NEAR FIELD COMMUNICATION

TECNOLOGIA E SICUREZZA

Andrea Draghetti

IMOLUG
Imola & Faenza linux User Group

Linux Day 27 Ottobre 2018

LINUX DAY

$ WHOAMI

+ Phishing Analysis and Contrast @ D3Lab
+ Team Member @ BackBox Linux

NEAR FIELD COMMUNICATION

La tecnologia NFC si è evoluta da una combinazione d'identificazione senza contatto o RFID (Radio Frequency Identification – Identificazione a Radio Frequenza) e altre tecnologie di connettività. Contrariamente ai più semplici dispositivi RFID, NFC permette una comunicazione bidirezionale: quando due apparecchi NFC (lo initiator e il target) vengono accostati entro un raggio di 4 cm, viene creata una rete peer-to-peer tra i due ed entrambi possono inviare e ricevere informazioni.

La tecnologia NFC opera alla frequenza di 13,56 MHz e può raggiungere una velocità di trasmissione massima di 424 kbit/s.

{Wikipedia}

NFC VS BLUETOOTH

Bluetooth

- Permette il trasferimento dati ad alta velocità
- Consente la comunicazione a medie distanze
- Richiede paring iniziale

NFC

- Comunicazione istantanea
- È orientato al trasferimento dati one-shot
- Può essere utilizzato per effettuare un paring Bluetooth

NFC VS QR CODE

QR Code

- Tecnologia a costo zero
- Solo read-only
- Non offre protezione asimmetrica

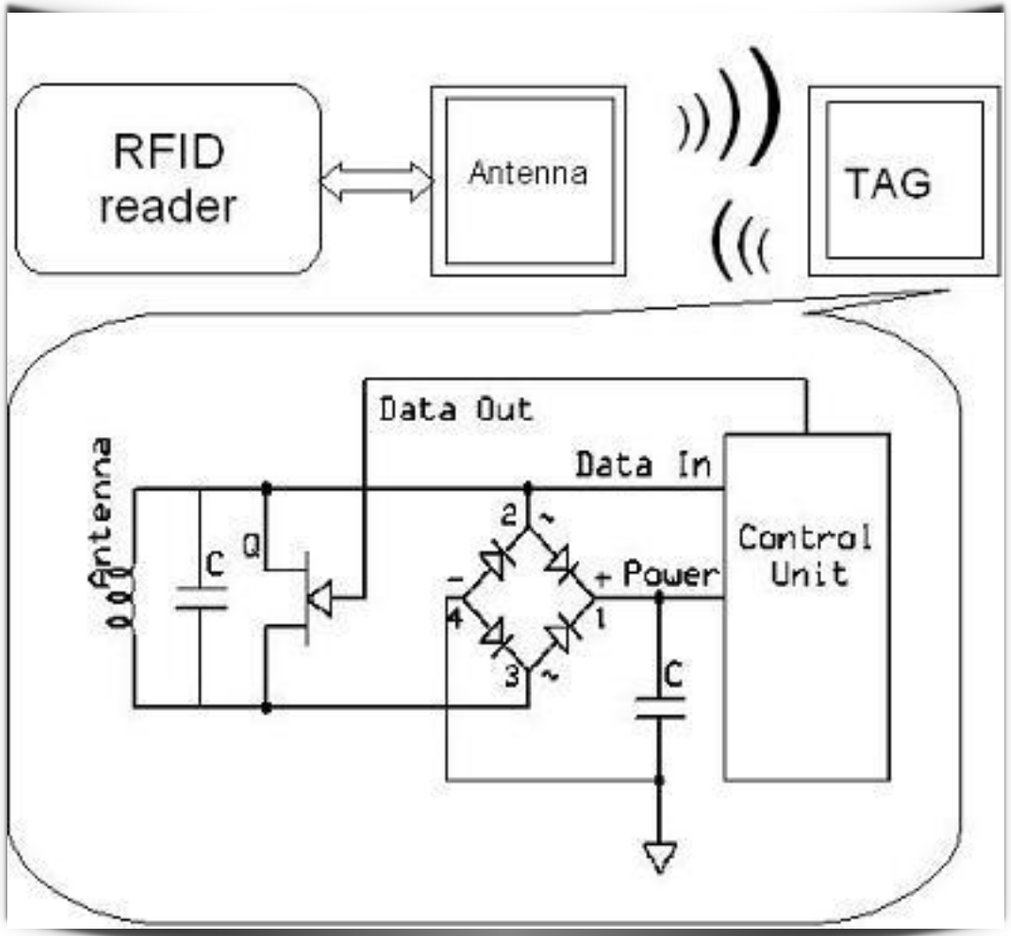
NFC

- Offre protezione simmetrica e asimmetrica
- I tag Nfc possono essere sia scritti che letti
- Richiede negli Smartphone la presenza del chipset

PRINCIPIO DI FUNZIONAMENTO

Il componente attivo emette un campo elettromagnetico che induce una corrente sul circuito del componente passivo.

Tale corrente è sufficiente ad alimentare il microcontrollore a bordo, ricevere il dato, effettuare l'elaborazione e trasmettere una risposta.



Fonte: http://www.scienceprog.com/how-does-rfid-tag-technology-works/

SCENARI APPLICATIVI

- Pagamenti
- Advertising
- Ticketing
- Tracking
- Gaming
- Social
- Medical

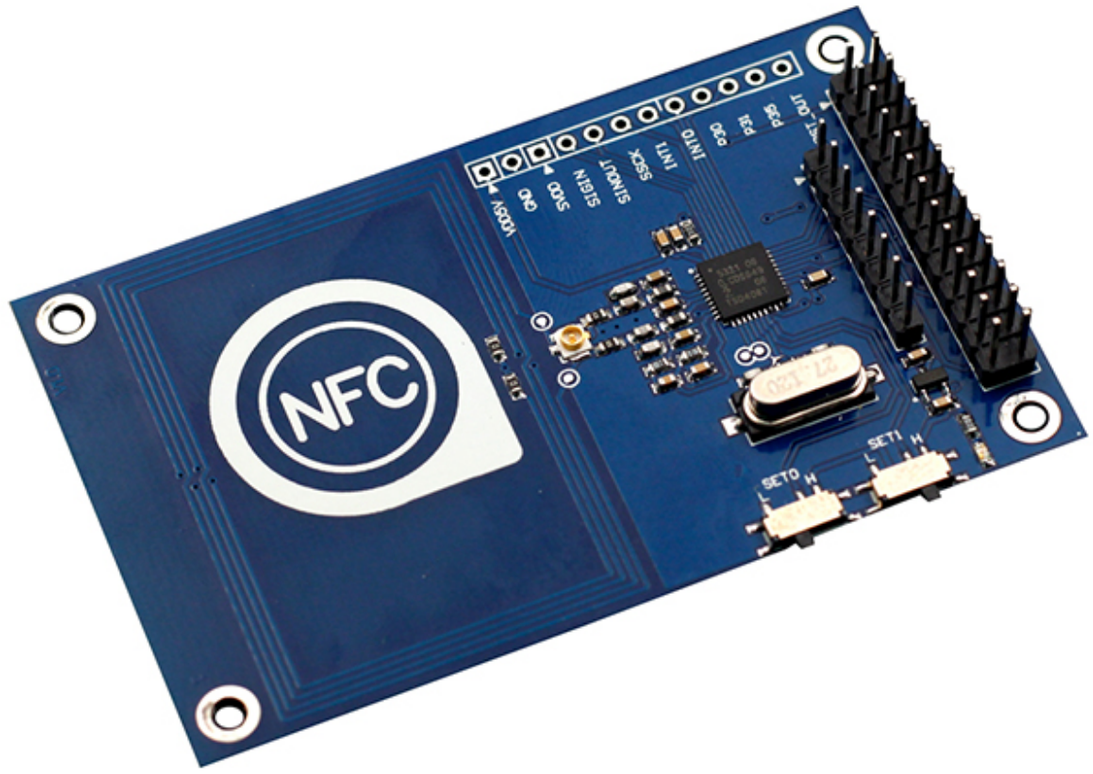
TAG NFC

CHIP NFC

- **NTAG**: Chip di ultima generazione che garantiscono una piena compatibilità con gli smartphone (fino a 888byte)
- **Mifare Classic**: Supporto la crittografia e progettati per un prolungato utilizzo, raramente supportati dagli smartphone (fino a 3440byte)
- **Mifare Ultralight**: Come i precedenti ma con minor spazio di memoria (46byte)
- **iCode**: Standard industriale compatibile con gli standard ISO 15693 e ISO 18000-3

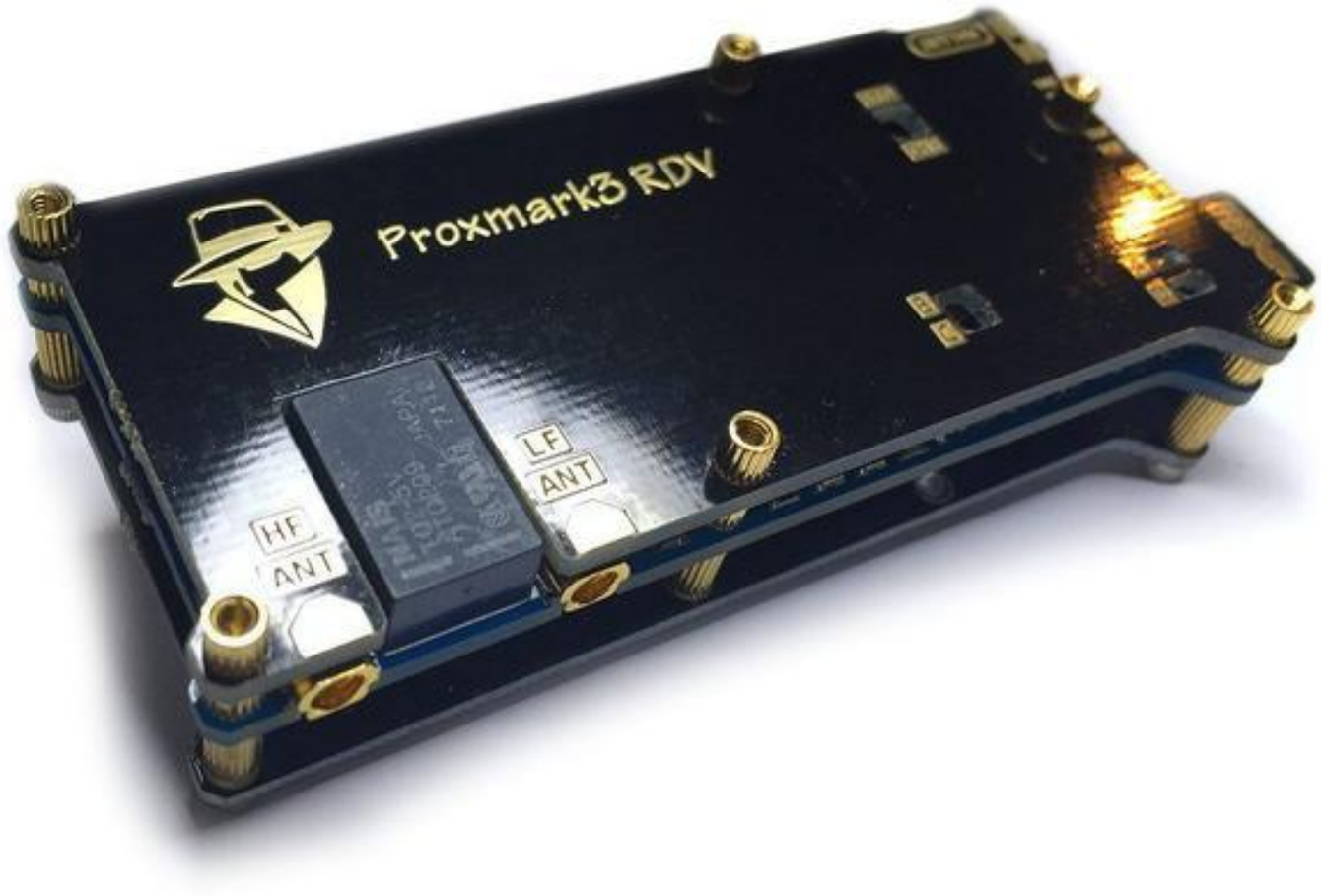
LETTORI NFC

ACR122U



PN532

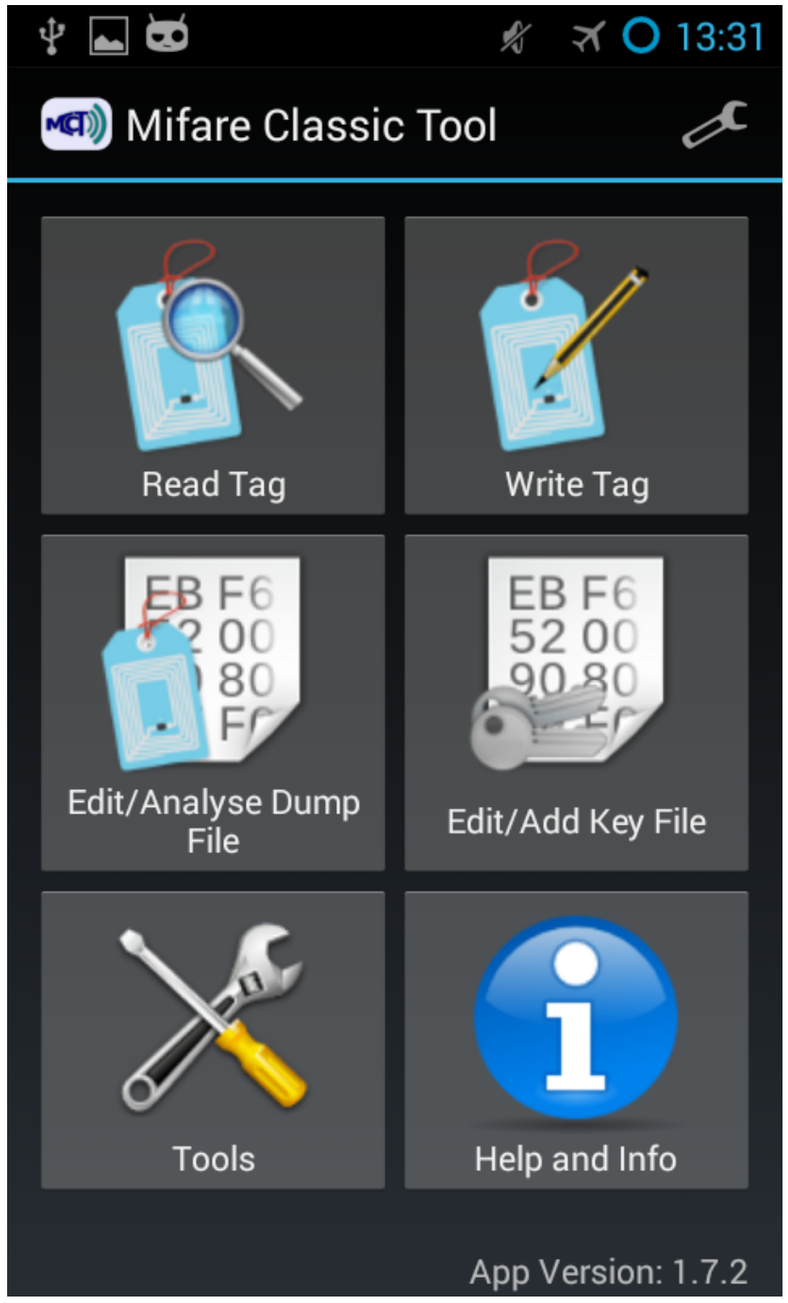
LETTORI NFC



Proxmark3

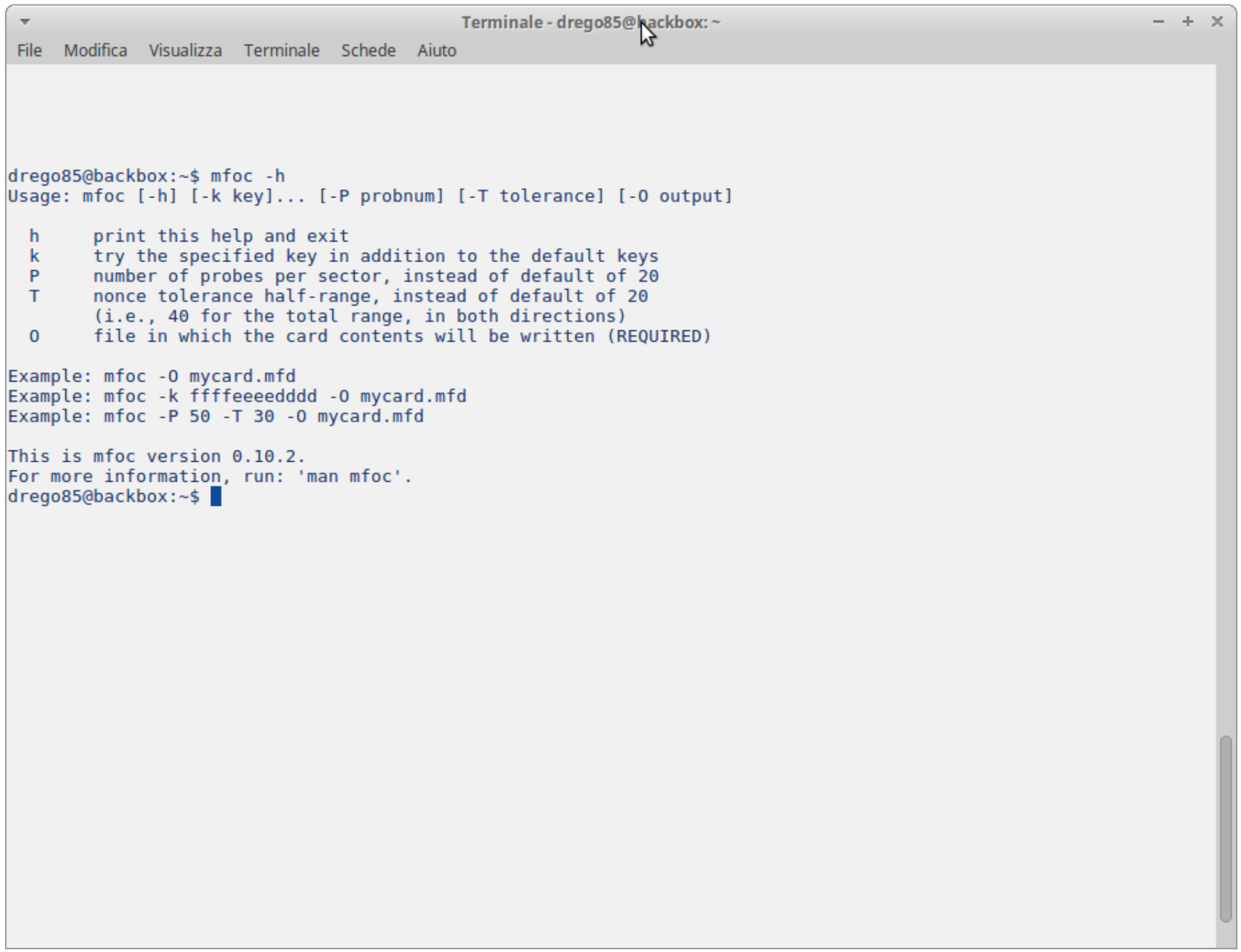
APPLICAZIONI ANDROID

NFC Tools



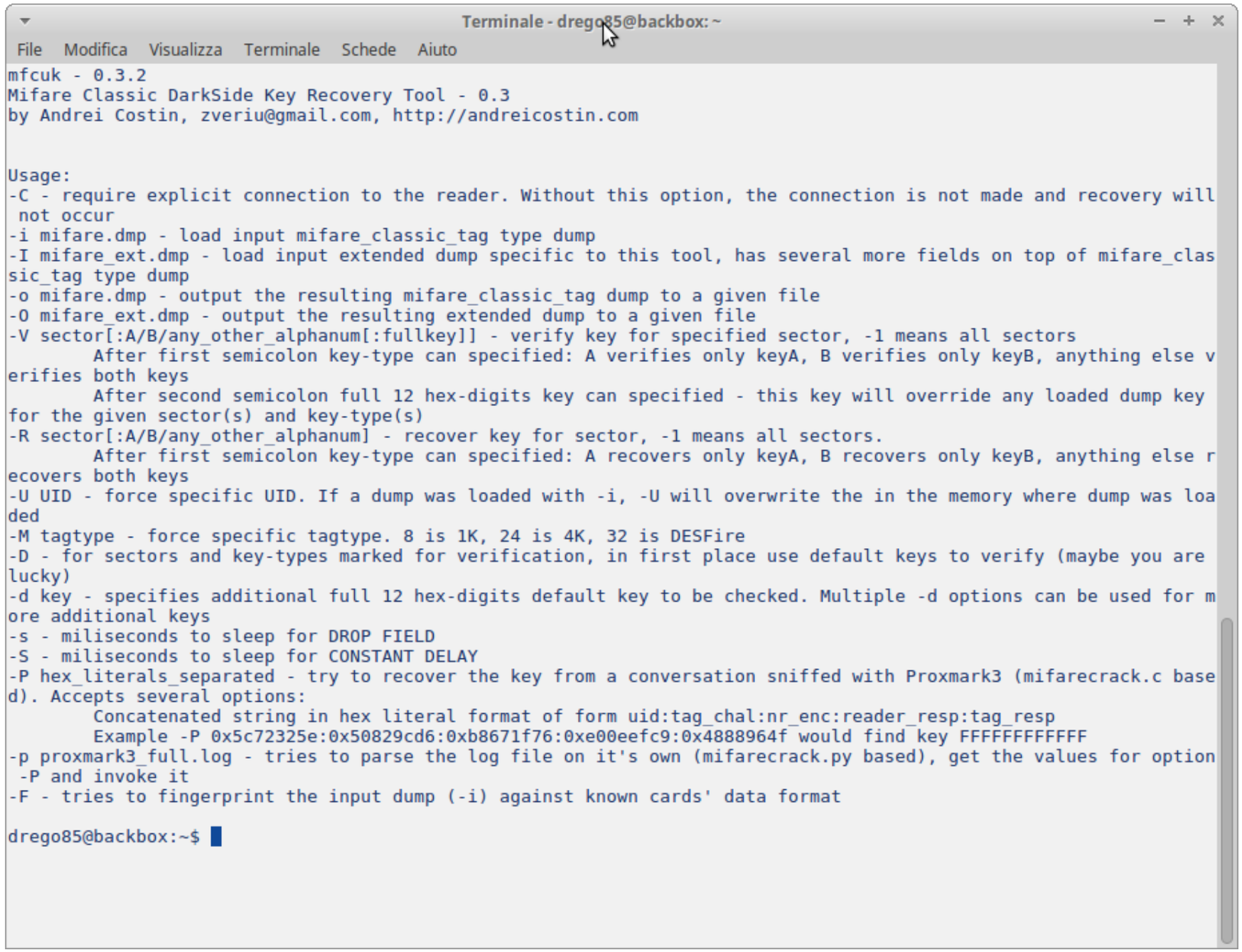
MIFARE Classic Tool

APPLICAZIONI LINUX: MFOC



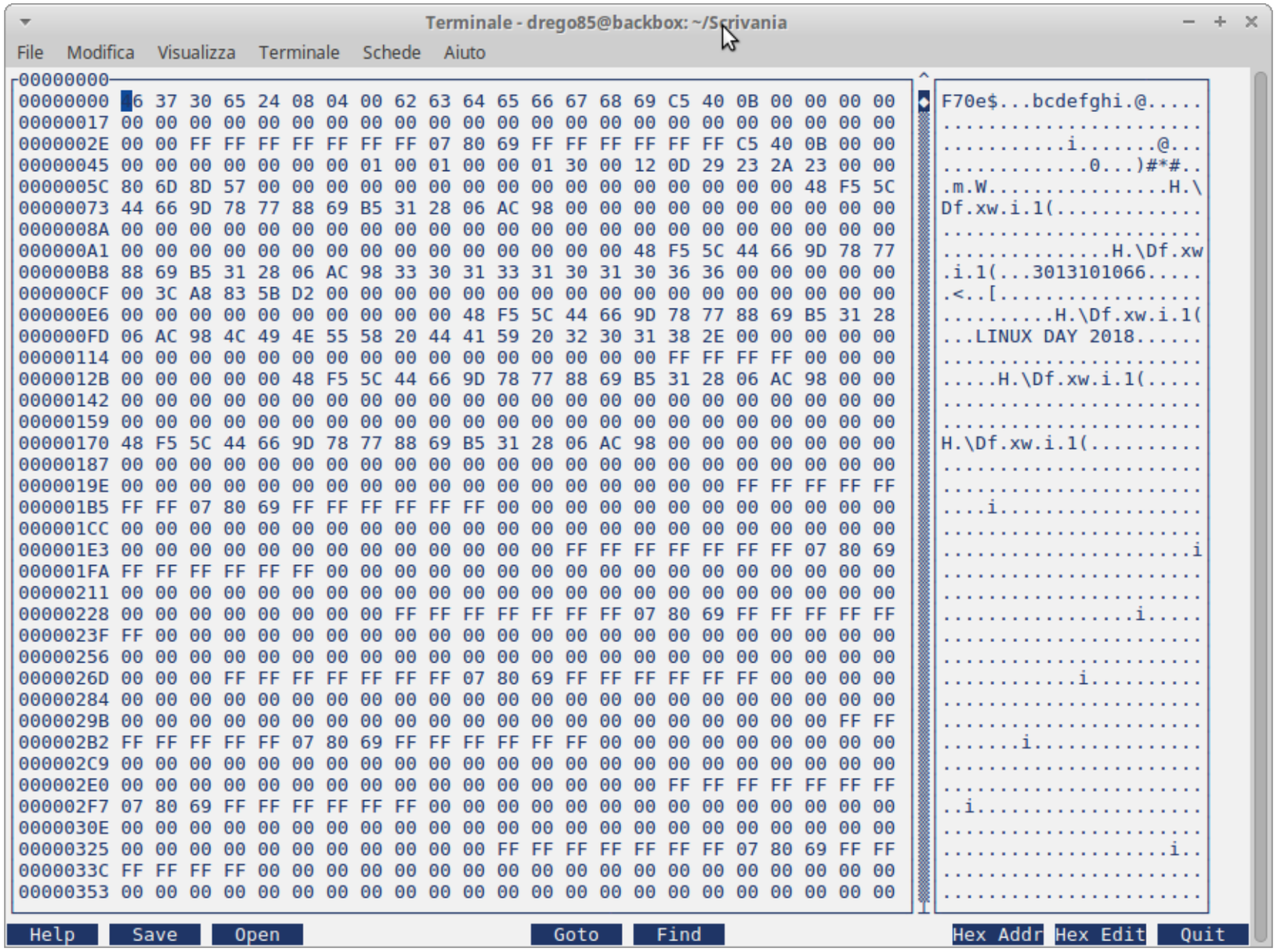
https://github.com/nfc-tools/mfoc

APPLICAZIONI LINUX: MFCUK



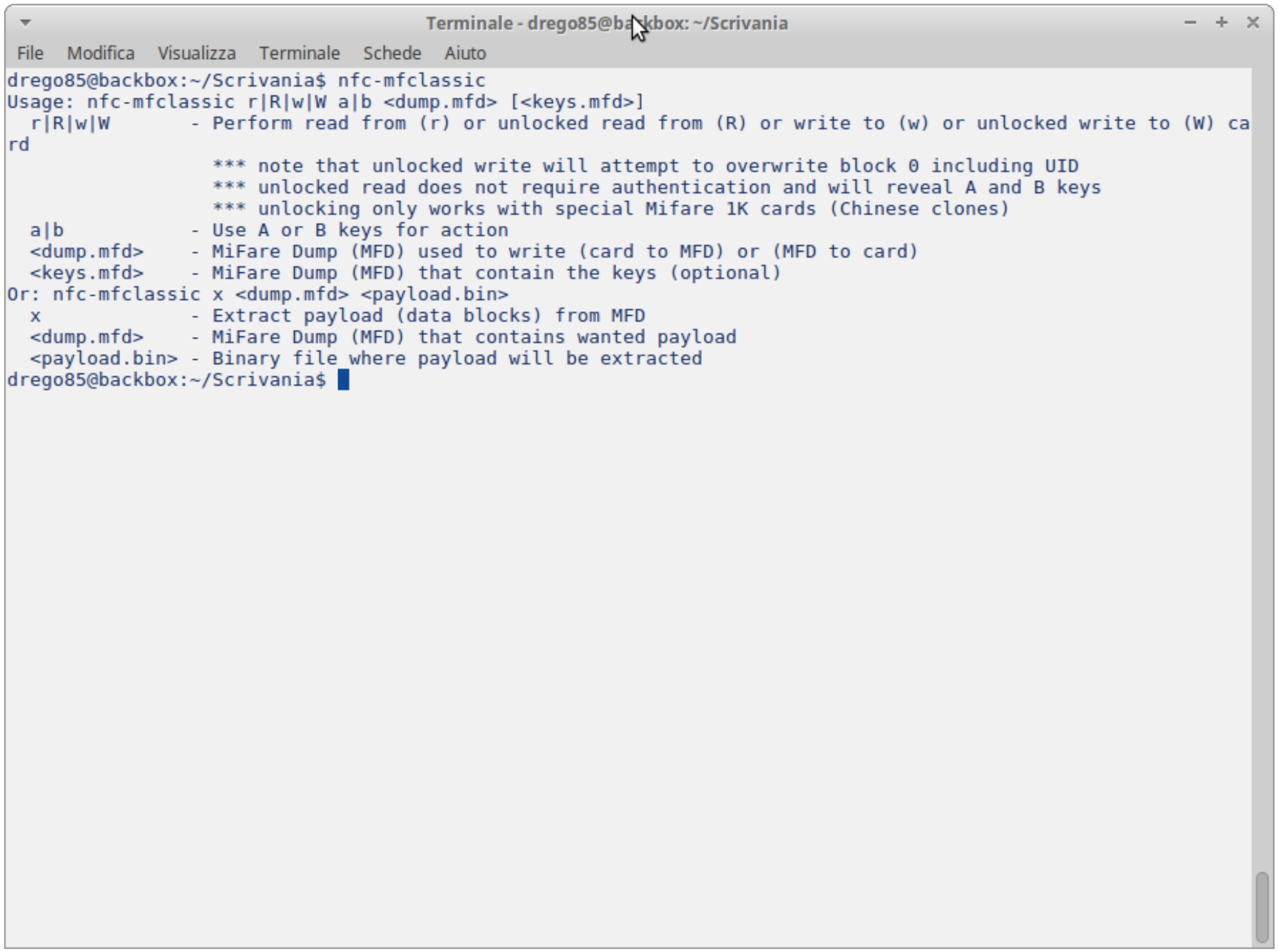
https://github.com/nfc-tools/mfcuk

APPLICAZIONI LINUX: HEXCURSE



https://github.com/LonnyGomes/hexcurse

APPLICAZIONI LINUX: NFC-MFCLASSIC



https://github.com/nfc-tools/libnfc

RASPBERRY: DIPENDENZE E PACCHETTI

$ sudo apt install autoconf build-essential libtool libusb-dev libpcsclite-dev
$ sudo apt install libnfc-bin libnfc-examples libnfc-dev

Mfoc e **Mfcuk** compilazione una volta scaricati i rispettivi sorgenti:

$ autoreconf -vis
$ ./configure
$ make
$ sudo make install

OPEN SOURCE RFID TOOL COLLECTION

RFID Tools as .deb

- binary .deb Package for Ubuntu x64 only
- containing mfok, fcuk and RFIDLab
- download rfid-tools_1.0.0_amd64.deb
- install prequesists: sudo apt-get install pcscd
- edit /etc/libccid_Info.plist

  <key>ifdDriverOptions</key>
  <string>0x0004</string>
- install:

  sudo dpkg -i rfid-tools_1.0.0_amd64.deb

Bootable USB-Stick image

- bootable Debian USB-Stick image file
- containing mfoc, fcuk, RFIDLab and the cyberflex-shell
- download attachment:rfid_tool_usb_stick.img
- write to USB-Stick:

  sudo dd if=rfid-tools_usb.img of=/dev/sdX bs=4096 count=262144
- user: root pw: toor

https://opensource.srlabs.de/projects/rfid

APPLICAZIONI WINDOWS

APPLICAZIONI WINDOWS

NFC: LAB MIFARE CLASSIC

Prendiamo in esempio un tag NFC Mifare Classic 1k

```
$ nfc-list -v
nfc-list uses libnfc 1.7.1
NFC device: ACS / ACR122U PICC Interface opened
[….]
[….]
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
```

NFC: LAB MIFARE CLASSIC

Effettuiamo il dump di questo TAG

```
$ mfoc -O original.mfd
Found Mifare Classic 1k tag
[….]
[….]
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] -> [x.....xxxxxxxxxx]
[Key: a0a1a2a3a4a5] -> [x.....xxxxxxxxxx]
[Key: d3f7d3f7d3f7] -> [x.....
```

NFC: LAB MIFARE CLASSIC

Se il tag non sfrutta le chiavi prestabilite

```
$ mfcuk -C -v 1 -w 6 -R 0:A -O original_ext.dmp -o original.dmp
mfcuk - 0.3.8
Mifare Classic DarkSide Key Recovery Tool - 0.3
by Andrei Costin, zveriu@gmail.com, http://andreicostin.com
[….]
[….]
INFO: Connected to NFC reader: ACS / ACR122U PICC Interface

INITIAL ACTIONS MATRIX - UID 56 f7 09 65 - TYPE 0x08 (MC1K)

VERIFY:
        Key A sectors: 0 1 2 3 4 5 6 7 8 9 a b c d e f
        Key B sectors: 0 1 2 3 4 5 6 7 8 9 a b c d e f
```

NFC: LAB MIFARE CLASSIC

Visualizziamo e/o Editiamo il dump

$ hexcurse original.mfd

NFC: LAB MIFARE CLASSIC

Scriviamo il dump editato su una nuova tag

```
$ nfc-mfclassic w B original_edited.mfd newtag.mfd
NFC reader: pn532_uart:/dev/ttyUSB0 opened
Found MIFARE Classic card:
ISO/IEC 14443A (106 kbps) target:
    ATQA (SENS_RES): 00  04
       UID (NFCID1): 8e  db  1a  2a
      SAK (SEL_RES): 08
Guessing size: seems to be a 1024-byte card
Writing 64 blocks |..failed to write trailer block 3
x.......................................................|
Done, 62 of 64 blocks written.
```

NFC: LAB MIFARE CLASSIC

Q&A

@AndreaDraghetti

BIBLIOGRAFIA

- Introduzione a NFC {Stefano Sanna} - http://bit.ly/2ywvl5l
- Hacking Mifare Classic Cards {Marcio Almedia} - https://ubm.io/2q7QUEV
- How to Crack Mifare Classic Cards {FireFart} - http://bit.ly/2ReiEmW