Hacking Nedap voting computers

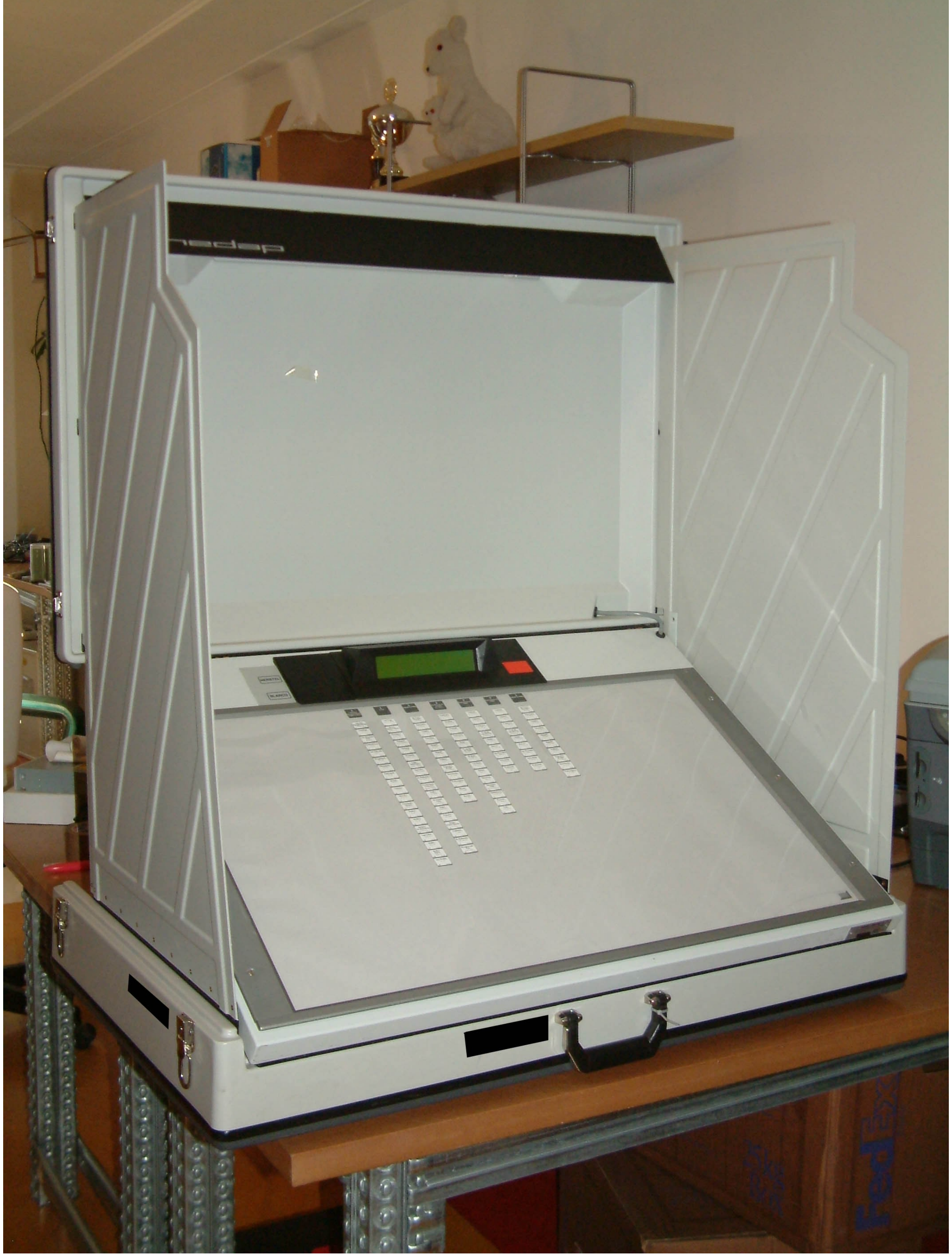
hack.lu
Andreas Bogk, Hannes Mehnert
20. October 2006

Overview

- Voting Computer
- Hardware
- Software
- Attacks

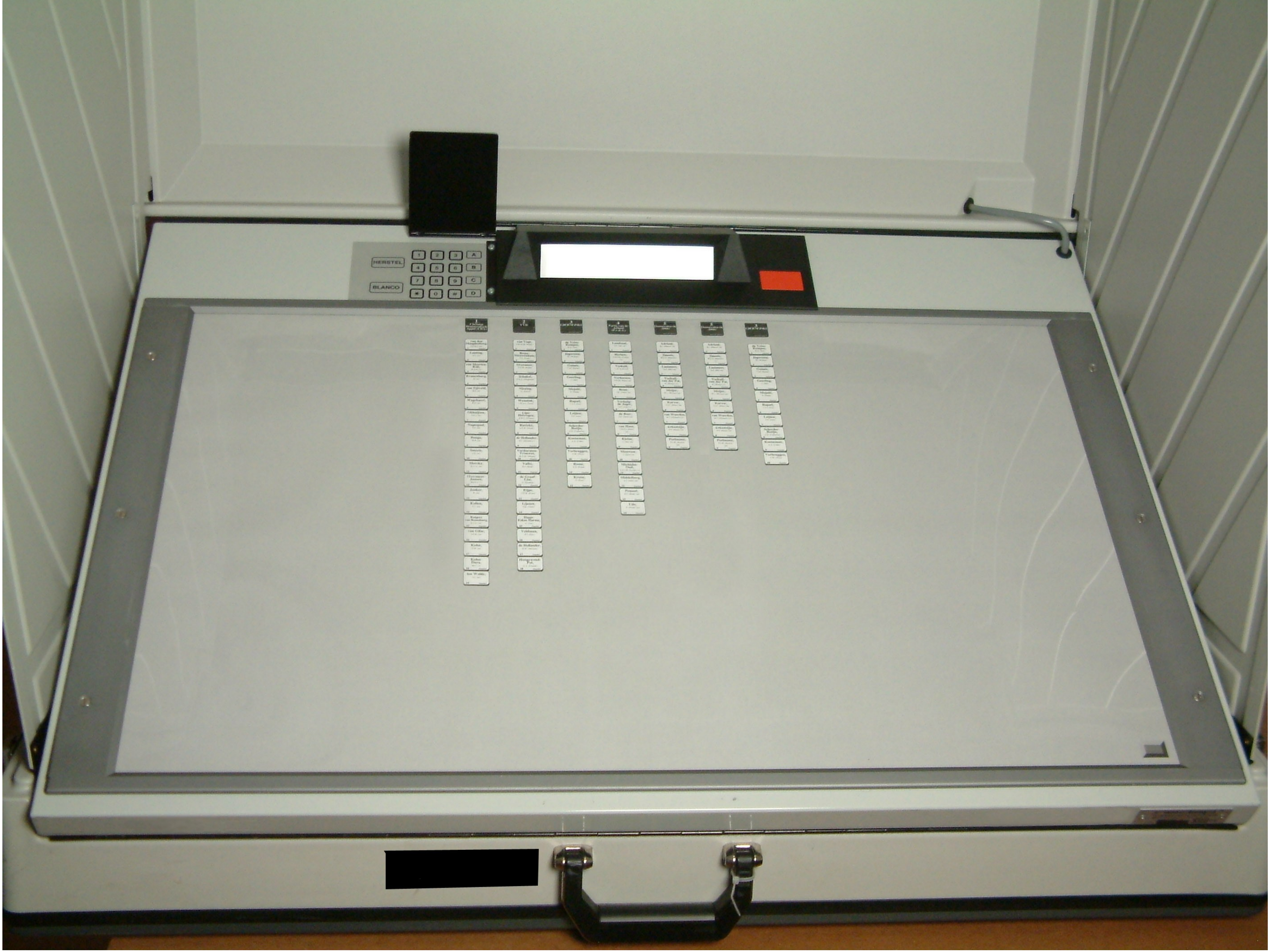
Random citations

- “Hackers have absolutely no chance”
- “Dedicated Special Purpose Machine”
- “I want to see that our Voting Machine is able to play chess”

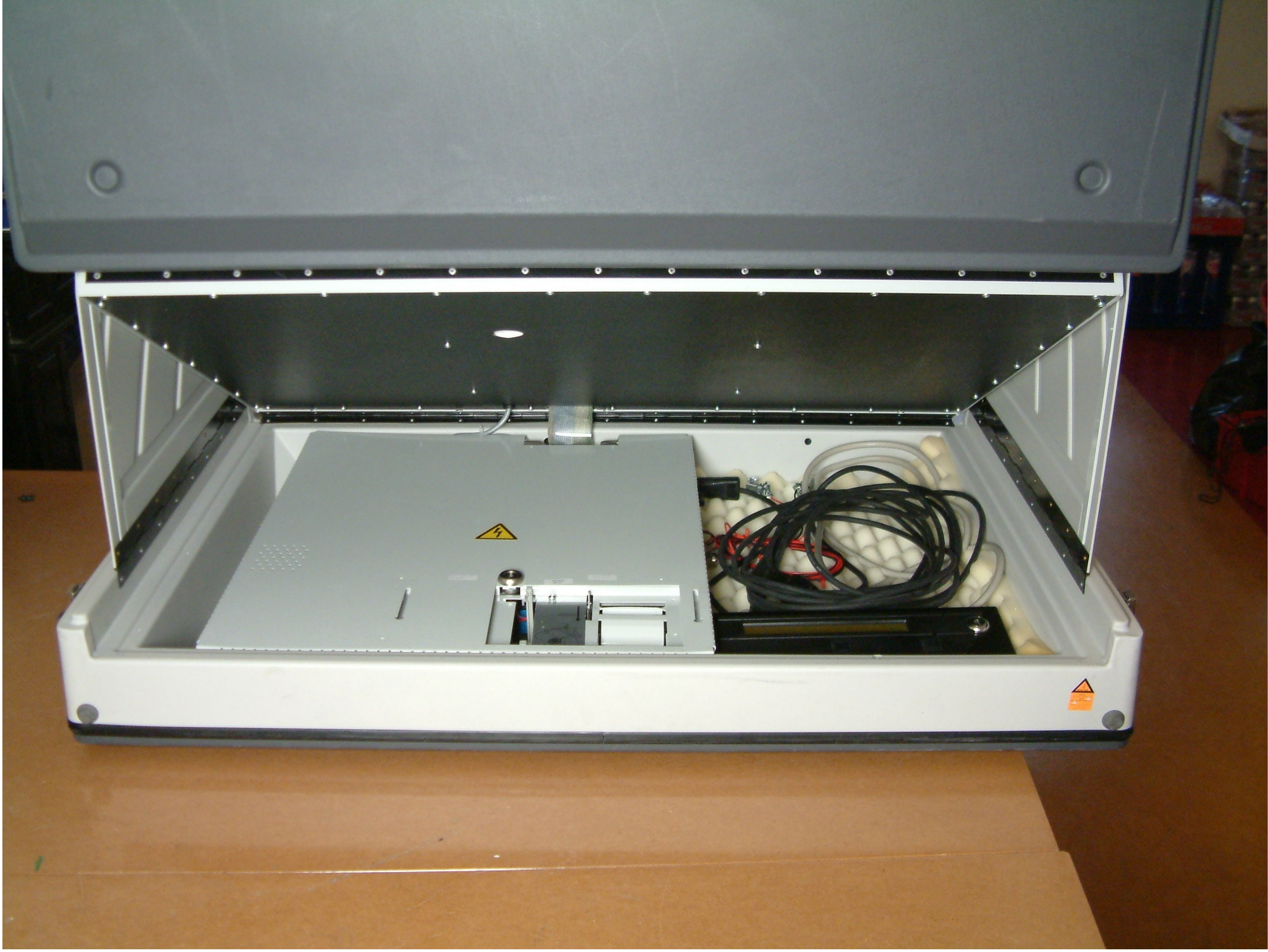


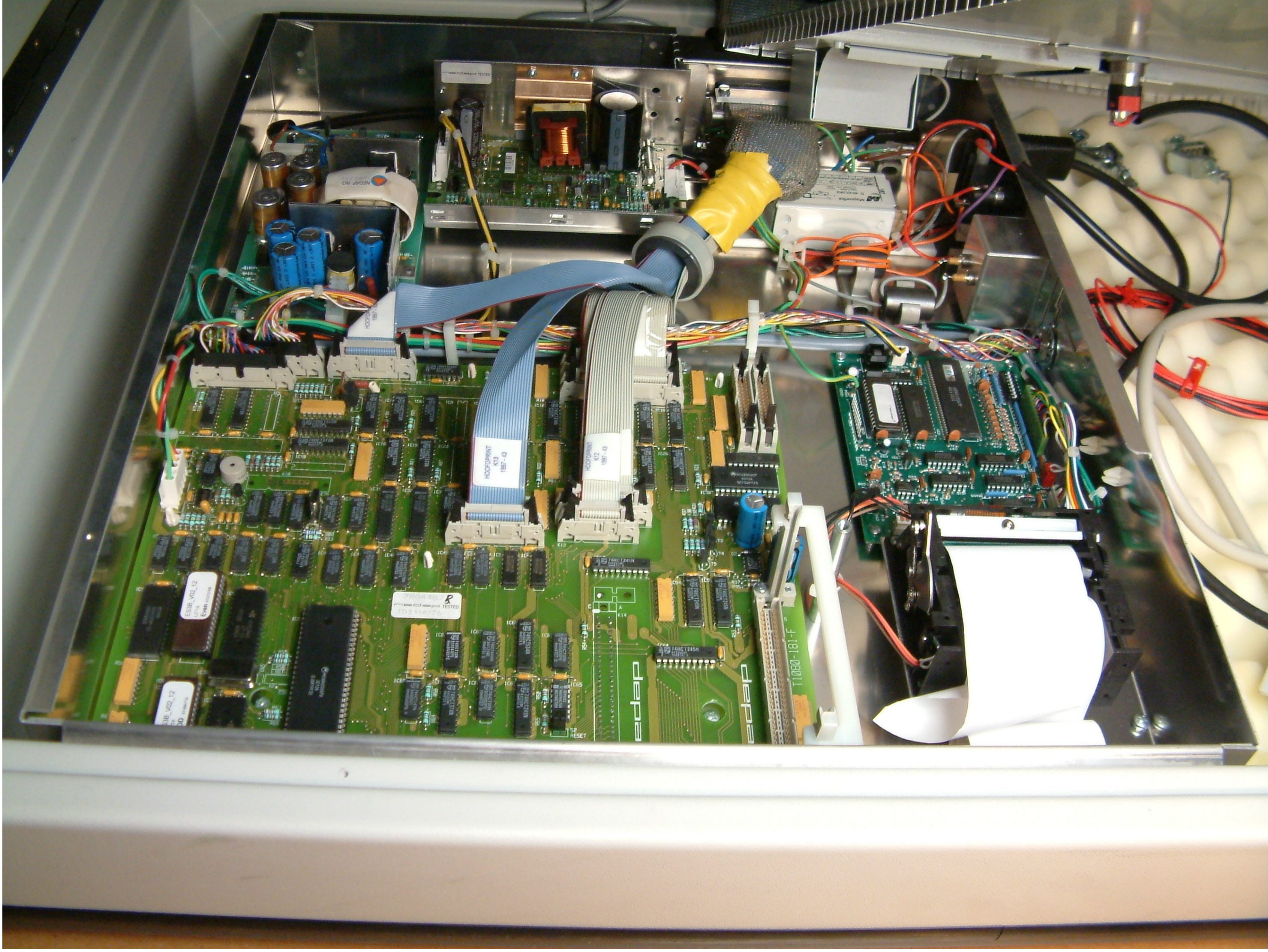
[redacted]

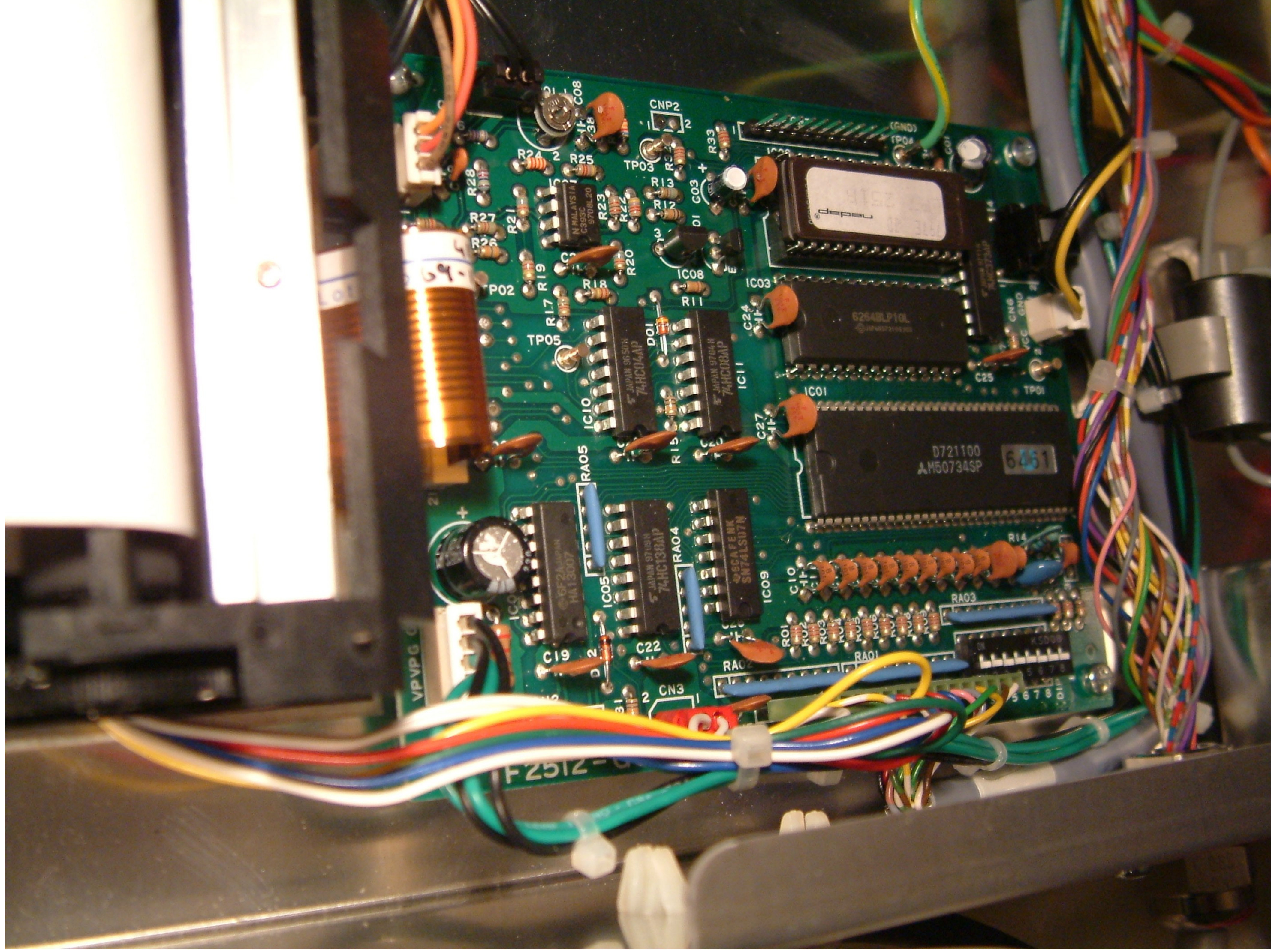
[redacted]

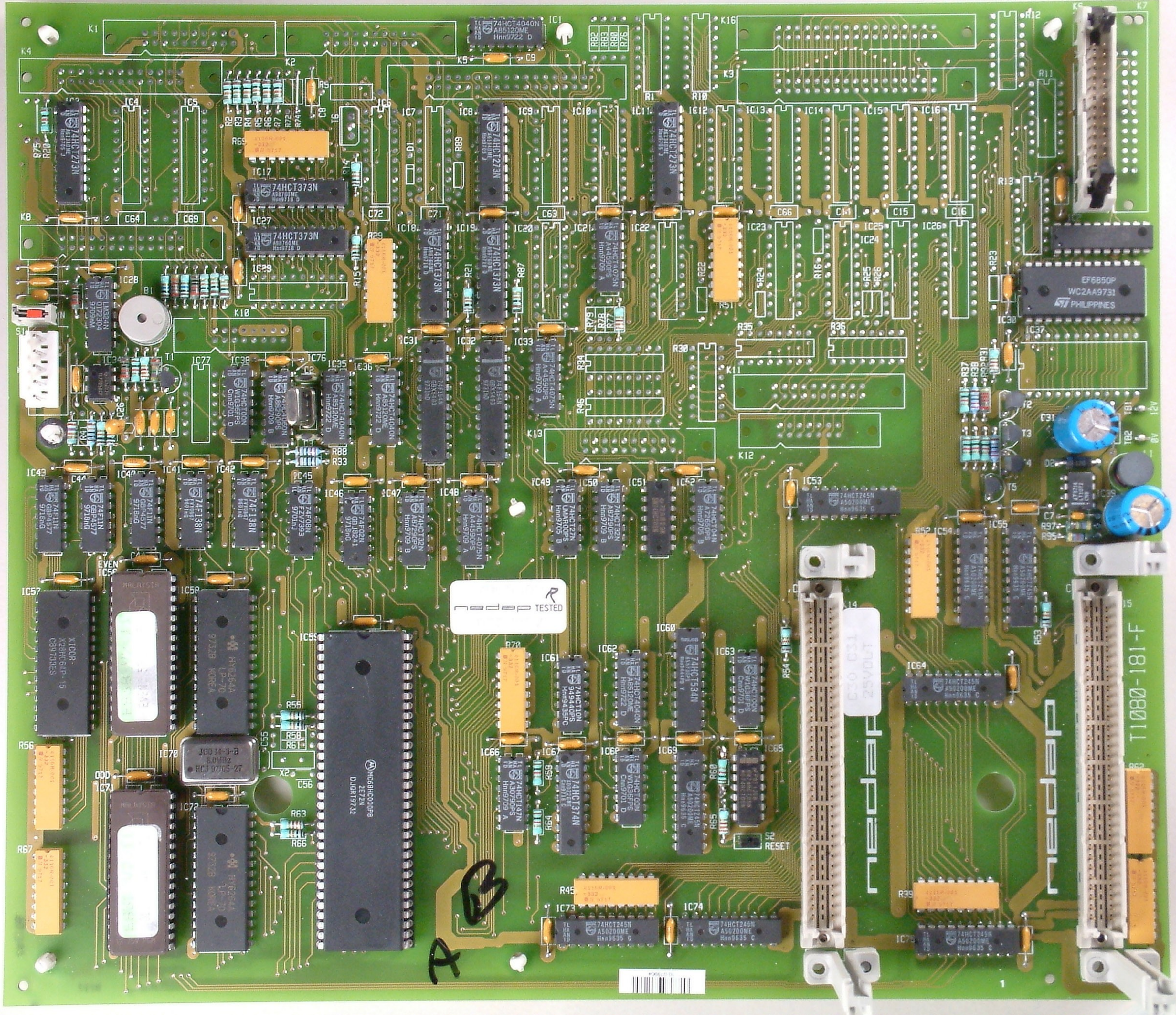


[redacted]




HOOFDPRINT
K13
1997-43
HOOFDPRINT
K12
1997-43
ES3B_V02_12
Even
ES3B_V02_12
7804482 R
TESTED
JD11H076
74HCT245N
74HCT245N
nedap
nedap
TI080-181-F
S2
RESET


CNP2
TP03
TP04
TP02
TP05
TP01
IC08
IC03
IC01
IC10
IC11
IC05
IC09
6264BLP10L
D721100
M50734SP
6461
74HC04AP
74HC08AP
74HC138AP
SN74LS07N
HA13007
C393C
RA05
RA04
RA03
RA02
RA01
CN3
F2512-



nedap TESTED
T1080-181-F
nedap
nedap
74HCT4040N
74HCT273N
74HCT373N
74HCT245N
EF6850P
PHILIPPINES
MC68HC000P8
XICOR X28HC64P-15
HY6264A LP-70 KOREA
MALAYSIA
8.0MHz
RESET
EVEN
ODD
12V
0V
A
B

Hardware

- 68000 processor at 8 MHz
- 16 kB Ram
- 256 kB EPROM
- 30x36 Touchpad
- 4x40 Display
- 2x40 Operator Display
- Serial
- 8 kB EEPROM

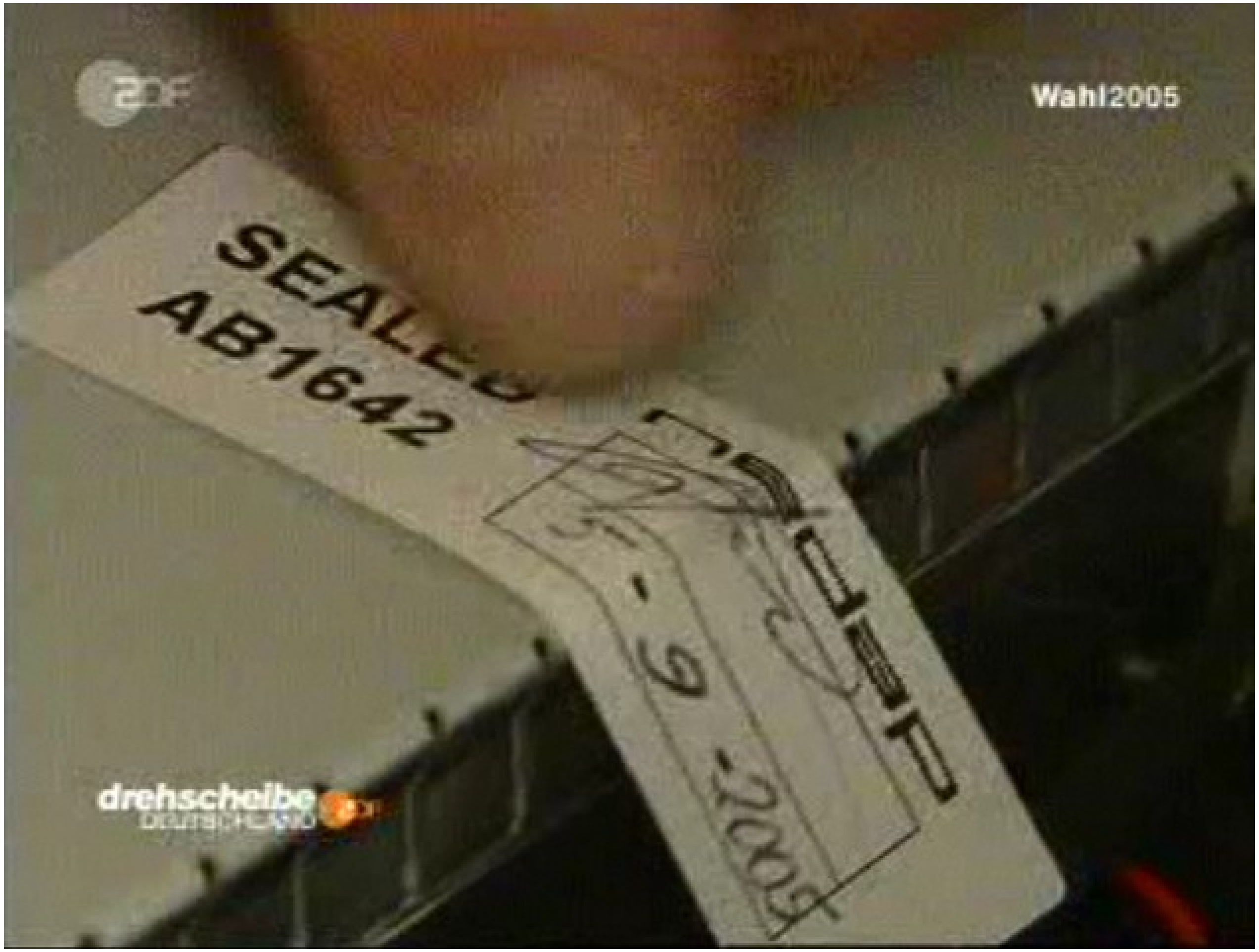
Software

- Reverse engineering 256kB
  - With IDA Pro
  - Traced wires for connection of ports
- USB EPROM emulators
- Gcc crosscompiler
- Newlib (small c library)
- keyboard/display driver
- Debug output via serial

Security Features

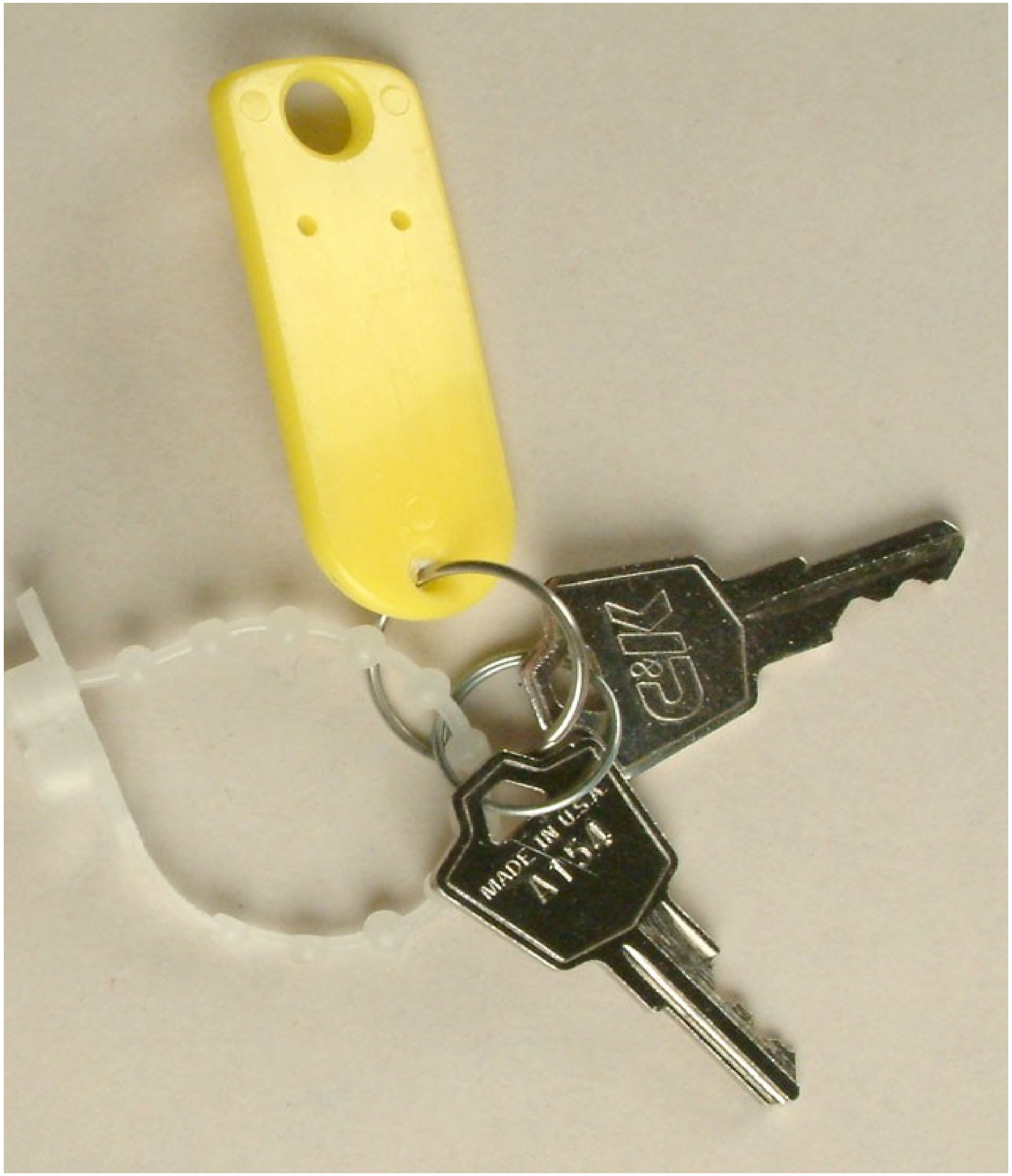
- Checksum (32bit sum of all bytes)
  - Printed on EPROMs
- Mechanic Lock
- Redundancy
- run_eprom_test at 0x1ae2
- No paper trail
- Maintenance mode “GEHEIM”

Seal – in Germany

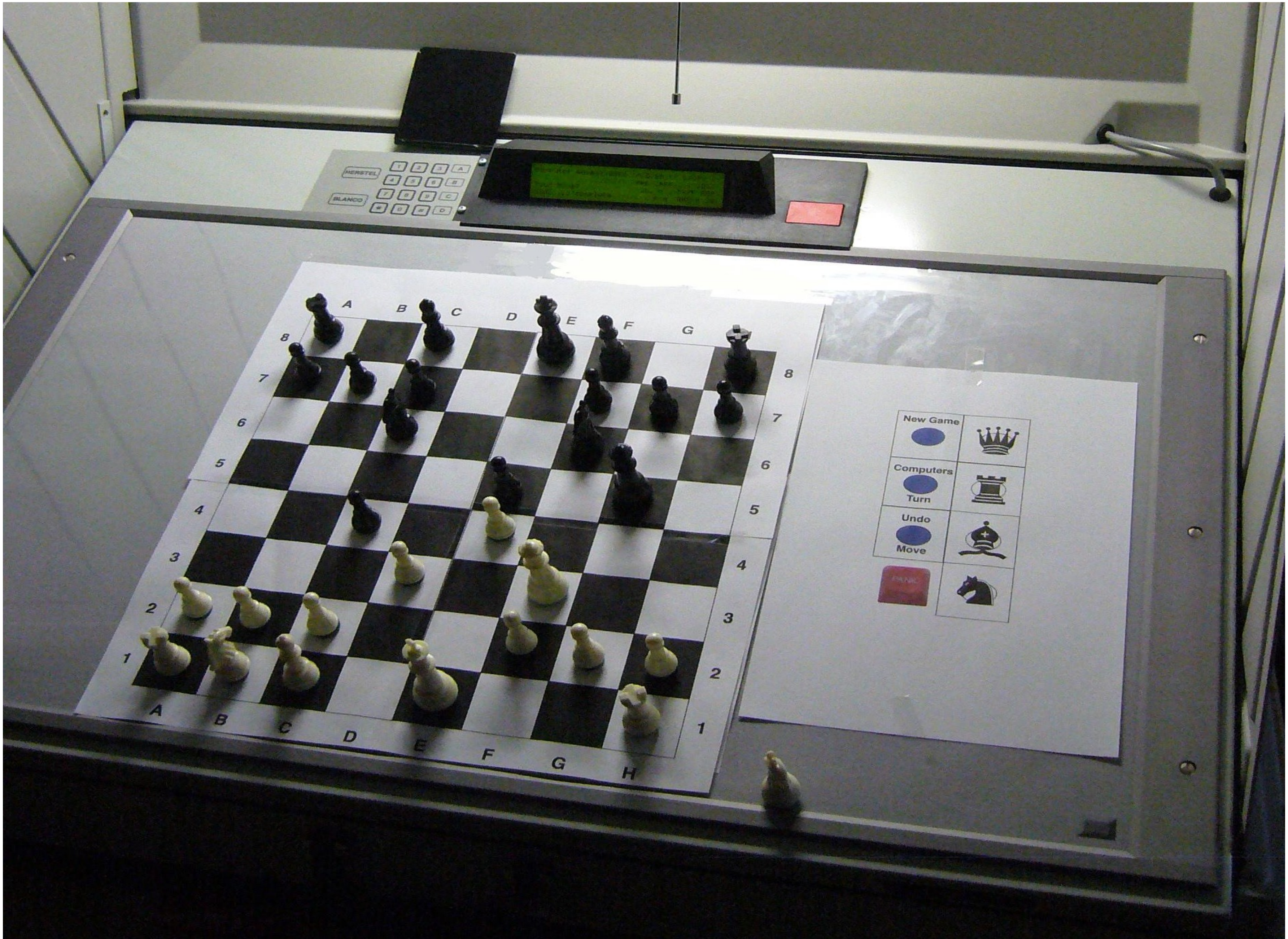


Locks

- PNR 115140126



Tom Kerrigan's Simple Chess

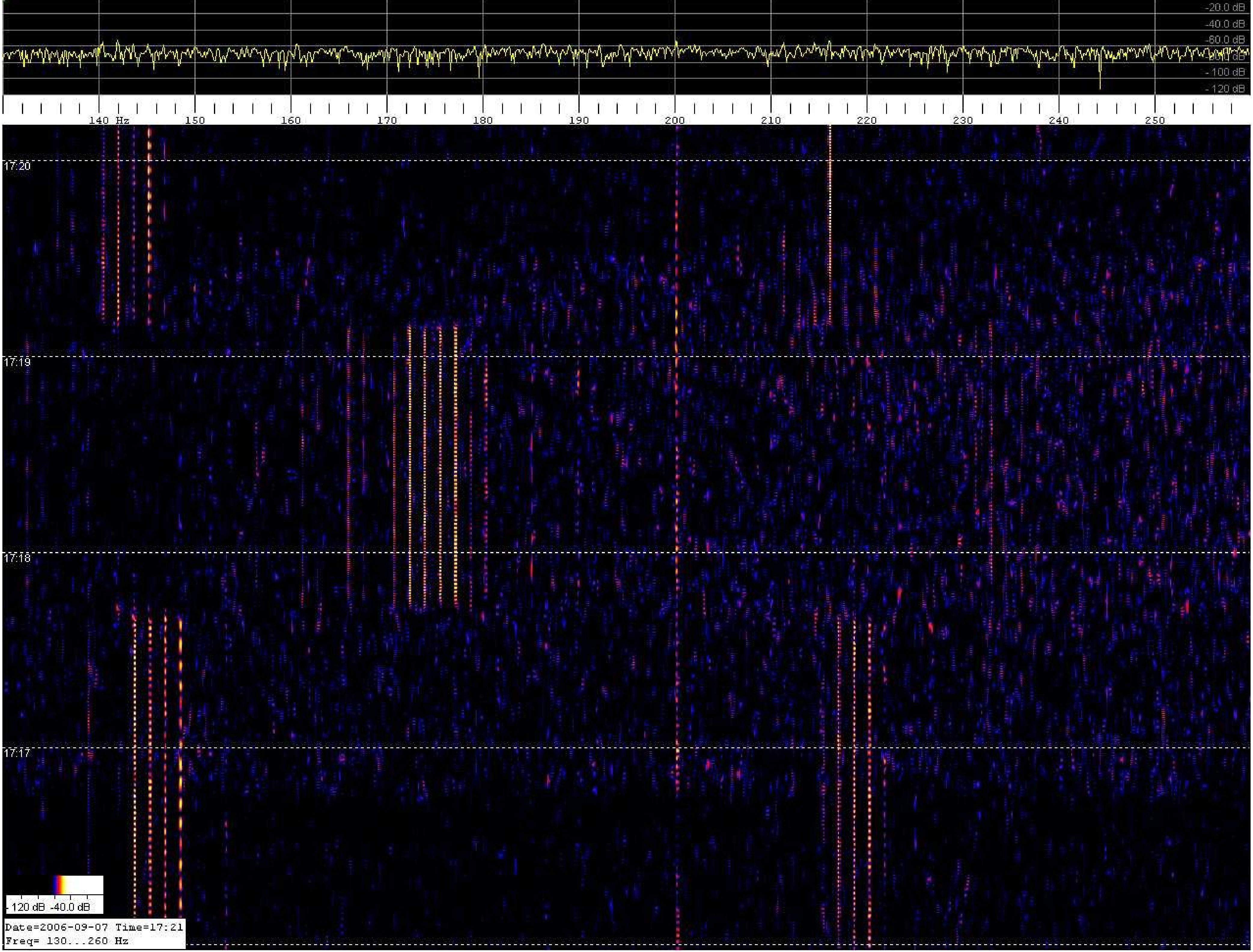


Attacks

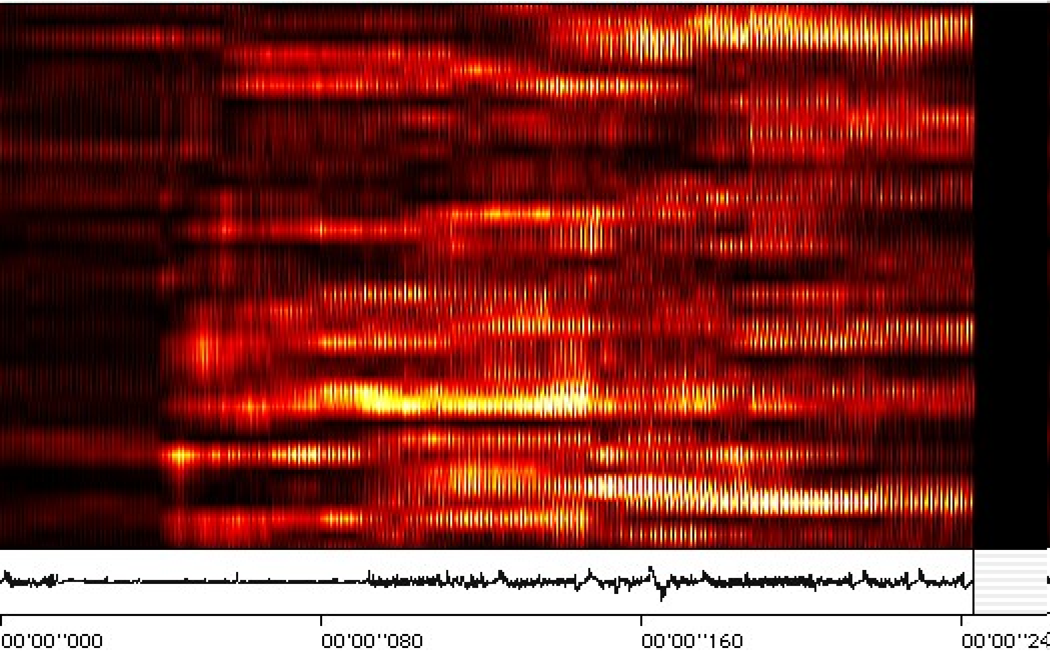
- Social Engineering
- MITM microcontroller
- Social Engineering
- PowerFraud
- Tempest

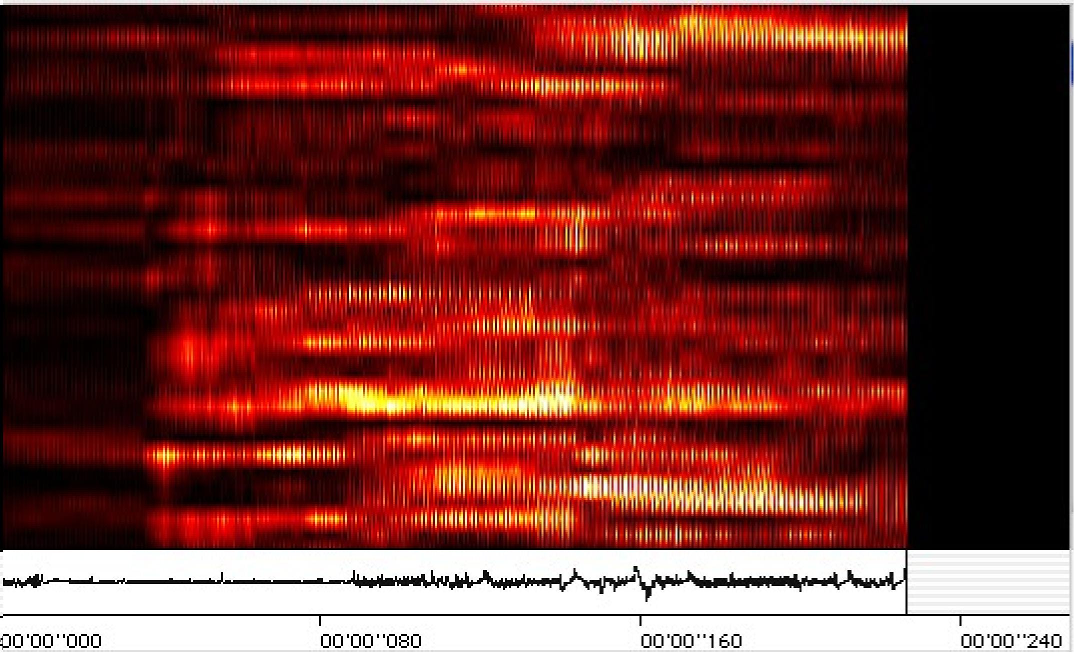
PowerFraud

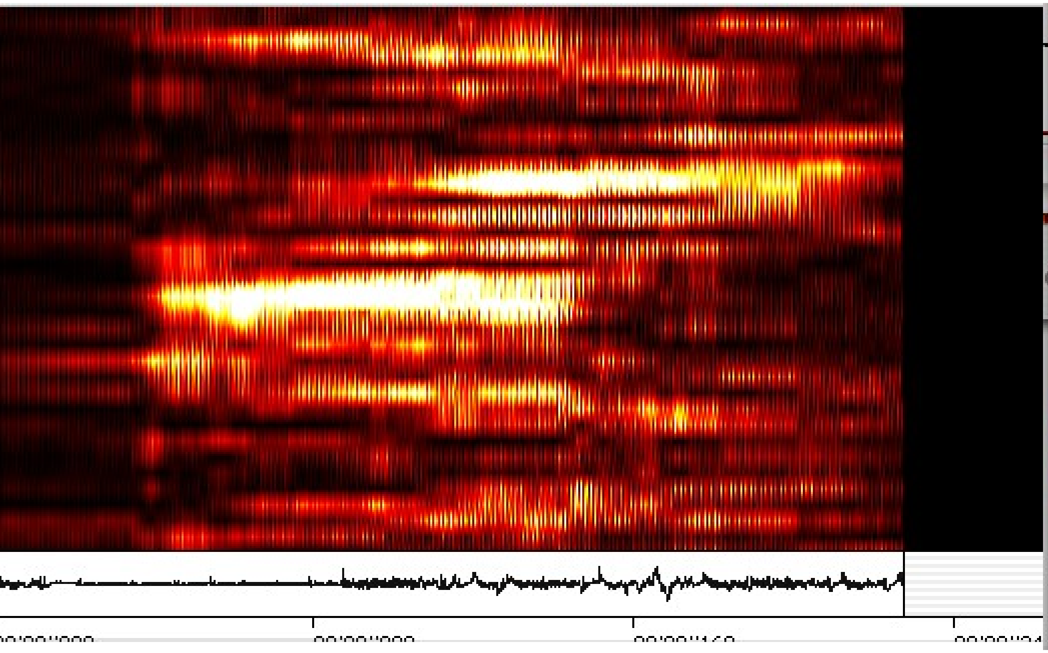
- Insider attack
- Custom firmware ranks a special party higher
- May measure on timing, count of votes whether real or test election

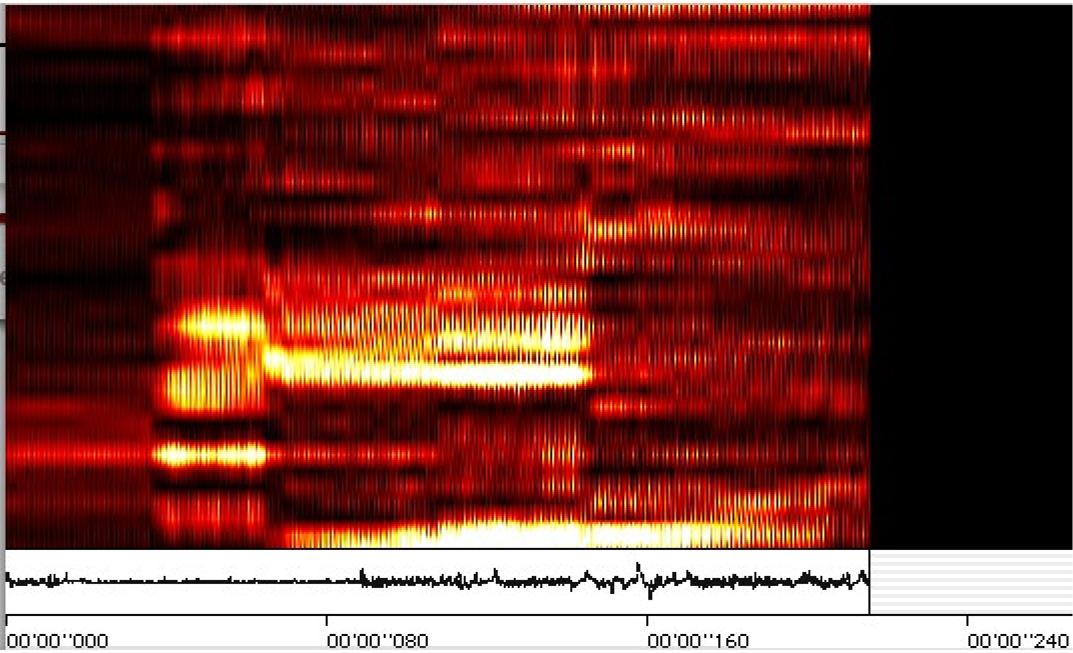


Date=2006-09-07 Time=17:21
Freq= 130...260 Hz


00'00''000
00'00''080
00'00''160
00'00''24


00'00''000
00'00''080
00'00''160
00'00''240


00'00''000
00'00''080
00'00''160
00'00''24


00'00''000
00'00''080
00'00''160
00'00''240

Deployed Countermeasures

- Germany (Election Sunday in Cottbus)
  - PTB read EPROM contents, compared with original images
- Netherlands
  - All ~ 8000 Voting Computers got a new firmware
    - Always display a special character
    - Sealed afterwards

Countermeasures

- Verify software
  - But how? Every voter should be able
- Prevent emanations
- Open Source Firmware?

Conclusion

- Don't trust black box voting!
- Don't trust black box voting!
- Never trust black box voting!

Links

- http://www.wijvertrouwenstemcomputersniet.nl/Nedap-en
- http://www.youtube.com/watch?v=B05wPomCjEY
- http://www.cev.ie/htm/report/download_first.htm
- http://itc.napier.ac.uk/e-Petition/bundestag/view_petition.asp?PetitionID=294