

MAGS TRIP EMAD NESS

08/06

VALID FROM

44/20

EXPIRES END

MALFUNCTION, MAJ.

OF-3

DEFCON

ISSUER

14

ISSUE

DC-44-20

SORT CODE



who am i ?

- **white hat hacker by night, weekends & when traveling..**
- **DEFCON goon**
- **DC4420 P.O.C. (London)**
- **security professional by day**



why mag stripe ?

- **old skool**
- **thoroughly insecure and yet still in use**
- **security by obscurity (again!)**
- **because it's there**
- **i have no life**



SCORE 1689

LIVES 



FW



AV

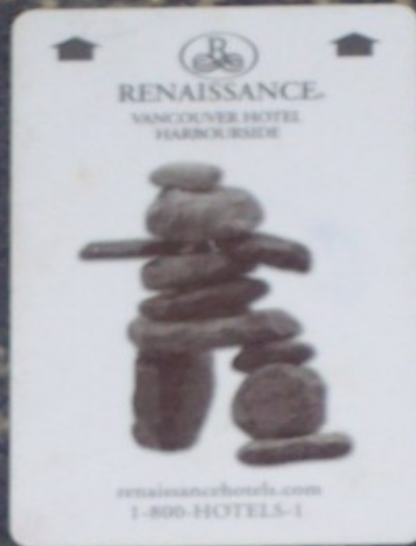


IDS

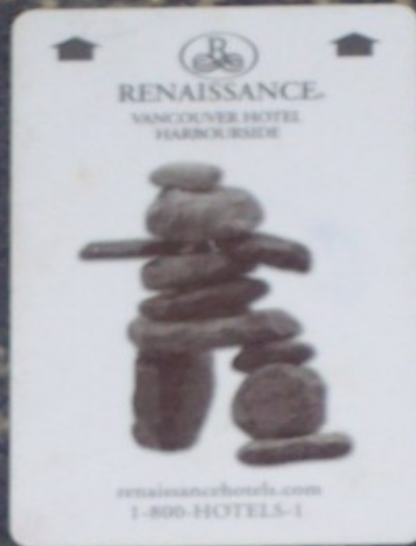


PEAKFLOW X

swipe cards



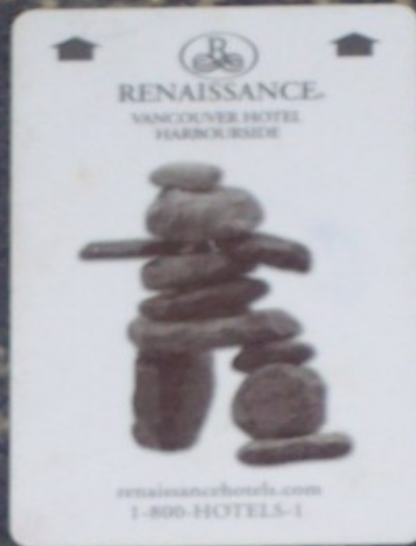
spot the room key...



spot the room key...



spot the ATM card...



spot the ATM card...



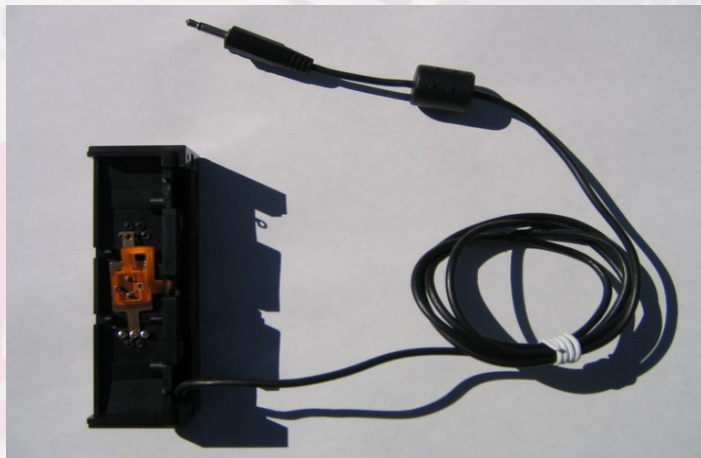
equipment - makstripe

- <http://www.makinterface.de>
- Parallel port
- Read / Write all 3 tracks
- Raw data
 - Does not care about checksums
 - Does not care about parity
- Windows support only :(
 - Doesn't work with VMWare :(:(

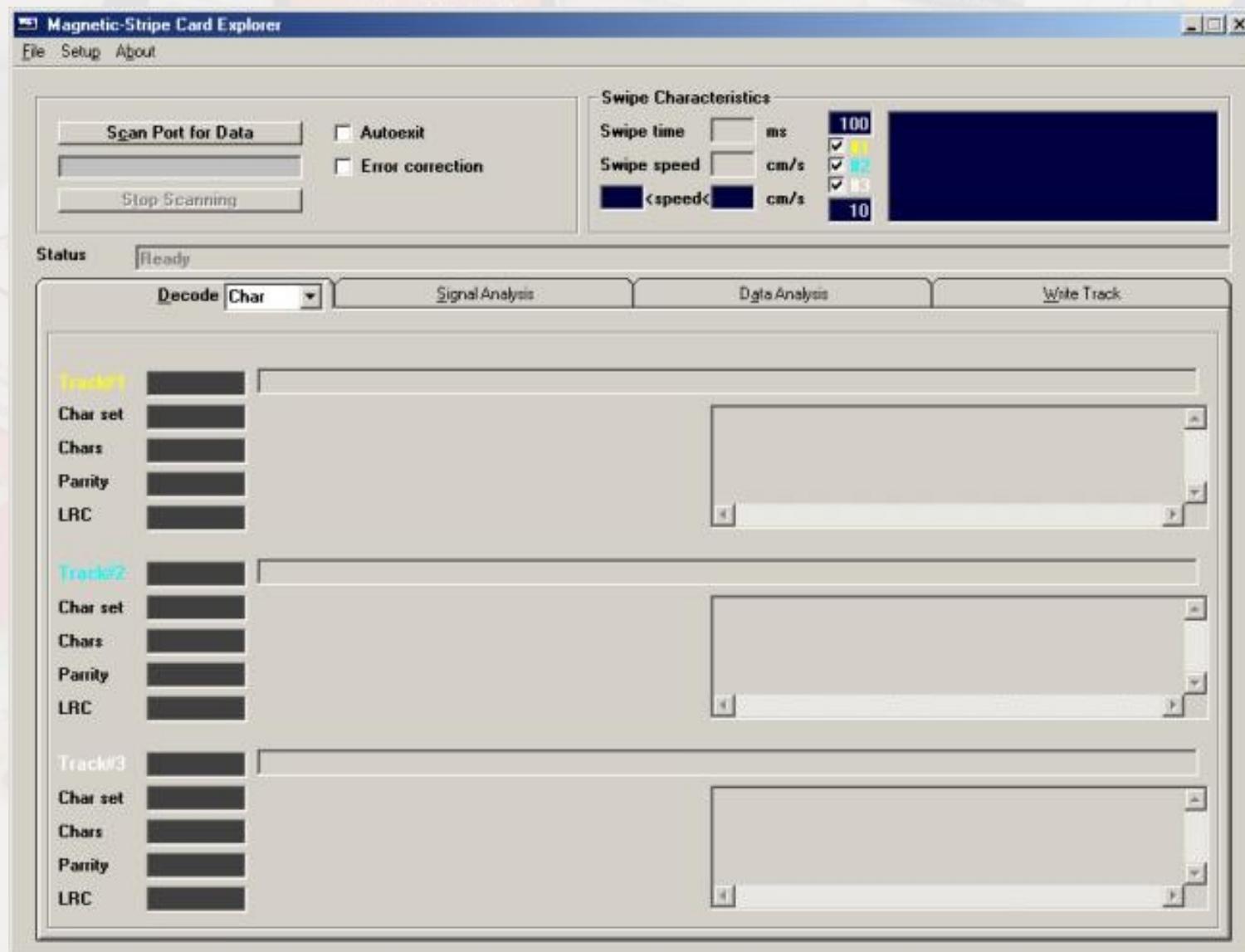


equipment

- <http://www.sephail.net/articles/magstripe>
- **Audio output**
 - Analyse WAV files offline
- **Read all 3 tracks plus non-standard**
- **Raw data**
 - Does not care about checksums
 - Does not care about parity
- **Read only**



equipment - makstripe



equipment - makstripe

Magnetic-Stripe Card Explorer

File Setup About

Scan Port for Data ☐ Autoexit
Stop Scanning ☐ Error correction

Swipe Characteristics

Swipe time: 211 ms 100
Swipe speed: 40 cm/s 27 <speed> 50 cm/s 10

Status: Idle

Decode Char Signal Analysis Data Analysis Write Track

Track#1 210 BPI %B4779 4 ^02011 10000000000 300 00?5

Char set: ALFA B4779 4
Chars: 79
Parity: Ok 0201 11 0000 0300 0000
LRC: Ok

Start Sentinel: %
Data: B4779 4
Field Separator: ^
Data:

Track#2 76 BPI ;47791 4-0201 11 0000?1

Char set: BCD 4779 4
Chars: 40 020 11 0000
Parity: Ok
LRC: Ok

Start Sentinel: ;
Data: 4779 4
Field Separator: =
Data: 020 11 0000

Track#3

Char set:
Chars:
Parity:
LRC:



equipment - makstripe

Magnetic-Stripe Card Explorer

File Setup About

Scan Port for Data ☐ Autoexit ☐ Error correction

Stop Scanning

Swipe Characteristics

Swipe time: 211 ms 100
Swipe speed: 40 cm/s 10
27 <speed> 50 cm/s

Status: Ready

Decode Binary Signal Analysis Data Analysis Write Track

Track#1 210 BPI ^B4779 4~ ^02011 11 0000000000 130 000?5

Char set: ALFA
Chars: 79
Parity: Ok
LRC: Ok

Track#2 76 BPI :4779 4-02011 11 130000 1

Char set: BCD
Chars: 40
Parity: Ok
LRC: Ok

Track#3

Char set:
Chars:
Parity:
LRC:



Char	Bits	from bit	to bit	parity	LRC
1	1010001	28	34	0k	
2	0010110	35	41	0k	-
3	0001011	42	48	0k	-
4	1001010	49	55	0k	-
5	1100111	56	62	0k	-
6	0000001	63	69	0k	-
7	1001010	70	76	0k	-
8	1100111	77	83	0k	-
9	0000001	84	90	0k	-
10	1000011	91	97	0k	-
11	0000001	98	104	0k	-
12	0010110	105	111	0k	-

13: 1111111
 14: 1111111 Examine bits per Character Total
 15: 1111111 Start with bit position Last
 16: 1111111
 17: 1111111

write - makstripe

Magnetic-Stripe Card Explorer

File Setup About

☐ Autoexit
 ☐ Error correction

Status: Ready

Decode **Signal Analysis** **Data Analysis** **Write Track**

Source data
☐ Track#1
☐ +
☐ Track#2
☐ +
☐ Track#3
☒ Custom

Destination
☒ Track#1
☐ Track#2
☐ Track#3

Reference Track
☐ Track#1
☒ Track#2
☐ Track#3

Prepare to write
 #1

Duration seconds

Write data to Track
0/1 adj.
BPI adj.
 ☐ Swipe speed=Ref.

Custom data
Data

☒ Track#1
☐ Track#2
☐ Track#3

Data properties
Nr. of Chars Total nr. of Bits
Character set Bits before data
BitsPerInch Bits in data
☒ recalculate LRC Bits after data



standard track formats

- **track 1**
 - IATA – 210 BPI, 7 bit, 79 alphanumeric characters
- **track 2**
 - ABA – 75 BPI, 5 bit, 40 numeric characters
- **track 3**
 - THRIFT – 210 BPI, 5 bit, 107 numeric characters



making sense of the data

- **character sets**

- <http://www.magtek.com/documentation/public/998750b5-4.pdf>



track standards - IATA

BRITISH AIRWAYS

GATE
D71

GATE CLOSES
2010

SEAT
19K

BA/

LAURIE/ADAM MR
BA 84 **LONDON**

PASSENGER TICKET AND BAGGAGE CHECK
LHR

BOARDING PASS

BRITISH AIRWAYS

NAME OF PASSENGER
LAURIE/ADAM MR

BA/

FROM
VANCOUVER

TO
LONDON

YVR
LHR

CARRIER / FLIGHT
BA 84

CLASS / DATE
W

TIME
2030

GATE
D71

GATE CLOSES
2010

SEAT
19K

SMOKE
XX

PCS
1

OK WT
0

UNCK WT
0

SEQ NO
136

PASSENGER TICKET AND BAGGAGE CHECK
NQ ETKT NO COUPON

Track 1: 210 BPI, 7 bit, 79
Alphanumeric characters



track standards - IATA

Data format

Airport

Flight No.

Day of year

Start

Format

From

To

Flight

Class

Day

Seat

Passenger

End

LRC



track standards - IATA

YVR

LHR

19K

LAURIE/ADAM MR

Start

Format

From

To

Flight

Class

Day

Seat

Passenger

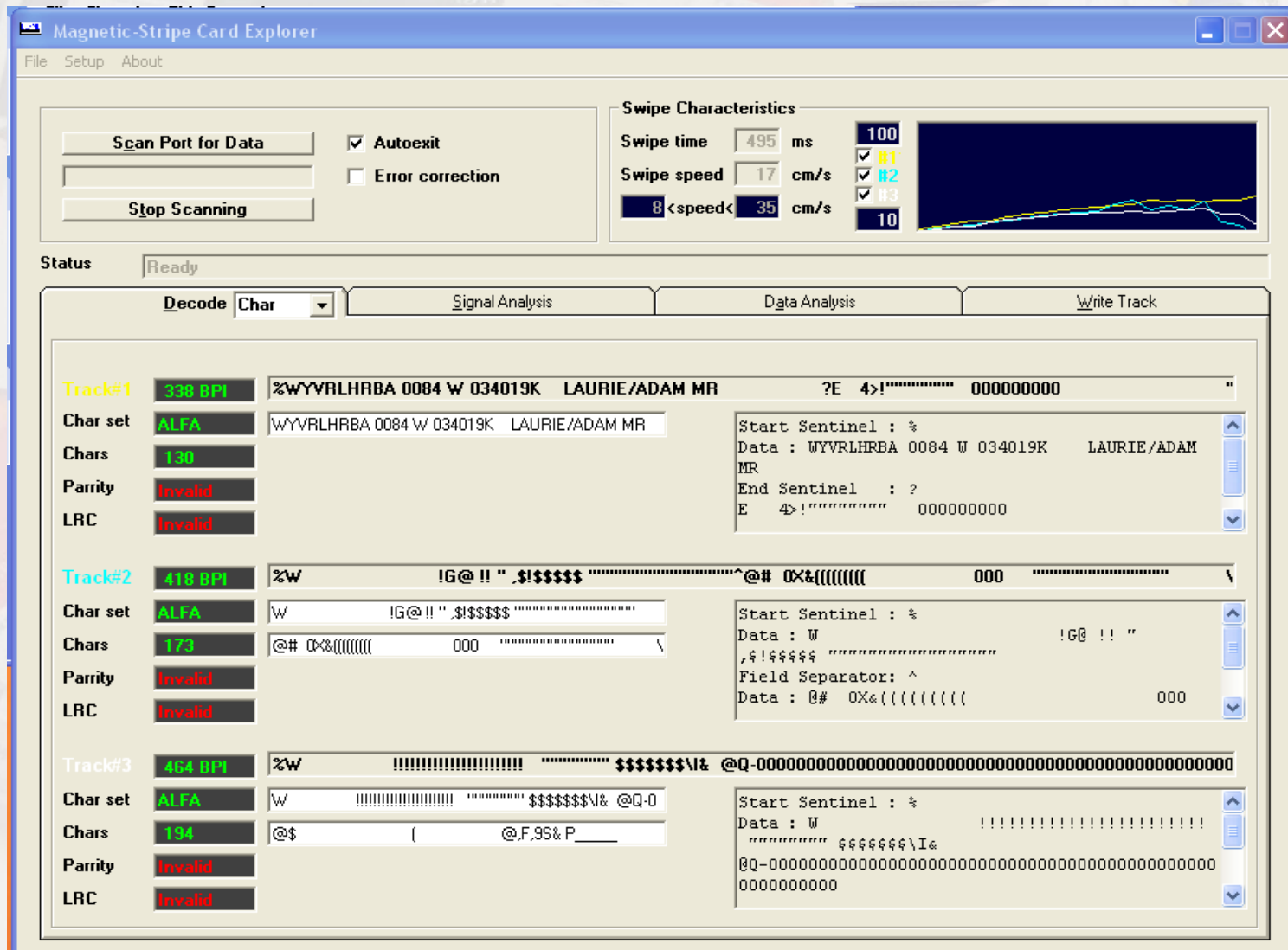
End

LRC

%WYVRLHRBA 0084 W 034019K LAURIE/ADAM MR ?E



before



after

Magnetic-Stripe Card Explorer

File Setup About

Scan Port for Data ☐ Autoexit
☐ Error correction
Stop Scanning

Swipe Characteristics
Swipe time 277 ms 100
Swipe speed 30 cm/s ☒ #1
24 <speed> 39 cm/s ☒ #2
☒ #3 10

Status Ready to read - Card can be swiped

Decode Char Signal Analysis Data Analysis Write Track

Track#1 166 BPI 2'OR 1=1;UPDATE FLT SET SEAT='1A' WHERE P='LAURIE/ADAM MR';?=

Char set ALFA 'OR 1=1;UPDATE FLT SET SEAT='1A' WHERE P='LAU

Chars 69

Parrrity Ok

LRC Invalid

Start Sentinel : %
Data : 'OR 1=1;UPDATE FLT SET SEAT='1A' WHERE
P='LAURIE/ADAM MR';
End Sentinel : ?
= LRC :

Track#2

Char set

Chars

Parrrity

LRC

Track#3 135 BPI

Char set Unknown

Chars

Parrrity

LRC

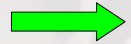


hotel door locks

- **passive**
 - all logic in the lock
- **active**
 - reader only
 - all logic on back-end
 - centralised alarms & reporting



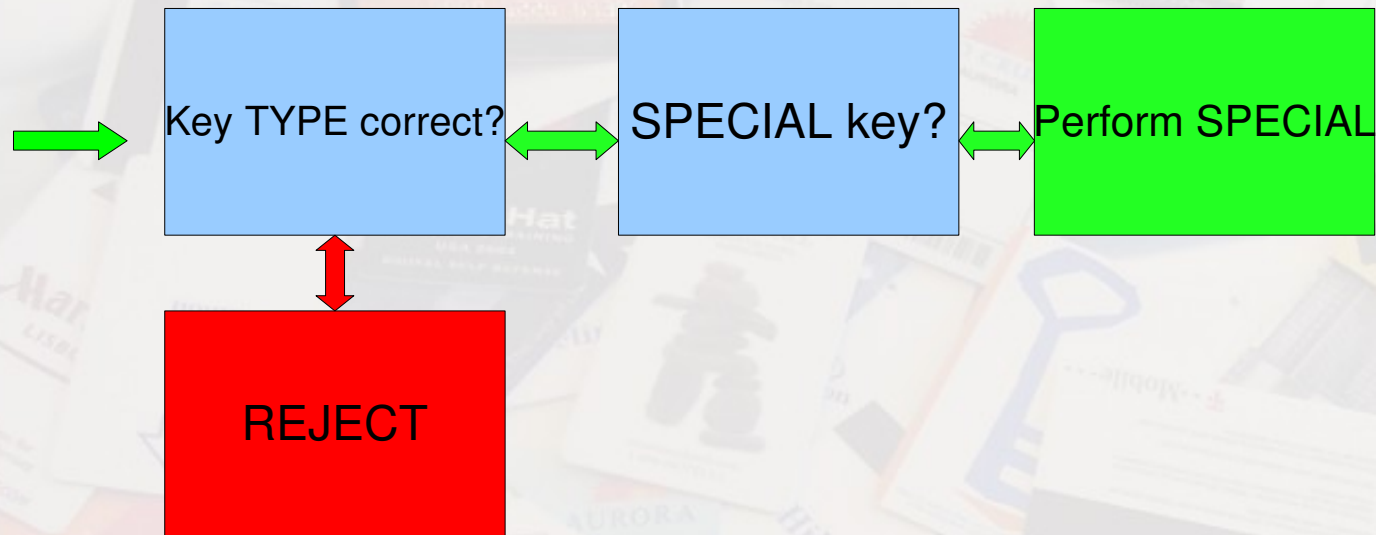
passive locks



Key TYPE correct?



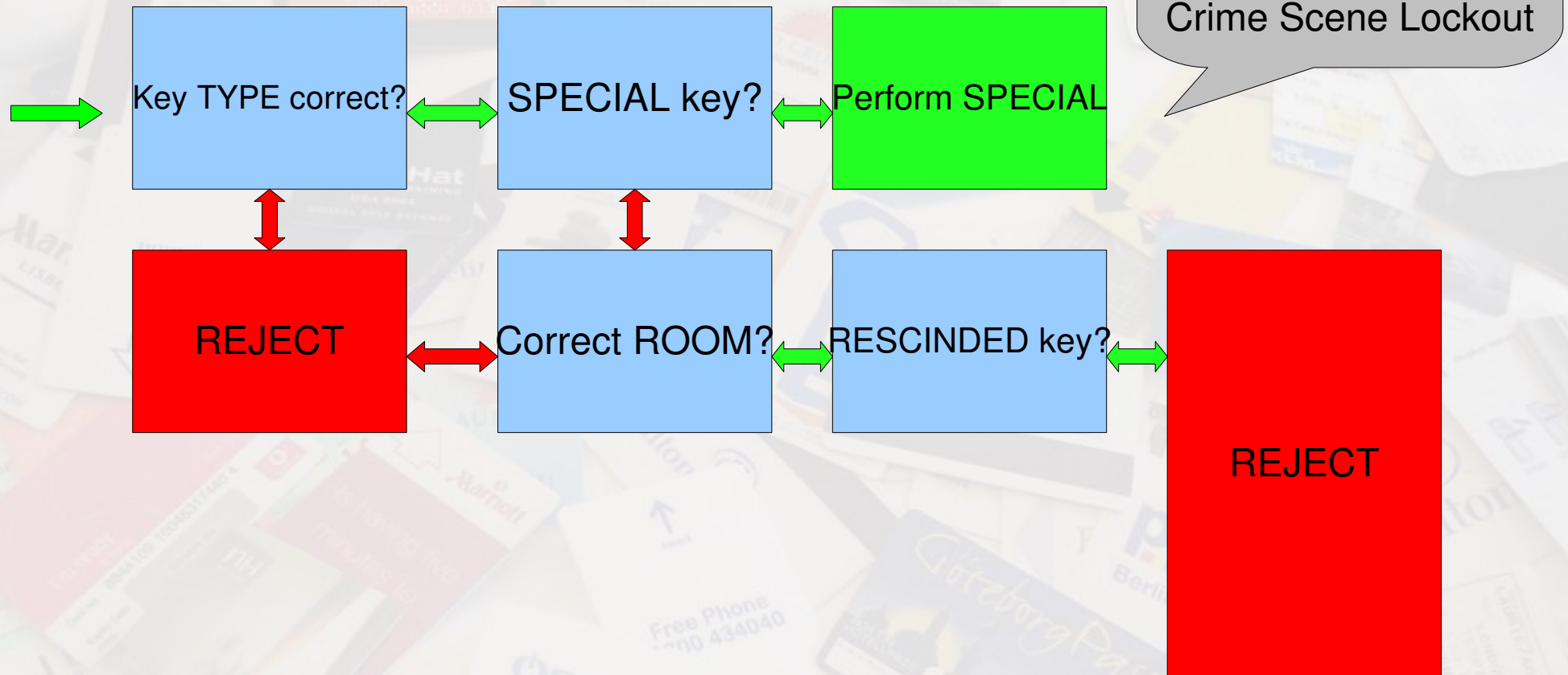
passive locks



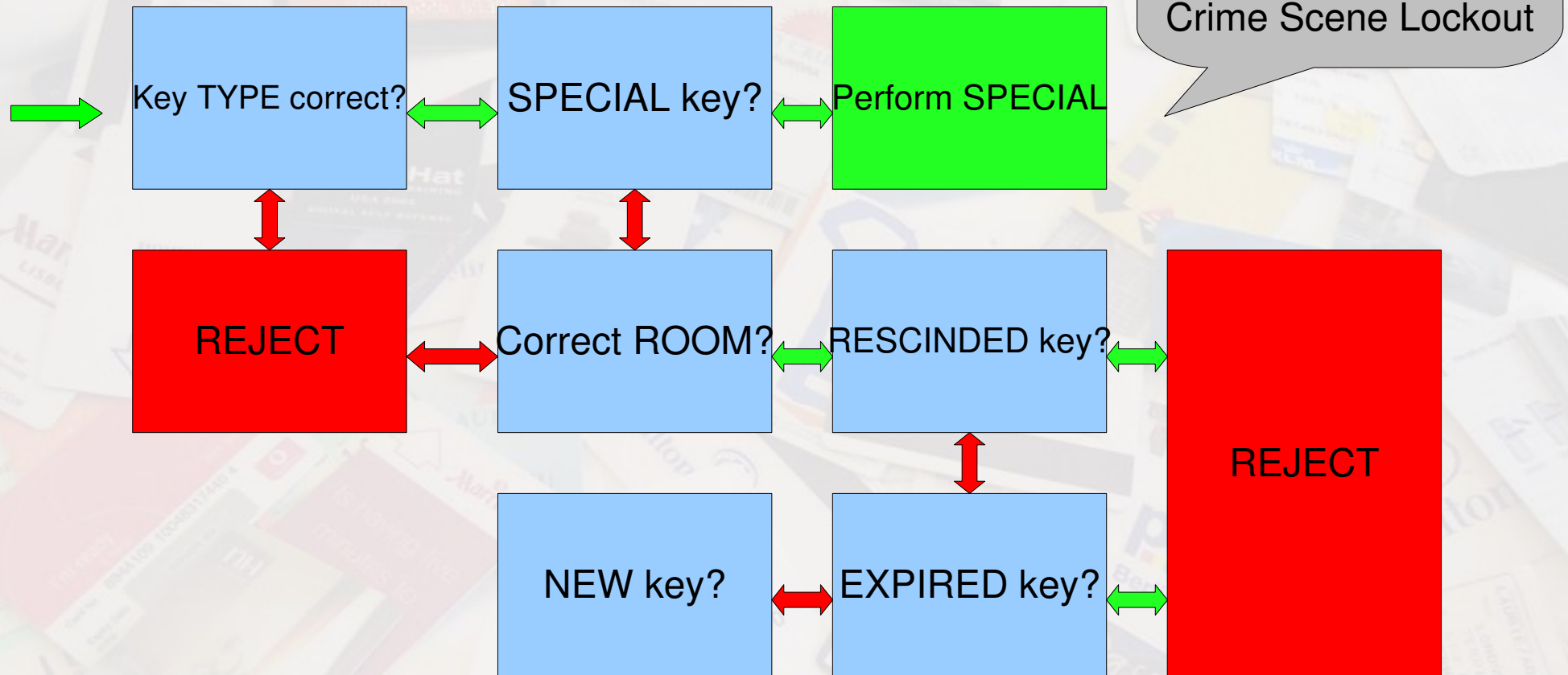
Housekeeping Open
One-Time Open
Guest Lockout
Crime Scene Lockout



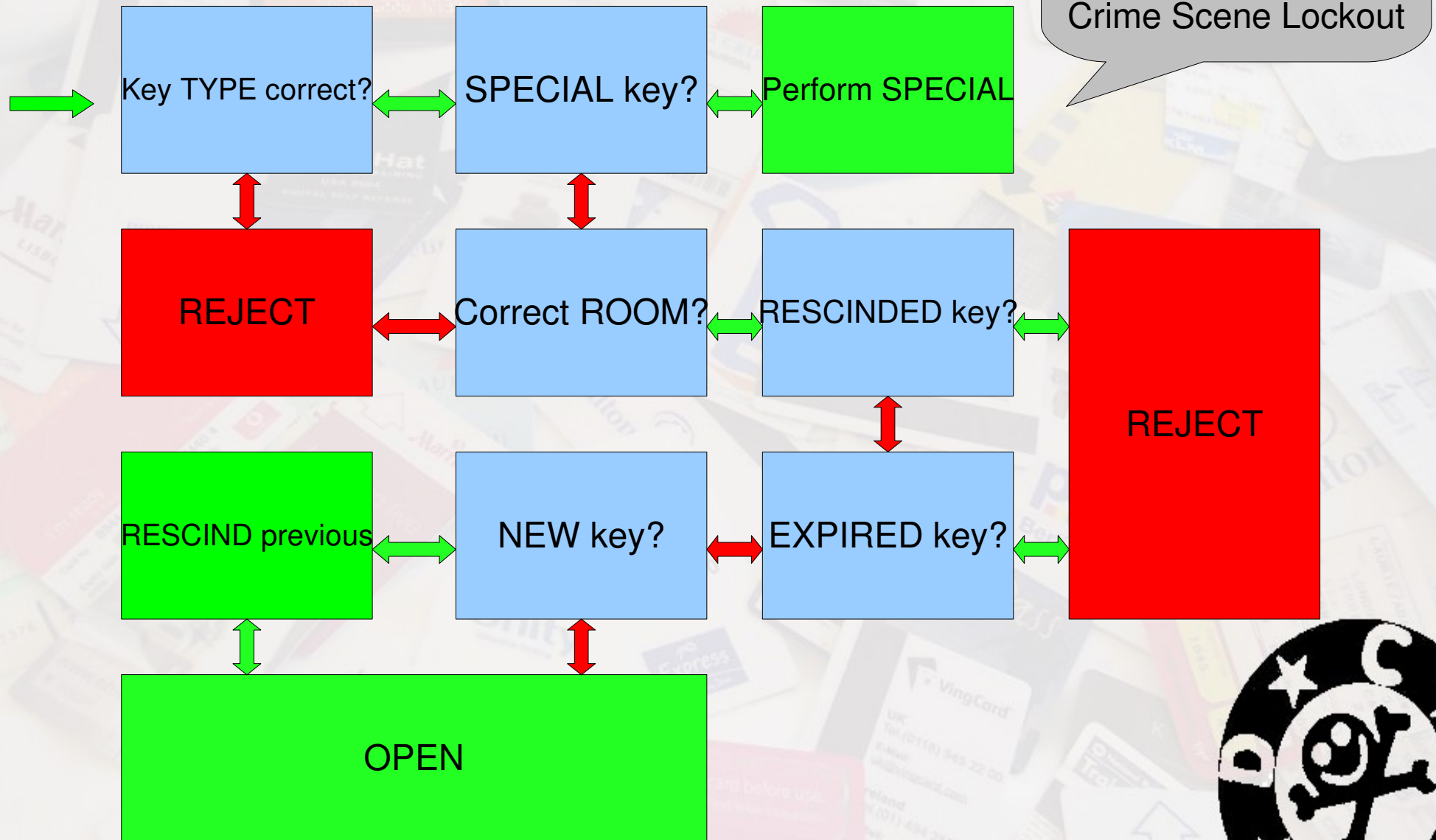
passive locks



passive locks



passive locks



keycard – multiple keys

- ;51011535280101766301250001200000000000?8
- ;51011535280201766301250001200000000000?;

Start	Property?	Room No.	Key No.	Magic Number?	Expire	Time	End	LRC
;	510115	3528	01	01766	30125	0001200	?	8
;	510115	3528	02	01766	30125	0001200	?	;



keycard – new key!

- ;51011535280101766301250001200000000000?8
- ;51011535280201766301250001200000000000?;
- ;51011535280301766301250001200000000000?:

Start	Property?	Room No.	Key No.	Magic Number	Expire	Time	End	LRC
;	510115	3528	01	01766	30125	0001200	?	8
;	510115	3528	02	01766	30125	0001200	?	;
;	510115	3528	03	01766	30125	0001200	?	:



keycard – rescinding

- ;51011506110107004311250001200000000000?6
- ;51011506110107032311250001200000000000?3

Start	Property?	Room No.	Key No.	Magic Number	Expire	Time	End	LRC
;	510115	0611	01	07004	31125	0001200	?	6
;	510115	0611	01	07032	31125	0001200	?	3



RESCINDING keys

New magic number

12345



85123

56787

23677

...



Lock stores
last 100 keys



active locks

- **all locks connected to central computer**
 - one wire
- **checking done against live database**
- **key swipe as messaging system**
 - room clean, out of service etc.
- **security**
 - access attempts
 - raise alarm!
 - audit trail
- **much more expensive**
 - harder to retrofit



non-standard stripes



non-standard equipment



magnasee

- magnetic field visualisation
- head alignment
 - audio
 - 1/2" Tape
 - lead-in
- Carbon Tetrachloride!
 - (carbon chloride, methane tetrachloride, perchloromethane, tetrachloroethane, or benziform)
 - + iron filings
 - banned as a carcinogen!! =:0



Magnasee alternative

- QView

- http://www.q-card.com/info_developer.asp



magnasee



K

RICH
LON
TEL
FAX
WWW

THIS EDGE IN SLOT



National Rail Enquiries

TrainTrackerTM

Departure and arrivals information for **direct trains** for today.

0871 200 4950

www.nationalrail.co.uk/train

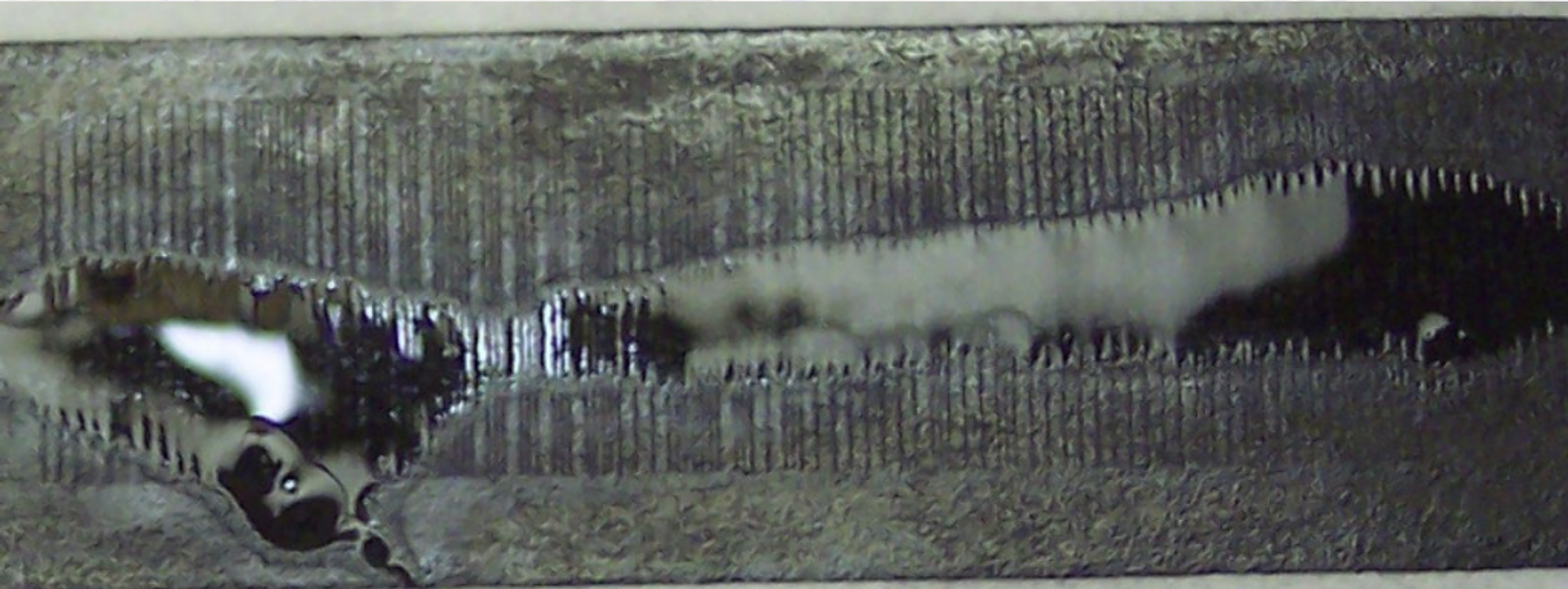
Travel on Train Companies' trains is subject to the National Rail Conditions of Carriage. This ticket is subject to the conditions of carriage of other operators on whose services this ticket is used. It is not transferable. Unless otherwise stated, it may be used on any Train Company service on any Permitted Route, and if marked "+", on London Underground trains between any two stations via any recognised route appropriate to the through journey being made. It is available for joining or alighting at an intermediate LRT Underground station.

Names of the Train Companies, copies of the National Rail Conditions of Carriage and of Permitted Routes are available at Ticket Offices.

RSP No. 4599/NRES

388 1108

magnasee

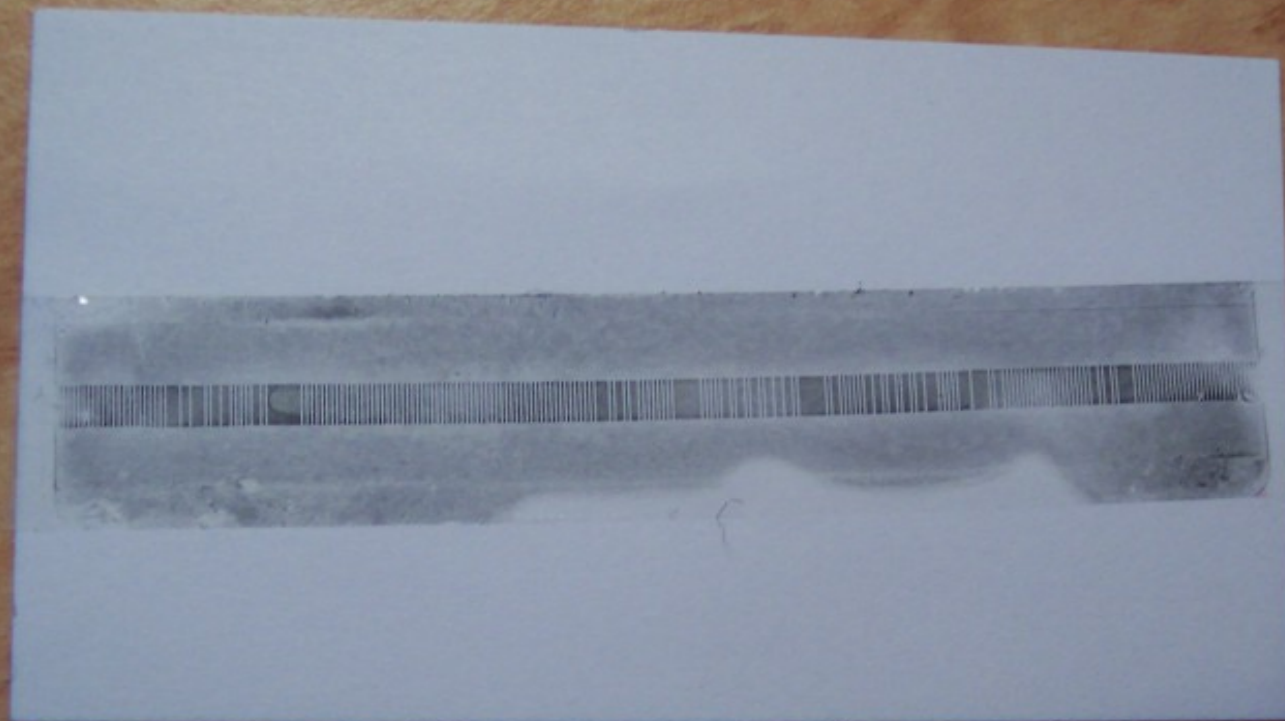


Companies' trains is subject to the

magnasee



magnasee

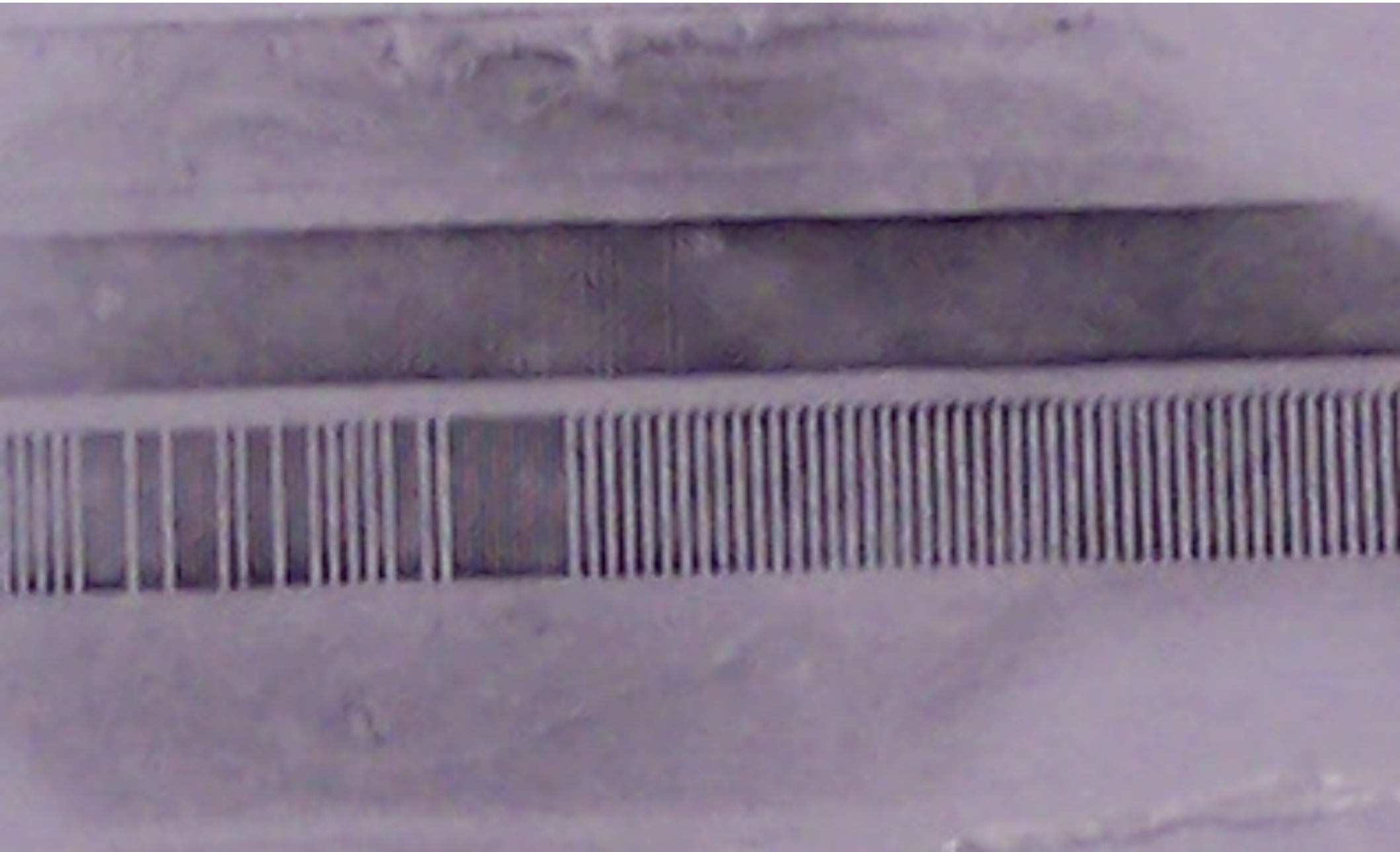


The top portion of the image features a collage of various cards and documents, including a 'top-up' card, a 'replay' card, a 'mobile' card, and a 'NCP' card. The text 'magnasee' is overlaid on this collage in a bold, black, sans-serif font.

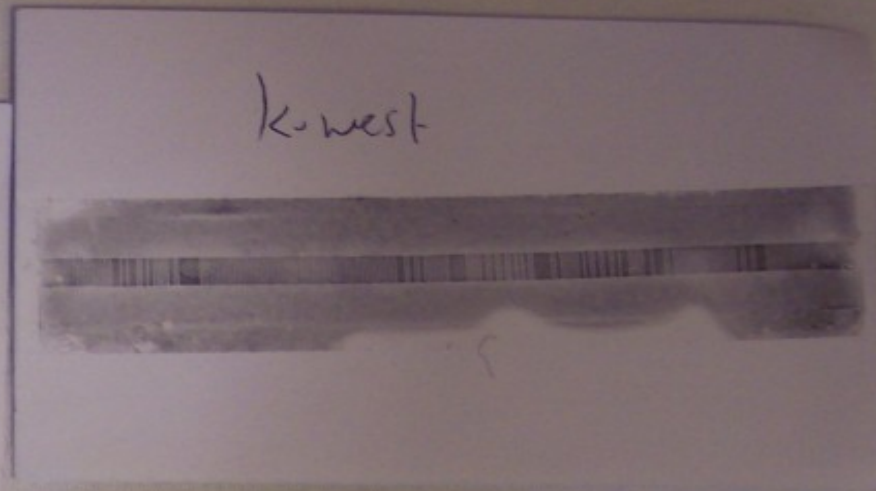
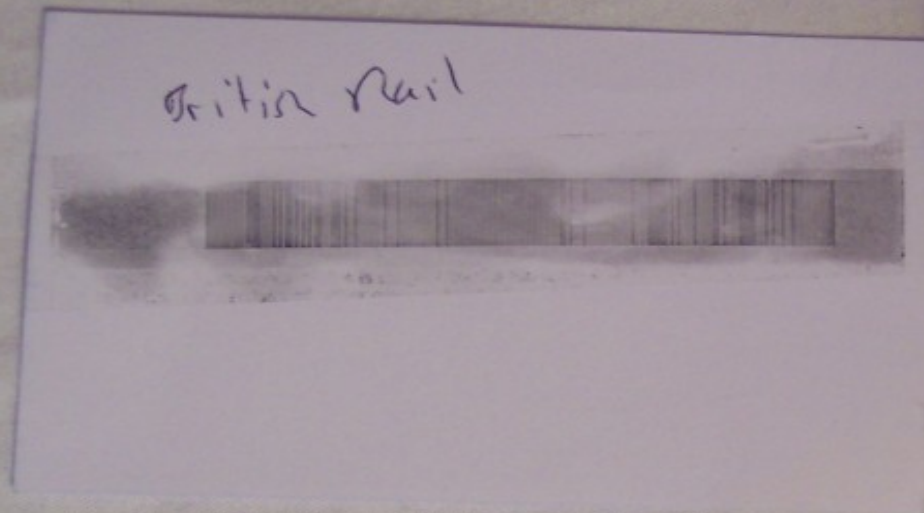
magnasee



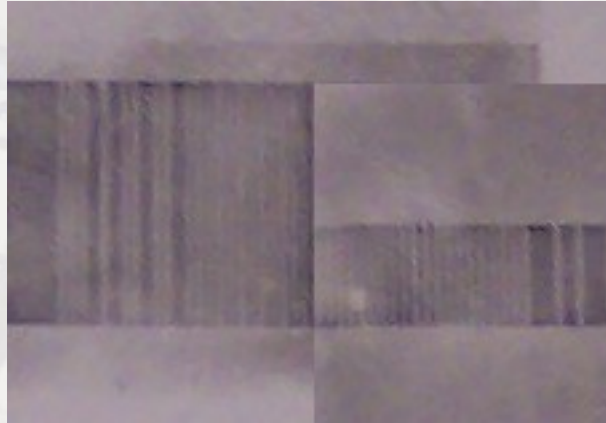
magnasee



size matters!



size matters!



**British Rail track is 2.5 times the width
of ISO standard**



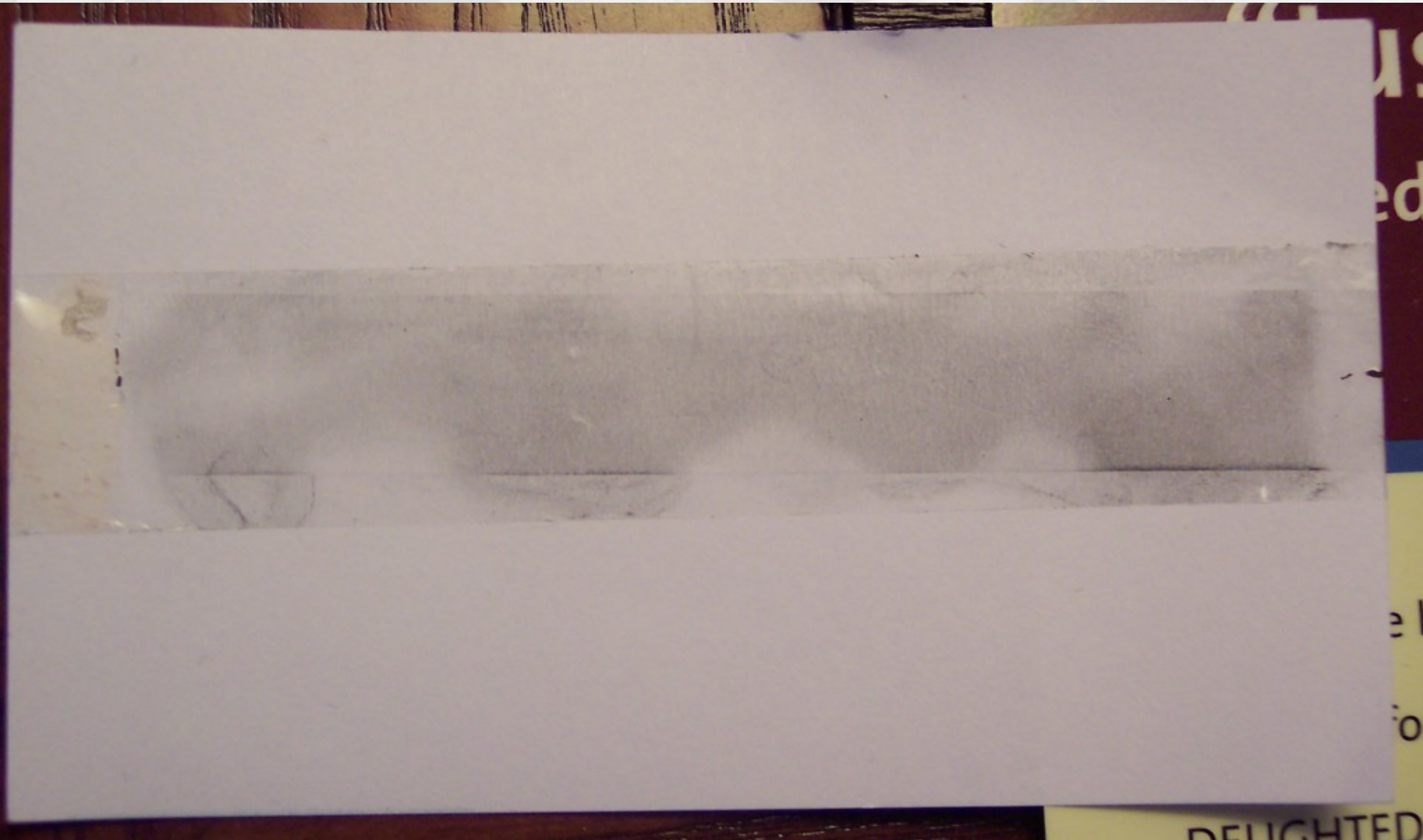
size matters!



But BPI is the same...



data matters!



data analysis

- **dmsb**
 - decode standard track formats & character sets
 - Joseph Battaglia
 - <http://www.sephail.net/articles/magstripe/>
- **binchop**
 - aid to look for patterns and parity
 - Major Malfunction
 - <http://www.alcrypto.co.uk>



data analysis

- **dab.py**

- decode Aiken Biphase WAV files
- Based on dab.c by Joseph Battaglia
 - <http://www.sephail.net/articles/magstripe/>

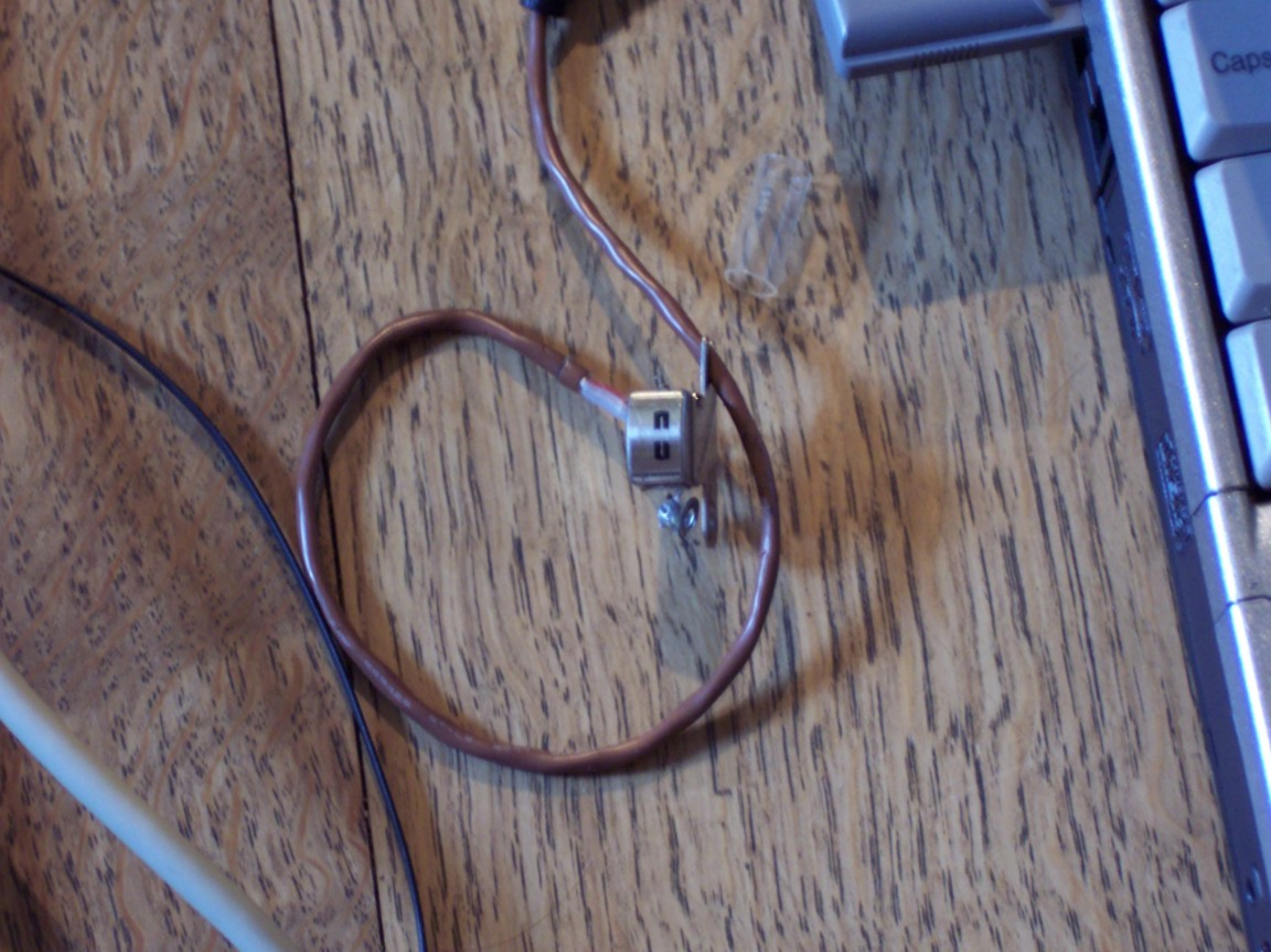
- **cab.py**

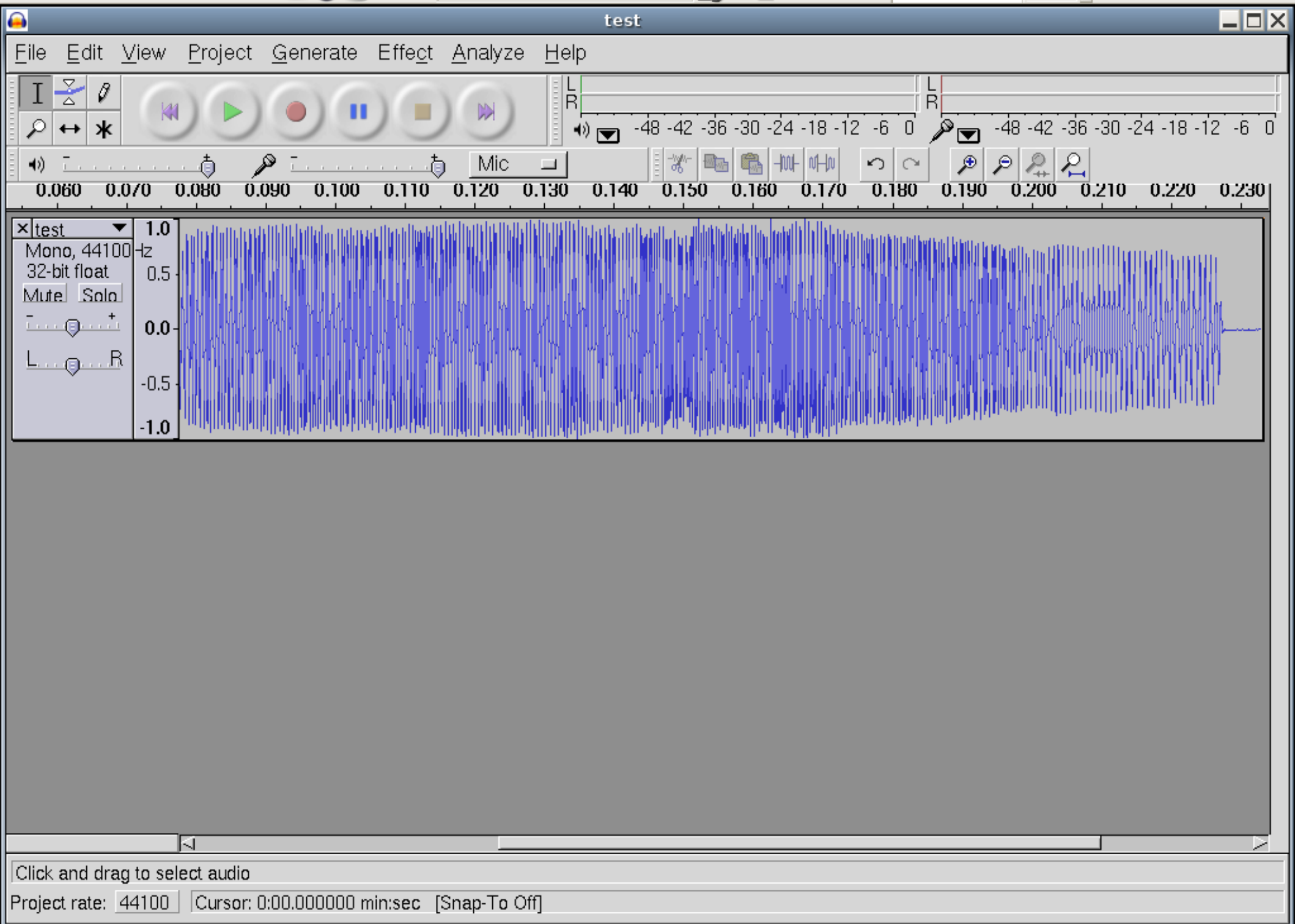
- create Aiken Biphase WAV files
- Major Malfunction
 - <http://www.alcrypto.co.uk>











Aiken Biphase

- **Form of FSK**

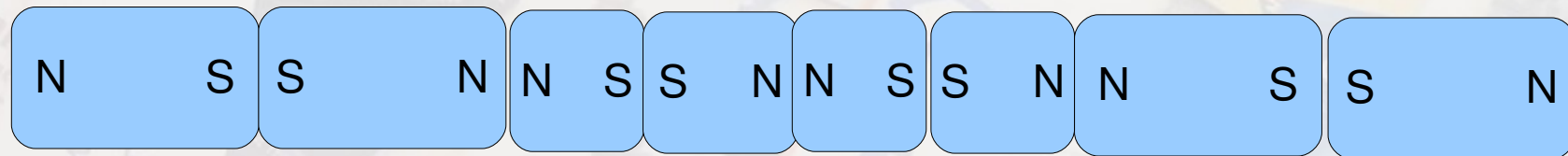
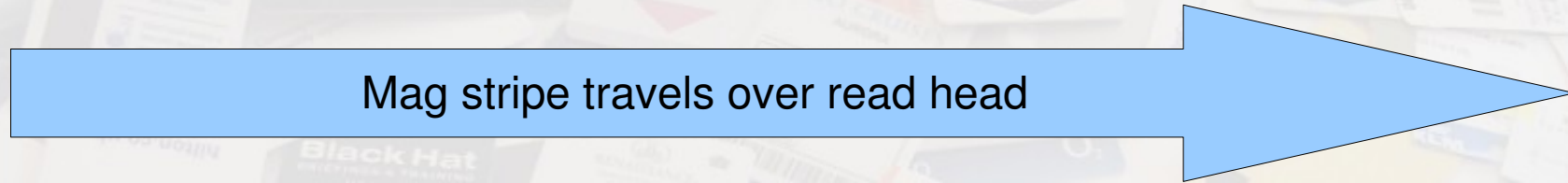
- Frequency Shift Keying
- F2F
 - Frequency Twice Frequency
 - ONE is exactly twice frequency of ZERO
- Used in a lot of protocols
 - IrDA, RFID, RF Remotes etc.

- **Self clocking**

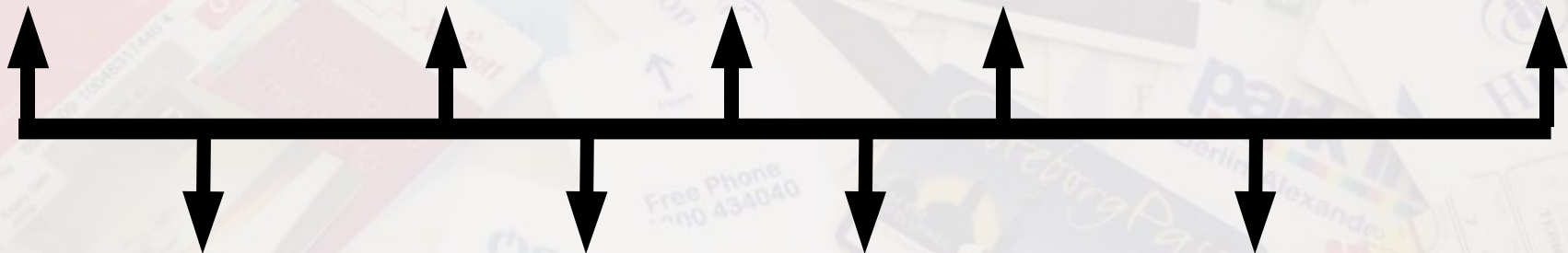
- Next tick timing based on current tick
- Allows for inaccurate manual swipe
- Extremely robust for hostile environments



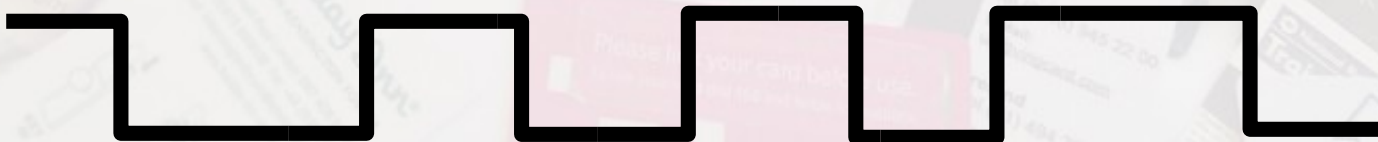
Magstripe to Waveform



North/North Flux Transition – Positive pulse

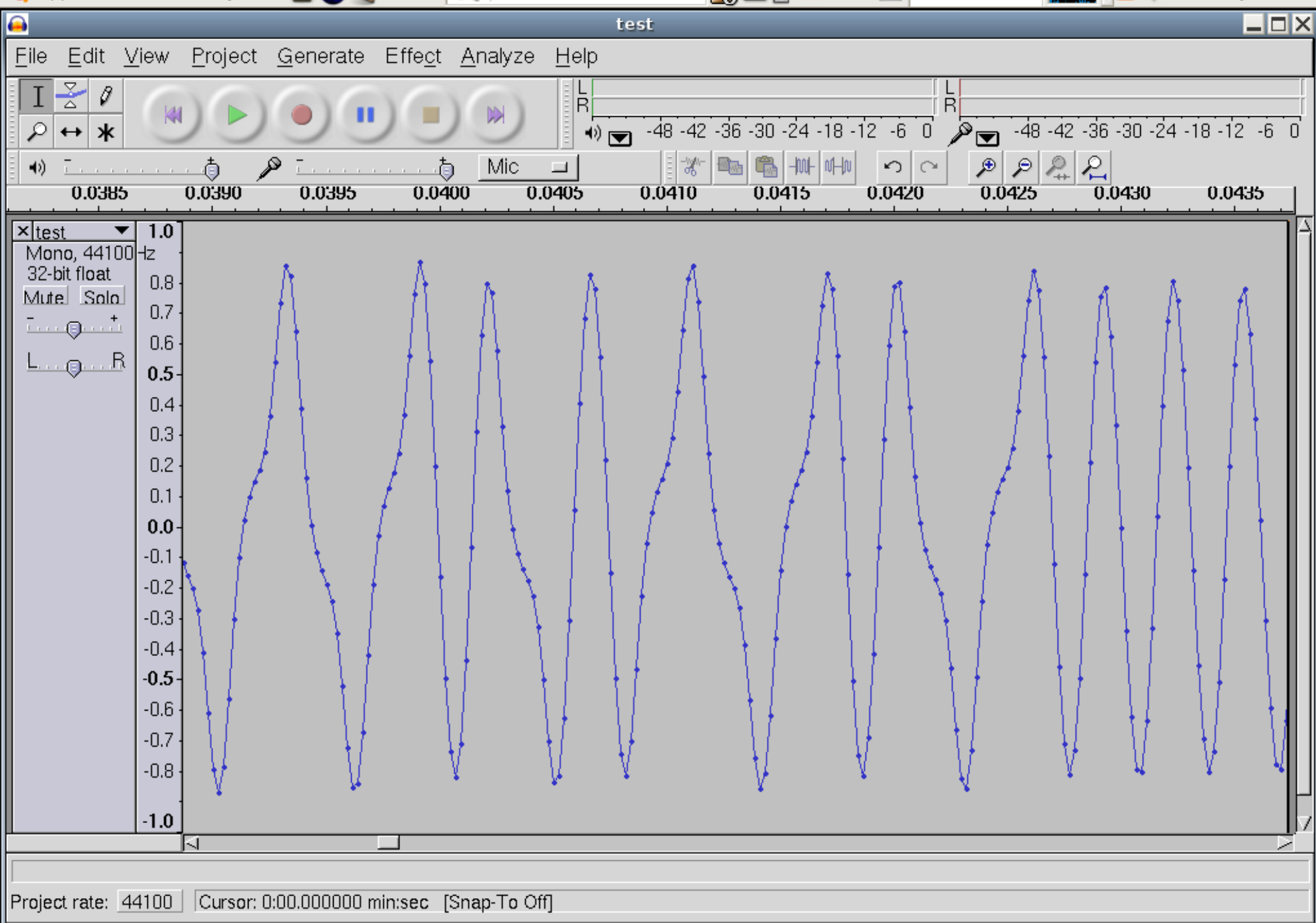


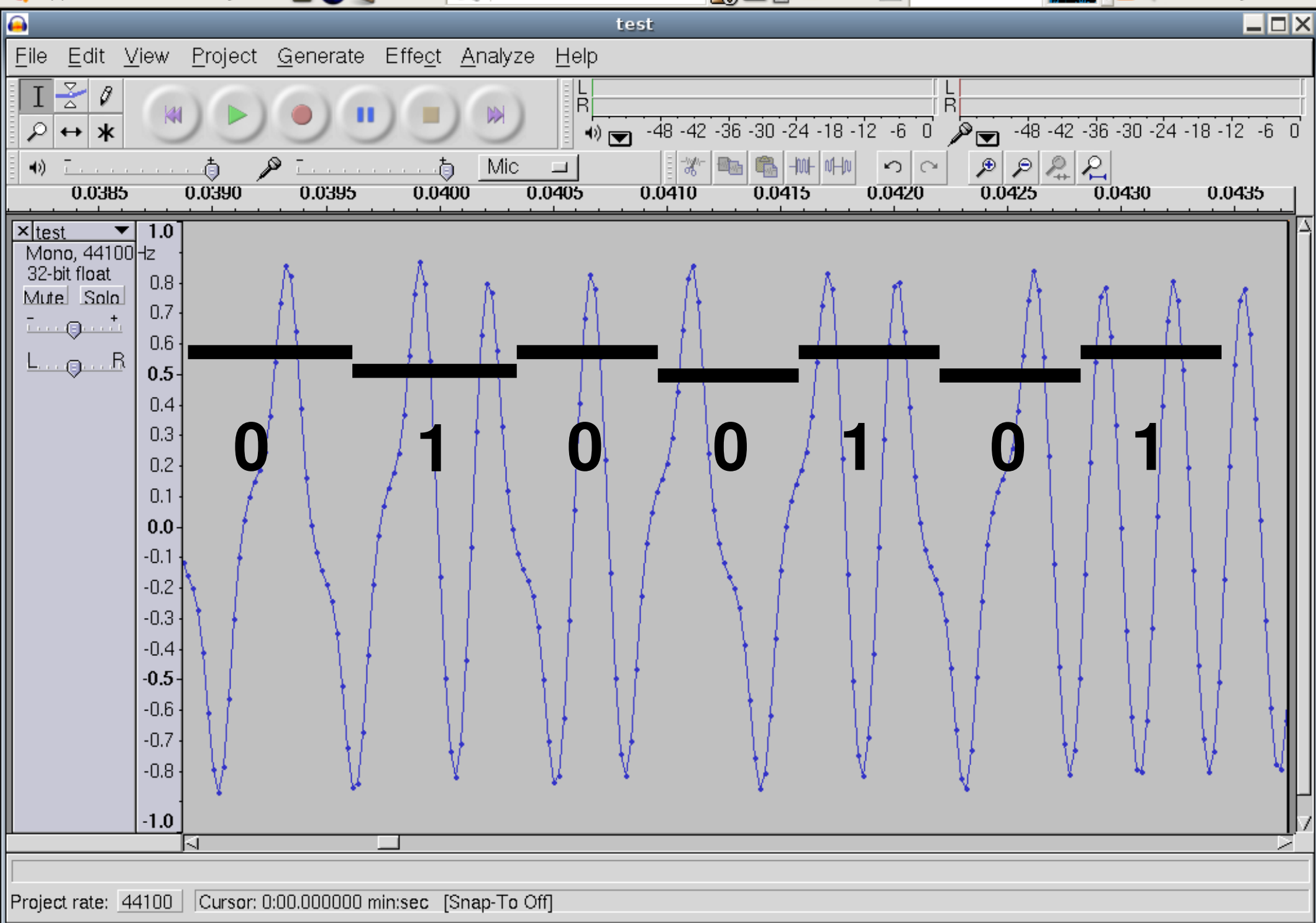
South/South – Negative pulse



F2F waveform



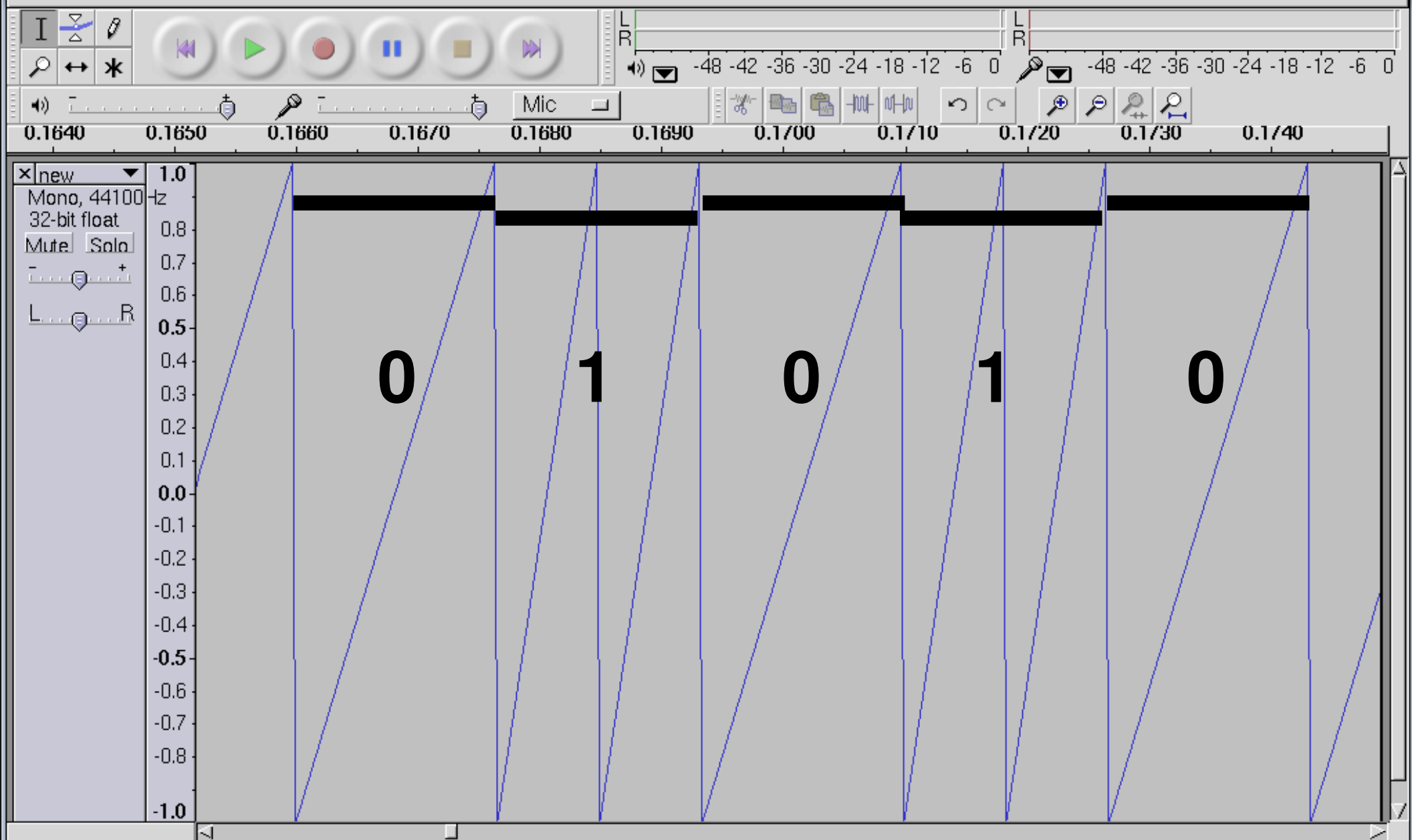




Generating Aiken WAVs

- **Should be pretty simple!**
 - One pulse for 0
 - Two pulses for 1





Testing: playback

- On-board sound card no good!
- Used Maya 44USB – higher quality



Result:

- I encoded:

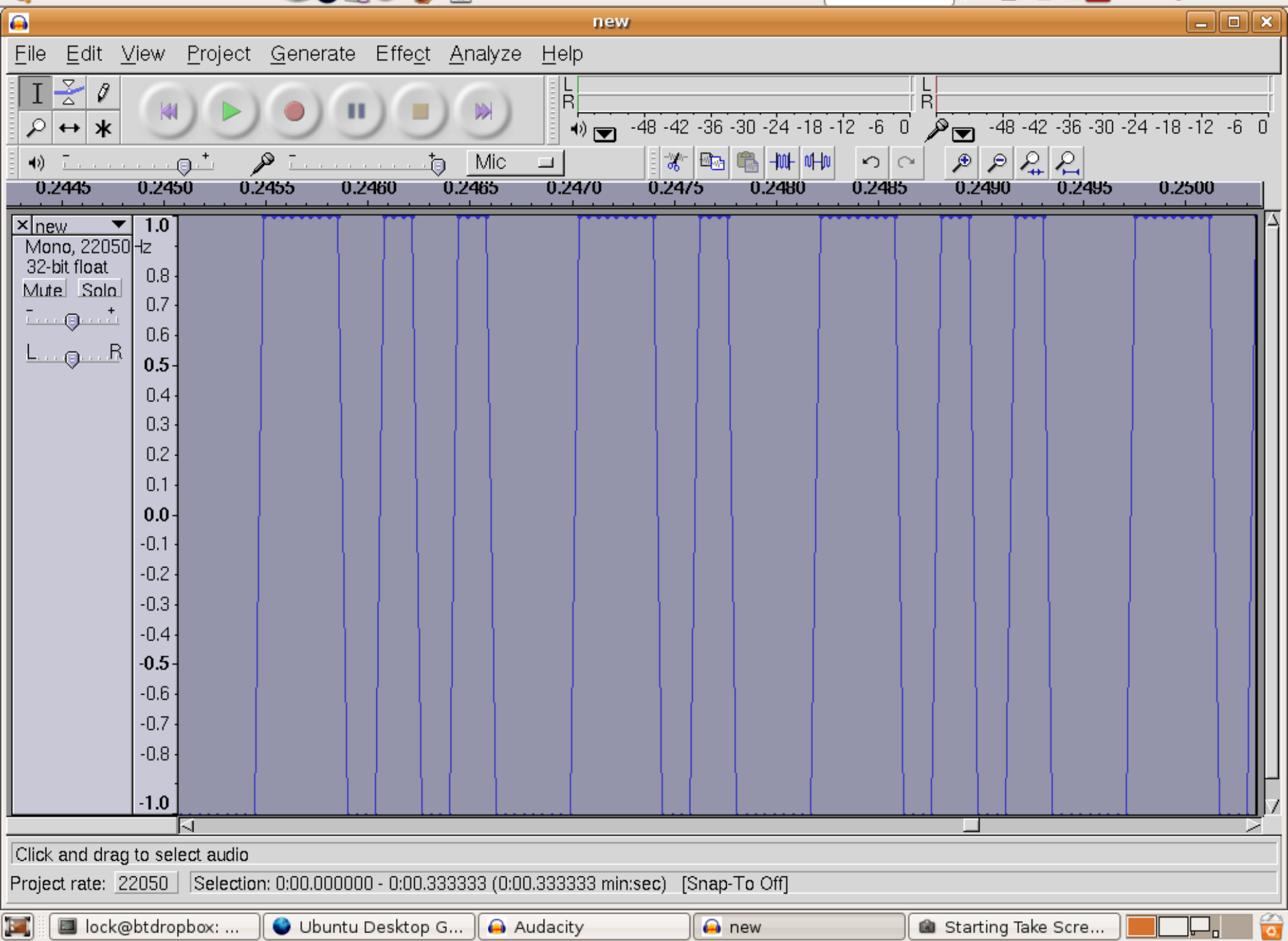
00010100010011111

- Reader saw:

0000001100110000001100001111111111

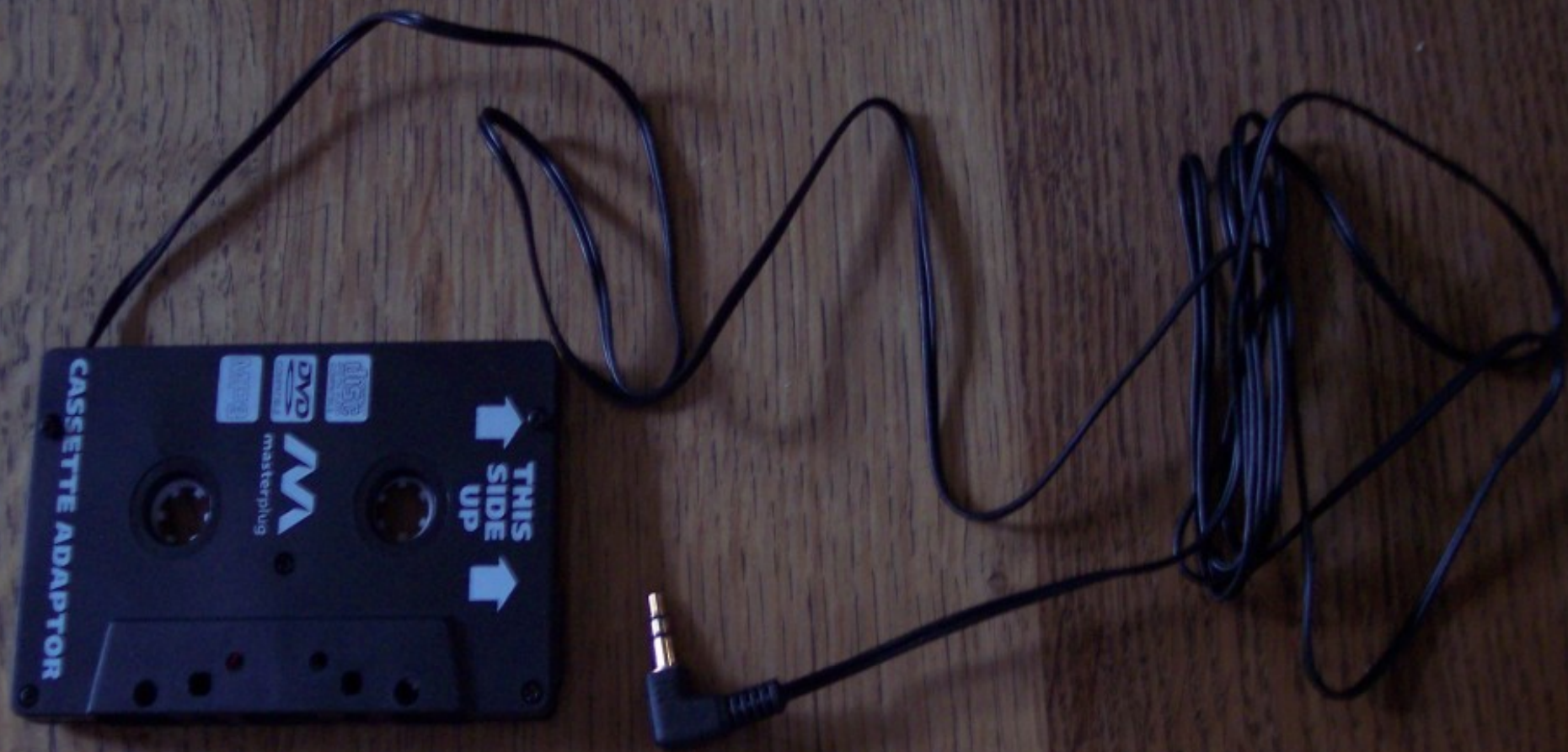
how weird is that???

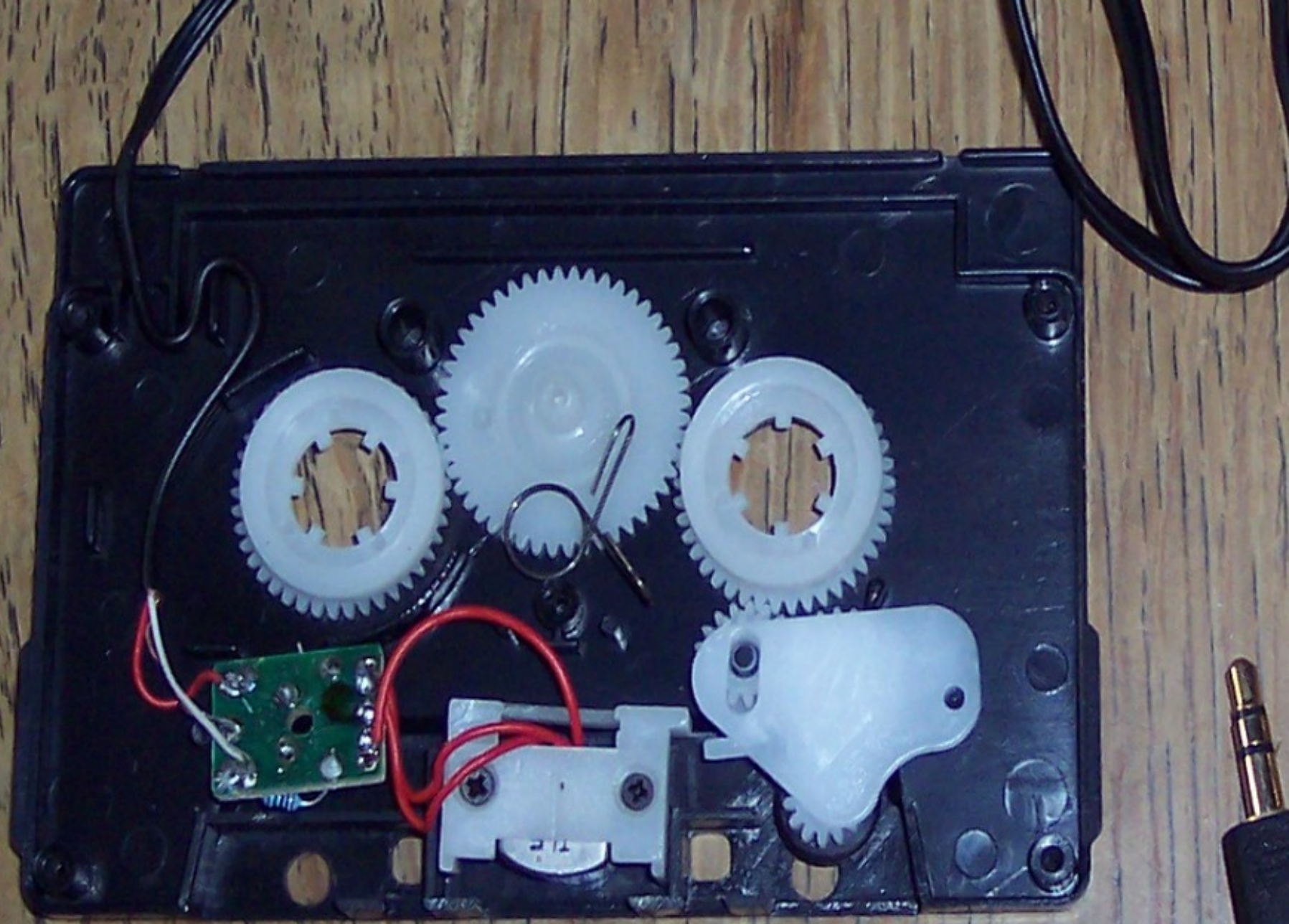




video







This top-up card enables you to add credit directly to your T-Mobile pay as you go or U-Fix account in a wide range of outlets. This card can only be used with the T-Mobile (UK) pay as you go and U-Fix service and is subject to these terms and conditions. Use of this card constitutes acceptance of those conditions. This is not a debit, credit or identity card, or a voucher of any kind. For more information, or if you experience difficulty whilst using this card, please dial 150, direct from your mobile phone.

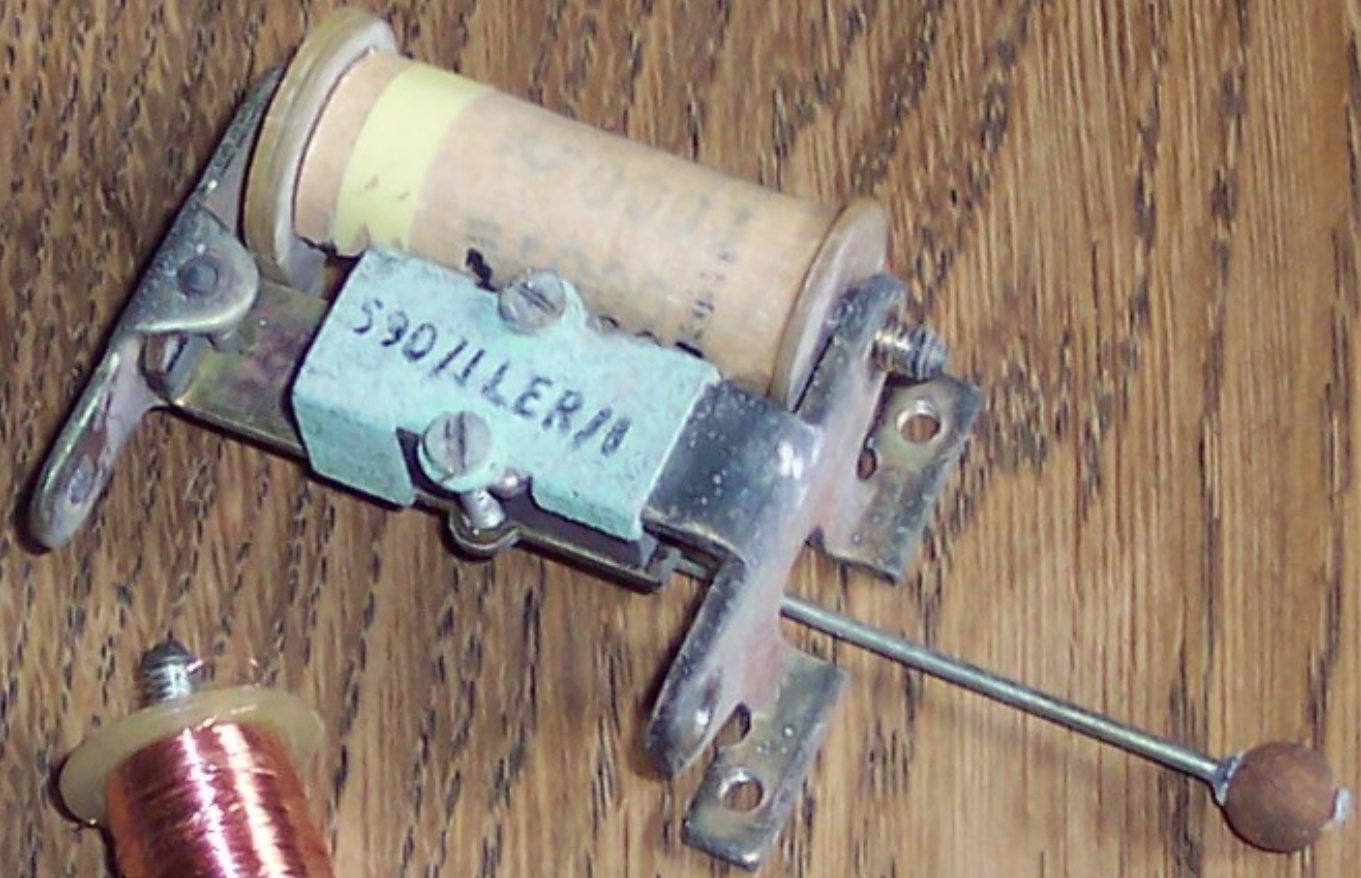
This card belongs to:

T · · Mobile ·

This top card enables you to add credit directly to your T-Mobile pay as you go or U-Fix account in a wide range of outlets. This card can only be used with the T-Mobile (UK) pay as you go and U-Fix service and is subject to these terms and conditions. Use of this card constitutes acceptance of those conditions. This is not a debit, credit or identity card, or a voucher of any kind. For more information, or if you experience difficulty whilst using this card, please dial 150, direct from your mobile phone.

This card belongs to:

T-Mobile





This top card enables you to add credit directly to your T-Mobile pay as you go or U-Fix account in a wide range of outlets. This card can only be used with the T-Mobile (UK) pay as you go and U-Fix service and is subject to these terms and conditions. Use of this card constitutes acceptance of those conditions. This is not a debit, credit or identity card, or a voucher of any kind. For more information, or if you experience difficulty whilst using this card, please dial 150, direct from your mobile phone.

This card belongs to:

T-Mobile

demonstration

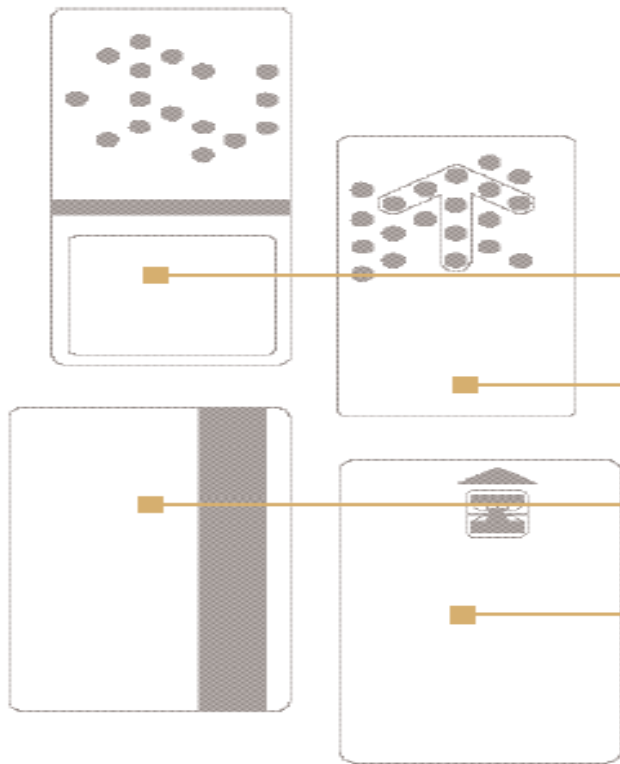


attack combining

mmirda + magstripe = drinks are on me!



evolution



Key cards for mechanical, optical, magnetic stripe and smart card operated locks.

Punched-hole cards

1. **Mechanical cards:** For all VingCard mechanical locking systems: 1040, 1050 and 1060 – VingCard Original.
2. **Optical cards:** For all VingCard optical electronic locking systems: 1070, 1080, 1090 and 1090e.
3. **Magnetic stripe cards:** For all VingCard magnetic stripe locking systems: 3000 and 2100 – Vision, 2100 Plus and DAVINCI.
4. **Smart cards and combination smart/magnetic stripe cards:** For all VingCard smart card locking systems – DAVINCI



Step 1



Step 2



Step 3



Step 4



next generation

- RFID
- biometric



RFID I/O tools: RFIDIoT

- <http://rfidiot.org>
 - python library
 - ISO 14443A/B
 - **MIFARE® Standard, MIFARE® 4k, MIFARE® Pro, MIFARE® Ultralight, MIFARE® DESFIRE, MIFARE® SmartMX, SLE 55Rxx, SLE 66CL160S, SLE 66CLX320P, SR17b, SR1X4K, ISO14443A Tags, ISO14443B Tags, Jewel Tag (IRT0302B11 KSW DIY Eng. Sample), Sharp B, ASK GTML2ISO, TOSMART P0b4**
 - support for ACG Dual ISO reader
 - <http://www.acg.de>
 - no drivers required – serial device

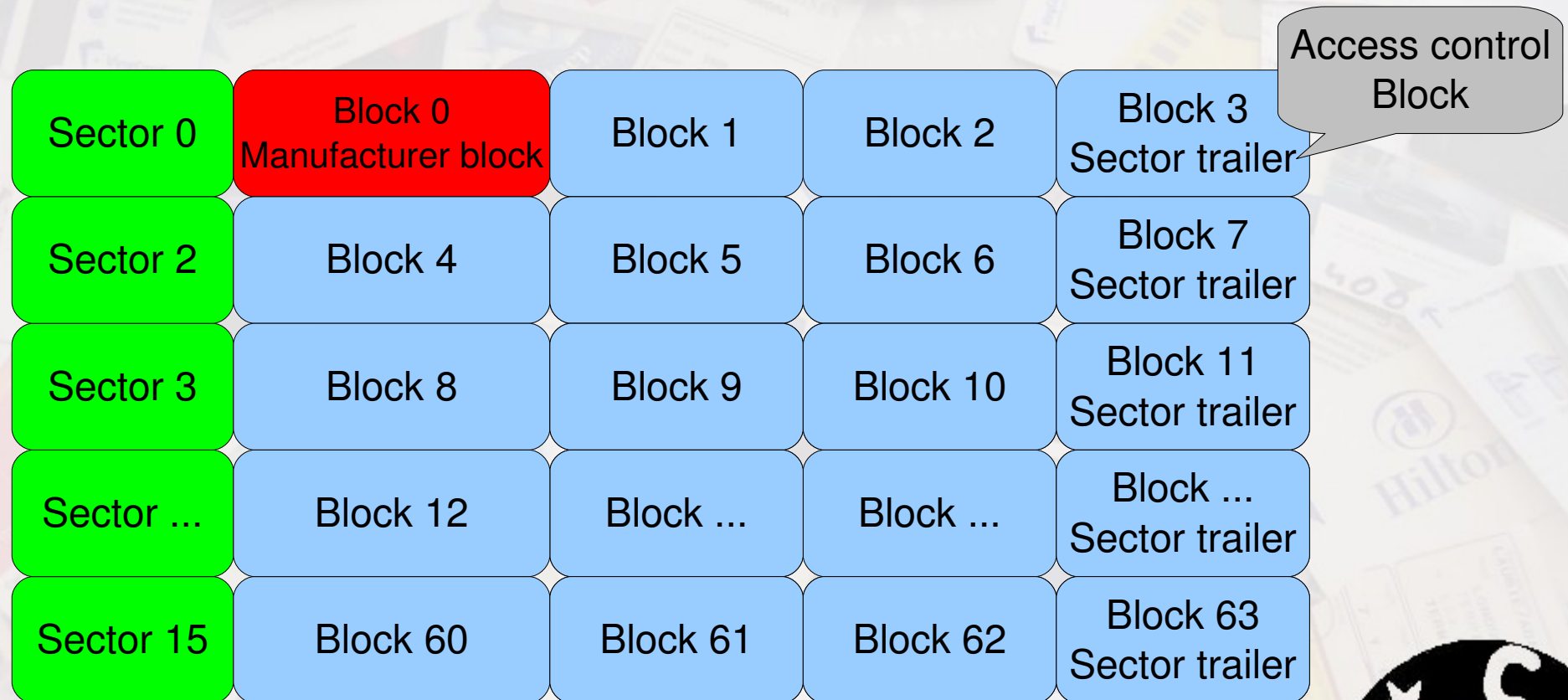


MIFARE tags

- Block layout
- Access controls
- Demonstration



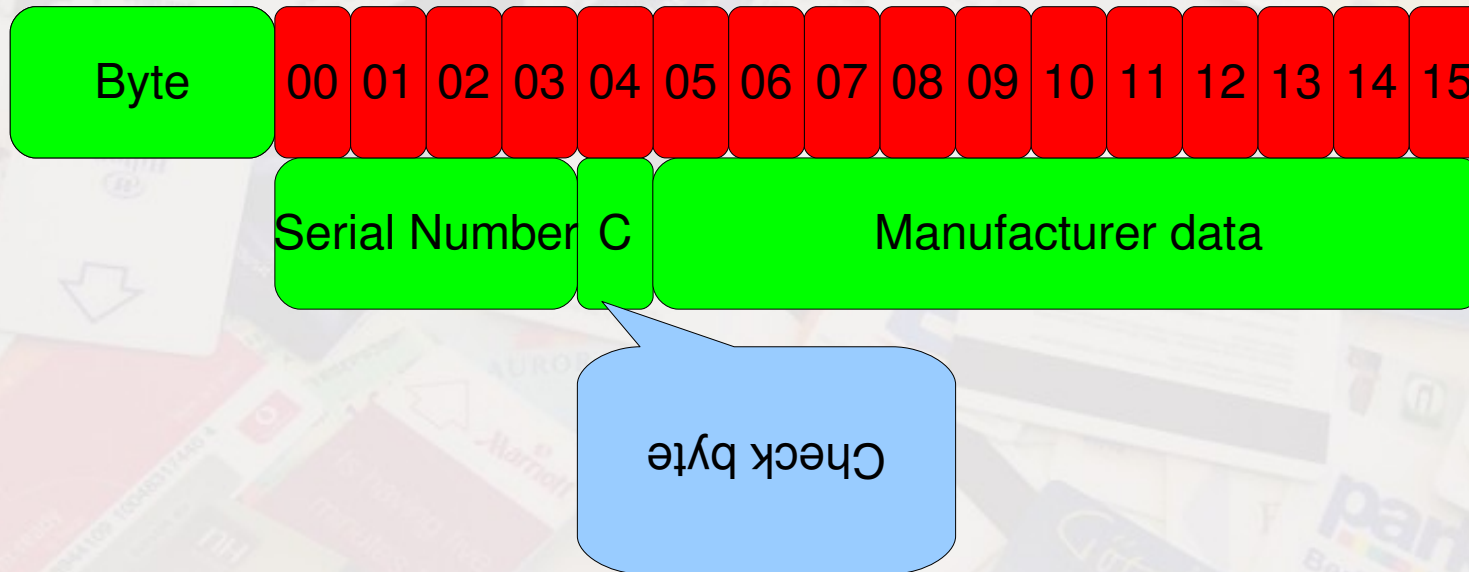
MIFARE 1K – block layout



16 sectors, 4 blocks per sector,
16 bytes per block = 1024 bytes



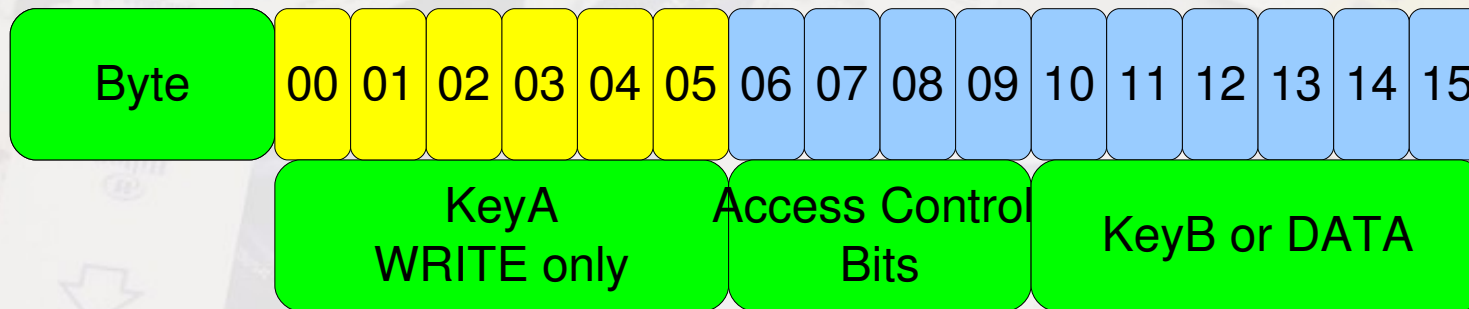
manufacturer block layout



Whole block is read only



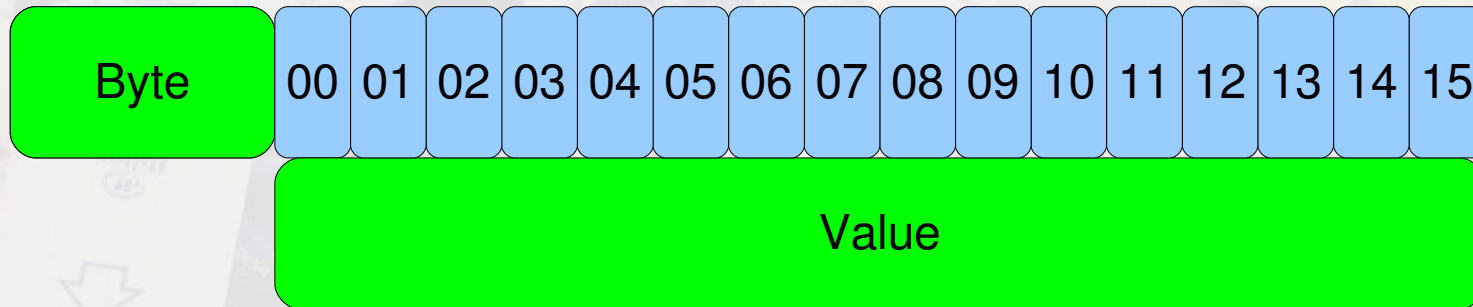
access control block layout



- **KeyA can never be read**
- **KeyB may be read and/or written**
 - depending on ACB
- **ACB for various combinations**
 - who may read/write keys
 - who may increment/decrement/restore value blocks



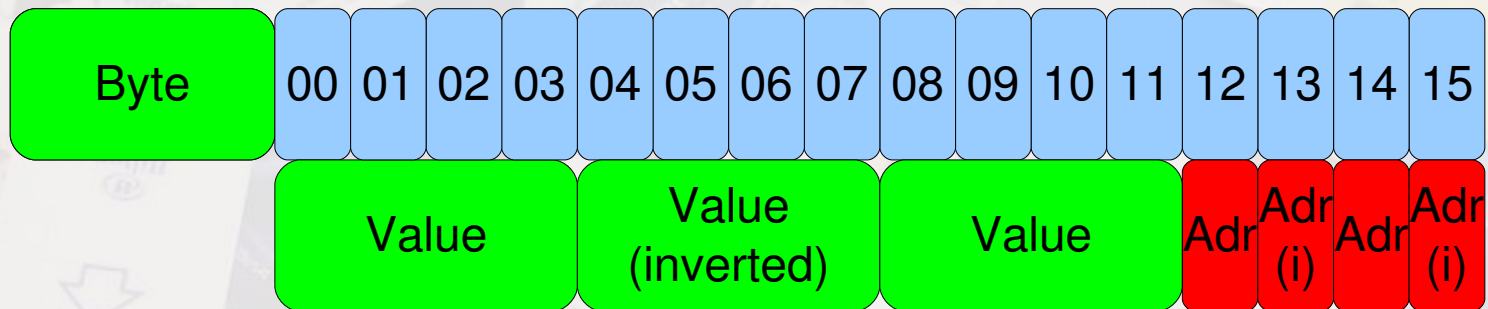
data block



- 1b bytes free storage



value block

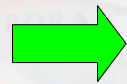


- **Value stored 3 times**
 - Twice non-inverted, once inverted
- **Address byte stored 4 times**
 - Twice non-inverted, twice inverted
 - Audit trails
 - Backup
 - Read only (by value commands)



tag operations

Card Select



Sector Login



Read/Write
etc.



demonstration



Questions?







TVBGoon ... will mod for...

- **beer**
- **caffeine**
- **pizza**
- **shwag**
- **loose women**



oh dear...



majormal@pirate-radio.org
<http://www.alcrypto.co.uk>

