[Case Study] Access Database Forensic Analysis

In the information age, the importance of the database is beyond doubt. However, information security of database has always been a headache for us. Misoperation, man-made sabotage, hardware failure, many different reasons can lead to loss of valuable digital data.
Today, the SalvationDATA will share some of the ACCESS database file recovery and extraction technologies.

Access database introduction

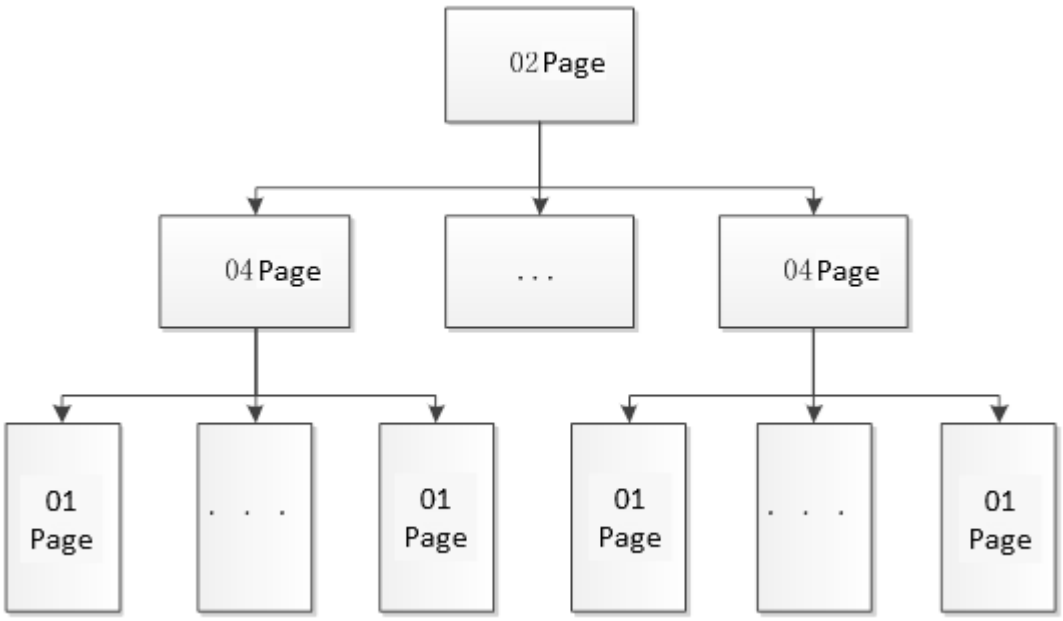
Microsoft Access is a database management system (DBMS) from Microsoft that combines the relational Microsoft Jet Database Engine with a graphical user interface and software-development tools.
Microsoft Access stores data in its own format based on the Access Jet Database Engine. It can also import or link directly to data stored in other applications and databases. It is now widely used by personal developers, enterprises, government organizations or even military agencies. Access is not only a simple database, it is also equipped with powerful data managing capability, providing convenience for data storage, query, reporting, etc.

How does Access database store data

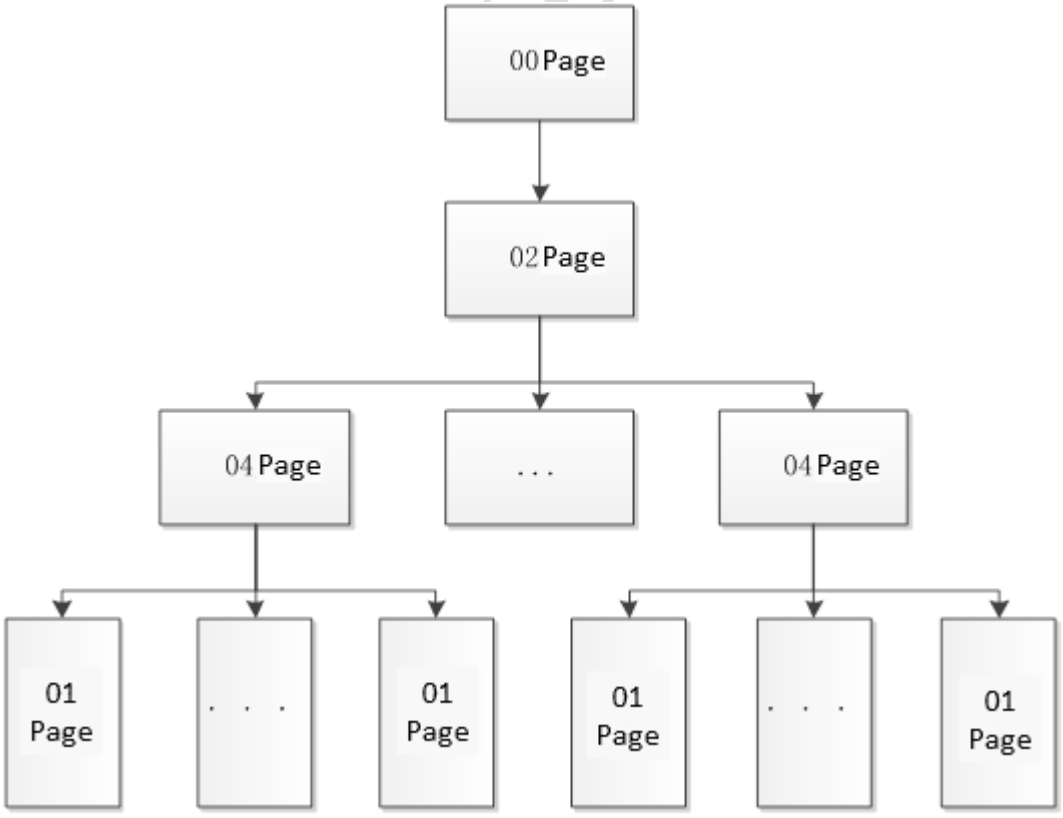
An Access database stores data based on a sort of page structure. Each page contains 4096 Bytes, and the first byte of this page indicates its type. These types includes:

00 – database info page, 01 – data page, 02 – table structure page, 04 – transition page

A typical Access database structure is shown in below picture. 02 page records management information for this database file, while 04 page records the page number of 01 page, and 01 pages are where the actual data is stored.



When reading an Access database table, the structure is as below picture shows. 00 page is fixed as the first page, 02 is the second, 04 records the page number of 01 pages, and 01 are the data pages. However, this time it is not data that is stored in 01 pages but table inform of this database.



The structure of 00 page is as below, database basic info is recorded in this page.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	00	01	00	00	53	74	61	6E	64	61	72	64	20	41	43	45	Standard ACE
00000010	20	44	42	00	02	00	00	00	B5	6E	03	62	60	09	C2	55	DB µn b` ÂU
00000020	E9	A9	67	72	40	3F	00	9C	7E	9F	90	FF	85	9A	31	C5	é©gr@? œ~Ÿ ÿ…š1Å
00000030	79	BA	ED	30	BC	DF	CC	9D	63	D9	E4	C3	D3	41	FB	8A	yºí0¼ßÌ cÙäÃÓAûŠ
00000040	BC	4E	4E	53	EC	37	95	EC	9C	FA	0E	F6	28	E6	DB	1E	¼NNSì7•ìœú ö(æÛ
00000050	8A	60	9C	3C	7B	36	3D	DA	DF	B1	BF	5C	13	43	07	07	Š`œ<{6=ÚßÂ¿\ C
00000060	B1	33	FC	C9	79	5B	5A	1D	7C	2A	A3	E0	7C	99	05	13	±3üÉy[Z |*£à|™
00000070	98	FD	90	5D	FE	62	7E	27	85	66	5F	95	F8	D0	89	24	˜ý]þb~'…f_•øÐ‰$
00000080	85	67	C6	1F	27	44	D2	EE	CF	65	ED	FF	07	C7	46	A1	…gÆ 'DÒîÏeíÿ ÇF¡
00000090	78	16	0C	ED	E9	2D	62	D4	54	06	00	00	34	2E	30	00	x íé-bÔT 4.0
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

The structure of 01 page is as below, user data is recorded in this page.

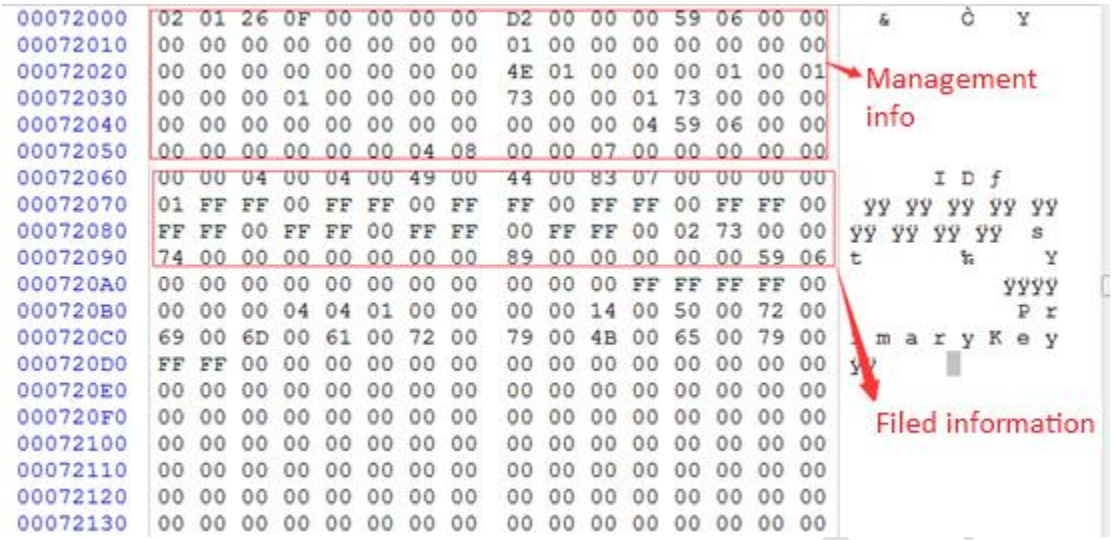
0007B000	01	01	57	0F	61	00	00	00	00	00	00	00	05	00	E2	0F	W a â
0007B010	C6	4F	A8	0F	8C	4F	6F	0F	00	00	00	00	00	00	00	00	ÆO¨ ŒOo
0007B020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0007B030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0007B040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0007B050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0007B060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0007B070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0007B080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0007B090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0007B0A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Management Information

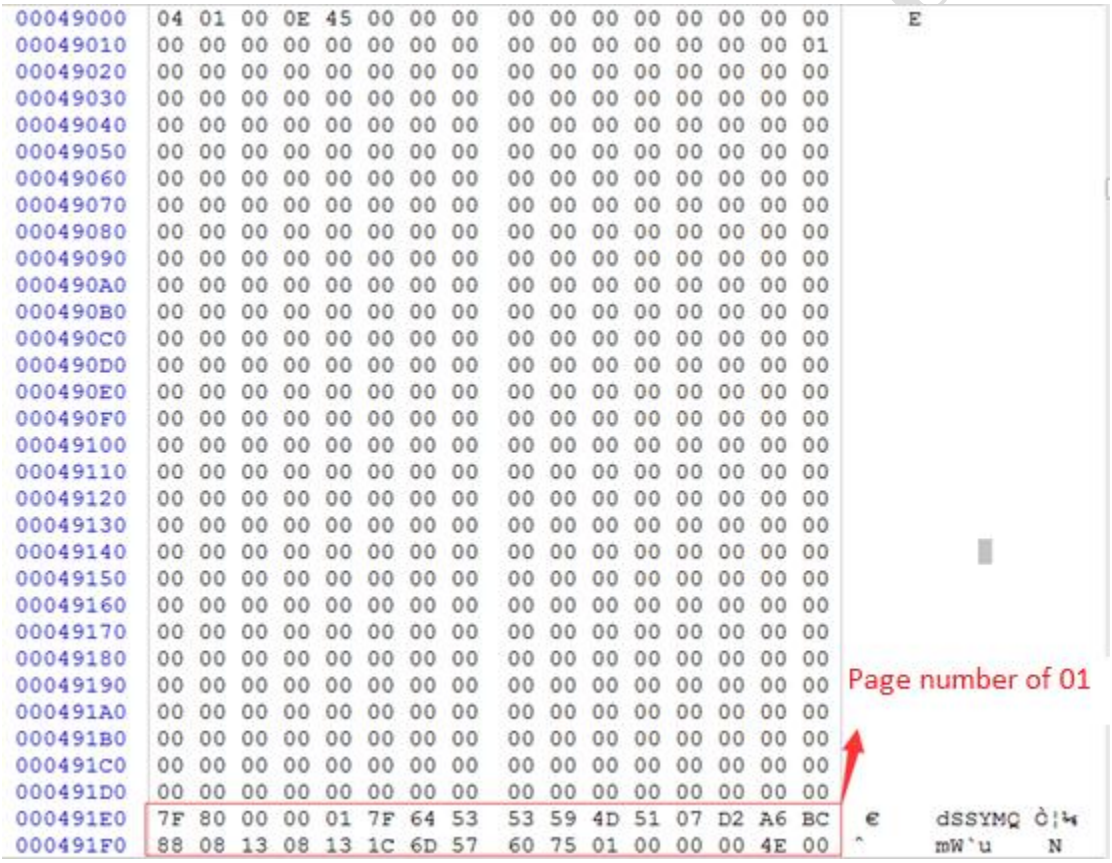
0007BF40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0007BF50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0007BF60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	04	
0007BF70	00	05	00	00	00	10	62	FD	90	FF	FE	35	30	30	30	26	bý ÿþ5000&
0007BF80	54	12	00	10	00	0A	00	06	00	03	00	0F	00	88	00	00	T ^
0007BF90	00	00	F1	6D	33	57	FF	FE	31	32	30	30	30	11	00	11	ñm3Wÿþ12000
0007BFA0	00	0A	00	06	00	03	00	07	04	00	03	00	00	00	7F	5E	^
0007BFB0	DE	5D	FF	FE	31	30	30	30	30	26	54	13	00	11	00	0A	Þ]ÿþ10000&T
0007BFC0	00	06	00	03	00	0F	00	81	00	00	00	00	0A	4E	77	6D	Nwm
0007BFD0	FF	FE	31	30	30	30	30	11	00	11	00	0A	00	06	00	03	ÿþ10000
0007BFE0	00	07	04	00	01	00	00	00	17	53	AC	4E	FF	FE	31	30	S¬Nÿþ10
0007BFF0	30	30	30	26	54	13	00	11	00	0A	00	06	00	03	00	0F	000&T

User data

The structure of 02 page is as below.



The structure of 04 page is as below.



How to recover data from Access database?

According to our forensic expert's analysis, when data is deleted from a database table, the raw data will not be erased. Only the management data recorded in 01 pages is changed, at the offset position 0x0F we found that 0F has changed to CF.

```
00000752  01 01 57 0F 61 00 00 00  00 00 00 00 05 00 E2 0F   W a          â
00000768  C6 4F A8 0F 8C 4F 6F 0F  00 00 00 00 00 00 00 00  ÆO¨ ŒOo
00000784  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000800  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000816  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000832  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000848  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000864  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000880  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000896  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000912  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Before Deletion

```
00000752  01 01 57 0F 61 00 00 00  00 00 00 00 05 00 E2 CF   W a          âÏ
00000768  C6 4F A8 0F 8C 4F 6F 0F  00 00 00 00 00 00 00 00  ÆO¨ ŒOo
00000784  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000800  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000816  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000832  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000848  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000864  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000880  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000896  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000912  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

After Deletion

However after deletion, the raw user data still remains. As show in below picture:

```
00001152  D7 C7 67 B9 79 9F 46 75  A4 C8 83 77 1A 8A 2C 07  ×Çg¹yŸFu¤Èƒw Š,
00001168  45 CE FA 66 70 9D 86 D7  FA F9 EE 11 14 8B 71 8D  EÎúfp †×úùî ‹q
00001184  19 BD 23 0D 33 31 6C AA  55 F9 42 A3 91 74 87 FB   ½# 31lªUùB£'t‡û
00001200  21 B0 4A 26 8E 35 F4 22  E1 09 91 6D 4F 93 E1 CC  !°J&Ž5ô"á 'mO"áÌ
00001216  07 72 69 D2 FA 38 19 49  32 76 18 8C DD 9B 8E 70   riÒú8 I2v ŒÝ›Žp
00001232  9D E7 0F 18 7F 7B 40 B5  52 E9 5C 18 AB 5D A3 21   ç    {@µRé\ «]£!
00001248  EE 9A 7B 50 F5 1C 52 FA  F5 00 DF B6 83 A5 AD B7  îš{Põ Rúõ ß¶ƒ¥-·
00001264  87 89 9C FC 91 83 2C F3  98 1E A1 6A 13 3B 12 0D  ‡‰œü'ƒ,ó˜ ¡j ;
00001280  3F 3A 4B A0 80 FF 30 AC  6F C9 20 E9 83 E8 8C B0  ?:K €ÿ0¬oÉ éƒèŒ°
```

User data after deletion

```
00001152  D7 C7 67 B9 79 9F 46 75  A4 C8 83 77 1A 8A 2C 07  ×Çg¹yŸFu¤Èƒw Š,
00001168  45 CE FA 66 70 9D 86 D7  FA F9 EE 11 14 8B 71 8D  EÎúfp †×úùî ‹q
00001184  19 BD 23 0D 33 31 6C AA  55 F9 42 A3 91 74 87 FB   ½# 31lªUùB£'t‡û
00001200  21 B0 4A 26 8E 35 F4 22  E1 09 91 6D 4F 93 E1 CC  !°J&Ž5ô"á 'mO"áÌ
00001216  07 72 69 D2 FA 38 19 49  32 76 18 8C DD 9B 8E 70   riÒú8 I2v ŒÝ›Žp
00001232  9D E7 0F 18 7F 7B 40 B5  52 E9 5C 18 AB 5D A3 21   ç    {@µRé\ «]£!
00001248  EE 9A 7B 50 F5 1C 52 FA  F5 00 DF B6 83 A5 AD B7  îš{Põ Rúõ ß¶ƒ¥-·
00001264  87 89 9C FC 91 83 2C F3  98 1E A1 6A 13 3B 12 0D  ‡‰œü'ƒ,ó˜ ¡j ;
00001280  3F 3A 4B A0 80 FF 30 AC  6F C9 20 E9 83 E8 8C B0  ?:K €ÿ0¬oÉ éƒèŒ°
```

And according to the data row structure, it is possible to recover deleted row data. The row structure is shown below:

Column	No.	Fixed Field	Flexible Field	Flexible Offset	Field Count	Bit Map

Conclusion

Based on the analysis on Access database structure above, we now understand how the raw data changes when data is deleted from an Access database. And we discovered that no matter if a data row, a table, or even the database file is deleted, we can always recover the data by analyzing the page structure on the base level.

So in this article, we introduced a practical and efficient solution to recover deleted data from Microsoft Access database.