Learning By Failing

Today,
I'm going to tell you
about a time I failed…

...over, and over again...

A while a go, I bought a cheap security camera.

My ideal IoT Camera

- Does not spy on me.
- Convenient to use.
- Does not spy on me.

How secure is this thing really?

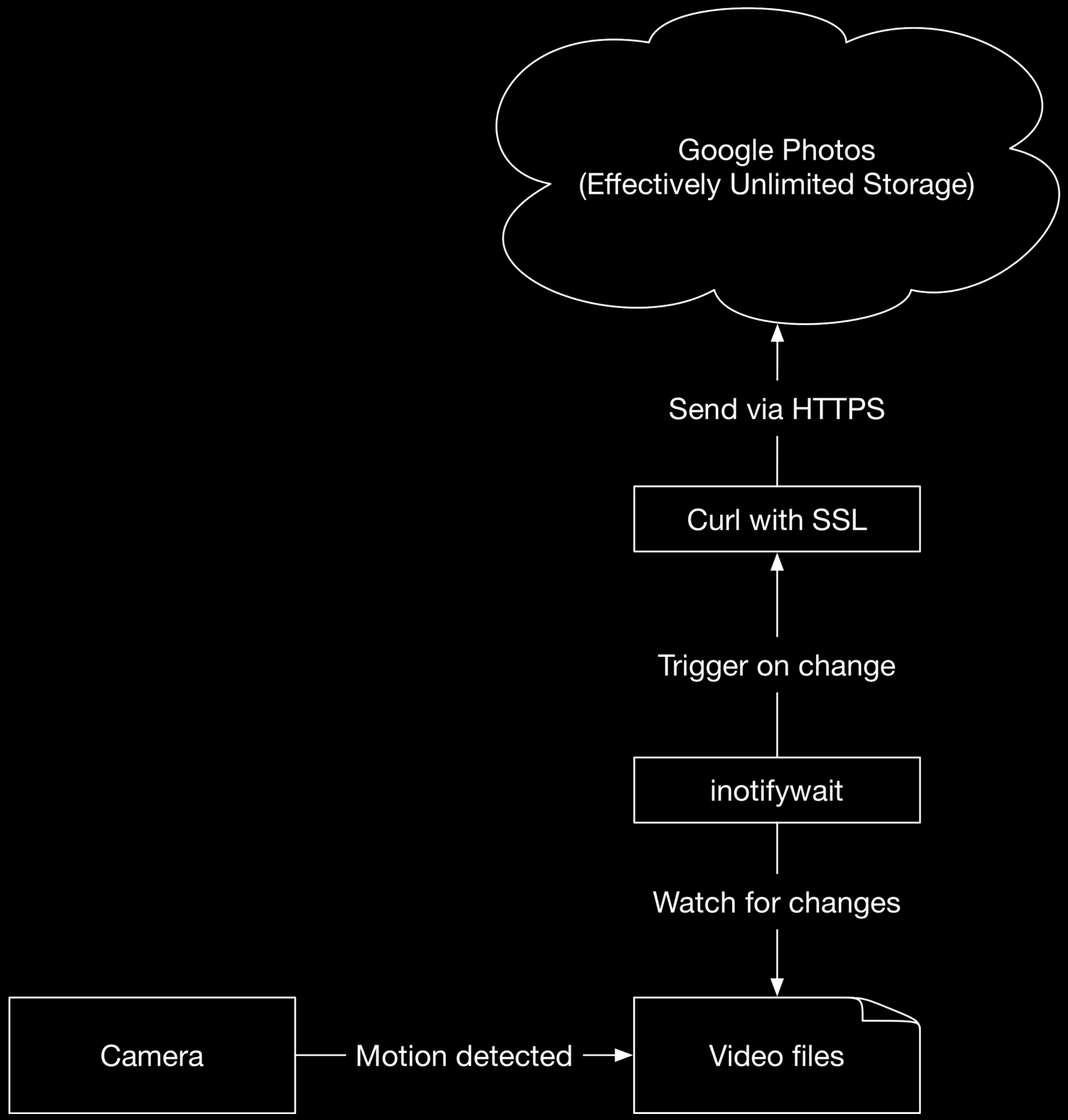
Can I SSH into it? Nope.
How about telnet? Nope.
Are there any open ports? Nope.

GitHub to the rescue!

```
nadav@mini:~/Projects$ ssh root@c1.local
root@c1.local's password:
Welcome to HiLinux.
~ #
```

Show me your dirty secrets.

```
/home/app # cat cloudAPI  | grep htt
http://openapi.kuaipan.cn/open/verificationURL
http://openapi.kuaipan.cn/1/account_info
http://openapi.kuaipan.cn/1/fileops/create_folder
http://openapi.kuaipan.cn/1/fileops/delete
http://openapi.kuaipan.cn/1/metadata/app_folder
http://api-content.dfs.kuaipan.cn/1/fileops/upload_locate
```

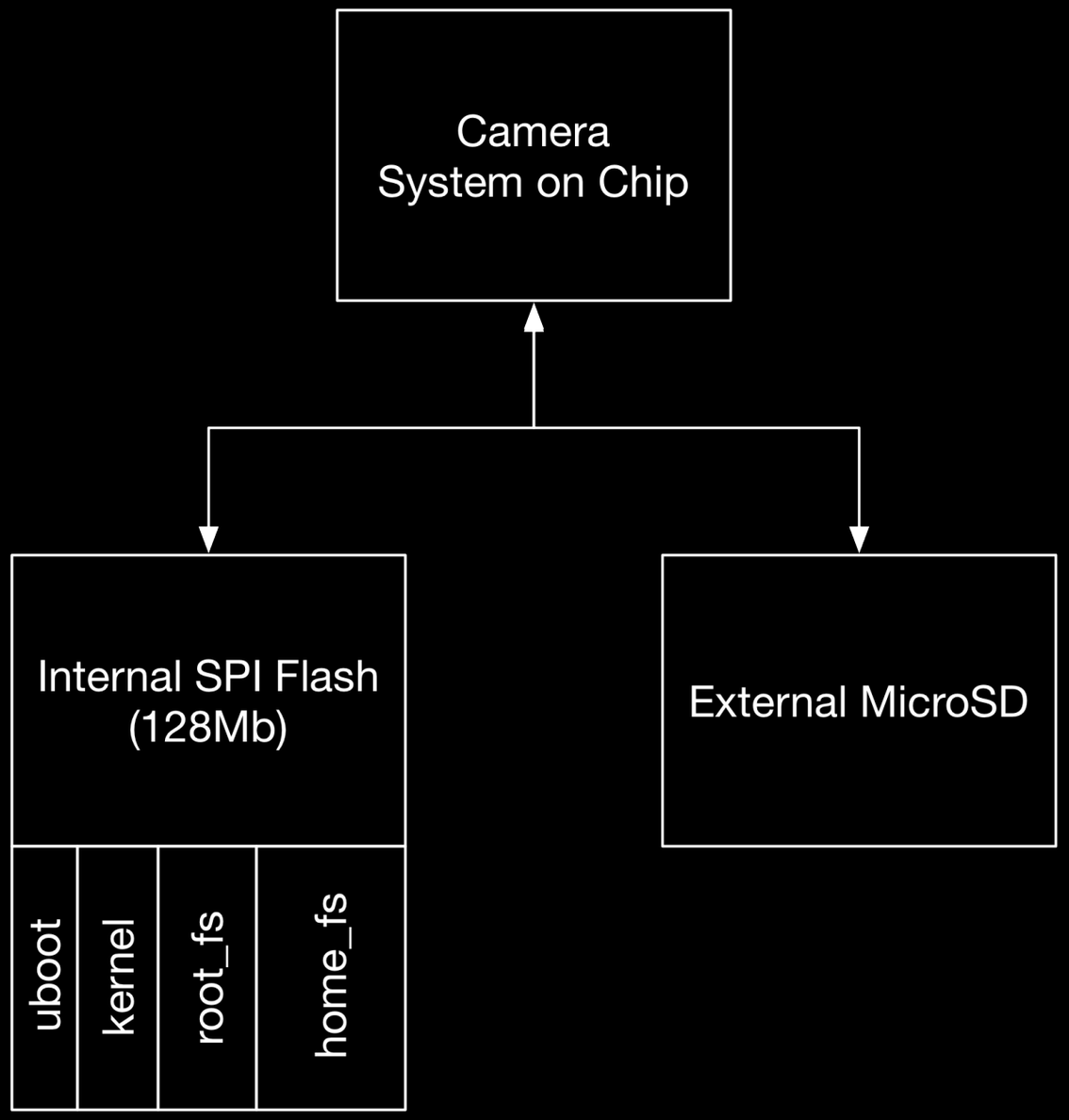

Google Photos
(Effectively Unlimited Storage)
Send via HTTPS
Curl with SSL
Trigger on change
inotifywait
Watch for changes
Camera
Motion detected
Video files

Compile all the things.

^ how using the SDK feels ^

Getting the binaries on the camera.

(cue ominous music)



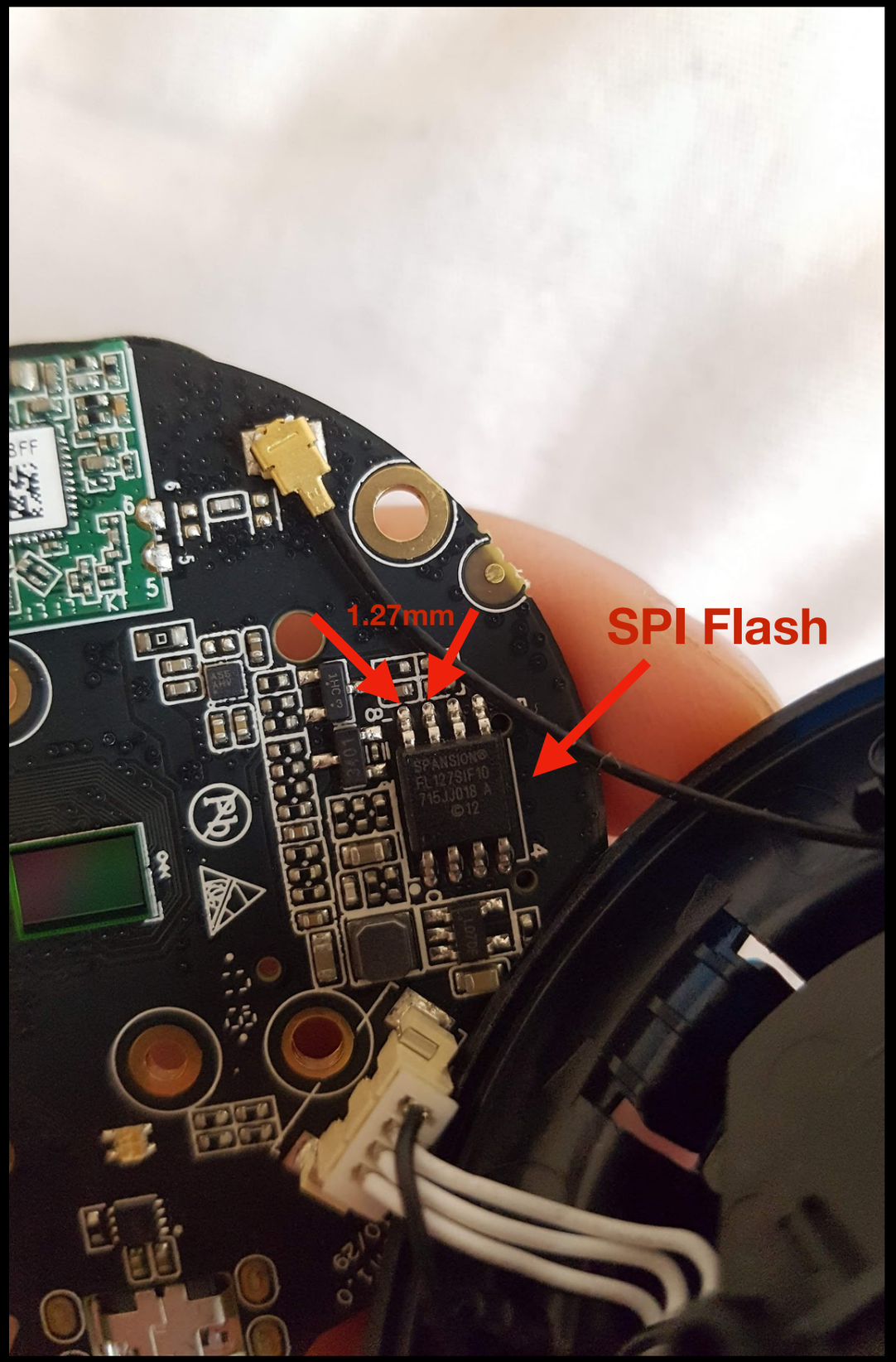
A rough view of the camera storage.

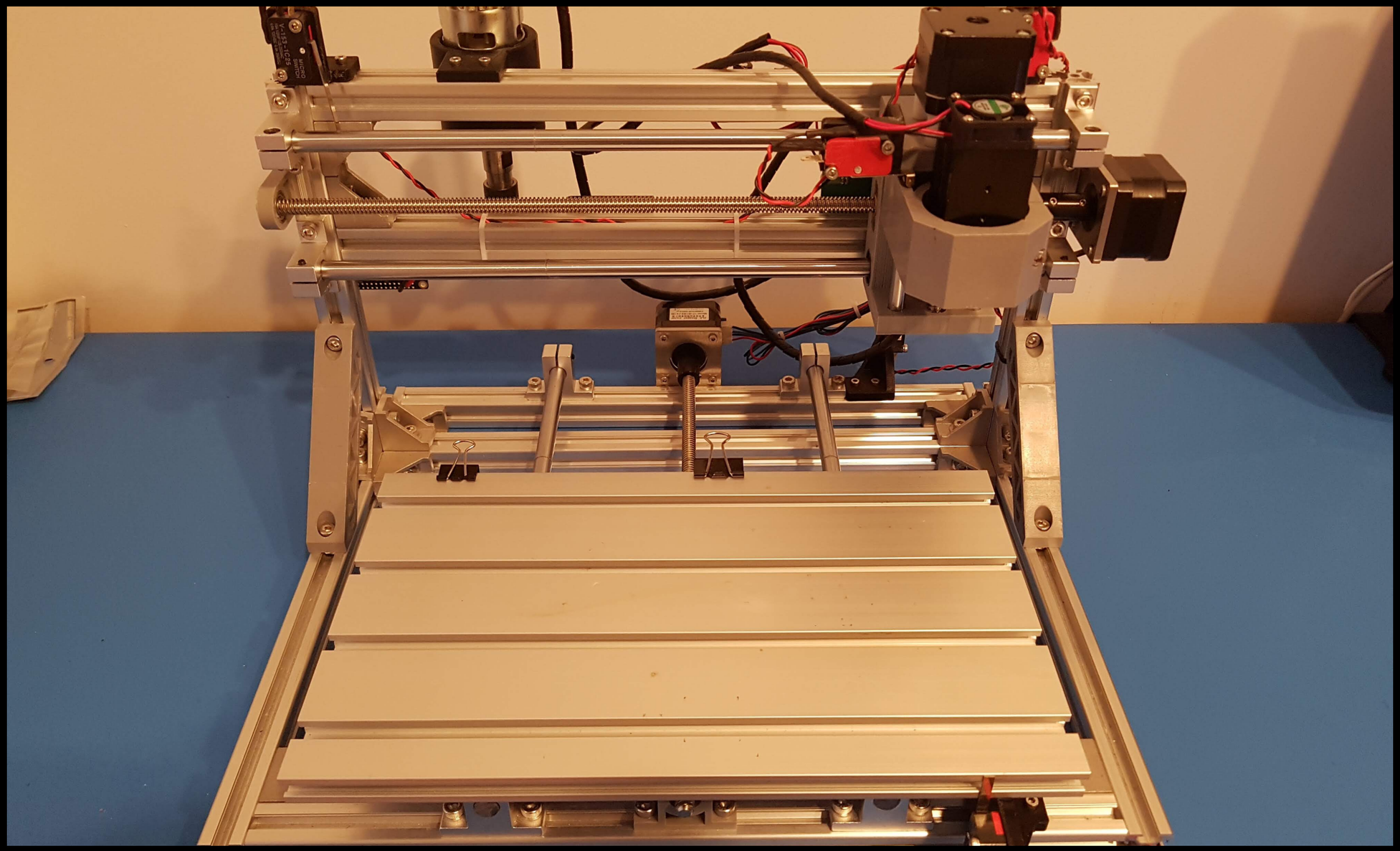
128 Mb != 128 MB


Delete! Delete! Delete!

I bricked it.

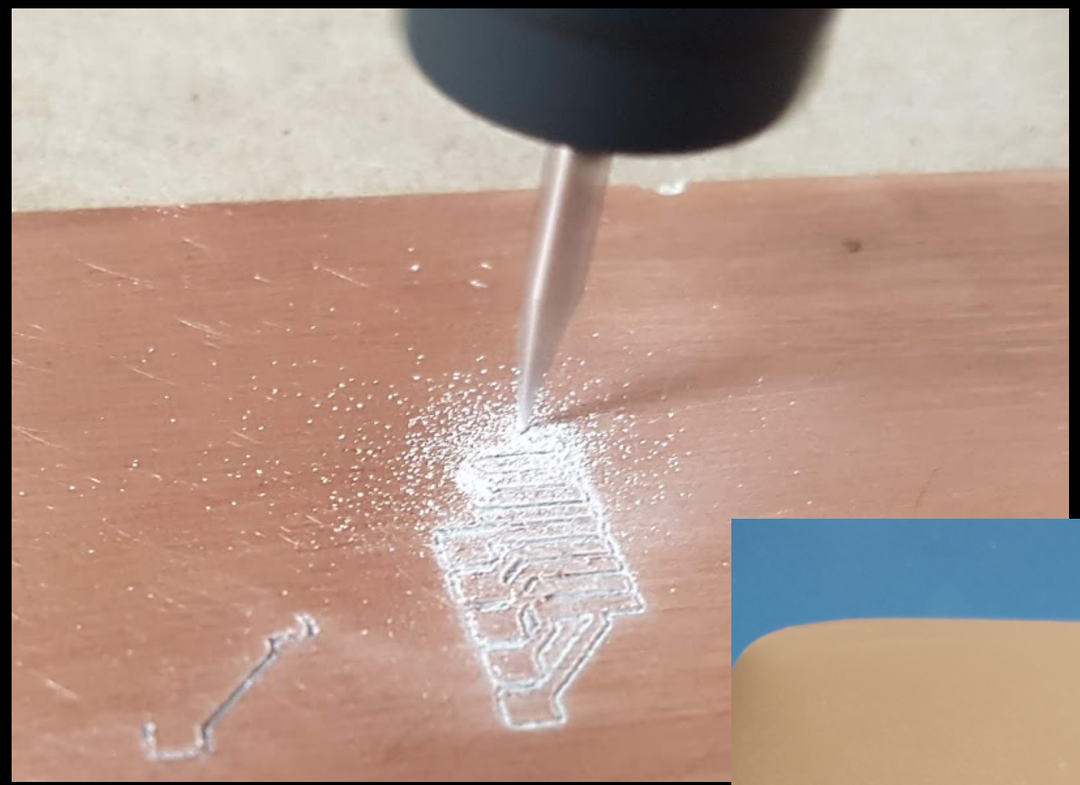
Tear it to bits.

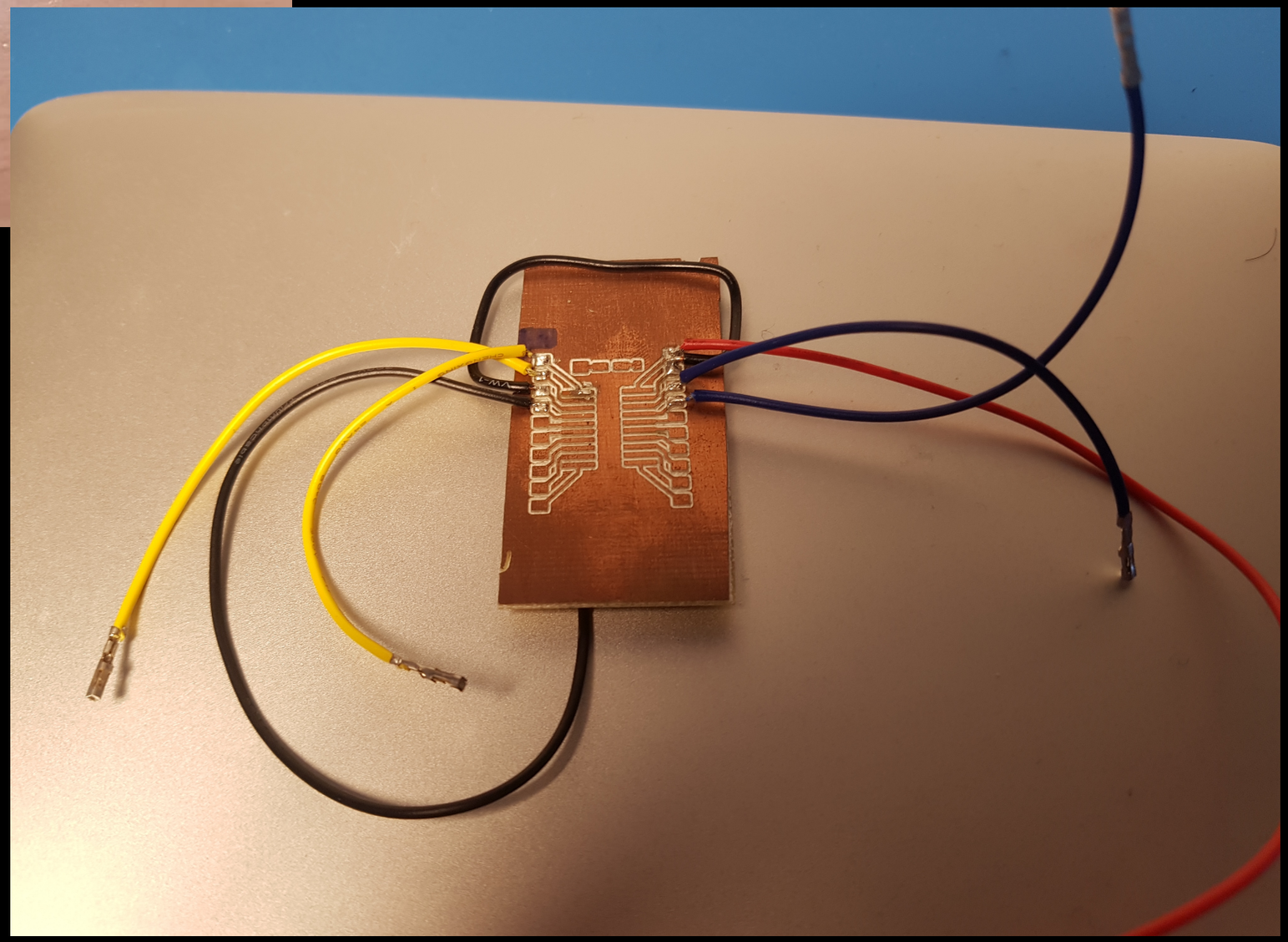




Custom adapter?


IMPERIAL-BEDROOMS





```
nadav@mini:~/Projects$ flashrom -p buspirate_spi:dev=/dev/tty.usbserial-
A100RUBF,spispeed=1M -c S25FL127S-256kB
flashrom v1.0 on Darwin 17.7.0 (x86_64)
flashrom is free software, get the source code at https://flashrom.org

Calibrating delay loop... OK.
No EEPROM/flash device found.
Note: flashrom can never write if the flash chip isn't found automatically.
```

But wait, theres more!

Success! Sort of...

Things I learned failing:

Cross-compile

Mill PCBs at home

Google all the things

Chase rabbit holes

RTFM

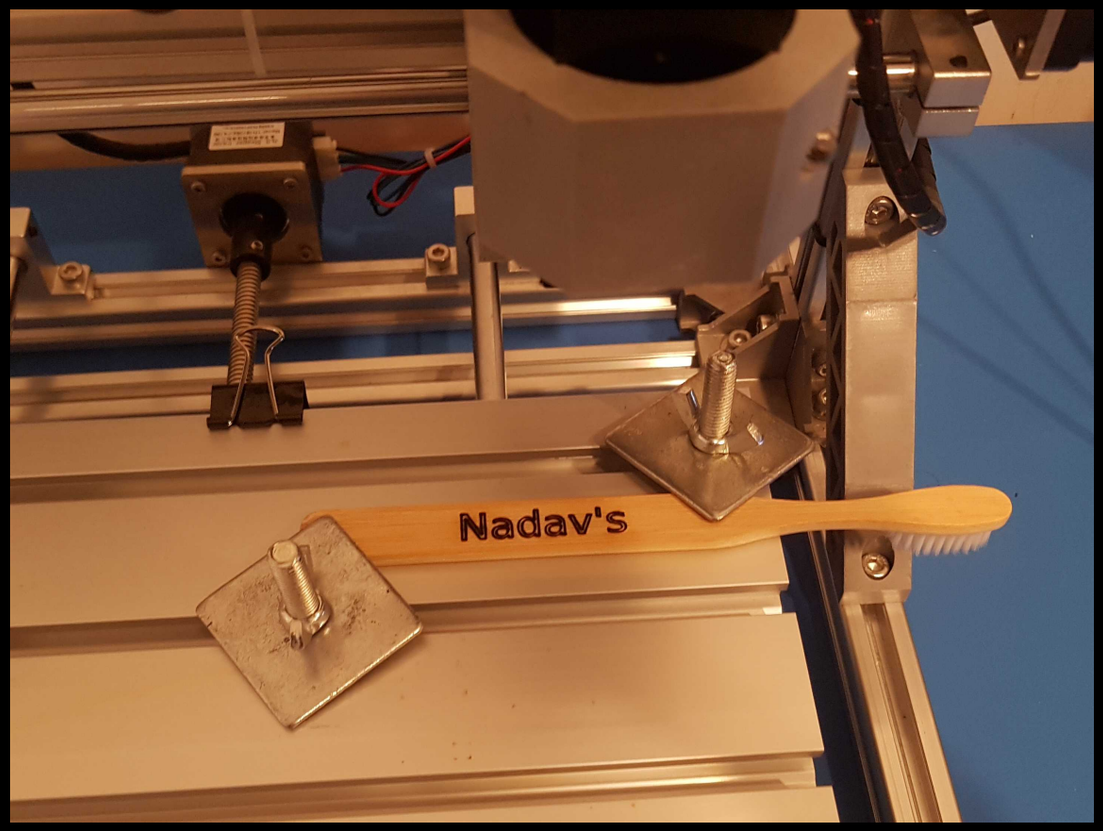
Read the docs and understand them.

RFTM

(Re-flash the MicroSD)

Thank You!

GitHub nadavami



My laser engraved toothbrush.