Oggi riprendiamo il discorso introduttivo sulla materia, la scorsa volta ci eravamo lasciati con le funzioni hash.

Queste sono diventati meccanismi di base per garantire l’integrità durante tutti i processi dell analisi forense.

Se dobbiamo analizzare 500 file dobbiamo calcolare 500 hash? Dipende, possiamo innanzitutto calcolare l’HASH di tutto il volume, se vogliamo aumentare la reliability possiamo farlo sui singoli file.

Quali sono le fasi della digital forensics, quelle che abbiamo già visto.

La chain of custody si concretizza in tutte le fasi ovviamente, bisogna sempre stare attenti a documentare sempre i reperti

Aprire un file msword cambia l’hash, dipende.

Cos’è un meccanismo di write-blocker, dice che è un meccanismo software che impedisce la scrittura sulla sorgente, ma non mi convince, ma in realtà è così

Problematiche di analisi “live”, perdità di ripetibilità delle operazioni, che potrebbero non essere più fatte e possono dare risultati differenti

Come possono essere affrontate le collisioni delle funzioni hash, praticamente si usano due hash differenti per minimizzare la possibilità di collisione, teoricamente non si può risolvere il problema

DISPOSITIVI DI MEMORIZZAZIONE:

bisogna tenere conto di come vengono memorizzati i dati, frammentazione, segmenti, etc…

CANCELLAZIONE DEI DATI:

Se effettuata tramite software standard rimuove solamente l’indirizzo dell’informazione associata ad ogni blocco di dati, si può recuperare con appositi strumenti(finchè la zona di memoria non viene allocata per altri blocchi), oppure viene spostato in un cestino.

Viene fatta tramite software di wiping che cancellano in modo accurato il dato

Dal video delle iene, la cancellazione non era fisica ma di tipo logico, e quindi si poteva recuperare la maggior parte dell’informazione nonostante fosse stata cancellata.

SLACK SPACE:

memoria non allocata, spazio tra l’ultimo bit e la fine del settore, può contenere dati nascosti-cancellati logicamente.

**IMAGE AND VIDEO FORENSICS**

Ovviamente ci deve essere una infarinatura generale di image processing, mega-ripasso incoming.

Authenticity(accurate representation of the original event) diversa da integrity(informazione inalterata dal tempo di acquisizione al temo della disposizione finale) , la funzione hash lavora sull’integrità

In molti paesi si sta lavorando per digitalizzare tutto, cioè vedere tutte le azioni che succedono nella realtà e registrarle in qualche modo(videocamere ovunque e quasi grande fratello)

Best practices nelle slide

Immagini e video impattano il sistema cognitivo? Il nostro immaginario viene fortemente condizionato.

Quello che si vede nei fil è troppo esagerato, non si possono creare informazioni dal nulla(fantasy)