Outlook Express Email Professional Module Recovery

Email Recovery – The Problem

- Missing vast amounts of e-mail evidence from unallocated clusters
- Scripts / Simple Carvers won't work because of the structure (non-contiguous blocks)
- Outlook Express Base64 Attachments can't be decoded from unallocated clusters (binary data contaminates structure)
- OE & AOL both use an index which is more than likely overwritten

DIGITAL DETECTIVE

Email Recovery – The Problem

- Lack of accurate documentation / complicated structures
- Some tools tested had flaws with email extraction
  - Missing dates
  - Misinterpretation of data
  - Not recovering all data
  - Some didn't recover deleted data!!!
- Not designed with partial data recovery in mind

DIGITAL DETECTIVE

Traditional Binary Structure of OE DBX File

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	CF	AD	12	FE	C5	FD	74	6F	66	E3	D1	11	9A	4E	00	C0	Ï-.þÅýtofãÑ.▮N.À
00000016	4F	A3	09	D4	05	00	00	00	05	00	00	00	18	06	00	00	O£.Ô.....
00000032	00	00	00	00	70	E3	52	01	00	C0	00	00	F0	8B	00	00	....pãR..À..ð▮..
00000048	54	E2	01	00	1C	3E	00	00	D8	18	00	00	F0	E1	A3	01	Tâ...>..Ø...ðá£.
00000064	80	F7	00	00	F0	E4	00	00	00	00	00	00	00	00	00	00	▮÷..ðä.....
00000080	00	00	00	00	B8	42	A4	01	04	76	01	00	01	01	00	00	....¸B¤..v.....
00000096	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00	00	.....
00000112	00	00	00	00	00	00	00	00	02	00	00	00	70	D9	A4	01	..........pÙ¤.
00000128	02	00	00	00	00	00	00	00	D4	2A	00	00	00	00	00	00	........Ô*.....
00000144	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

File Signature (4 Bytes)

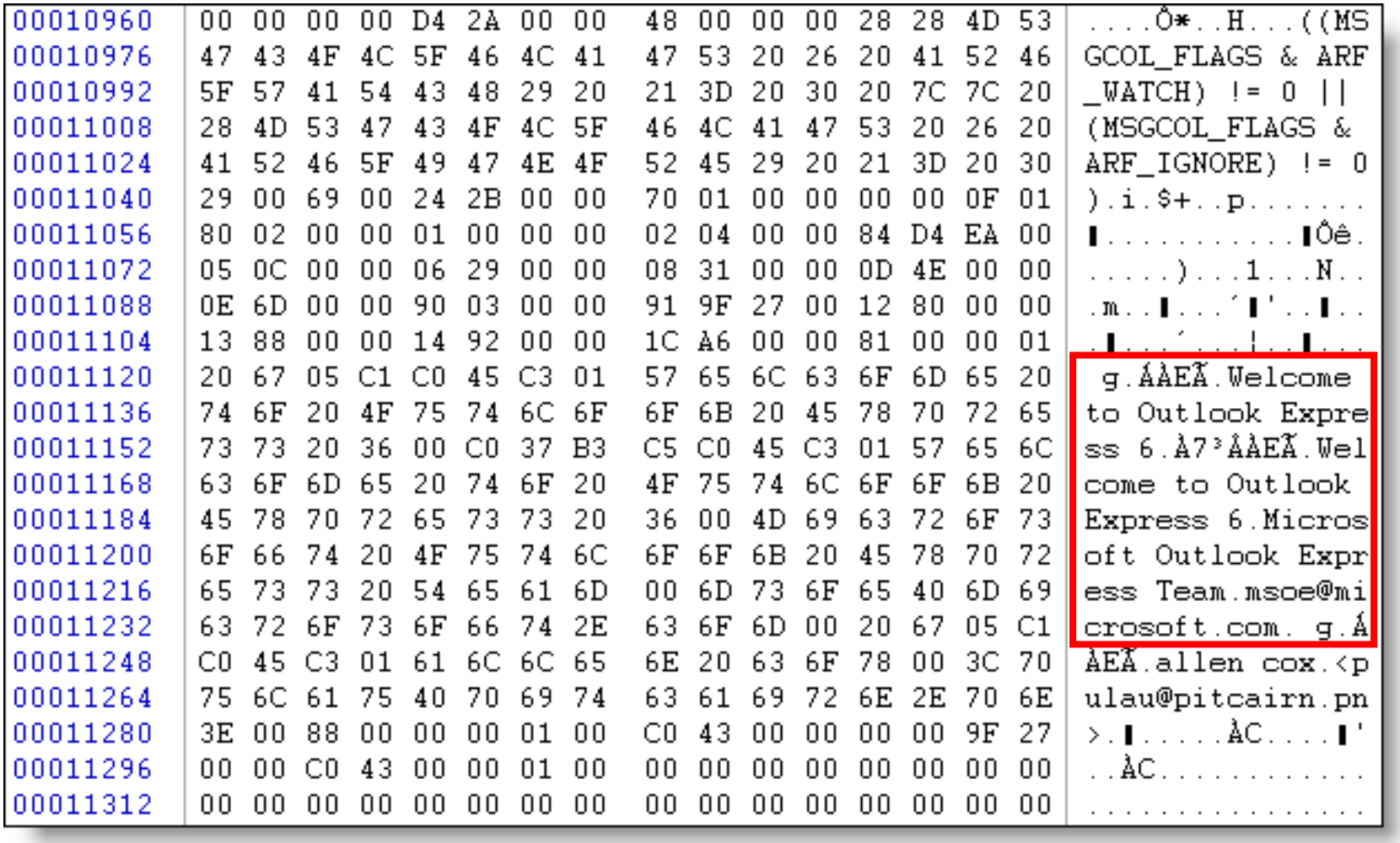
- CF AD 12 FE (0xFE12ADCF)

File Function Identifier (CLSID – 16 Bytes in standard format)

- {6F74FDC5-E366-11D1-9A4E-00C04FA309D4}
- CLSID for Message Store

DIGITAL DETECTIVE

OE DBX Index



```
00010960  00 00 00 00 D4 2A 00 00  48 00 00 00 28 28 4D 53  ....Ô*..H...((MS
00010976  47 43 4F 4C 5F 46 4C 41  47 53 20 26 20 41 52 46  GCOL_FLAGS & ARF
00010992  5F 57 41 54 43 48 29 20  21 3D 20 30 20 7C 7C 20  _WATCH) != 0 || 
00011008  28 4D 53 47 43 4F 4C 5F  46 4C 41 47 53 20 26 20  (MSGCOL_FLAGS & 
00011024  41 52 46 5F 49 47 4E 4F  52 45 29 20 21 3D 20 30  ARF_IGNORE) != 0
00011040  29 00 69 00 24 2B 00 00  70 01 00 00 00 00 0F 01  ).i.$+..p.......
00011056  80 02 00 00 01 00 00 00  02 04 00 00 84 D4 EA 00  ▌...........▌Ôê.
00011072  05 0C 00 00 06 29 00 00  08 31 00 00 0D 4E 00 00  .....)...1...N..
00011088  0E 6D 00 00 90 03 00 00  91 9F 27 00 12 80 00 00  .m..▌...´▌'..▌..
00011104  13 88 00 00 14 92 00 00  1C A6 00 00 81 00 00 01  .▌...´...¦..▌...
00011120  20 67 05 C1 C0 45 C3 01  57 65 6C 63 6F 6D 65 20   g.ÁÀEÃ.Welcome 
00011136  74 6F 20 4F 75 74 6C 6F  6F 6B 20 45 78 70 72 65  to Outlook Expre
00011152  73 73 20 36 00 C0 37 B3  C5 C0 45 C3 01 57 65 6C  ss 6.À7³ÅÀEÃ.Wel
00011168  63 6F 6D 65 20 74 6F 20  4F 75 74 6C 6F 6F 6B 20  come to Outlook 
00011184  45 78 70 72 65 73 73 20  36 00 4D 69 63 72 6F 73  Express 6.Micros
00011200  6F 66 74 20 4F 75 74 6C  6F 6F 6B 20 45 78 70 72  oft Outlook Expr
00011216  65 73 73 20 54 65 61 6D  00 6D 73 6F 65 40 6D 69  ess Team.msoe@mi
00011232  63 72 6F 73 6F 66 74 2E  63 6F 6D 00 20 67 05 C1  crosoft.com. g.Á
00011248  C0 45 C3 01 61 6C 6C 65  6E 20 63 6F 78 00 3C 70  ÀEÃ.allen cox.<p
00011264  75 6C 61 75 40 70 69 74  63 61 69 72 6E 2E 70 6E  ulau@pitcairn.pn
00011280  3E 00 88 00 00 00 01 00  C0 43 00 00 00 00 9F 27  >.▌.....ÀC....▌'
00011296  00 00 C0 43 00 00 01 00  00 00 00 00 00 00 00 00  ..ÀC............
00011312  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

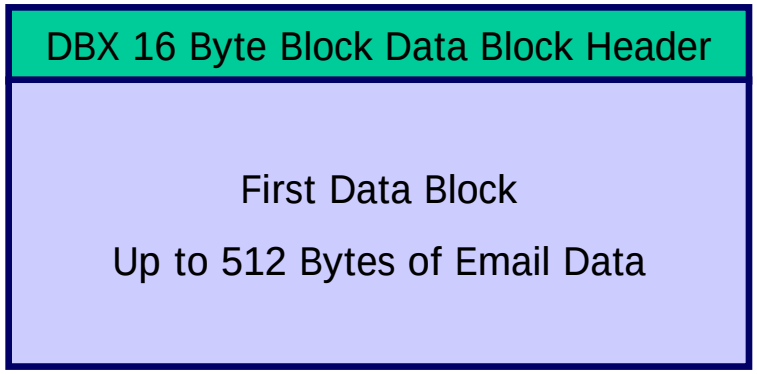
Index contains summary, and pointer to email data Header Block

DIGITAL DETECTIVE

Binary Structure of OE Email

OE Block Structure

- **DATA BLOCK HEADER**
  - **16 Bytes**
- **DATA BLOCK**
  - **Variable –**
  - **Up to 512 Bytes**

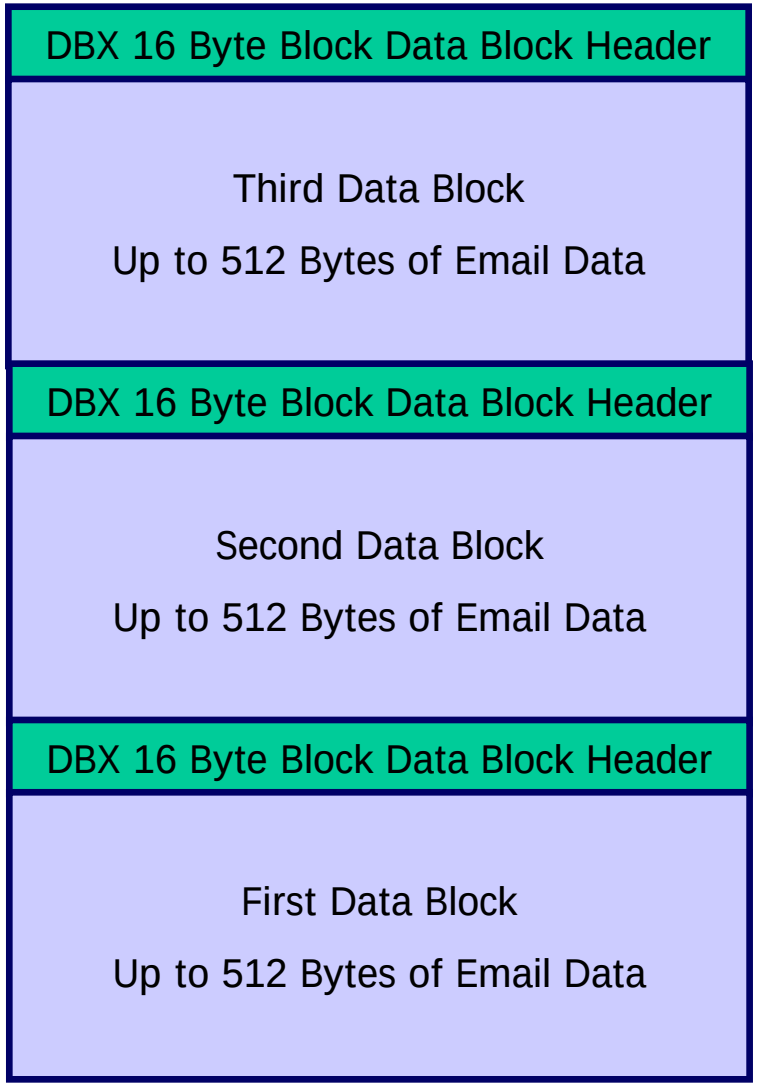


DIGITAL DETECTIVE

Typical DBX Email Structure

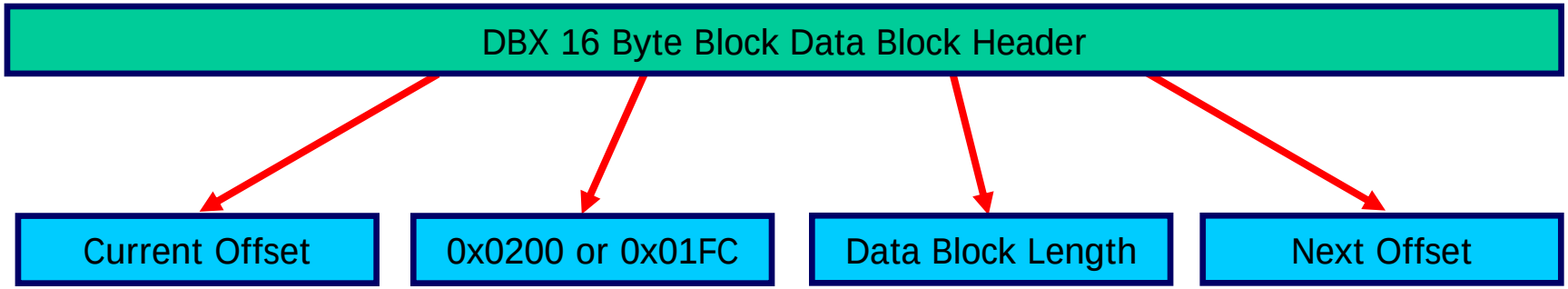
EML / DBX Data Block

- 16 Byte Data Header
- Up to 512 Bytes of Data
- Not always contiguous
- Difficult to carve
- Non-standard header
- MIME format
- Attachments in Base64 for email
- Data split by 16 Byte Data Block!



DIGITAL DETECTIVE

16 Byte Data Header Block



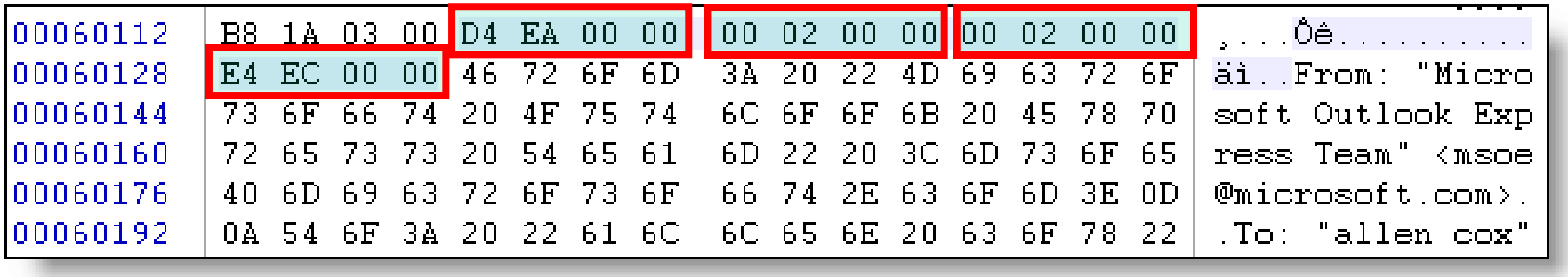
Data Block Header

4 x UInt32 Values (16 Bytes in total)

- **Block1 - Offset of this Data Block Header in DBX File**
- **Block2 - Always 512 for live entries and 508 for deleted**
- **Block3 - Length of Data Block following this header**
- **Block4 - Offset of Next Data Block Header in DBX File**

DIGITAL DETECTIVE

Data Header Block Example



00060112	B8	1A	03	00	D4	EA	00	00	00	02	00	00	00	02	00	00
00060128	E4	EC	00	00	46	72	6F	6D	3A	20	22	4D	69	63	72	6F
00060144	73	6F	66	74	20	4F	75	74	6C	6F	6F	6B	20	45	78	70
00060160	72	65	73	73	20	54	65	61	6D	22	20	3C	6D	73	6F	65
00060176	40	6D	69	63	72	6F	73	6F	66	74	2E	63	6F	6D	3E	0D
00060192	0A	54	6F	3A	20	22	61	6C	6C	65	6E	20	63	6F	78	22

....Ôê.....	
äì..From: "Micro	
soft Outlook Exp	
ress Team" <msoe	
@microsoft.com>.	
.To: "allen cox"	

Block1 (Current Offset)

- **0x0000EAD4 = 60116**

Block2 (Indicates whether deleted block or not)

- **0x00000200 = 512**

Block3 (Length of Data Block)

- **0x00000200 = 512**

Block4 (Next Offset)

- **0x0000ECE4 = 60644**

DIGITAL DETECTIVE

Data Block

00060112	B8	1A	03	00	D4	EA	00	00	00	02	00	00	00	02	00	00	¸...Ôê..........
00060128	E4	EC	00	00	46	72	6F	6D	3A	20	22	4D	69	63	72	6F	äì..From: "Micro
00060144	73	6F	66	74	20	4F	75	74	6C	6F	6F	6B	20	45	78	70	soft Outlook Exp
00060160	72	65	73	73	20	54	65	61	6D	22	20	3C	6D	73	6F	65	ress Team" <msoe
00060176	40	6D	69	63	72	6F	73	6F	66	74	2E	63	6F	6D	3E	0D	@microsoft.com>.
00060192	0A	54	6F	3A	20	22	61	6C	6C	65	6E	20	63	6F	78	22	.To: "allen cox"
00060208	20	3C	70	75	6C	61	75	40	70	69	74	63	61	69	72	6E	<pulau@pitcairn
00060224	2E	70	6E	3E	0D	0A	53	75	62	6A	65	63	74	3A	20	57	.pn>..Subject: W
00060240	65	6C	63	6F	6D	65	20	74	6F	20	4F	75	74	6C	6F	6F	elcome to Outloo
00060256	6B	20	45	78	70	72	65	73	73	20	36	0D	0A	44	61	74	k Express 6..Dat
00060272	65	3A	20	57	65	64	2C	20	39	20	4A	75	6C	20	32	30	e: Wed, 9 Jul 20
00060288	30	33	20	31	34	3A	32	31	3A	30	37	20	2B	31	32	30	03 14:21:07 +120
00060304	30	0D	0A	4D	49	4D	45	2D	56	65	72	73	69	6F	6E	3A	0..MIME-Version:
00060320	20	31	2E	30	0D	0A	43	6F	6E	74	65	6E	74	2D	54	79	1.0..Content-Ty
00060336	70	65	3A	20	74	65	78	74	2F	68	74	6D	6C	3B	0D	0A	pe: text/html;..
00060352	09	63	68	61	72	73	65	74	3D	22	69	73	6F	2D	38	38	.charset="iso-88

- **From: “Microsoft Outlook Express…”**
- **512 Bytes in Length**

DIGITAL DETECTIVE

Deleted Email Message

What happens when a message is deleted?

- Data Header Block (16 Byte)
  - Block2 & Block3 updated to show deleted
- Data Block (Up to 512 Bytes)
  - First FOUR bytes overwritten
  - UInt32 of previous data header block offset

DIGITAL DETECTIVE

Contact Details

Craig Wilson

craig.wilson@digital-detective.co.uk

www.digital-detective.co.uk

Digital Detective Group
PO Box 698
Folkestone
Kent
CT20 9FW
United kingdom

support@digital-detective.co.uk
+ 44 (0) 844 330 8892

Hours: Mon - Fri
0800 - 1800 GMT

+ 44 (0)20 3384 3587