Corso di Digital Forensics

CdLM in Informatica

Università degli Studi di Salerno

Docente: Ugo Fiore

5bis – Mac forensics

Mac Forensics

Schema Generale

Nulla cambia rispetto a Windows circa la priorità di acquisizione ed analisi

1. Acquisizione ed analisi delle informazioni altamente volatili
2. Acquisizione dei file
3. Acquisizione delle immagini di disco
4. Analisi dei file
5. Analisi delle immagini di disco

Cambiamenti più pronunciati riguardano invece le differenti versioni di macOS

Informazioni Altamente Volatili

Introduzione e Nozioni

Informazioni Altamente Volatili

Acquisizione

- A partire da macOS 11, il tool per acquisire la memoria (Surge Collect Pro)
- necessita di un particolare **driver**
- la cui installazione richiede il **riavvio del sistema**,
- limitando quindi l'utilità dell'operazione ai casi in cui il driver sia già installato

File e Immagini di Disco

Acquisizione

File

Acquisizione | 1/2

- I file di interesse sono sparsi in varie locazioni del file system
- Nomi e percorsi dei file cambiano frequentemente col susseguirsi delle versioni
- Per questo motivo esistono tool che permettono di raccoglierli

Immagini di disco

Acquisizione | 2/2

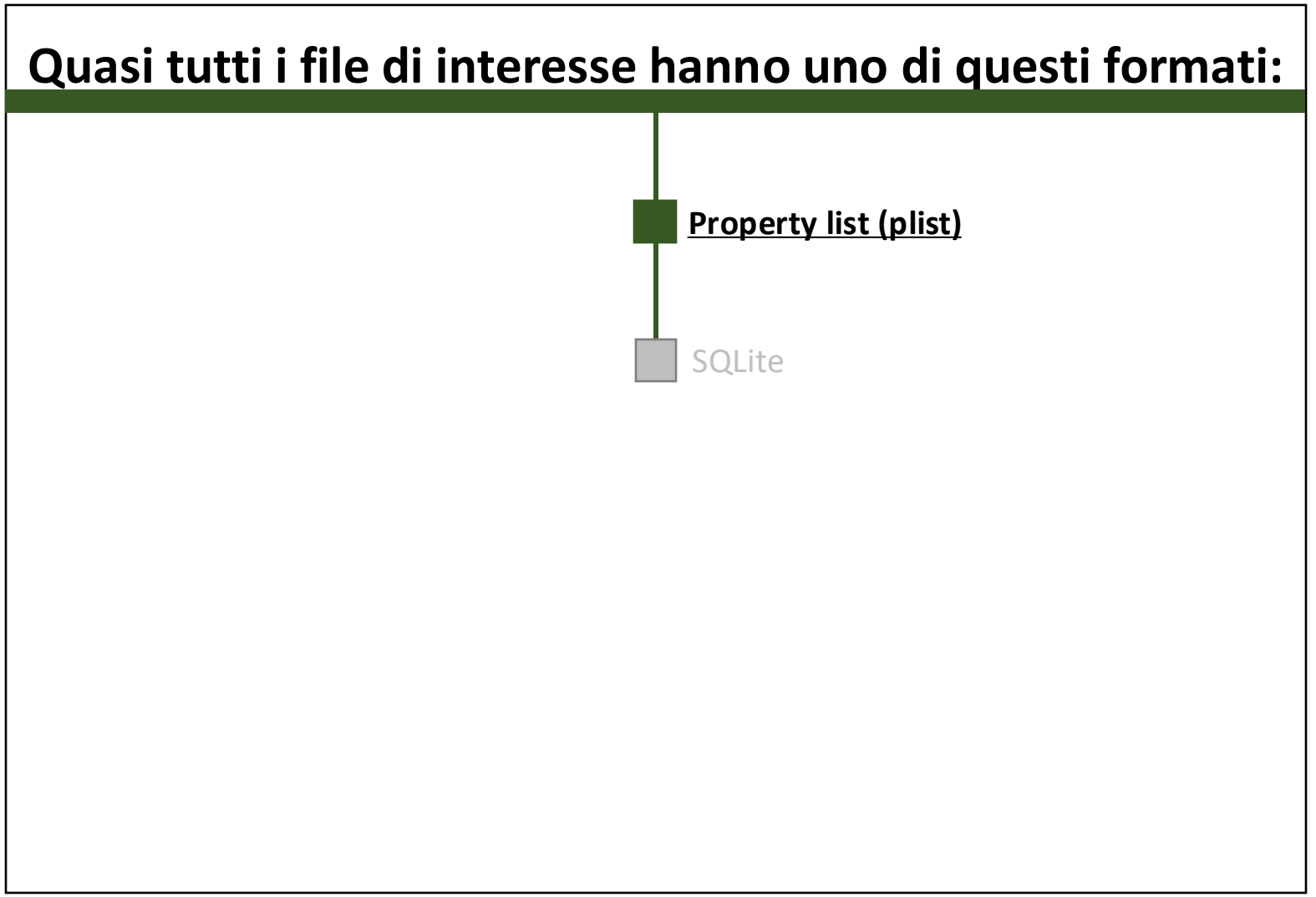
- Apple File System (APFS) supporta la cifratura a livello di file system
- Inoltre, le immagini APFS cifrate provenienti da Mac con processore della famiglia M richiedono, per la decifratura, chiavi memorizzate nei processori stessi.
- Per questo motivo occorre fare il boot del Mac in questione da un supporto esterno
- Secure boot: “No Security”
- Allowed Boot Media: “Allow booting from external or removable media”

Informazioni utili

Formati dei file

Informazioni utili

Formati dei file



Informazioni utili

plist

- Formato binario

PLUTIL(1) General Commands Manual PLUTIL(1)

NAME
plutil – property list utility

SYNOPSIS
plutil [command_option] [other_options] file
...

DESCRIPTION
plutil can be used to check the syntax of property list files, or convert
a plist file from one format to another. Specifying - as an input file
reads from stdin.

Informazioni utili

plist

- /usr/libexec/PlistBuddy

```
Usage: PlistBuddy [-cxlh] <file.plist>
   -c "<command>" execute command, otherwise run in interactive mode
   -x output will be in the form of an xml plist where appropriate
   -l if the path to <file.plist> contains symbolic links, they will
      not be followed.
   -h print the complete help info, with command guide
```

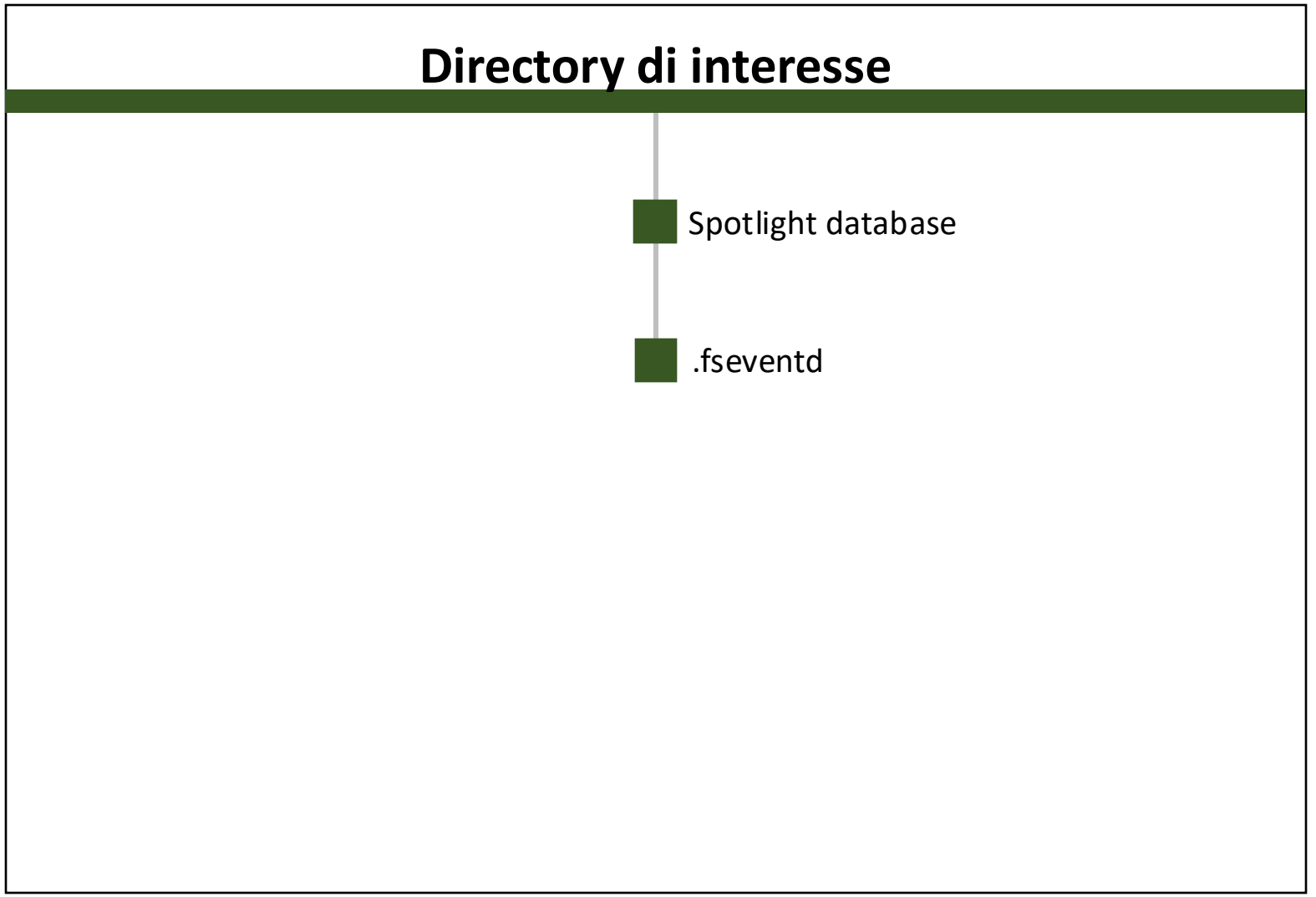
Informazioni utili

Formati dei file

Quasi tutti i file di interesse hanno uno di questi formati:

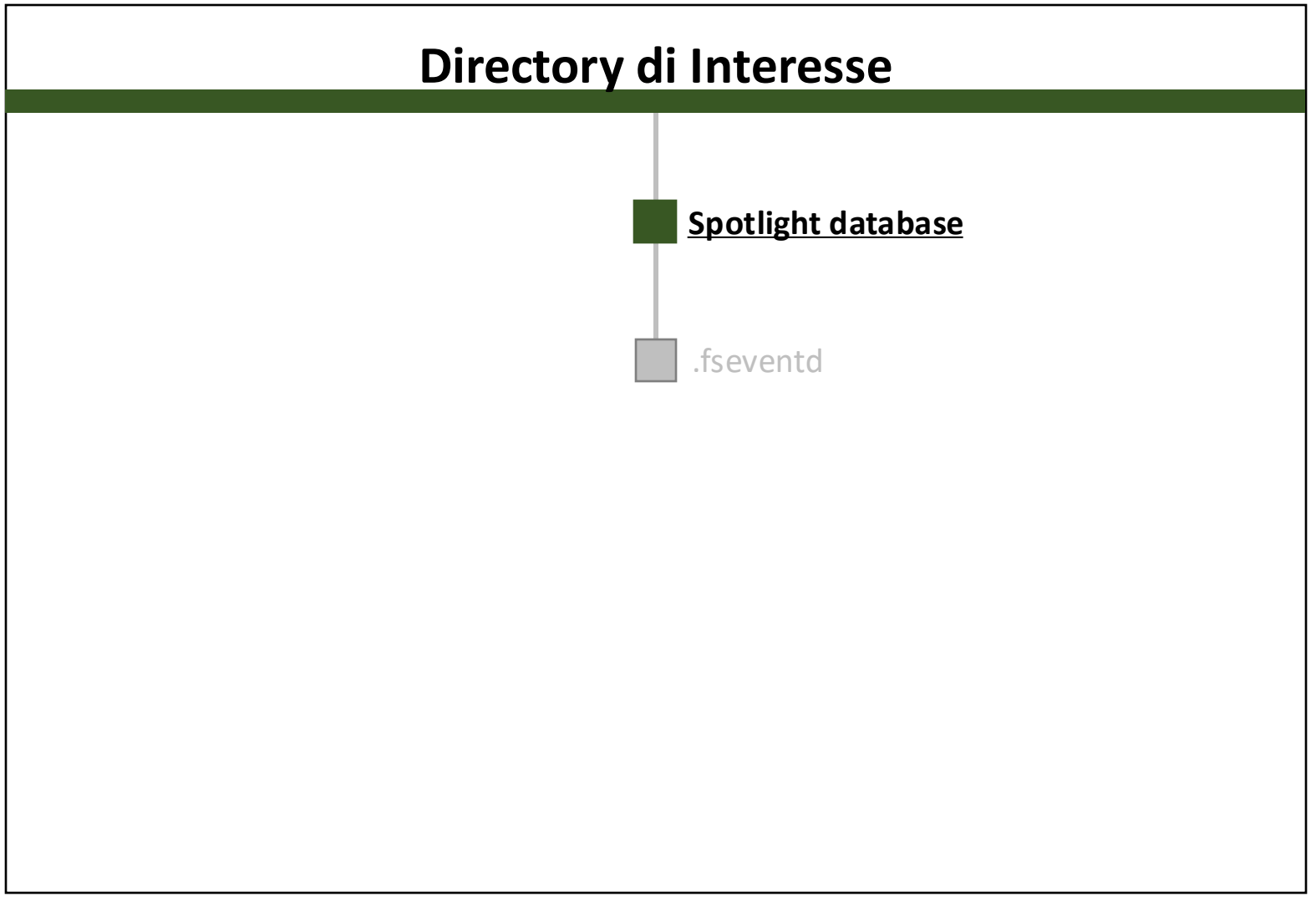
Informazioni utili

Directory di Interesse



Informazioni utili

Directory di Interesse



Directory di Interesse

Spotlight database | 1/3

- La directory .Spotlight-V100 è specifica del sistema operativo macOS e contiene i file e le directory utilizzati dal servizio Spotlight, che è il motore di ricerca integrato di macOS.

Immagini di disco

Spotlight database | 2/3

- La directory .Spotlight-V100 contiene i seguenti elementi principali:
  - Sottodirectory Store-V2 o simili: Contiene i file dell'indice principale per il volume. Questi file sono organizzati per UUID del volume e includono:
    - File di database (es. store.db o file binari) che memorizzano i metadati indicizzati.
    - File di supporto per la gestione dell'indice, come contentIndex.db .
  - File .store: Un file di metadati che descrive lo stato dell'indice.
  - Sottodirectory temporanee: Create durante l'indicizzazione o l'aggiornamento dell'indice, spesso con nomi casuali.
  - File di configurazione: Impostazioni specifiche per l'indicizzazione del volume, come esclusioni o priorità.

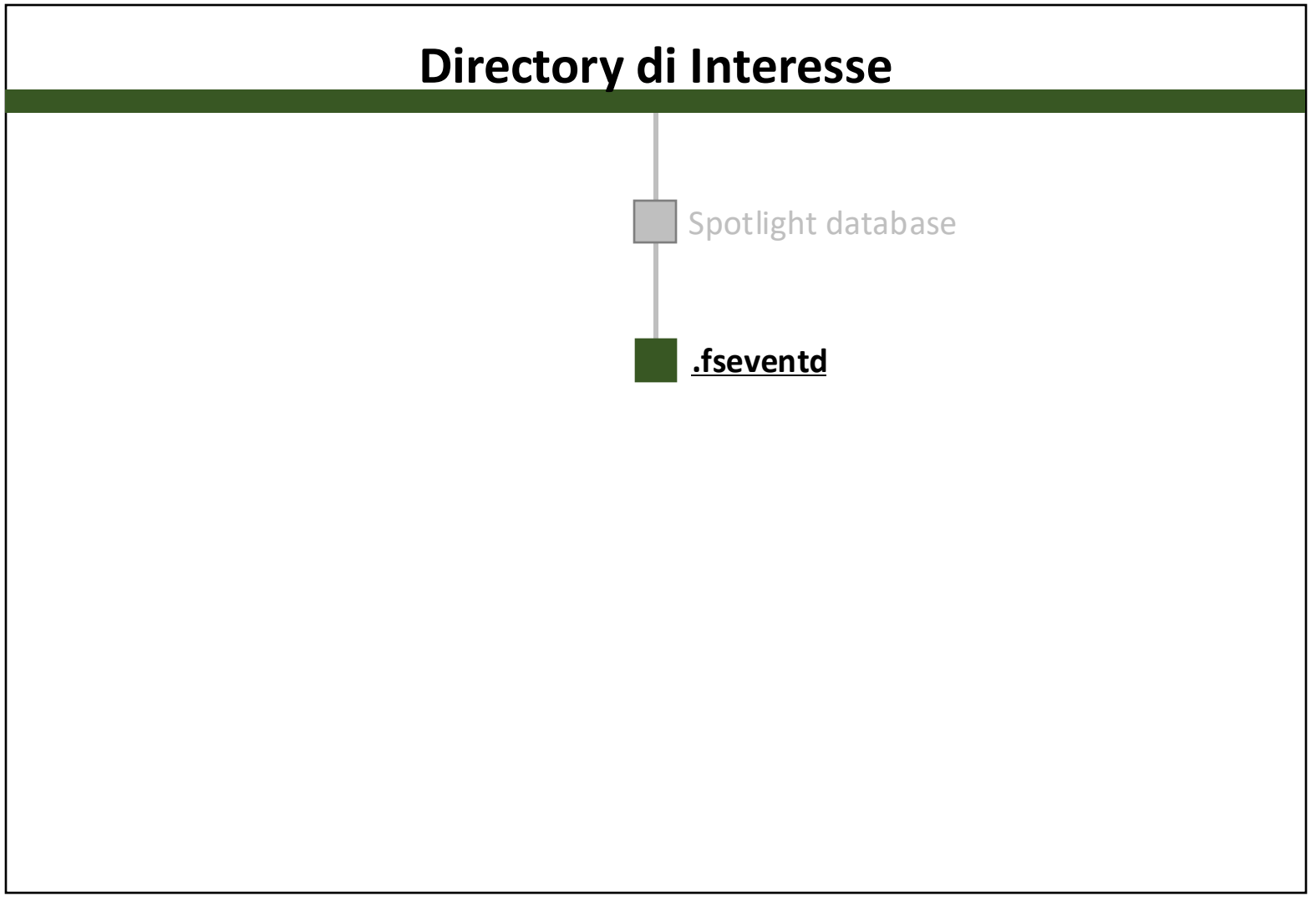
Immagini di disco

Spotlight database | 2/3

- La directory .Spotlight-V100 contiene i seguenti elementi principali:
  - Index: Questa directory contiene l'indice di Spotlight, che include informazioni dettagliate sui file, come contenuto di testo, metadati, e altri attributi. L'indice viene costantemente aggiornato man mano che vengono create, modificate o eliminate le risorse del file system.
  - VolumeConfig.plist: Questo file contiene le configurazioni specifiche del volume per Spotlight, come le opzioni di esclusione e le impostazioni di indicizzazione.
  - VolumeInfo.plist: Questo file contiene informazioni sul volume, come il tipo di file system, l'UUID del volume, e altri dettagli tecnici.

Informazioni utili

Directory di Interesse



Immagini di disco

.fseventd | 1/2

- La directory .fseventd è specifica del sistema operativo macOS e contiene file e directory utilizzati dal servizio fseventd, che fa parte del sistema di monitoraggio dei file system di macOS

Immagini di disco

.fseventd | 2/2

- .fseventd può contenere i seguenti elementi:
  - Un file di testo contenente un UUID (Universally Unique Identifier) che identifica univocamente il volume. Questo file serve a distinguere i volumi nei log degli eventi, specialmente quando più dischi sono collegati al sistema.
  - File di log compressi con nomi esadecimali (es. 0000000035fa46b6), che registrano eventi del file system.

Unified logs

log

- Il comando log

log(1) General Commands Manual log(1)

NAME

log – Access system wide log messages created by os_log, os_trace and other logging systems.

Unified logs

Console

- L’app Console mostra tutti i log