# FILE SYSTEM ANALYSIS- PART I

COMP 597 – Computer Forensics

# File System Analysis

- What is file system analysis?

# File System Analysis

- What is a file system?

# File System Abstraction Model

- Disk
- Partition/volume
- Data unit

# File System - Organization

- File system
- Content
- Metadata
- File name
- Application data

# File System - Organization

Example:

- Search for files with “.jpg" extension
- Search for files that contains date in them
- Restore deleted files
- Search for files that were created by a specific user

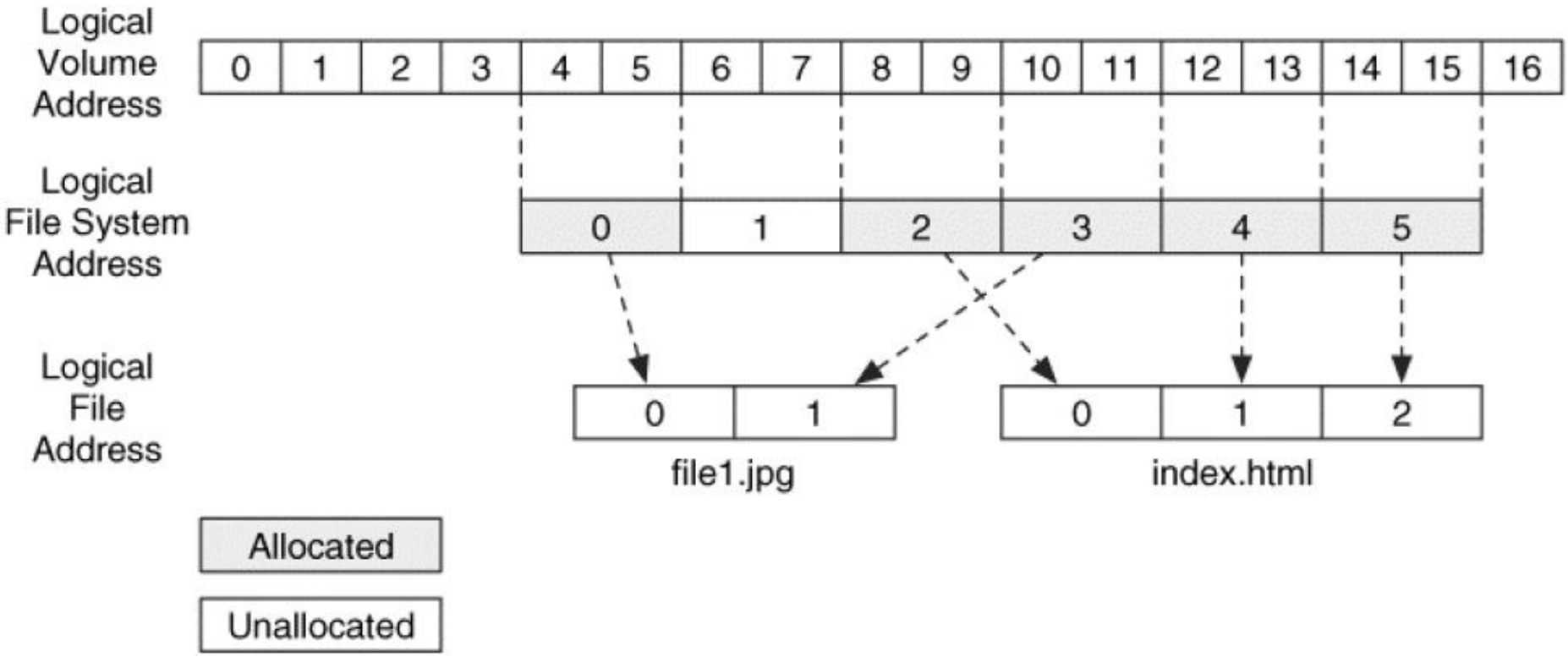
# Content Data

- File and directory data
- Organized into equal sized blocks
- Require tools to inspect its contents

# Addressing Scheme

- Logical volume addresses
- Logical file system addresses
- Logical file addresses

# Addressing Scheme




From: File System Forensic Analysis, 2nd edition, Brian Carrier

# Allocation Strategy

- What is a fragmented file?

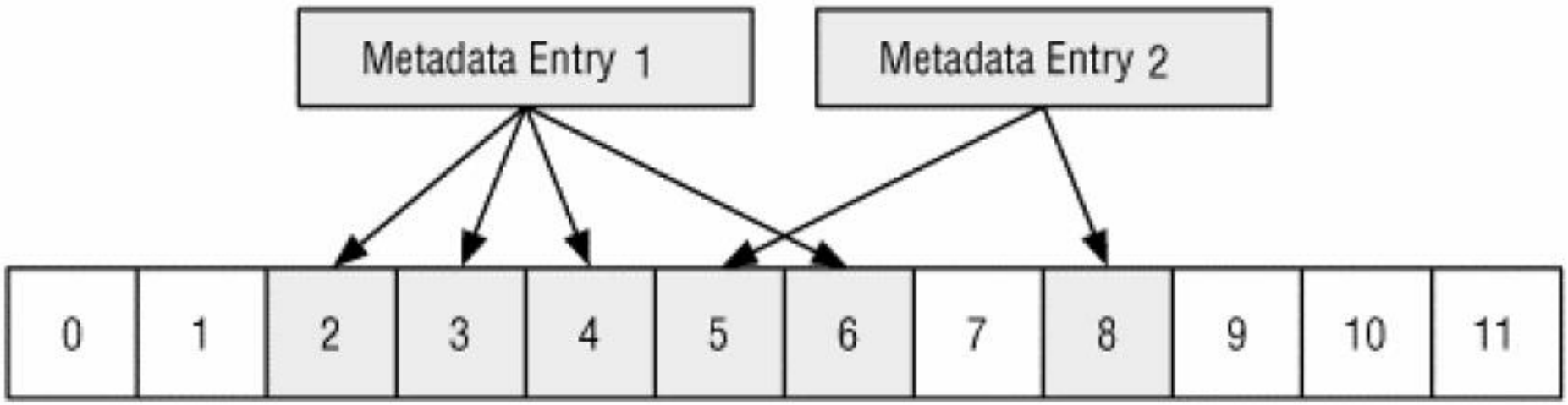
# Allocation Strategy

- First available
- Next available
- Best fit

# Content Analysis

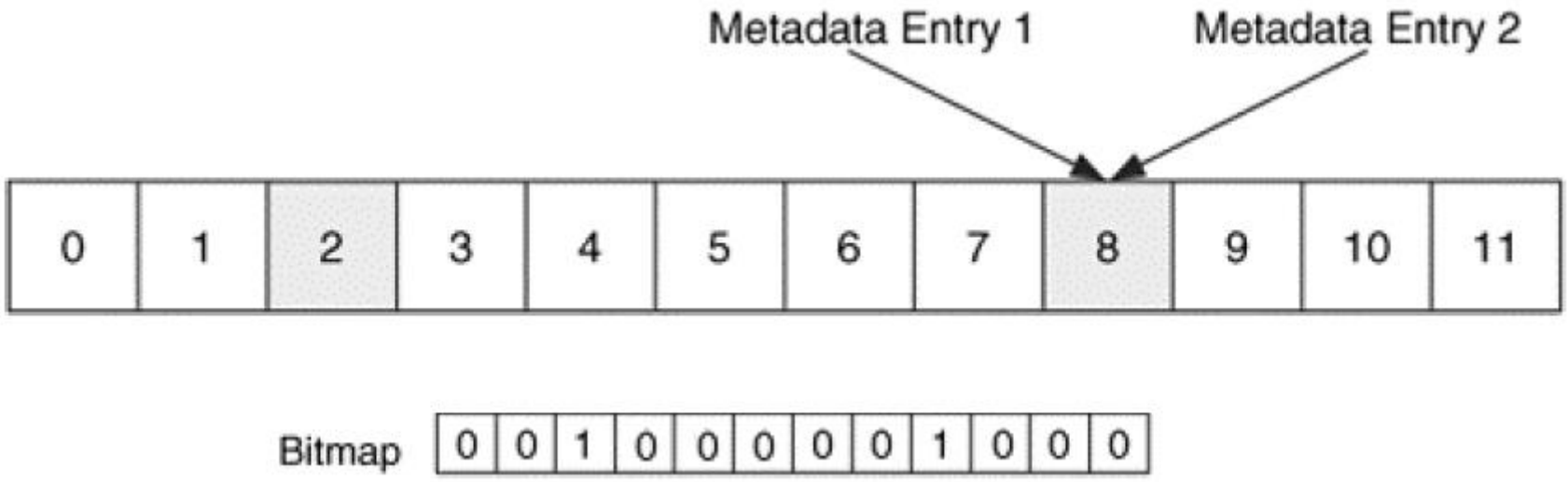
- Block analysis
- Physical search
- Logical file search
- Allocation status
- Consistency checks

# Content Analysis - Example




**From: File System Forensic Analysis, 2nd edition, Brian Carrier**

# Consistency Checks




**From: File System Forensic Analysis, 2nd edition, Brian Carrier**

# Metadata Analysis

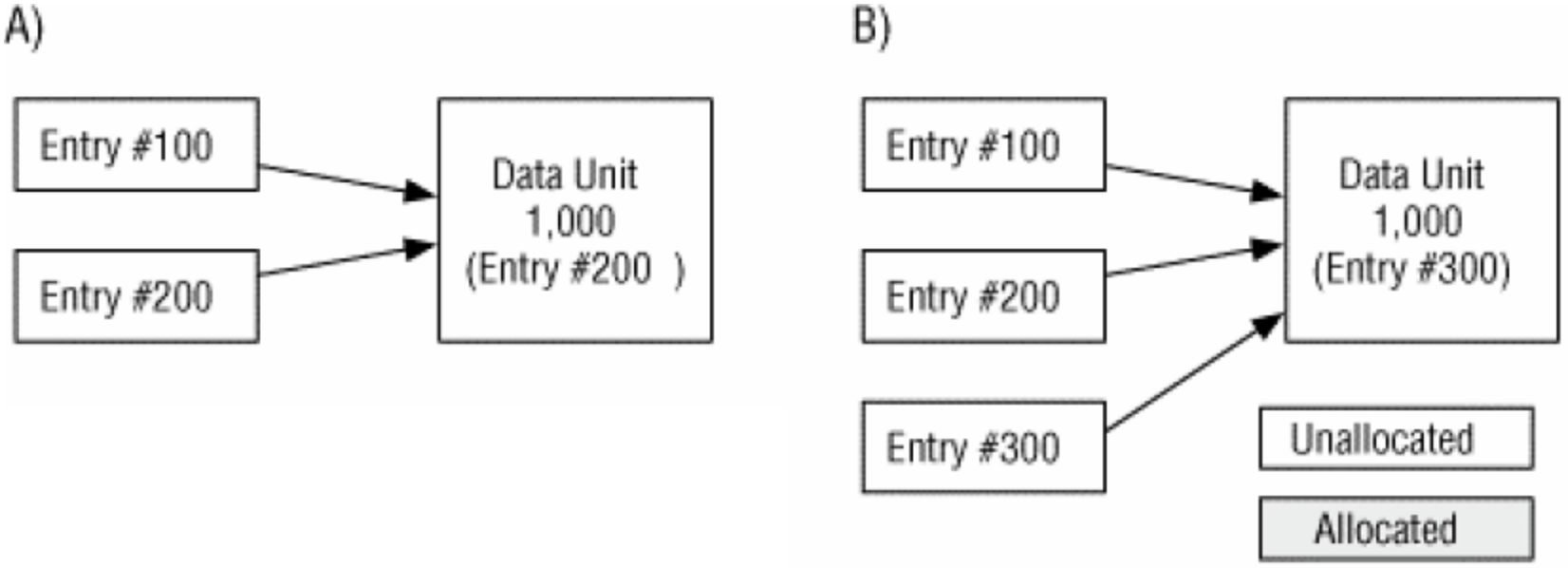
- Metadata lookup
- Slack space analysis
- Deleted file Recovery

# Slack Space

1. between the end of the file and the end of the sector where the file ends

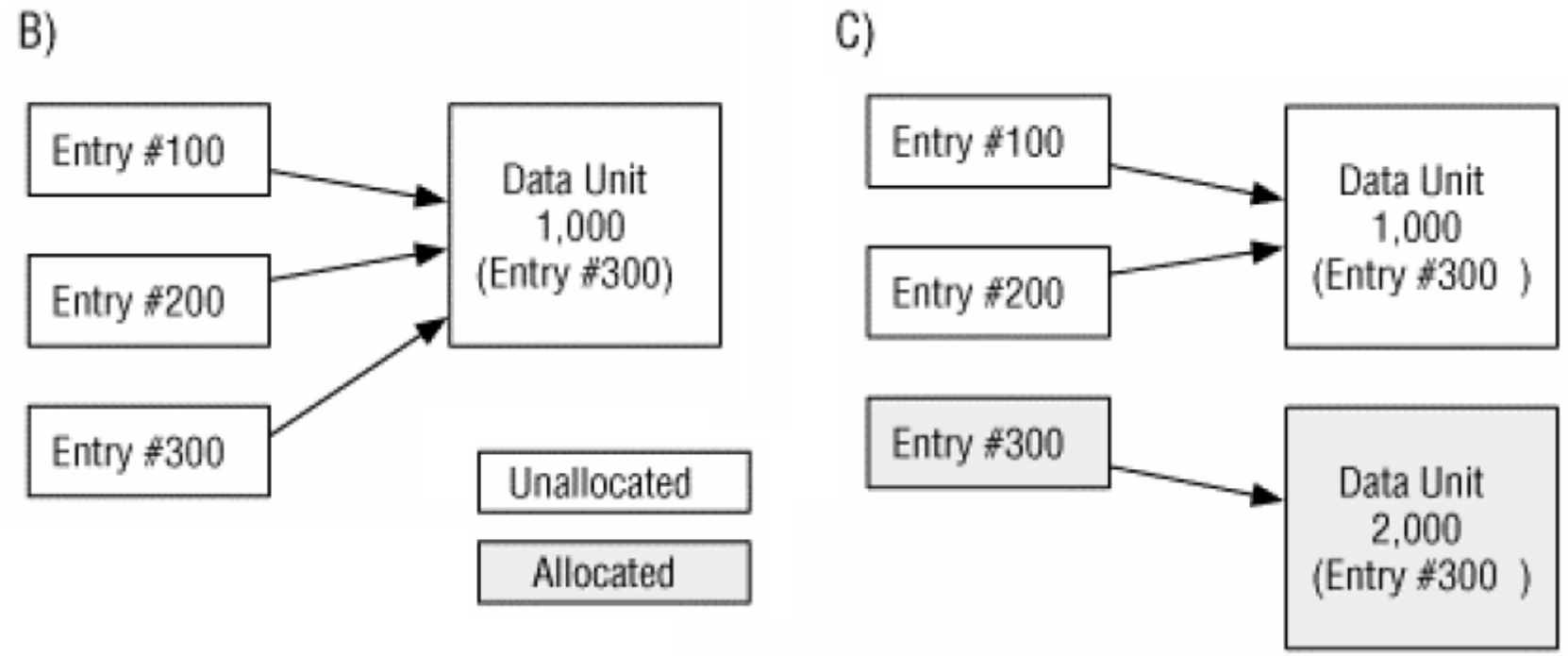
2. in the sectors that contain no file content

# Metadata Analysis – Exercise 1




**From: File System Forensic Analysis, 2nd edition, Brian Carrier**

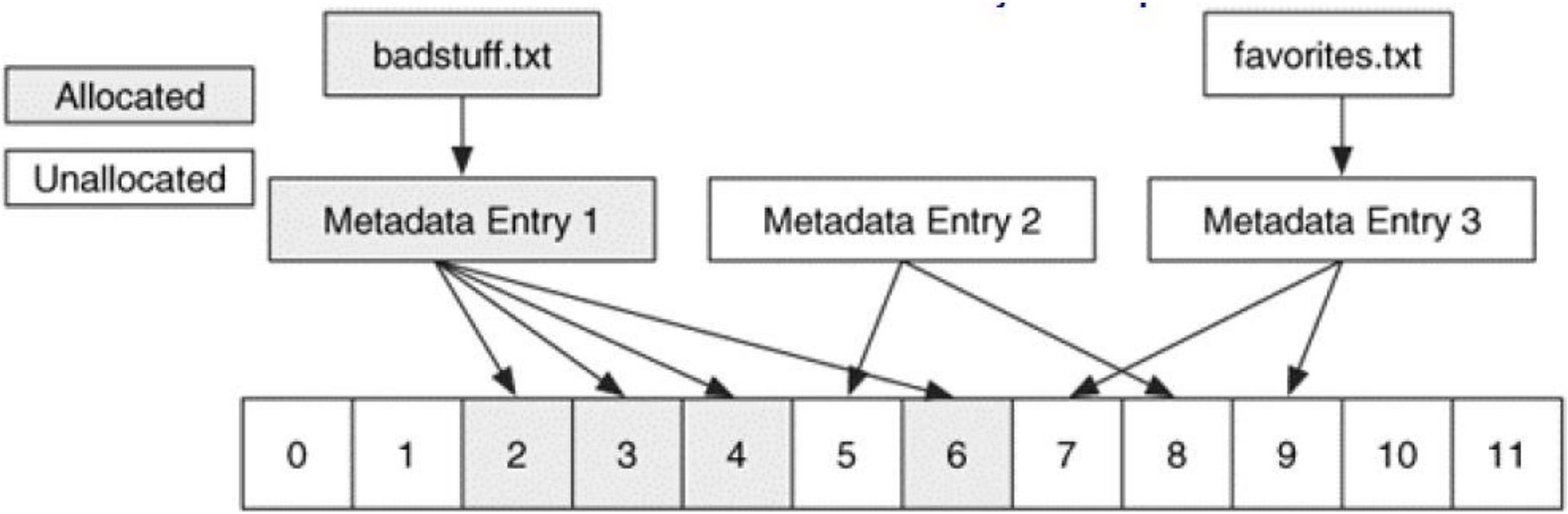
# Metadata Analysis – Exercise 2



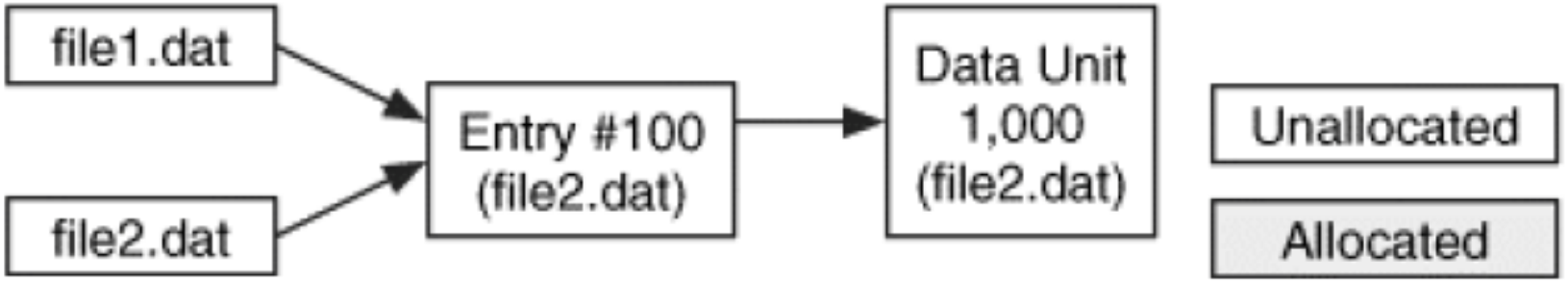

From: File System Forensic Analysis, 2nd edition, Brian Carrier

# File Name Analysis

- name-based file recovery



# File Name Analysis




**From: File System Forensic Analysis, 2nd edition, Brian Carrier**

# File Name Analysis

- Listing of file/directory names
- Searching for file names

# File System Analysis - TSK

- fsstat
- fls
- blkstat, blkcat
- blkls
- ifind
- istat
- mactime

# File System

- Is it enough to understand how a specific file system works?

# References


1. File System Forensic Analysis, 2nd edition, Brian Carrier, 2005.

2. Digital Forensics with Open Source Tools, by Cory Altheide, Harlan Carvey, 2011.