



## Riscufefe #5 badge repo

Some howto's below.

## The GLITCHIFIER9000 in a nutshell

### A Factual incorrect primer on Fault injection

- Invented by the CIA as ~~torture~~ Enhanced Interrogation for humans
  - Humans like Oxygen  $\Leftrightarrow$  Chips like Electricity

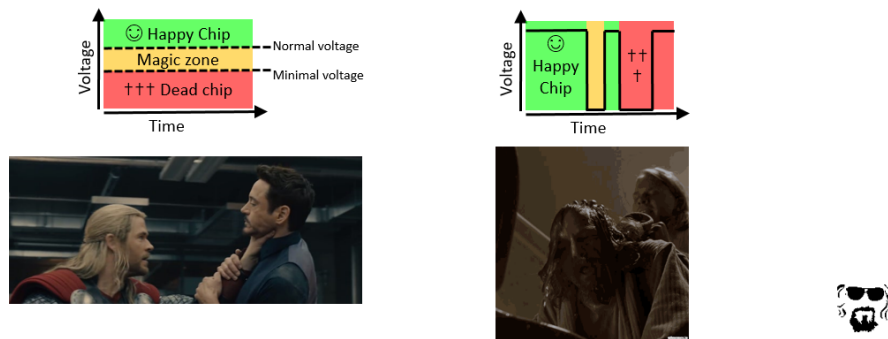


Figure 1: What is voltage glitching?

- Crowbar!

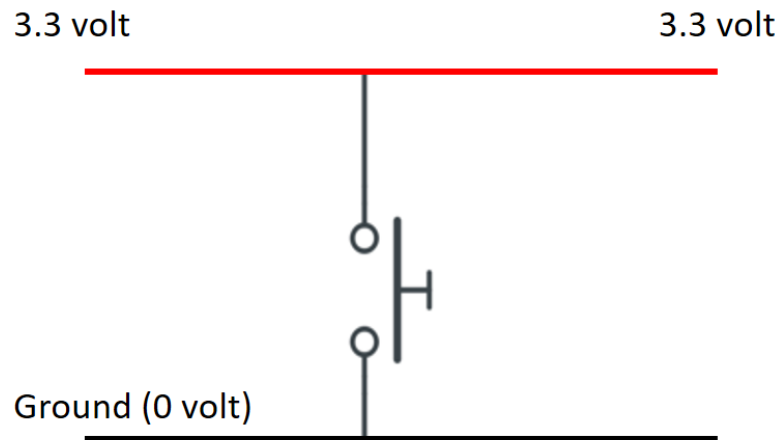


Figure 2: Normal operation

- Crowbar!

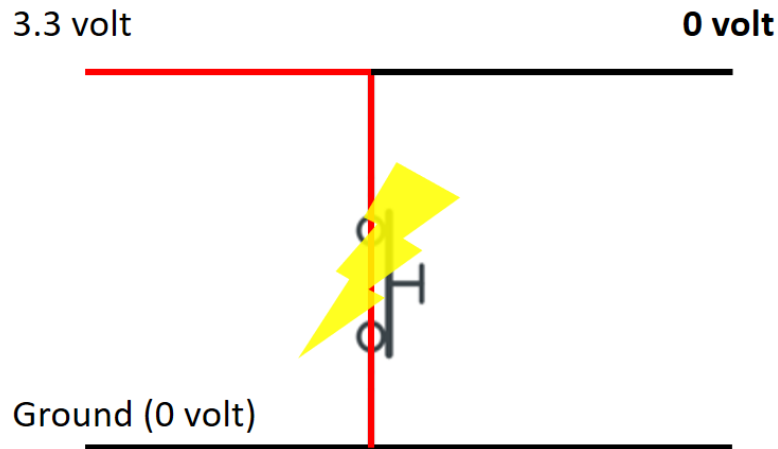


Figure 3: While glitching

Check out the schematics [in this repo](#) for more information!

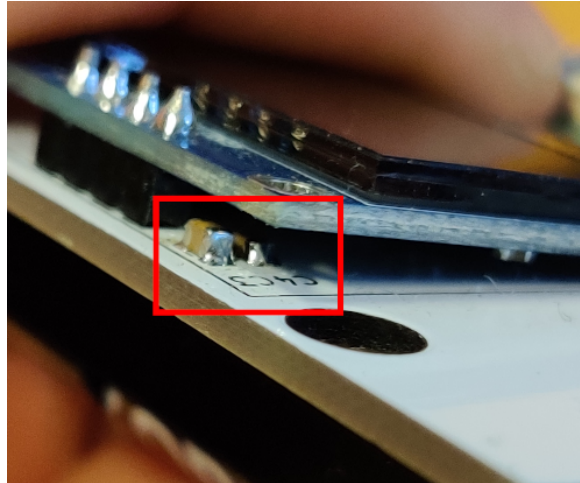
NOTE: The trigger input is currently set to the button for demo purposes, the use a different pin you have to modify [this line](#).

## Hardware DIY instructions

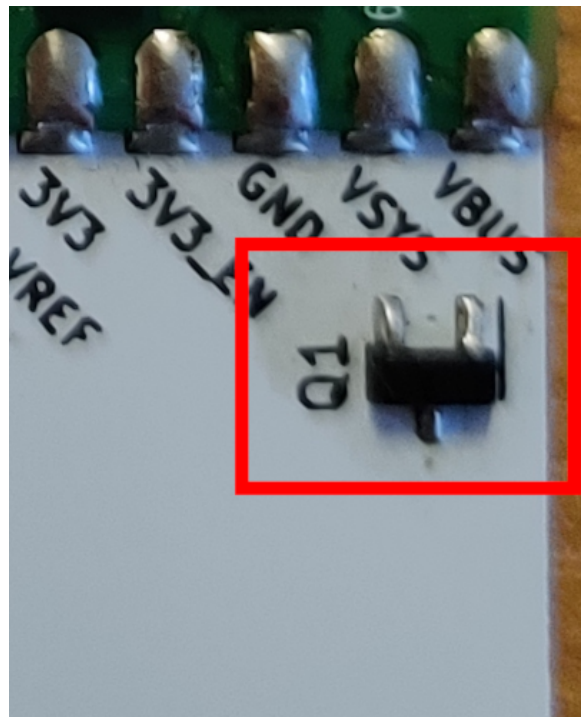
### Minimal badge functionality

To get minimal badge functionality:

1. Solder C3, C4



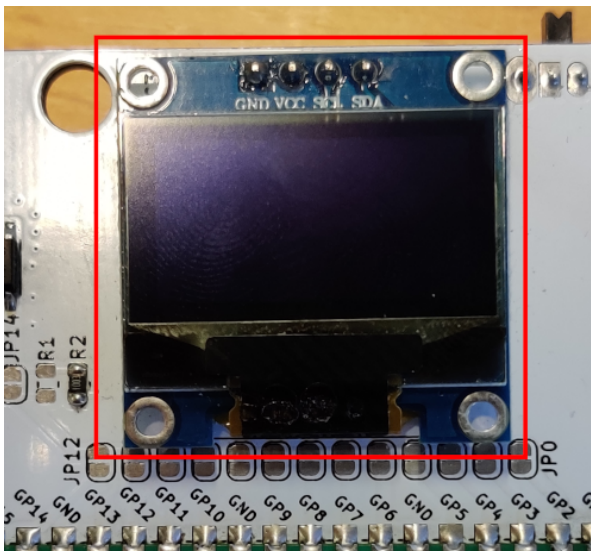
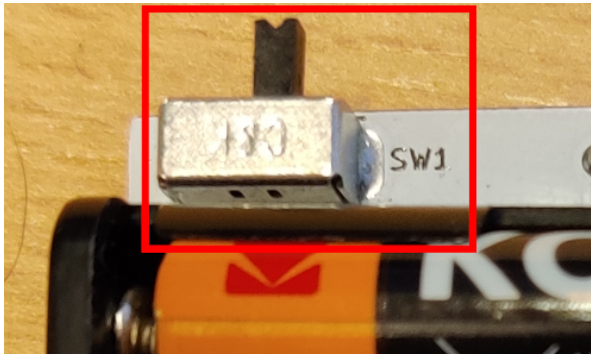
2. To protect your PICO from having battery and USB power at the same time, solder Q1:

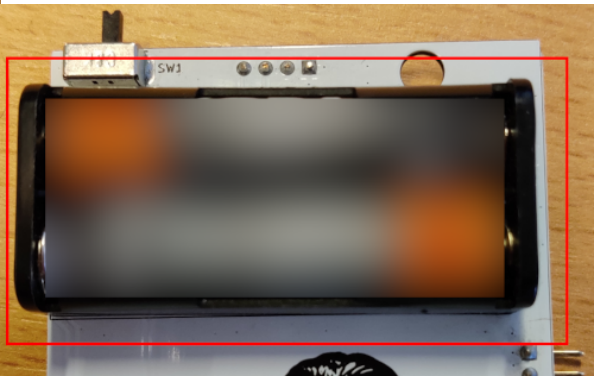


3. To be able to switch off the batteries, solder SW1:

4. Attach the screen to the front:

5. Attach the AAA battery holder to the back:





6. Insert 2xAAA batteries:

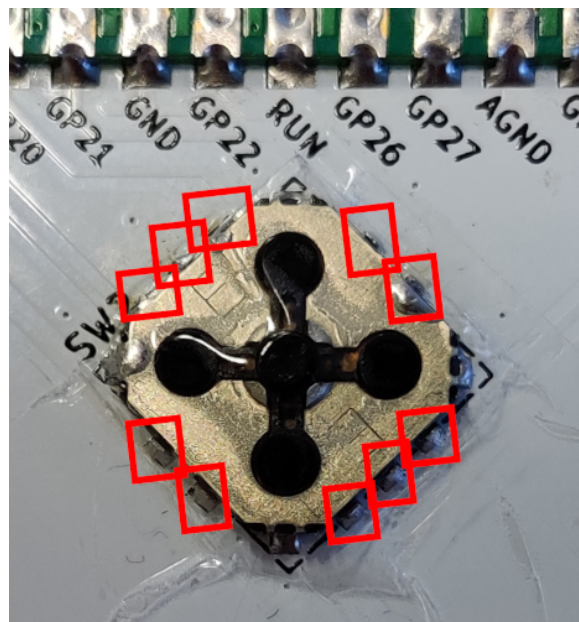


You should now be able to see stuff on the screen, and you can interact over USB / serial.

## Button controls

To control the badge with the button:

1. Solder the 10 (3, 2, 3, 2) points of the button at SW1:



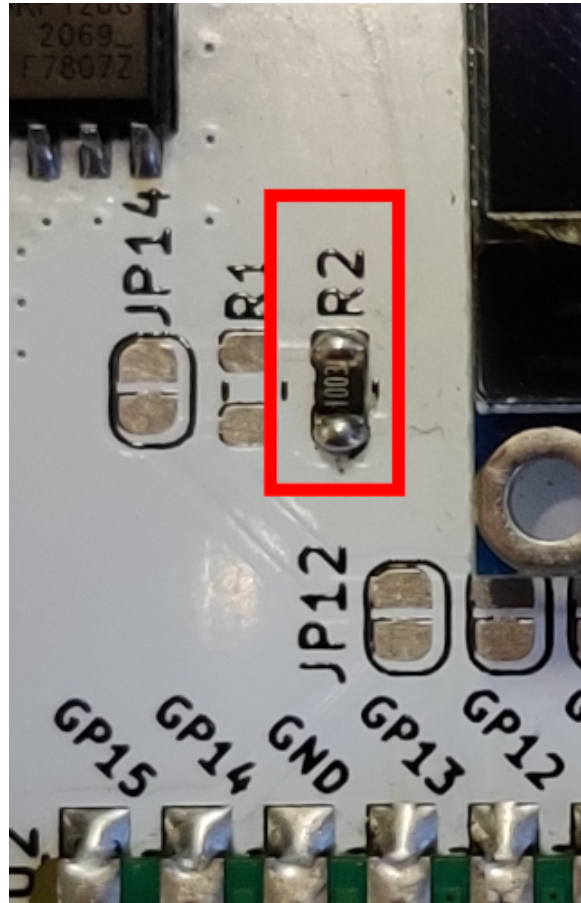
You should now be able to use the button.



## GLITCHIFIER9000

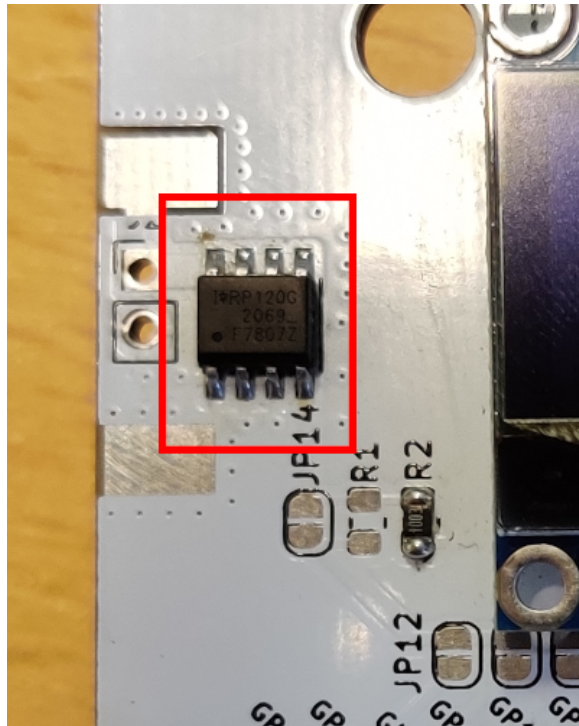
To add GLITCHIFIER9000 functionality:

1. Solder R2



2. Solder unlabeled SOT8 MOSFET:





Ready to glitch!

## Talk to the badge over USB

1. Plug in micro-usb cable.

Ready to talk!

## On Windows

1. Install a program to talk serial, like [putty](#)

**Download PuTTY: latest release (0.78)**

[Home](#) | [FAQ](#) | [Feedback](#) | [Licence](#) | [Updates](#) | [Mirrors](#) | [Keys](#) | [Links](#) | [Team](#)  
[Download](#) - [Stable](#) - [Snapshot](#) | [Docs](#) | [Changes](#) | [Wishlist](#)

This page contains download links for the latest released version of PuTTY. Currently this is 0.78, released on 2022-10-29.

When new releases come out, this page will update to contain the latest, so this is a good page to bookmark or link to. Alternatively, here is a [permanent link to the 0.78 release](#).

Release versions of PuTTY are versions we think are reasonably likely to work well. However, they are often not the most up-to-date version of the code available. If you have a problem with this release, then it might be worth trying out the [development snapshots](#), to see if the problem has already been fixed in those versions.

**Package files**

You probably want one of these. They include versions of all the PuTTY utilities (except the new and slightly experimental Windows pterm).

(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

We also publish the latest PuTTY installers for all Windows architectures as a free-of-charge download at the [Microsoft Store](#); they usually take a few days to appear there after we release them.

**MSI ("Windows Installer")**

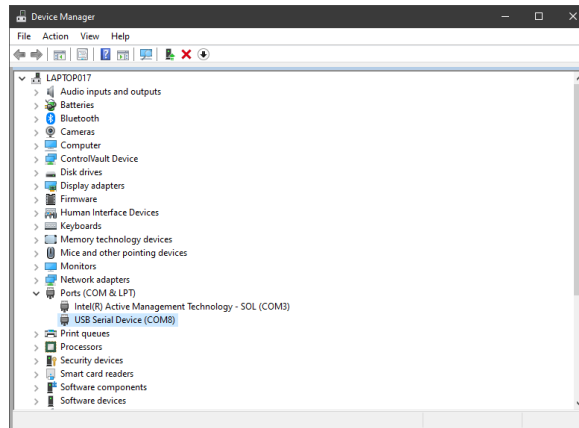
64-bit x86:	<a href="#">putty-64bit-0.78-installer.msi</a>	<a href="#">(signature)</a>
64-bit Arm:	<a href="#">putty-arm64-0.78-installer.msi</a>	<a href="#">(signature)</a>
32-bit x86:	<a href="#">putty-0.78-installer.msi</a>	<a href="#">(signature)</a>

**Unix source archive**

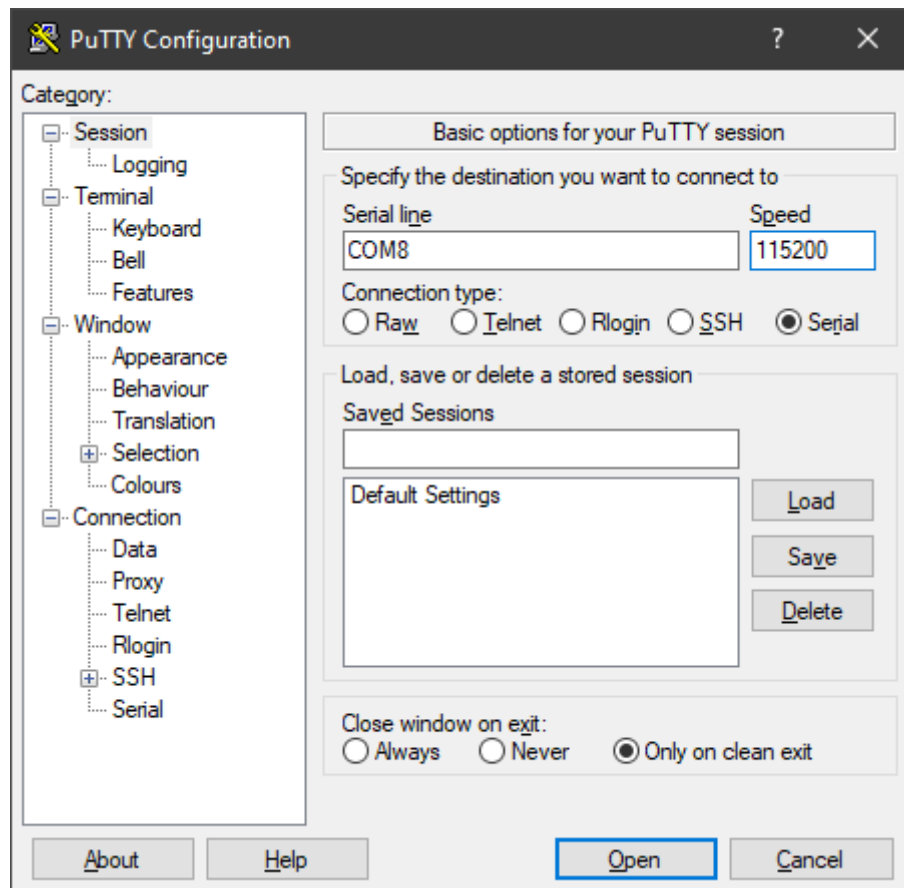
.tar.gz:	<a href="#">putty-0.78.tar.gz</a>	<a href="#">(signature)</a>
----------	-----------------------------------	-----------------------------

**Alternative binary files**

2. Find the COM port that pops up when you plug in the USB cable in device manager



3. Set up that COM port with speed 115200



4. Type some buttons, see what happens (also try CTRL+C and CTRL+D)



To do stuff over serial, connect with `SERIALPORT`, baudrate 115200.

## Misc

To build this document in to various formats:

```
quarto render README.qmd --to pdf && \  
quarto render README.qmd --to html && \  
quarto render README.qmd --to docx && \  
quarto render README.qmd --to gfm
```