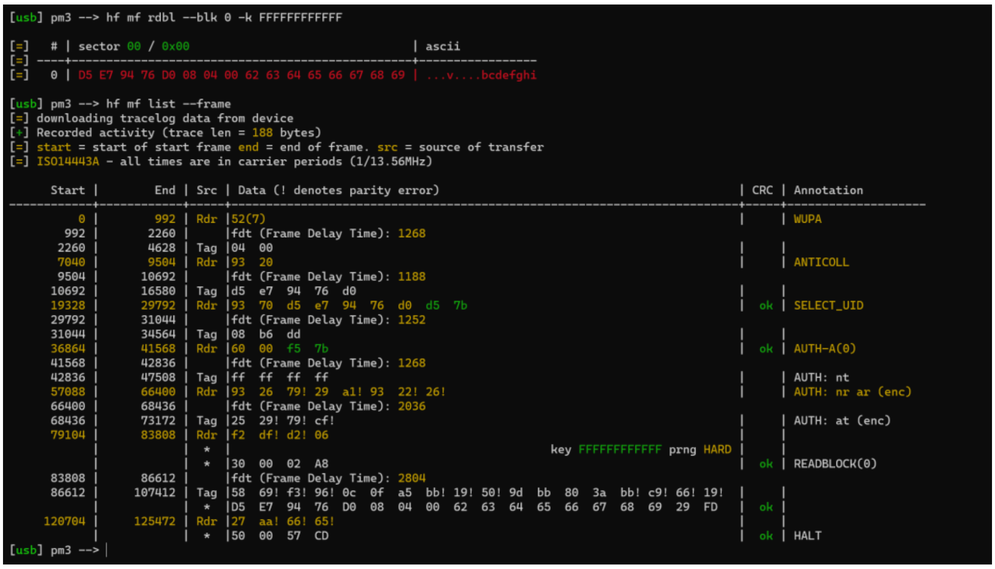
ISO/IEC 14443A FDT Timming and How To Reduce FDT

Introduction

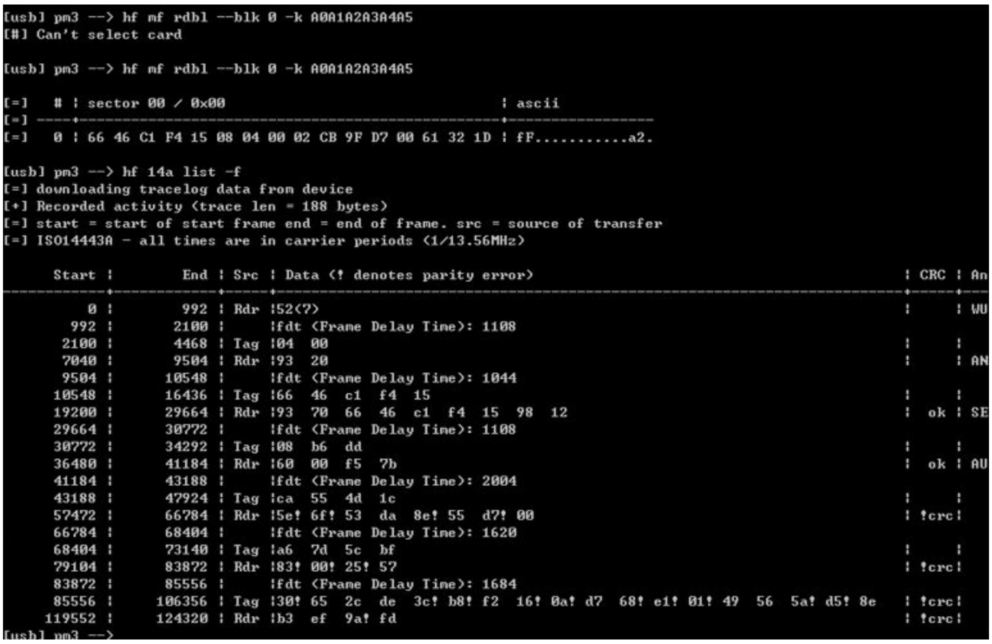
Many versions of the Chameleon, it's FDT is too long when it emulate Mifare-1, so some reader can't read or write it. I statisticsed some of them:

1. STM32xxx: ReadBlock's FDT --2804



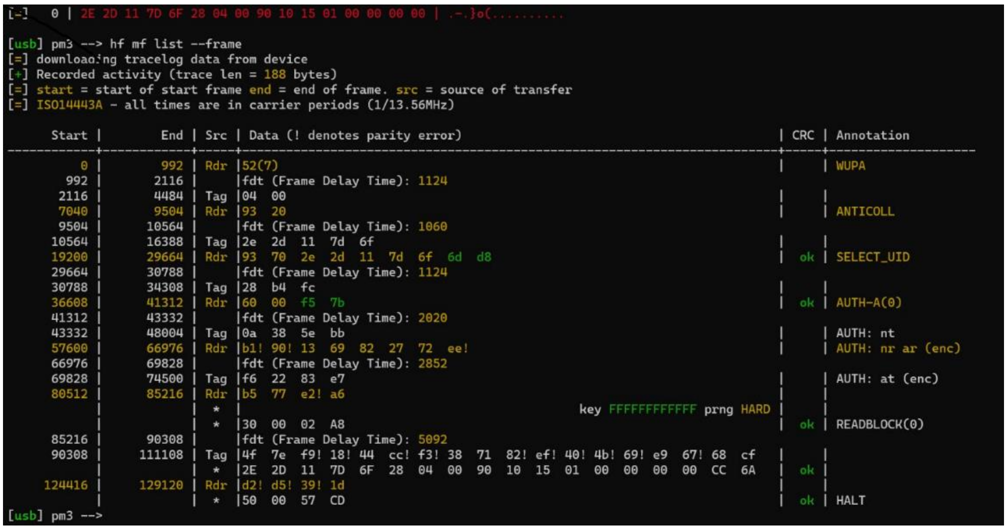
```
[usb] pm3 --> hf mf rdbl --blk 0 -k FFFFFFFFFFFF

[=]   # | sector 00 / 0x00                                | ascii
[=] ----+-------------------------------------------------+-----------------
[=]   0 | D5 E7 94 76 D0 08 04 00 62 63 64 65 66 67 68 69 | ...v....bcdefghi

[usb] pm3 --> hf mf list --frame
[=] downloading tracelog data from device
[+] Recorded activity (trace len = 188 bytes)
[=] start = start of start frame end = end of frame. src = source of transfer
[=] ISO14443A - all times are in carrier periods (1/13.56MHz)

      Start |        End | Src | Data (! denotes parity error)                                           | CRC | Annotation
------------+------------+-----+-------------------------------------------------------------------------+-----+--------------------
          0 |        992 | Rdr |52(7)                                                                    |     | WUPA
        992 |       2260 |     |fdt (Frame Delay Time): 1268
       2260 |       4628 | Tag |04  00                                                                   |     |
       7040 |       9504 | Rdr |93  20                                                                   |     | ANTICOLL
       9504 |      10692 |     |fdt (Frame Delay Time): 1188
      10692 |      16580 | Tag |d5  e7  94  76  d0                                                       |     |
      19328 |      29792 | Rdr |93  70  d5  e7  94  76  d0  d5  7b                                       |  ok | SELECT_UID
      29792 |      31044 |     |fdt (Frame Delay Time): 1252
      31044 |      34564 | Tag |08  b6  dd                                                               |     |
      36864 |      41568 | Rdr |60  00  f5  7b                                                           |  ok | AUTH-A(0)
      41568 |      42836 |     |fdt (Frame Delay Time): 1268
      42836 |      47508 | Tag |ff  ff  ff  ff                                                           |     | AUTH: nt
      57088 |      66400 | Rdr |93  26  79! 29  a1! 93  22! 26!                                          |     | AUTH: nr ar (enc)
      66400 |      68436 |     |fdt (Frame Delay Time): 2036
      68436 |      73172 | Tag |25  29! 79! cf!                                                          |     | AUTH: at (enc)
      79104 |      83808 | Rdr |f2  df! d2! 06                                                           |     |
            |            |  *  |                                          key FFFFFFFFFFFF prng HARD     |     |
            |            |  *  |30  00  02  A8                                                           |  ok | READBLOCK(0)
      83808 |      86612 |     |fdt (Frame Delay Time): 2804
      86612 |     107412 | Tag |58  69! f3! 96! 0c  0f  a5  bb! 19! 50! 9d  bb  80  3a  bb! c9! 66! 19!  |     |
            |            |  *  |D5  E7  94  76  D0  08  04  00  62  63  64  65  66  67  68  69  29  FD   |  ok |
     120704 |     125472 | Rdr |27  aa! 66! 65!                                                          |     |
            |            |  *  |50  00  57  CD                                                           |  ok | HALT
[usb] pm3 --> |
```

2. GP xxx: ReadBlock's FDT--1684



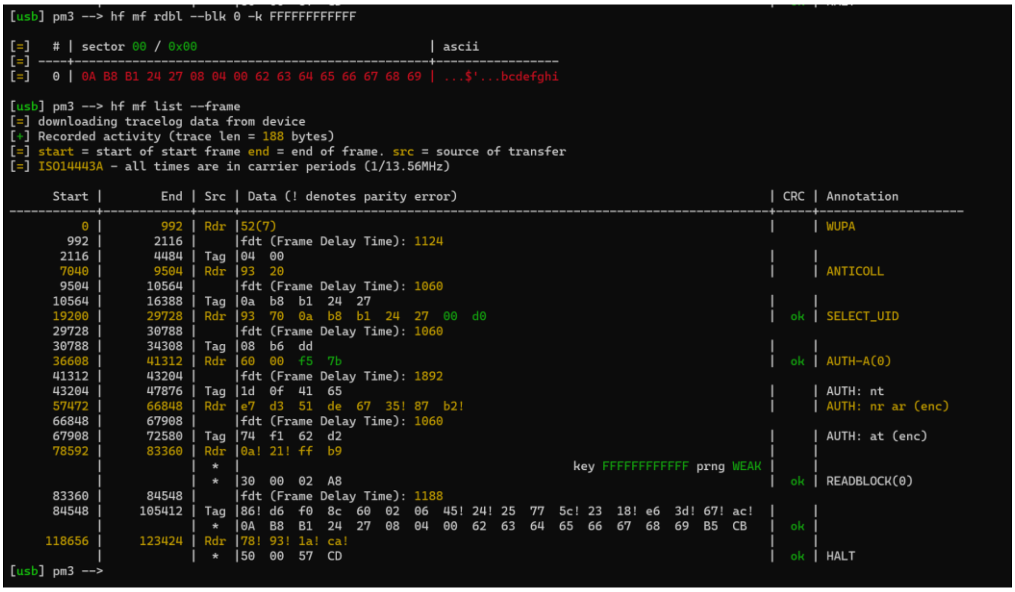
```
[usb] pm3 --> hf mf rdbl --blk 0 -k A0A1A2A3A4A5
[#] Can't select card

[usb] pm3 --> hf mf rdbl --blk 0 -k A0A1A2A3A4A5

[=]   # ¦ sector 00 / 0x00                                ¦ ascii
[=] ----+-------------------------------------------------+-----------------
[=]   0 ¦ 66 46 C1 F4 15 08 04 00 02 CB 9F D7 00 61 32 1D ¦ fF...........a2.

[usb] pm3 --> hf 14a list -f
[=] downloading tracelog data from device
[+] Recorded activity (trace len = 188 bytes)
[=] start = start of start frame end = end of frame. src = source of transfer
[=] ISO14443A - all times are in carrier periods (1/13.56MHz)

      Start ¦        End ¦ Src ¦ Data (! denotes parity error)                                           ¦ CRC ¦ An
------------+------------+-----+-------------------------------------------------------------------------+-----+---
          0 ¦        992 ¦ Rdr ¦52(7)                                                                    ¦     ¦ WU
        992 ¦       2100 ¦     ¦fdt (Frame Delay Time): 1108
       2100 ¦       4468 ¦ Tag ¦04  00                                                                   ¦     ¦
       7040 ¦       9504 ¦ Rdr ¦93  20                                                                   ¦     ¦ AN
       9504 ¦      10548 ¦     ¦fdt (Frame Delay Time): 1044
      10548 ¦      16436 ¦ Tag ¦66  46  c1  f4  15                                                       ¦     ¦
      19200 ¦      29664 ¦ Rdr ¦93  70  66  46  c1  f4  15  98  12                                       ¦  ok ¦ SE
      29664 ¦      30772 ¦     ¦fdt (Frame Delay Time): 1108
      30772 ¦      34292 ¦ Tag ¦08  b6  dd                                                               ¦     ¦
      36480 ¦      41184 ¦ Rdr ¦60  00  f5  7b                                                           ¦  ok ¦ AU
      41184 ¦      43188 ¦     ¦fdt (Frame Delay Time): 2004
      43188 ¦      47924 ¦ Tag ¦ca  55  4d  1c                                                           ¦     ¦
      57472 ¦      66784 ¦ Rdr ¦5e! 6f! 53  da  8e! 55  d7! 00                                           ¦ !crc¦
      66784 ¦      68404 ¦     ¦fdt (Frame Delay Time): 1620
      68404 ¦      73140 ¦ Tag ¦a6  7d  5c  bf                                                           ¦     ¦
      79104 ¦      83872 ¦ Rdr ¦83! 00! 25! 57                                                           ¦ !crc¦
      83872 ¦      85556 ¦     ¦fdt (Frame Delay Time): 1684
      85556 ¦     106356 ¦ Tag ¦30! 65  2c  de  3c! b8! f2  16! 0a! d7  68! e1! 01! 49  56  5a! d5! 8e   ¦ !crc¦
     119552 ¦     124320 ¦ Rdr ¦b3  ef  9a! fd                                                           ¦ !crc¦
[usb] pm3 -->
```

3. ChameleonUltra: ReadBlock's FDT --5092



```
[=]   0 | 2E 2D 11 7D 6F 28 04 00 90 10 15 01 00 00 00 00 | .-.}o(..........

[usb] pm3 --> hf mf list --frame
[=] downloaa:ng tracelog data from device
[+] Recorded activity (trace len = 188 bytes)
[=] start = start of start frame end = end of frame. src = source of transfer
[=] ISO14443A - all times are in carrier periods (1/13.56MHz)

     Start |        End | Src | Data (! denotes parity error)                                          | CRC | Annotation
-----------+------------+-----+------------------------------------------------------------------------+-----+--------------------
         0 |        992 | Rdr |52(7)                                                                   |     | WUPA
       992 |       2116 |     |fdt (Frame Delay Time): 1124
      2116 |       4484 | Tag |04  00                                                                  |     |
      7040 |       9504 | Rdr |93  20                                                                  |     | ANTICOLL
      9504 |      10564 |     |fdt (Frame Delay Time): 1060
     10564 |      16388 | Tag |2e  2d  11  7d  6f                                                      |     |
     19200 |      29664 | Rdr |93  70  2e  2d  11  7d  6f  6d  d8                                      |  ok | SELECT_UID
     29664 |      30788 |     |fdt (Frame Delay Time): 1124
     30788 |      34308 | Tag |28  b4  fc                                                              |     |
     36608 |      41312 | Rdr |60  00  f5  7b                                                          |  ok | AUTH-A(0)
     41312 |      43332 |     |fdt (Frame Delay Time): 2020
     43332 |      48004 | Tag |0a  38  5e  bb                                                          |     | AUTH: nt
     57600 |      66976 | Rdr |b1! 90! 13  69  82  27  72  ee!                                         |     | AUTH: nr ar (enc)
     66976 |      69828 |     |fdt (Frame Delay Time): 2852
     69828 |      74500 | Tag |f6  22  83  e7                                                          |     | AUTH: at (enc)
     80512 |      85216 | Rdr |b5  77  e2! a6                                                          |     |
           |            |  *  |                                              key FFFFFFFFFFFF prng HARD|     |
           |            |  *  |30  00  02  A8                                                          |  ok | READBLOCK(0)
     85216 |      90308 |     |fdt (Frame Delay Time): 5092
     90308 |     111108 | Tag |4f  7e  f9! 18! 44  cc! f3! 38  71  82! ef! 40! 4b! 69! e9  67! 68  cf |     |
           |            |  *  |2E  2D  11  7D  6F  28  04  00  90  10  15  01  00  00  00  00  CC  6A |  ok |
    124416 |     129120 | Rdr |d2! d5! 39! 1d                                                          |     |
           |            |  *  |50  00  57  CD                                                          |  ok | HALT
[usb] pm3 -->
```

4. Mifare-1 Card: ReadBlock's FDT--1188

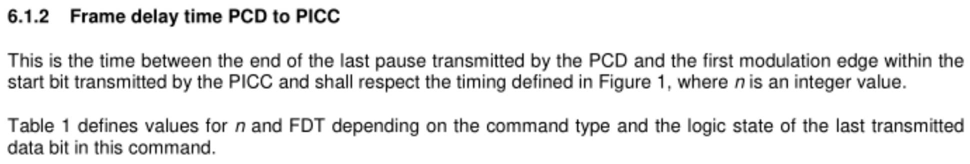


```
[usb] pm3 --> hf mf rdbl --blk 0 -k FFFFFFFFFFFF

[=]   # | sector 00 / 0x00                                | ascii
[=] ----+-------------------------------------------------+-----------------
[=]   0 | 0A B8 B1 24 27 08 04 00 62 63 64 65 66 67 68 69 | ...$'...bcdefghi

[usb] pm3 --> hf mf list --frame
[=] downloading tracelog data from device
[+] Recorded activity (trace len = 188 bytes)
[=] start = start of start frame end = end of frame. src = source of transfer
[=] ISO14443A - all times are in carrier periods (1/13.56MHz)

     Start |        End | Src | Data (! denotes parity error)                                          | CRC | Annotation
-----------+------------+-----+------------------------------------------------------------------------+-----+--------------------
         0 |        992 | Rdr |52(7)                                                                   |     | WUPA
       992 |       2116 |     |fdt (Frame Delay Time): 1124
      2116 |       4484 | Tag |04  00                                                                  |     |
      7040 |       9504 | Rdr |93  20                                                                  |     | ANTICOLL
      9504 |      10564 |     |fdt (Frame Delay Time): 1060
     10564 |      16388 | Tag |0a  b8  b1  24  27                                                      |     |
     19200 |      29728 | Rdr |93  70  0a  b8  b1  24  27  00  d0                                      |  ok | SELECT_UID
     29728 |      30788 |     |fdt (Frame Delay Time): 1060
     30788 |      34308 | Tag |08  b6  dd                                                              |     |
     36608 |      41312 | Rdr |60  00  f5  7b                                                          |  ok | AUTH-A(0)
     41312 |      43204 |     |fdt (Frame Delay Time): 1892
     43204 |      47876 | Tag |1d  0f  41  65                                                          |     | AUTH: nt
     57472 |      66848 | Rdr |e7  d3  51  de  67  35! 87  b2!                                         |     | AUTH: nr ar (enc)
     66848 |      67908 |     |fdt (Frame Delay Time): 1060
     67908 |      72580 | Tag |74  f1  62  d2                                                          |     | AUTH: at (enc)
     78592 |      83360 | Rdr |0a! 21! ff  b9                                                          |     |
           |            |  *  |                                              key FFFFFFFFFFFF prng WEAK|     |
           |            |  *  |30  00  02  A8                                                          |  ok | READBLOCK(0)
     83360 |      84548 |     |fdt (Frame Delay Time): 1188
     84548 |     105412 | Tag |86! d6  f0  8c  60  02  06  45! 24! 25  77  5c! 23  18! e6  3d! 67! ac! |     |
           |            |  *  |0A  B8  B1  24  27  08  04  00  62  63  64  65  66  67  68  69  B5  CB |  ok |
    118656 |     123424 | Rdr |78! 93! 1a! ca!                                                         |     |
           |            |  *  |50  00  57  CD                                                          |  ok | HALT
[usb] pm3 -->
```

5.

Timming

Timming is defined in ISO/IEC 14443-3 and 14443-2:



6.1.2 Frame delay time PCD to PICC

This is the time between the end of the last pause transmitted by the PCD and the first modulation edge within the start bit transmitted by the PICC and shall respect the timing defined in Figure 1, where *n* is an integer value.

Table 1 defines values for *n* and FDT depending on the command type and the logic state of the last transmitted data bit in this command.

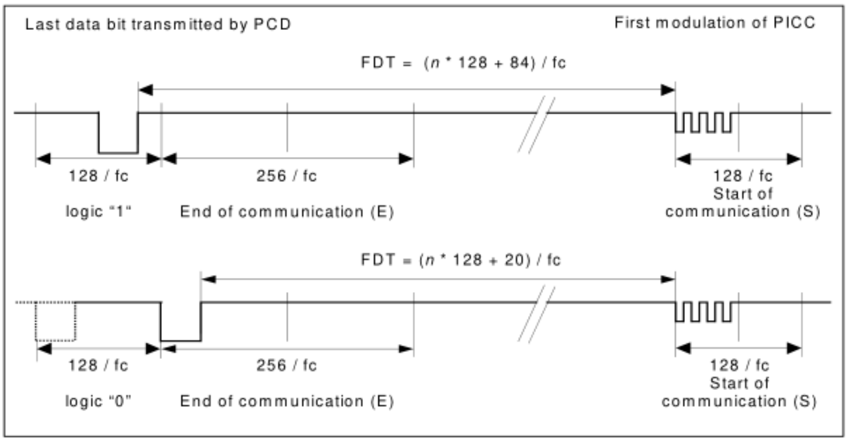
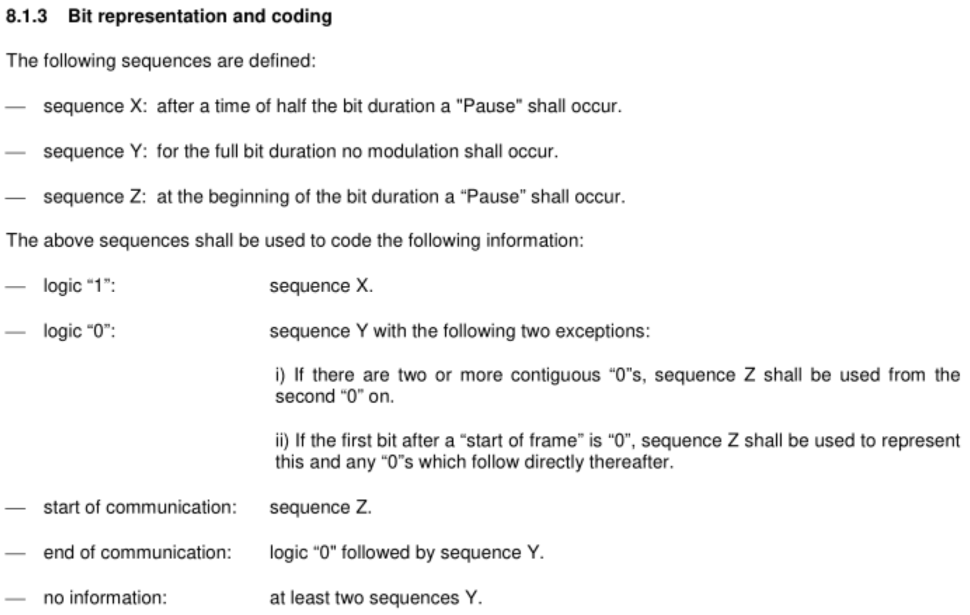


Figure 1 — Frame delay time PCD to PICC

If the last data bit is "logic 1", FDT=(n*128+84)/fc
If the last data bit is "logic 0", FDT=(n*128+20)/fc

As a matter of fact, FDT is between EOF and SOF, So:
If the last data bit is "logic 1", FDTa = FDT-256/fc-32/fc = (n*128-204)/fc
If the last data bit is "logic 0", FDTa = FDT-(256/fc-32/fc) = (n*128-204)/fc
Note: 32/fc is a "Pause" was defined in 14443-2



8.1.3 Bit representation and coding

The following sequences are defined:

- sequence X: after a time of half the bit duration a "Pause" shall occur.
- sequence Y: for the full bit duration no modulation shall occur.
- sequence Z: at the beginning of the bit duration a "Pause" shall occur.

The above sequences shall be used to code the following information:

- logic "1": sequence X.
- logic "0": sequence Y with the following two exceptions:

  i) If there are two or more contiguous "0"s, sequence Z shall be used from the second "0" on.

  ii) If the first bit after a "start of frame" is "0", sequence Z shall be used to represent this and any "0"s which follow directly thereafter.
- start of communication: sequence Z.
- end of communication: logic "0" followed by sequence Y.
- no information: at least two sequences Y.

Now, Calculate n of Mifare-1 Emulator:

1. STM32xxx: ReadBlock's FDT—2804, n=9+(2804-1268)/128=21
2. GP xxx: ReadBlock's FDT—1684, n=9+(1684-1044)/128=14

3. ChameleonUltra: ReadBlock's FDT—5092, n=9+(5092-1124)/128=40
4. Mifare-1 Card: ReadBlock's FDT—1188, n=9+(1188-1060)/128=10

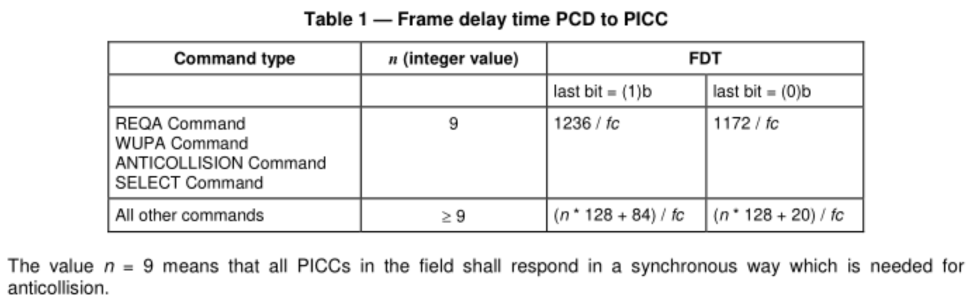


Table 1 — Frame delay time PCD to PICC

Command type	*n* (integer value)	FDT	
		last bit = (1)b	last bit = (0)b
REQA Command WUPA Command ANTICOLLISION Command SELECT Command	9	1236 / *fc*	1172 / *fc*
All other commands	≥ 9	(*n* * 128 + 84) / *fc*	(*n* * 128 + 20) / *fc*

The value *n* = 9 means that all PICCs in the field shall respond in a synchronous way which is needed for anticollision.

Reduce FDT

1. Deal Command after the last "Pause" instead of EOF. This method of operation will save (256±32)/fc
2. Faster processor.
   i. ChameleonUltra: 64MHz, FDT--40
   ii. STM32xxx: 135.6MHz, FDT--21
   iii. GP xxx: 250MHz, FDT--14
   iv. NFC Emulator V1.1: FDT--13