

Checking Access File Security MDB / MDE vs ACCDB / ACCDE

This article describes a simple way of comparing the security of the **MDB & ACCDB** file formats together with the compiled versions **MDE & ACCDE**.

First of all, I created three very simple test **MDB** files in **Access 2003** format.

1. A backend file **BE.mdb** with one table **Table1**.
The table had 4 fields (ID, Surname, FirstName, YearGroup) and 2 records Ann Jones / Ben Smith
The BE file was encrypted with password **dinsdale**.
2. A frontend file **FE.mdb**. I then linked this to **Table1** in the **BE** file
3. The frontend was copied, encrypted with the password **MDS** and saved as **FE - PWD.mdb**

Both versions of the frontend were then saved as **MDE** files: **FE.mde** & **FE - PWD.mde**

In early versions such as **Access 97**, **password strings** could be directly read using a text or hex editor. This appalling security lapse was fixed in later versions.

I checked both the frontend and backend files using a **hex editor** and searched for the two password strings. Although password data is stored in the file, the password information **CANNOT** be directly read using a hex editor in **Access 2003 MDB** files.

However, when I viewed the **BE** file using the hex editor, the details of **Table1** were found unencrypted in several locations. Both field names and the actual data were visible even though the file is password protected.

Password protected MDB BE file

Field names

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00022EE0	00	00	FC	01	00	00	54	00	61	00	62	00	6C	00	65	00	...ü...T.a.b.l.e.
00022EF0	31	00	00	00	36	00	00	00	00	00	00	00	DD	57	20	D2	1...6.....YW Ö
00022F00	FD	1E	BF	4A	BD	D2	92	04	4C	C6	18	BF	07	00	00	00	ý.¿J%Ö'.LÆ.¿....
00022F10	DD	F1	98	52	E6	E9	39	4B	B7	88	C4	7C	14	94	B4	AC	Ýñ~Ræé9K^Ä ."~
00022F20	04	00	00	00	00	00	8D	09	49	00	44	00	00	00	40	00I.D...Ø.
00022F30	00	00	00	00	00	00	64	8D	02	E6	CF	BB	7D	4F	8B	62d..æI»}O<b
00022F40	B2	4F	2C	78	2C	82	07	00	00	00	DD	F1	98	52	E6	E9	*O,x,,...Ýñ~Ræé
00022F50	39	4B	B7	88	C4	7C	14	94	B4	AC	0A	00	00	00	00	00	9K^Ä ."~.....
00022F60	8D	09	53	00	75	00	72	00	6E	00	61	00	6D	00	65	00	..S.u.r.n.a.m.e.
00022F70	00	00	42	00	00	00	00	00	00	00	D8	B8	66	C2	50	CF	..B.....Ø.fÂPİ
00022F80	41	49	A6	9D	57	83	4D	80	82	FD	07	00	00	00	DD	F1	ÄI .WfME,ý....Ýñ
00022F90	98	52	E6	E9	39	4B	B7	88	C4	7C	14	94	B4	AC	0A	00	"Ræé9K^Ä ."~
00022FA0	00	00	00	00	8D	09	46	00	6F	00	72	00	65	00	6E	00F.o.r.e.e.n.
00022FB0	61	00	6D	00	65	00	00	00	44	00	00	00	00	00	00	00	a.m.e...D.....
00022FC0	48	DB	66	CE	6E	E5	42	41	8F	7F	3A	5D	35	B0	B1	DD	HÜfîñâBA...:]5°±Ý
00022FD0	07	00	00	00	DD	F1	98	52	E6	E9	39	4B	B7	88	C4	7C	...Ýñ~Ræé9K^Ä
00022FE0	14	94	B4	AC	04	00	00	00	00	00	8D	09	59	00	65	00	."~.....Y.e.
00022FF0	61	00	72	00	47	00	72	00	6F	00	75	00	70	00	00	00	a.r.G.r.o.u.p...

Data

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0002EFA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0002EFB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0002EFC0	00	00	04	00	02	00	00	00	09	00	00	00	FF	FE	4A	6FýþJo
0002EFD0	6E	65	73	FF	FE	41	6E	6E	16	00	11	00	0A	00	02	00	nesýþAnn.....
0002EFE0	0F	04	00	01	00	00	00	07	00	00	00	FF	FE	53	6D	69ýþSmi
0002EFF0	74	68	FF	FE	42	65	6E	16	00	11	00	0A	00	02	00	0F	thýþBen.....

For comparison, the **entire file is encrypted** in a **password protected ACCDB file**

Password protected ACCDB BE file

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0002C040	14	C6	49	F5	A9	B0	16	10	5E	B1	70	EB	8B	5C	54	D2	.Eİö°...^tpë<\Tò
0002C050	7F	90	00	AB	26	E7	C0	A4	85	06	B8	0F	2F	CD	AB	1A	...«&çà«.../í«.
0002C060	6D	1E	D0	42	D1	94	59	9F	A5	6E	90	EA	19	F7	C1	E1	m.DBÑ~Yÿñ.ê.÷Áá
0002C070	6A	80	E9	66	2C	E6	D8	8E	DB	54	63	27	8F	FF	A7	D9	jééf,æðžÚTc'.ýSÙ
0002C080	F9	3D	02	6F	FC	66	18	BA	F7	C2	A6	5F	13	CF	B5	5F	ù=.ouíf.°÷À!_.İp_
0002C090	A4	BE	98	BF	84	56	4A	F2	A2	57	0F	E2	F3	DF	71	10	«%~ç„VJò«W.áoBq.
0002C0A0	73	AF	FF	EA	59	CC	00	1E	B5	76	5F	C0	70	40	AO	09	s`ýéYİ..pv àp@ .
0002C0B0	1E	35	43	6C	46	60	E4	C7	68	73	D5	C6	3E	71	EE	CB	.5C1F`àÇhsÖ&»qiÈ
0002C0C0	95	D8	03	DC	9C	E9	2C	FO	53	D5	44	31	66	06	56	54	•Ø.Üœé,ßSÖD1f.VT
0002C0D0	16	2C	5E	85	E2	79	BF	CF	85	CA	C6	7D	D5	04	48	69	.,^...âyçİ...È&)Ö.Hi
0002C0E0	DD	41	02	56	08	D4	8A	66	F8	C7	53	F6	C3	87	F3	47	ÝA.V.ÖŠfæÇSö&+óG
0002C0F0	06	A7	FE	C9	F9	F3	C1	89	7D	C3	11	4E	CE	69	53	45	.SpÉúóÁ&ç).İ.NİiSE
0002C100	26	72	92	DD	BE	72	89	22	54	0B	4F	3B	C4	24	FA	D0	ær'Ý&rt«"T.O;Ä\$úD
0002C110	38	C4	37	48	08	BC	3C	21	D3	D1	F5	BF	31	AB	CC	E2	ßÄ7H.¼<!ÖNöç1«İä
0002C120	F5	AC	51	0A	C6	22	6E	F8	29	2D	8B	89	21	C3	FO	F9	ö-Q.È"nø)-«ç!Ä\$ù
0002C130	6C	DF	9C	74	C2	E3	EE	91	E7	71	74	72	81	EO	86	D1	lBøtÄäi`cçtr.àtN

Next, I wanted to see how secure the **backend** data would be from someone who didn't know the **BE** password. To do so, each **frontend** file was then checked using a **hex editor** looking specifically for the **BE** password text strings **PWD** and **dinsdale**. These were found in several locations:

MDB file

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
000112F0	00	0F	06	00	CB	66	BF	2C	F5	2C	E5	40	CB	66	BF	2CËfç,ö,â@Ëfç,
00011300	F5	2C	E5	40	00	00	20	00	54	00	61	00	62	00	6C	00	ö,â@...T.a.b.l.
00011310	65	00	31	00	3A	71	84	00	00	40	01	3D	00	00	00	00	e.1.:q...@.=....
00011320	00	00	19	00	00	80	00	00	00	00	00	00	00	00	FF	FE€.....ÿb
00011330	4D	53	20	41	63	63	65	73	73	3B	50	57	44	3D	64	69	MS Access;PWD=di
00011340	6E	73	64	61	6C	65	3B	54	00	61	00	62	00	6C	00	65	nsdale;T.a.b.l.e
00011350	00	31	00	6B	00	6B	00	6B	00	6B	00	6B	00	6B	00	6B	.1.k.k.k.k.k.k.k
00011360	00	5F	00	3A	00	2E	00	2C	00	20	00	0B	00	FF	07	00	._:.... ...ÿ..
00011370	11	00	0A	00	00	80	01	00	00	0F	06	00	C2	7C	C7	15€.....Â ç.
00011380	F5	2C	E5	40	E6	85	EB	2A	F5	2C	E5	40	01	11	00	0B	ö,â@æ...ë*ö,â@....
00011390	00	00	80	01	00	00	0F	06	00	CB	66	BF	2C	F5	2C	E5	..€.....Ëfç,ö,â
000113A0	40	CB	66	BF	2C	F5	2C	E5	40	00	00	20	00	54	00	61	@Ëfç,ö,â@...T.a
000113B0	00	62	00	6C	00	65	00	31	00	3A	71	84	00	00	40	01	.b.l.e.1.:q...@.
000113C0	3D	00	00	00	00	00	00	19	00	00	80	00	00	00	00	00	=.....€.....
000113D0	00	00	00	FF	FE	4D	53	20	41	63	63	65	73	73	3B	50	...ÿbMS Access;P
000113E0	57	44	3D	64	69	6E	73	64	61	6C	65	3B	54	00	61	00	WD=dinsdale;T.a
000113F0	62	00	6C	00	65	00	31	00	6B	00	6B	00	6B	00	6B	00	b.l.e.1.k.k.k.k.

MDE file

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00011540	00	CB	66	BF	2C	F5	2C	E5	40	CB	66	BF	2C	F5	2C	E5	.Ëfç,ö,â@Ëfç,ö,â
00011550	40	00	00	20	00	54	00	61	00	62	00	6C	00	65	00	31	@...T.a.b.l.e.1
00011560	00	6A	D8	84	00	00	40	00	39	00	00	00	00	00	00	19	.j@...@.9.....
00011570	00	00	80	00	00	00	00	00	00	00	00	FF	FE	4D	53	20	..€.....ÿbMS
00011580	41	63	63	65	73	73	3B	50	57	44	3D	64	69	6E	73	64	Access;PWD=dinsd
00011590	61	6C	65	3B	54	00	61	00	62	00	6C	00	65	00	31	00	ale;T.a.b.l.e.1.
000115A0	6B	00	6B	00	6B	00	6B	00	6B	00	6B	00	6B	00	5F	00	k.k.k.k.k.k.k._.
000115B0	3A	00	2E	00	2C	00	2C	00	0B	00	FF	07	00	11	00	37	:...,. ...ÿ....7
000115C0	00	00	00	01	00	00	0F	01	00	C5	77	3B	C8	32	8B	E3Äw;È2<ä
000115D0	40	FD	7D	3B	C8	32	8B	E3	40	0A	00	02	80	4D	00	53	@ý);È2<â@...€M.S
000115E0	00	79	00	73	00	57	00	53	00	44	00	50	00	52	00	65	.v.s.W.S.D.P.R.e

As you can see, **converting the file to MDE format does not encrypt the linked table name or the password needed to open the BE file. The BE file is completely insecure**

Next, I checked whether adding a password to the FE had any effect

Password protected MDB file

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00011300	F5	2C	E5	40	00	00	20	00	54	00	61	00	62	00	6C	00
00011310	65	00	31	00	3A	71	84	00	00	40	01	3D	00	00	00	00
00011320	00	00	19	00	00	80	00	00	00	00	00	00	00	00	FF	FE
00011330	4D	53	20	41	63	63	65	73	73	3B	50	57	44	3D	64	69
00011340	6E	73	64	61	6C	65	3B	54	00	61	00	62	00	6C	00	65
00011350	00	31	00	6B	00	6B	00	6B	00	6B	00	6B	00	6B	00	6B
00011360	00	5F	00	3A	00	2E	00	2C	00	20	00	0B	00	FF	07	00
00011370	11	00	0A	00	00	80	01	00	00	0F	06	00	C2	7C	C7	15
00011380	F5	2C	E5	40	E6	85	EB	2A	F5	2C	E5	40	01	11	00	0B
00011390	00	00	80	01	00	00	0F	06	00	CB	66	BF	2C	F5	2C	E5
000113A0	40	CB	66	BF	2C	F5	2C	E5	40	00	00	20	00	54	00	61
000113B0	00	62	00	6C	00	65	00	31	00	90	15	84	00	00	40	01
000113C0	3D	00	00	00	00	00	00	19	00	00	80	00	00	00	00	00
000113D0	00	00	00	FF	FE	4D	53	20	41	63	63	65	73	73	3B	50
000113E0	57	44	3D	64	69	6E	73	64	61	6C	65	3B	54	00	61	00
000113F0	62	00	6C	00	65	00	31	00	6B	00	6B	00	6B	00	6B	00
00011400	6B	00	6B	00	6B	00	5F	00	3A	00	2E	00	2C	00	20	00
00011410	0B	00	FF	07	00	11	00	39	00	00	00	01	00	00	0F	01

Password protected MDE file

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00011550	40	00	00	20	00	54	00	61	00	62	00	6C	00	65	00	31
00011560	00	35	B5	84	00	00	40	00	39	00	00	00	00	00	00	19
00011570	00	00	80	00	00	00	00	00	00	00	00	FF	FE	4D	53	20
00011580	41	63	63	65	73	73	3B	50	57	44	3D	64	69	6E	73	64
00011590	61	6C	65	3B	54	00	61	00	62	00	6C	00	65	00	31	00
000115A0	6B	00	6B	00	6B	00	6B	00	6B	00	6B	00	6B	00	5F	00
000115B0	3A	00	2E	00	2C	00	20	00	0B	00	FF	07	00	11	00	37
000115C0	00	00	00	01	00	00	0F	01	00	C5	77	3B	C8	32	8B	E3
000115D0	40	FD	7D	3B	C8	32	8B	E3	40	0A	00	02	80	4D	00	53
000115E0	00	79	00	73	00	57	00	53	00	44	00	50	00	52	00	65

The above screenshots show that **adding a password to the frontend does not encrypt the linked table name or the password needed to open the BE file. The BE file remains completely insecure**

For comparison, I converted all the test files to **ACCDB** format but otherwise **identical to those above**

1. A backend file **BE.accdb** with one table **Table1**. The file was encrypted with password **dinsdale**.
 2. A frontend file **FE.accdb**. I then linked this to **Table1** in the **BE** file
 3. The frontend was copied, encrypted with the password **MDS** and saved as **FE - PWD.accdb**
- In **ACCDB** files, much stronger 128-bit encryption is used which encrypts the **entire file**

NOTE:

For that reason, zipping an encrypted ACCDB/ACCDE file will have little effect on file size
By comparison zipping a password protected MDB/MDE file does reduce file size

Both versions of the frontend were then saved as **ACCDE** files: **FE.accde** & **FE - PWD.accde**

The same tests were run as for the **MDB / MDE** files

ACCDB file

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00011070	2C	E5	40	31	04	76	29	F5	2C	E5	40	00	00	00	00	54
00011080	00	61	00	62	00	6C	00	65	00	31	00	88	00	00	40	00
00011090	68	00	00	00	00	00	00	19	00	00	11	00	09	00	00	80
000110A0	01	00	00	0F	06	00	A8	E8	21	28	F5	2C	E5	40	E9	69
000110B0	23	28	F5	2C	E5	40	00	00	20	00	54	00	61	00	62	00
000110C0	6C	00	65	00	31	00	5D	1A	88	00	00	40	00	68	00	00
000110D0	00	00	00	00	19	00	00	80	00	00	00	00	00	00	00	00
000110E0	FF	FE	4D	53	20	41	63	63	65	73	73	3B	50	57	44	3D
000110F0	64	69	6E	73	64	61	6C	65	3B	54	00	61	00	62	00	6C
00011100	00	65	00	31	00	31	07	00	40	00	6E	00	00	00	00	00
00011110	00	77	00	77	00	77	00	6B	00	6B	00	6B	00	6B	00	5F

ACCDE file

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
000110B0	23	28	F5	2C	E5	40	00	00	20	00	54	00	61	00	62	00
000110C0	6C	00	65	00	31	00	C0	A6	88	00	00	40	00	63	00	00
000110D0	00	00	00	00	19	00	00	80	00	00	00	00	00	00	00	00
000110E0	FF	FE	4D	53	20	41	63	63	65	73	73	3B	50	57	44	3D
000110F0	64	69	6E	73	64	61	6C	65	3B	54	00	61	00	62	00	6C
00011100	00	65	00	31	00	31	07	00	40	00	69	00	00	00	00	00
00011110	00	77	00	77	00	77	00	6B	00	6B	00	6B	00	6B	00	5F
00011120	00	3A	00	2F	00	2C	00	20	00	0B	00	FF	47	00	11	00

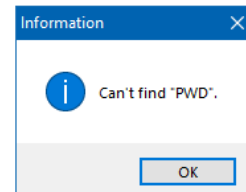
Neither ACCDB nor ACCDE files offer any additional security in terms of the BE file.

As a result, this remains insecure

For comparison, here are the results using password protected (encrypted) ACCDB / ACCDE files

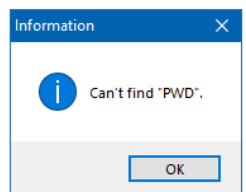
Password protected ACCDB file

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00011050	8F	1C	91	D9	CC	35	2E	A5	42	C6	E0	OC	23	AE	5E	B8
00011060	DC	AA	ED	07	A3	F4	70	2B	F3	20	EB	8B	24	ED	FB	0B
00011070	10	0A	E5	2E	B7	F4	8B	77	DC	28	9C	24	DB	F1	D8	6F
00011080	BC	5A	7D	51	C2	B4	CC	BA	8A	F0	F4	1E	45	3C	BD	5C
00011090	53	40	C5	F8	51	80	D3	23	70	91	E2	88	A7	OC	EB	1D
000110A0	62	58	EB	2D	DB	61	40	1B	D5	AB	2E	CE	78	49	4A	3A
000110B0	8E	9F	1C	D0	D1	84	EF	86	B4	75	38	C8	5C	8B	B8	67
000110C0	2A	ED	13	F0	6A	E8	1C	D6	47	49	80	EF	02	07	39	C5
000110D0	B1	FA	E9	8B	71	08	95	22	CC	B2	0B	93	D2	21	01	59
000110E0	34	4C	56	BD	E9	4E	74	51	66	B6	73	63	73	70	B1	A8
000110F0	0C	40	8C	11	7E	22	C7	24	E0	52	F7	78	C9	99	61	93
00011100	4F	08	FD	00	7D	82	17	F2	95	BB	2A	2C	B1	52	F5	22
00011110	ED	6C	92	BD	22	CF	8A	22	C0	94	CE	50	14	56	37	CE



Password protected ACCDE file

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
000110A0	95	8C	D7	59	BA	14	B6	1C	B7	46	FB	83	CC	D8	6C	17
000110B0	CC	0F	8E	B6	7B	B4	86	10	38	46	20	C8	AB	8A	CE	30
000110C0	7A	0A	7B	E4	1D	33	98	D5	F0	2D	15	D8	FD	E4	AF	98
000110D0	B0	9A	29	1B	24	1F	60	AD	4D	27	36	C2	D6	30	8B	C0
000110E0	1E	18	17	D4	85	EA	CE	9E	56	34	7D	A0	B9	E3	B8	C3
000110F0	8D	B9	3D	24	89	50	11	ED	0D	A8	47	39	B0	C6	F9	0A
00011100	25	0D	C4	68	FC	4C	4E	71	18	84	31	25	E3	OC	25	77
00011110	43	B7	21	18	3C	4D	BB	68	C2	C8	68	E5	53	14	0F	5A
00011120	83	B0	21	8F	F0	E6	0D	5F	F9	19	1A	6F	78	68	32	4C
00011130	D0	18	03	26	85	06	16	B5	43	31	57	F6	09	AA	D3	9F
00011140	3E	3E	EC	5B	7E	5A	A6	A5	DE	D2	9B	DF	6E	AD	D8	DC



The password protected ACCDB & ACCDE files encrypt the entire file including BOTH the linked table name and password information

Therefore, to keep the data in a BE file secure, the FE file needs to be in ACCDB/ACCDE format and encrypted using password protection.

Password Recovery utilities

Password recovery utilities can be useful if you forget the password to your own applications but can just as easily be used for other applications that are not your own work.

Running a quick online check will soon find several utilities (mostly free) that will crack passwords on MDB files. This is usually very quick as the level of encryption is relatively weak

By comparison, I am only aware of one commercial utility that will crack ACCDB passwords.

This is done by 'brute force' trying every possible combination of characters until one is successful.

If a strong password is used, the process can take MANY hours and is therefore unlikely to be worth the effort in most cases.

Obviously, there are many other factors involved in making databases as secure as possible including:

- a) The use of workgroup security for MDB/MDE files
- b) Protecting the location of the BE file by saving on a secure network and limiting user permissions to the folder
- c) Using strong passwords that cannot easily be hacked

However, an Access database can NEVER be made 100% secure. A capable and determined hacker can break any Access database given sufficient time and determination

I would welcome feedback on the information provided in this article