



Computer Forensic

Giuseppe Augiero

Analisi del File System

Agenda

- ▶ Cosa è la computer forensic.
- ▶ Come è organizzato un file system.
- ▶ I tool da usare.
- ▶ Timeline.

Computer Forensic

- ▶ L'informatica forense è la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico al fine di essere valutato in un processo giuridico.

Come nasce?

- ▶ E' una disciplina di recente formazione.
- ▶ Nasce intorno ai primi anni 80 ad opera dei laboratori della FBI.
- ▶ Spesso viene erroneamente identificata come una parte dell' IT Security.

Cosa permette?

- ▶ Aiuta a ricostruire eventi passati e attività svolte.
- ▶ Mostra l'uso e l'abuso di infrastrutture IT.
- ▶ Mostra segni di violazione della normativa o di attività illecite.
- ▶ Permette di dimostrare possesso e gestione dei dati digitali.

Reati

- ▶ Reati informatici.
- ▶ Reati non informatici in cui sono stati utilizzati mezzi tecnologici.



Livelli del File System

- ▶ Fisico.
- ▶ File System.
- ▶ Data.
- ▶ Metadata.
- ▶ File Name.

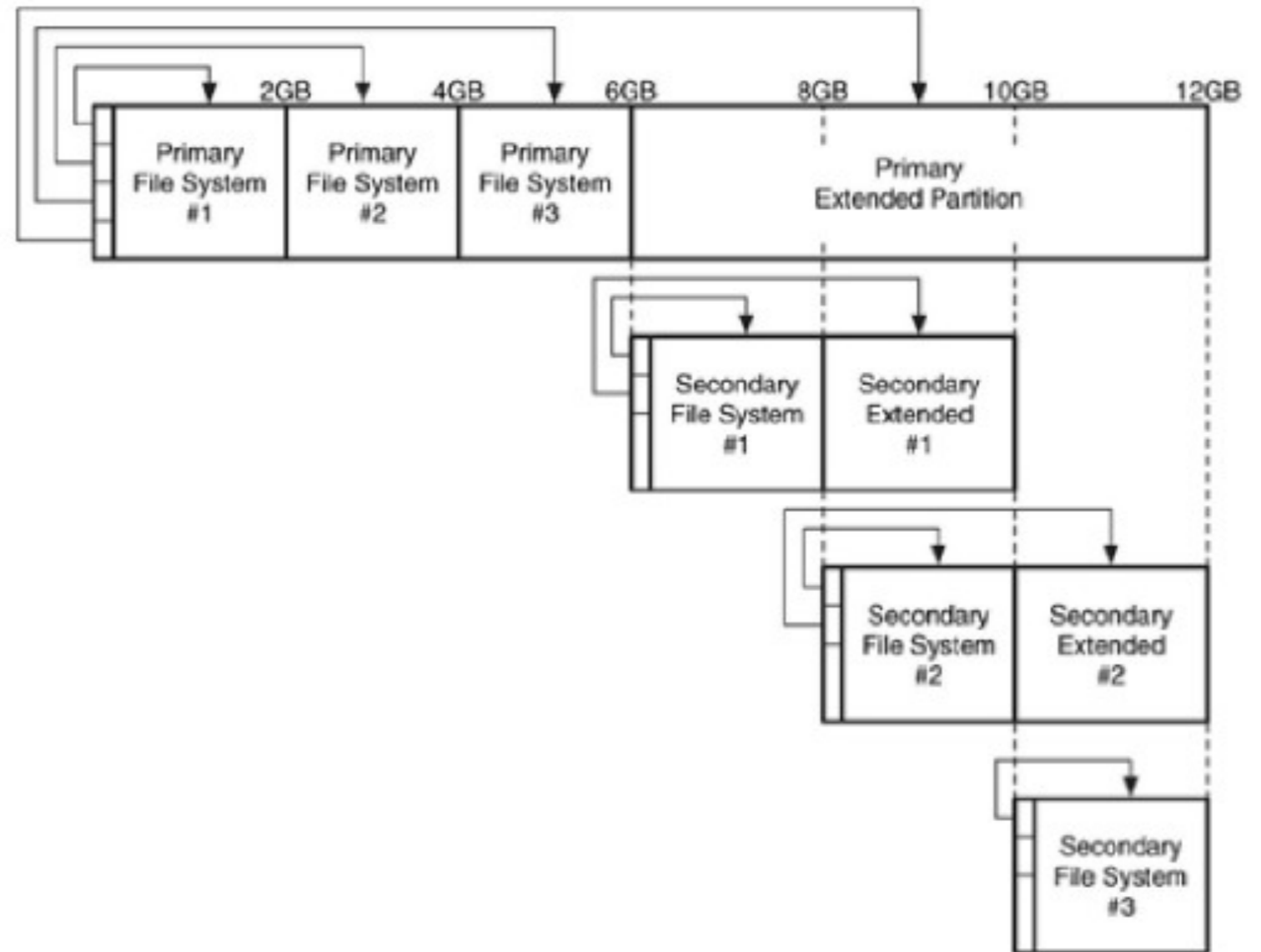
FS Layer

- ▶ Dettagli strutturali (dimensione blocchi, posizione).
- ▶ Queste informazioni sono immagazzinate nei superblocchi, boot sector, mbr.

Partizioni

- ▶ Nel primo settore troviamo una partition table per 4 partizioni.
- ▶ Primary file system.
- ▶ Primary extended partion.
- ▶ Secondary file system.
- ▶ Secondary extended.

Esempio di struttura



MBR

Byte	Description
0-445	Boot Code
446-461	Partion table 1
462-477	Partion table 2
478-493	Partion table 3
494-509	Partion table 4
510-511	Signature (0xAA55)

Partion Entries

Byte	Description
0-0	Boot flag
1-3	CHS start
4-4	Partiotion type
5-7	CHS end
8-11	LBA start
12-15	Size (sectors)

Data Layer

- ▶ Contiene i dati veri e propri.
- ▶ Settori di 512 byte.
- ▶ Settori consecutivi raggruppabili indirizzabili (cluster, blocchi).
- ▶ Le dimensioni dei cluster viene indicata nel superblock o bootsec.
- ▶ Blocchi allocati o non allocati.

Meta-data Layer

- ▶ Strutture che descrivono un file: inode, master file table e fat.
- ▶ Puntatori ai dati e informazioni (Mactime e permessi).
- ▶ Ogni struttura di metadati ha un indirizzo.

Filename Layer

- ▶ Conservati in:
- ▶ Metadata
- ▶ Directory file

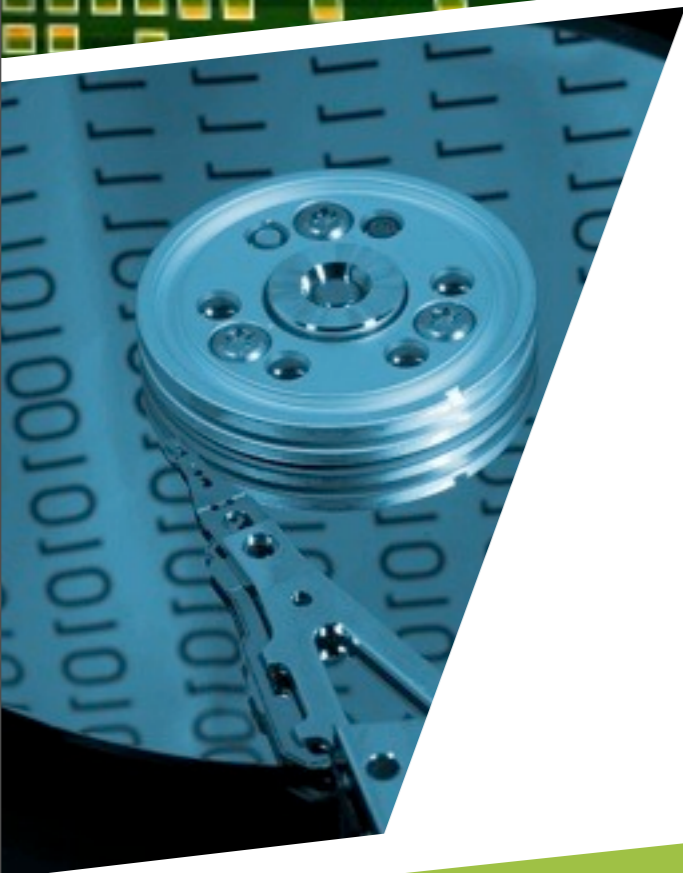
Cancellazione di file

- ▶ Cosa succede quando cancello un file?
- ▶ Fat
- ▶ Ntfs
- ▶ Ext3



Sleuth kit

- ▶ Sviluppato da Brian Carrier.
- ▶ Insieme di tool per l'analisi e il recupero di informazioni di:
 - ▶ disk layout, partizioni.
 - ▶ file system, directory, file.
 - ▶ timestamps.
 - ▶ files cancellati o spazio non allocati



Approccio a livelli

- ▶ **Fisico:** mmls, mmcat, mmstat
- ▶ **File system:** fsstat.
- ▶ **Metadata:** icat, ils, ifind, istat
- ▶ **Filename:** fls, ffind
- ▶ **Content (data):** blkcalc, blkcat, blkls.

Foremost

- ▶ Basato su scapel.
- ▶ Permette di effettuare il “data carving”.
- ▶ Analizza l’intestazione e il footer di qualsiasi file con formato conosciuto.
- ▶ Ottimo per analizzare dischi di swap, dischi corrotti, traffico di rete.

Timeline

- ▶ Fondamentali per le analisi degli incidenti.
- ▶ Possono essere creati con molti strumenti.
- ▶ Estremamente sensibili alle variazioni del sistema.
- ▶ E' la prima attività che è consigliabile eseguire.

Mac time

FS	Data	Gran	M	A	C	B
EXT2/3/4	Epoch	1s	Mod	Access	Mod Inode	-
FAT	Local	2s	Mod	Access	-	Create
NTFS	UTC	100ns	Mod	Access	Mod MFT	Create

Supertimeline

- ▶ E' possibile analizzare più informazioni riguardandi dati temporali e combinarli in unica timeline.

Domande?

GRAZIE

www.augiero.it

giuseppe@augiero.it



Licenza di utilizzo

Queste slide sono protette dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo e il copyright delle slide (ivi inclusi, ma non limitatamente, ogni immagine, fotografia, animazione, video, audio, musica, testo, tabella, disegno) sono di proprietà dell'autore. Le slide possono essere riprodotte e utilizzate liberamente dagli istituti di ricerca, scolastici e universitari italiani afferenti al Ministero dell'Istruzione, dell'Università e della Ricerca per scopi istituzionali e comunque non a fini di lucro. In tal caso non è richiesta alcuna autorizzazione.

Ogni altro utilizzo o riproduzione, completa o parziale (ivi incluse, ma non limitatamente, le riproduzioni su supporti ottici e magnetici, su reti di calcolatori e a stampa), sono vietati se non preventivamente autorizzati per iscritto dall'autore. L'informazione contenuta in queste slide è ritenuta essere accurata alla data riportata nel frontespizio. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, reti, etc. In ogni caso essa è soggetta a cambiamenti senza preavviso. L'autore non assume alcuna responsabilità per il contenuto delle slide (ivi incluse, ma non limitatamente, la correttezza, la completezza, l'applicabilità, l'adeguatezza per uno scopo specifico e l'aggiornamento dell'informazione).

In nessun caso possono essere rilasciate dichiarazioni di conformità all'informazione contenuta in queste slide. In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata fedelmente e integralmente anche per utilizzi parziali.