COMPUTER FORENSICS

Lezione 17: L'Analisi
i File System
(1ª parte)

A.A. 2021/22

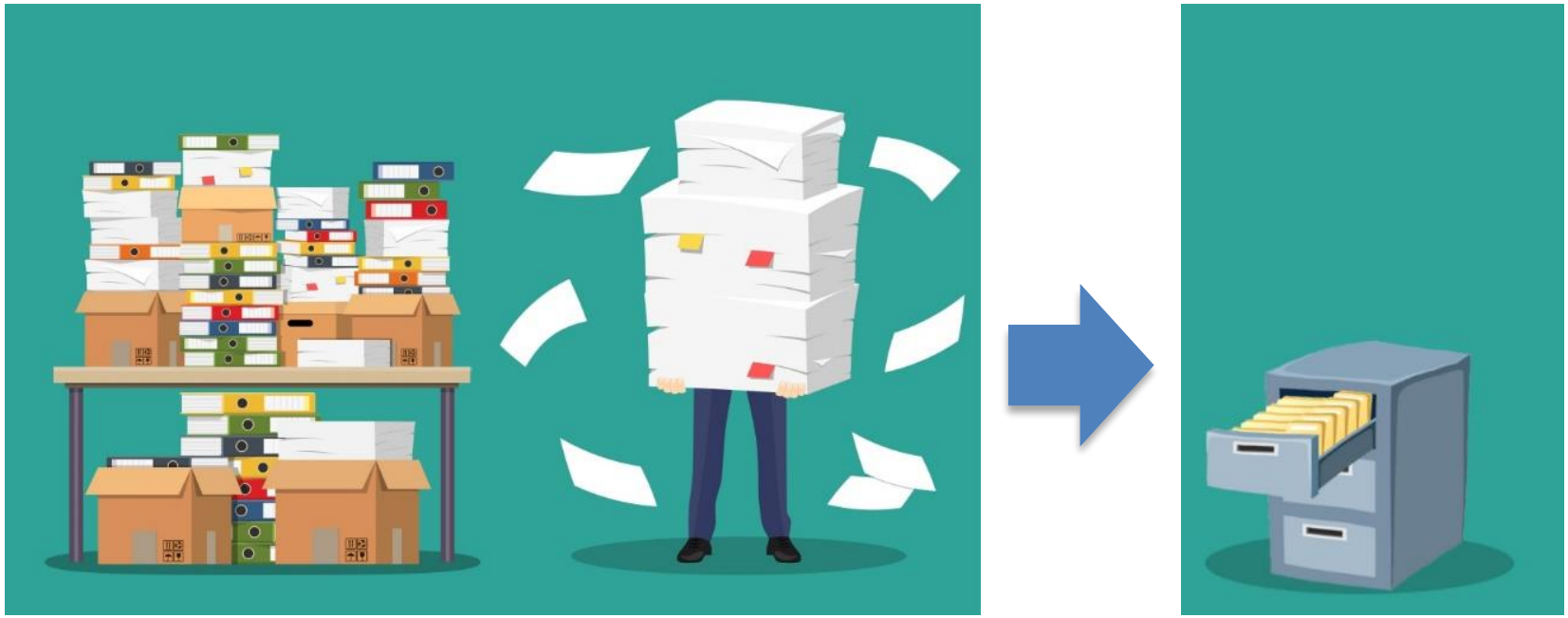
Dott. Lorenzo LAURATO

File System

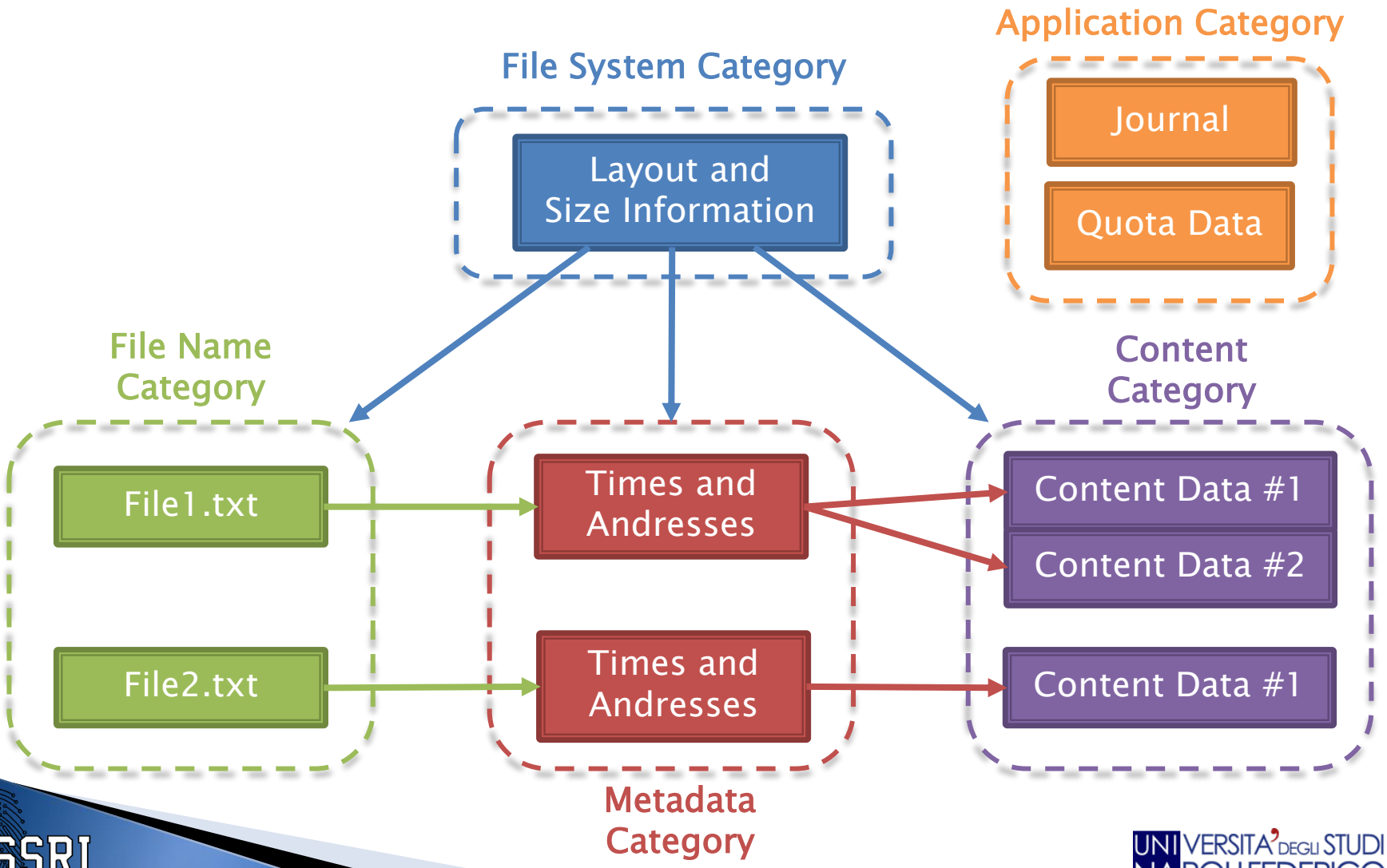
- Overview

File System

- Sistema che permette la memorizzazione dei dati, organizzandoli gerarchicamente in file e directory, in modo tale da ritrovarli velocemente.



File System


Application Category
File System Category
Journal
Quota Data
Layout and Size Information
File Name Category
Content Category
File1.txt
Times and Andresses
Content Data #1
Content Data #2
File2.txt
Times and Andresses
Content Data #1
Metadata Category

File System

Dati Essenziali

- Dati che se modificati/alterati causano il malfunzionamento del sistema:
  - Indirizzamento del contenuto del file
  - Nome del File
  - Dimensione del file

TRUSTED DATA

Dati Non Essenziali

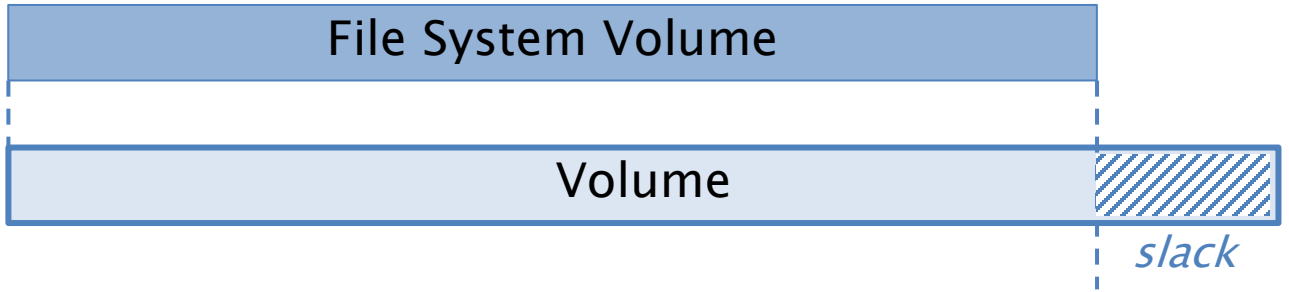
- Informazioni accessorie
  - Dati temporali
  - Permessi utente

UNTRUSTED DATA

File System:
File System Category

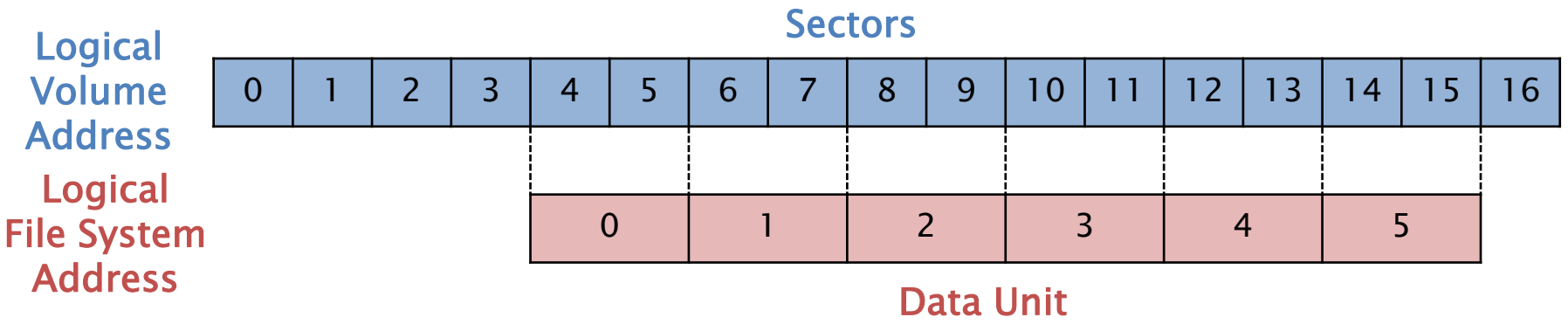
- Informazioni generali sul File System:
  - Solitamente posizionati nel primo settore
  - Essenziali: informazioni sul layout dei dati

- Analisi:
  - Informazioni sulla generazione del File System
  - Informazioni sul layout
  - Controllo di consistenza: *volume slack*



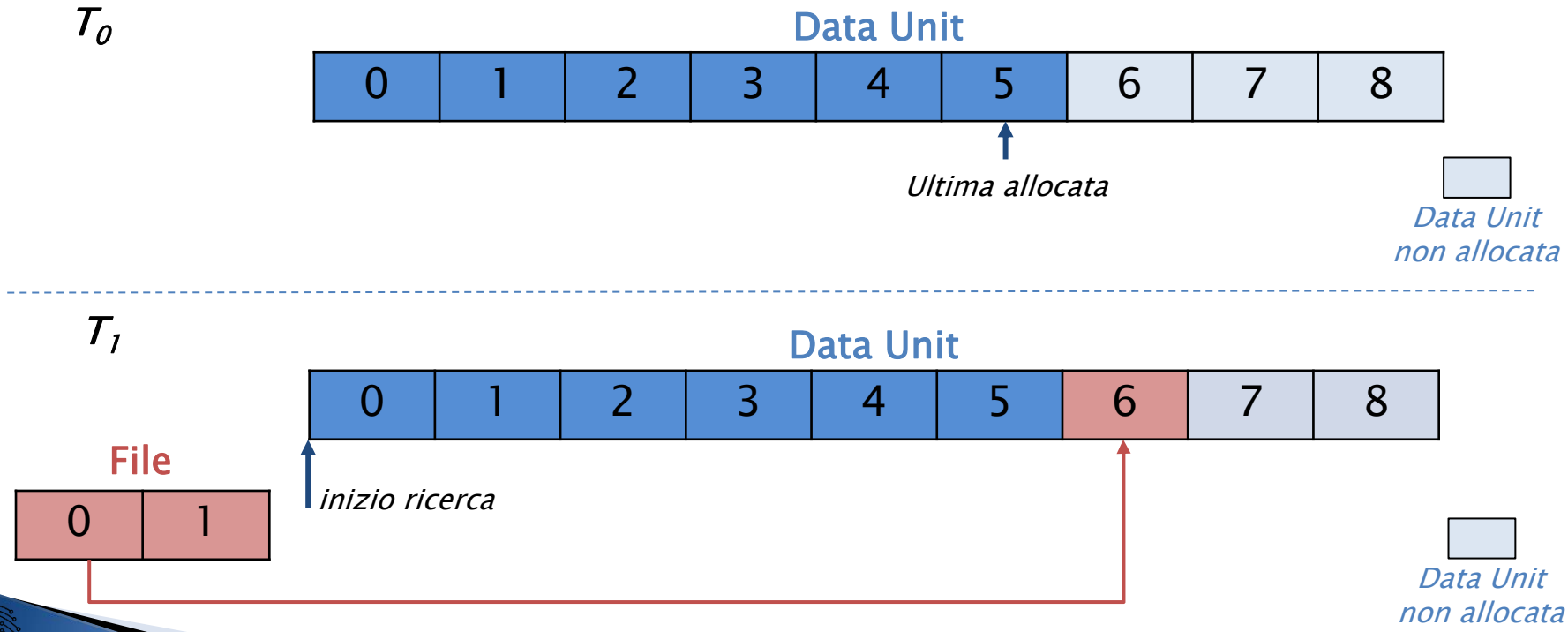
File System:
Content Category

- Locazioni di memoria impiegate per la memorizzazioni del contenuto dei file:
  - **Data Unit**: *raggruppamento di più settori*
    - STATO: allocato e non allocato
    - **Logical File System address**



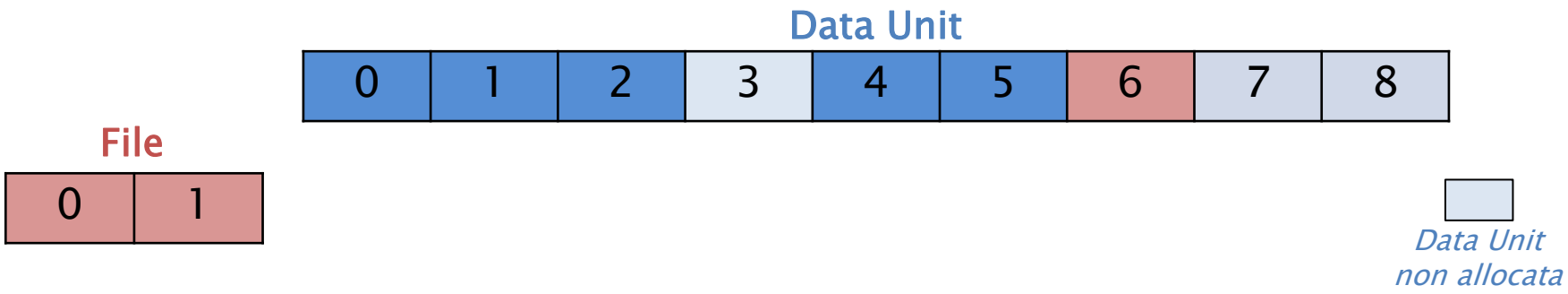
File System: *Content Category*
strategie di allocazione

- Strategia del primo disponibile:
  - Si cerca una «data unit» libera ogni volta partendo dall'inizio del file system.

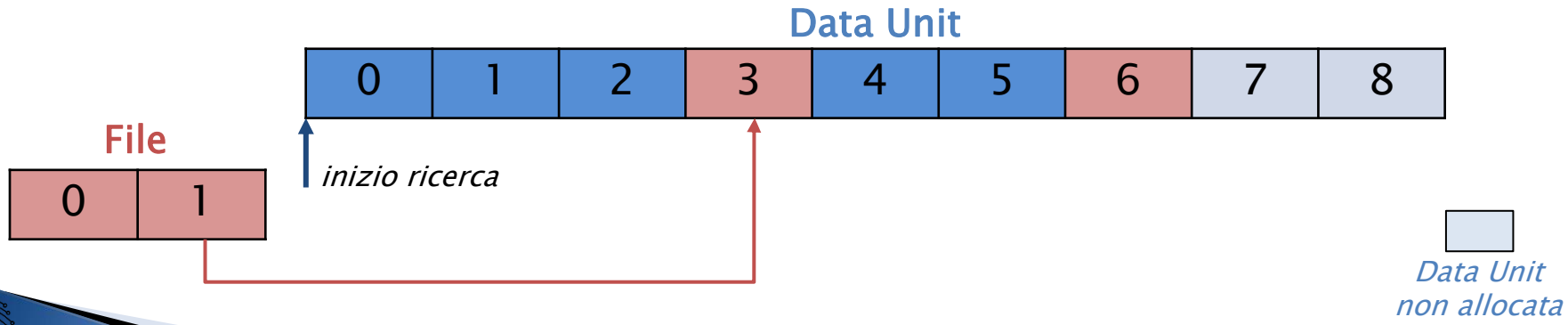


File System: *Content Category*
strategie di allocazione

T_2

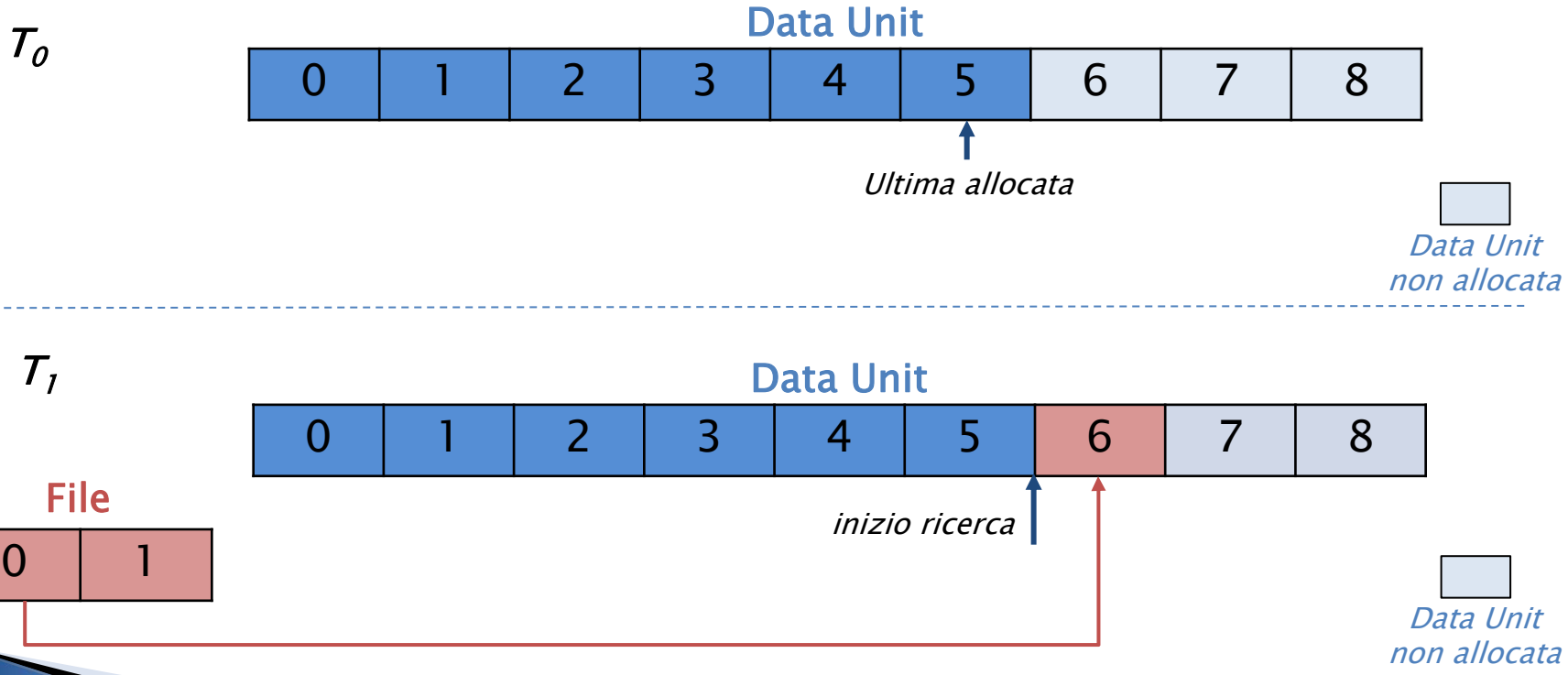


T_3

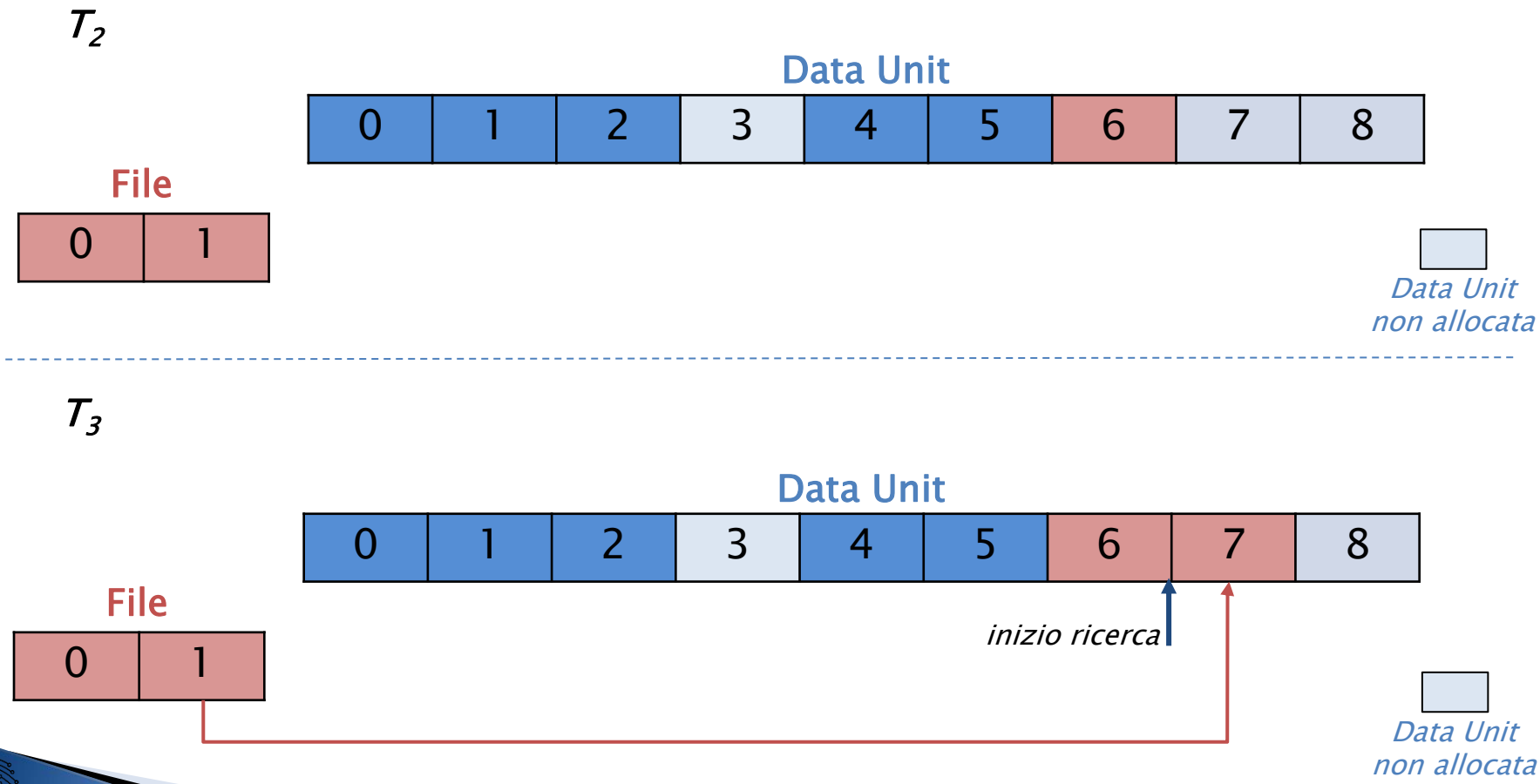


File System: *Content Category*
strategie di allocazione

- Strategia del prossimo disponibile:
  - Si cerca una «data unit» libera partendo dall'ultima locazione allocata

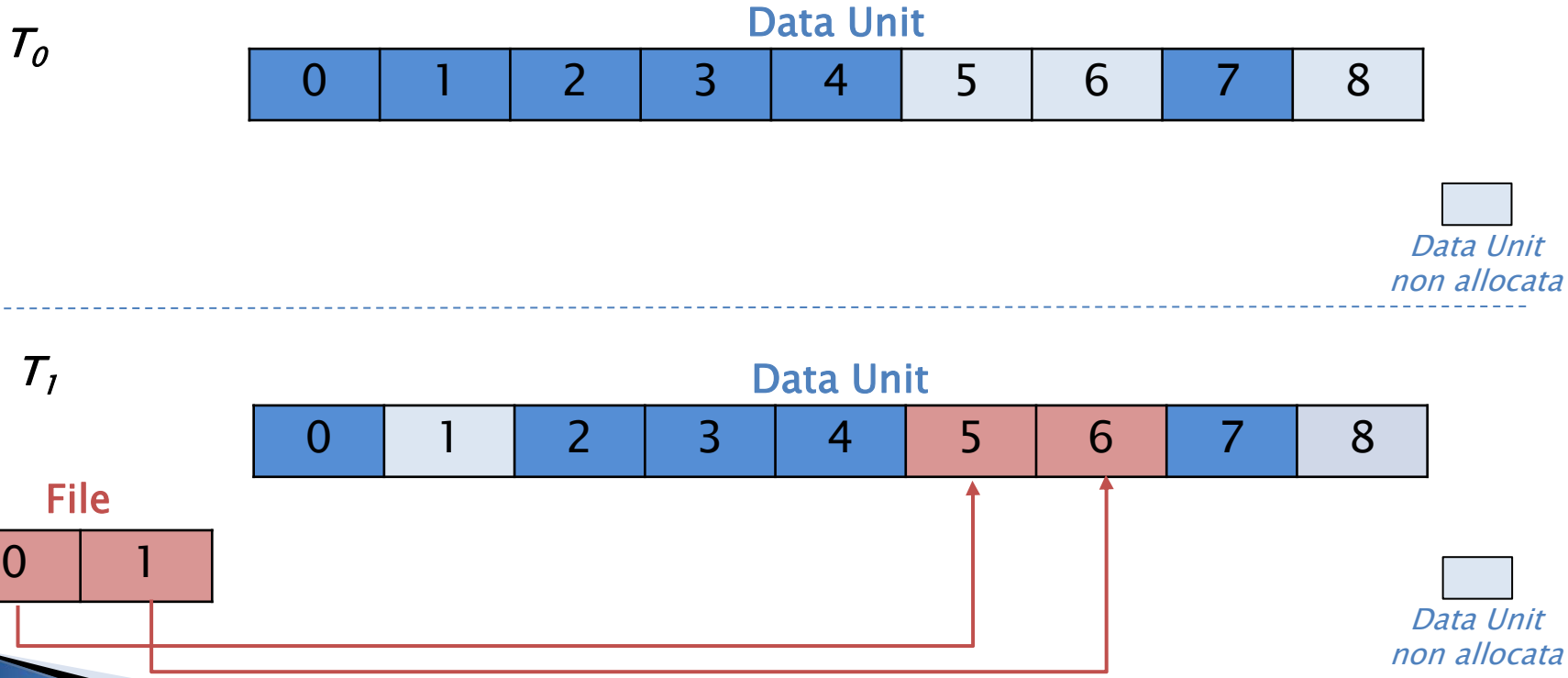


File System: *Content Category*
strategie di allocazione



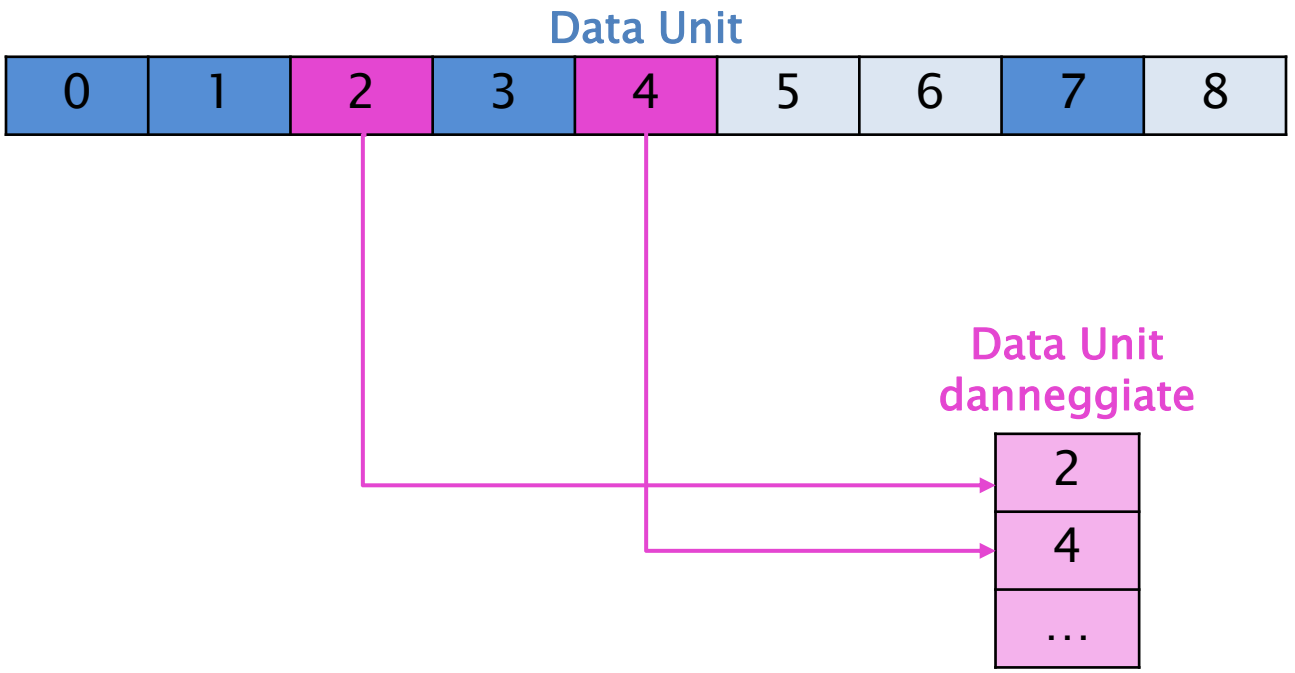
File System: *Content Category*
strategie di allocazione

- Strategia del più adatto:
  - Si cercano «data unit» libere che possano contenere consecutivamente il file



File System: *Content Category*

data unit danneggiate

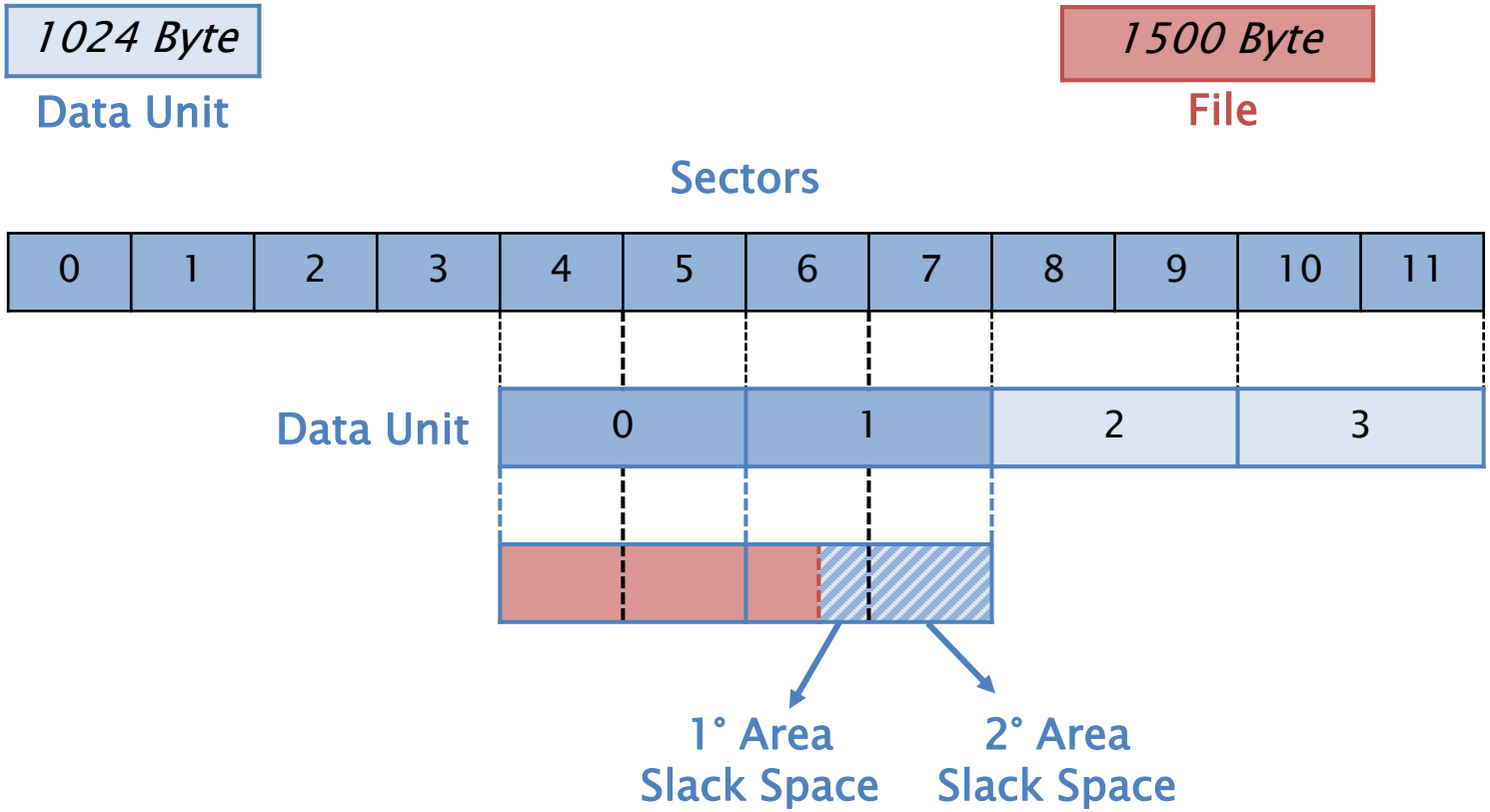


File System: *Content Category*
analisi

1) **Data Unit View**: ricerca di *settori* noti del File System
2) **Logical File System Searching**: ricerca la presenza di un contenuto specifico nei *data unit*
3) **Data Unit Allocation Status**: ricerca nei *data unit* non allocati
4) **Consistency Check:** ricerca di Data Unit non referenziati in «metadata category» *(Orphan Data Unit)*

File System
Slack Space

- Parte non usata di una Data Unit allocata



File System

Slack Space

1024 Byte

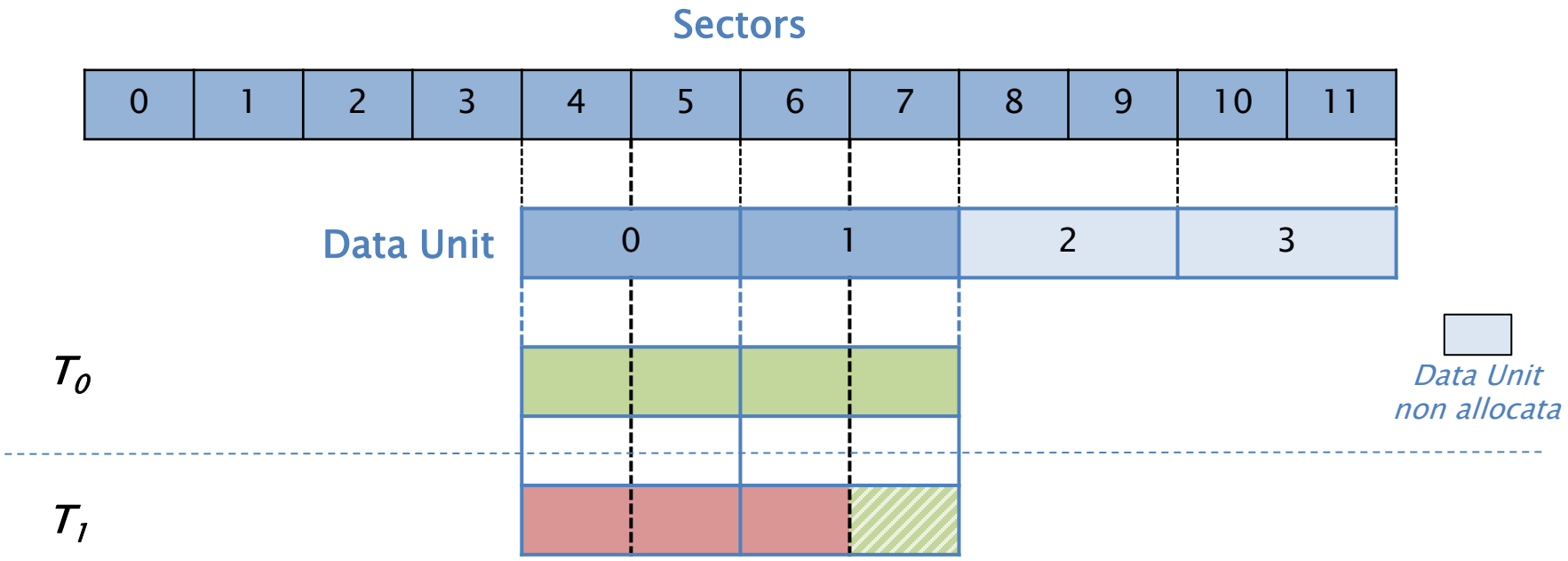
Data Unit

2048 Byte

File 01

1536 Byte

File 02



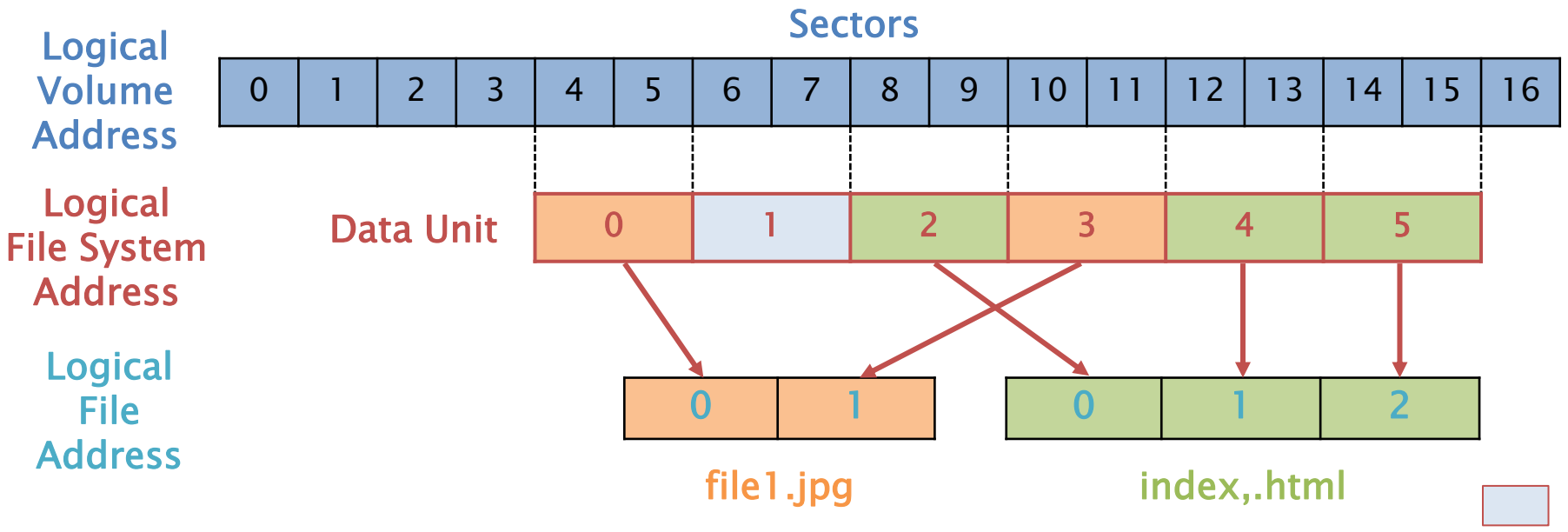
File System:
Metadata Category

- Descrivono i file presenti in «content category»:
  - Informazioni temporali: *data di creazione/accesso/modifica*
  - Indirizzo delle Data Unit allocate per il File

- Analisi:
  - Ricerca di maggiori informazioni su di un file
  - Ricerca di file in base agli attributi descritti in questa categoria:
    - *es.: file creati dopo il 01/01/20*

File System: *Metadata Category*
Logical File Address

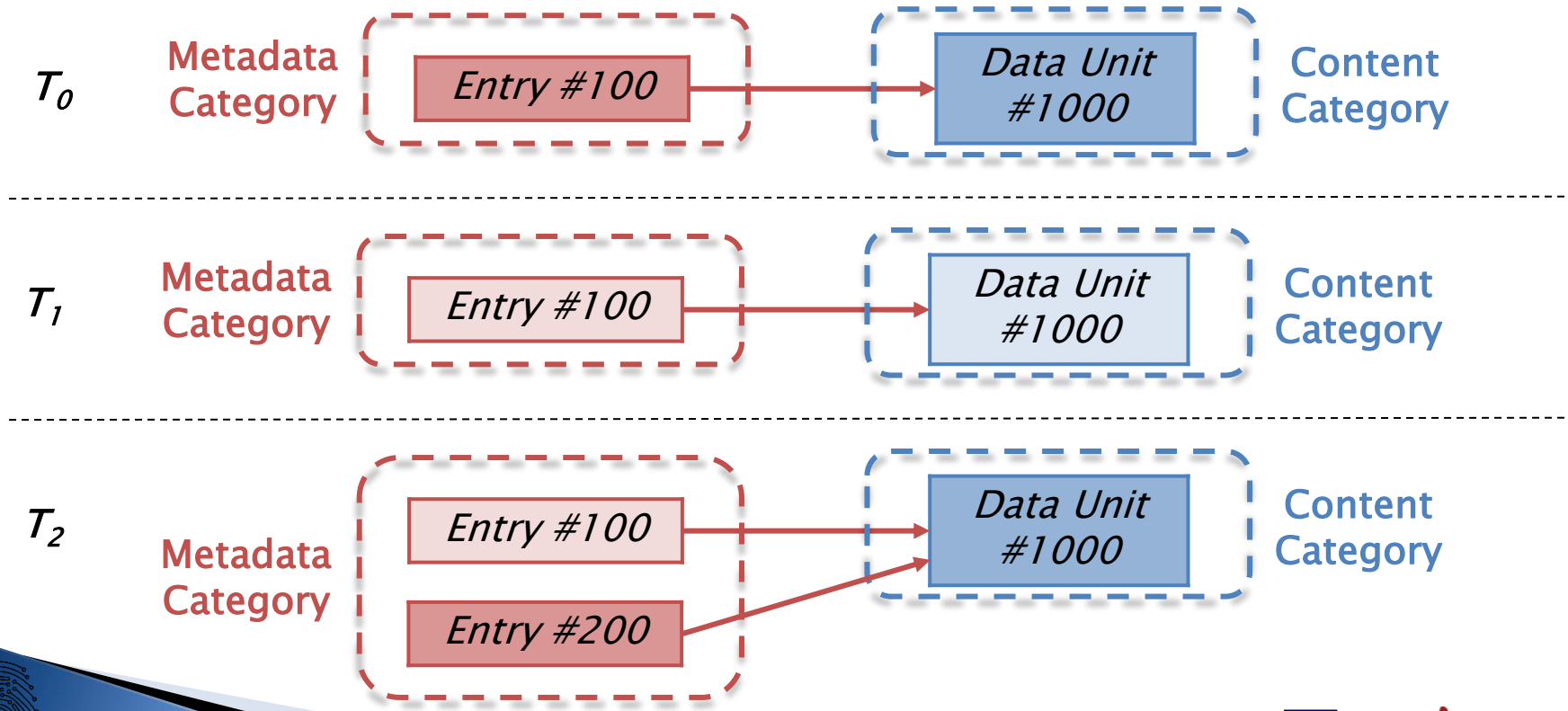
- Indirizzo di parte del file allocata nella data unit:
  - È contenuto nella data unit



File System: *Metadata Category*

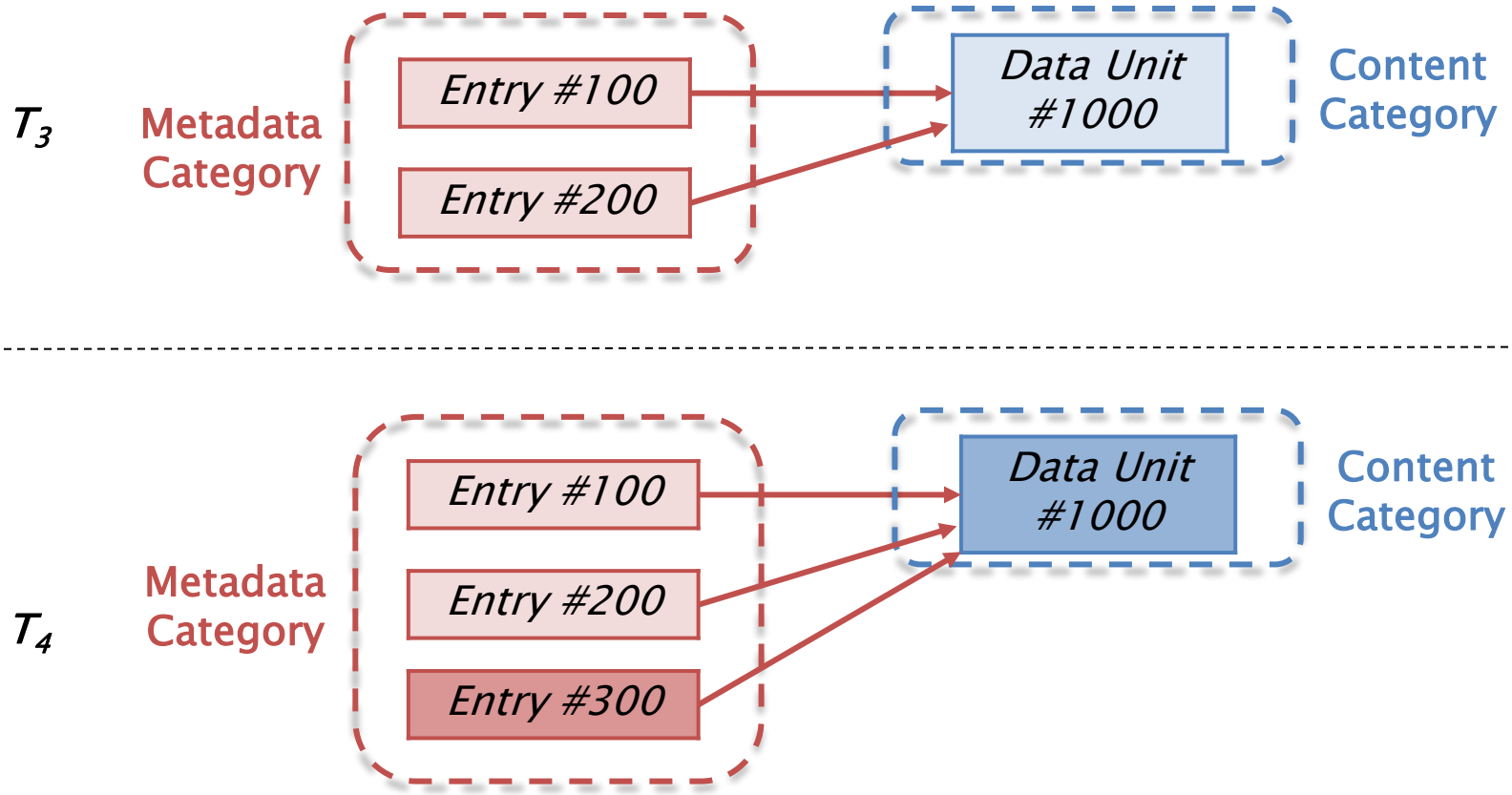
File Recovery

- Recupero dei file cancellati analizzando le entry in «metadata category» con lo stato non allocato.



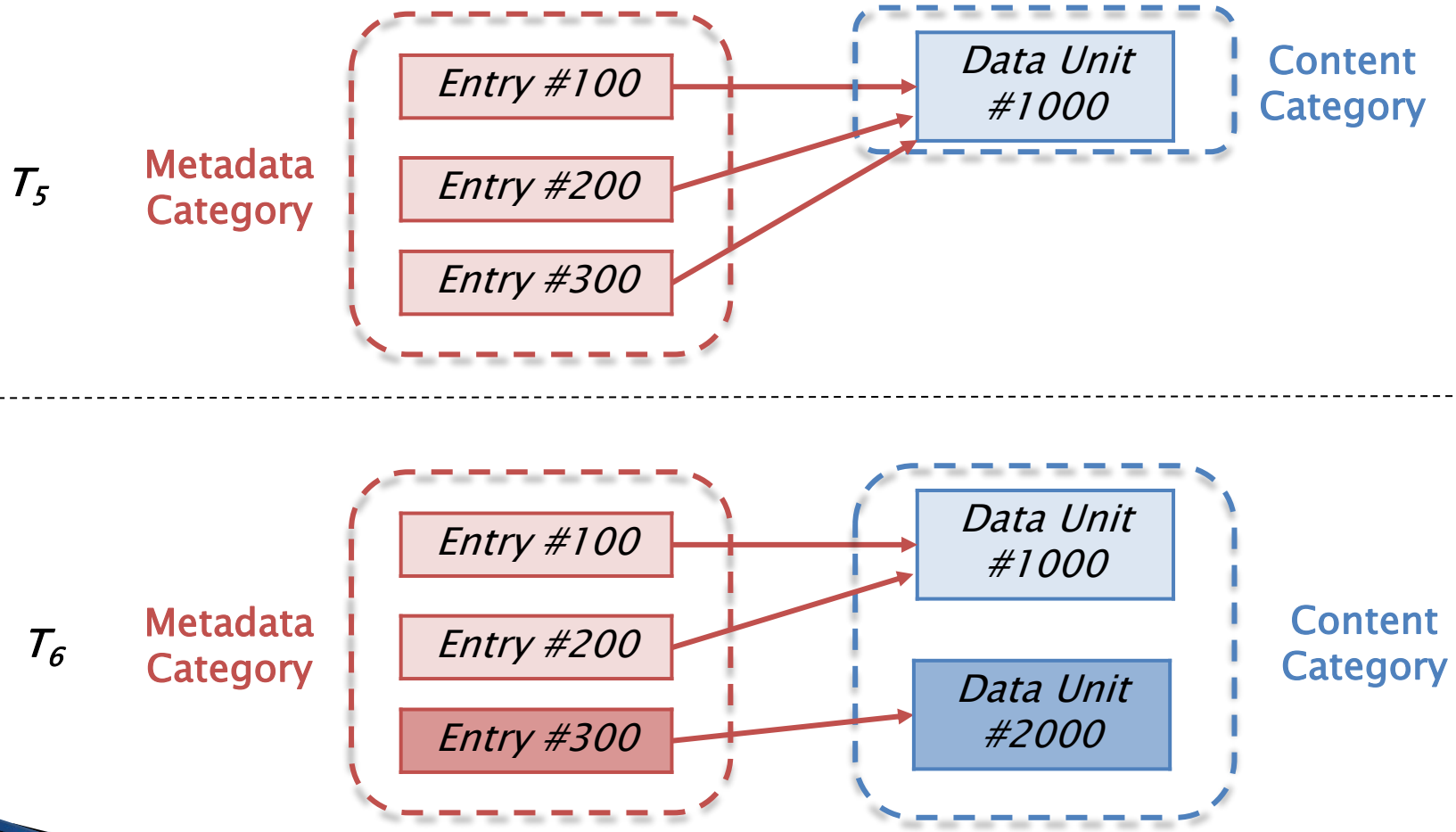
File System: *Metadata Category*

File Recovery



File System: *Metadata Category*

File Recovery



File System
Compressed File

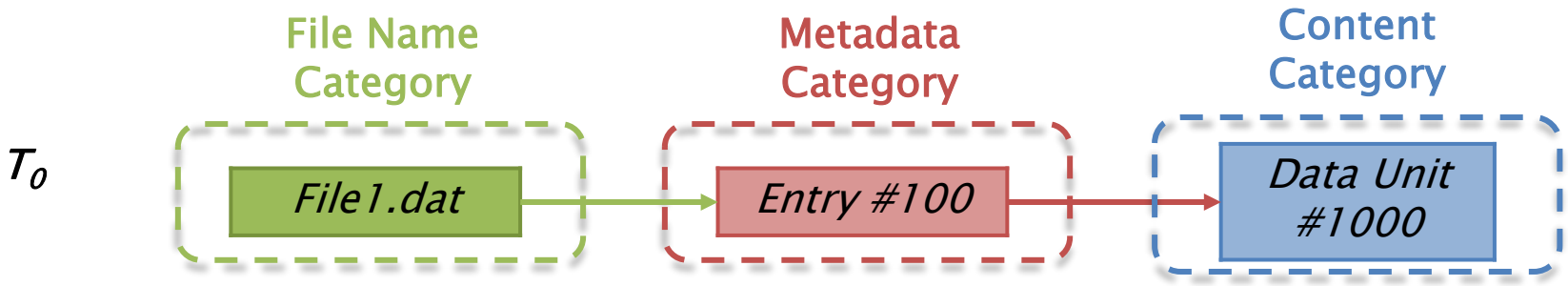
- Memorizzare i dati in un formato compresso occupano meno Data Unit

- Tre livelli di compressione:
  - Compressione dei soli dati all'interno del file *(es.:JPEG, mp3, etc.)*
  - Compressione di tutto il file: creazione di un nuovo file. *(Es.: zip, rar, etc.)*
  - *Compressione eseguita dal File System: invisibile lato applicativo e utente*

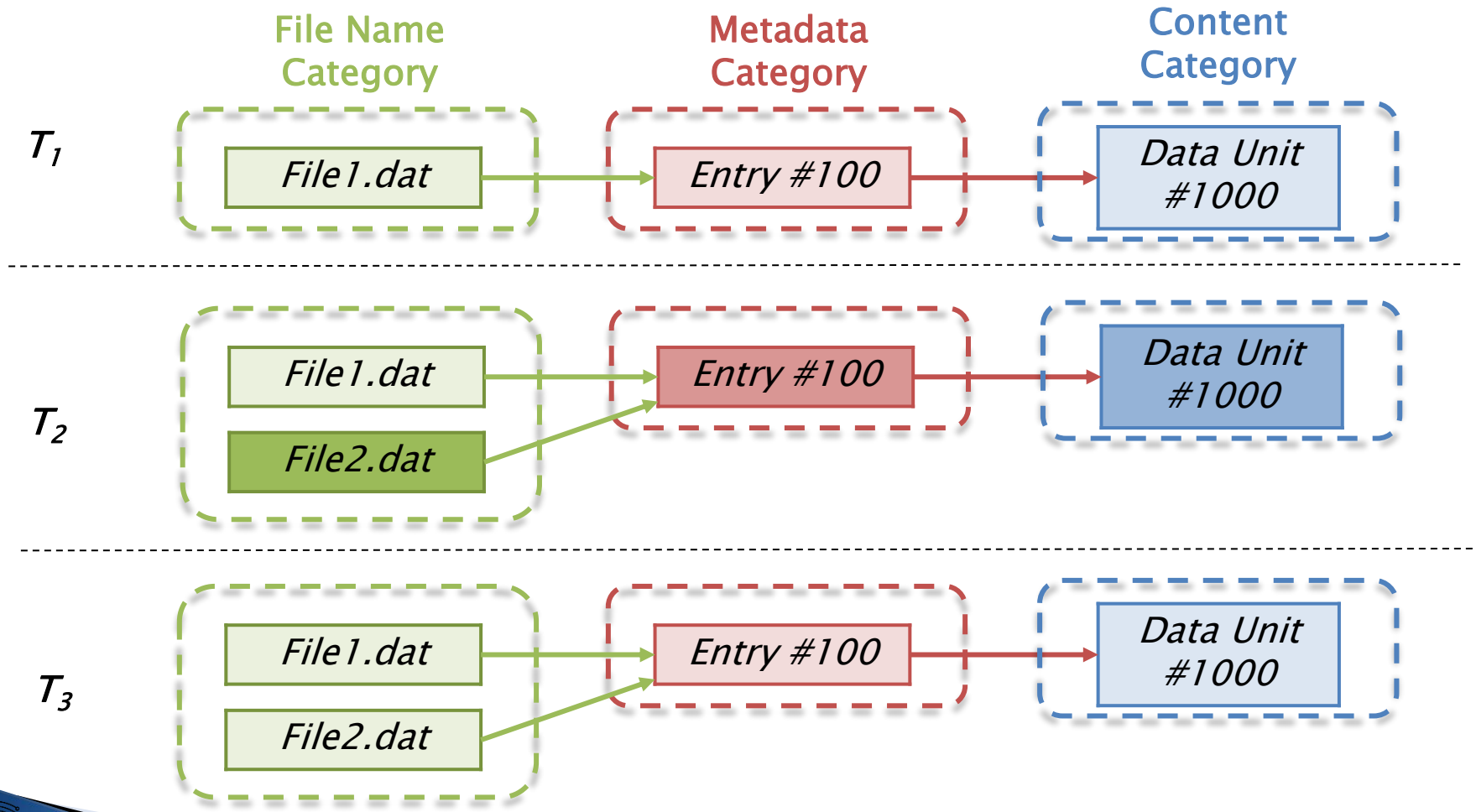
File System:
File Name Category

- Nome assegnato a ciascun file:
  - *Nome del file – Indirizzo della struttura metadato.*

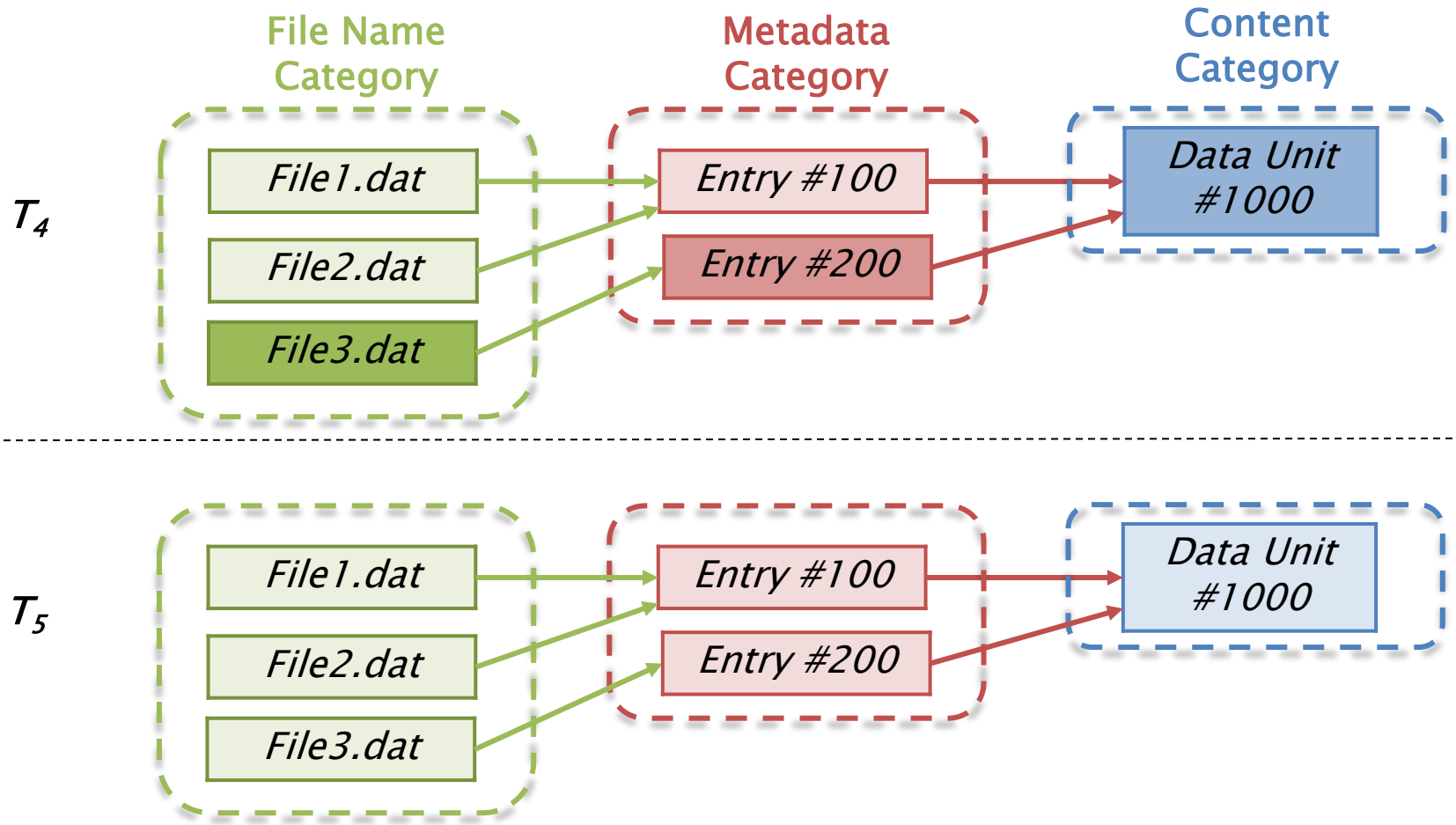
- *File Recovery:*
  - Recupero dei file cancellati ricercando i «File Name» con lo stato non allocato:
    - Analisi della struttura metadati indirizzata



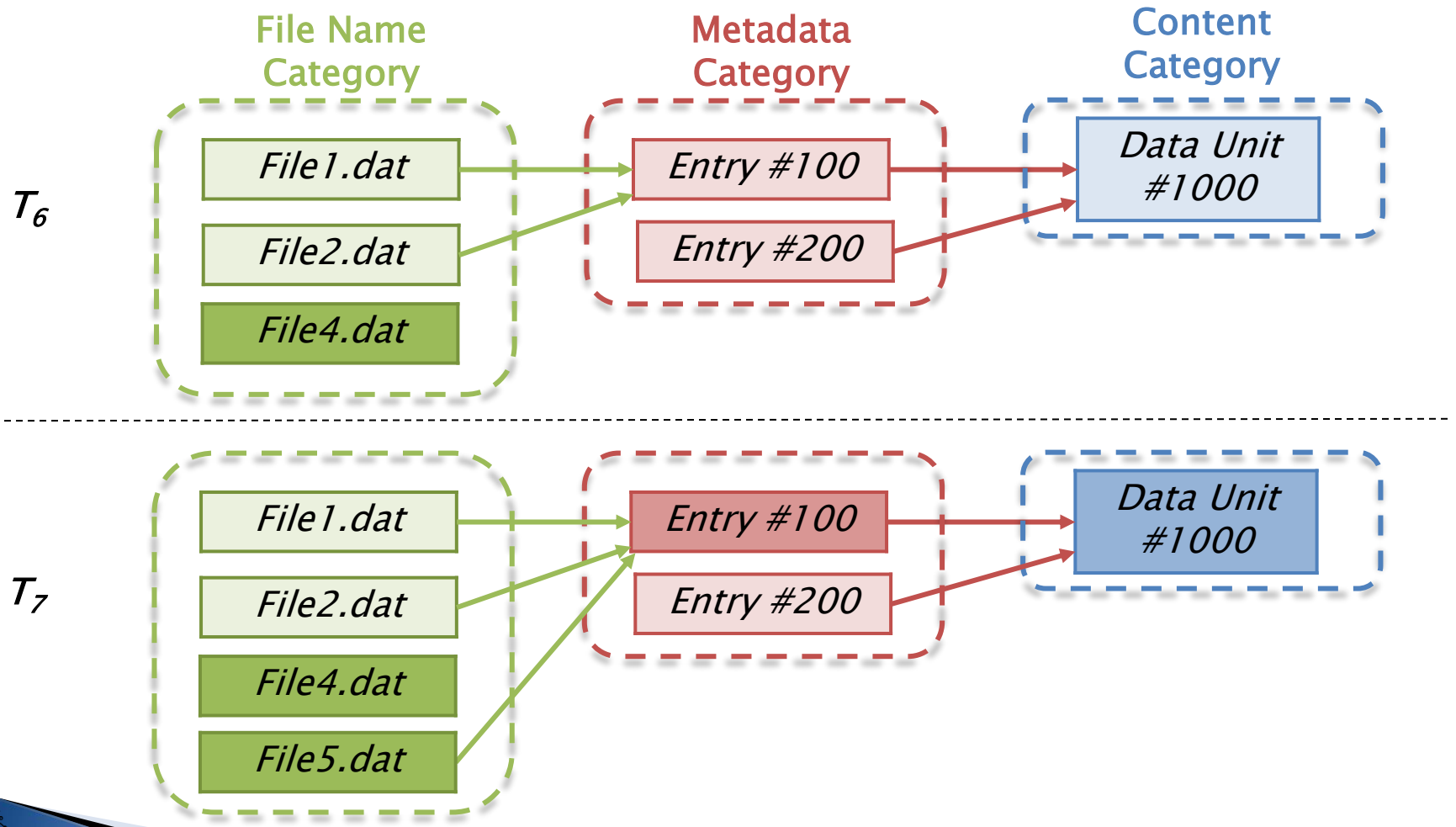
File System: *File Name Category*
File Recovery



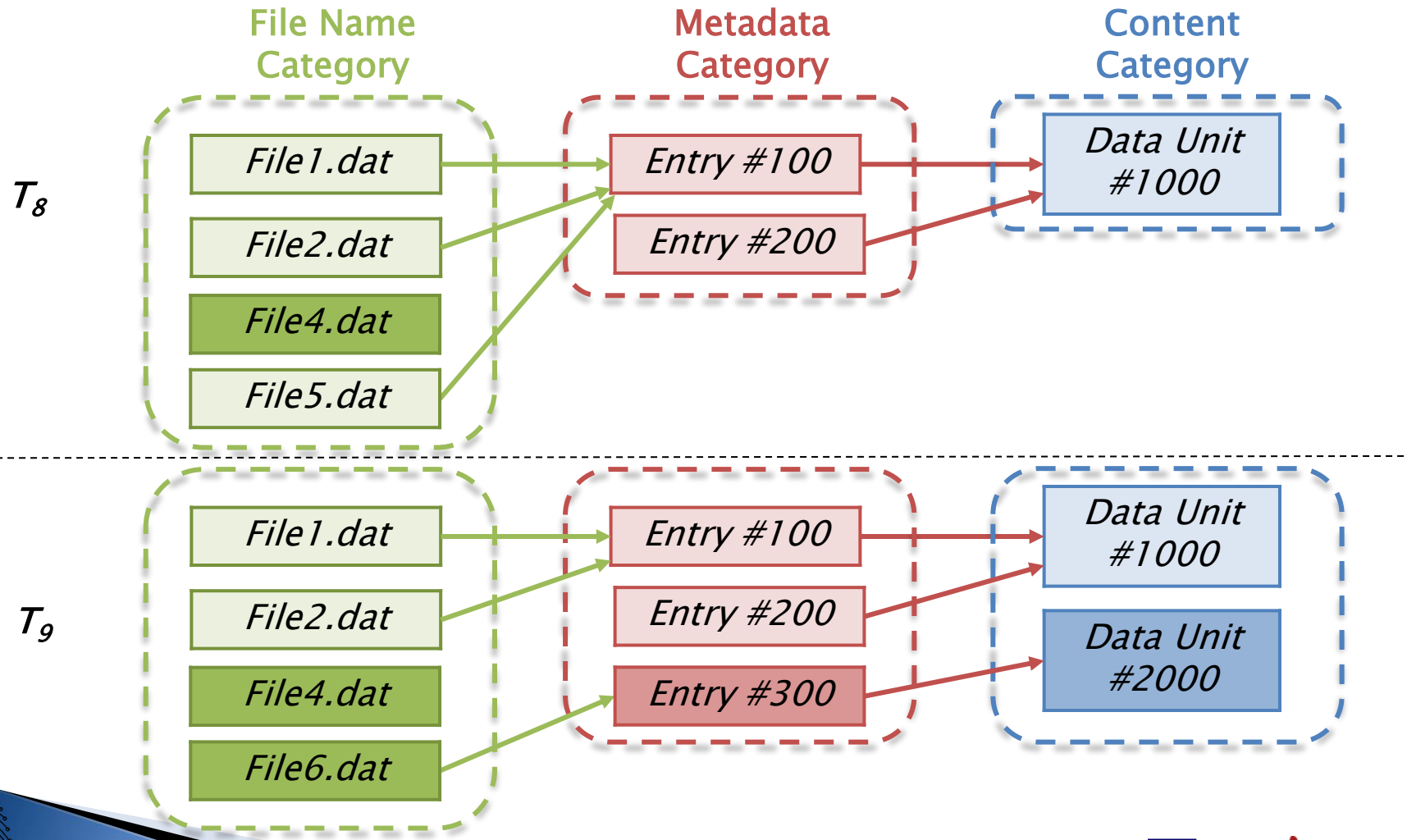
File System: *File Name Category*
File Recovery



File System: *File Name Category*
File Recovery



File System: *File Name Category*
File Recovery



File System:
Application Category

- Dati non essenziali al File System:
  - Sono più efficienti se conservati nel File System.
  - *Es: Spazio occupato, Journaling.*

- *Journaling*
  - Conservazione delle modifiche da effettuare ed effettuate sui metadati:
    - **Evitare l'inconsistenza**:
      - *Completamento delle operazioni di modifica*
      - *Ripristino dei dati a prime delle modifiche (rollback)*
  - Analisi: ricostruire eventi di un incidente recente.

SSRI Lorenzo Laurato s.r.l.

Via Coroglio nr. 57/D (BIC- Città della Scienza)
80124 Napoli

Tel. 081.19804755
Fax 081.19576037

lorenzo.laurato@unina.it
lorenzo.laurato@ssrilab.com

www.docenti.unina.it/lorenzo.laurato
www.computerforensicsunina.forumcommunity.net