MAGS TRIP EMAD NESS

VALID FROM
04/06

EXPIRES END
44/20

OF-3

MALFUNCTION, MAJ.

CANSECWEST
ISSUER

06
ISSUE

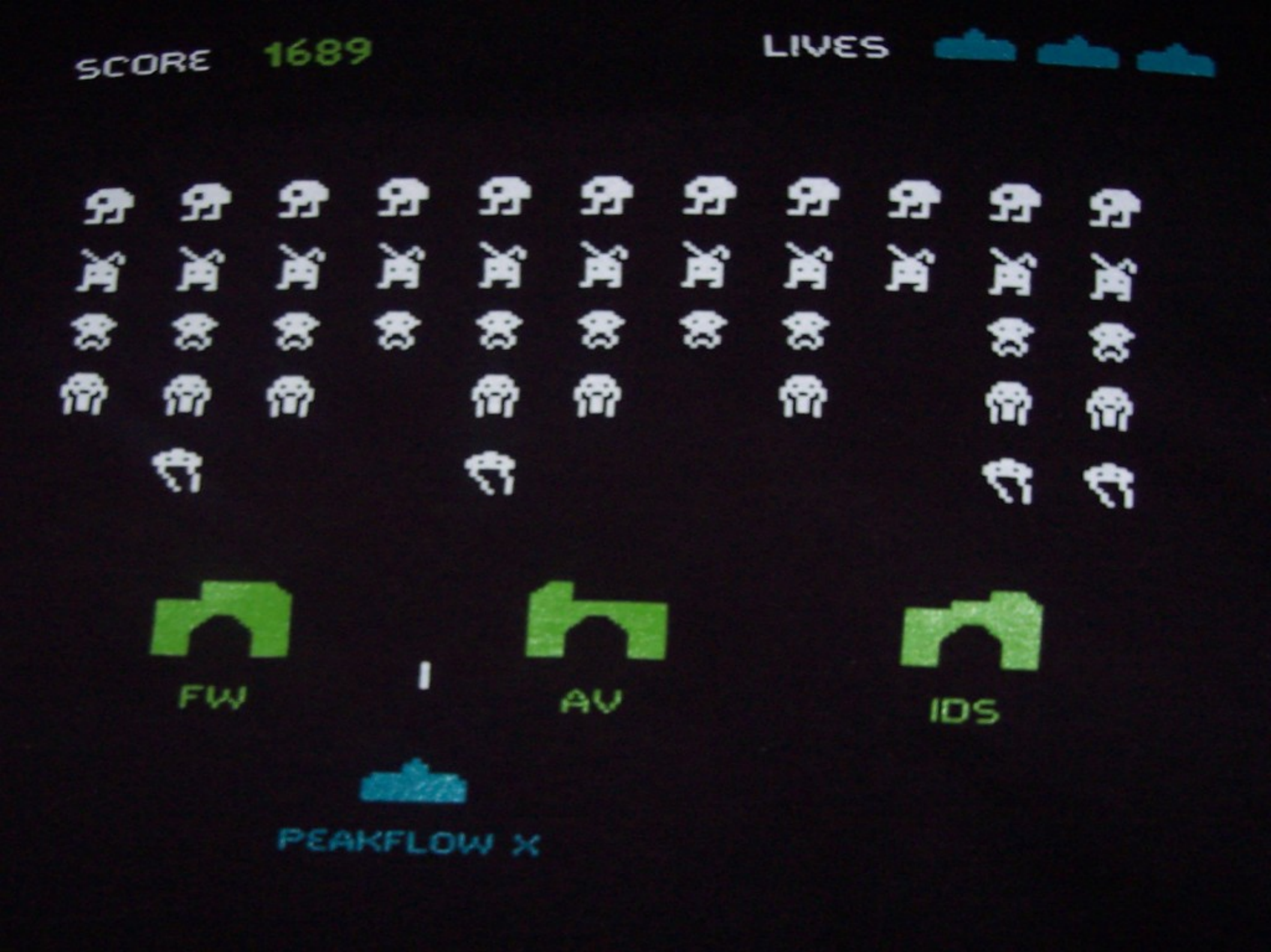
DC-44-20
SORT CODE

who am i ?

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

why mag stripe ?

- old skewl
- 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


TESCO mobile
Every little helps
top-up
top-up card
RENAISSANCE
VANCOUVER HOTEL
HARBOURSIDE
renaissancehotels.com
1-800-HOTELS-1
Card must be Activated
Please see leaflet for details
Top-up
O2
Cashpoint
Lloyds TSB
cashpoint
VALID FROM
EXPIRES END

spot the room key...

spot the room key...

spot the ATM card...

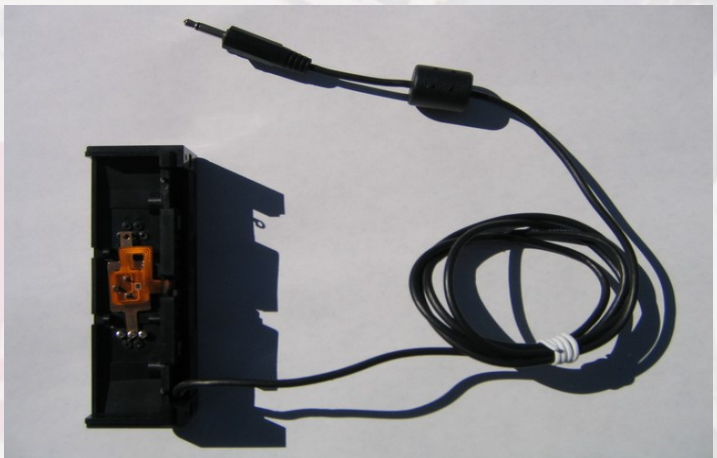
spot the ATM card...

equipment - makstripe

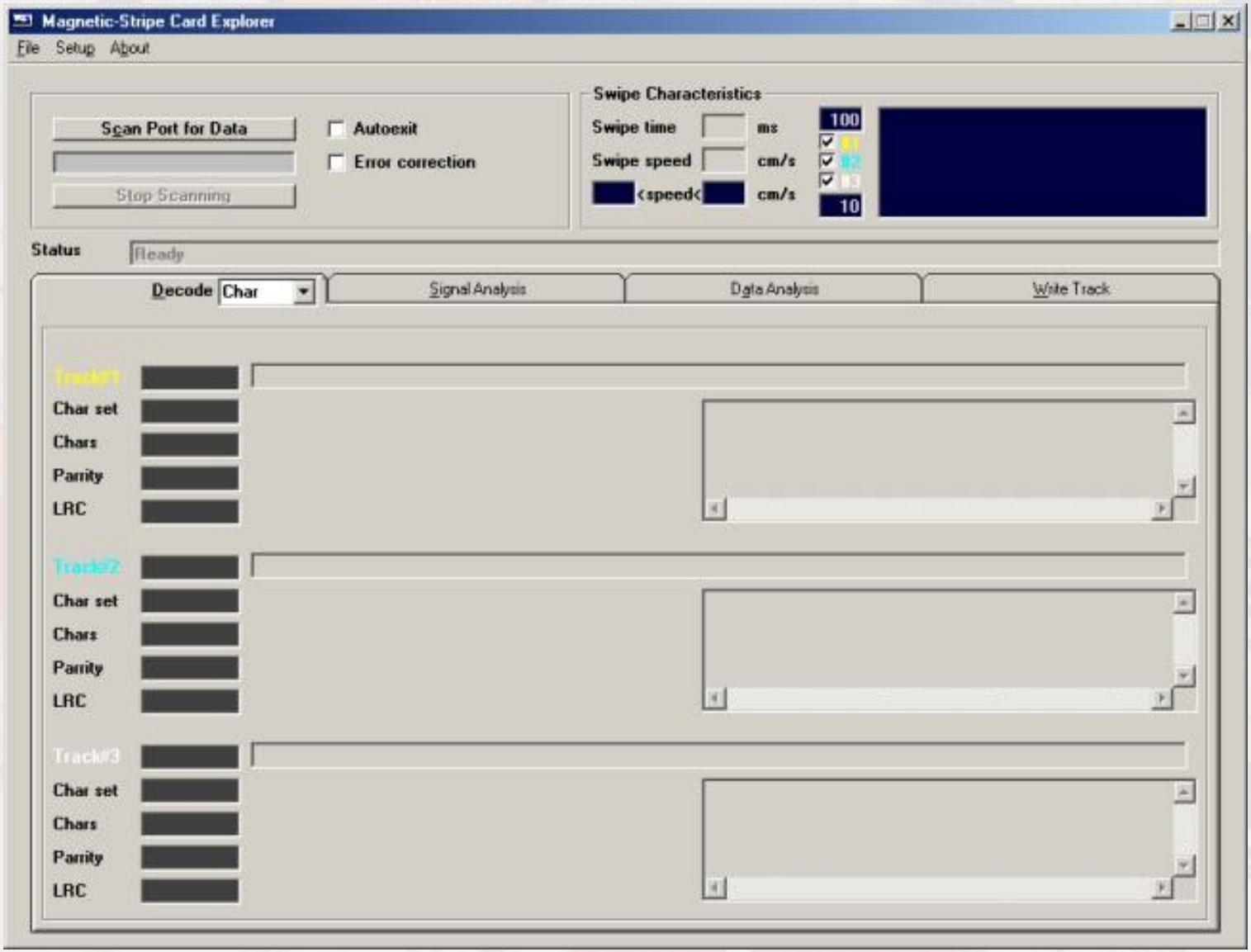
- http://www.makinterface.de
- Parallel port
- Read / Write all 3 tracks
- Raw data
  - Does not care about checksums
  - Does not care about parity
- Windows support only :(
  - not working with VMWare :(:(

equipment

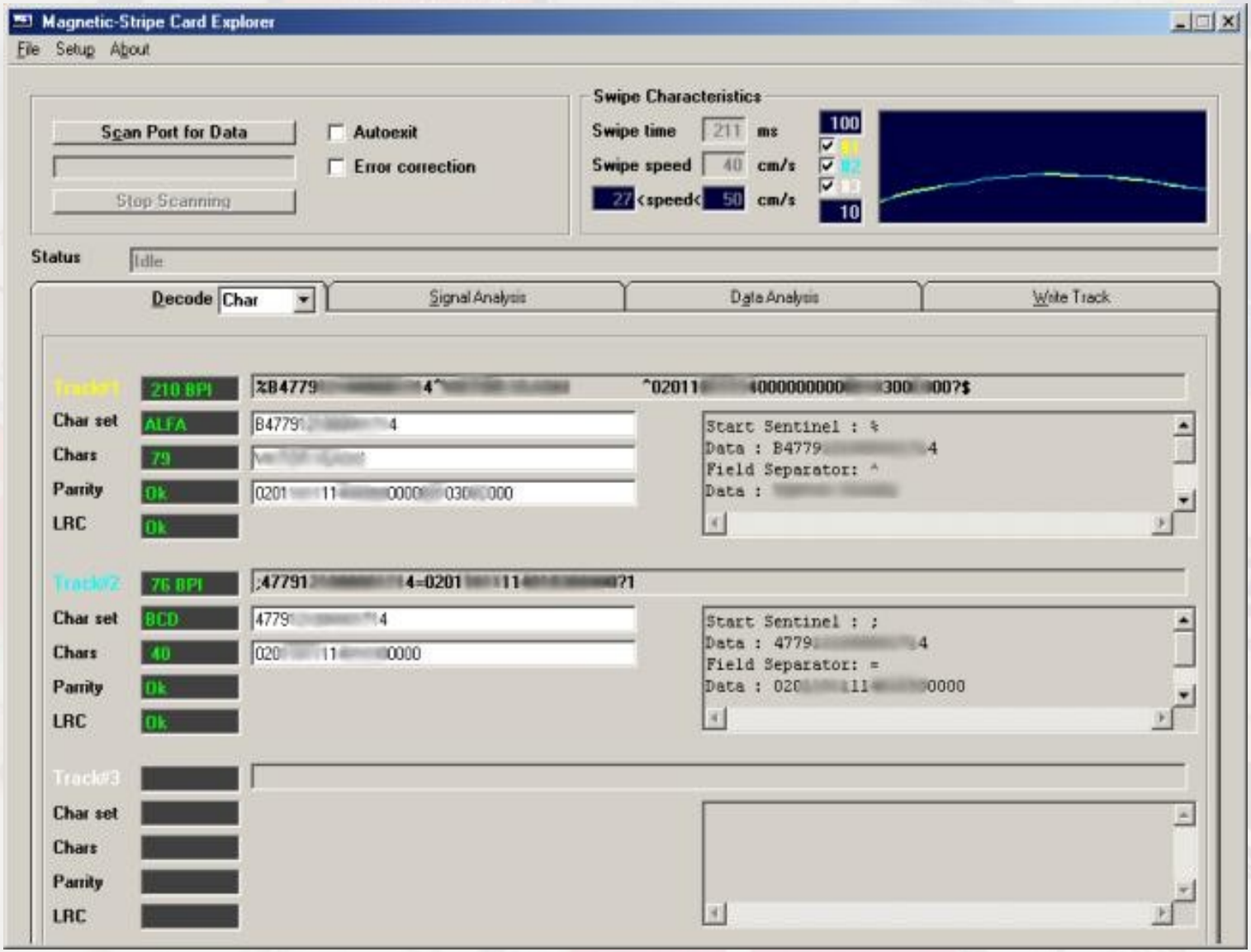
- http://www.sephail.net/articles/magstripe
- Audio output
  - Analyse WAV files offline
- Read all 3 tracks plus non-standard
- Raw data
  - Does not care about checksums
  - Does not care about parity
- Read only



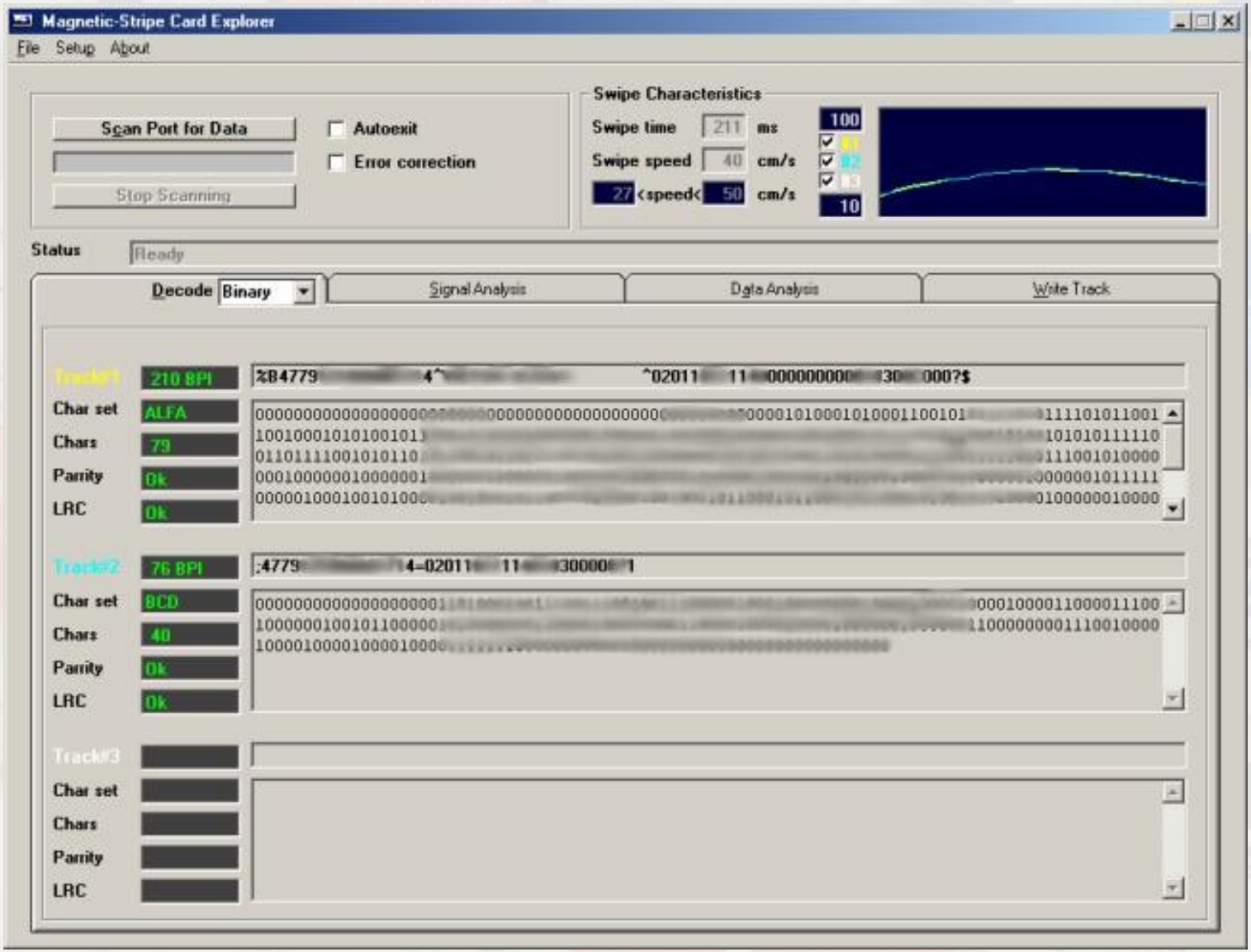
equipment - makstripe



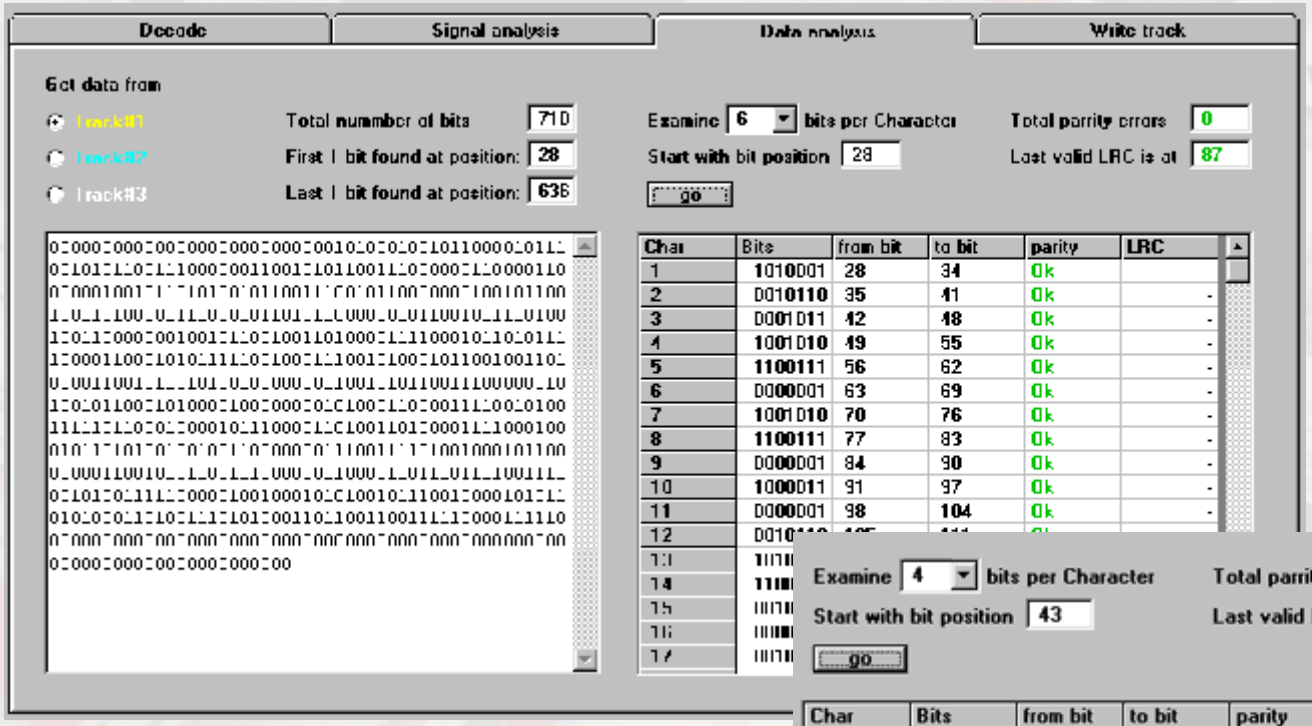
equipment - makstripe

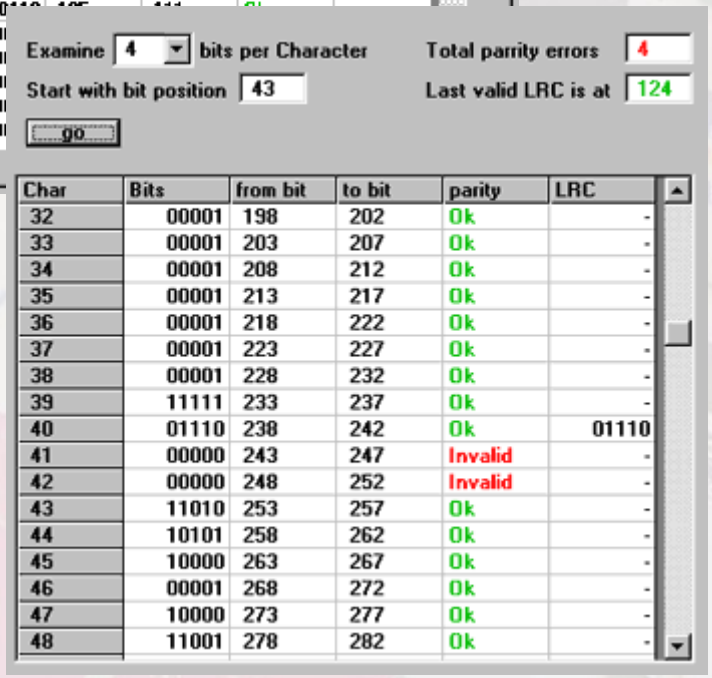


equipment - makstripe

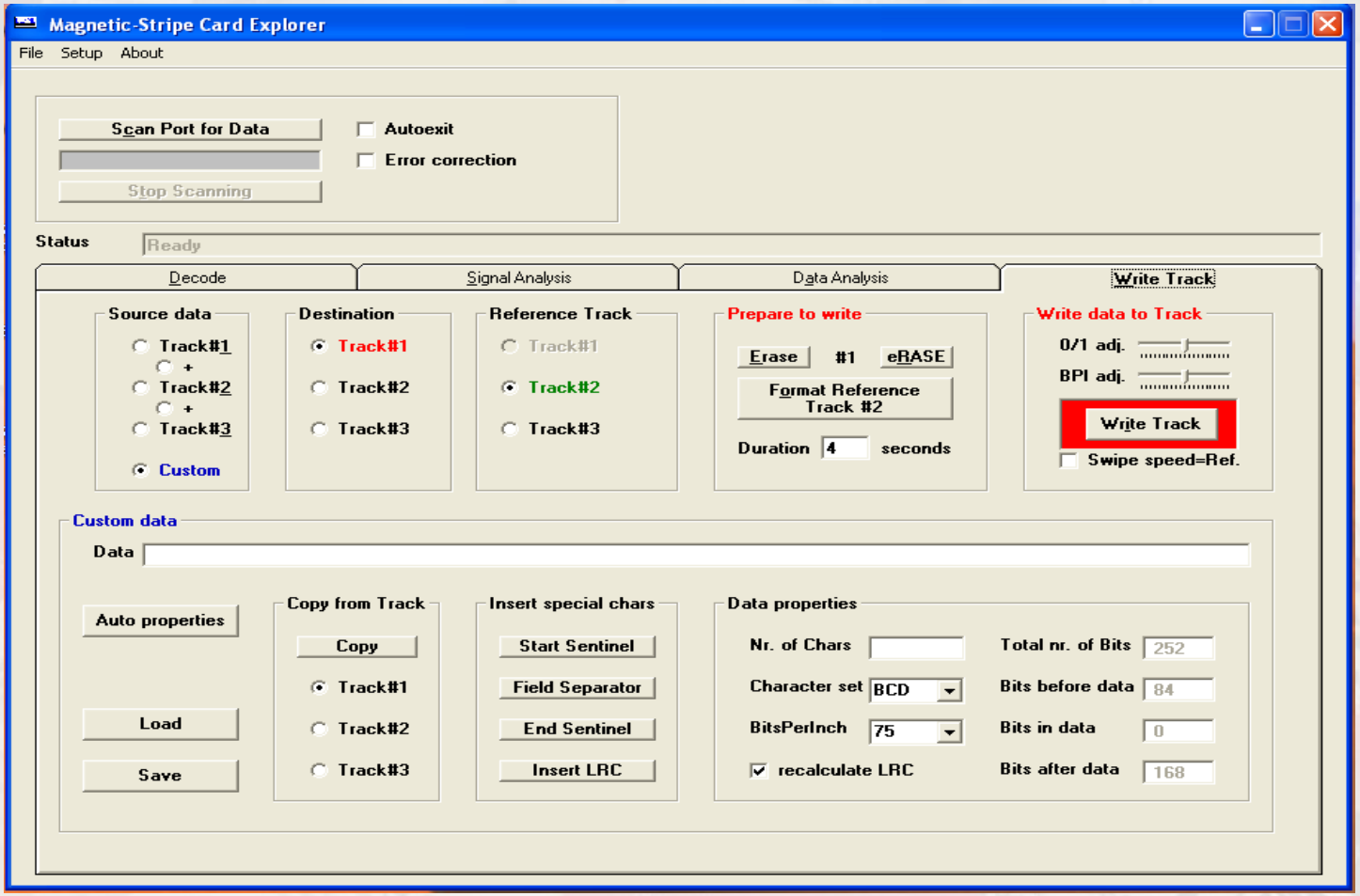


analysis - makstripe





write - makstripe



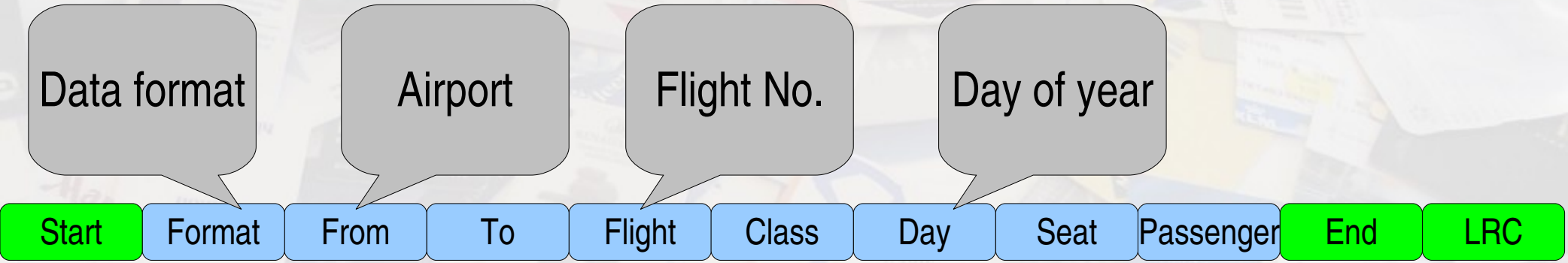
standard track formats

- 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

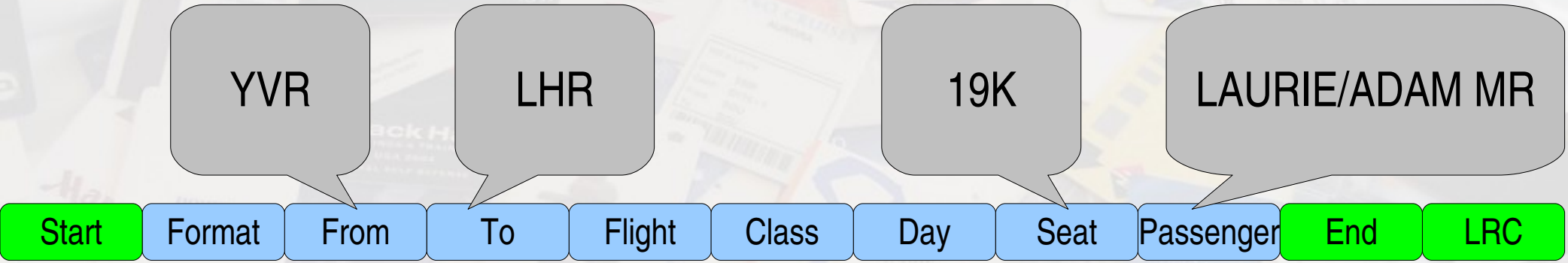
track standards - IATA

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

track standards - IATA

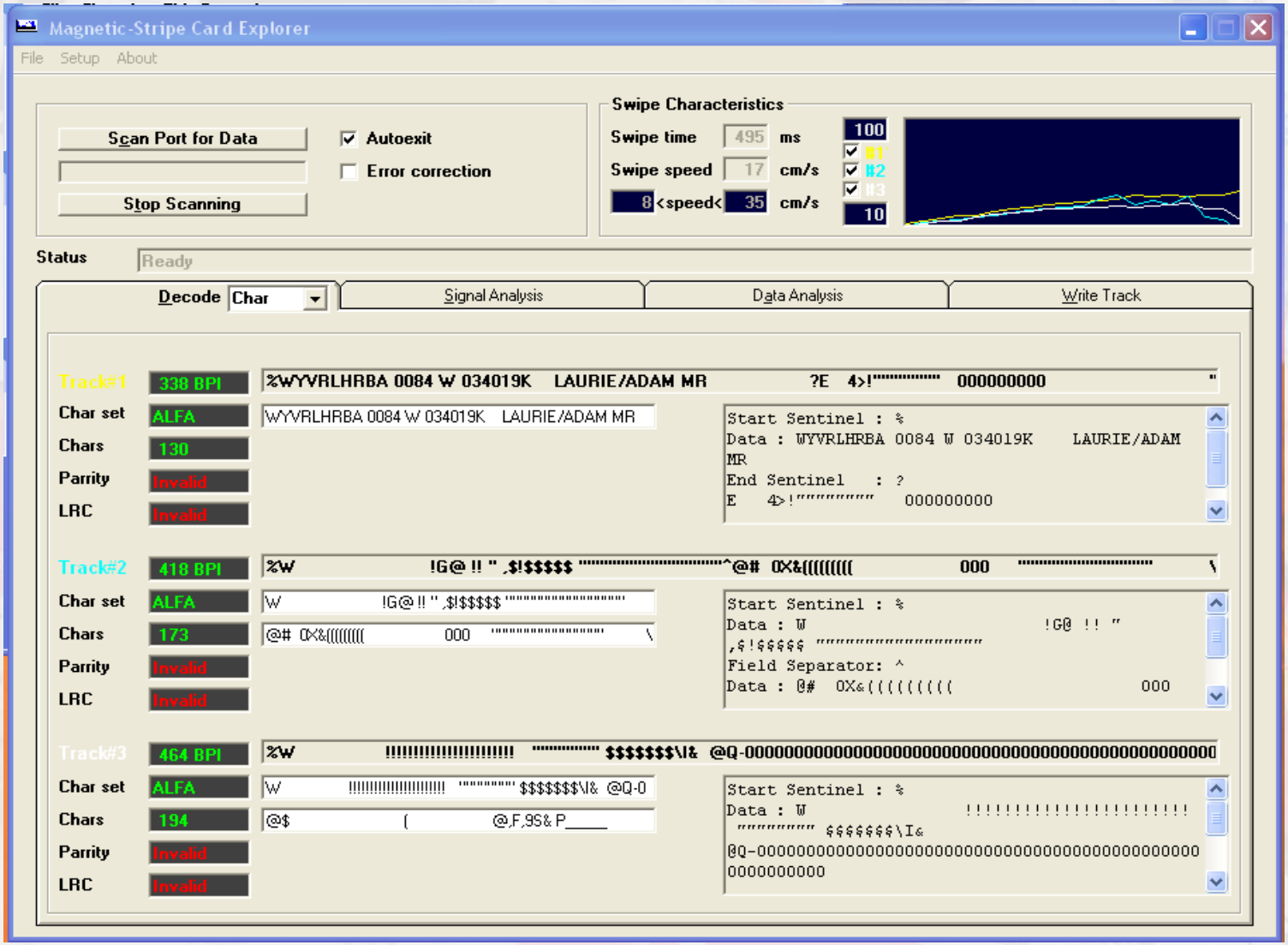


track standards - IATA

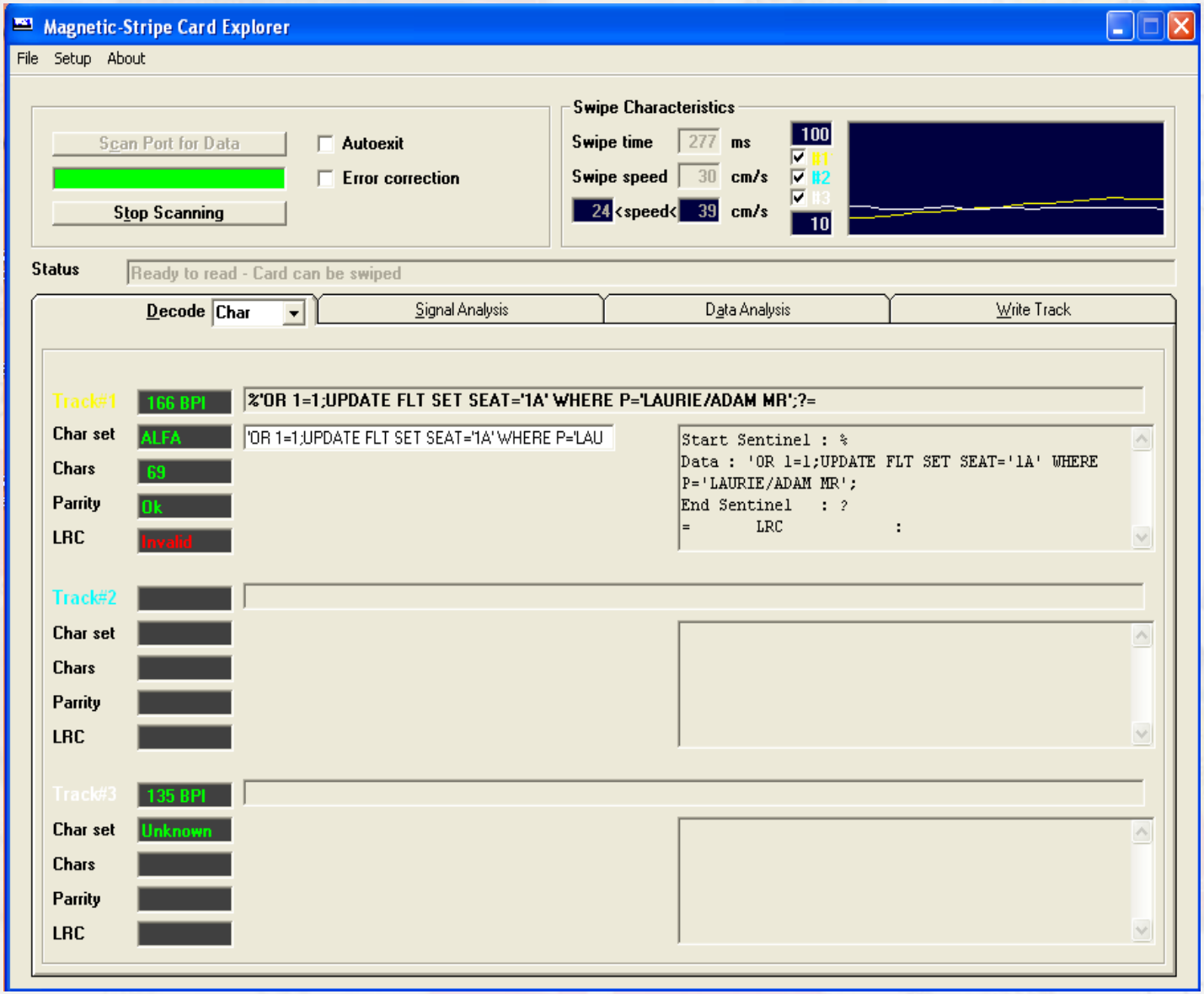


%WYVRLHRBA 0084 W 034019K LAURIE/ADAM MR ?E

before


Magnetic-Stripe Card Explorer
File Setup About
Scan Port for Data
Stop Scanning
Autoexit
Error correction
Swipe Characteristics
Swipe time 495 ms
Swipe speed 17 cm/s
8 <speed< 35 cm/s
100
#1
#2
#3
10
Status
Ready
Decode Char
Signal Analysis
Data Analysis
Write Track
Track#1 338 BPI
%WYVRLHRBA 0084 W 034019K LAURIE/ADAM MR ?E 4>!"""""""""""" 000000000 "
Char set ALFA
Chars 130
Parrity Invalid
LRC Invalid
WYVRLHRBA 0084 W 034019K LAURIE/ADAM MR
Start Sentinel : %
Data : WYVRLHRBA 0084 W 034019K LAURIE/ADAM
MR
End Sentinel : ?
E 4>!"""""""""""" 000000000
Track#2 418 BPI
%W !G@ !! " ,$!$$$$$ """""""""""""""""""""""""^@# 0X&((((((((((000 """""""""""""""""""""""""" \
Char set ALFA
Chars 173
Parrity Invalid
LRC Invalid
W !G@ !! " ,$!$$$$$ """""""""""""""""""""""""
@# 0X&((((((((((000 """""""""""""""""""""""""" \
Start Sentinel : %
Data : W !G@ !! "
,$!$$$$$ """""""""""""""""""""""""
Field Separator: ^
Data : @# 0X&(((((((((((000
Track#3 464 BPI
%W !!!!!!!!!!!!!!!!!!!!!!!! """""""""""""" $$$$$$$\I& @Q-0000000000000000000000000000000000000000000000000000000000
Char set ALFA
Chars 194
Parrity Invalid
LRC Invalid
W !!!!!!!!!!!!!!!!!!!!!!!! """""""""""""" $$$$$$$\I& @Q-0
@$ (@.F.9S& P_____
Start Sentinel : %
Data : W !!!!!!!!!!!!!!!!!!!!!!!!
"""""""""""""" $$$$$$$\I&
@Q-0000000000000000000000000000000000000000000000000000000000
0000000000

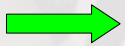
after


Magnetic-Stripe Card Explorer
File Setup About
Scan Port for Data
Stop Scanning
Autoexit
Error correction
Swipe Characteristics
Swipe time 277 ms
Swipe speed 30 cm/s
24 <speed< 39 cm/s
100
#1
#2
#3
10
Status
Ready to read - Card can be swiped
Decode Char
Signal Analysis
Data Analysis
Write Track
Track#1 166 BPI
%'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
Parrity 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
Parrity
LRC
Track#3 135 BPI
Char set Unknown
Chars
Parrity
LRC

hotel door locks

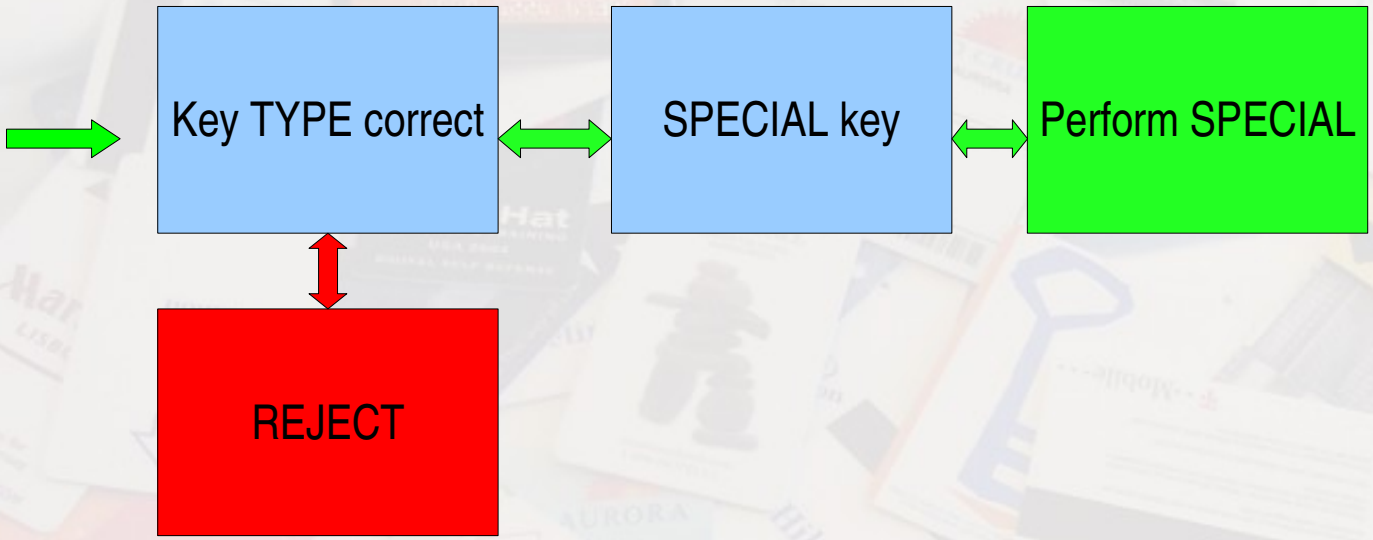
- passive
  - all logic in the lock
- active
  - reader only
  - all logic on back-end
  - centralised alarms & reporting

passive locks



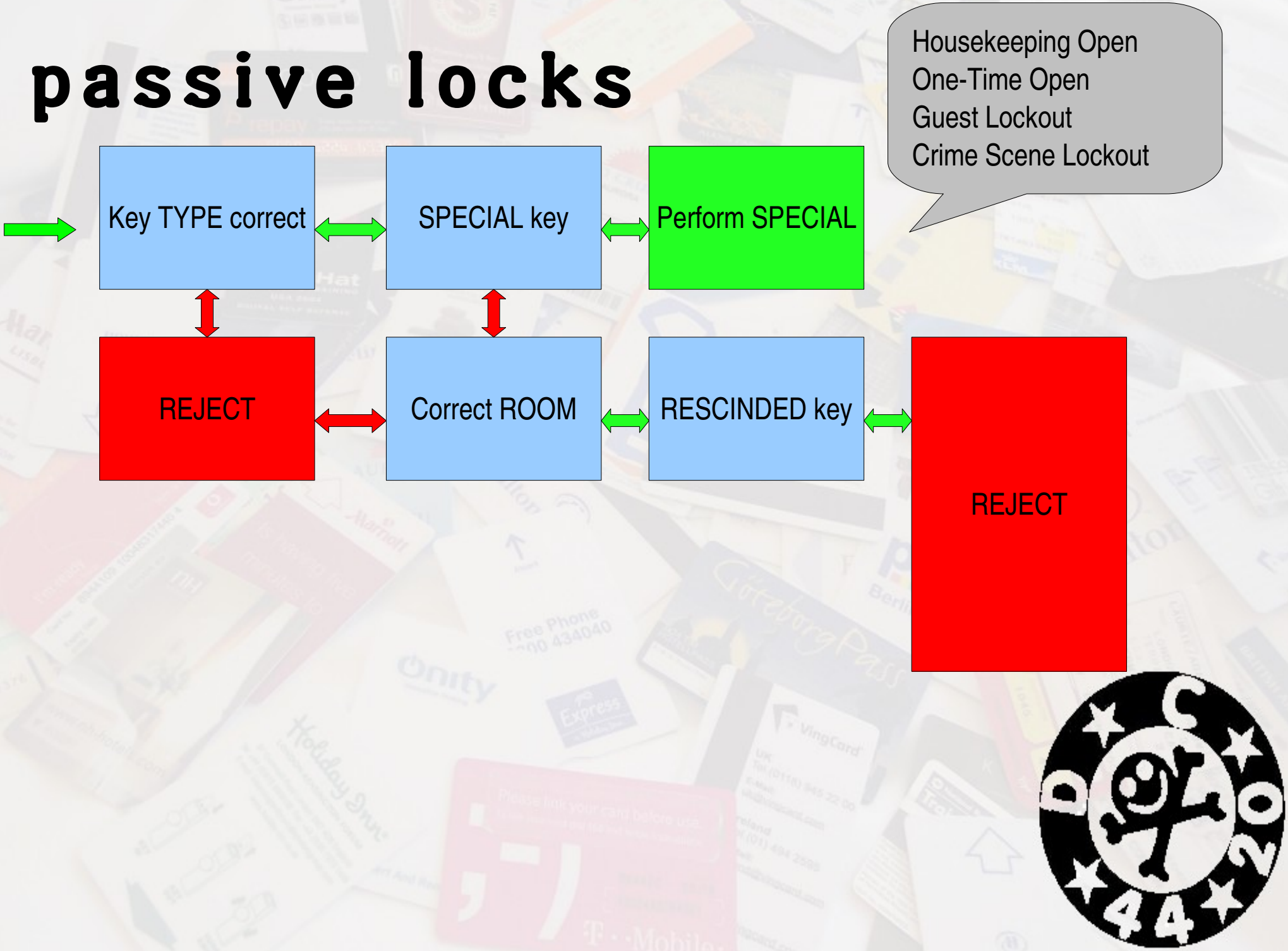
Key TYPE correct

passive locks

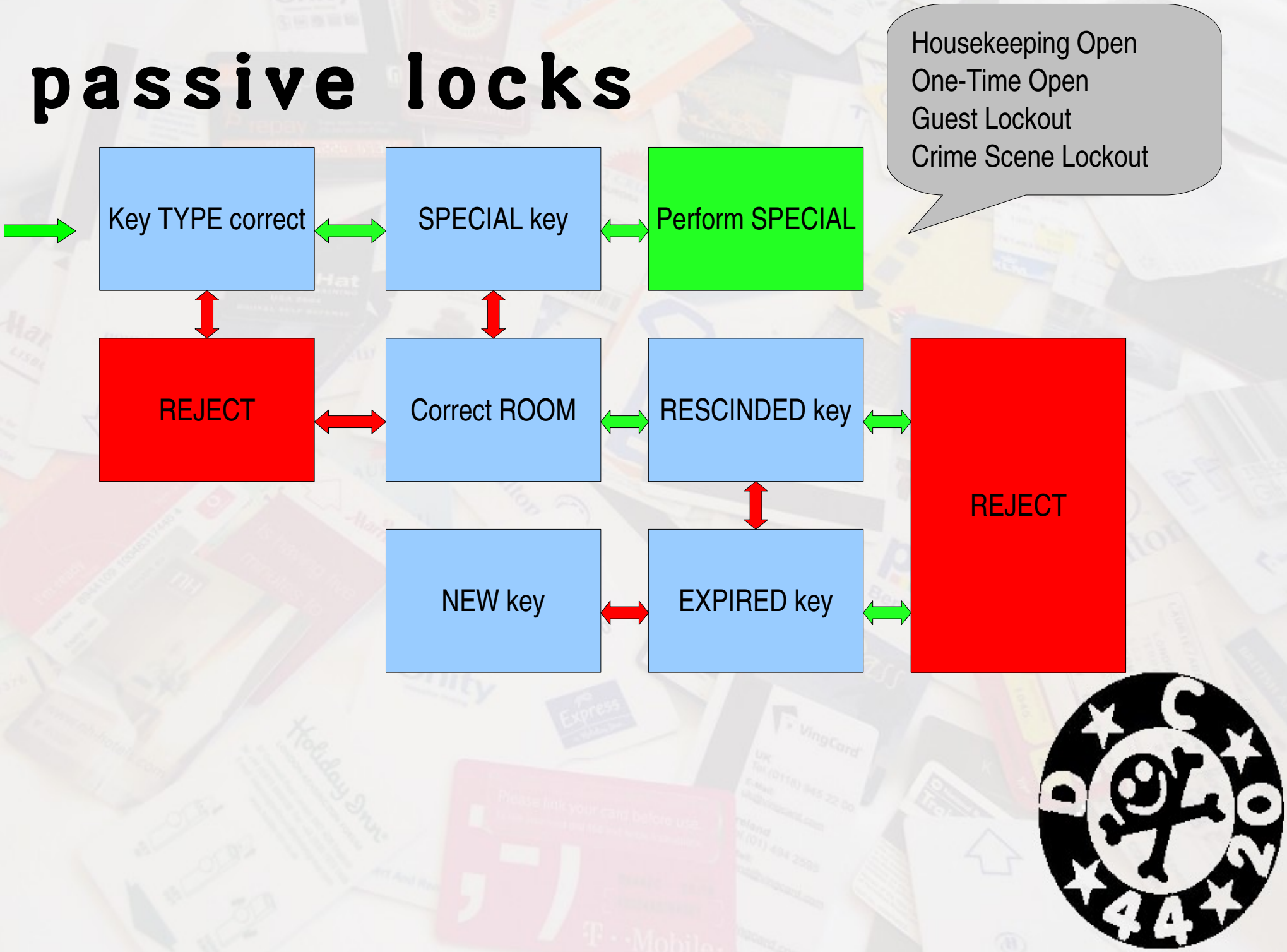


Housekeeping Open
One-Time Open
Guest Lockout
Crime Scene Lockout

passive locks

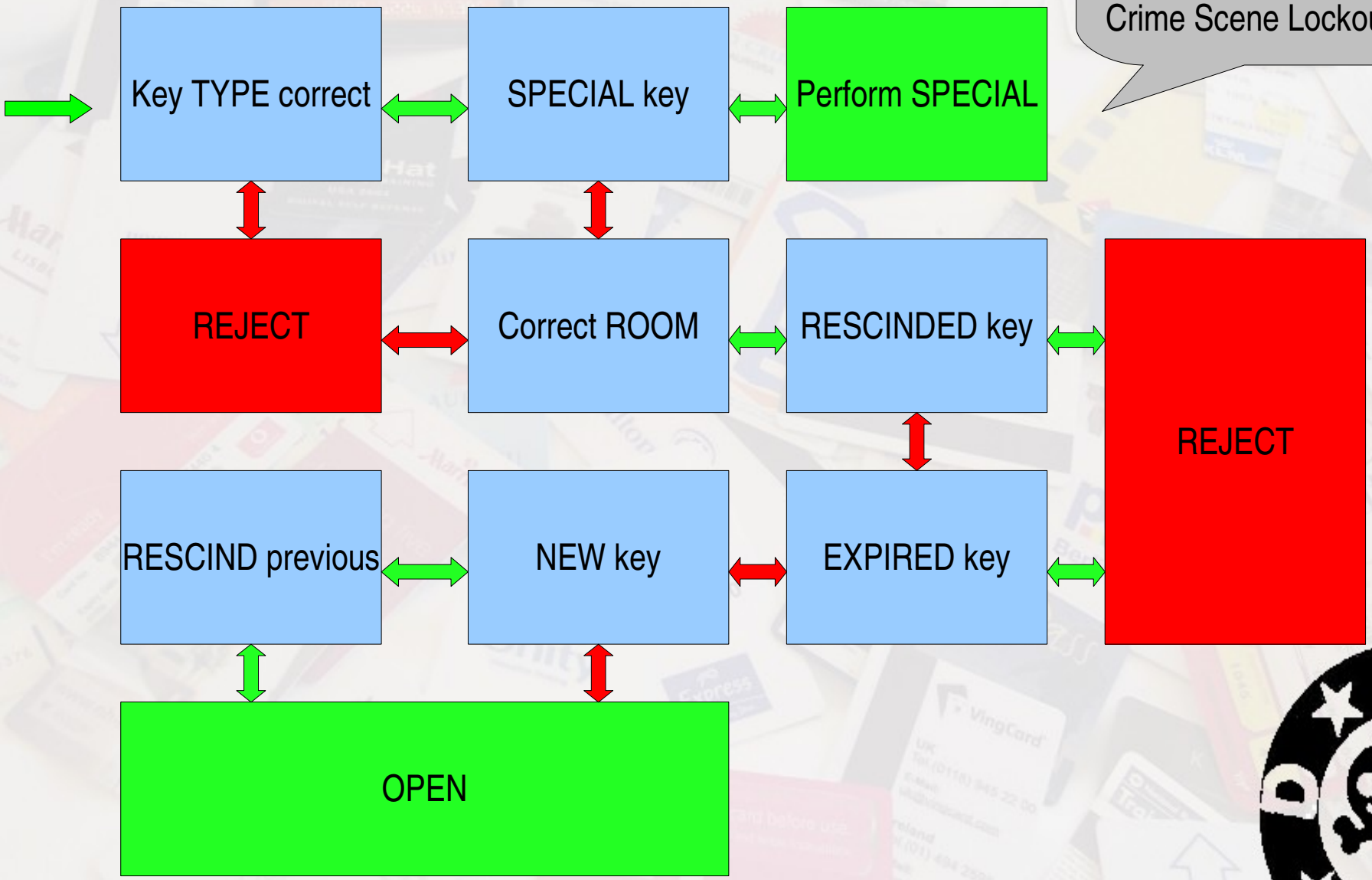


passive locks



passive locks

Housekeeping Open
One-Time Open
Guest Lockout
Crime Scene Lockout



keycard – multiple keys

- ;5101153528010176630125000120000000000?8
- ;5101153528020176630125000120000000000?;

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

keycard – multiple keys

- ;5101153528010176630125000120000000000?8
- ;5101153528020176630125000120000000000?;
- ;5101153528030176630125000120000000000?:

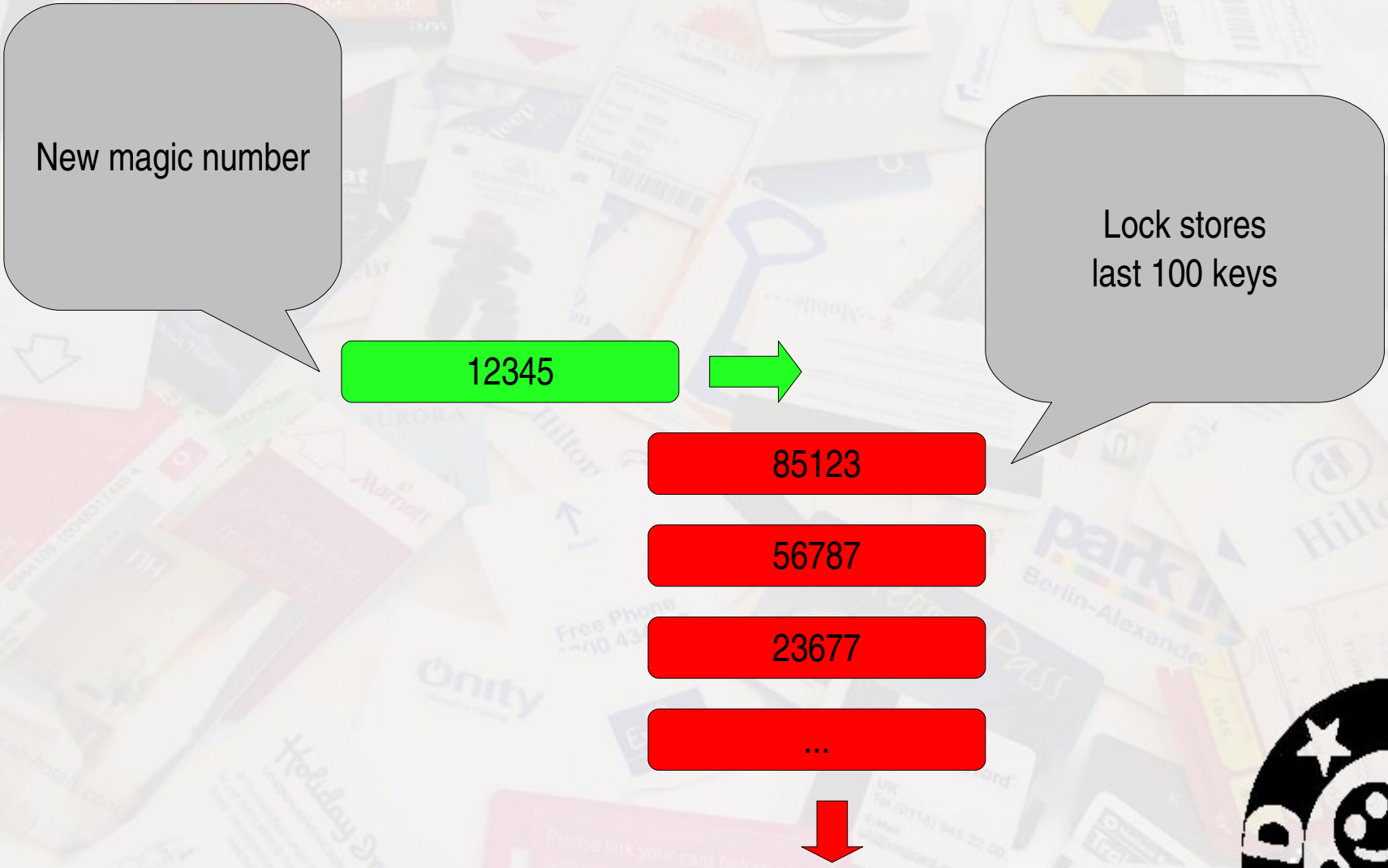
Start	Property?	Room No.	Key No.	Magic Number?	Expire	Key Type?	End	LRC
;	510115	3528	01	01766	30125	0001200..	?	8
;	510115	3528	02	01766	30125	0001200..	?	;
;	510115	3528	03	01766	30125	0001200..	?	:

keycard – rescinding

- ;5101150611010700431125000120000000000?6
- ;5101150611010703231125000120000000000?3

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

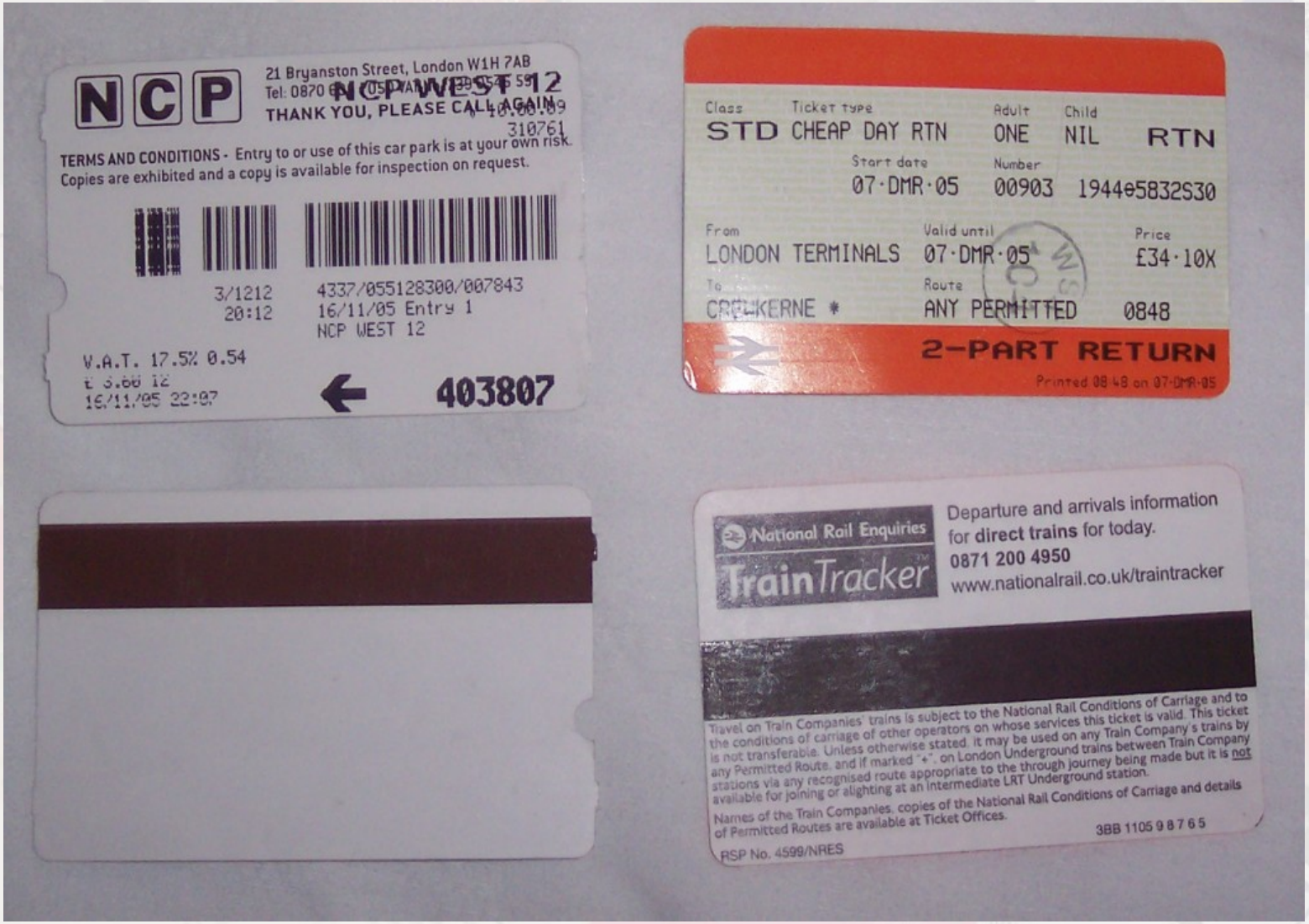
RESCINDING keys



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 keys



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!! =:O

magnasee

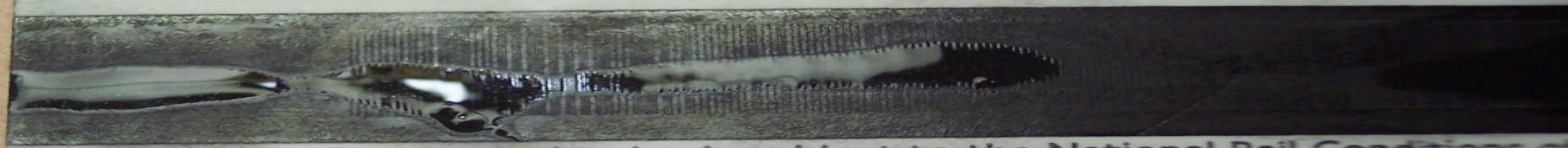

K WEST
RICHMOND WAY
LONDON W14 0AX
TEL +44 (0)20 7674 1000
FAX +44 (0)20 7674 1050
www.k-west.co.uk
THIS EDGE IN SLOT

THIS EDGE IN SLOT

National Rail Enquiries

TrainTracker™

Departure and arrivals infor
for **direct trains** for today.
0871 200 4950
www.nationalrail.co.uk/trai



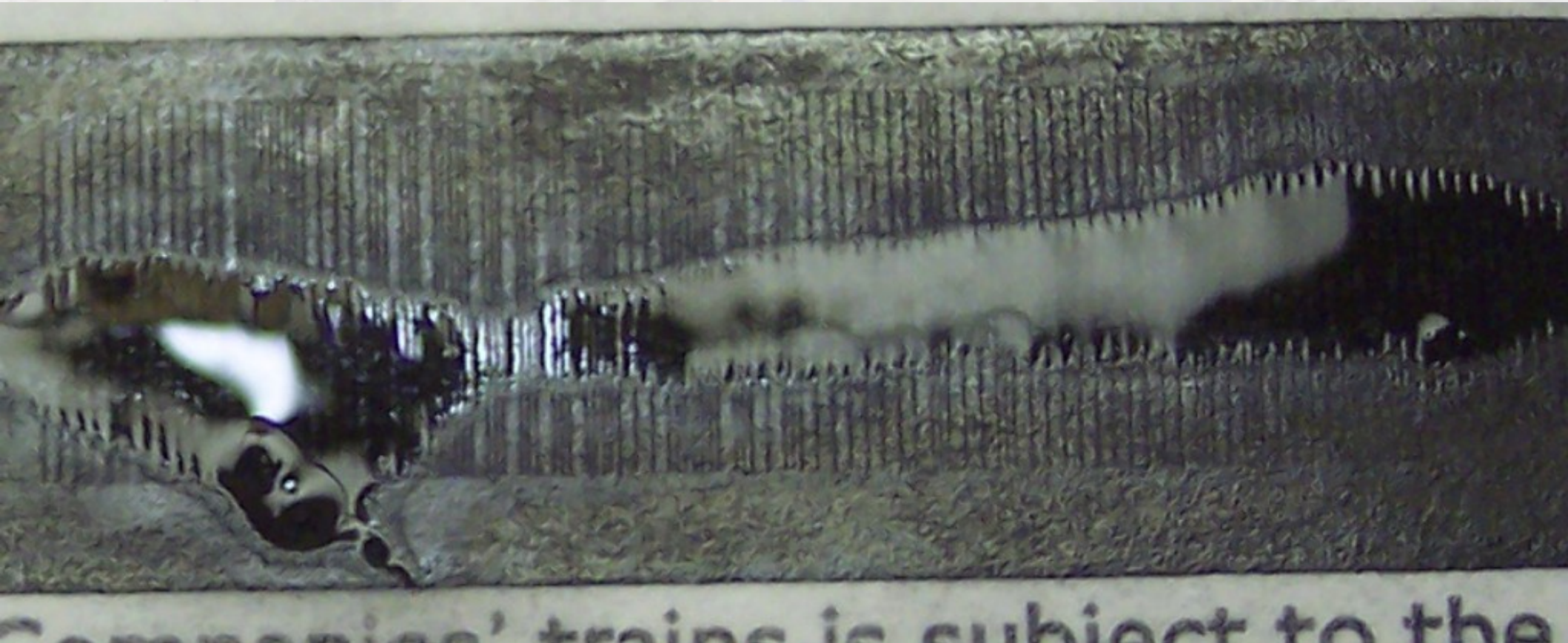
Travel on Train Companies' trains is subject to the National Rail Conditions o
the conditions of carriage of other operators on whose services this ticket is
is not transferable. Unless otherwise stated, it may be used on any Train Co
any Permitted Route, and if marked "+", on London Underground trains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

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

RSP No. 4599/NRES

3BB 110

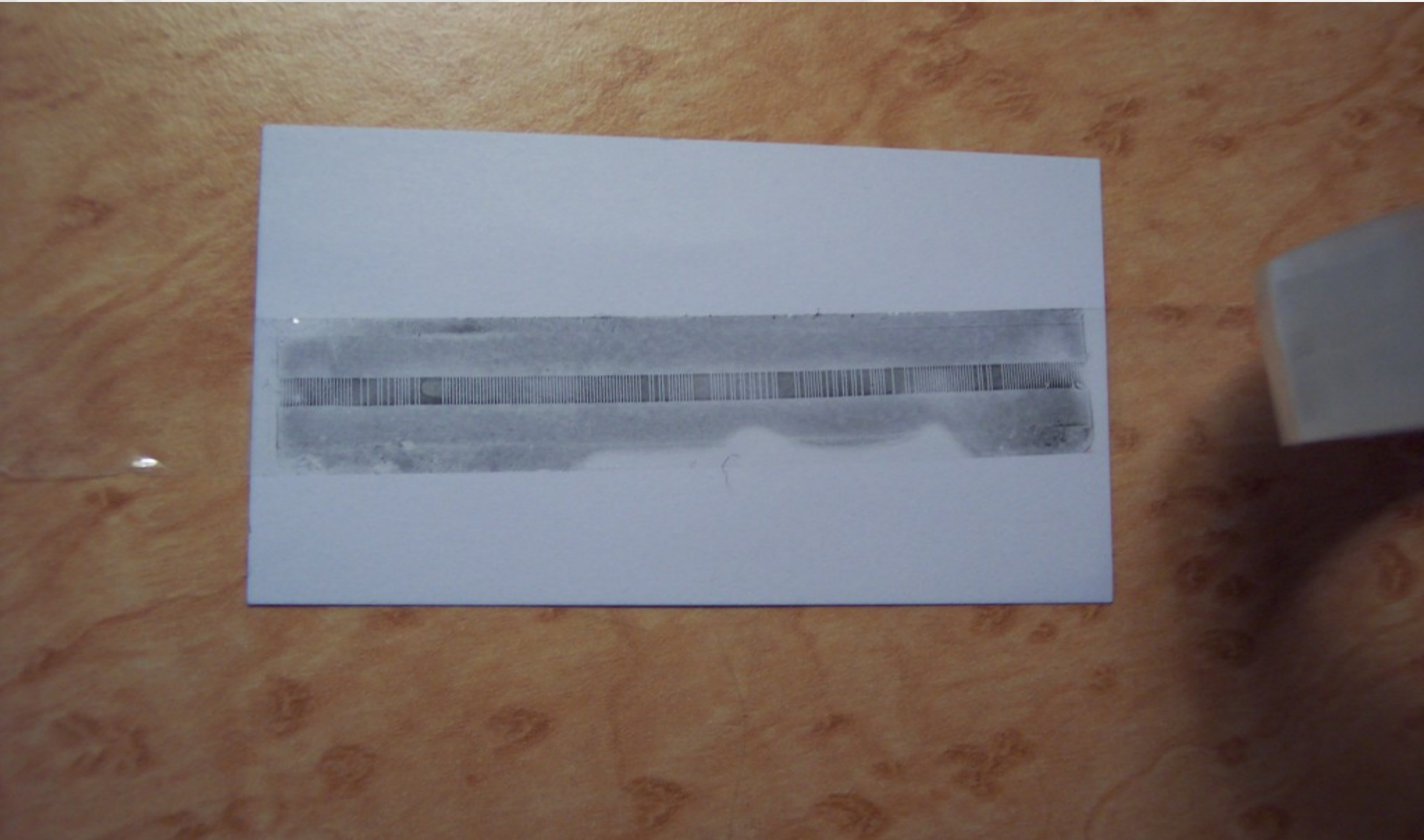
magnasee



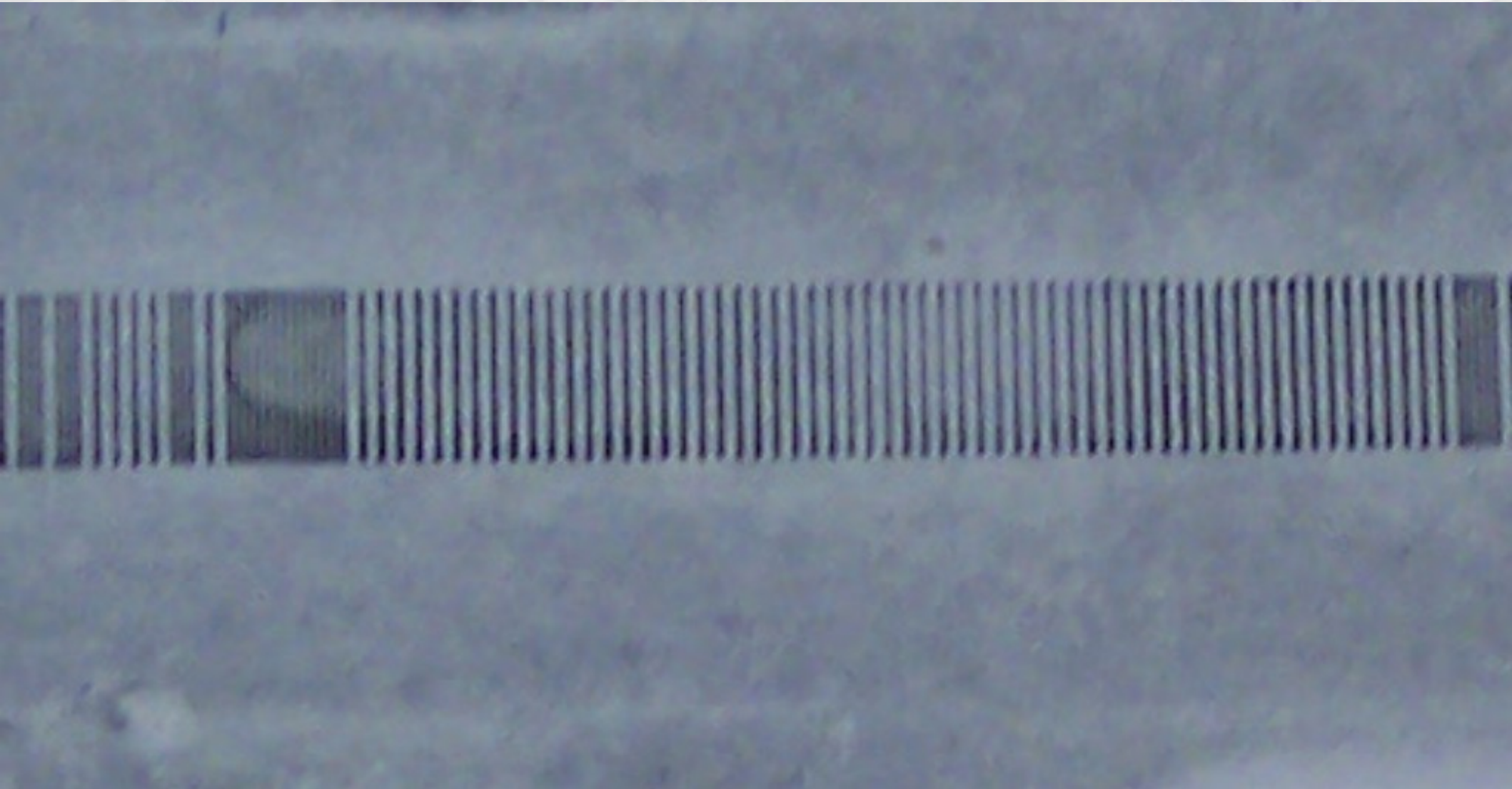
magnasee


K WEST
RICHMOND WAY
LONDON W14 0AX
TEL +44 (0)20 7674 1000
FAX +44 (0)20 7674 1050
www.k-west.co.uk
THIS EDGE IN SLOT

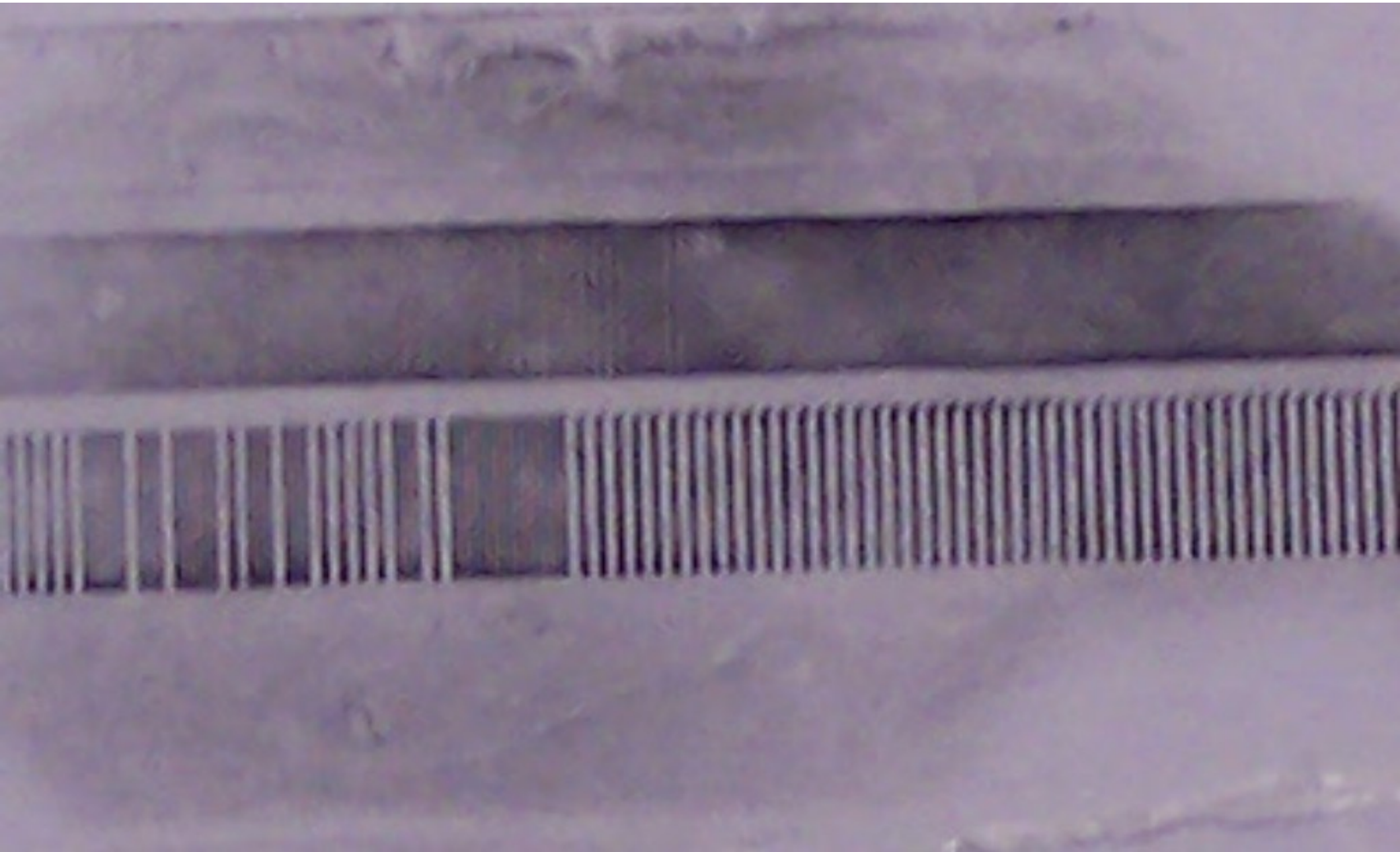
magnasee



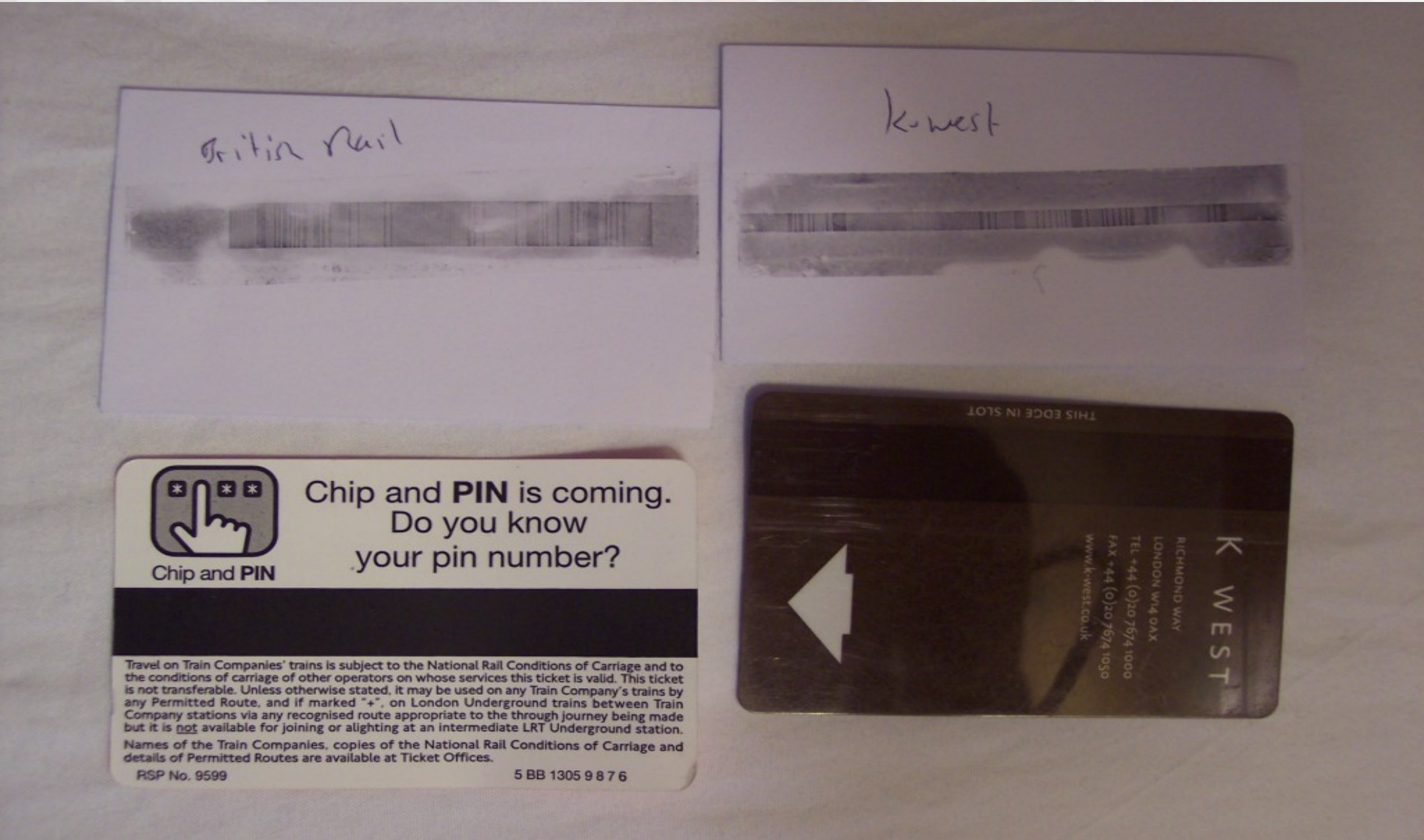
magnasee



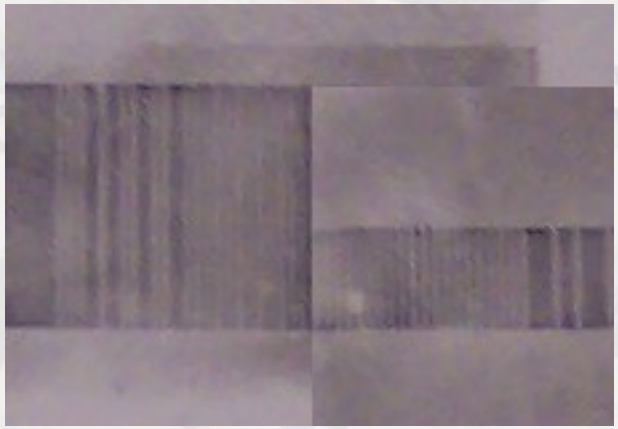
magnasee



size matters!



size matters!

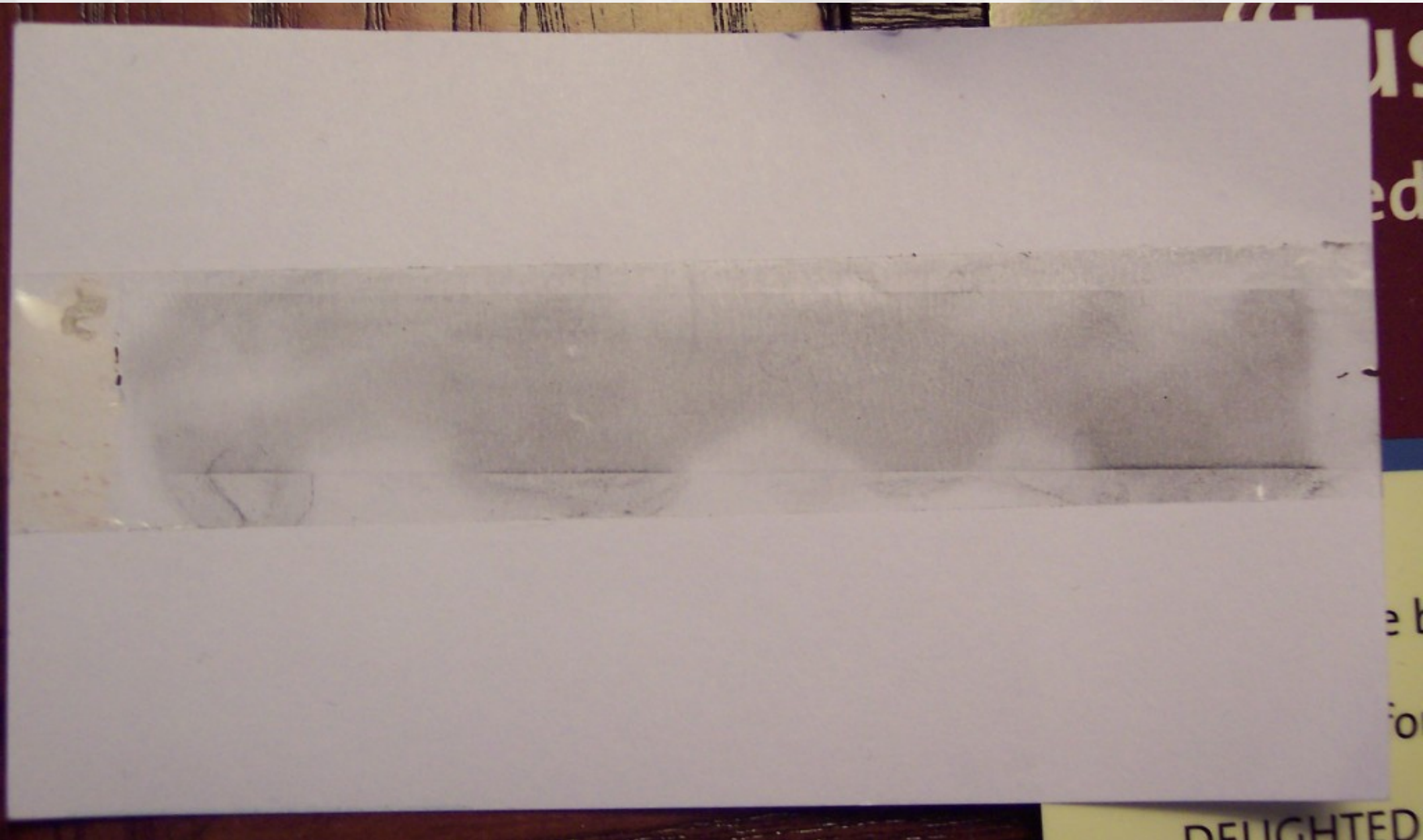


British Rail track is 2.5 times the width of ISO standard

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

demonstration

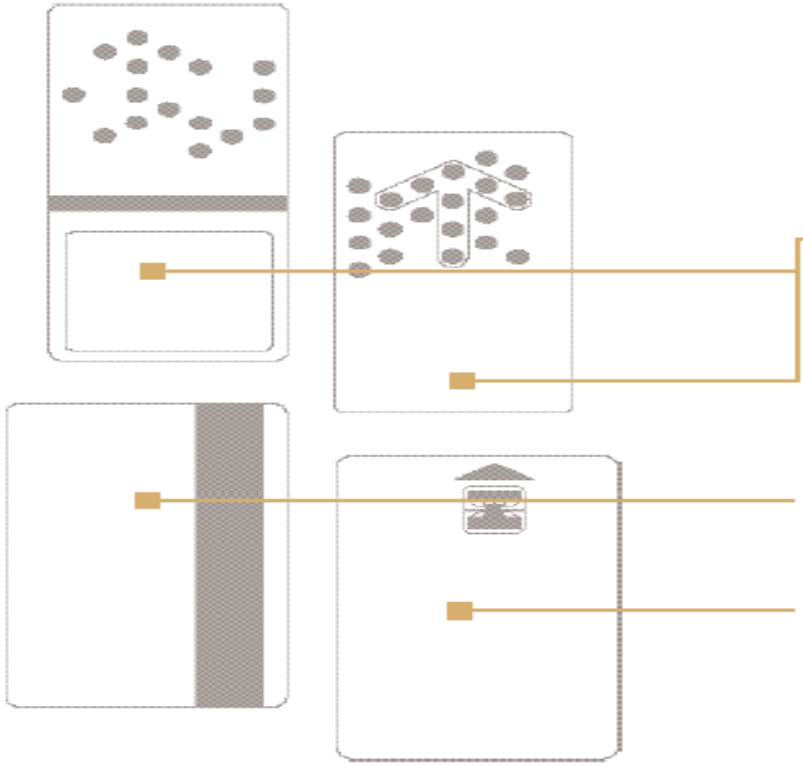
making sense of the data

- character sets
  - http://www.magtek.com/documentation/public/99875065-4.pdf

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. **Mechanial 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 generatio

- 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, SR176, SRIX4K, ISO14443A Tags, ISO14443B Tags, Jewel Tag (IRT0302B11 KSW DIY Eng. Sample), Sharp B, ASK GTML2ISO, TOSMART P064
  - support for ACG Dual ISO reader
    - http://www.acg.de
    - no drivers required – serial device

MIFARE tags

- Block layout
- Access controls
- Demonstration

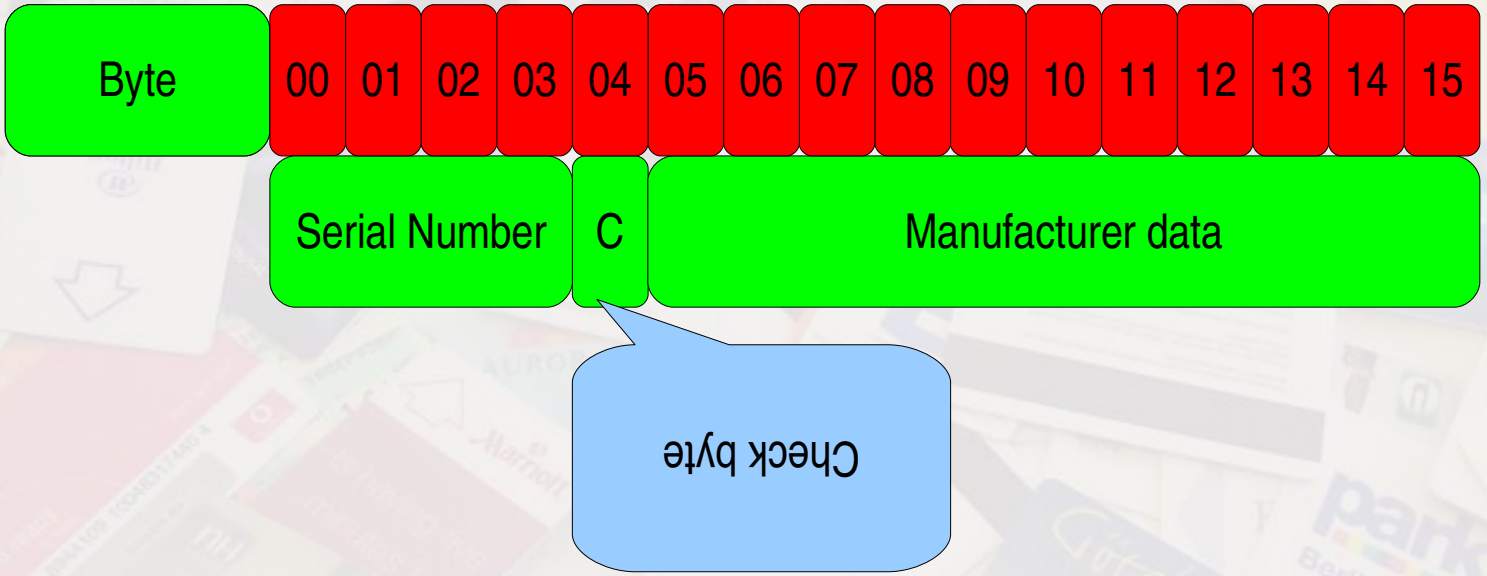
MIFARE 1K – block layout

Sector 0	Block 0 Manufacturer block	Block 1	Block 2	Block 3 Sector trailer
Sector 2	Block 4	Block 5	Block 6	Block 7 Sector trailer
Sector 3	Block 8	Block 9	Block 10	Block 11 Sector trailer
Sector ...	Block ...	Block ...	Block ...	Block ... Sector trailer
Sector 15	Block 60	Block 61	Block 62	Block 63 Sector trailer

Access control Block

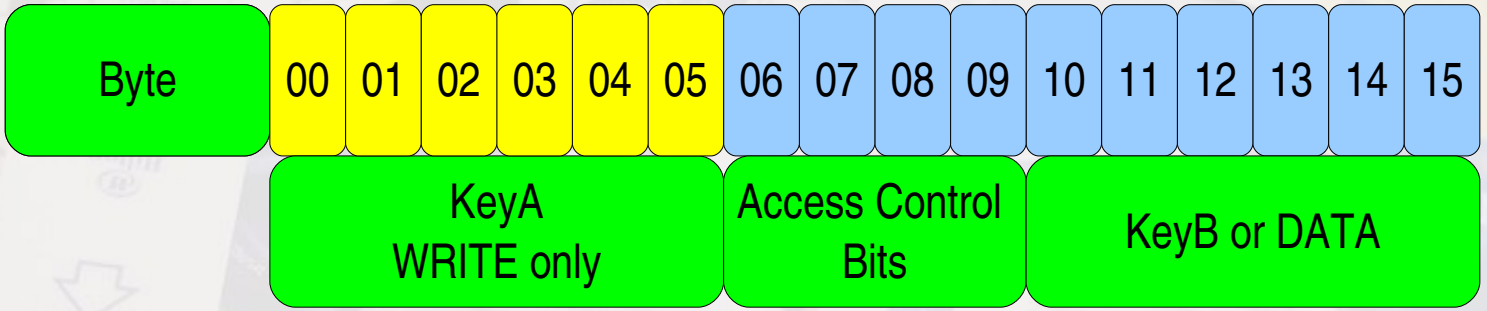
16 sectors, 4 blocks per sector,
16 bytes per block = 1024 bytes

manufacturer block layout



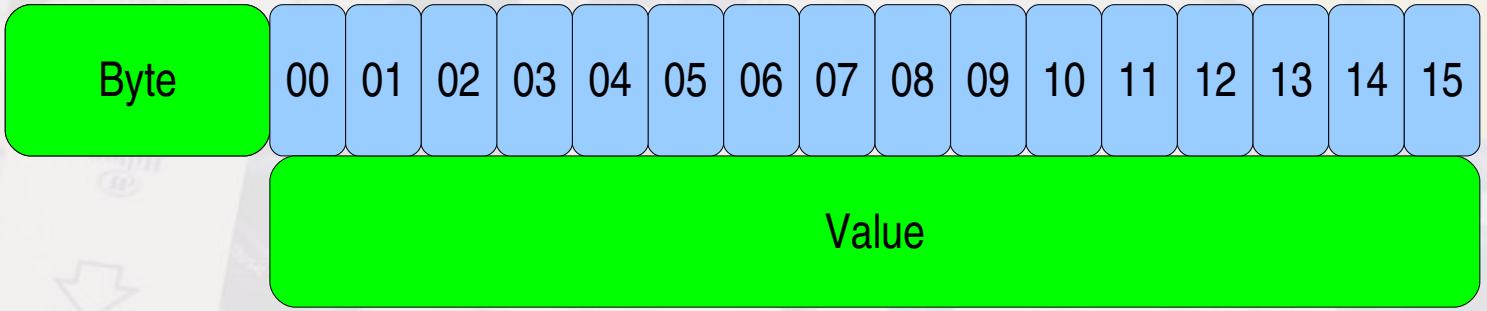
Whole block is read only

access control block layout



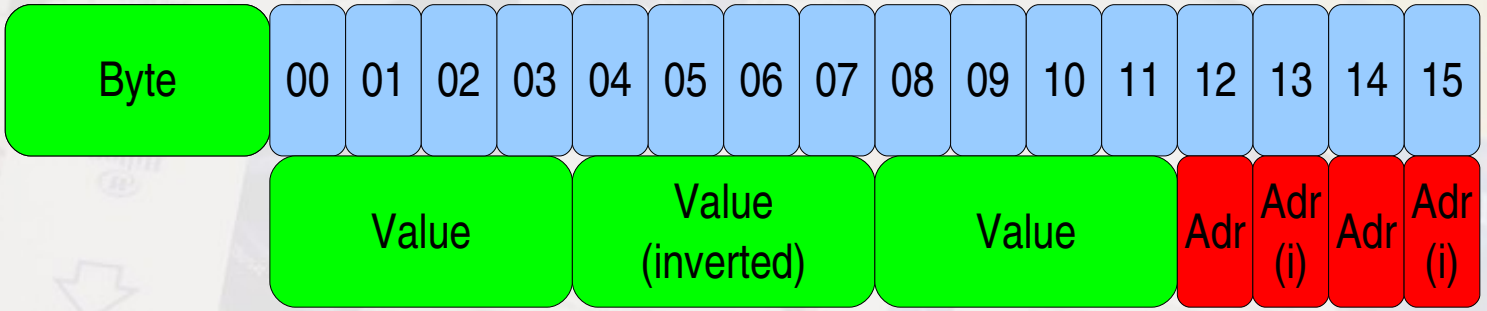
- KeyA can never be read
- KeyB may be read and/or written
  - Depending on ACB
- ACB for various combinations
  - Who may read/write keys
  - Who may increment/decrement/restore value blocks

data block



- 16 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

demonstration

Questions?

oh dear...

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