SQLite Recovery

Deok9

DDeok9@gmail.com

Contents of Table

Introduction

SQLite Recovery

- **SQLite** □□□ □□
  - □□□ □□□ □□□□□ □□ □□
    - ✓ □□□ □□□□ □□□□ □□□□, **Strings** □□ □□□□ □□ □□□□ □ □ □□
    - ✓ □□□ □□□□ □□□ □□ □ □□□□ □□□□□ □ □□□
  - **SQLite Viewer**□ □ □ □□□ □□□□ □□
    - ✓ **SQLite Viewer**□ □□□ □ □□□ □□□ □□□□ **Cell**□ □□□□□ □□

Case

Target

- □□□ □□□□□ □□ □□

App	Data Type	Location(WinXP)
Safari	Cache	%USERPROFILE%\Local Settings\Application Data\Apple Computer\Safari\Cache.db
I-Phone	Mobile Comm	%USERPROFILE%\Local Settings\Application Data\Apple Computer\MobileSync\Backup\ <Random>\manifest
Firefox	History Cookie	%USERPROFILE%\Local Settings\Application Data\Mozilla\Firefox\Profiles\<Random>\ places.SQLite or cookies.SQLite
Chrome	Cache History Cookie	%USERPROFILE%\Local Settings\Application Data\Google\Chrome\UserData\Default\ Cache or History or Cookies

Zero Fill

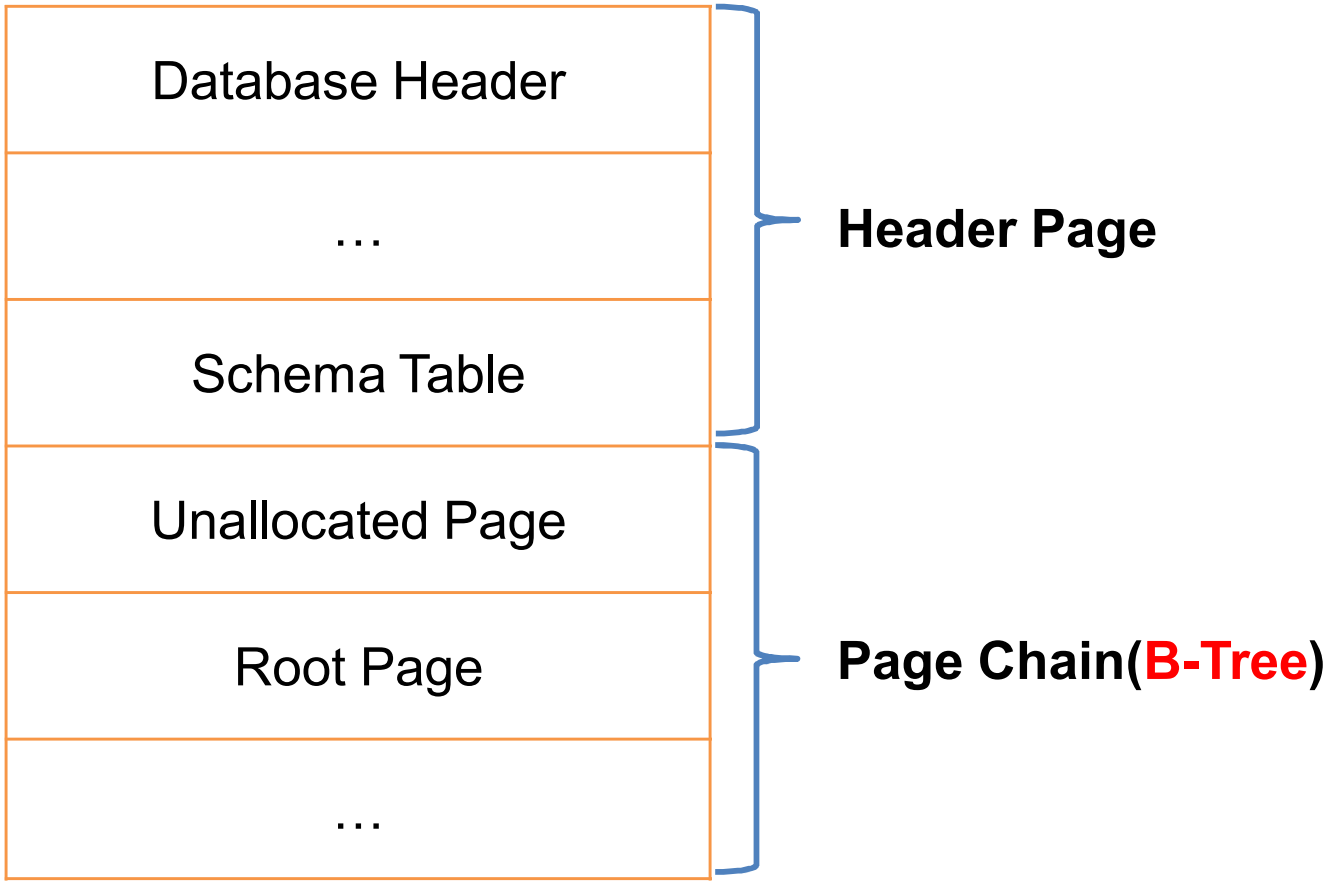
If delete(group_msg):
group_msg = unallocated space

Zero Fill

How

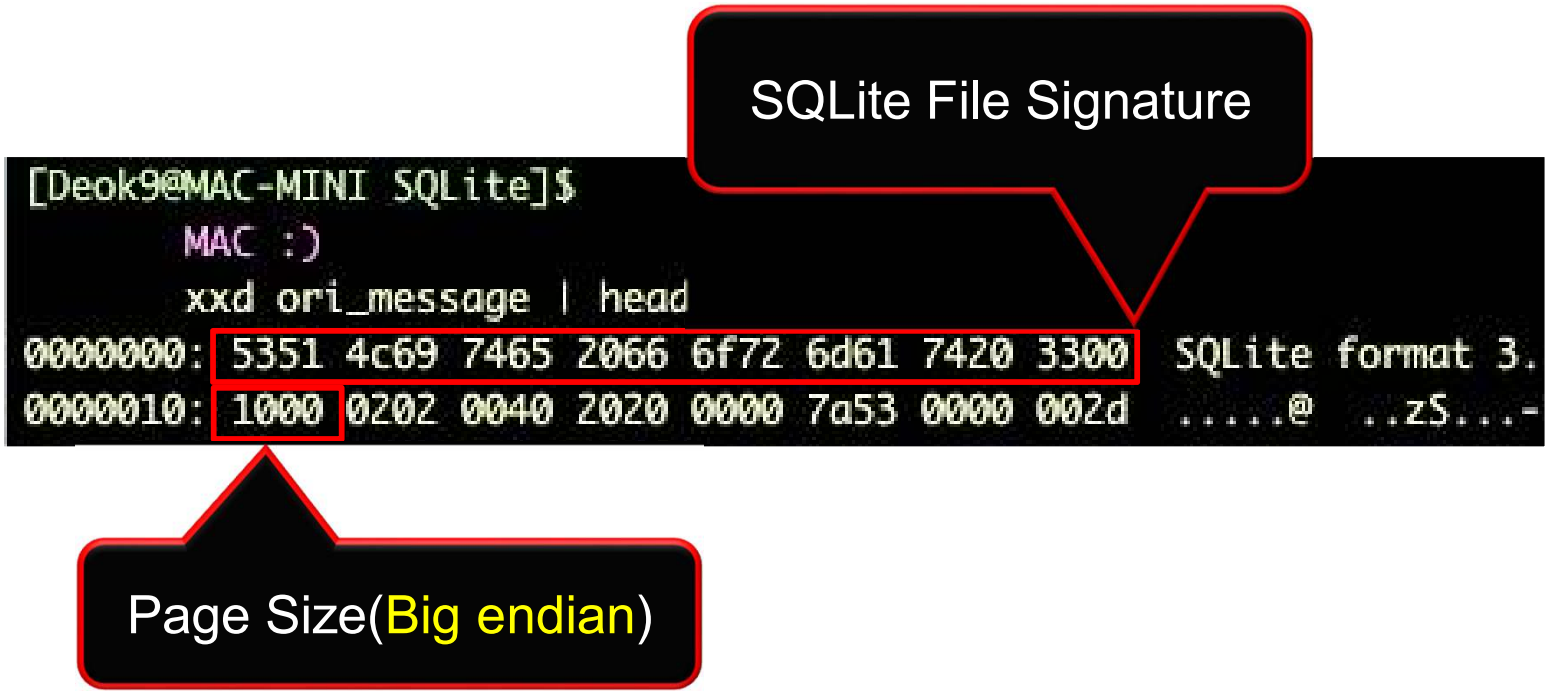
SQLite □□(□□)

- **Header Page + Page Chain**



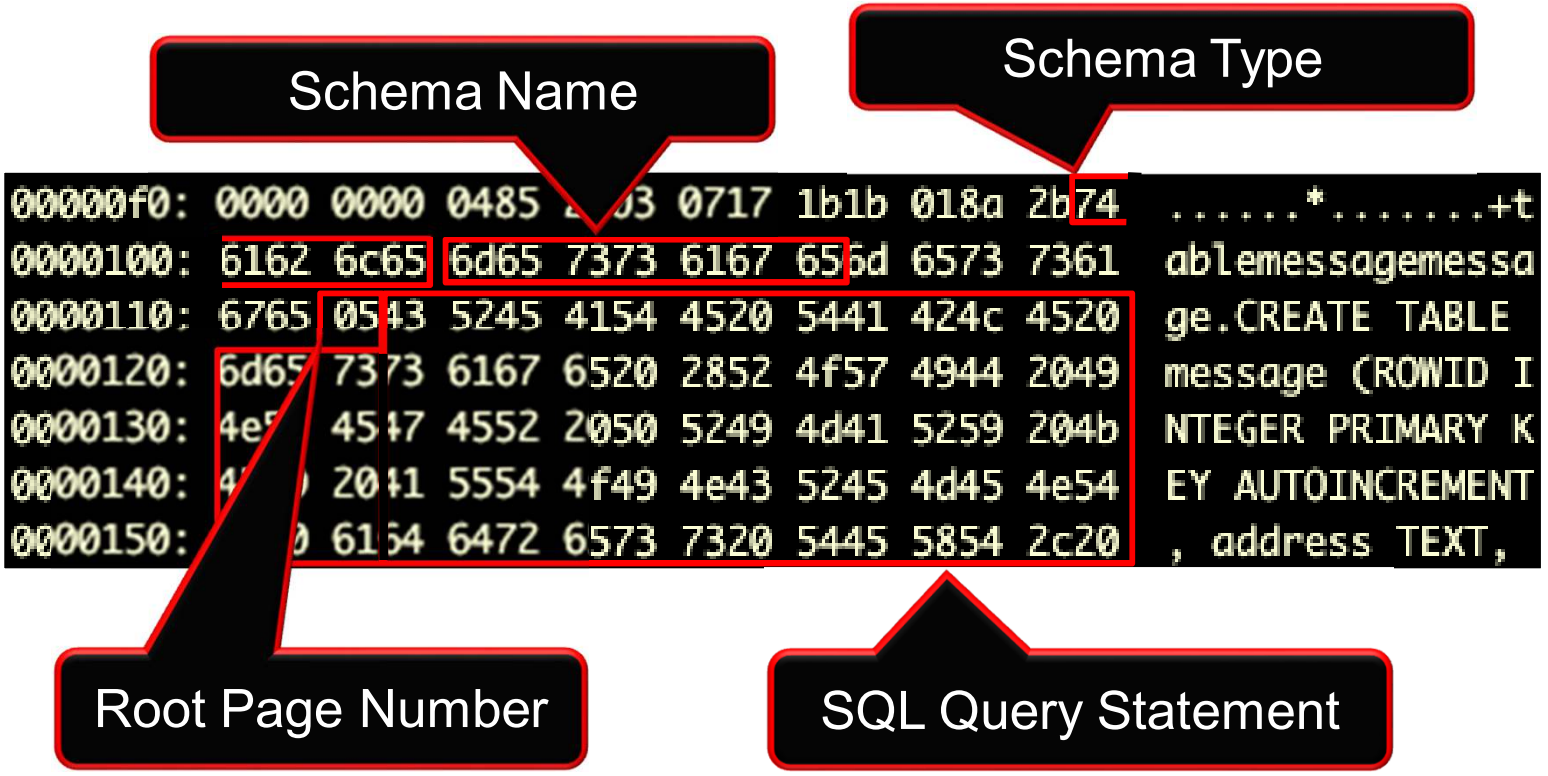
□□ □□□ □□□ □□□□

- **Database Header**



□□□□ □□ □□□ □□□ □□□□

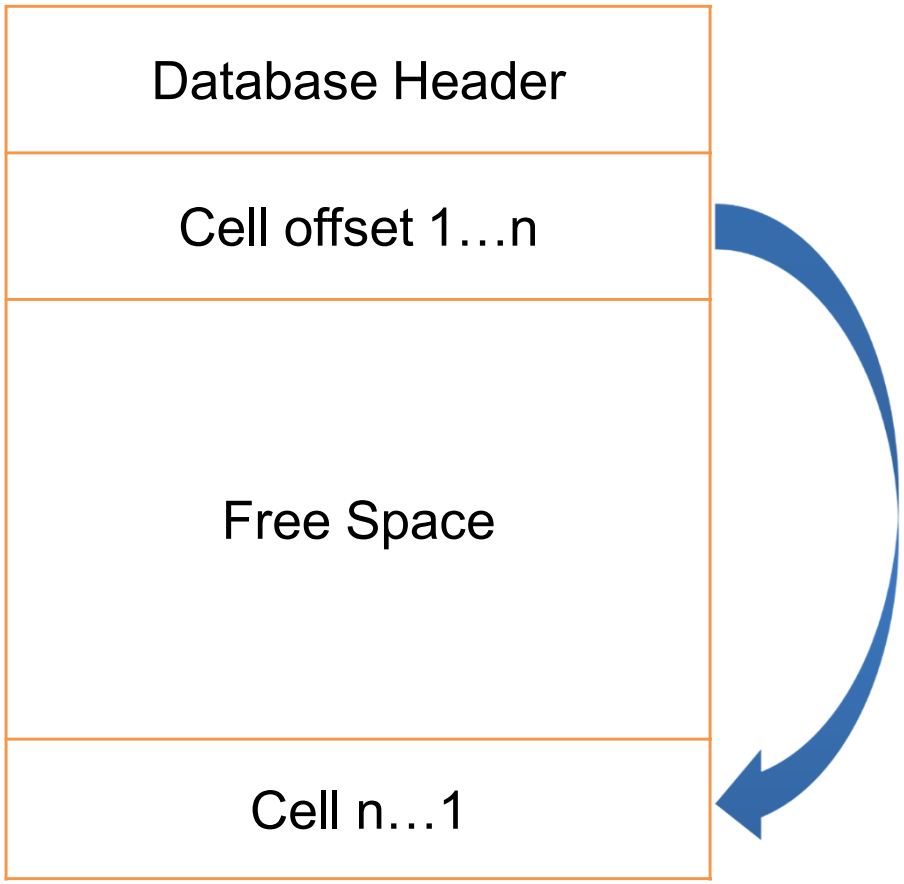
- **Database Schema Table**



How

□□□ □□(□□)

- **Page Header + Cell offset + Free Space + Cell**



□□ □□□□ □□□□ □□□□ Leaf □□□

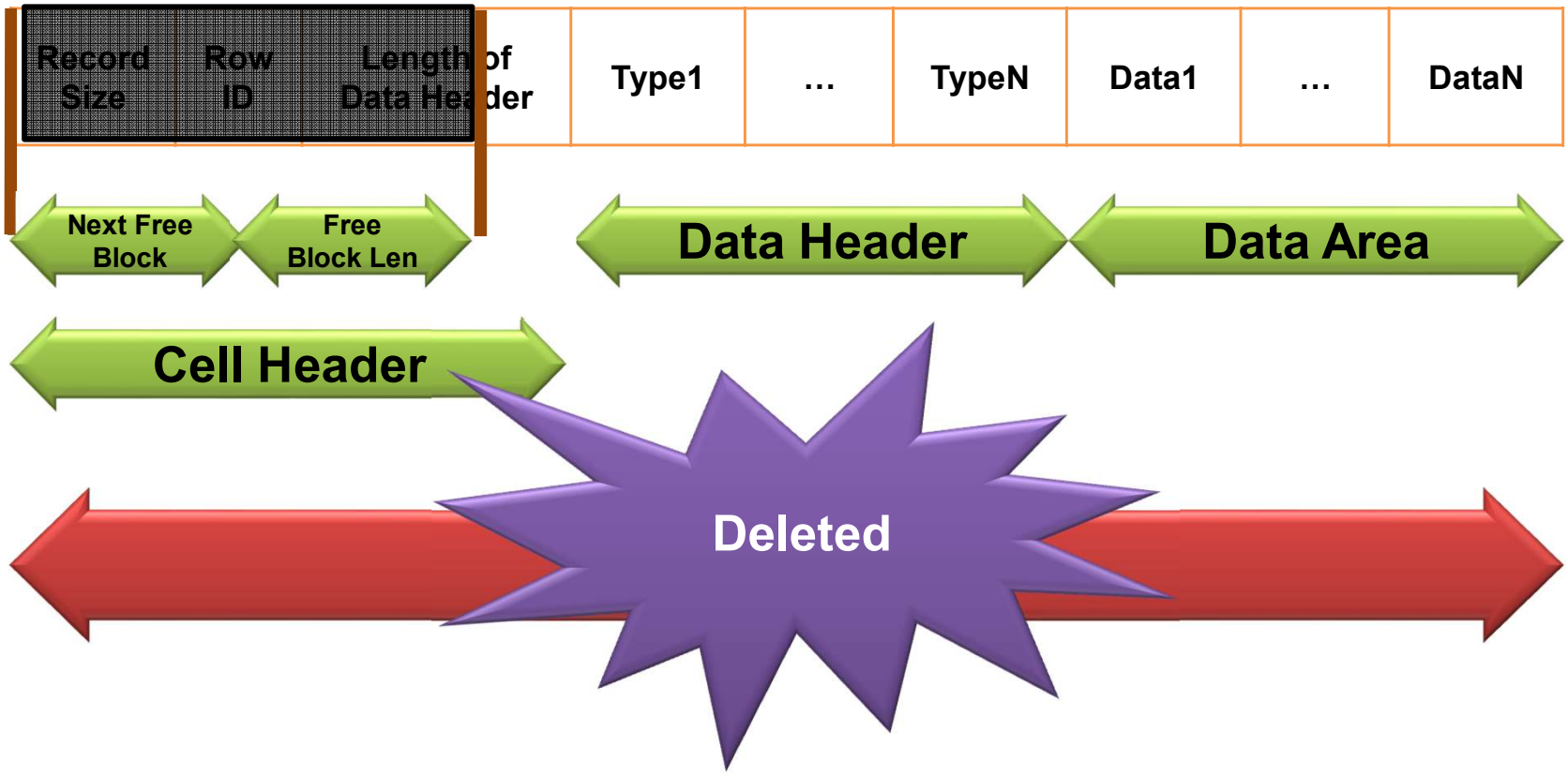
- **Leaf** □□□ □□

Offset	Contents
0	Page Flag : 0x0D
1-2	First Unallocated Block Offset
3-4	Cell Count
5-6	First Cell Offset
7	Over 3Byte Unallocated Block Count

- □□□ □ □□□□ □□ □□□ □□

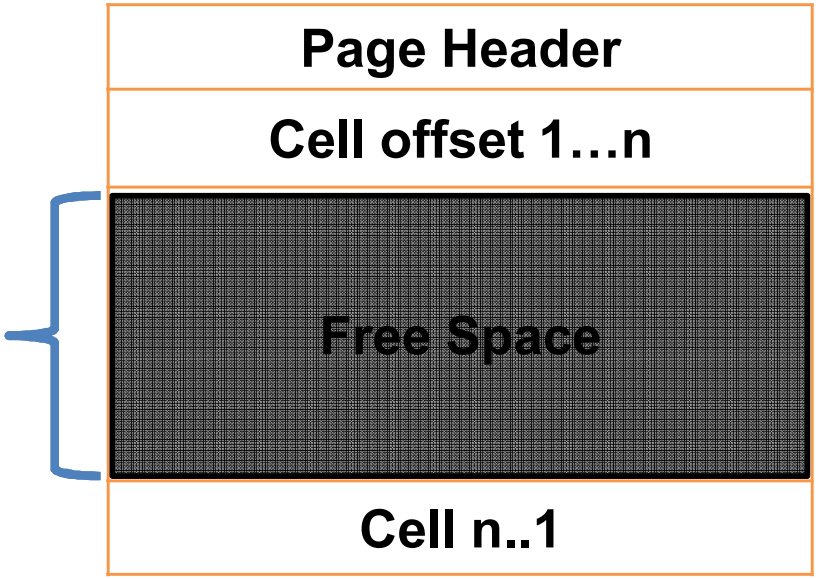
□□ Leaf □□□ □□ Cell□ □□ □□?

- Leaf Cell □□(□□)



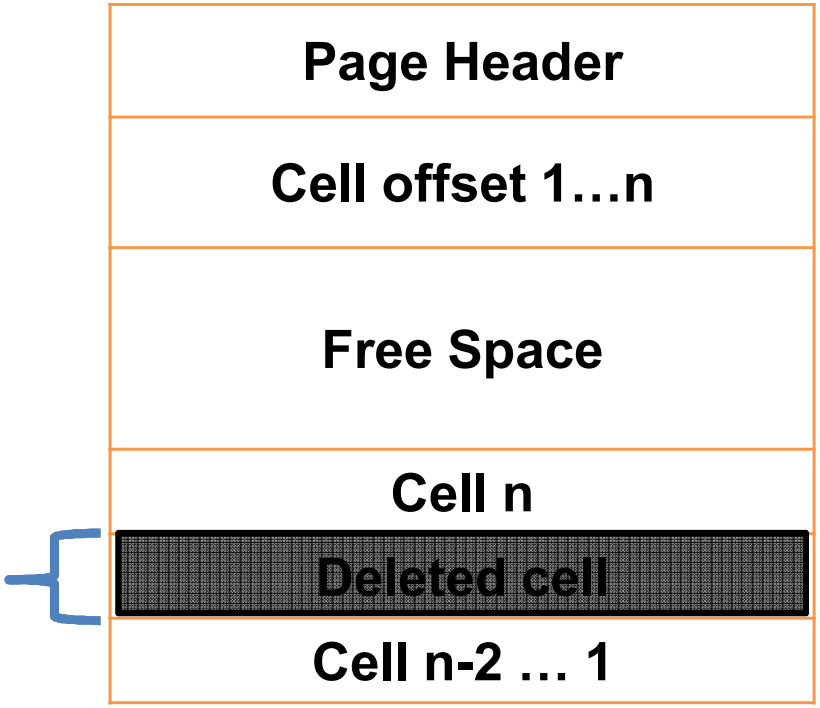
□□ Free Space □□ □□

1. **Leaf □□□□ □□□.**
2. **Free Space□ □□□.**
    1. **□□□ □□□ □□□ 5~6□ □□ □□ □ □□ □□ □□ □□**
    2. **□ □□□ □□□ □□□□ 0x0000□ □ □□□ □□**
    3. **□□ □ □□□ n□ □ n □□□ □□□ □□□□ □**



□□□□ Free Block □□

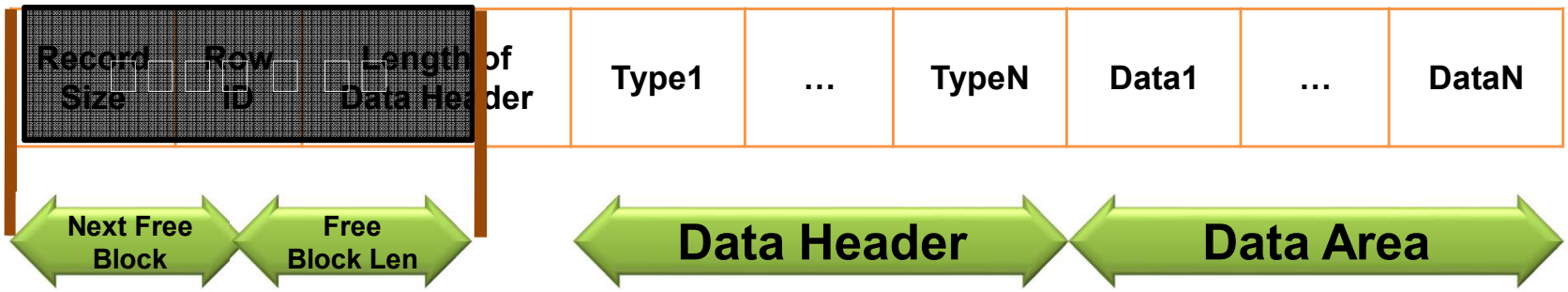
1. **Leaf □□□□ □□□.**
2. **□ □□ Free Block□ □□□.**
    1. **□□□ □□□ □□□ 1~2□ □□ □□ □ □□ □ □□ □□□□ □□**
    2. **□□□ Leaf Cell □□□ □□□□□**



How

□□□ □□□ □1

- □□□□ □ □□
  - Legnth of Record
  - Row ID
  - Length of Data Header □□□



□□□ □□□ □2

- □□ □□□ □□□ □□□ □□□□

  - □□□ □□□ □□ □□□ □□□ □□

Value	Data Type	Data Size
0	NULL	0
N (N=1-4)	Signed Integer	N
5	[illegible]	6
6	Signed Integer	8
7	IEEE float	8
8-11	Reserved	
N>12 (N:even)	BLOB	(N-12)/2
N>13 (N:odd)	TEXT	(N-13)/2

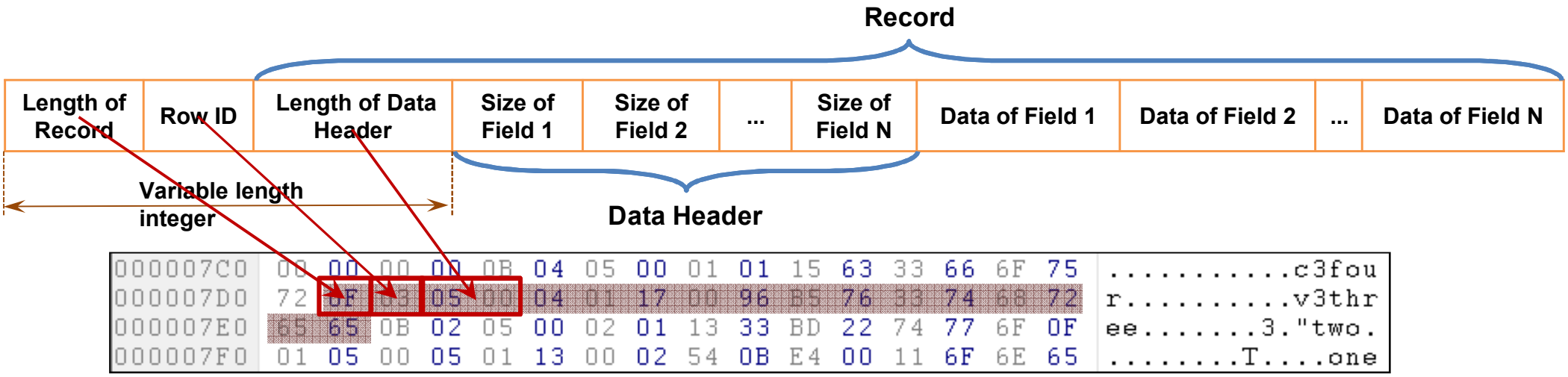
  - □□□ □□ □ □

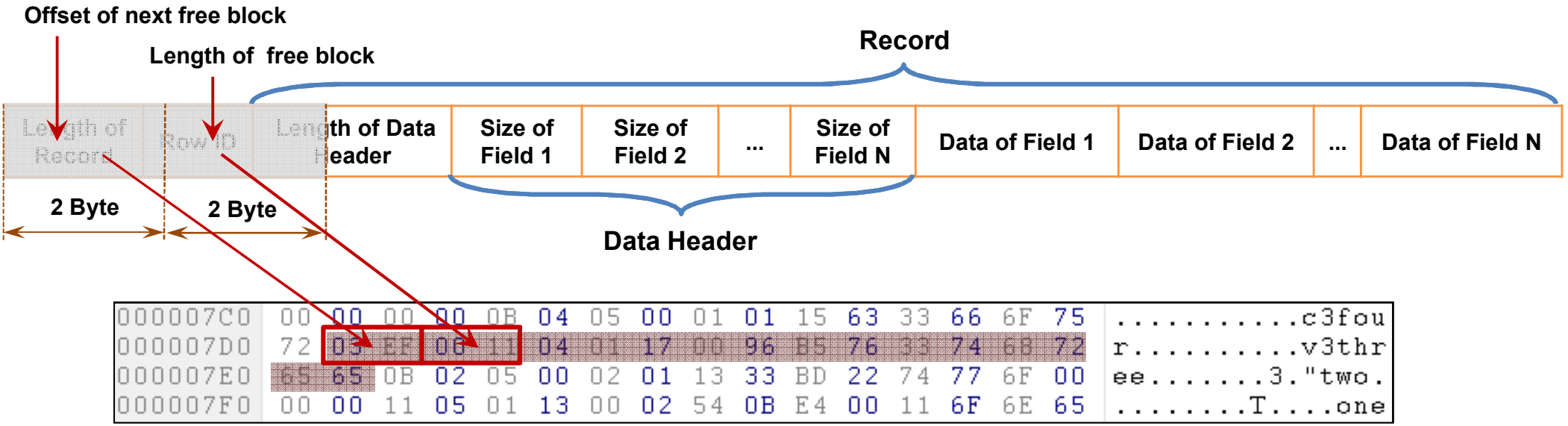
How

□□□ □□□ □3

- **Length of Record□?**
  - □□□ □□□ □□□ □□□ □□ □□□□, □□□□ □ □
- **Row ID□?**
  - □□□ □□ □□□ □□ □□□? □□□ **0xFF –** □□ □□ □□ *** n(□ 200** □□**)□** □□□□

□□□ □□□(□□□ □□□ □□□ □□)


Record
Length of Record
Row ID
Length of Data Header
Size of Field 1
Size of Field 2
...
Size of Field N
Data of Field 1
Data of Field 2
...
Data of Field N
Variable length integer
Data Header
000007C0 00 00 00 00 0B 04 05 00 01 01 15 63 33 66 6F 75 .....c3fou
000007D0 72 0F 03 05 00 04 01 17 00 96 B5 76 33 74 68 72 r.....v3thr
000007E0 65 65 0B 02 05 00 02 01 13 33 BD 22 74 77 6F 0F ee.....3."two.
000007F0 01 05 00 05 01 13 00 02 54 0B E4 00 11 6F 6E 65 ....T....one


Offset of next free block
Length of free block
Record
Length of Record
Row ID
Length of Data Header
Size of Field 1
Size of Field 2
...
Size of Field N
Data of Field 1
Data of Field 2
...
Data of Field N
2 Byte
2 Byte
Data Header
000007C0 00 00 00 00 0B 04 05 00 01 01 15 63 33 66 6F 75 .....c3fou
000007D0 72 03 EF 00 11 04 01 17 00 96 B5 76 33 74 68 72 r.....v3thr
000007E0 65 65 0B 02 05 00 02 01 13 33 BD 22 74 77 6F 00 ee.....3."two.
000007F0 00 00 11 05 01 13 00 02 54 0B E4 00 11 6F 6E 65 ....T....one

Conclusion

Recover Iphone Message

- □□□ □□□ □□□