

# SQLite Recovery

---

*Deok9*

*DDeok9@gmail.com*





**1. Introduction**

**2. Case**

**3. How**

**4. Conclusion**

# Introduction



## SQLite Recovery

- **SQLite** □□□ □□

- □□□ □□□ □□□□□ □□ □□

- ✓ □□□ □□□□ □□□□ □□□□, **Strings** □□ □□□□ □□ □□□□ □ □ □□

- ✓ □□□ □□□□ □□□ □□ □ □□□□ □□□□□ □ □□□

- **SQLite Viewer** □ □ □ □□□ □□□□ □□

- ✓ **SQLite Viewer** □ □□□ □ □□□ □□□ □□□□ **Cell** □ □□□□□ □□

# Case



## Target

- ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

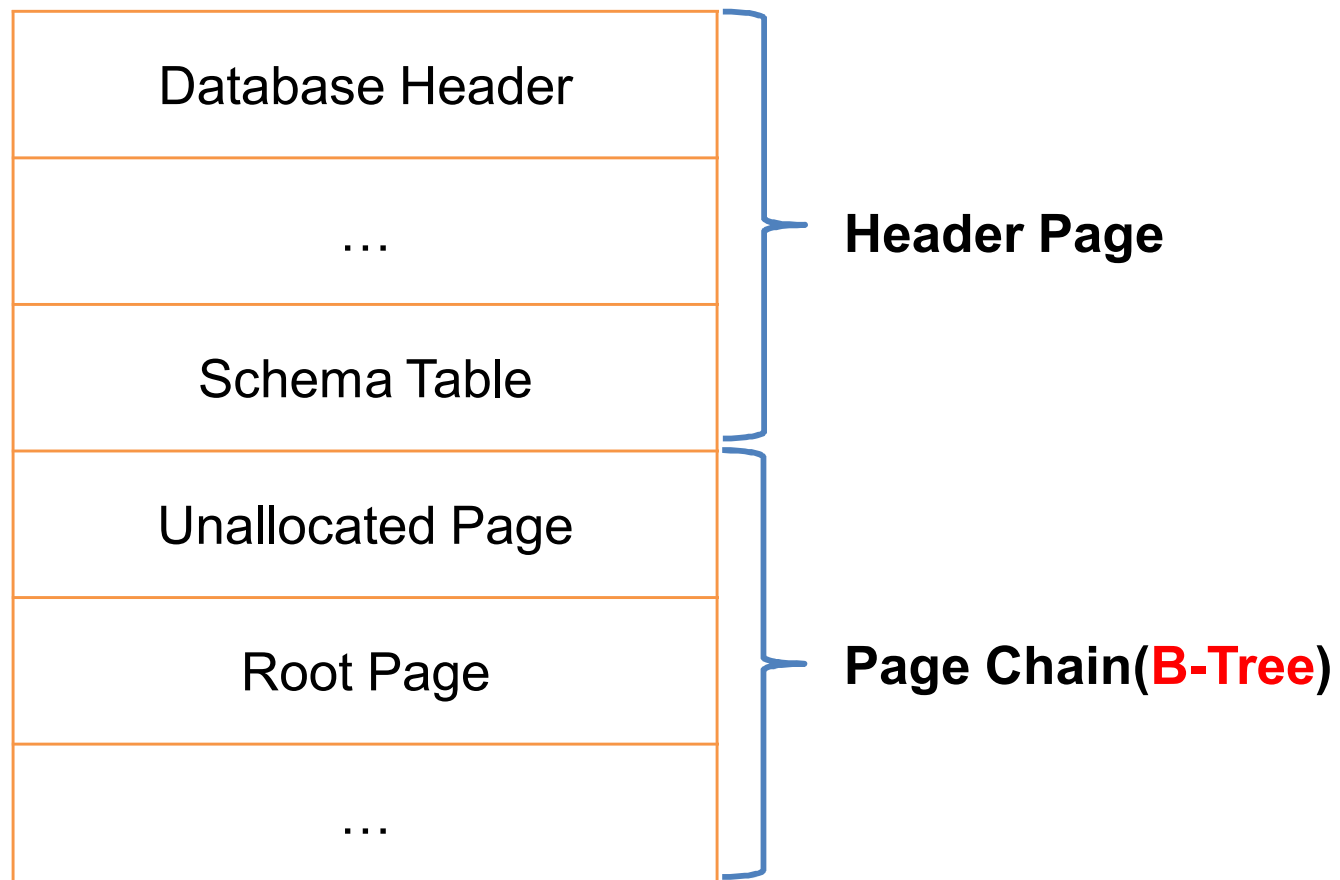
App	Data Type	Location(WinXP)
Safari	Cache	%USERPROFILE%\Local Settings\Application Data\Apple Computer\Safari\Cache.db Zero Fill
I-Phone	Mobile Comm	%USERPROFILE%\Local Settings\Application Data\Apple Computer\MobileSync\Backup\%Random%\iPhone\iPhoto\iPhoto.sqlite If delete(group_msg): group_msg = unallocated space
Firefox	History Cookie	%USERPROFILE%\Local Settings\Application Data\Mozilla\Firefox\Profiles\<Random>\places.SQLite or cookies.SQLite Zero Fill
Chrome	Cache History Cookie	%USERPROFILE%\Local Settings\Application Data\Google\Chrome\UserData\Default\Cache or History or Cookies

# How



## SQLite □□(□□)

- Header Page + Page Chain







□ □ □ □ □ □ □ □ □ □

- Database Header

The diagram illustrates the structure of an SQLite file header. It features a terminal window with the following output:

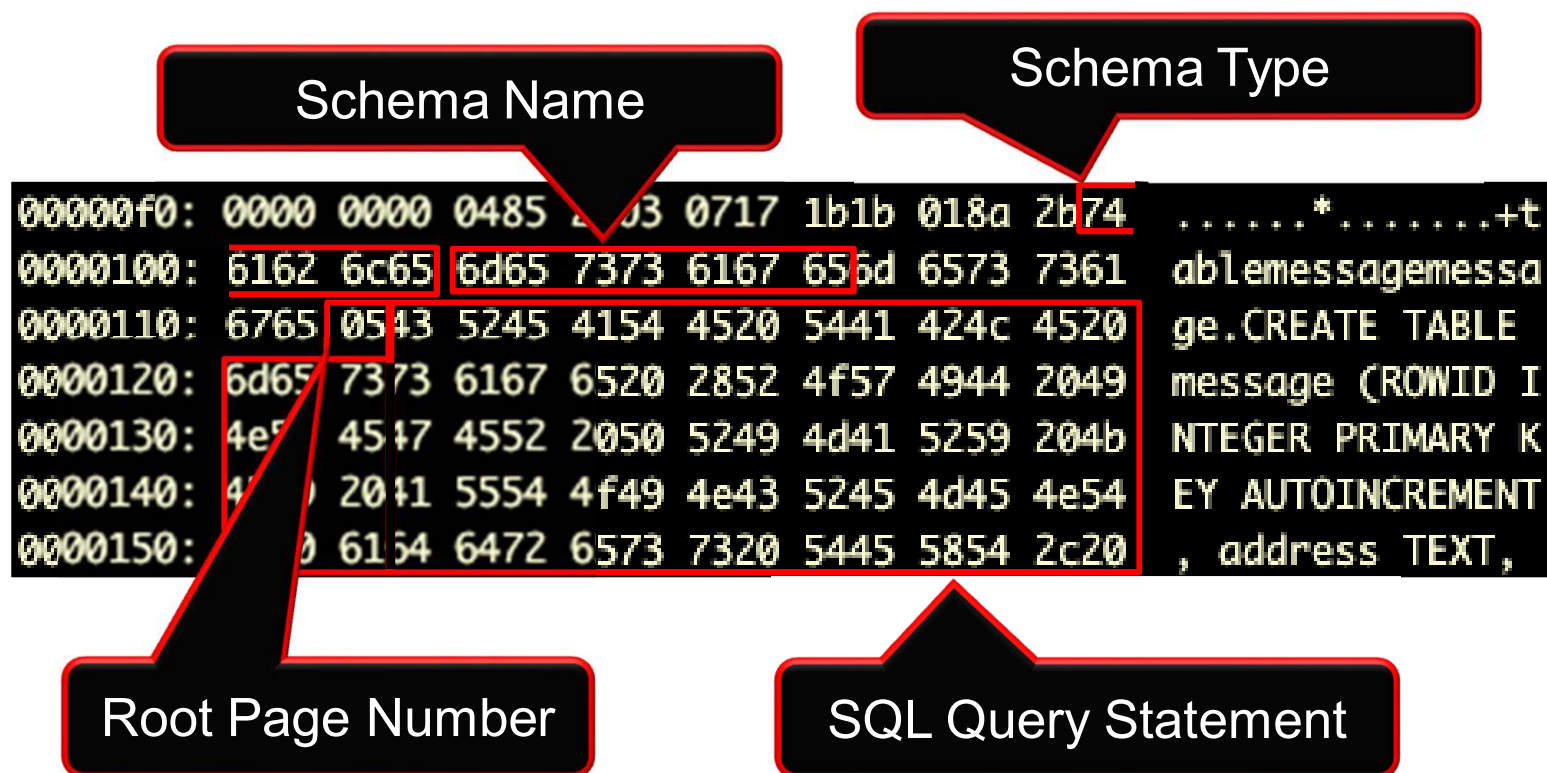
```
[Deok9@MAC-MINI SQLite]$  
MAC :)  
xxd ori_message | head  
00000000: 5351 4c69 7465 2066 6f72 6d61 7420 3300 SQLite format 3.  
00000010: 1000 0202 0040 2020 0000 7a53 0000 002d .....@ ..zS...-
```

Two callouts highlight specific fields:

- SQLite File Signature:** A red callout box points to the first eight bytes of the header (00000000: 5351 4c69 7465 2066 6f72 6d61 7420 3300), which correspond to the ASCII string "SQLite format 3.".
- Page Size(Big endian):** A red callout box points to the first four bytes of the second line (00000010: 1000 0202 0040 2020), which represent the page size in big-endian format.



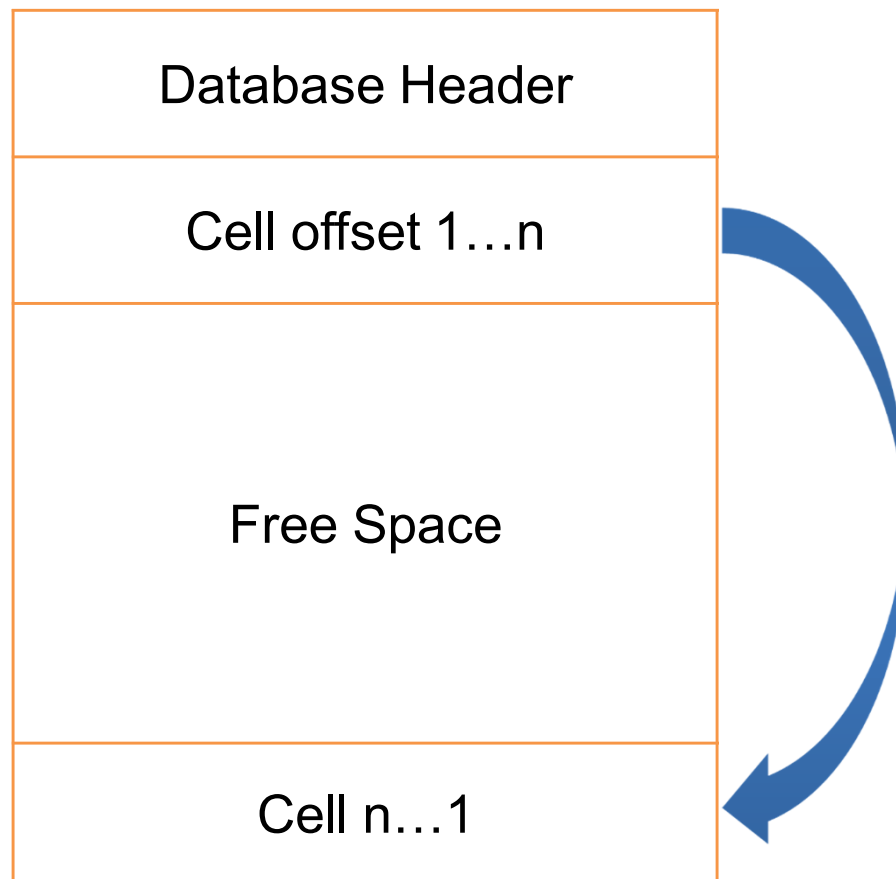
- **Database Schema Table**





□□□ □□(□□)

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





□□ □□□□ □□□□ □□□□ **Leaf** □□□

- **Leaf** □□□ □□

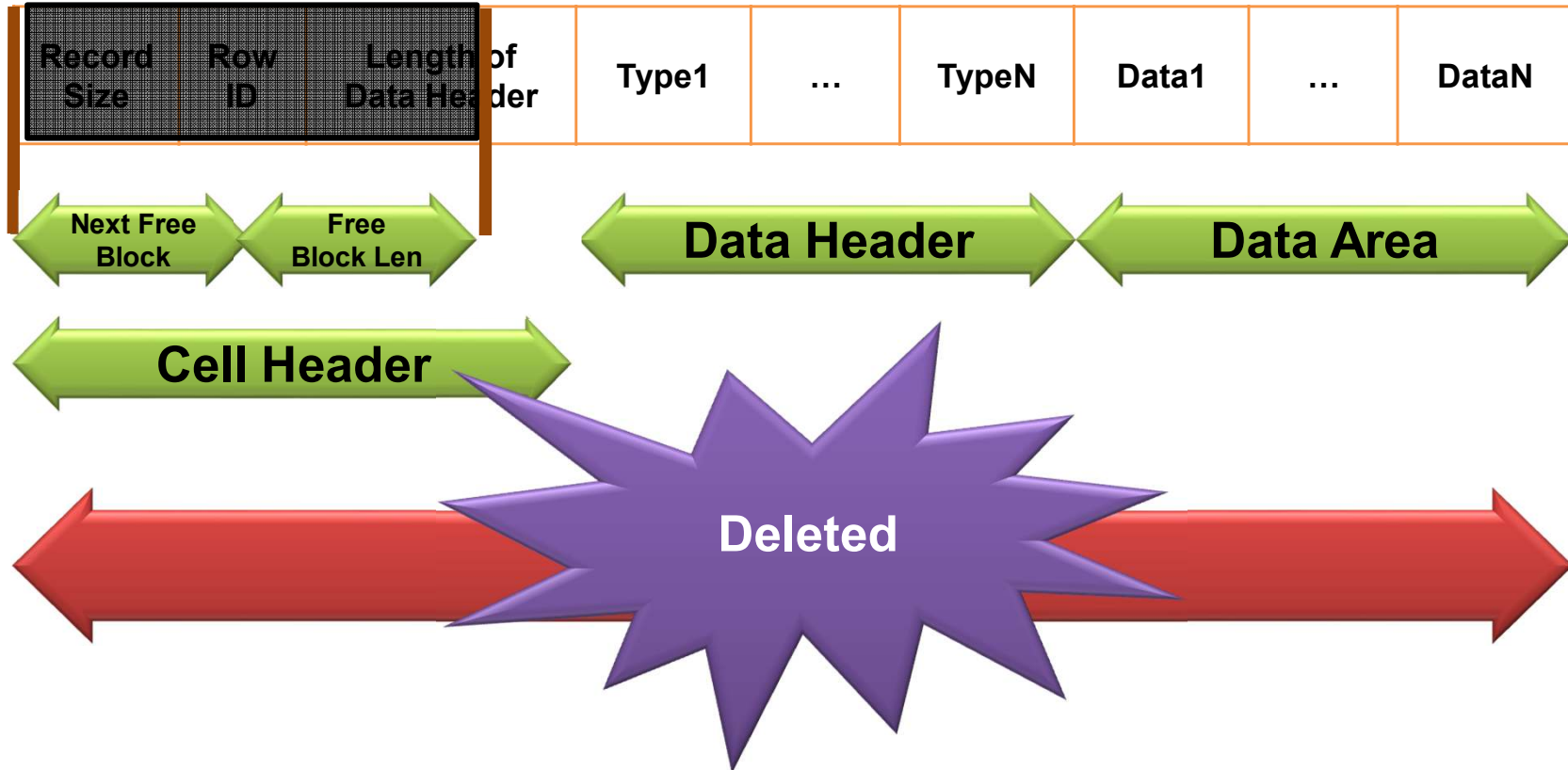
Offset	Contents
0	Page Flag : 0x0D
1-2	First Unallocated Block Offset
3-4	Cell Count
5-6	First Cell Offset
7	Over 3Byte Unallocated Block Count

- □□□ □ □□□□ □□ □□□ □□



□□ Leaf □□□ □□ Cell □□□ □□?

- Leaf Cell □□(□□)





## Free Space

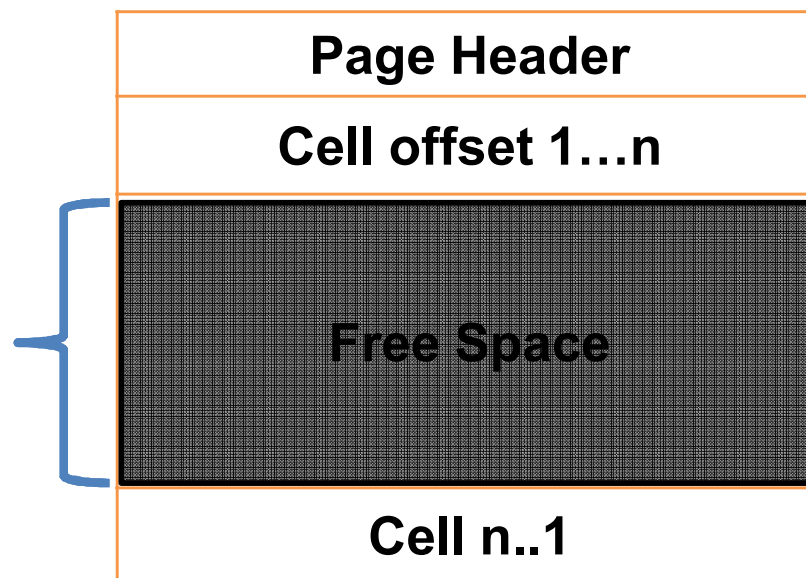
1. Leaf .

2. Free Space.

1. 5~6

2. 0x0000

3. n n





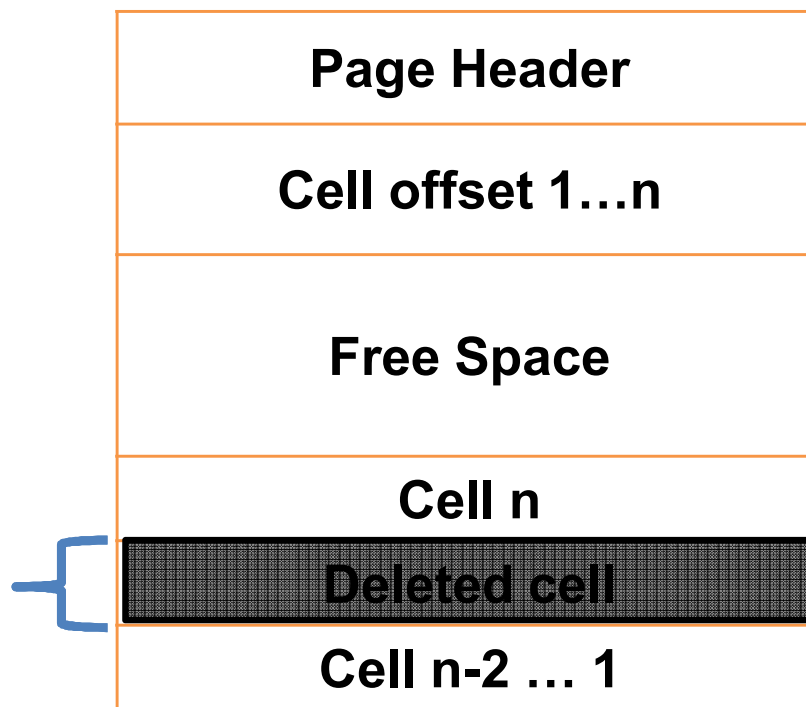
Free Block

1. Leaf

2. Free Block

1. 1~2

2. Leaf Cell

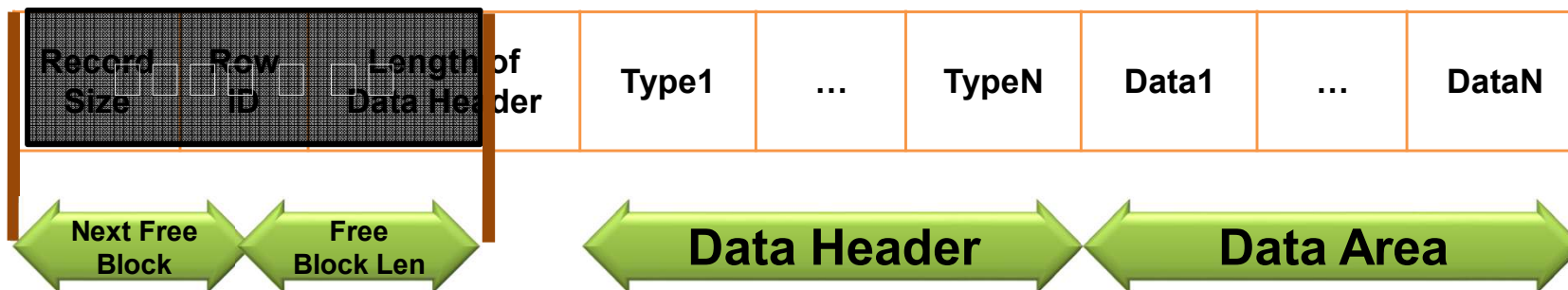




□ □ □ □ □ 1

■ □ □ □ □ □ □

- Length 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	- - - - -	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

- □□□ □□ □ □



□□□ □□□ □3

## ▪ Length of Record□?

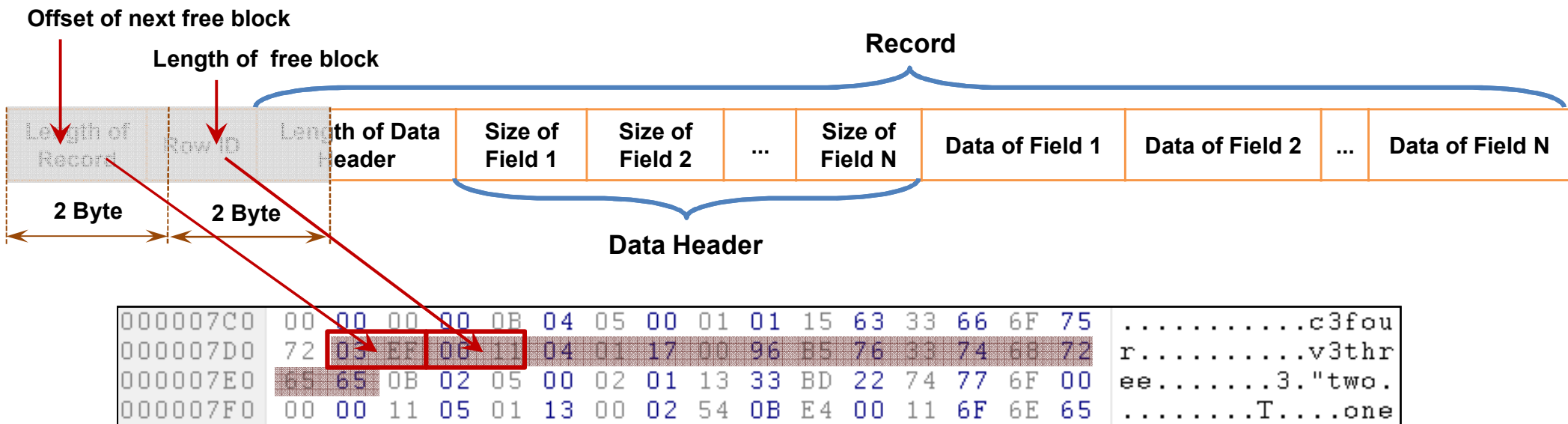
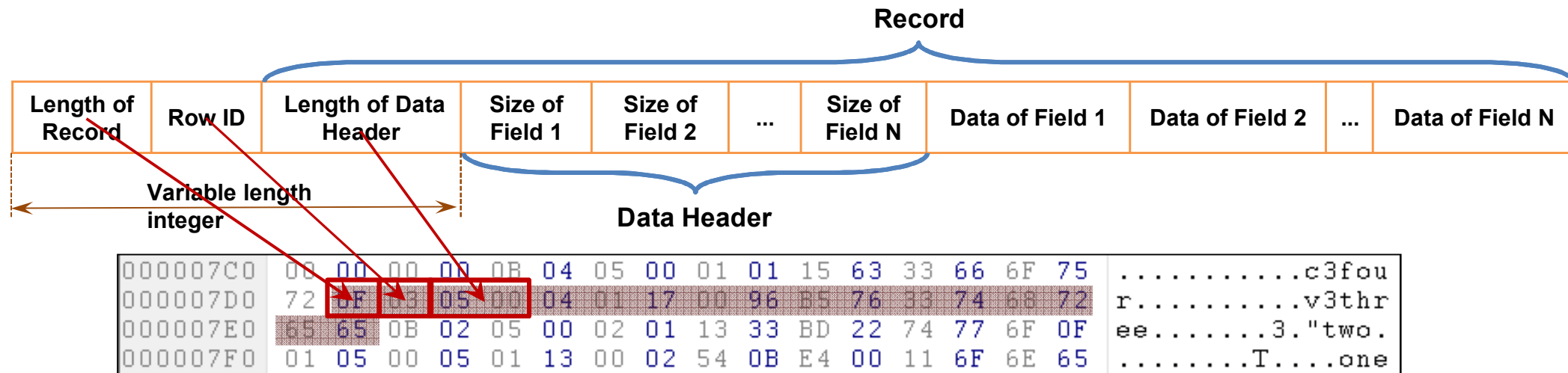
- □□□ □□□ □□□ □□□ □□ □□□□, □□□□ □ □

## ▪ Row ID□?

- □□□ □□ □□□ □□ □□□? □□□ **0xFF** – □□ □□ □□ \* n(□ **200** □□)□ □□□□



□□□ □□□(□□□ □□□ □□□ □□)



## Recover Iphone Message

- □□□ □□□

```
sqlite3recover.py
1 # -*- coding: utf-8 -*-
2 #!/usr/bin/python
3
4 import sys

Phone Number :019924631790???와이파이 안댄다 ㅋㅋ 오늘은 시빅센터갔다가 버클리가따와요 ㅋㅋ대회하고 연락해♥

Phone Number :010302932720?

Phone Number :010307273690?) FSK

이메일확인 첨부자료 출력작성하여 팩스02-564-8367 6.22(금)회신부탁 .노무법인영광

Phone Number :0256145450???문서보관실에 보관중이던 짐수레 사용하신분 긴급히 연락주시요.
-경영지원팀

Phone Number :+8210663655370??

아 ㅏㅏㅋㅋㅋ 넵 ㅏ 일단 사람들
깨면 말해보께여

60
61 #-----File Open-----#
62 try:
63     f = open(file_path,"rb")
64     fsize = os.path.getsize(file_path)
65 except IOError:
66     print >> sys.stderr, 'Not file or File open error'
67     exit(1)
68
```