# Enhancing VICE

## How to break things when enhancing them

The problem of lush implemented container formats for emulation and what communities will make out of them

Christian Bartsch
The Software Preservation Society
http://www.softpres.org

KryoFlux Products & Services Ltd
http://www.kryoflux.com

# Disclaimer

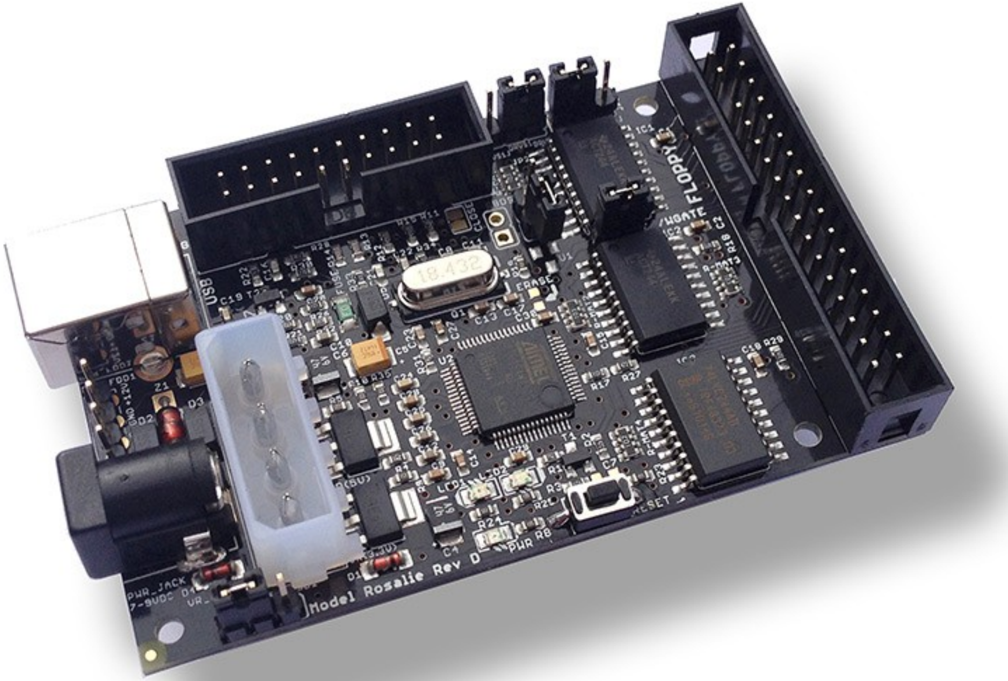
Community based development is good!

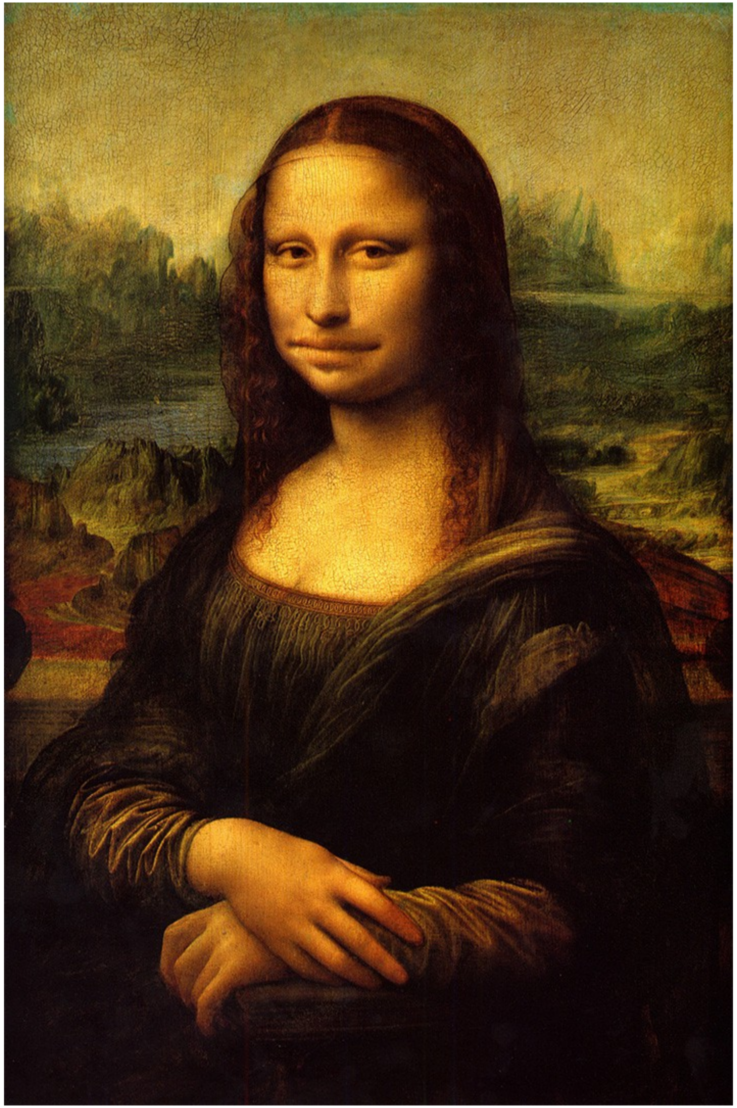
We would not have many emulators without “the the community”!

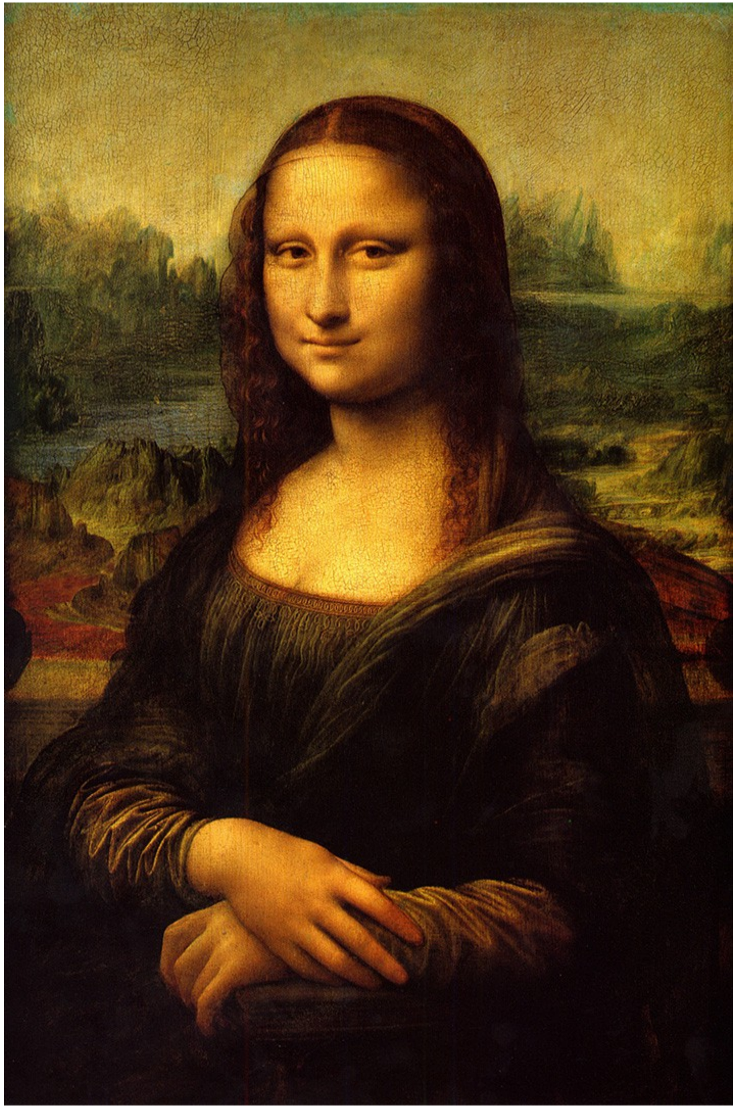
# The Software Preservation Society

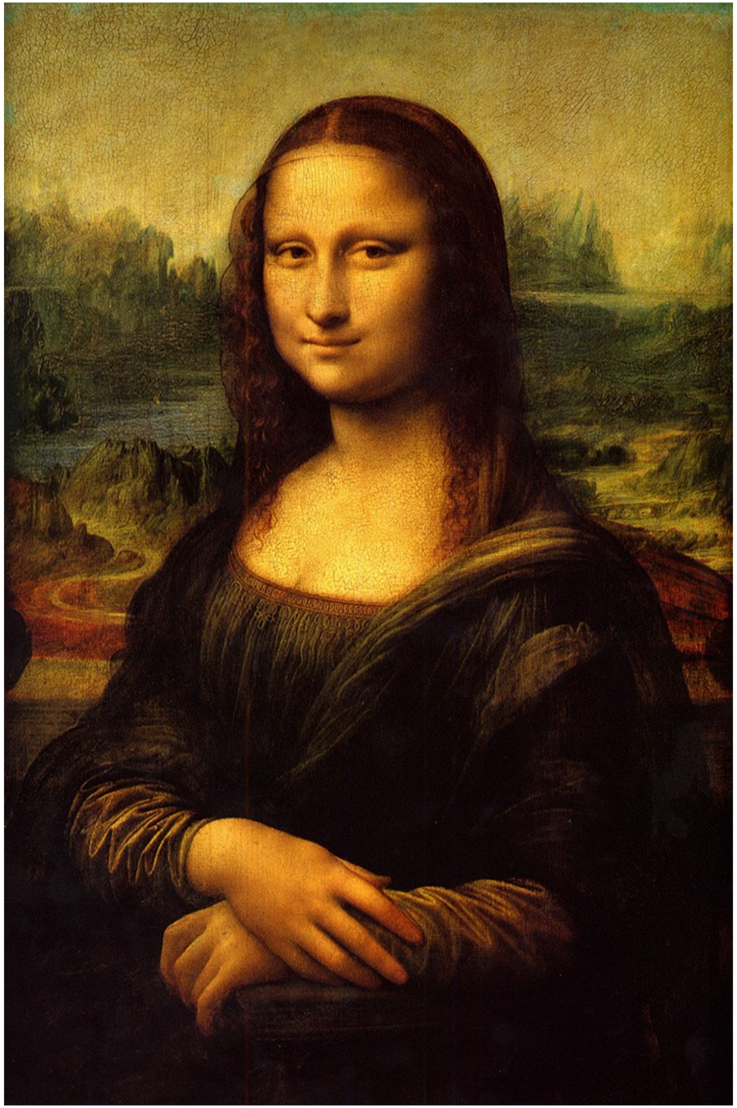
- Founded 2001 by István Fábián
- Only available for the future were pirated copies
- “Digital Graffiti”
- Games digitally preserved: 8,000+
- Founding member of FGAMP.eu
- Development of IPF container and KryoFlux floppy controller

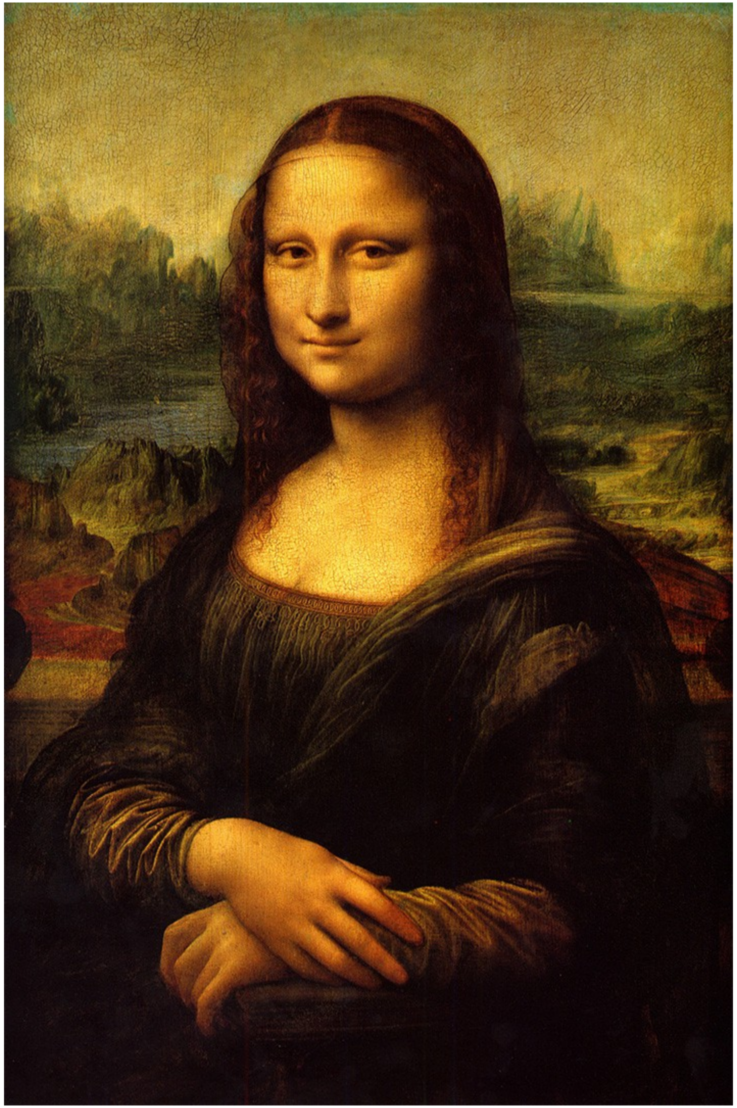
# The KryoFlux

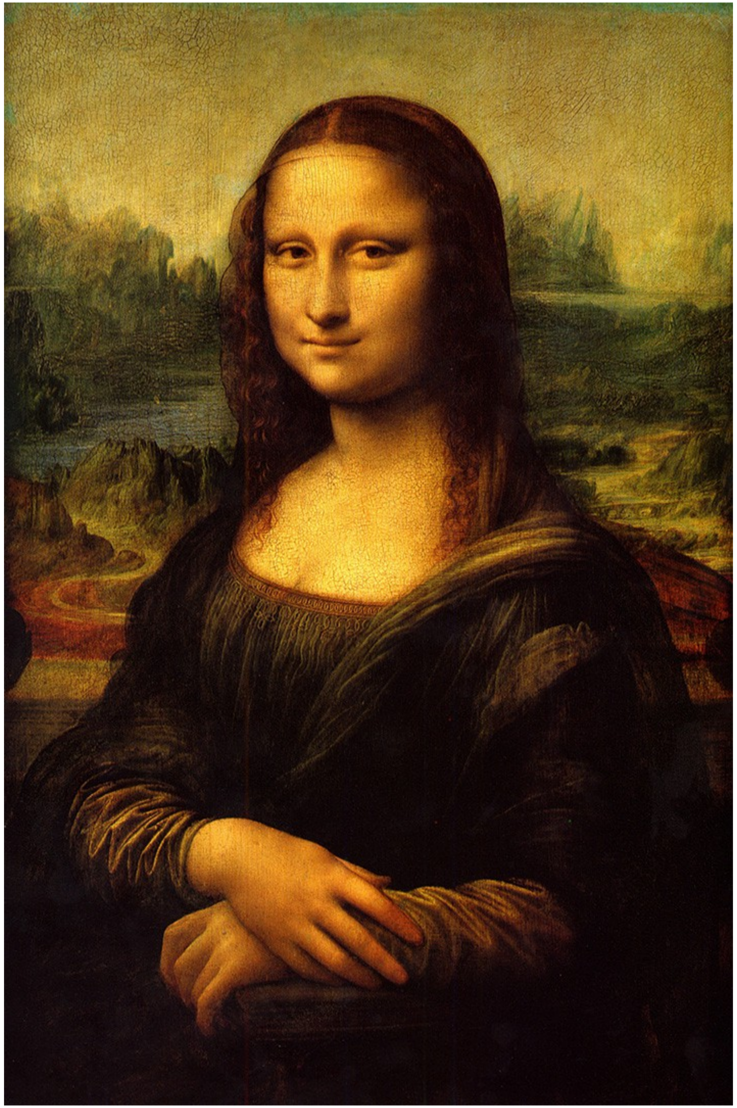












# Problems of Emulators

- Development mostly community driven
- Theory vs. reality
- Information (“hard facts”) proprietary
- Concept based on assumptions and myths
- Quick and dirty vs. industrial code
- Faster is better

# Working with “cracks”: second hand data for development

- Emulator development based on software “at hand”
- Copy protection removed
- Enhancements + bug fixes
- Data uses standard “DOS” disk coding
- Result: Emulation made as good as needed
- Over time: Emulator and image format create a de-facto standard

# Sector dumps
# (e.g. D64, ADF, IMG)

- Most common: sector dumps
- Pure data after controller, decoded
- No structure (all tracks have same geometry)
- Little or no meta data
- Extended over time
- Can not store anomalies, hidden data etc. needed for protection

# Copy Protection
## pushes a platform to the limits

- Copy protection is war!
- Proprietary formats and encoding
- Hidden data in unused areas (“fake DOS”)
- Uses undocumented hardware features

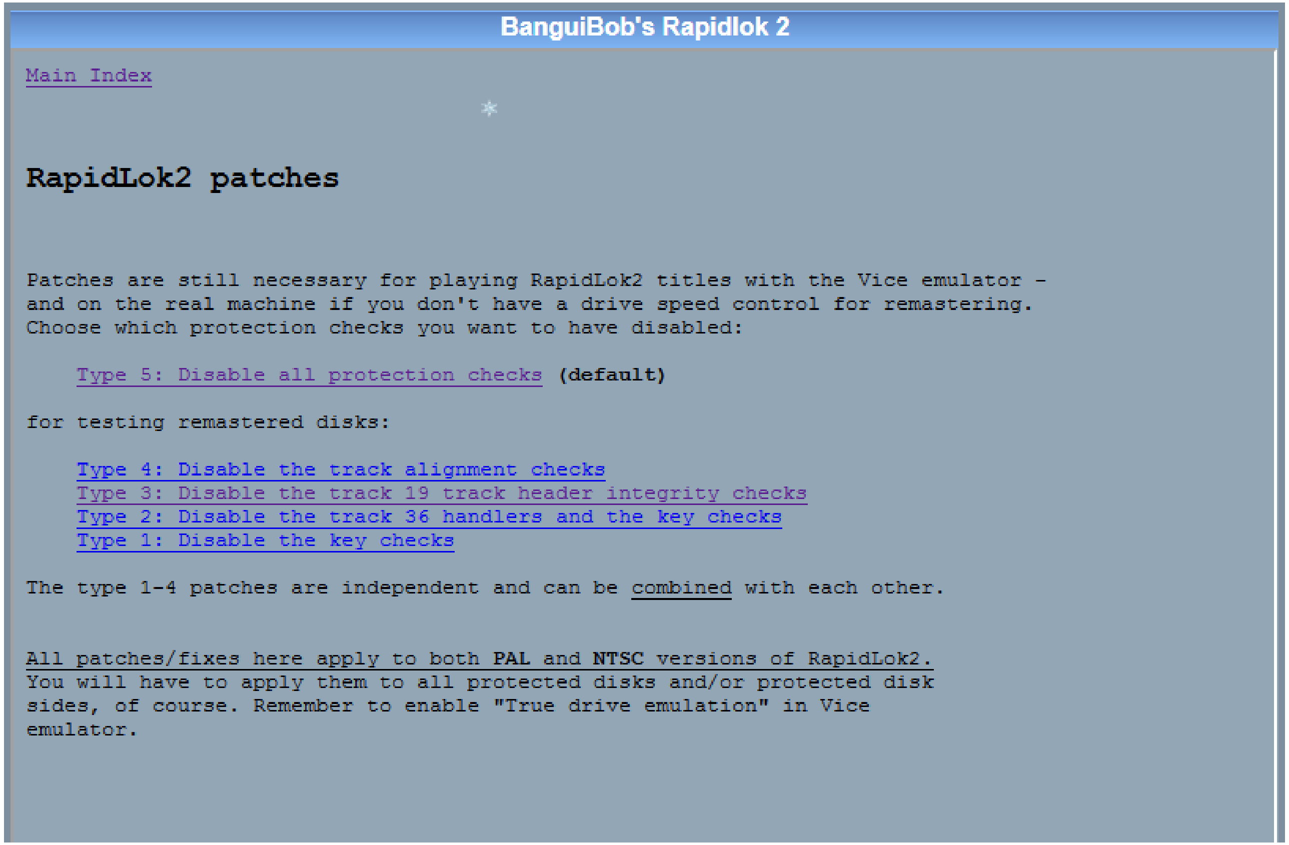
# More formats are born (e.g. G64, ExtADF)

- Meant to store “raw data”
- Ingestion so far done on original systems
- Data seen after processing through legacy devices, e.g. Commodore 1541 floppy drive
- Symptoms rather than cause stored: is 5 the result of 4+1 or 2+3?
- Well meant, badly executed due to lack of knowledge

# Still does not work: data modification

- Most people want quick solutions
- Most people don't care about purity
- Most people don't care about being scientifically correct
- Data is modified to fit needs
- “Working”, half-cracked, images end up in community driven preservation efforts

# Examples for “How-To”s for data modification



BanguiBob's Rapidlok 2

Main Index

## RapidLok2 patches

Patches are still necessary for playing RapidLok2 titles with the Vice emulator - and on the real machine if you don't have a drive speed control for remastering. Choose which protection checks you want to have disabled:

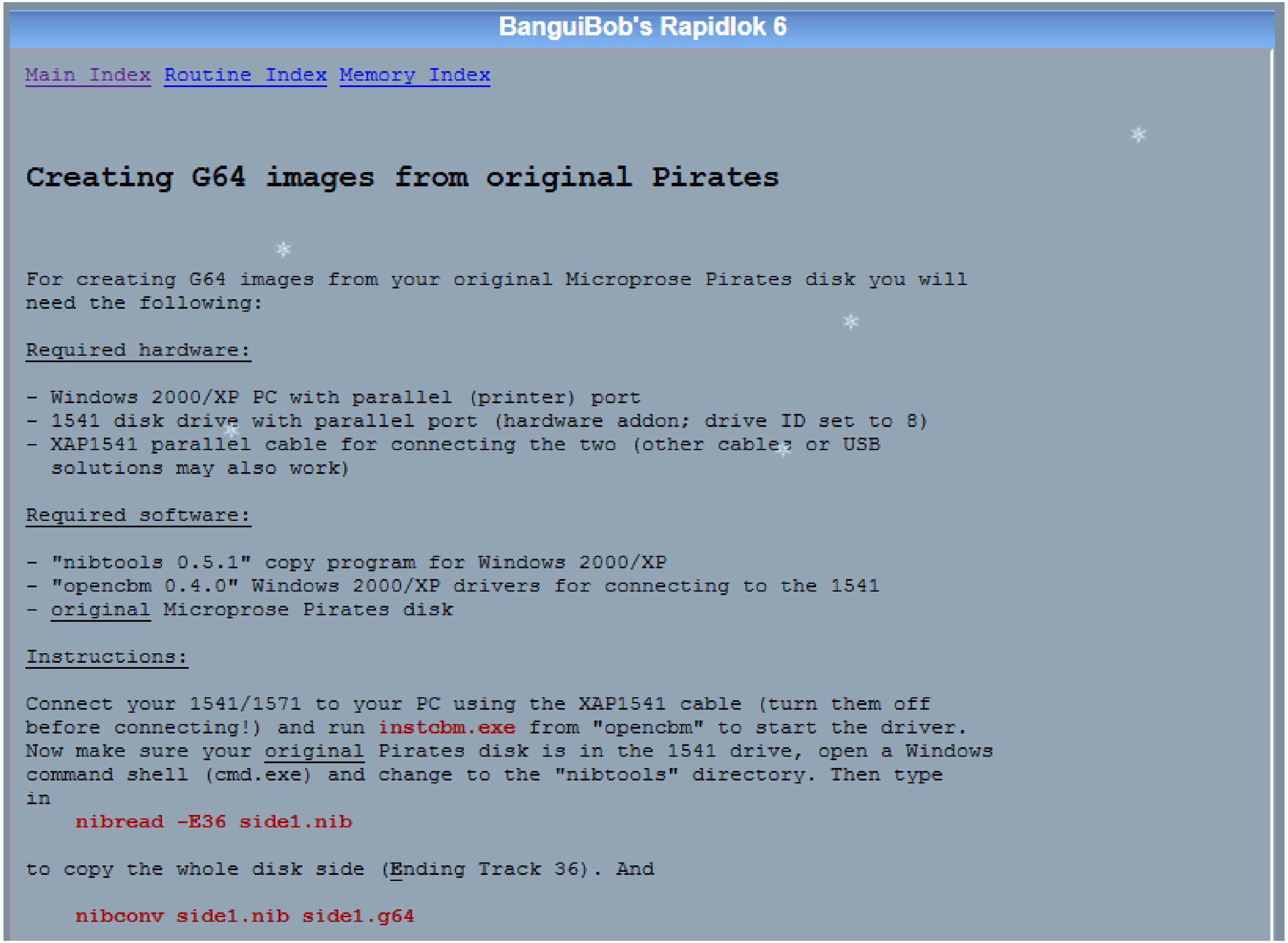
Type 5: Disable all protection checks **(default)**

for testing remastered disks:

Type 4: Disable the track alignment checks
Type 3: Disable the track 19 track header integrity checks
Type 2: Disable the track 36 handlers and the key checks
Type 1: Disable the key checks

The type 1-4 patches are independent and can be combined with each other.

All patches/fixes here apply to both PAL and NTSC versions of RapidLok2. You will have to apply them to all protected disks and/or protected disk sides, of course. Remember to enable "True drive emulation" in Vice emulator.



BanguiBob's Rapidlok 6

# Creating G64 images from original Pirates

For creating G64 images from your original Microprose Pirates disk you will need the following:

Required hardware:

- Windows 2000/XP PC with parallel (printer) port
- 1541 disk drive with parallel port (hardware addon; drive ID set to 8)
- XAP1541 parallel cable for connecting the two (other cables or USB solutions may also work)

Required software:

- "nibtools 0.5.1" copy program for Windows 2000/XP
- "opencbm 0.4.0" Windows 2000/XP drivers for connecting to the 1541
- original Microprose Pirates disk

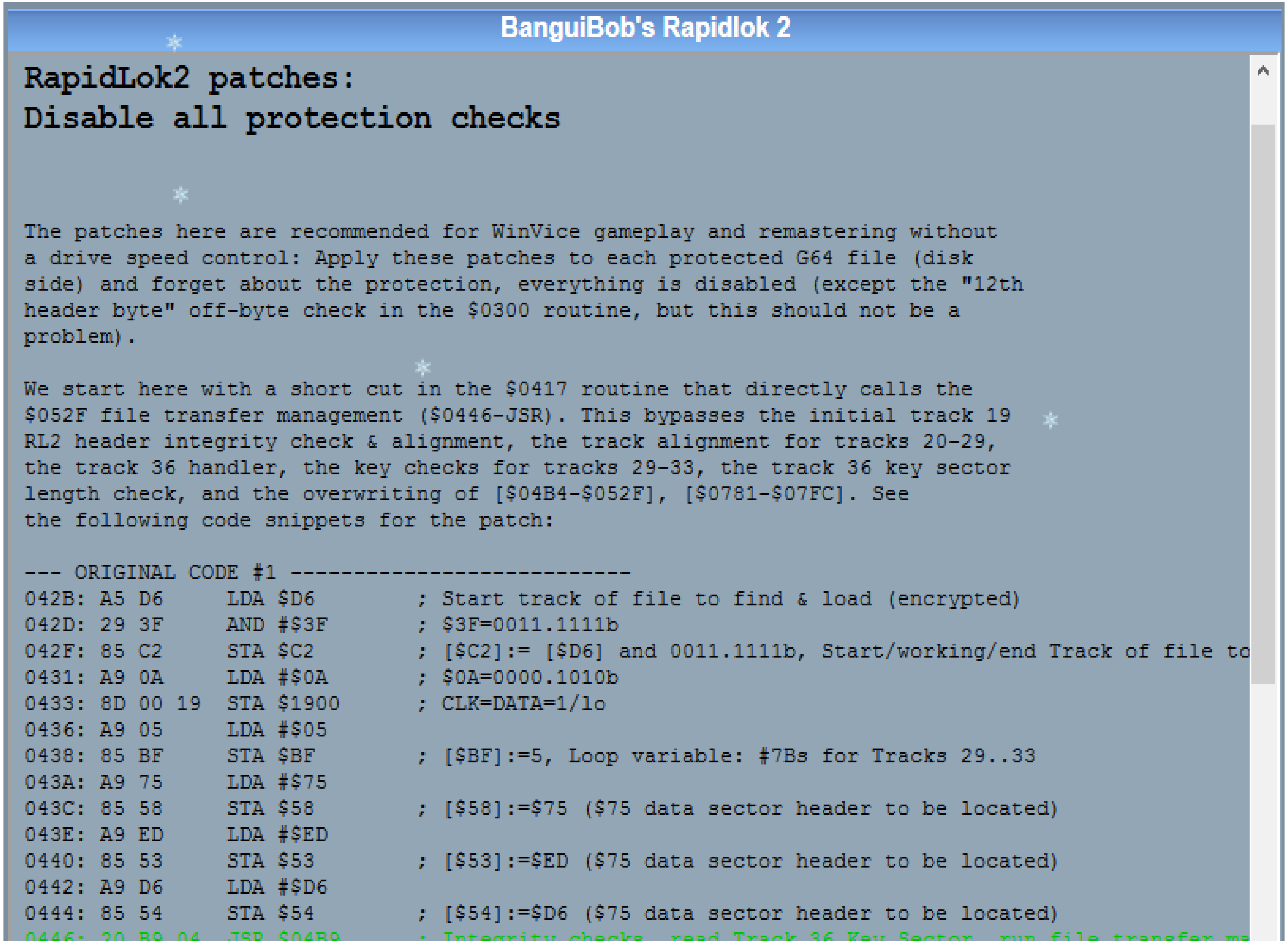
Instructions:

Connect your 1541/1571 to your PC using the XAP1541 cable (turn them off before connecting!) and run instcbm.exe from "opencbm" to start the driver. Now make sure your original Pirates disk is in the 1541 drive, open a Windows command shell (cmd.exe) and change to the "nibtools" directory. Then type in

```
    nibread -E36 side1.nib
```

to copy the whole disk side (Ending Track 36). And

```
    nibconv side1.nib side1.g64
```



# RapidLok2 patches:
# Disable all protection checks

The patches here are recommended for WinVice gameplay and remastering without a drive speed control: Apply these patches to each protected G64 file (disk side) and forget about the protection, everything is disabled (except the "12th header byte" off-byte check in the $0300 routine, but this should not be a problem).

We start here with a short cut in the $0417 routine that directly calls the $052F file transfer management ($0446-JSR). This bypasses the initial track 19 RL2 header integrity check & alignment, the track alignment for tracks 20-29, the track 36 handler, the key checks for tracks 29-33, the track 36 key sector length check, and the overwriting of [$04B4-$052F], [$0781-$07FC]. See the following code snippets for the patch:

```
--- ORIGINAL CODE #1 ---------------------------
042B: A5 D6     LDA $D6        ; Start track of file to find & load (encrypted)
042D: 29 3F     AND #$3F       ; $3F=0011.1111b
042F: 85 C2     STA $C2        ; [$C2]:= [$D6] and 0011.1111b, Start/working/end Track of file to
0431: A9 0A     LDA #$0A       ; $0A=0000.1010b
0433: 8D 00 19  STA $1900      ; CLK=DATA=1/lo
0436: A9 05     LDA #$05
0438: 85 BF     STA $BF        ; [$BF]:=5, Loop variable: #7Bs for Tracks 29..33
043A: A9 75     LDA #$75
043C: 85 58     STA $58        ; [$58]:=$75 ($75 data sector header to be located)
043E: A9 ED     LDA #$ED
0440: 85 53     STA $53        ; [$53]:=$ED ($75 data sector header to be located)
0442: A9 D6     LDA #$D6
0444: 85 54     STA $54        ; [$54]:=$D6 ($75 data sector header to be located)
0446: 20 B9 04  JSR $04B9      ; Integrity checks, read Track 36 Key Sector, run file transfer ma
```

# Summer 2012: SPS enhances VICE

- True data read (KryoFlux) – but does not work
- Real hardware analysed & simulated
- Floppy emulation precision lifted from 1MHz to 16MHz (as in real hardware)
- VICE now can play 1:1 G64 dumps without modification
- Missing functionality added to G64
- G64 can now also be written perfectly back to disk

# But!

Several old images don't work in VICE anymore, mostly because copy protection fails!

# Lessons learned

- Always store what you have read in the first place
- Don't modify data
- If you need to modify or transform (which means you don't want to “repair” ingestion or emulation!), mark modified data and sources
- Archive various versions of emulator (binary + source!)
- Add version notes to whatever research you conduct or information you release

# Thanks for listening!

Christian Bartsch

The Software Preservation Society

http://www.softpres.org

cb@softpres.org

KryoFlux Products & Services Ltd

http://www.kryoflux.com

cb@kryoflux.com

# Remember:

- What has not been preserved is on your wanted list
- What you deem preserved comes off that list and you stop looking for it
- Make sure your dump is authentic, make sure it is verified
- You won't be able to come back to re-image years later – the media is dying