I file system e il journaling

Un viaggio all'interno del mondo dei file system e come funzionano

Cos'è un file system. Essenzialmente un file system è quel sistema di gerarchie che permettono al sistema operativo e di conseguenza a noi, la suddivisione in cartelle, i permessi dei vari file e l'ordine generale di esso. I file system sono lo scheletro di un pc e ogni sistema operativo adotta uno o più file system supportati. Alcuni file system sono: NTFS, FAT32, FAT16, exFAT, ext4, ext3, ext2, APFS, Mac FS, ReFS, etc …
Noi in questa serie di introduzioni ai controlli ed alla scienza più grande dietro tutto questo che è l'informatica forense, parleremo per semplicità di Windows, che adotta come file system il NTFS (New Technology File System).

MACB Timestamps

Prima di parlare di journaling e concetti più complessi, parliamo di una feature che viene sottovalutata ma è fondamentale la conoscenza e comprensione adeguata di essa per continuare. I timestamp sono delle date più orari salvati per scopi. I MACB timestamp sono una serie di 4 timestamp fondamentali che indicano degli eventi basici. Ecco il significato di MACB e i timestamp indicati:

- (M) Modified / Modificato, l'ultima volta che il contenuto del file è stato cambiato
- (A) Access / Accesso, l'ultima volta che il file è stato aperto (sembra utile in verità irrilevante)
- (C) Changed / Cambiato, indica un cambiamento del suo indice sulla Master File Table ($MFT)
- (B) Birth / Creazione, il momento in cui il file è apparso sul disco

Il timestamp access è irrilevante perché con tutti i servizi per compatibilità e altro, un accesso del file può avvenire anche con delle applicazioni in background, il che rende il tutto molto inaffidabile quando si dimostra l'esecuzione di un file, e quindi porta a false flag.

Master File Table

La Master File Table è un file che indica ogni singolo file presente sul disco fisso. Il parsing di tale artefatto è fondamentale per una conoscenza accurata dei file presenti sul disco.

$USNJrnl

Il file che contiene il comunemente noto "journal" è il $USNJrnl, un file che si trova nella cartella C:\$Extend, cartella nascosta e inaccessibile attraverso explorer normalmente. Il journal del file system è un log di ogni singola attività che è stato possibile registrare sul file system. Qualsiasi spostamento di un determinato file, un cambiamento di dati, una rinominazione o una eliminazione; tutto viene salvato sul journal. Una particolarità di questo artefatto, è che il file $USNJrnl in se è vuoto, ma esso ha due stream di dati alternative che contengono le seguenti informazioni:

- $Max: contiene informazioni come la dimensione massima del journal
- $J: contiene le informazioni effettive, quindi tutti gli USN records dei vari eventi

Tali informazioni vengono comunemente lette attraverso l'utilizzo dell'utility di sistema fsutil. Non è l'unico modo per leggere tali informazioni. Esse si possono leggere anche tramite utility esterne tipo OSForensic, etc…

$LogFile

Il $LogFile è un file particolare che è simile in funzionalità al $USNJrnl, ma invece di salvare USN Records, salva i cambiamenti ai metadata dei file, diverso dal salvare cambiamenti al file in se. Questo comprende i timestamp MACB del file relativo a varie casistiche e collegamenti alla Master File Table. Questo artefatto è estremamente utile e prezioso, anche se è particolarmente difficile da parsare e come argomento non c'è tanta documentazione. L'unico tool che parsa questo artefatto conosciuto almeno da me in questo momento si chiama NTFS Log Parser. Come tutti i tool indicati ci sarà una pagina apposta con i vari download.

Conclusione

Il filesystem è una parte da analizzare interessante, perché il tutto sta nel prendere queste informazioni nude e spoglie, e collegarle per avere un knowledge basico di come i file si sono spostati nel tempo. È un argomento vasto e ne sto coprendo solo la superficie, quindi di conseguenza invito a informarsi da ste basi e continuare ad interessarsi a questi argomenti. Qui chiudo.