)
- Bloccare parti mobili
- Ridurre rischi in base alla natura del supporto
- Ridurre rischi dovuti al trasporto

Conservazione: catena di custodia

Catena di custodia

- Documentare movimenti e interazioni con la potenziale prova digitale
- Storia del supporto a partire dalla fase di raccolta
- Formato cartaceo o digitale
- Deve contenere
  - Identificativo unico dell'evidenza
  - Quando, dove, chi e perché ha avuto accesso all'evidenza
  - Documentare e giustificare ogni alterazione inevitabile, con il nome del responsabile



Analisi

L’analisi deve consentire la ricostruzione degli eventi passati attraverso la lettura dei dati rinvenuti.
Poiché ogni copia coincide con l’originale, l’analisi va eseguita su una copia dei dati acquisiti e non sull’originale
Caratteristiche dell’analisi

- Riproducibilità: Ogni singola operazione deve produrre sempre lo stesso risultato (si intende risultato oggettivo, cioè i dati e non la loro valutazione)
- Metodologie: si può applicare la Regola delle 5W
  - WHO? («Chi?»)
  - WHAT? («Che cosa?»)
  - WHEN? («Quando?»)
  - WHERE? («Dove?»)
  - WHY? («Perché?»)

Analisi: metodologia

- Che cosa è successo e come si è svolto?
  - Individuare i dati utili a ricostruire I fatti
  - Comunicazioni
  - Documenti
  - Log
  - Metadati (date, luoghi, coordinate…)
- Chi è coinvolto?
  - Comunicazioni
  - Metadati (date, utenti)
- Quando è accaduto?
  - Comunicazioni
  - Metadati (date, utenti)
- Da dove a dove?
  - Comunicazioni
  - Documenti
  - Log
  - Metadati (date, luoghi, coordinate…)
  - Tabulati telefonici
- Quante volte si è verificato?
  - Comunicazioni
  - Documenti
  - Log
  - Metadati (date…)
- C’era consapevolezza?
  - Comunicazioni
  - Cancellazione dati
  - Documenti
  - Log
  - Metadati (date…)
  - Navigazione web
  - Competenze utente

Analisi: strategie operative

- Ricerche
  - Autore
  - Intervallo di date
  - Tipo di file
  - Parola chiave
  - Per hash
  - Per thread (email)
- Recupero dati
  - Recupero dati cancellati, carving…
- Interpretazione dati
- Conversione tra formati
- Crack password
  - File tipicamente protetti
  - Tipologie di attacco
- Artefatti del sistema operativo

Analisi: carving

Il data carving è un processo di estrazione di un set di dati da un insieme di dati molto più ampio.

La tecnica del data carving è utilizzata solitamente durante le indagini di analisi forense per analizzare lo spazio non allocato.

Durante questo procedimento è ignorata la struttura del file system.

I file sono individuati e catalogati in base all'header e al footer trovato.

Distinguiamo

- Data carving base
  - L'header e footer dei file non sono sovrascritti
  - Il file non è frammentato
  - Il file non è compresso
  - Il file estratto è l'insieme di bit contenuti tra header e footer
- Data carving avanzato
  - I frammenti non sono sequenziali
  - I frammenti non sono ordinati
  - Mancano dei frammenti

Analisi: timeline

Spesso è necessario ricostruire la cronologia delle attività svolte

Occorre creare una linea temporale relativa agli eventi verificatesi e richiede l'integrazione delle varie informazioni temporali (timestamp) create dal sistema operativo, dal file system e dalle applicazioni utente.

- Metadata dei file (timestamp della creazione, ultimo accesso ed ultima modifica dei file)
- Esecuzione dei programmi (S.O. registra informazioni sull'esecuzione dei programmi)
  - File prefetch su Windows
  - Registro di Windows
  - File log di sistema ….
- Artefatti generati dai programmi ad ogni esecuzione
  - Elenco file aperti o salvati
  - File di cronologia di navigazione
  - File di log ….

Valutazione

La valutazione è una fase necessaria per stabilire:

- Se il reperto informatico è stato
  - alterato
  - inquinato
  - contraffatto
- Se le procedure di acquisizione sono state legittime
- Se il reperto è
  - attendibile
  - integro
  - Autentico
- Il significato dei dati presenti sul supporto

Presentazione

La presentazione è l'elemento con cui si valuta tutta l'attività svolta.

Essa deve comprendere in maniera dettagliata:

- Le fasi dell'analisi
- Le metodologie applicate
- Gli strumenti utilizzati
- I risultati ottenuti
  - Integrando con gli allegati
  - Foto dei reperti
- La risposta al quesito