



TIMDOWS

Using a mobile phone to clone a MIFARE card

Posted on *June 20, 2016* by *Tim Theeuwes*

Overview

1. Why?
2. MIFARE Classic?
3. MIFARE Ultralight?
4. Reading and capturing contents of the card
5. About this manufacturer block (Sector 0 – Block 0)
6. The UID thing that messes with my head
7. Writing a 4Byte dump on a different card

Why?

The MIFARE NFC card is used in many

environments. I got a trash card, a card that I have to use to open the underground trash bin, that I want to clone. As the replacement costs for a lost / broken card is €10 a clone would be a good investment.



By holding the card in front of the reader, I can open the trashcan, ohw happy days.

In my search for information, I found the following pages interesting:

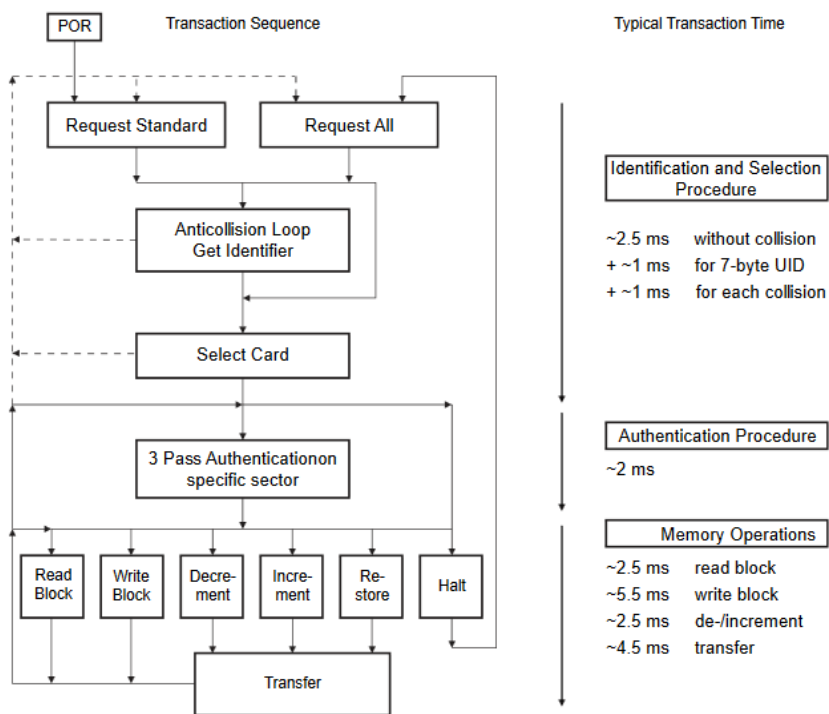
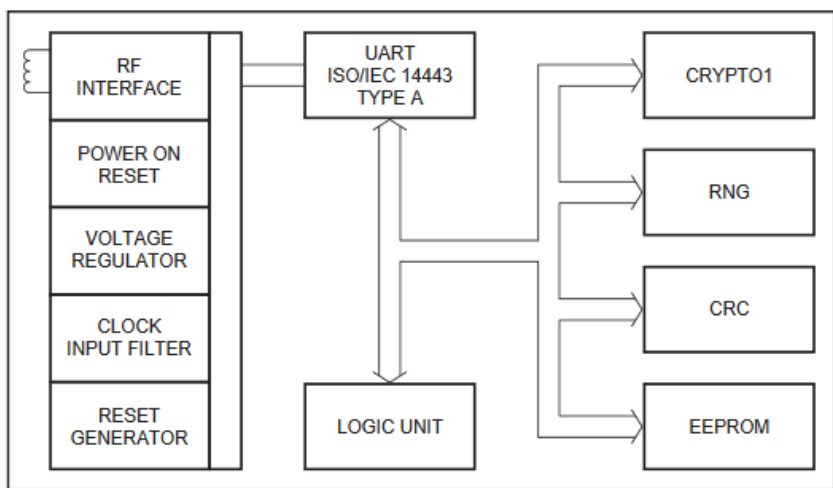
- <https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf>
- <http://www.proxmark.org/forum/viewtopic.php?id=1535>

- <http://www.shopnfc.it/en/content/7-nfc-device-compatibility>
- <http://publications.icaria.de/mct/releases/2>
- http://www.scnf.org.uk/smartstore/4-7_B_ID_Questions_Answeres_V8.pdf
- http://cache.nxp.com/documents/data_sheet/pspll=1
- <https://learn.adafruit.com/adafruit-pn532-rfid-nfc/mifare>
- [http://www.nxp.com/documents/data_sheet/\(Ultralight / 7Byte UID\)](http://www.nxp.com/documents/data_sheet/(Ultralight%20/7Byte%20UID))
- <https://www.kismetwireless.net/code-old/svn/hardware/kisbee-02/firmware/drivers/rf/pn532/helpers/>
- <http://stackoverflow.com/questions/21700on-nfc-tags-truly-unique-cloneable>
- <http://stackoverflow.com/questions/28409functionality-of-host-card-emulation-in-android>
- <https://store.rysgcc.com/products/new-proxmark3-kit>

MIFARE Classic?

Some informational dumps:

- 16 bits CRC per block
- Anticollision loop
- 1kB or 4kB of EEPROM
- CRYPTO1 stream cipher (**mjah, close to zero security**)
- Manufacturer / data / value blocks

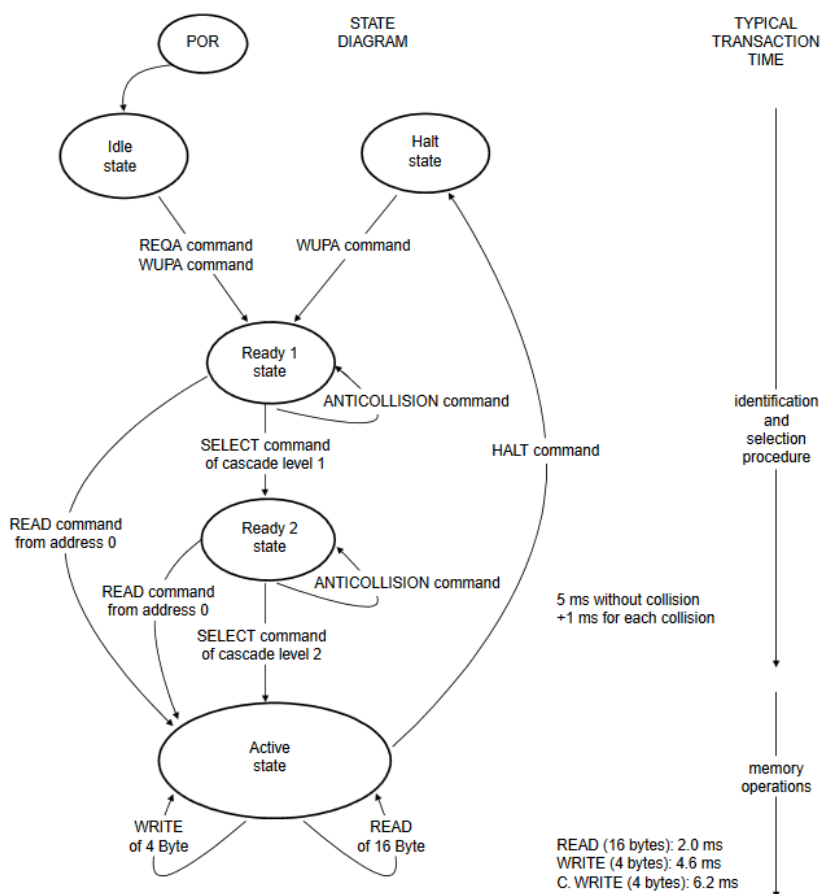
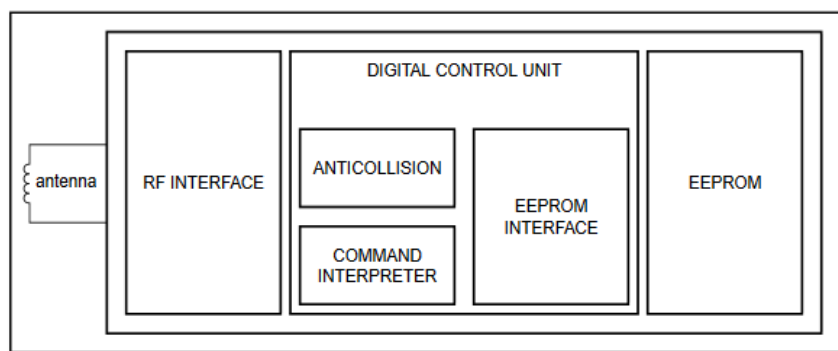


001a0024

MIFARE Ultralight?

MiFare Ultralight cards typically contain 512 bits (64 bytes) of memory, including 4 bytes (32-bits) of OTP (One Time Programmable) memory where the individual bits can be written but not erased.

MiFare Ultralight cards have a **7-byte UID** that uniquely identifies the card.




Reading and capturing contents of the card

After some investigation I noticed that my Samsung mobile phone has a NFC reader.

I used the <https://github.com/ikarus23/MifareClassicTool> on my Samsung S6, the the result was a bit disappointing:

Tag Info



This device
does not
support Mifare
Classic!

READ MORE...

Generic Info

UID:
049889CA3E2D80 (7 byte, CL2)

RF Technology:
ISO/IEC 14443, Type A

ATQA:
0044

SAK:
08

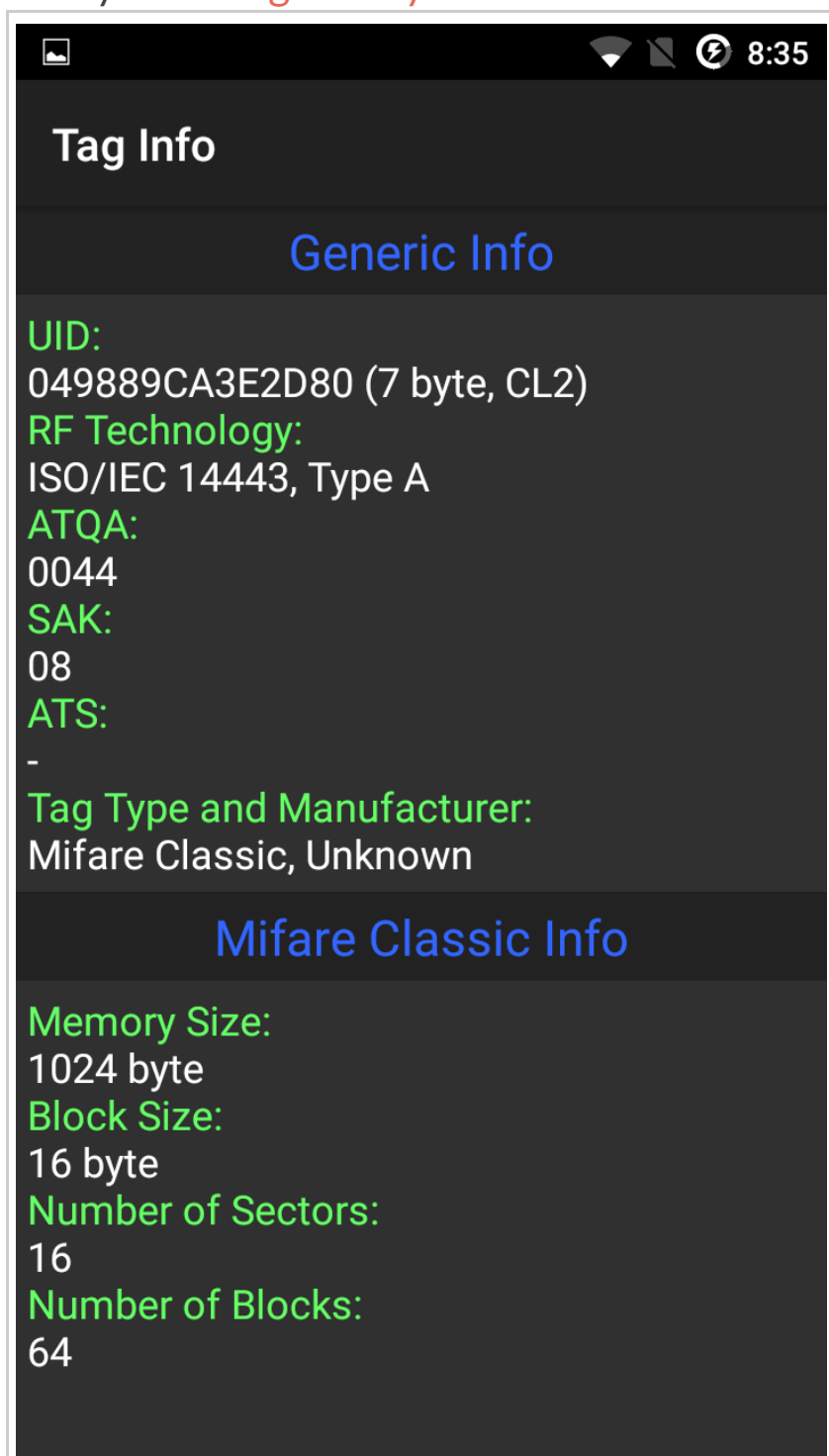
ATS:
-

Tag Type and Manufacturer:
Mifare Classic, Unknown

On a Samsung S6


After some **googling**, I found that the hardware chip, used to read NFC tags, was just not on my S6.

But it showed that it was on an old S3, that I had laying around, it just worked like a charm on my **Samsung Galaxy S3 with Android 6**:



On a Samsung S3

In order to read the contents of the card, the MIFARE card can be read easily.

8:47

Map Keys to Sectors

Create Map for Sectors: [All](#) CHANGE

Choose some key file(s):

SELECT ALL SELECT NONE

☐ UID_049889CA3E2D80

☒ extended-std.keys

☒ std.keys

New tag found (UID: 049889CA3E2D80)

Key Mapping Progress:

CANCEL START MAPPING AND READ TAG

Use the supplied key sets and start mapping and read tag



8:47

Read Tag

Reading tag...
(Don't remove tag)



Pom pie dom...



8:48

Dump Editor (UID: 0...



Sector: 0

```
049889CA3E2D80884400C20000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFF078069FFFFFFFFFFFF
```

Sector: 1

```
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFF078069FFFFFFFFFFFF
```

Sector: 2

```
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFF078069FFFFFFFFFFFF
```

Sector: 3

```
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFF078069FFFFFFFFFFFF
```

Sector: 4

```
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
```

Caption: ([Update Colors](#))

[UID & ManufInfo](#) | [ValueBlock](#) | [KeyA](#) | [KeyB](#) | [ACs](#)

Detailed information about every sector on the card (if any data would be present except the UID)

So the only interesting information is in Sector: 0, also called the manufacturer block. I also noticed that the UID was 7Byte, making it a MIFARE Ultralight card grrrrrrr...

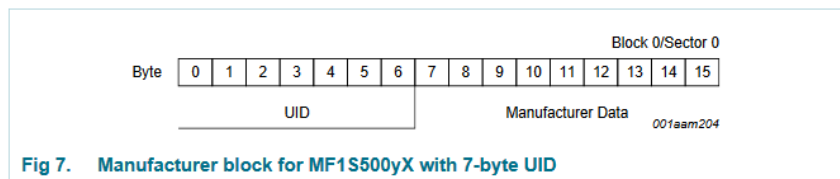
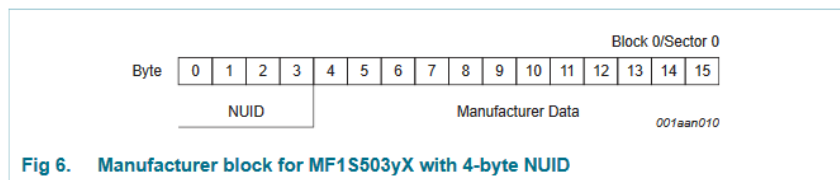
About this manufacturer block (Sector 0 – Block

This part of the card is the only interesting part, as no other data is written to any sector/block as far as I can see.

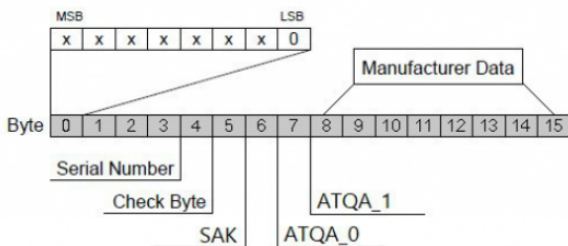
In order to understand the difference between a 4Byte and 7Byte UID (i.e. MIFARE Classic vs MIFARE Ultralight), I have added some pictures:

Manufacturer block

This is the first data block (block 0) of the first sector (sector 0). It contains the IC manufacturer data. This block is programmed and write protected in the production test. The manufacturer block is shown in [Figure 6](#) and [Figure 7](#) for the 4-byte NUID and 7-byte UID version respectively.



A more detailed picture explains some more information is included after the serial number on block 0:



$$\text{Check Byte} = \text{SN0} \wedge \text{SN1} \wedge \text{SN2} \wedge \text{SN3}$$

SAK = 0x08

ATQA 0 = 0x04

ATQA 1 = 0x00

Examples of the wrong and right values for sector 0 block 0:

[illegible]

A more detailed picture of the 7byte UID:

Memory organization

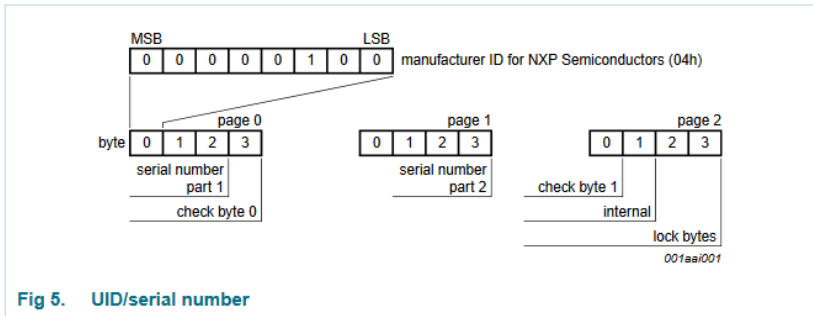
The 512-bit EEPROM memory is organized in 16 pages with 4 bytes per page. In the erased state the EEPROM cells are read as logic 0, in the written state as logic 1.

Table 5. Memory organization

Page address		Byte number			
Decimal	Hex	0	1	2	3
0	00h	serial number			
1	01h	serial number			
2	02h	serial number	internal	lock bytes	lock bytes
3	03h	OTP	OTP	OTP	OTP
4 to 15	04h to 0Fh	user memory			

UID/serial number

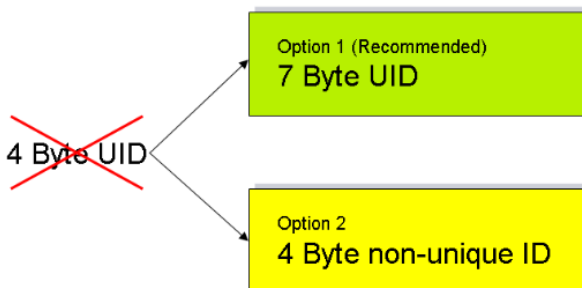
The unique 7-byte serial number (UID) and its two check bytes are programmed into the first 9 bytes of memory covering page addresses 00h, 01h and the first byte of page 02h. The second byte of page address 02h is reserved for internal data. These bytes are programmed by the IC manufacturer and because of the security requirements are write protected.



The UID thing that messes with my head

As you could see on my tag info, the UID on my trash card is 7 byte, so it works a bit different than the 4 byte one.

In Q2 2010 NXP customers have been informed of important updates on the IDs of MIFARE Classic and related products.



Unique 4 Byte IDs will be discontinued. Customers will have the choice to purchase either products with unique 7 Byte IDs (our recommended option) or 4 Byte IDs, which are not globally unique any more.
This document lists common questions and our answers on the topic.

The **different types of UID** are explained as follows:

ISO/IEC 14443 Type A defines a Unique Identifier to be used for card selection and activation. The standard defines single, double and triple size UIDs which correspondingly consist of 4, 7 and 10 Byte.

What is the difference between a 4 Byte UID and a 4 Byte ID?

A 4 byte UID is an identifier which has been assigned by the card manufacturer using a controlled database. This database ensures that a single identifier is not used twice. In contradiction, a 4 byte ID is an identifier which may be assigned to more than one contactless chip over the production time of a product so that more than one card with the same identifier may be deployed into one particular contactless system.

Writing a 4Byte dump on a different card

As it is just cool to write a cards dump back, I have found a 4Byte UID MIFARE Classic 1kB card.

8:11

Tag Info

Generic Info

UID:
DEDEDA77 (4 byte)

RF Technology:
ISO/IEC 14443, Type A

ATQA:
0004

SAK:
08

ATS:
-

Tag Type and Manufacturer:
MIFARE Classic 1k, NXP

("Tag Type and Manufacturer" might be wrong.
See "Help and Info" for more information.)

Mifare Classic Info

Memory Size:
1024 byte

Block Size:
16 byte

Number of Sectors:
16

Number of Blocks:
64

Card information



Dump Editor (UID: D...

Sector: 0

DEDEDA77AD880400C847002000000014
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF

Caption: ([Update Colors](#))
UID & ManufInfo | ValueBlock | KeyA | KeyB | ACs

Content of Sector: 0

Ebay has a solution for everyting. UID writable MIFARE Classic cards. These cards make it possible to write Sector 0 – block 0 (i.e. the manufacturer block).





Write Tag



Write Block



Write Dump (Clone)

Write a dump (or some sectors of it) to a tag. Blocks containing unknown data (---) will be skipped!

SELECT DUMP



Show Options



Use these Access Conditions for all sectors:



08778F



Advanced: Enable writing to manufacturer block



Factory Format



Incr./Decr. Value Block

Write tag and enable writing to manufacturer block



8:12



Write Sectors

Select the sectors you want to write:

SELECT ALL

SELECT NONE



Sector 0

CANCEL

OK

Select what to write from the dump



Map Keys to Sectors

Create Map for Sectors: 0 - 0 [CHANGE](#)

Choose some key file(s):

[SELECT ALL](#)

[SELECT NONE](#)

☐ UID_049889CA3E2D80

☒ extended-std.keys

☒ std.keys

Key Mapping Progress:

[CANCEL](#)

[START MAPPING AND WRITE DUMP](#)

Click start mapping and write dump

Compare the two tags, only the SAK is different, I hope that will still work in a real live situation

10:53

Tag Info

Generic Info

UID:

DEDEDA77 (4 byte)

RF Technology:

ISO/IEC 14443, Type A

ATQA:

0004

SAK:

88

ATS:

-

Tag Type and Manufacturer:

MIFARE Classic 1K, Infineon

("Tag Type and Manufacturer" might be wrong.
See "Help and Info" for more information.)

Mifare Classic Info

Memory Size:

1024 byte

Block Size:

16 byte

Number of Sectors:

16

Number of Blocks:

64

Cloned card

Tag Info

Generic Info

UID:

DEDEDA77 (4 byte)

RF Technology:

ISO/IEC 14443, Type A

ATQA:

0004

SAK:

08

ATS:

-

Tag Type and Manufacturer:

MIFARE Classic 1k, NXP

("Tag Type and Manufacturer" might be wrong.
See "Help and Info" for more information.)

Mifare Classic Info

Memory Size:

1024 byte

Block Size:

16 byte

Number of Sectors:

16

Number of Blocks:

64

Original card

← Preventing CSRF in ASP.NET Core
combined with AngularJS

Storing passwords in a
database with the
IDataProtector in
ASP.NET Core 1.0 →

46 thoughts on “Using a mobile phone to clone a MIFARE card”



Luuk Wuijster says:

December 4, 2016 at 22:41

Is het ook mogelijk om een app te gebruiken om het nfc te broadcasten? Dus dat je je telefoon gewoon als kaart gebruikt.

Reply



Tim Theeuwes says:

January 9, 2017 at 23:02

Een mobiele telefoon zou dat moeten kunnen (draadloos betalen met je NFC chip tegen een

pinapparaat aan).

Maar niet in de app gevonden die ik zelf gebruik.

Een proxmark3 aanschaffen zou echt top zijn:

<https://store.rysgcc.com>

Reply



Ruben says:

October 19, 2017 at 10:31

Is afhankelijk van de reader.

Sommige readers ondersteunen enkel passieve kaarten, andere ook actieve (emulatie).

Reply

Pingback: [Díl 19. – Pražská Lítačka – Kafemlejnec.TV](#)



Rick says:

March 28, 2017 at 23:21

Dit is misschien een domme vraag, maar is het mogelijk om een Dump van een kaart met een 7 byte UID te schrijven op kaart met een 4 Byte UID?

Reply



Tim says:

April 19, 2017 at 15:15

Dit is mij nog niet gelukt.

Wat ik zoek zijn 7 byte UID cards die changeable block/sector 0 hebben.

Als iemand weet waar ik deze kan halen....dan hoor ik dat heel graag

Reply



Martijn says:

June 21, 2017 at 22:15

Heb je die al gevonden?

Reply



Alexandra says:

June 27, 2017 at 13:44

Hi Tim,

Mooi werk. Ik was het zelf ook al aan het uitvogelen toen ik jouw pagina tegenkwam. Ik heb deze gevonden met 7 byte UID:

<https://www.amazon.co.uk/Genuine-Philips-Mifare-Cards-Byte/dp/B016DQBO2W> maar ik weet niet of het merk iets

uitmaakt.

Reply



Jared says:

June 8, 2017 at 01:13

so did it work?

Reply



Nacho says:

July 19, 2017 at 14:30

Hi, so interesting.

i have a question: i'd like to emulate de dump with the mobile.

do you think is possible?

i have been looking for an app in google play but I didnt find anything yet.

i would like to emulate my card access.

thanks a lot

Reply



rutg798 says:

August 16, 2017 at 11:58

Is het je ooit gelukt de afval pas te

copyeren, ik kan tot nu toe geen
herschrijfbaar 7 bytes UID card vinden.

Reply



harry says:

August 23, 2017 at 12:11

het lukt me wel met een jailbreak
iphone 6.

op mijn s7 edge ook.

je moet pad laden dan die bytes fixen.
staan op Google.

pas is je adres daarom staan die vast. op
pas.

via fix kan je deze laden

Reply



Remon Sami says:

October 31, 2017 at 11:59

hoi Harry

graag meer info a.u.bbyte fixen
??

link naar site , link naar software,
waar kun je pas kopen ??

remon

Reply



Ray says:

September 13, 2017 at 07:02

Sorry maar het is nooit gelukt de afval pas te copyeren, ik heb zak van 10 UID (sleutelhanger) en jouwe structie de UID is 7byte en sector 0 writeble de probleem is niet schrijf op sector 0 maar A/B key , ik heb CRC error (key not match) dus ik mess stapje waar de key decoded !!??
graag help ik heb nog meer UID besteld van china en ik hope meer info van je .
Ray

Reply



Ray says:

September 13, 2017 at 07:07

kort corectie :BCC error (key not match)

Reply



kristan oppersma says:

September 26, 2017 at 13:15

Is het mogelijk om de data op de kaart zelf aan te passen

Reply



max says:

September 30, 2017 at 13:06

“only the SAK is different, I hope that will still work in a real live situation”

Did you get it working?

Reply



Keith says:

October 1, 2017 at 03:49

I am getting a “BCC of block 0 is not valid” error when trying to write block 0.

Reply



Keith says:

October 20, 2017 at 06:55

I don't get all the stuff you're staying about Figure 6 and Figure 7, it's not well explained.

I used the app to try to copy a fob, and it seems to have corrupted each copy so now it's unreadable.

Reply



Ole says:

December 11, 2017 at 13:34

i have the exact same blue keyring nfcs.

but sector 0 is not writable, wtf.

Reply



Dave5568 says:

December 16, 2017 at 14:55

Waarom moeilijk doen als het makkelijk kan ?

Ik heb de kaart met mijn mobieltje (Sony) gekopieerd en simuleer nu voortaan de kaart ! (20 seconde app downloaden en 1 sec. kopie, gelijk werken)

Bij mij thuis hebben we dus allemaal ons eigen mobieltje en toch altijd "dezelfde" kaart bij ons :))

(Nooit meer je kaart kwijt of niet bij je !)

Mijn advies: nooit je kaart uitlenen (of je mobiel laten hacken) anders kunnen ze op jou naam lekker afval dumpen ! !

Reply



Henk says:

December 20, 2017 at 23:05

Welke app heb je dit mee gedana?

Reply



Leo2489 says:

January 15, 2018 at 23:06

Dave5568 met welke app simuleer je de kaart?

Reply



JJ says:

December 17, 2017 at 13:01

Interessant Tim. Vandaag begonnen met checken hoe ik eenvoudig een vuilcontainer card kan kopiëren voor alle gezinsleden. Zou een device zoals dit werken?

<https://www.aliexpress.com/item/English-Rfid-NFC-Copier-Reader-Writer-Cloner-Copy-10-Frequency-Programmer-5Pcs-125khz-EM4305-Keyfobs-5Pcs/32814673337.html>

Reply



Henk says:

December 18, 2017 at 12:03

Welke Android app is hiervoor

gebruikt?

Reply



Henk says:

December 18, 2017 at 12:09

Laat maar zitten, ik heb niet goed gekeken zie ik al.

Reply

Pingback: [!2ke](#)

Pingback: [루비게임 엘리트게임 루비게임주소](#)



Alinkacvh says:

March 16, 2018 at 00:48

[URL=<http://porno-besik.net/>]
[IMG]<http://s4.pic4you.ru/y2018/02-13/12461/6183409-thumb.jpeg>[/IMG]
[/URL]

Здоровый босс дрючит в
сраку
шикарную секретаршу азитку на
своем столе. Отправив всех по
домам,
он пригласил телку в личный
кабинет, натянул презик и
очень больно выебал ее в очень

узкую

попку на собственном столе...

Смотрите

[url=https://42.herber.pl/714265]азиатки

секретарши порно[/url]

и наслаждайтесь отличным

анальным трахом с азиатской

секретаршей...

Reply



Thomasinfed says:

March 20, 2018 at 12:48

Living in France is one thing desired by many individuals. If you want to live in France then you have to get French property. You can read the advertisement section of the newspapers which has the section of houses for sale in France. After making a suitable choice, you should research about the properties for sale in France. French property is now a days very much wanted also.

If you want to live in France and spend your life there you should select a proper house. French property is not cheap and you need to make a major investment. You must also know about

the properties for sale in France at various locations. The houses for sale in France come in different prices depending on the location

Reply

Pingback: [검증사이트](#)



Inku says:

March 29, 2018 at 06:41

I tried with one of those UID writable cards, and Mifare Classic Tools gave me an error.

Maybe changing a phone would work? I've heard that Android actually doesn't support the command of writing a UID.

Reply



ikarus says:

April 5, 2018 at 20:37

Hi Tim, great write up!

Maybe you want to update the post because your assumptions about Mifare Classic vs. Mifare Ultralight are wrong. Even the tag with the 7 byte UID is a Mifare Classic tag. There are Mifare Classic tags with 4 or 7 byte UIDs! Check out section 1.3 of the

datasheet

http://www.nxp.com/documents/data_sheet/MF1S50YYX.pdf Also, MCT app can only read Mifare Classic tags and not Mifare Ultralight.

Reply



MartinFum says:

May 1, 2018 at 17:05

Hi All im newbie here. Good post! Thx!
Love your stories!

Reply

Pingback: [java](#)



Mathias says:

May 20, 2018 at 12:43

Good article. Where can I get UID /
Block 0 changable cards with a 7byte
UID?

Reply



RobertJorgo says:

May 21, 2018 at 13:07

Do you love teen hardcore sex? Or
when young girls suck cocks until guys
cum? Or you like crazy dorm actions

with drunk students drink beer and fuck at parties? All of these and much more you will see on this site 18-teen-porn.com. All kinds of teen porn with beautiful girls. Big tits, small tits, shaved and hairy pussies penetrated by cocks, skilled mouths suck dicks and sure with lots of sperm! Have fun with our teen HD videos!

With a huge variety of quality teen porn, this top notch tube is sure to grant the best adult experiences online. Once you step inside, you get to see a lot of niches and plenty of available HD videos, all carefully selected and with daily updates to keep you aroused. Enjoy an impressive number of amateur teen porn, cam girls gone wild and a whole lot of other categories in one single and very impressive collection of teen videos. Each comes with HD image and the tube's fantastic streaming speed, something which will surely improve your adult experiences. Only rate teen porn and quality action, girls on fire in the mood to spin large inches of cock into each of their tiny love holes. Barely legal hotties working cock like true pornstars and a huge number of amateurs trying to make it into the

big league. Either way you like your porn, this awesome teen tube will provide young flesh and spicy action at any hour. Only exclusive teen porn which is not available on other movie sites or tubes. Quality content with premium action and girls to die for. Enjoy such fantastic content on a tube that's set to become number one, a tube which will make your delight with a very large variety of niches. Never mind browsing for teen sex on other tubes, this one right here offers a huge variety of movies and what you need for unbelievable experiences.

<http://www.datingnzcougar.info/>

Reply



RertJorgo says:

May 21, 2018 at 16:08

Do you love teen hardcore sex? Or when young girls suck cocks until guys cum? Or you like crazy dorm actions with drunk students drink beer and fuck at parties? All of these and much more you will see on this site 18-teen-porn.com. All kinds of teen porn with beautiful girls. Big tits, small tits,

shaved and hairy pussies penetrated by cocks, skilled mouths suck dicks and sure with lots of sperm! Have fun with our teen HD videos!

With a huge variety of quality teen porn, this top notch tube is sure to grant the best adult experiences online.

Once you step inside, you get to see a lot of niches and plenty of available HD videos, all carefully selected and with daily updates to keep you aroused.

Enjoy an impressive number of amateur teen porn, cam girls gone wild and a whole lot of other categories in one single and very impressive collection of teen videos. Each comes with HD image and the tube's fantastic streaming speed, something which will surely improve your adult experiences. Only rate teen porn and quality action, girls on fire in the mood to spin large inches of cock into each of their tiny love holes. Barely legal hotties working cock like true pornstars and a huge number of amateurs trying to make it into the big league. Either way you like your porn, this awesome teen tube will provide young flesh and spicy action at any hour. Only exclusive teen porn which is not available on other movie

sites or tubes. Quality content with premium action and girls to die for. Enjoy such fantastic content on a tube that's set to become number one, a tube which will make your delight with a very large variety of niches. Never mind browsing for teen sex on other tubes, this one right here offers a huge variety of movies and what you need for unbelievable experiences.

<http://www.datingnzcougar.info/>

Reply

Pingback: [New top story on Hacker News: Using a mobile phone to clone a mifare card – World Best News](#)

Pingback: [New top story on Hacker News: Using a mobile phone to clone a mifare card – Tech + Hckr News](#)

Pingback: [New top story on Hacker News: Using a mobile phone to clone a mifare card – techofacts](#)

Pingback: [New top story on Hacker News: Using a mobile phone to clone a mifare card – JkNews](#)

Pingback: [New top story on Hacker](#)

News: Using a mobile phone to clone a mifare card – techspace

Pingback: [New top story on Hacker News: Using a mobile phone to clone a mifare card | Do Mithay Bol](#)

Pingback: [New top story on Hacker News: Using a mobile phone to clone a Mifare card \(2016\) | World News](#)

Pingback: [New top story on Hacker News: Using a mobile phone to clone a Mifare card \(2016\) – ÇlusterAssets Inc.,](#)

Leave a Reply

Your email address will not be published.

Required fields are marked *

Comment

Name *

Email *

Website

POST COMMENT



tim@inexpro.nl



Zerif Lite powered by WordPress