

Jon Marler - K4CHN - Aug 2024

Hacking the Quansheng UV-K5



K4CHN / Jon Marler

Amateur Radio Operator / Hacker

- First radio - Lafayette KT-200
- Passed Technician @ DefCon 27
- Passed General @ DefCon 28
- Passed Extra @ DefCon 29
- 40m voice
- Fairly active on 40m FT8
- Monitor 14.230 SSTV
- Breaker and fixer of all things



Presentation Agenda

Hacking the Quansheng UV-K5 Portable Radio

- Wiki, Models, and Features
- Functional Design & Hardware Specs
- Band filters (Spurious emissions are bad, m'kay?)
- Basic Mods & Manufacturing Issue Fixes
- Firmware Hacking
- Advanced Hardware Mods & Hacking

Quansheng UV-K5 - Wiki

Quansheng UV-K5 - Wiki

What's the best source of info & hacking documentation?

- Ludwich66 Wiki - https://github.com/ludwich66/Quansheng_UV-K5_Wiki/wiki
 - Links to various custom firmware
 - Telegram & Facebook groups
 - News about UV-K5
 - Hardware info & schematics
 - Hardware mod info & links
 - Battery pack mods



Quansheng UV-K5 - Models

Quansheng UV-K5 - General Specs

What are the specs on this radio?

- 2m & 70cm TX @ 5w - 50-600MHz, FM, NOAA, & Air Band RX
- Dual channel watch/scan, 200 channel memory, and channel copy
- Scrambler, DTMF/MDC1200, VOX TX
- Flashlight LED
- Firmware stored in **R/W flash memory**
- Price: \$12 ~ \$30 USD depending on accessories and model

Frequency Ranges*

F1: 50.0000-76.0000MHz (RX only)

F2: 76.0000MHz-107.9750MHz (RX only)

F3: 108.0000-135.9750MHz (RX only)

F4: 136.0000-173.9750MHz (TX and RX)

F5: 174.0000-349.9750MHz (RX only)

F6: 350.0000-399.9750MHz (RX only)

F7: 400.0000-469.9750MHz (TX and RX)

F8: 470.0000-600.0000MHz (RX only)

* Stock firmware

FCC Part 15b Certified

Quansheng UV-K5 - Models

How many models are there?



UV-K5



UV-5R Plus

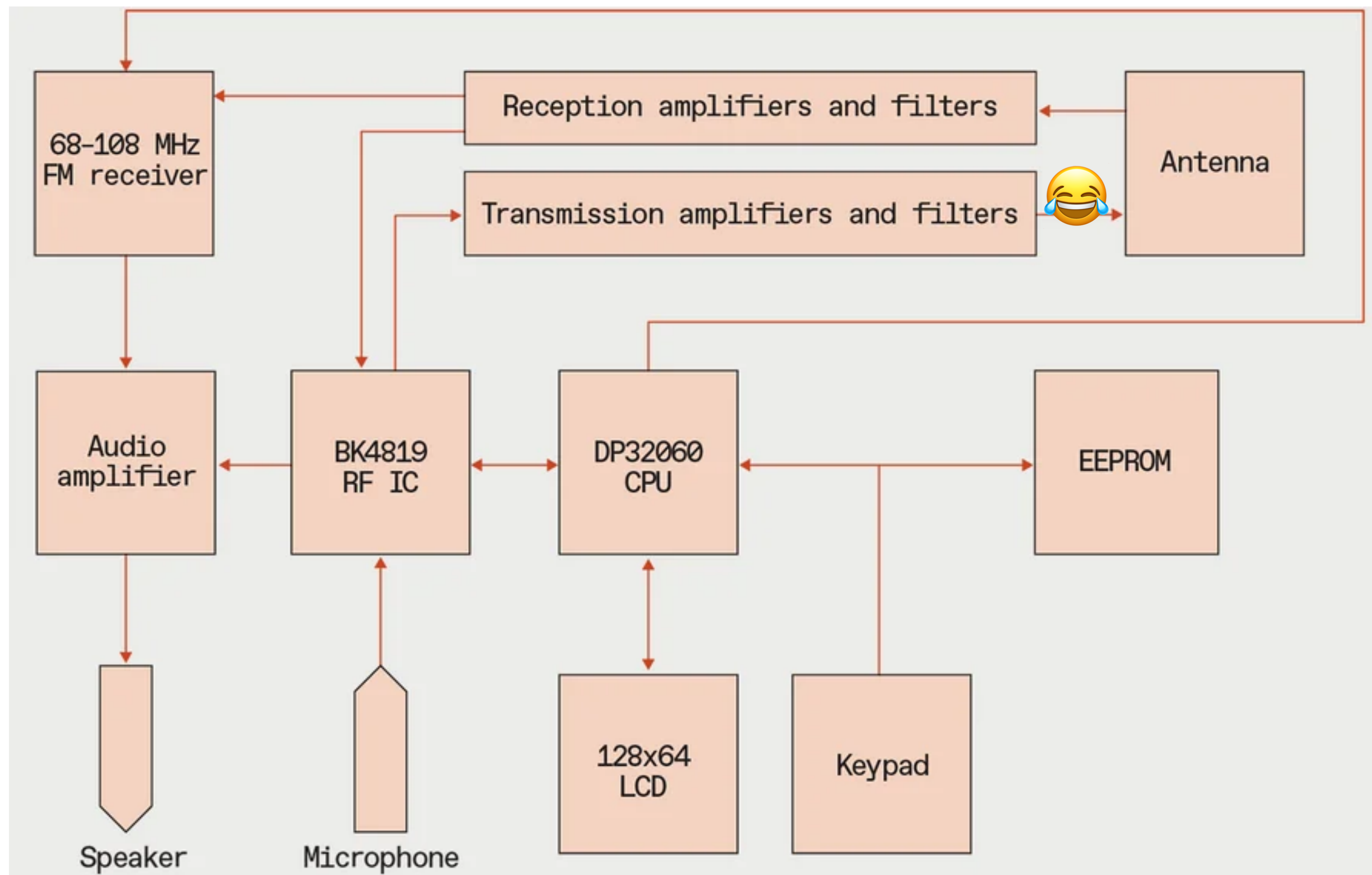


UV-K5(8)

Quansheng UV-K5 - Stock Hardware

Quansheng UV-K5 - Functional Design

How does this radio work?

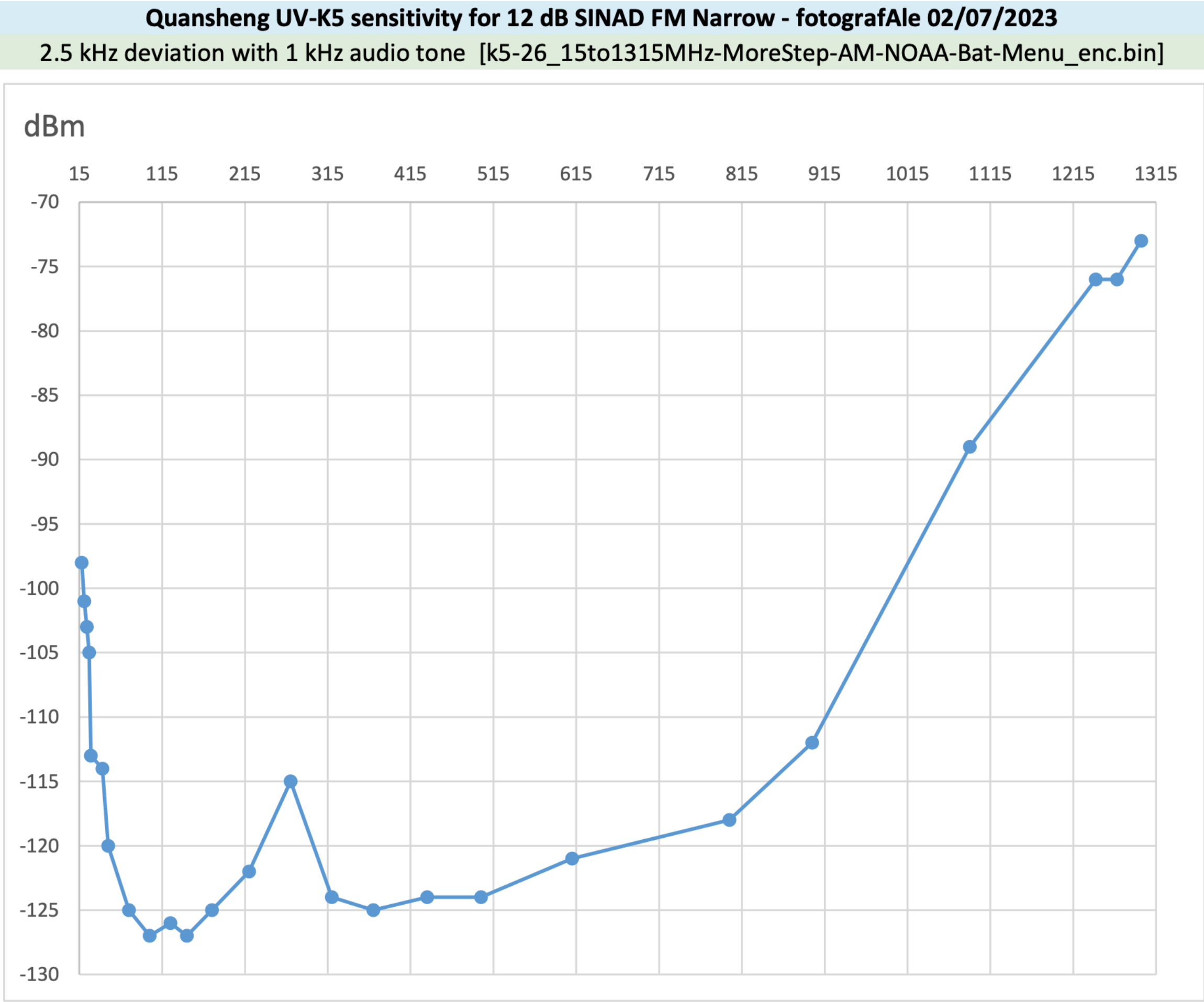


Courtesy: Phil McAllen

Quansheng UV-K5 - Sensitivity

Measured sensitivity of the UV-K5

Frequency	Level
MHz	dBm
16	-98
18	-98
21	-101
24	-103
27	-105
29	-113
43	-114
50	-120
75	-125
100	-127
125	-126
145	-127
175	-125
220	-122
270	-115
320	-124
370	-125
435	-124
500	-124
610	-121
800	-118
900	-112
1090	-89
1242	-76
1268	-76
1297	-73
1315	-73



Quansheng UV-K5 - Stock Antenna

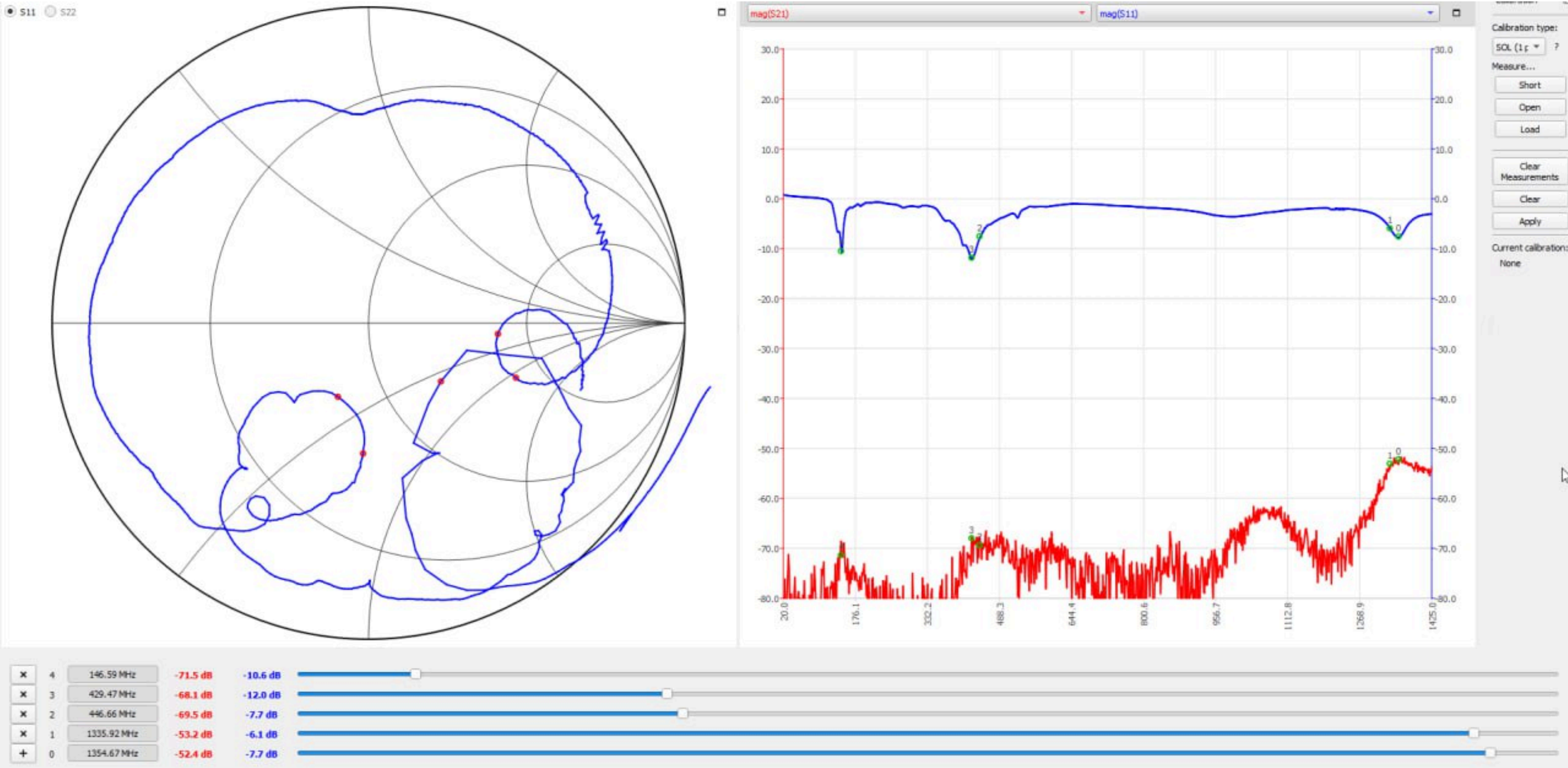
What does the antenna look like inside?



Photo Courtesy of: OneOfEleven

Quansheng UV-K5 - Stock Antenna

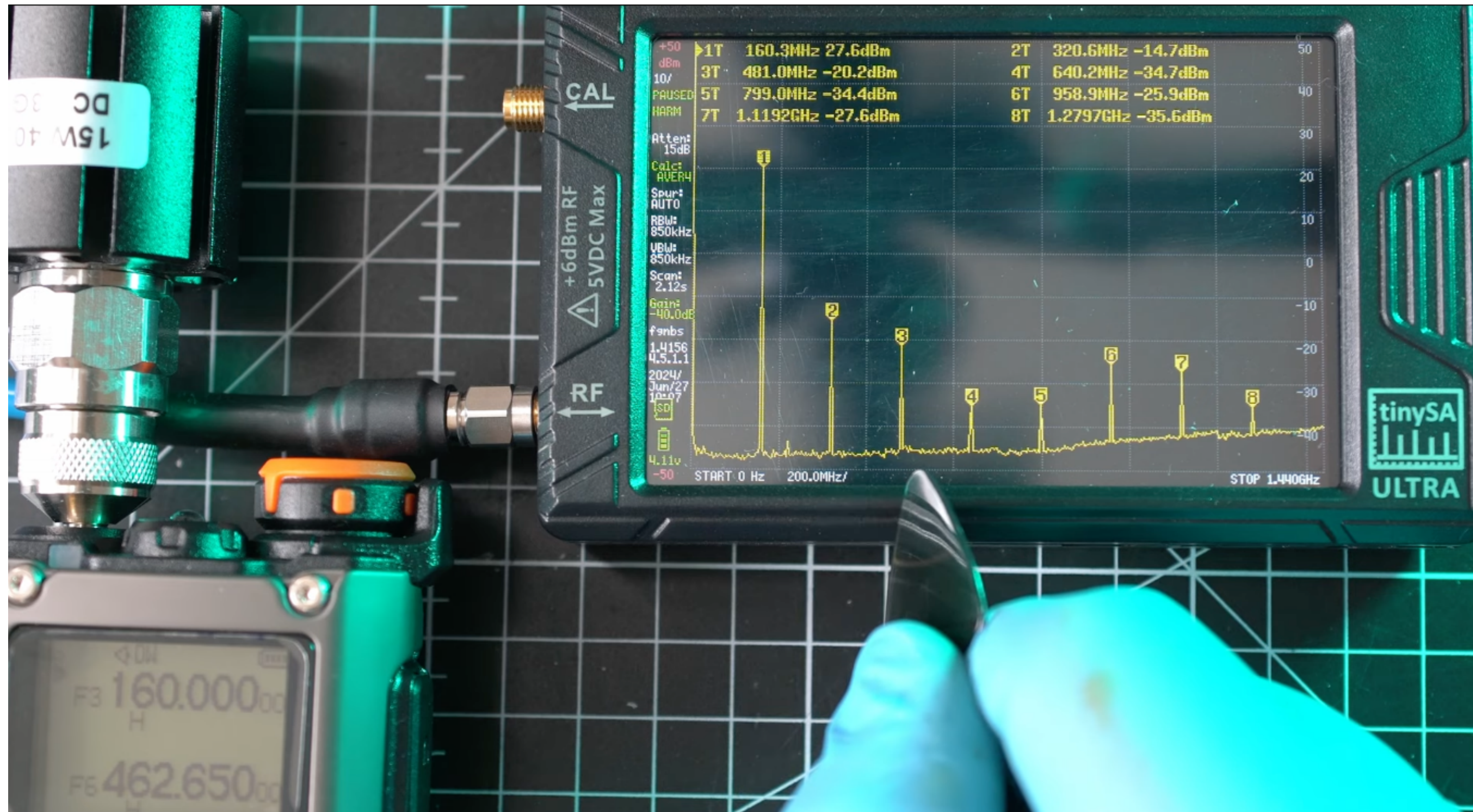
Frequency Analysis of Stock Antenna



Quansheng UV-K5 - Band Filters

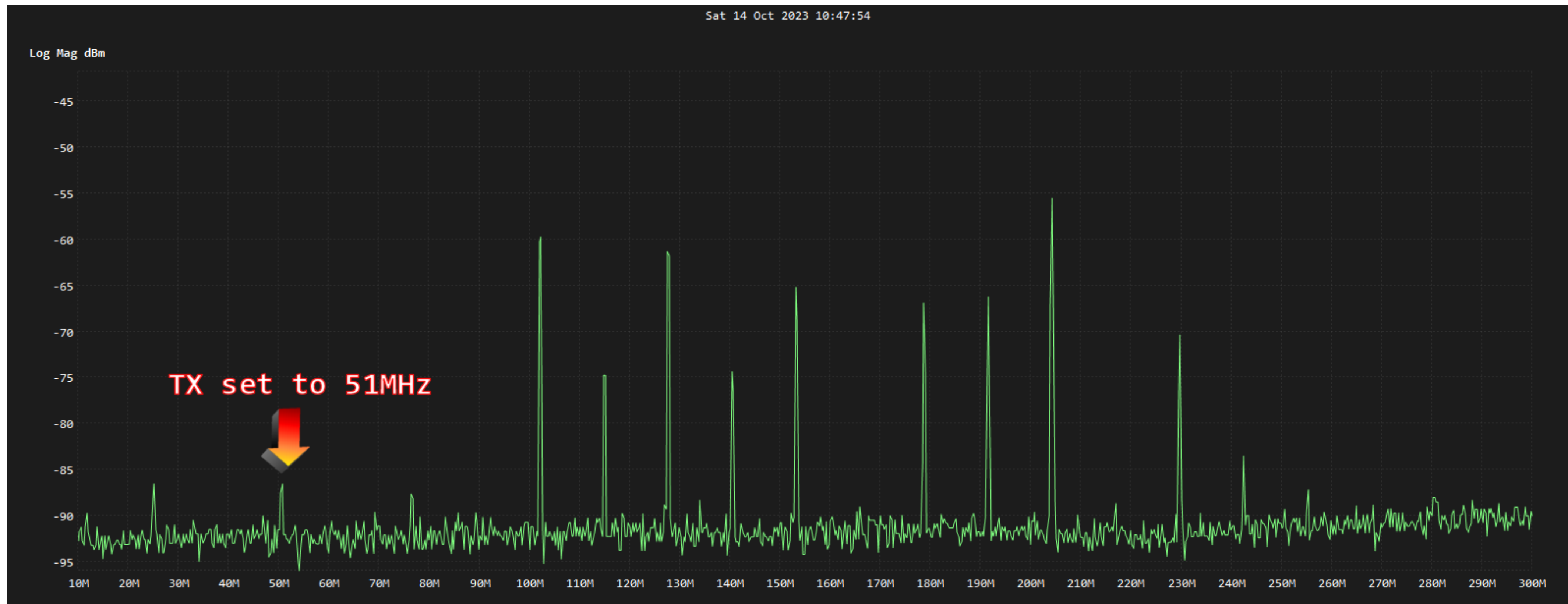
Quansheng UV-K5 - Band Filters

How do the band filters of the UV-K5 perform?



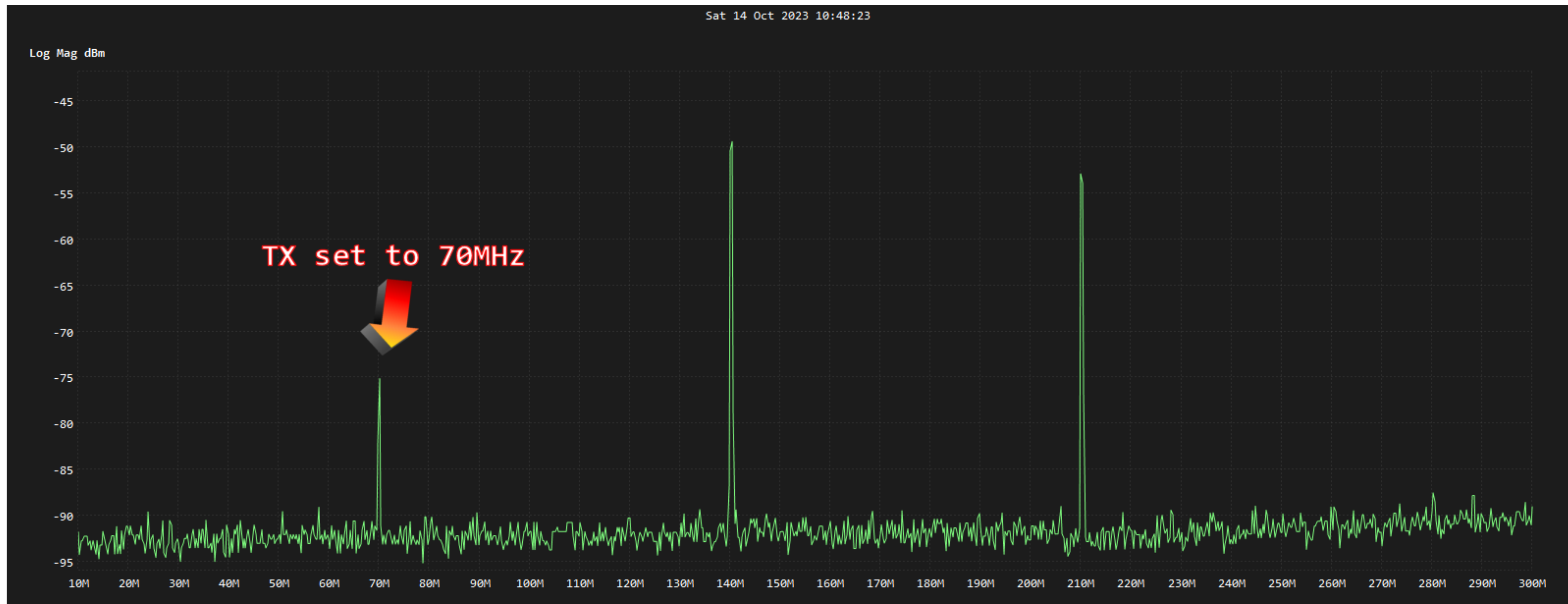
Quansheng UV-K5 - Band Filters

How do the band filters of the UV-K5 perform?



Quansheng UV-K5 - Band Filters

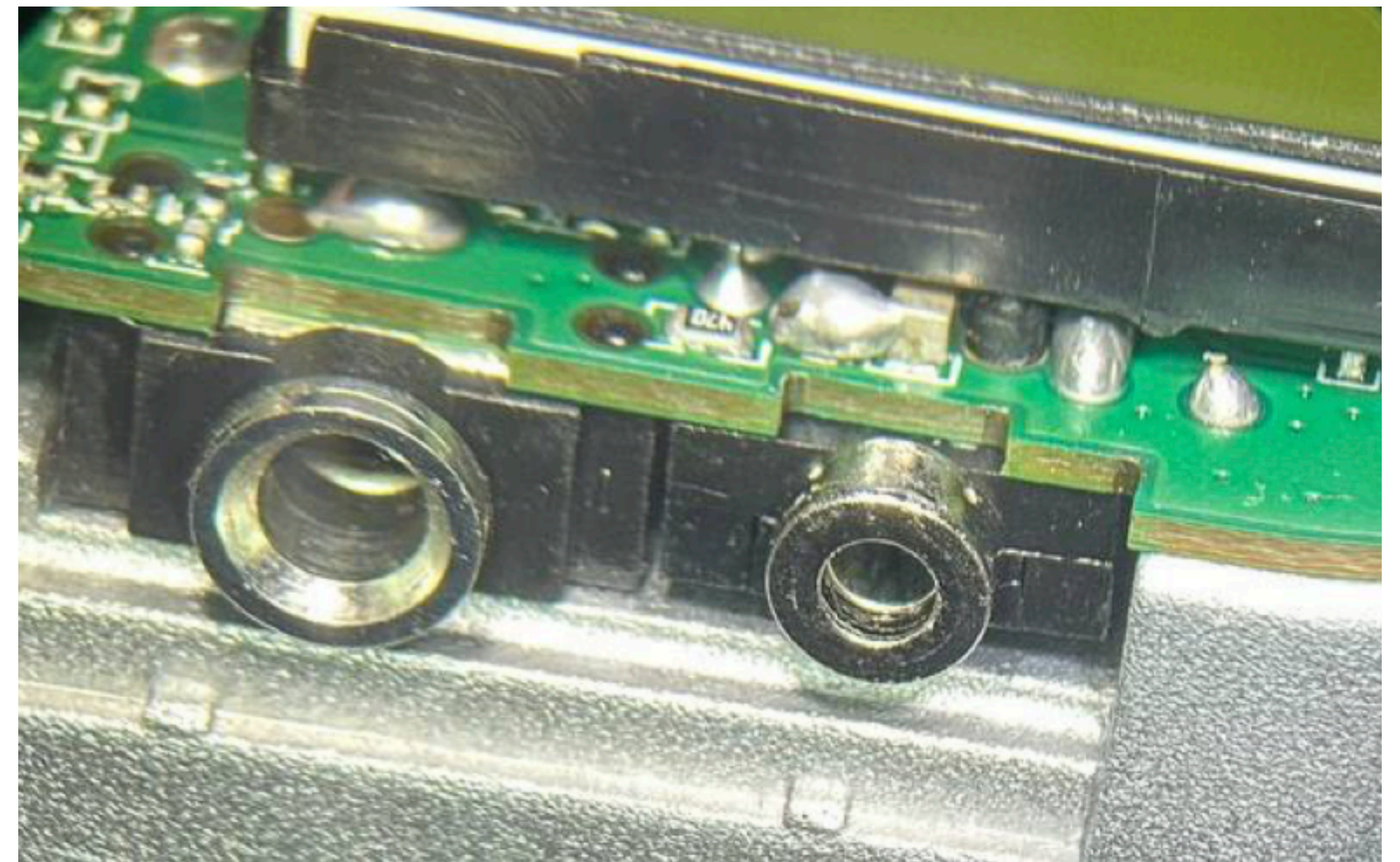
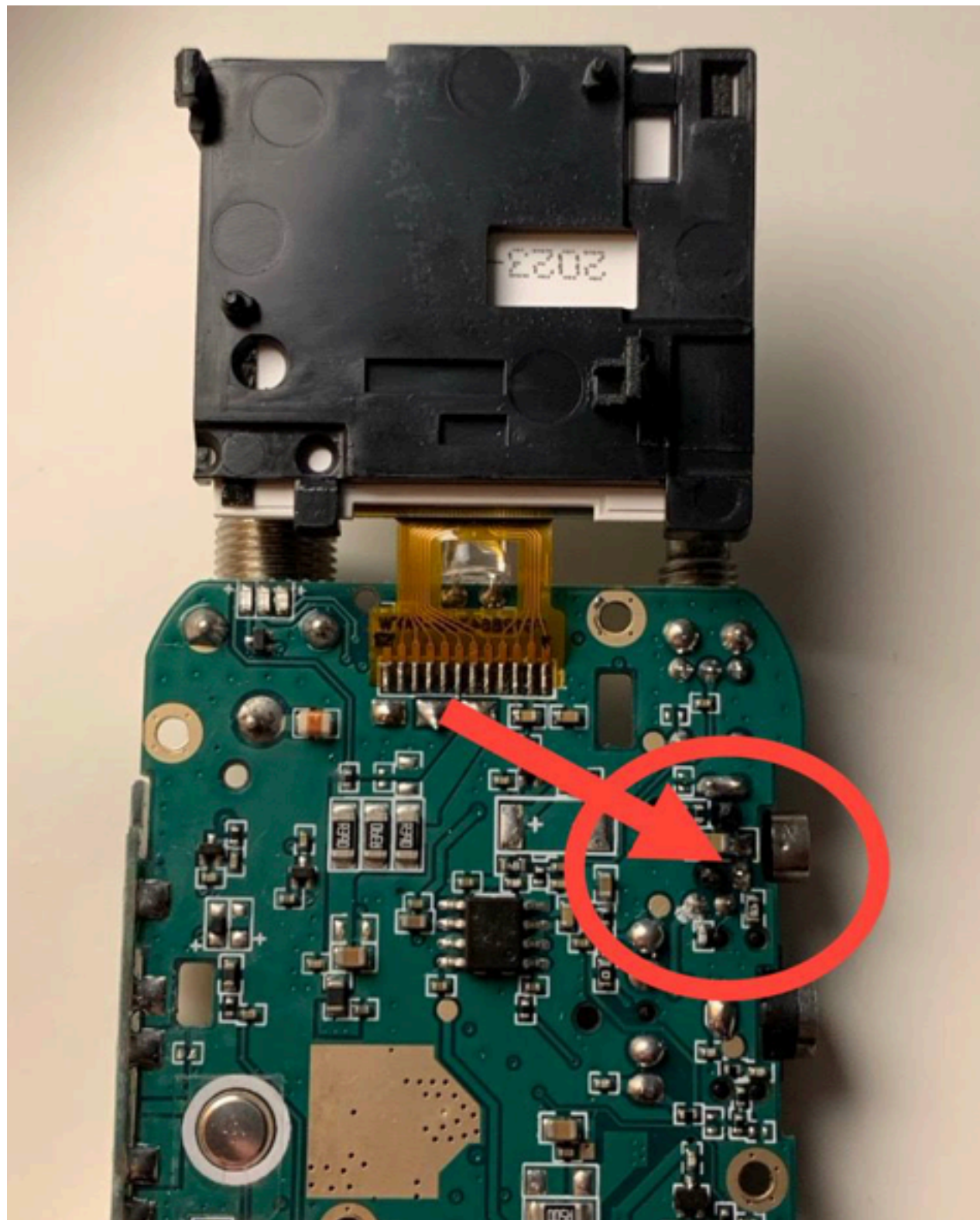
How do the band filters of the UV-K5 perform?



Quansheng UV-K5 - Basic Mods

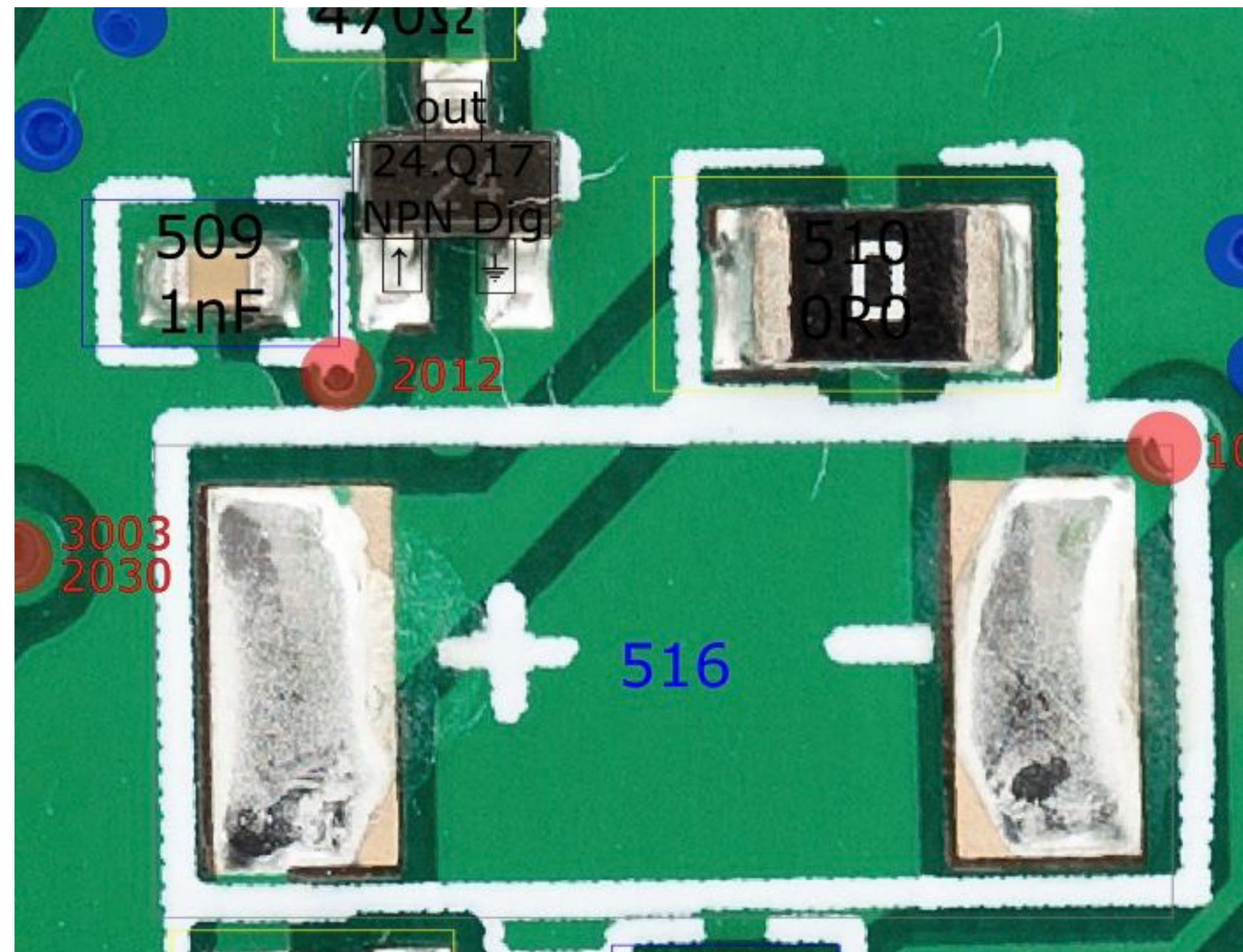
Quansheng UV-K5 - Basic Hardware Mods

What are some common manufacturing defects we can fix?



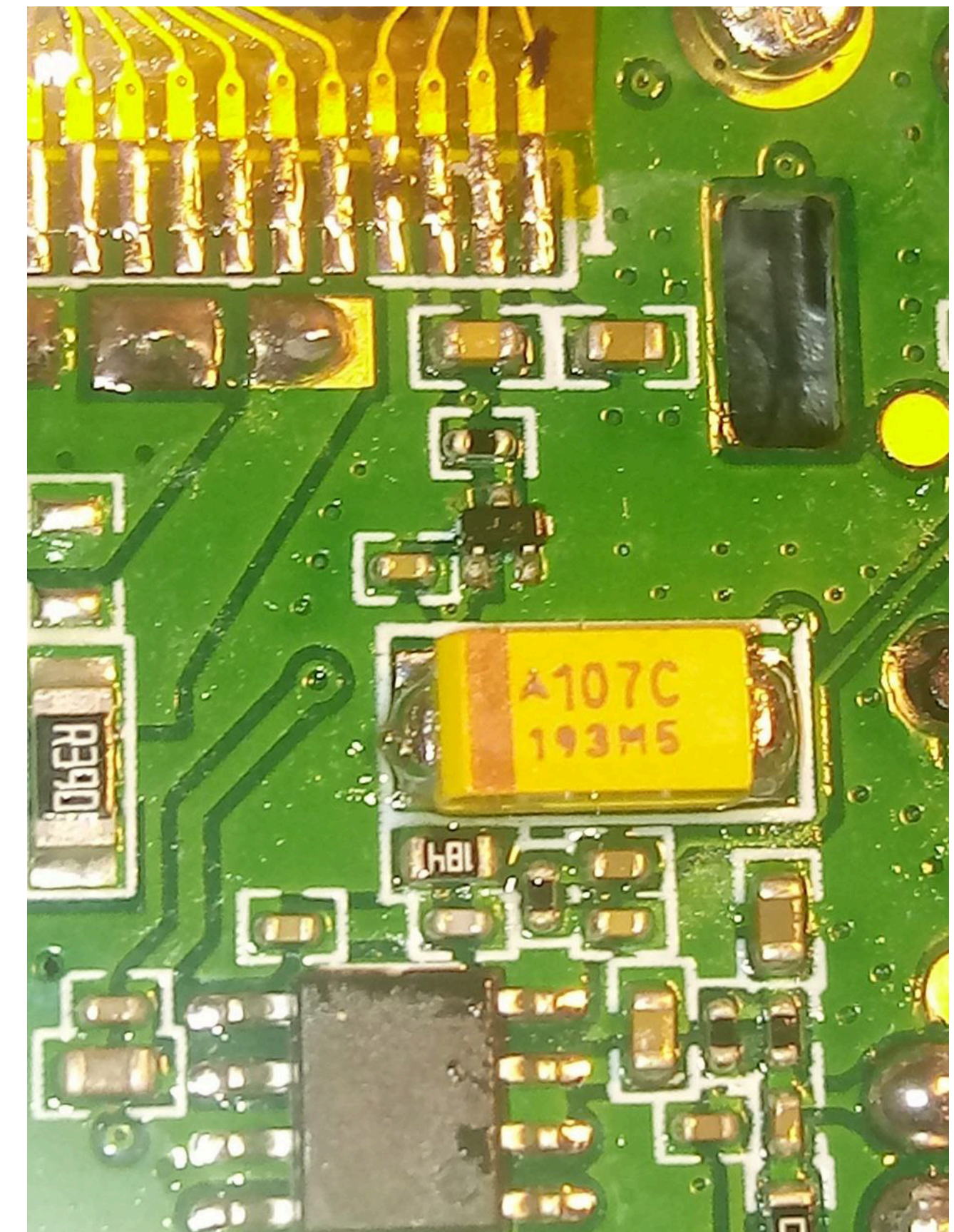
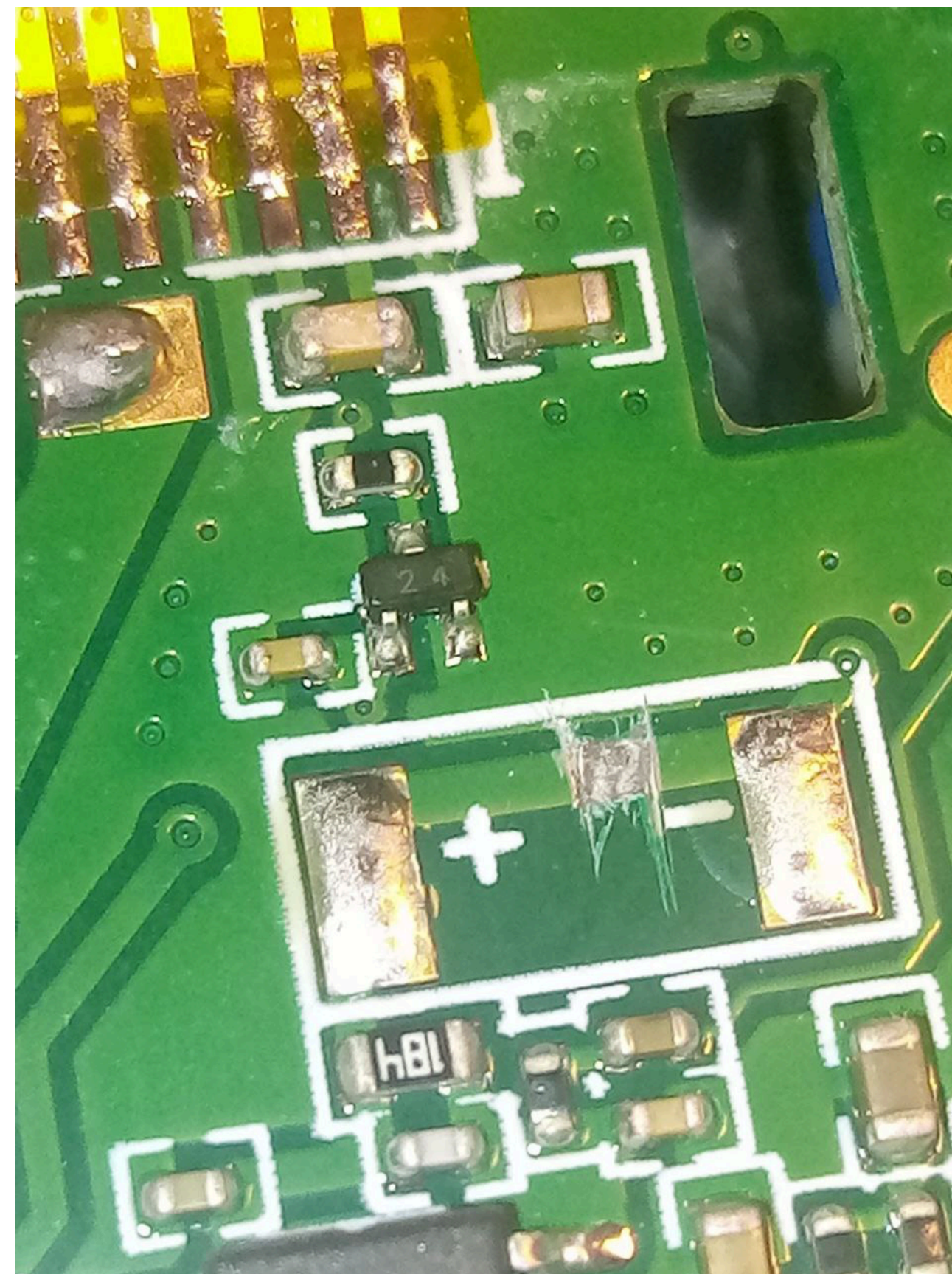
Quansheng UV-K5 - Manufacturing Defects

Adding a capacitor to address external PTT busy lockout issue



Quansheng UV-K5 - Manufacturing Defects

Adding a capacitor to address external PTT busy lockout issue



Quansheng UV-K5 - Firmware Hacking

Quansheng UV-K5 - Firmware Hacking

Beginner level hacking with stock firmware

- Official UVMOD - <https://whosmatt.github.io/uvmod/>
 - Works with stock firmware
 - Add custom apps
 - RSSI, S-Meter, & Battery voltage display
 - Spectrum analyzer (two flavors)
 - Text Messenger
 - Pong
 - Custom boot screen
- Bootscreen skip
- Backlight timeout
- TX disable
- Mic gain boost
- Roger beep
- Enable SWD Debug Port
- Frequency tweaks
 - Change steps
 - Change NOAA, AIR COPY, & FM frequencies



Quansheng UV-K5 - Firmware Hacking

Advanced level hacking with stock firmware

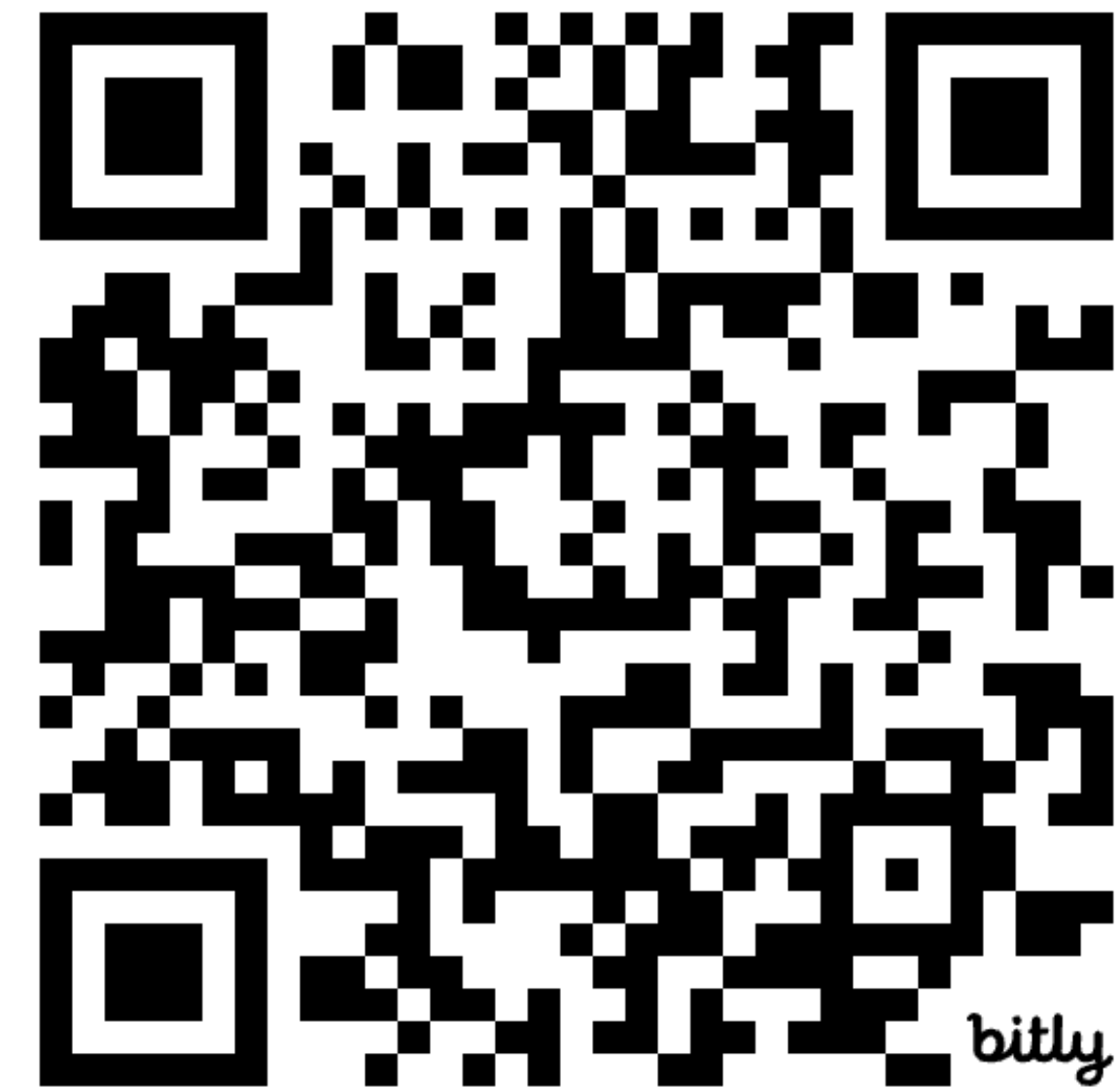
- RECON UVMOD - <http://uvmod.ddns.net/>
 - Works with stock firmware
 - Same features as official UVMOD
 - Full RX/TX unlock
 - Enhanced RX range unlock
 - Enable AM RX on all Bands
 - Custom Freq. Band Ranges
 - Custom repeater tones & ZVEI2



Quansheng UV-K5 - Firmware Hacking

Advanced level hacking with stock firmware

- EGZUMER - <https://github.com/egzumer/uv-k5-firmware-custom>
 - Fully open-source firmware from OneOfEleven & fagci
 - Full RX/TX unlock
 - AM RX & squelch fixes
 - Scanning & channel naming fixes
 - SSB demodulation
 - Stock bug fixes & new bugs to replace them
 - Customizable menus & menu navigation fixes
 - Customized button shortcuts and fixes



Quansheng UV-K5 - Firmware Hacking

Advanced level hacking with stock firmware

- UVK5CEC - <https://github.com/phdlee/uvk5cec>
 - Fork of the EGZUMER firmware
 - Support for FT8 & WSPR using WSJT-X
 - Integration with UK5DigManager 0.7
 - DIG.M (Digital Mode) for digital mode support
 - APRS & SSTV via APRS cable to PC
 - CW w/ external input support (CW, CWF, CWN)



Advanced Hardware Hacks

Quansheng UV-K5 - Hardware Hacking

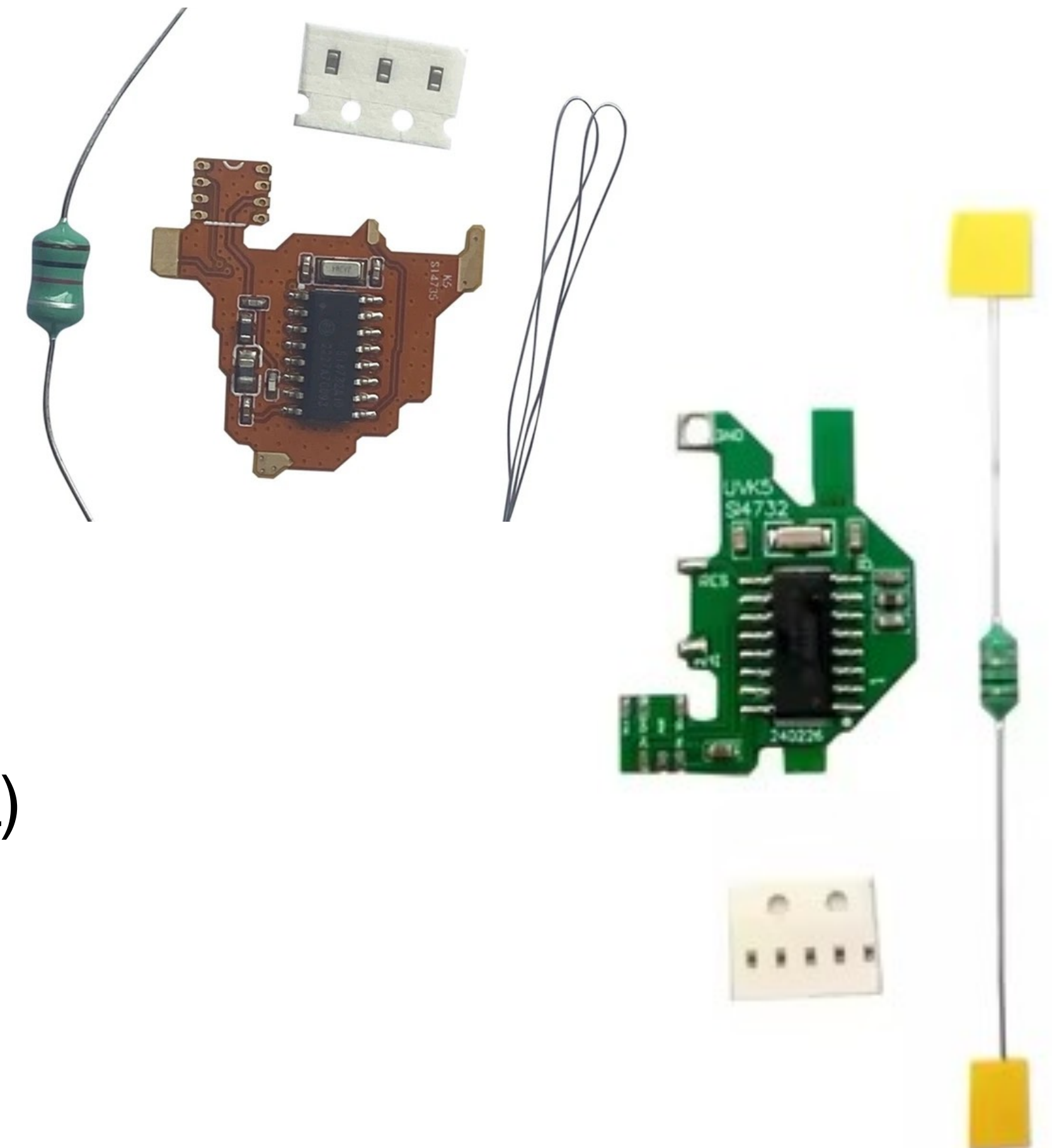
Advanced level hardware mods



Quansheng UV-K5 - Hardware Hacking

Advanced level hacking with the Si4732

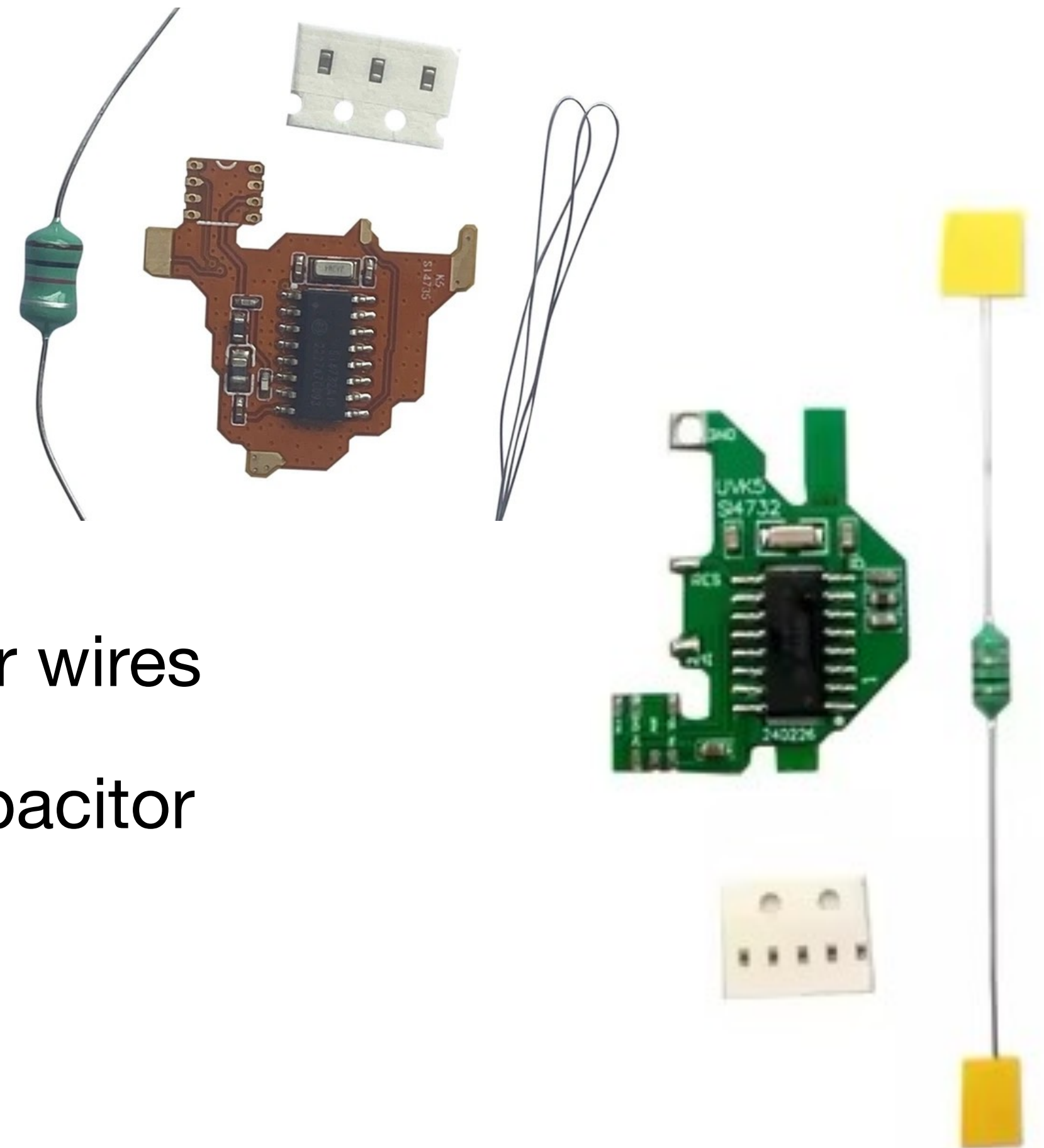
- Version 1 - Teda (Dario IV3NFC)
 - Replaces stock RF amplifier with Si4732(A10)
 - Improves AM reception
 - SSB demodulation & audio amplification
 - Redesigned FM & HF bandpass filters (RX only)
 - Available on AliExpress & Amazon (Shipped from China)
 - Uses CEC modded firmware to support Si4732 chip
 - **Requires SMD component removal & soldering**



Quansheng UV-K5 - Hardware Hacking

Si4732 Board Version 1 Installation Tips

- Use an appropriate soldering iron
- Fix the manufacturing defects first & test
- Use low-melt solder for removing the RX chip
- Flux is your friend
- Use some removed parts leg or wire strand for the jumper wires
 - Solder to the daughterboard first then the resistor / capacitor
- Save the parts you removed
- Buy a radio just for modding



Quansheng UV-K5 - Hardware Hacking

Si4732 Board Version 2

- Version 2 - R (Telegram DEV)
 - Replaces stock RF amplifier with Si4732
 - Improves AM reception
 - SSB demodulation & audio amplification
 - Additional antenna input with ESD
 - Redesigned FM & HF bandpass filters (RX only)
 - Thinner flex PCB & simpler installation steps
 - Available on AliExpress & Amazon (Shipped from China)
 - **Requires SMD component removal & soldering**



Quansheng UV-K5 - Hardware Hacking

Si4732 Board Version 2 Installation Tips

- Remove the LED and install the SMA jack for the second antenna
 - If you don't use the second antenna, install the new choke
- The antenna connector is easy to break
- Dedicate this radio to **RX only**
 - Disconnect the stock antenna (Remove cap)
 - Disable TX in firmware
- Use an IPX connector & coax to SMA / BNC
 - Buy an SMA jack w/ coax & IPX connector
- Use a microscope for soldering



Quansheng UV-K5 - Hardware Hacking

Si4732 Board Version 2.5

- Version 2.5
 - Adds amplifier to HF antenna
 - Includes IPX connector on mod board
 - Includes audio bypass mod
 - **Requires SMD component removal & soldering**



V2 Mod Installation

Quansheng UV-K5 - V2 Install

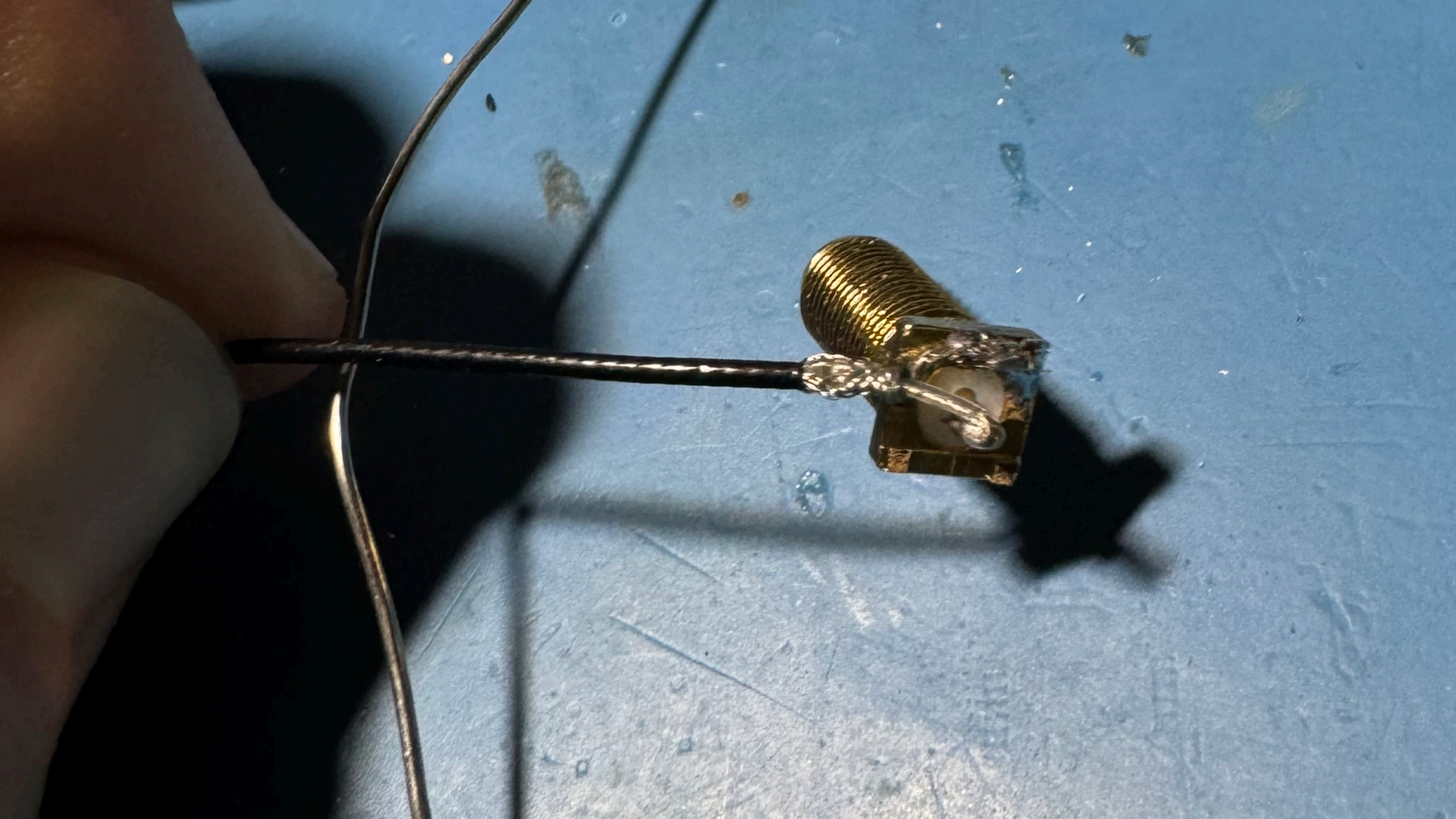
Photos & Video of V2 mod installation

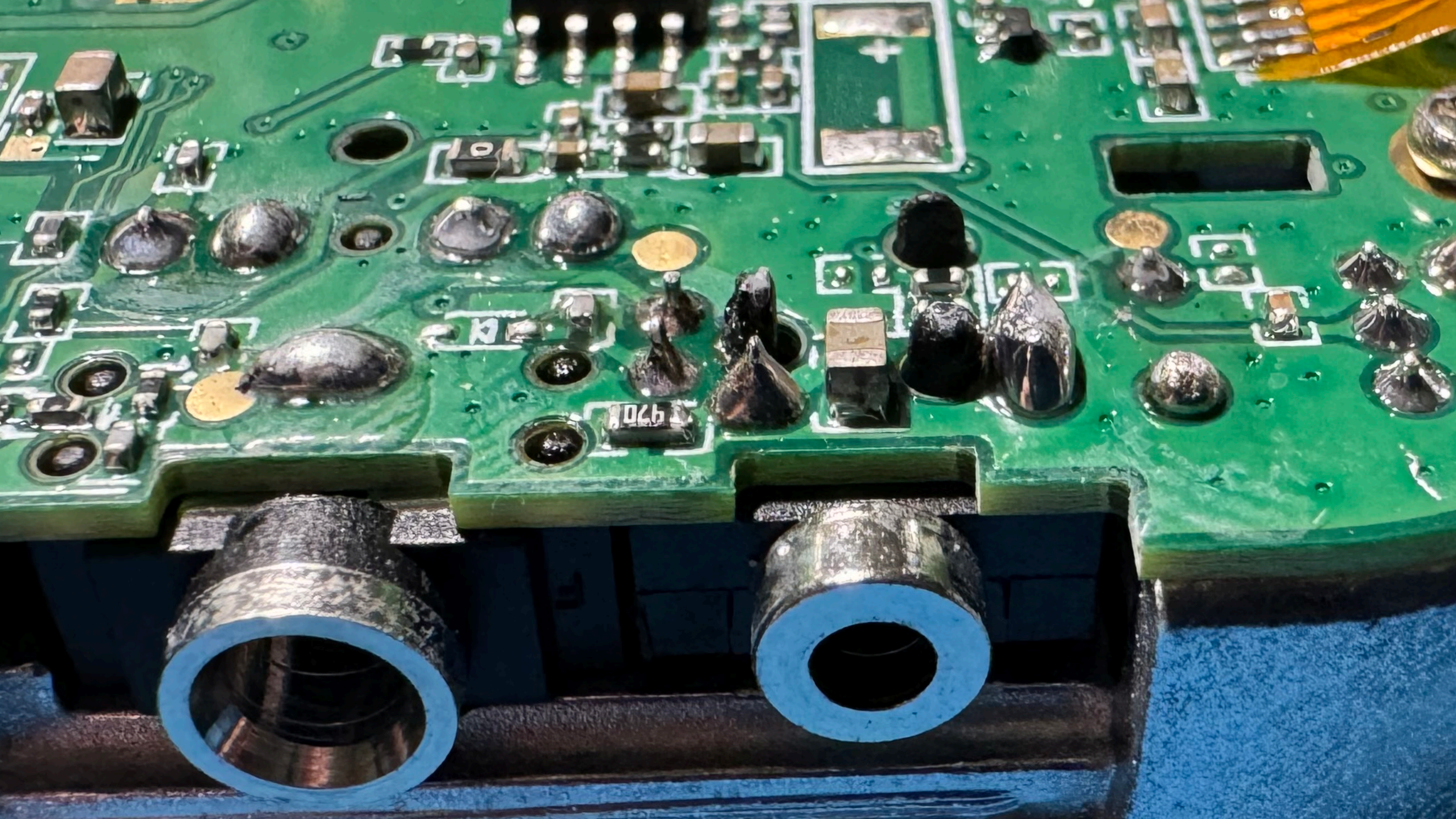
- Before you start:
 - Use a soldering iron with a blade and/or fine tip
 - Have some fine jumper wire available
 - Flux is your friend!
 - Visual magnification is **mandatory**
 - Low melt solder / Chip Quik & UV solder mask
 - **This is an advanced mod!!! Buy a spare or two!**

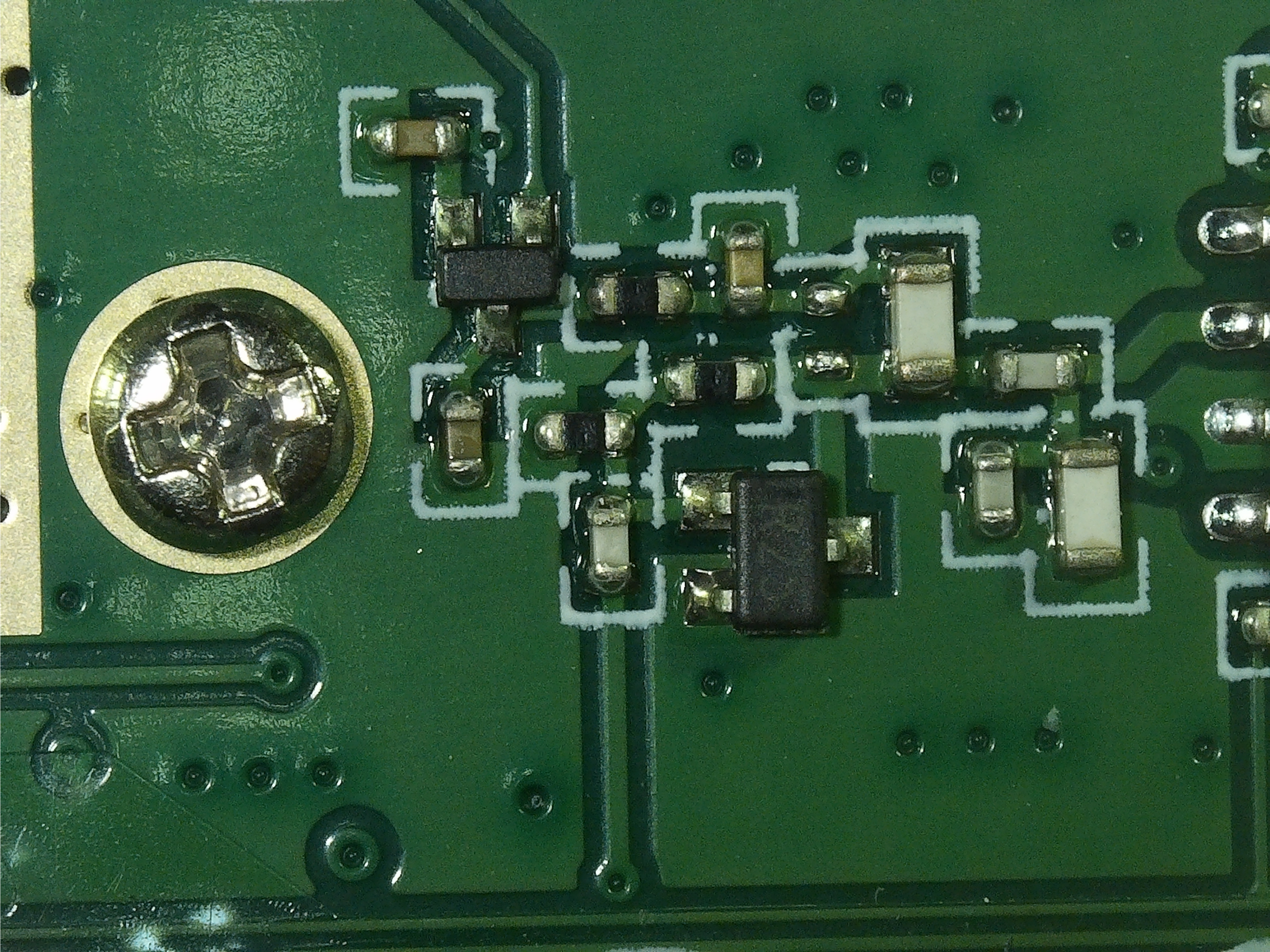


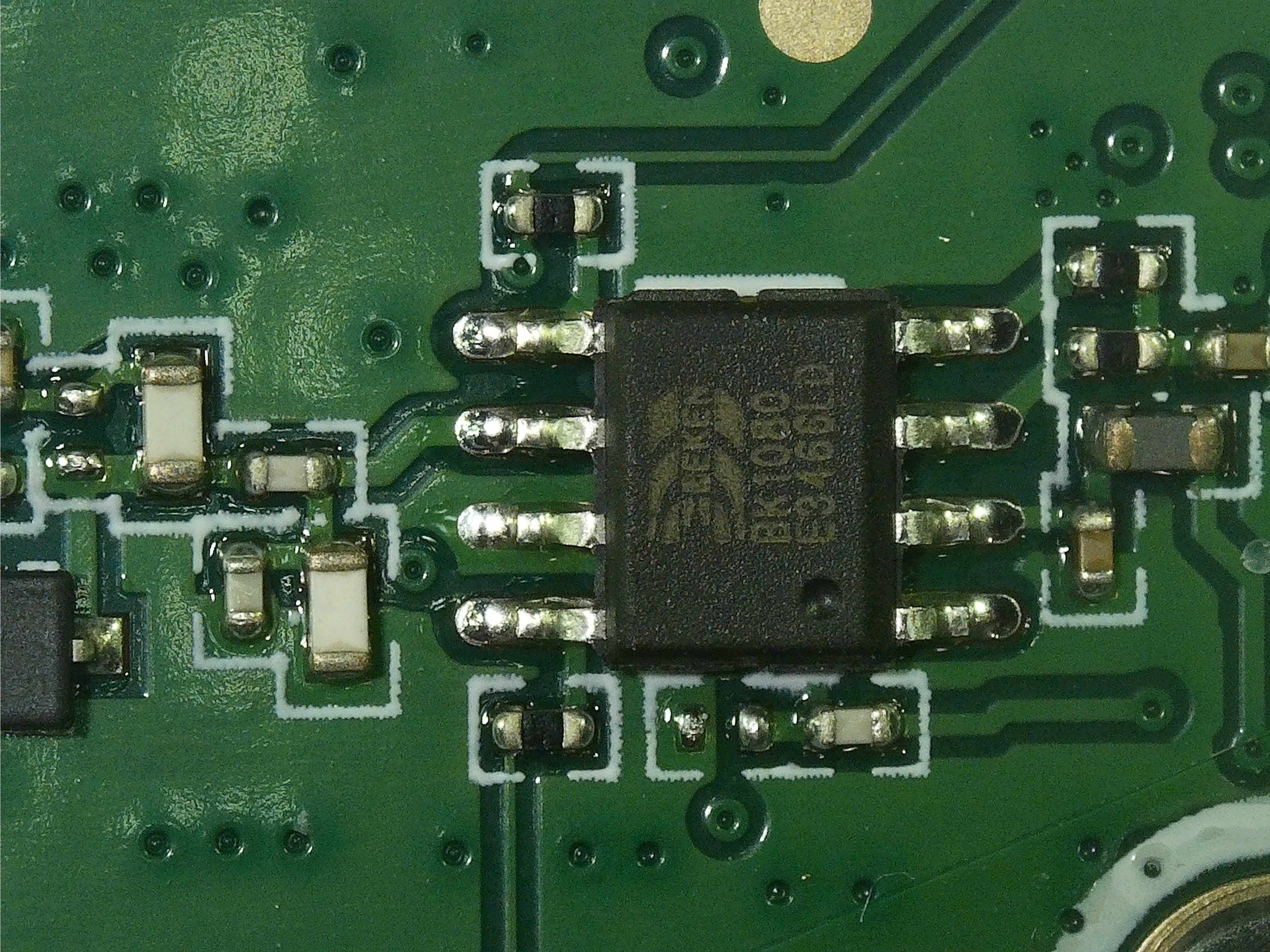


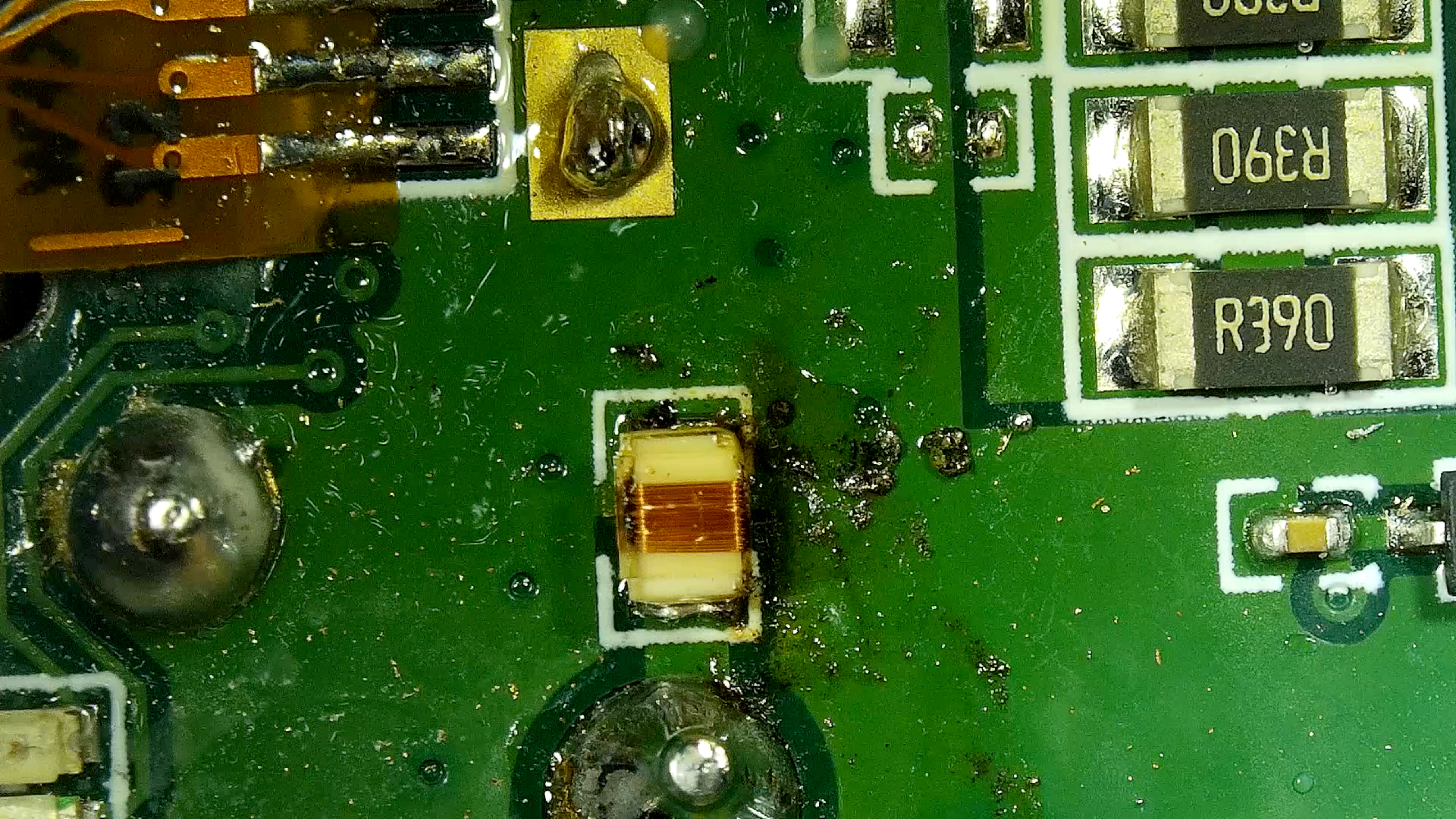


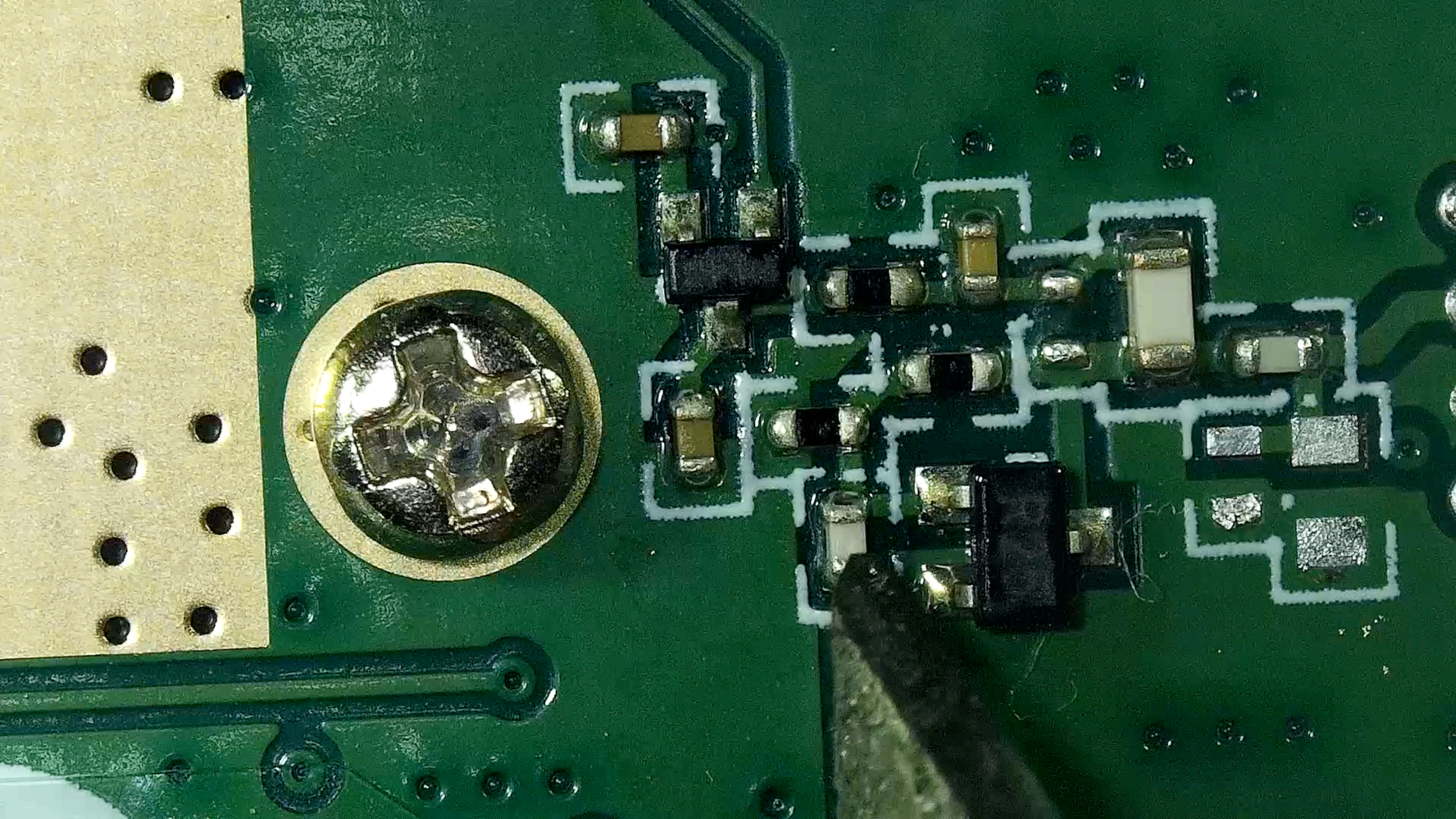


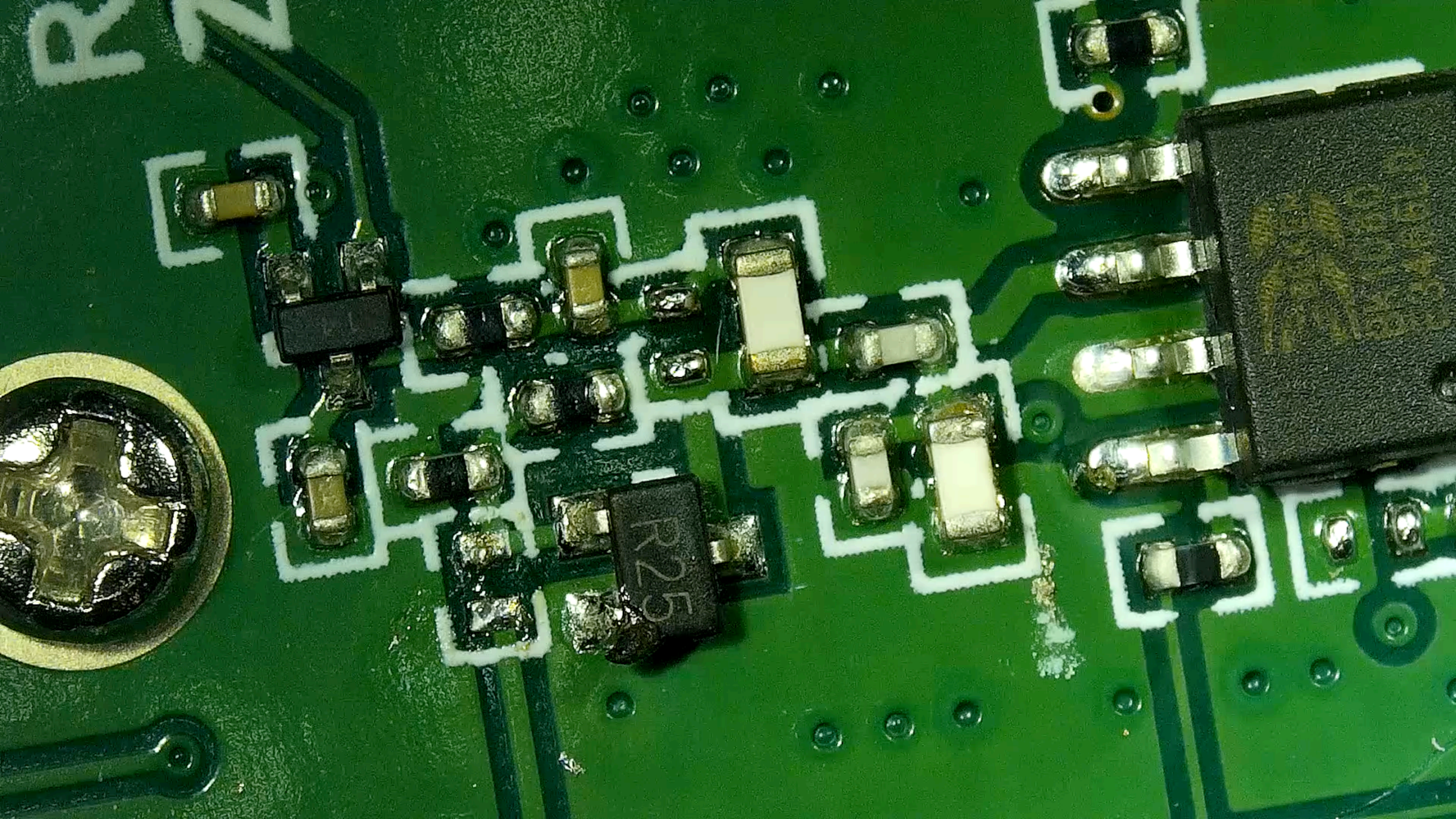


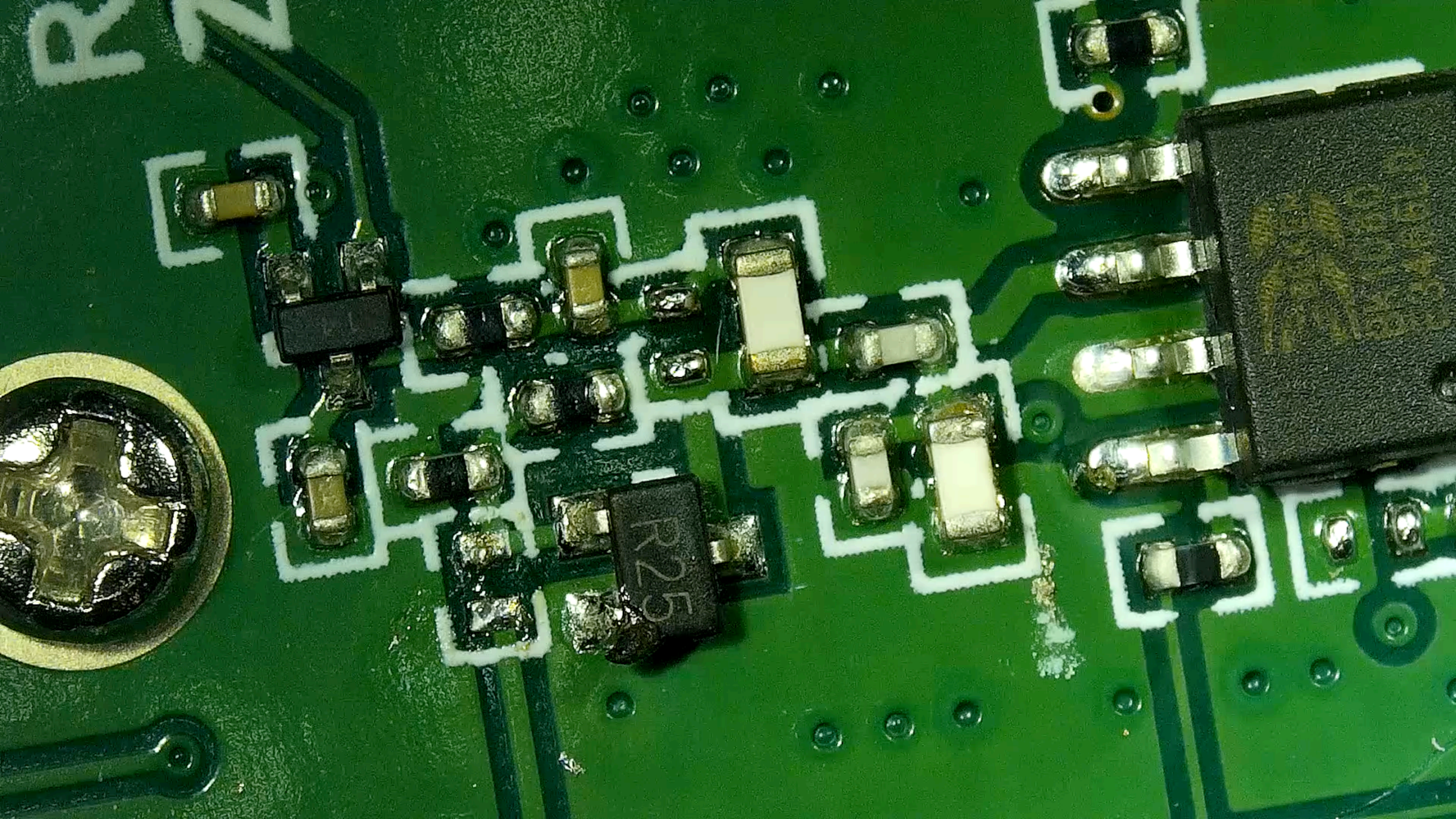


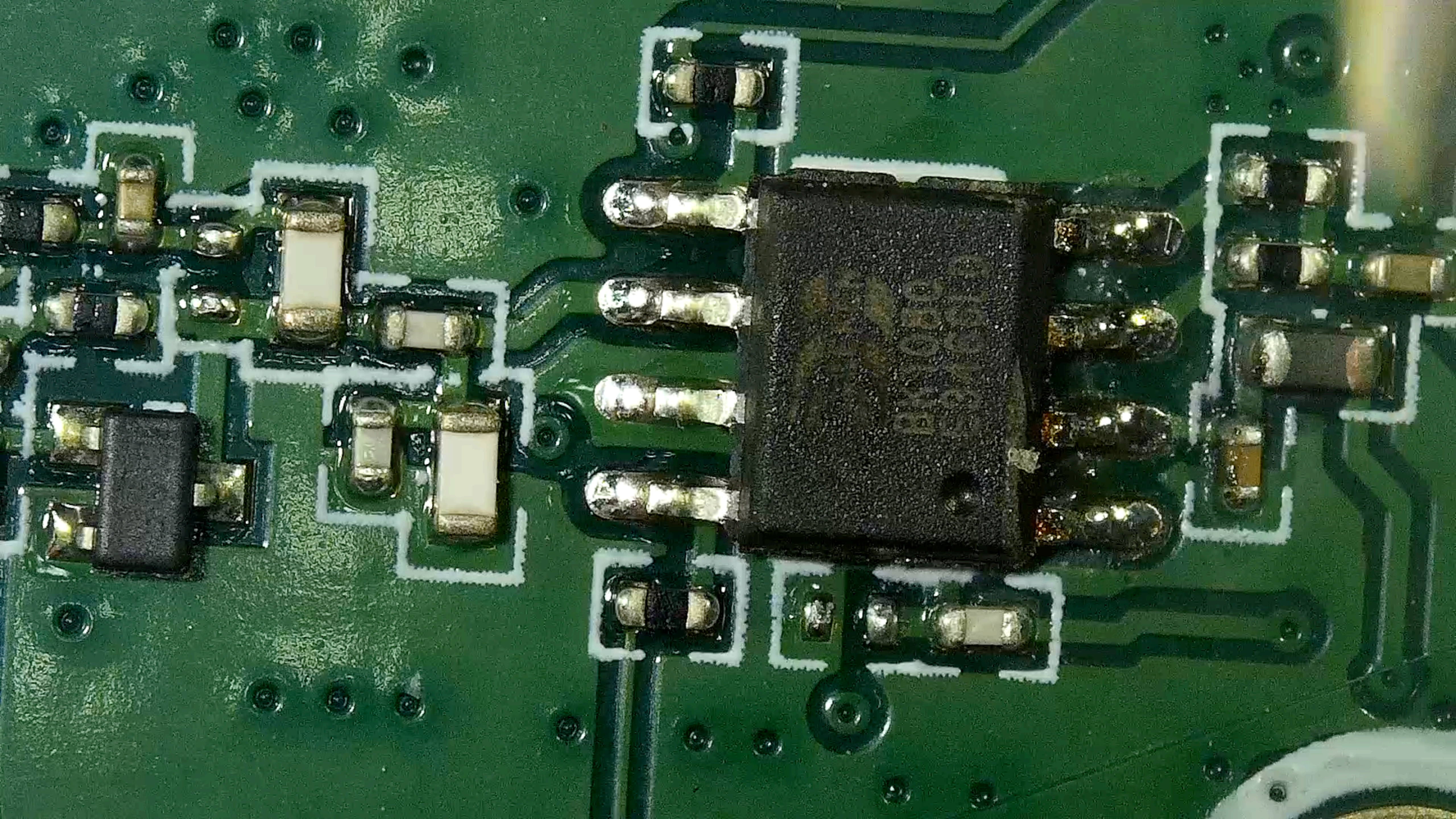


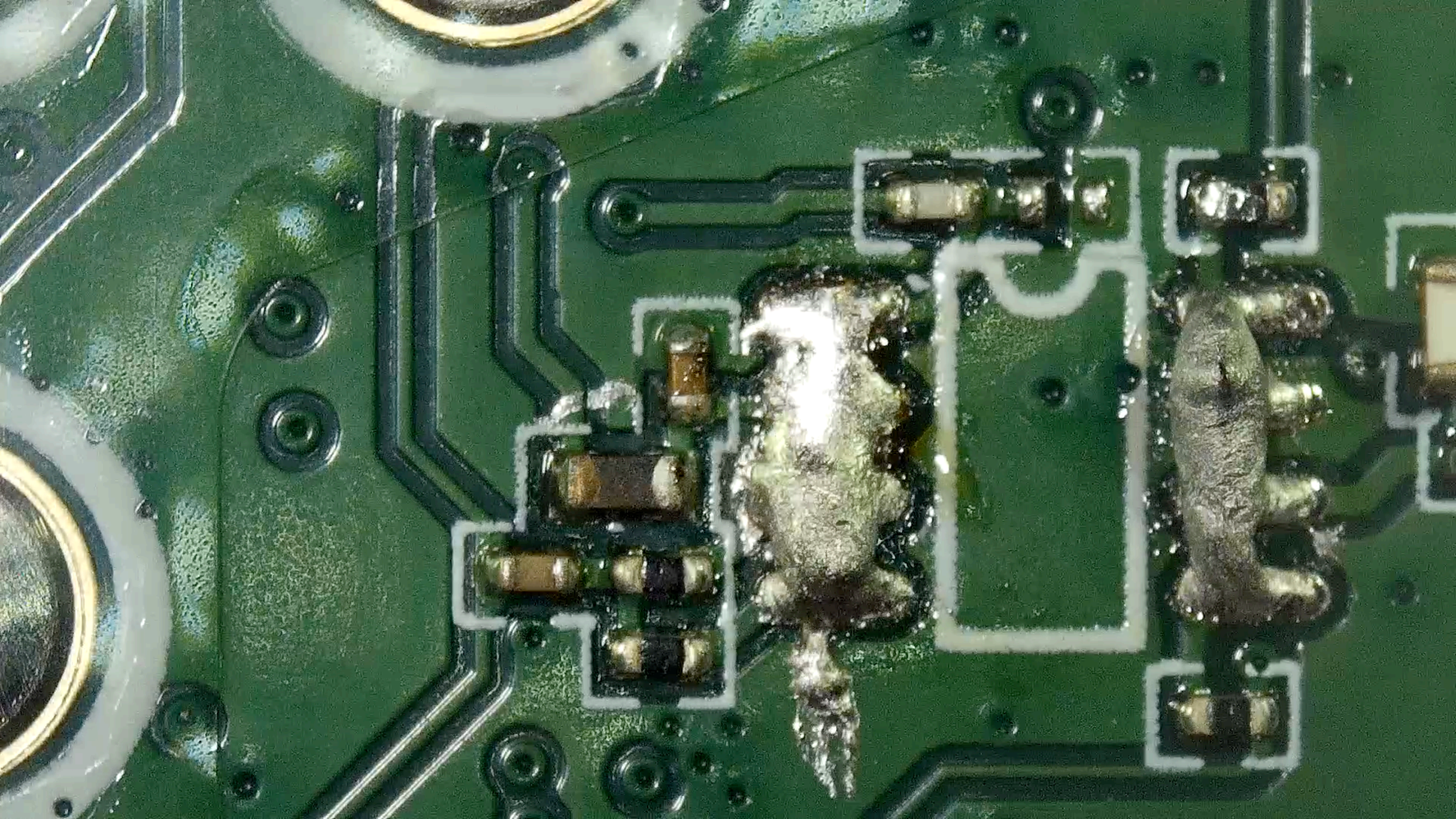


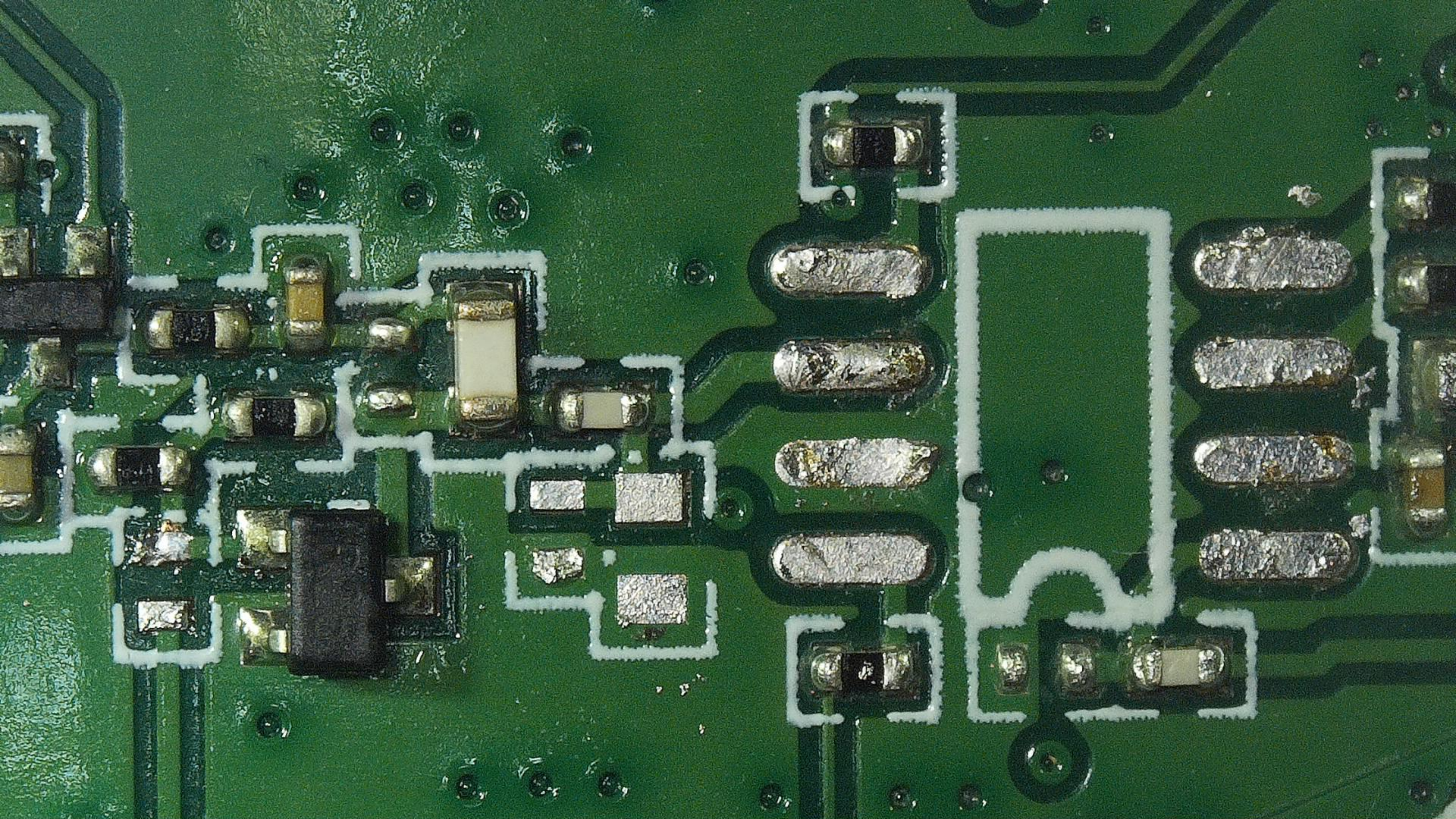


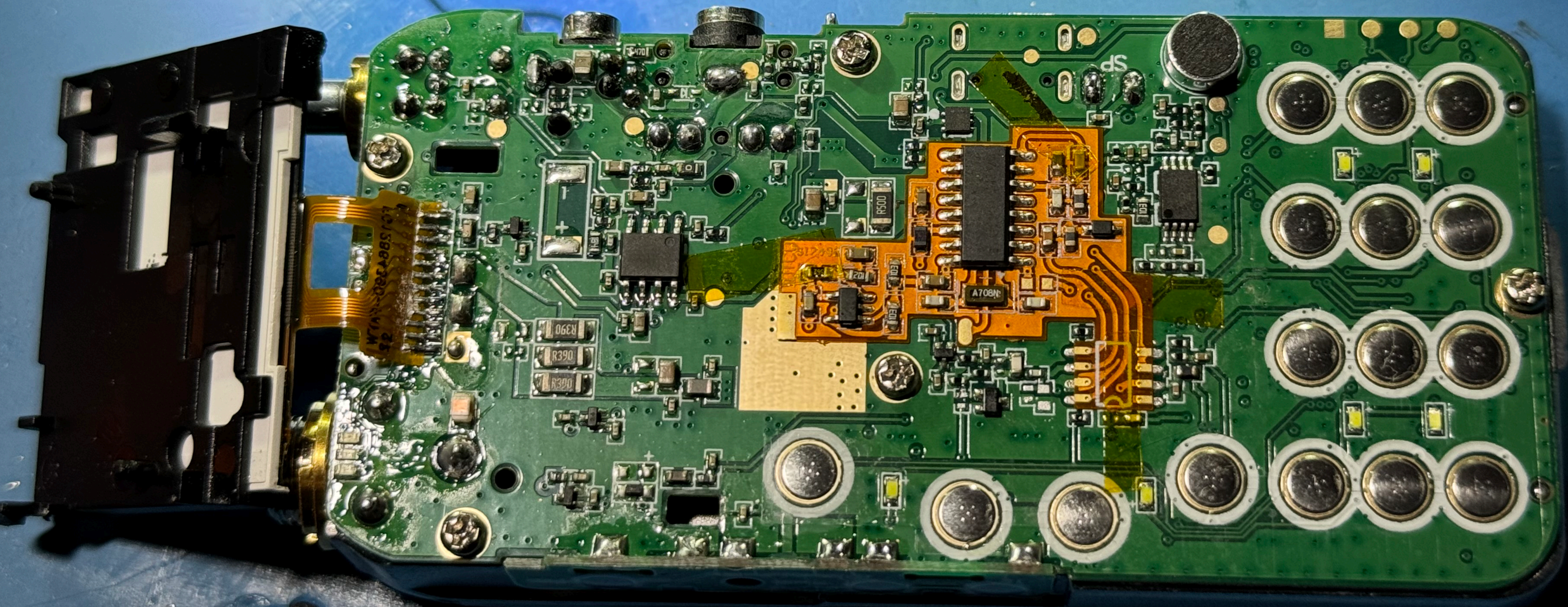


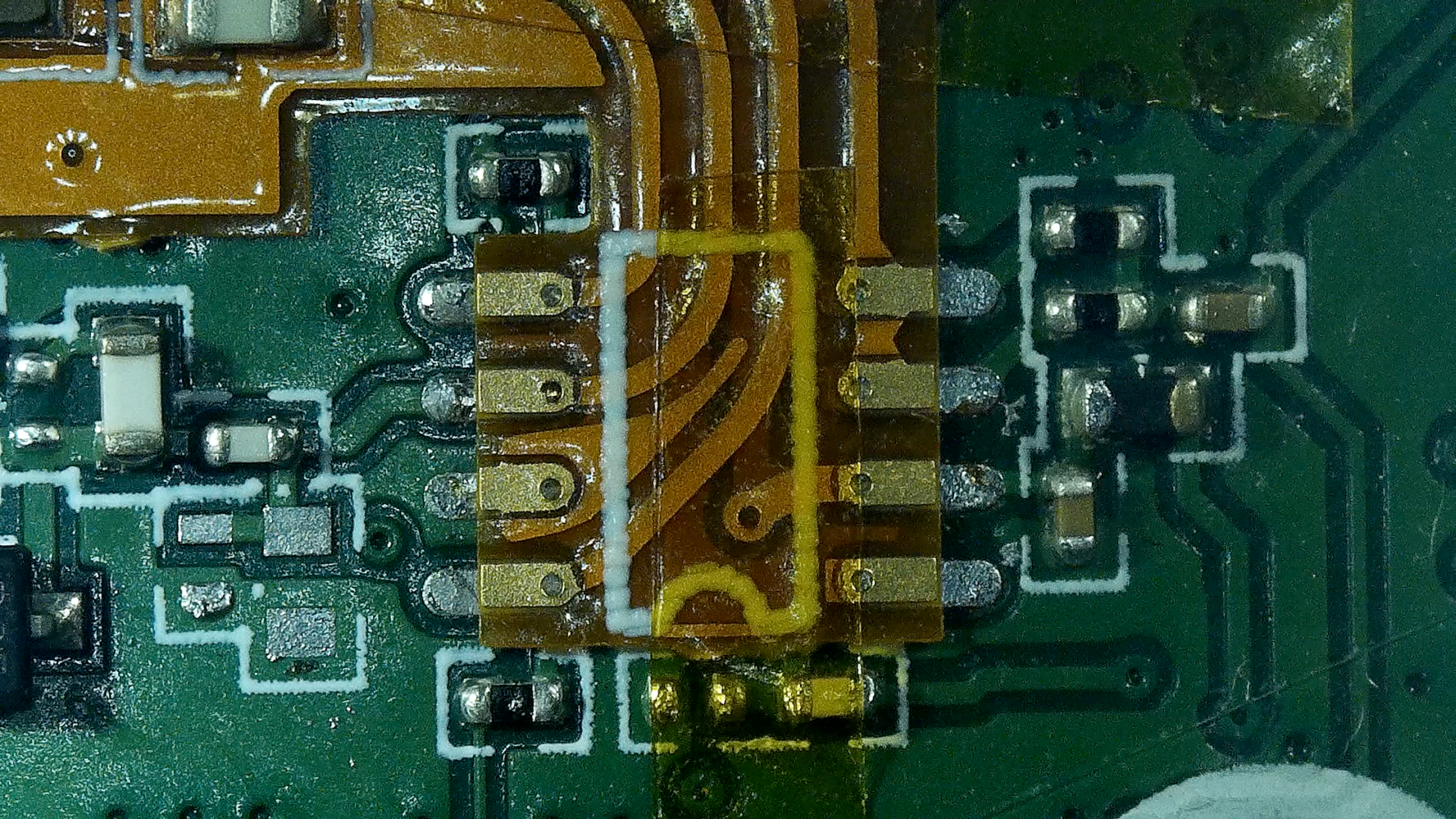


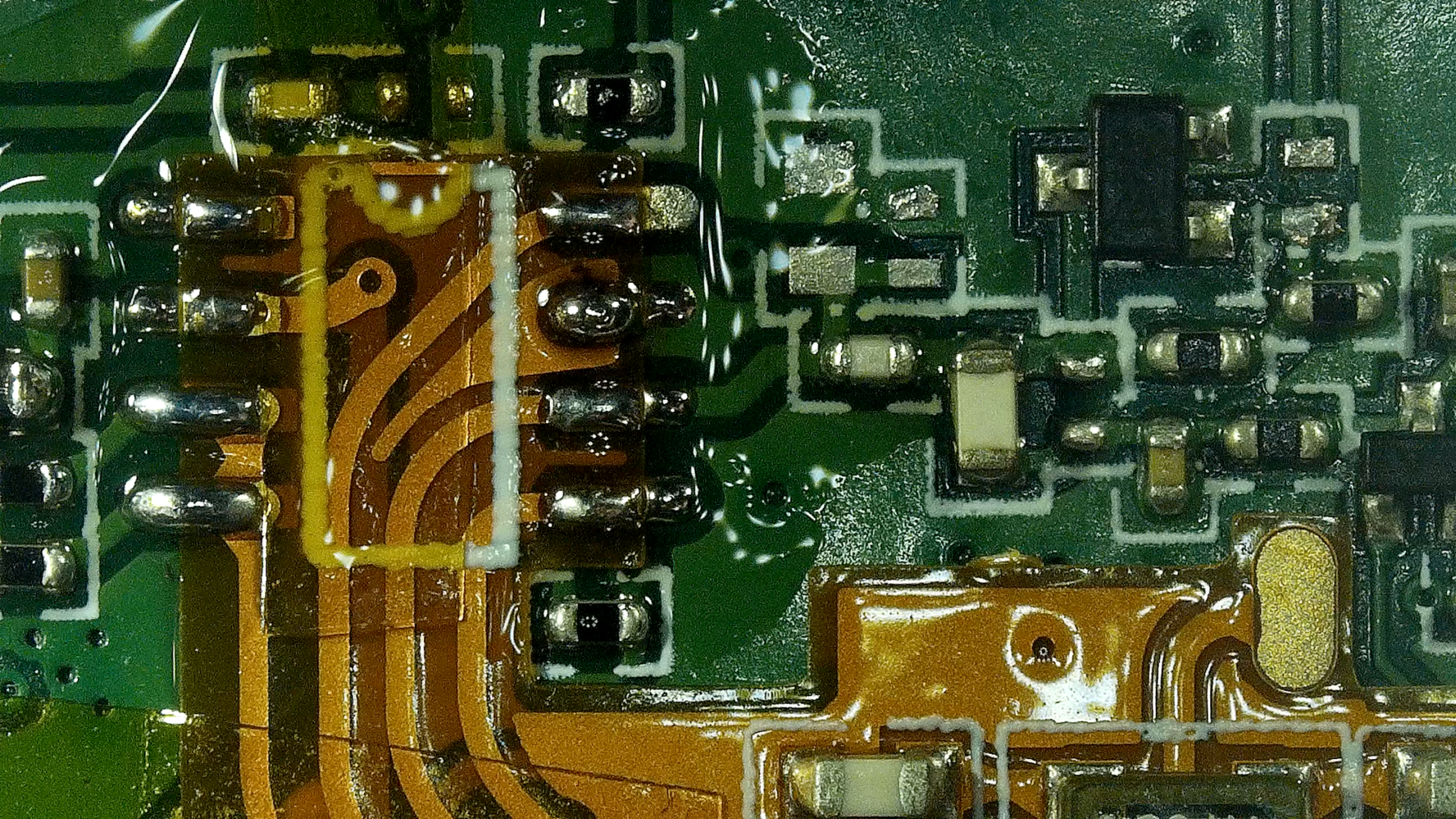


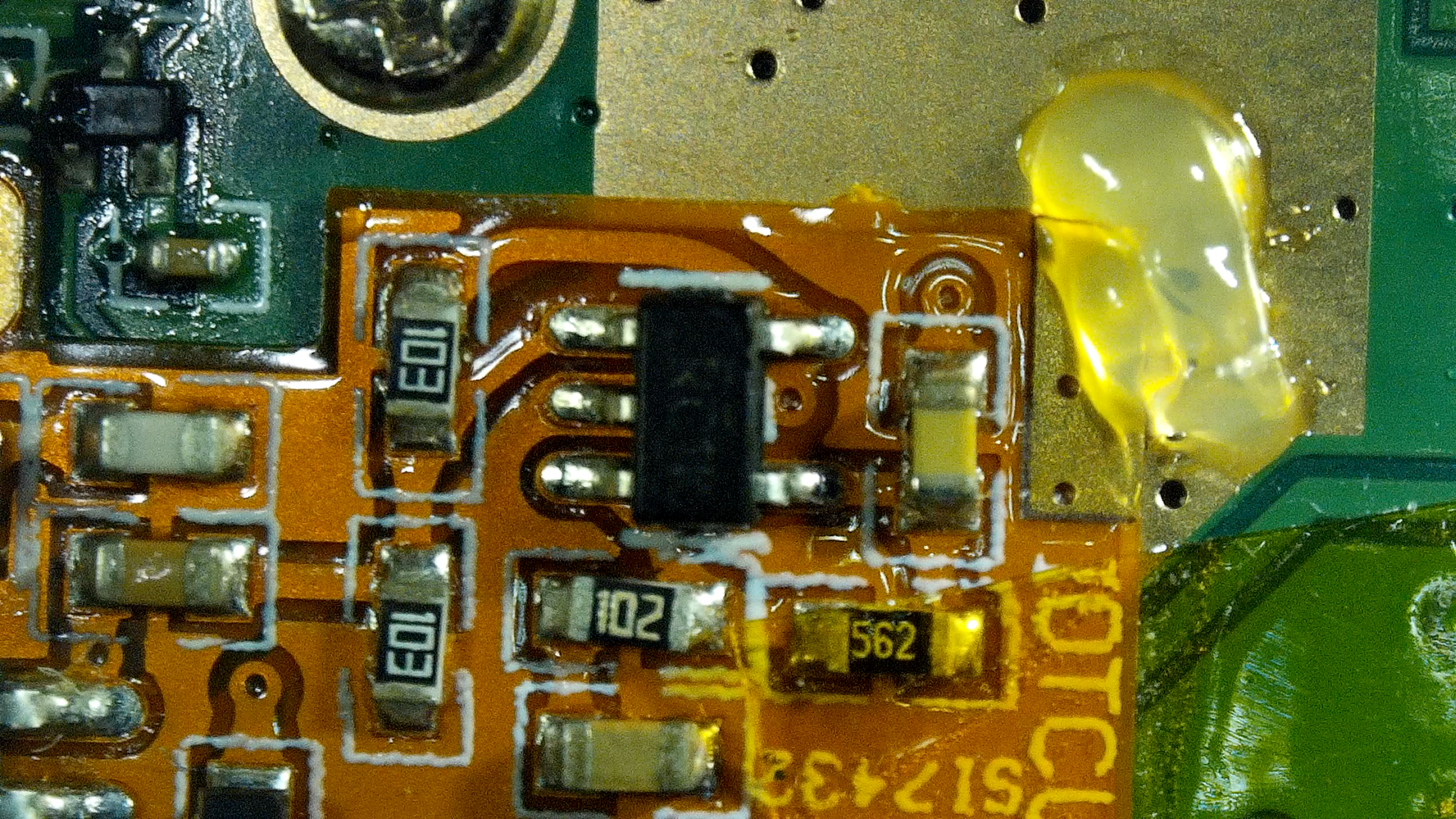












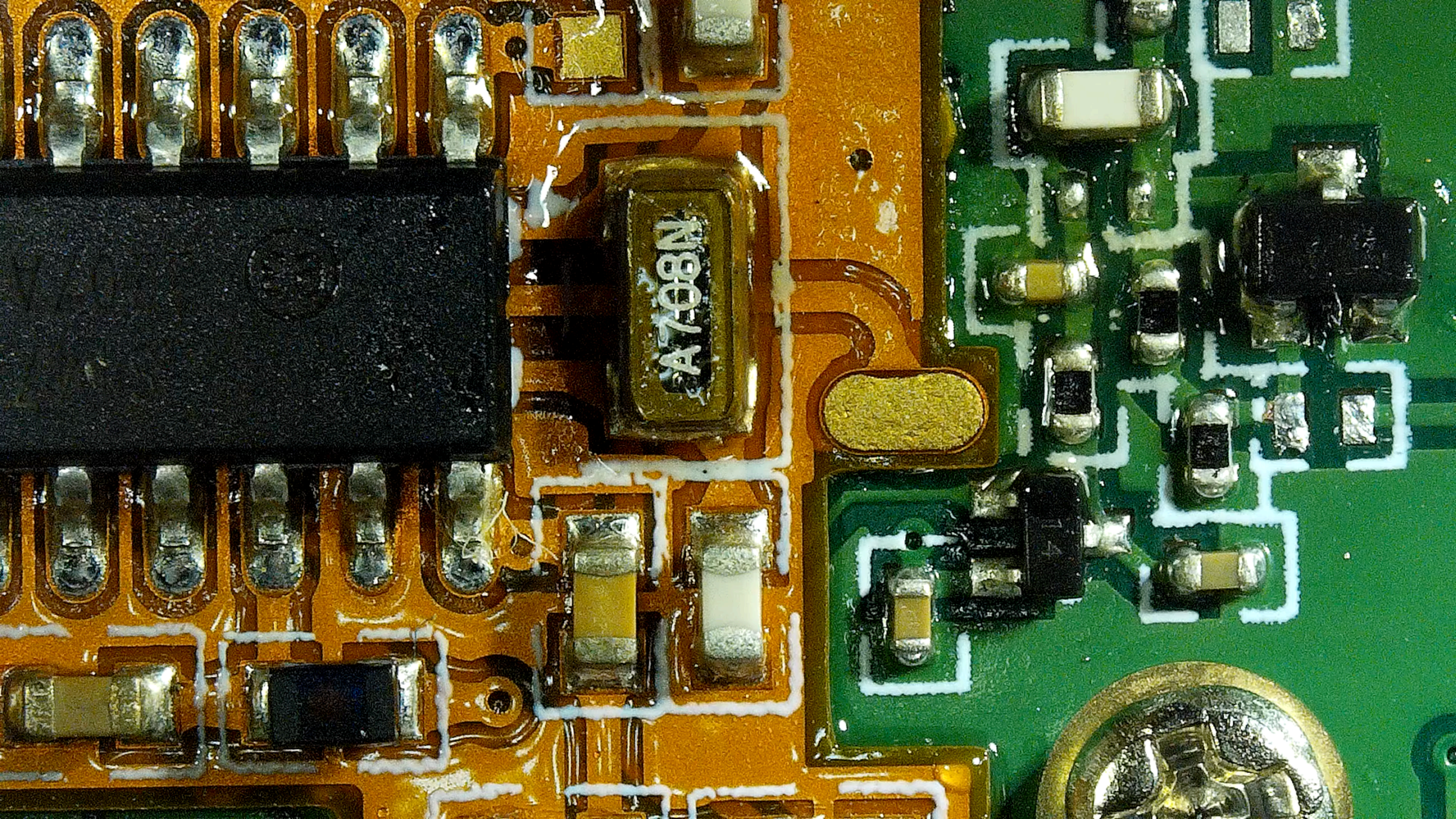
CS12432
T0T0C

562

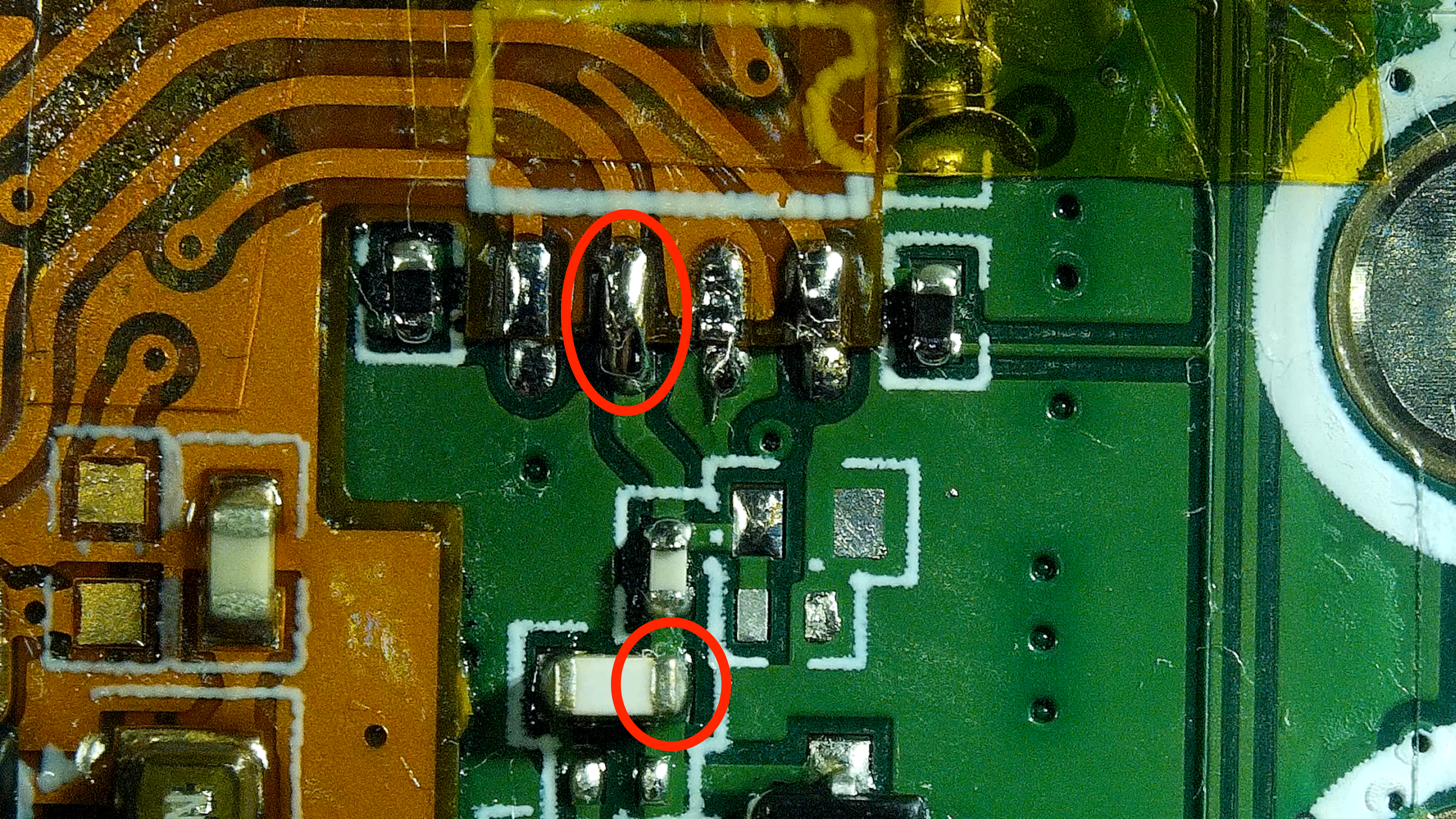
102

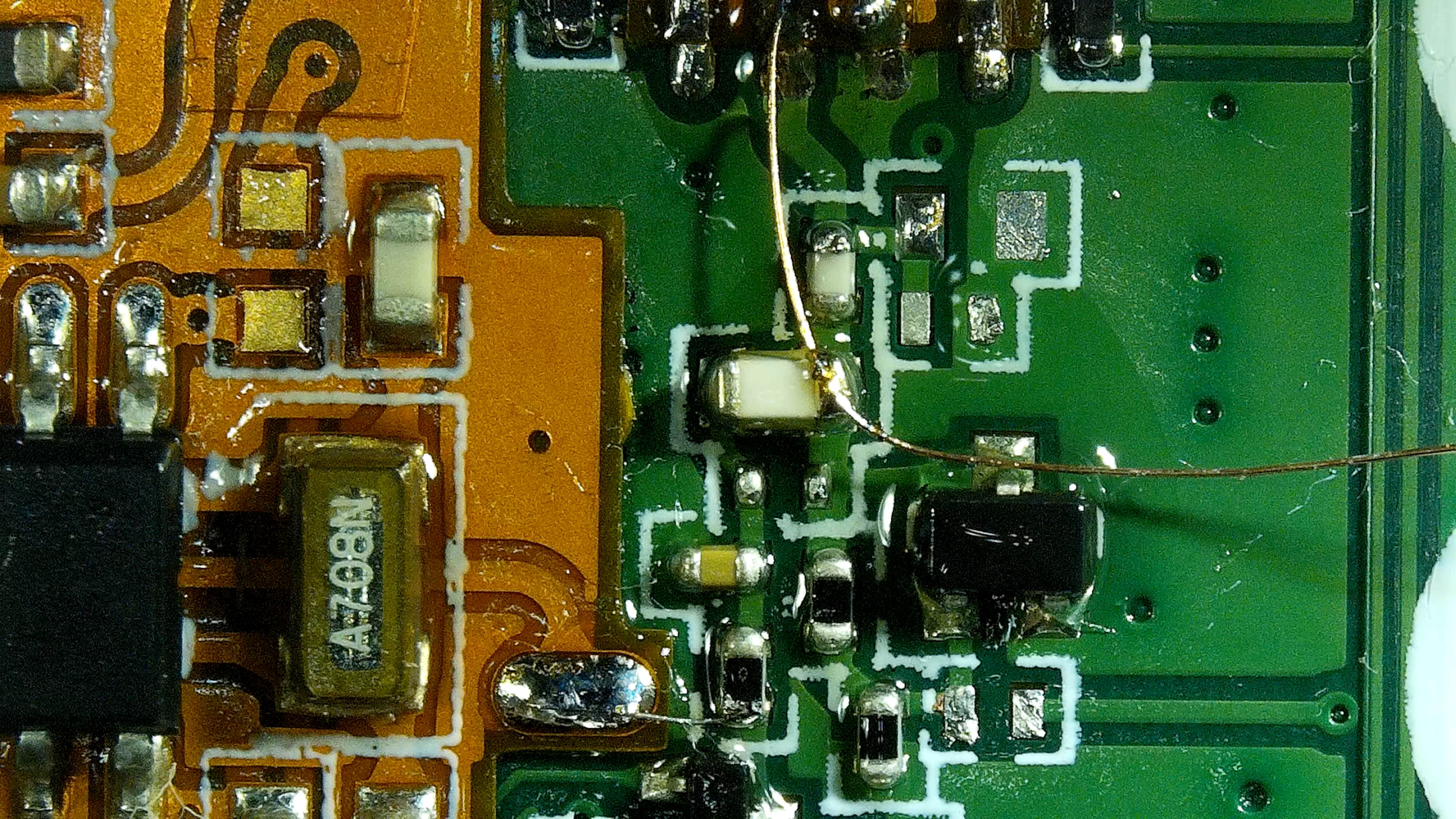
103

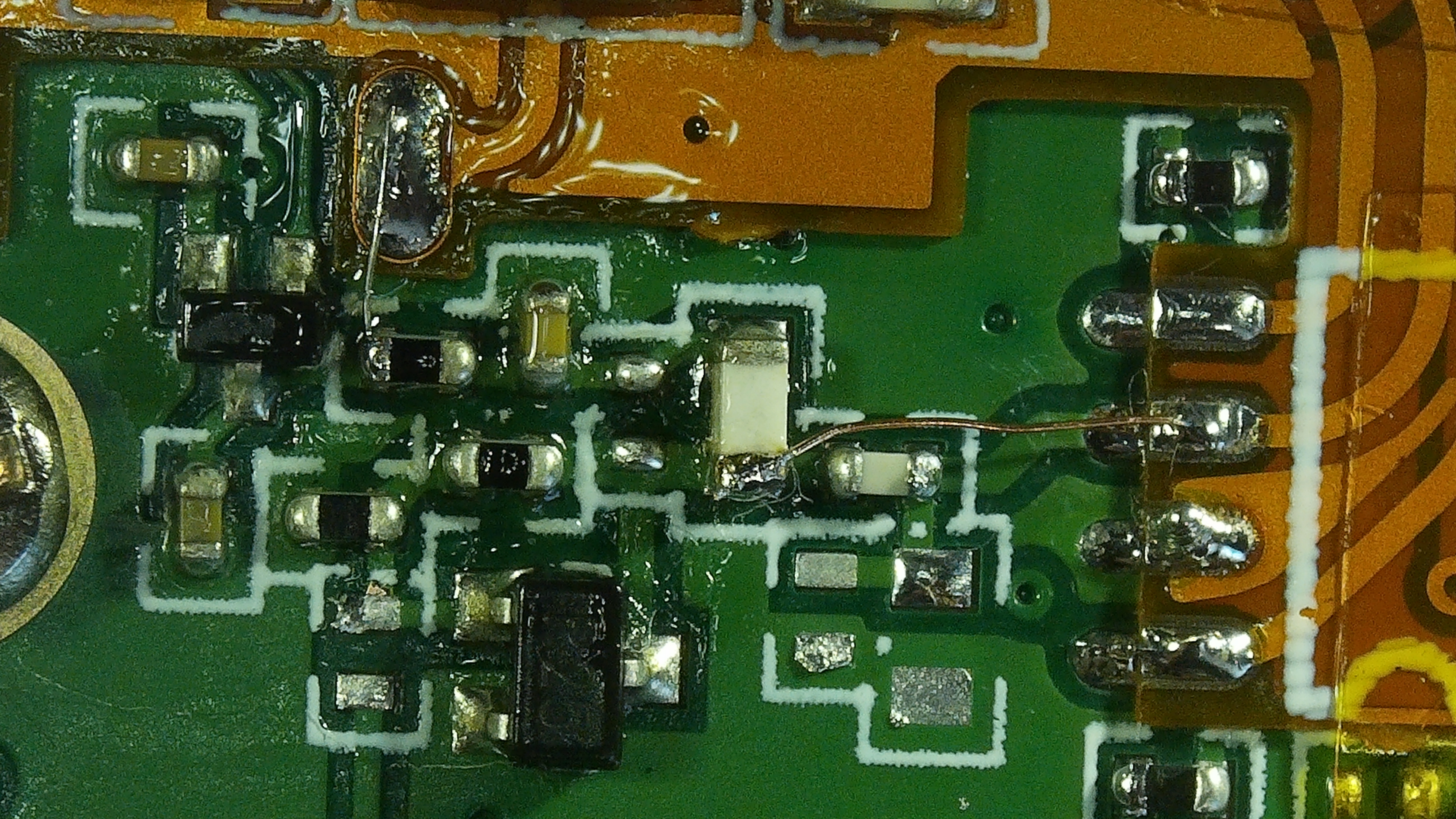
103

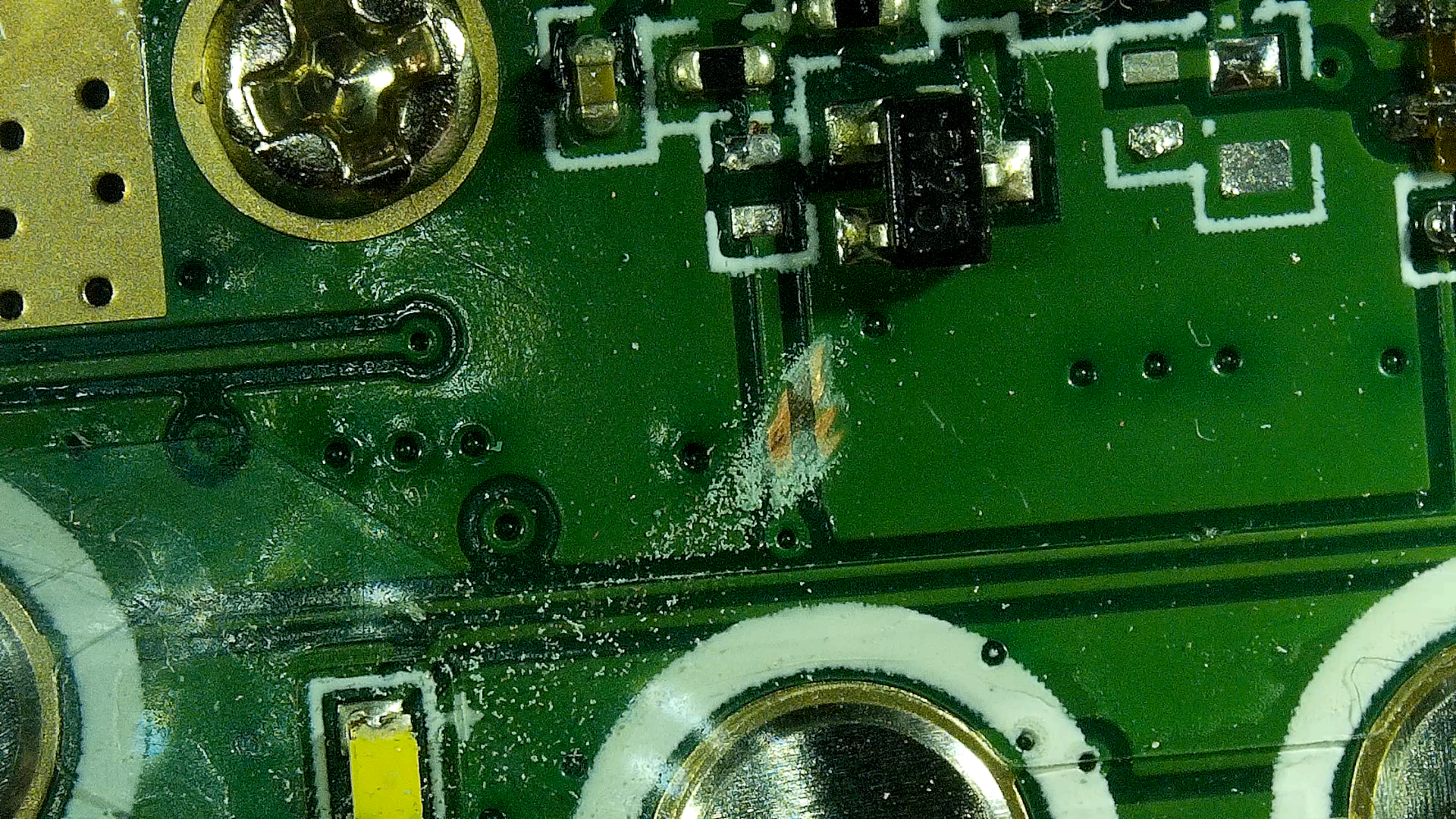


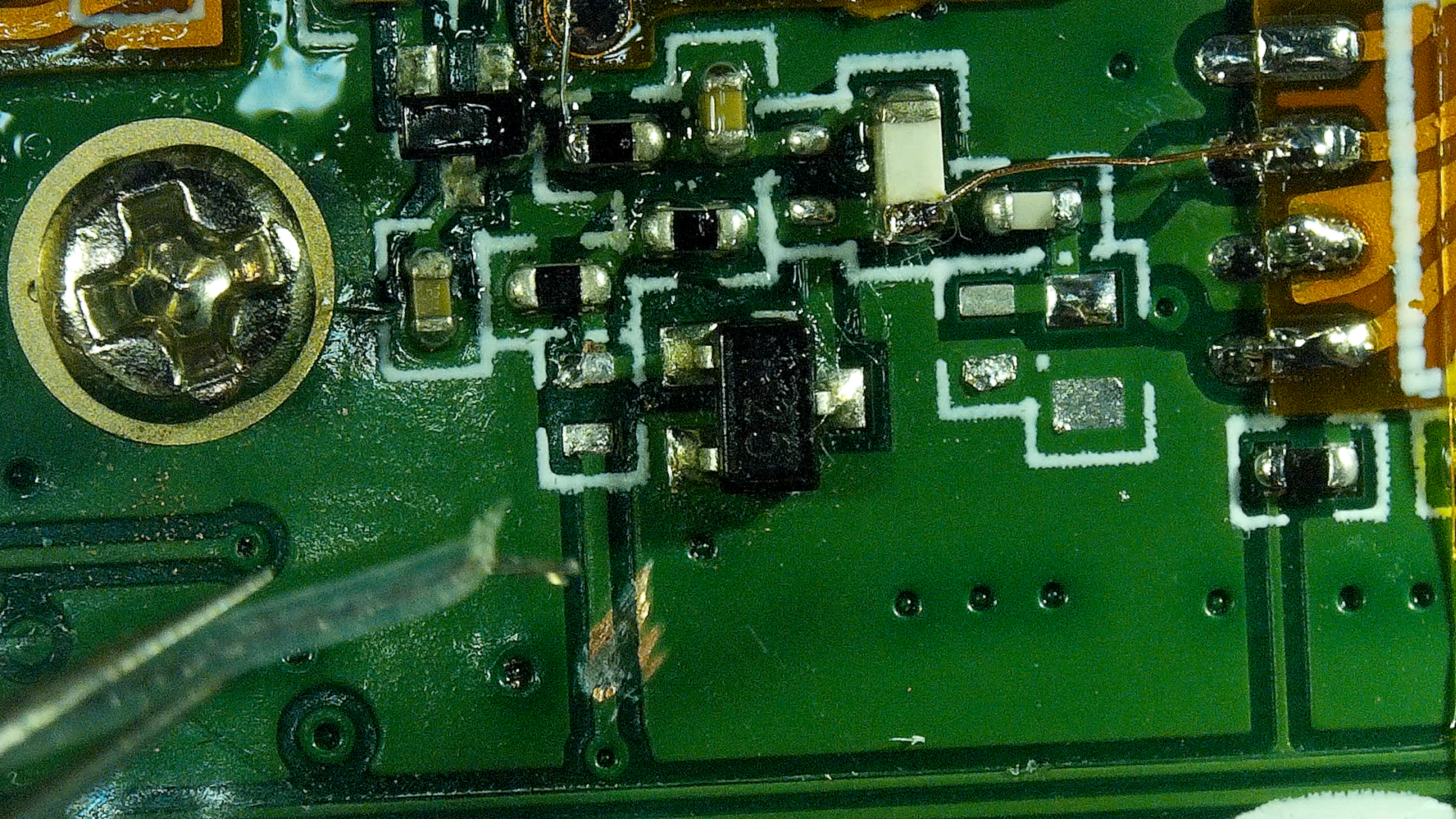
A708N

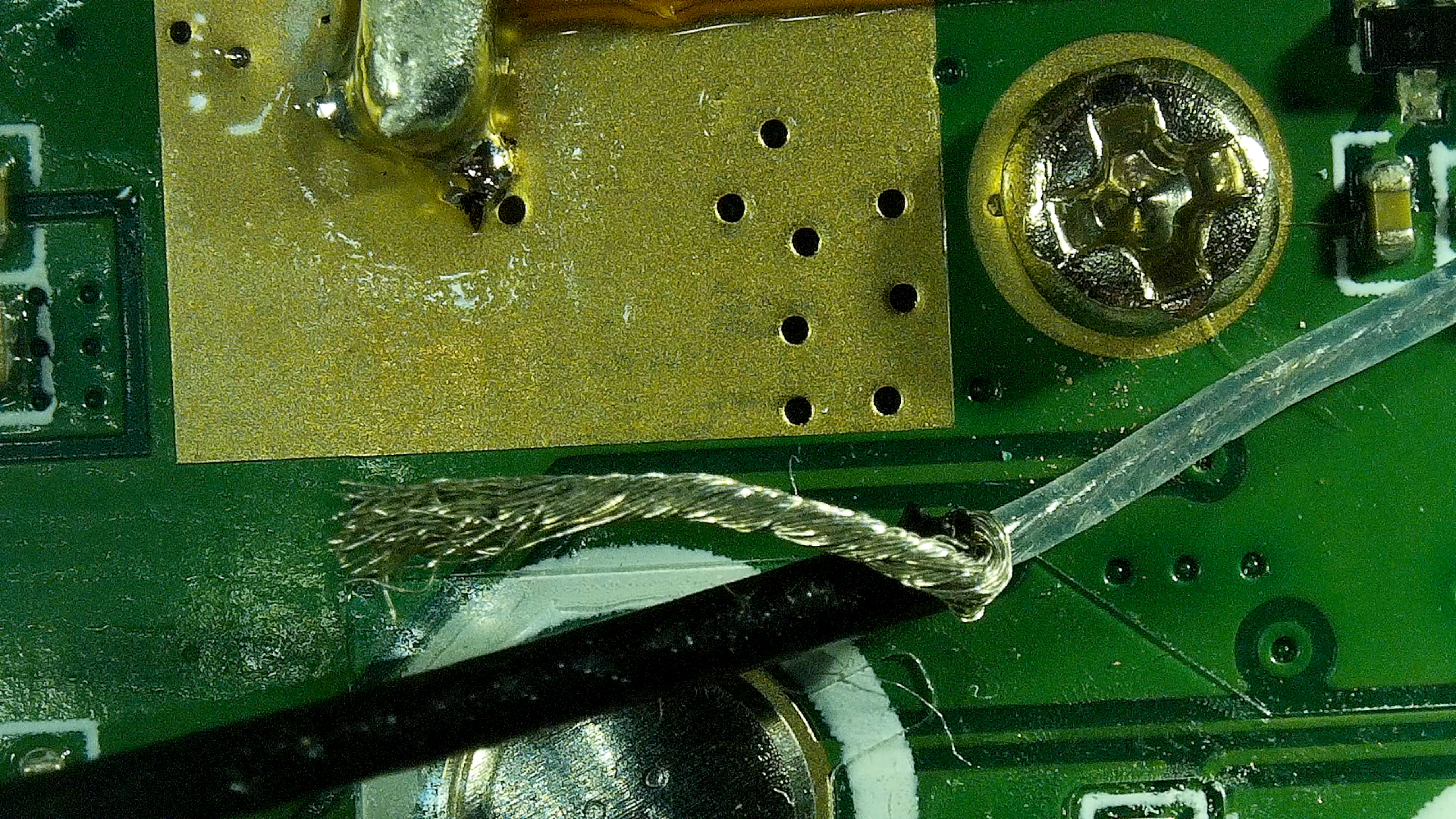
















YAESU

HF/VHF/UHF ALL MODE TRANSCEIVER FT-991A



F
M-LIST

MENU
SETUP

BAND

MODE

A=B

A/B

RCL/STO

TUNE

C.S

TXW

FAST

LOCK

CLAR

V/M

late

Thank You!

Stay in Touch

How to stay in touch with me

- QRZ - <https://www.qrz.com/db/K4CHN>
- Email: K4CHN@arrrl.net
- Github: <https://www.github.com/jmarler>
 - <https://github.com/jmarler/DefCon32HRVPresentations>
 - Contains all links from presentation & presentation itself
 - Scan QR code to go straight here ↗

