SYNACKTIV

Cheap hardware hacking! mais à quel prix...

Bière Sécu

Bordeaux

04/04/2024

whoami

SYNACKTIV

- **Jean-Christophe Delaunay** (`prenom.nom@synacktiv.com`)
- **Pentest ~8 ans**
  - Windows (Active Directory)
  - Passcracking
- **RE/pwn depuis ~5 ans**
  - Software
  - Hardware

Contexte : audit produit

SYNACKTIV

- Accès physique
- Pas de docs
- Pas de code source
- Pas de *firmware*

Contexte : audit produit

SYNACKTIV

- **Oubli du client ?**
  - Oui → sauvé
  - Non :
    - ~~supplier~~
    - ~~bouder~~
    - se débrouiller → dump ?

État des lieux

SYNACKTIV

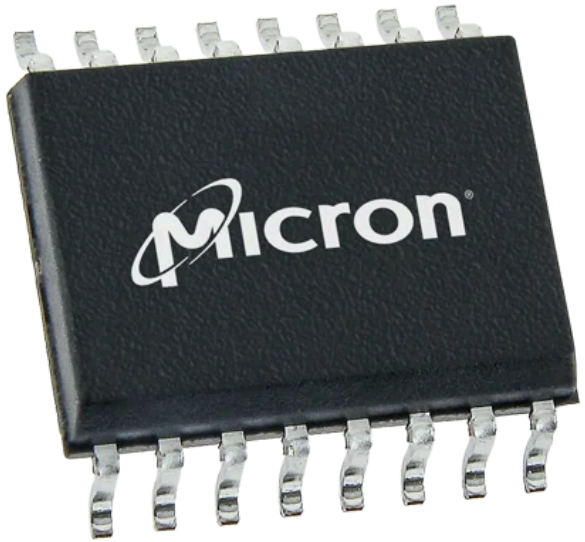
- **OuKanKomen ?**
  - *Microcontroller* (MCU) ? → on espère que non !
  - Flash externe ? → yes !

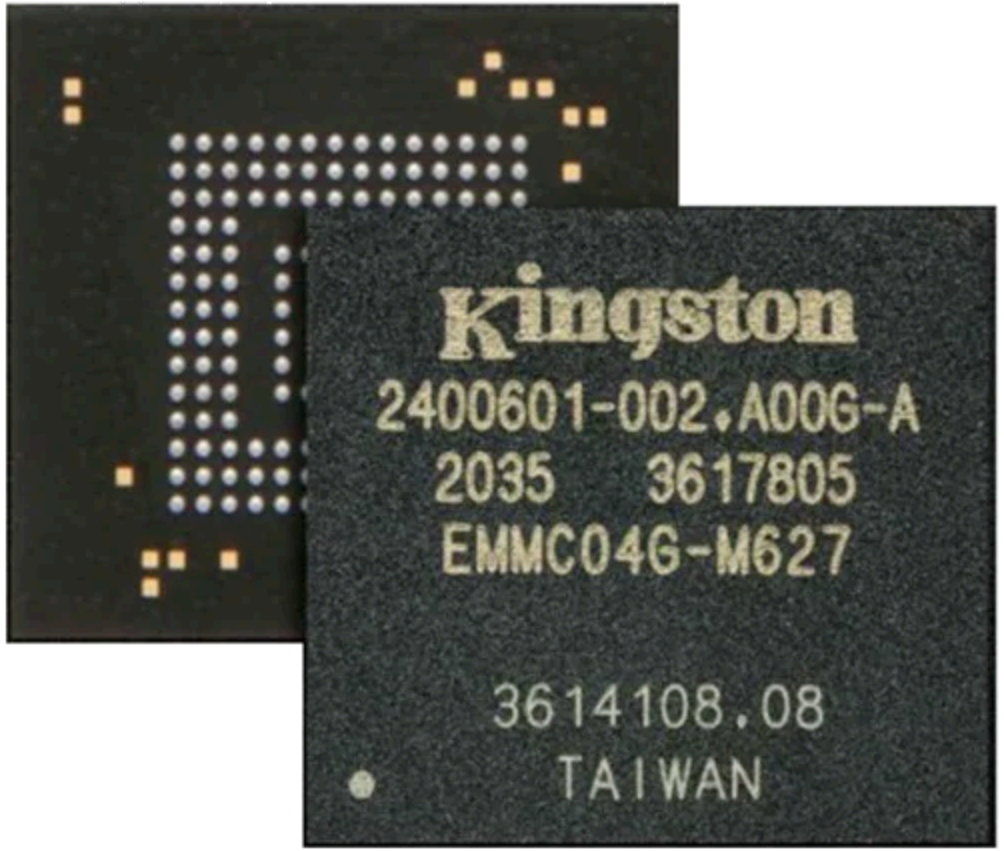
Flash externe

SYNACKTIV

Types

- NAND/NOR
- eMMC
- autre ?



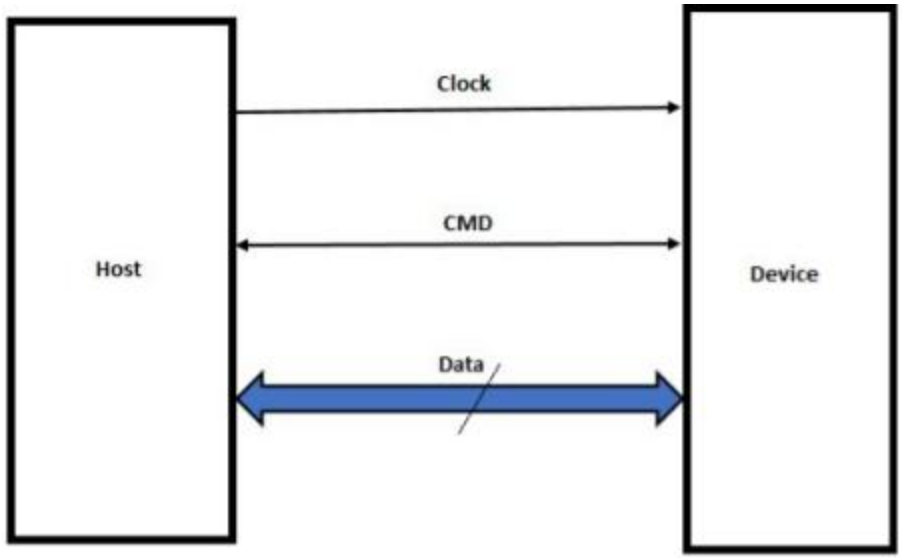


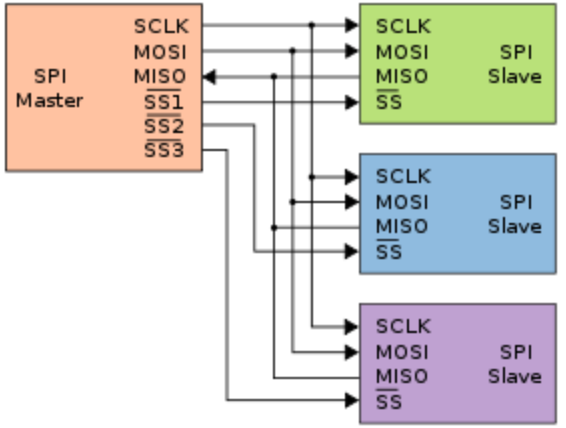
Flash externe

SYNACKTIV

Protocoles

- SPI
- SDIO
- ONFI
- etc.





Flash SPI externe

SYNACKTIV

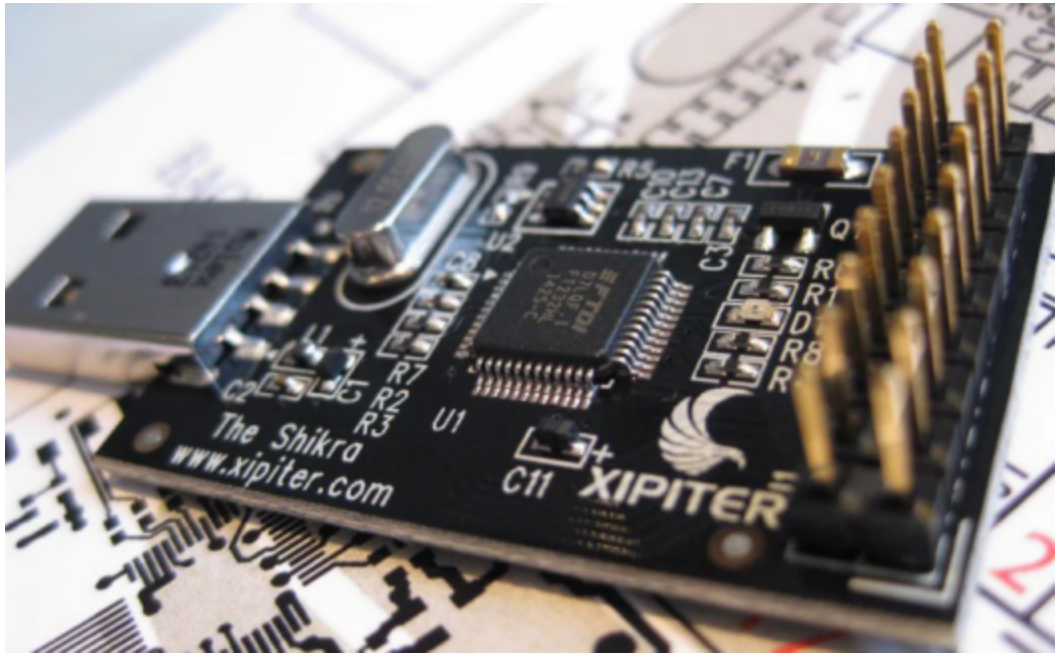
Interface

- avec la puce *in situ*
- avec la puce désoudée
- via des points de test

Matériel

SYNACKTIV

- Une multitude de matériel
- prix très variable...
- ... et qualité aussi



CH341a

- **Supporte I2C, SPI et UART**
- **Supporte officiellement 3.3v/5v**
- ***form factor* pratique**
- **peu cher**
- **pas de constructeur officiel**

→ **trouvable partout**

CH341A 24 25 Series EEPROM Flash BIOS USB Programmer with Software & Driver | CH341A Programmateur USB Flash BIOS pour 24 séries EEPROM 25 SPI

Visiter la boutique TECNOIOT

★★★★½ 36

12[51] €

Retours GRATUITS

Les prix des articles vendus sur Amazon incluent la TVA. En fonction de votre adresse de livraison, la TVA peut varier au moment du paiement. Pour plus d'informations, Veuillez voir les détails.

Marque	TECNOIOT
Interface matérielle	USB
Appareils compatibles	Ordinateur personnel

CH341a

SYNACKTIV

- Supporte I2C, SPI et UART
- Supporte `officiellement` 3.3v/5v
- *form factor* pratique
- `peu cher`
- `pas de constructeur officiel`

→ trouvable partout

CH341A 24 25 Series EEPROM Flash BIOS USB Programmer with Software & Driver | CH341A Programmateur USB Flash BIOS pour 24 séries EEPROM 25 SPI

Visiter la boutique TECNOIOT

★★★★½ 36

12[51] €

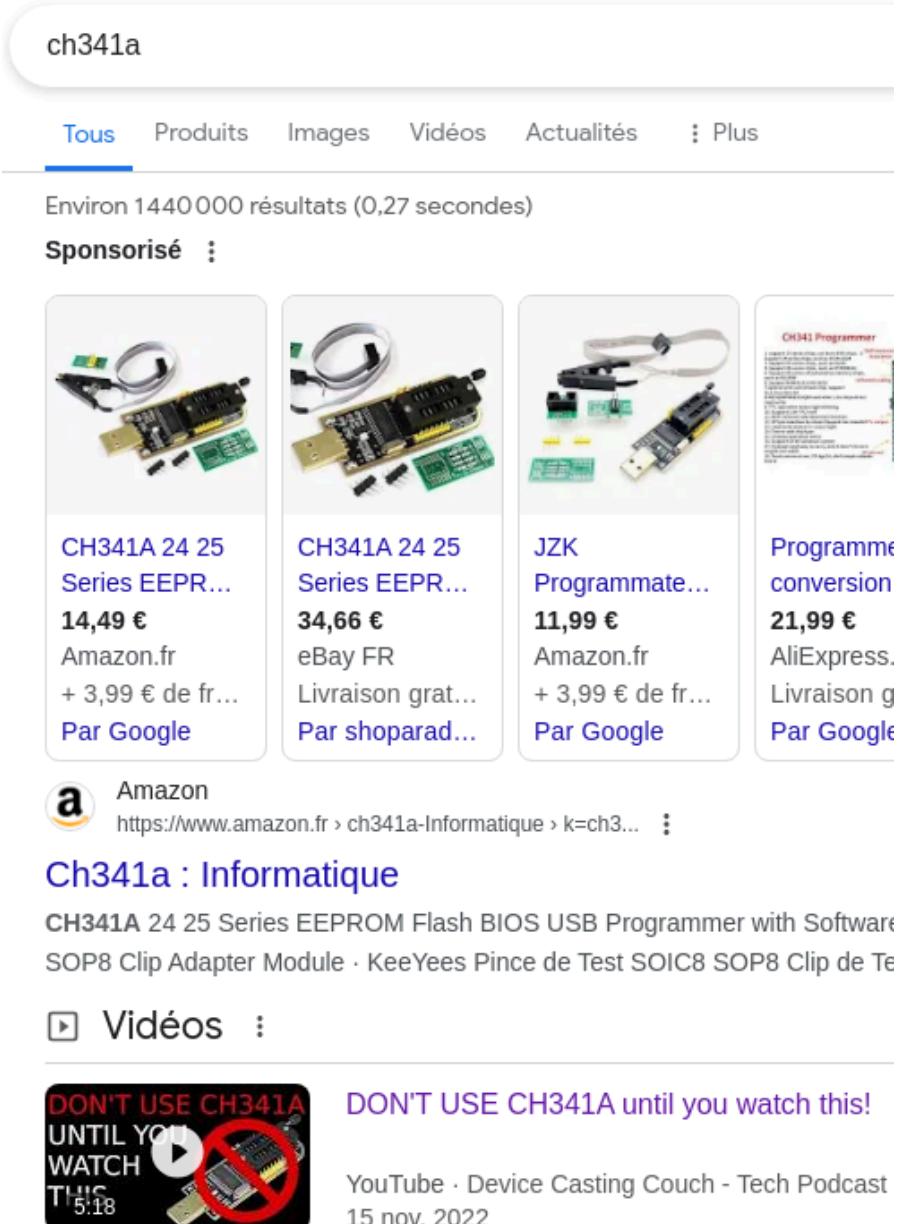
Retours GRATUITS

Les prix des articles vendus sur Amazon incluent la TVA. En fonction de votre adresse de livraison, la TVA peut varier au moment du paiement. Pour plus d'informations, Veuillez voir les détails.

Marque	TECNOIOT
Interface matérielle	USB
Appareils compatibles	Ordinateur personnel

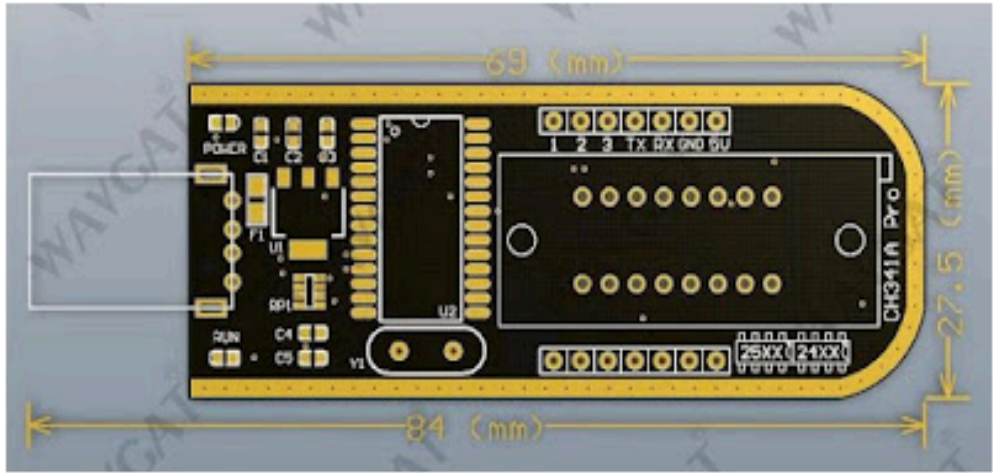
CH341a : what could go wrong?

SYNACKTIV



CH341a : what could go wrong?

SYNACKTIV



CH341A Mini Programmer PCB (by WAVGAT/AliExpress)

Now, let's return to the schematic and analyze it a bit. The chip is powered from 5V, so its I/O ports will also use 5V. **Basically this is a 5V device.** The problem is that any memory you fit in the socket will be powered from 3.3V. And this seems to be the only function of the 3.3V regulator (besides the 3.3V pin on the SPI connector). I don't know why the designer even used a regulator, if it didn't provide a switch to choose between 3.3V or 5V levels and supply.

Credits: onetransistor.eu

CH341a : datasheet

SYNACKTIV

VCC	Voltage source (VCC connects to power, GND to ground)	-0.5	6.5	V
VIO	The voltage of input or output pin	-0.5	VCC+0.5	V

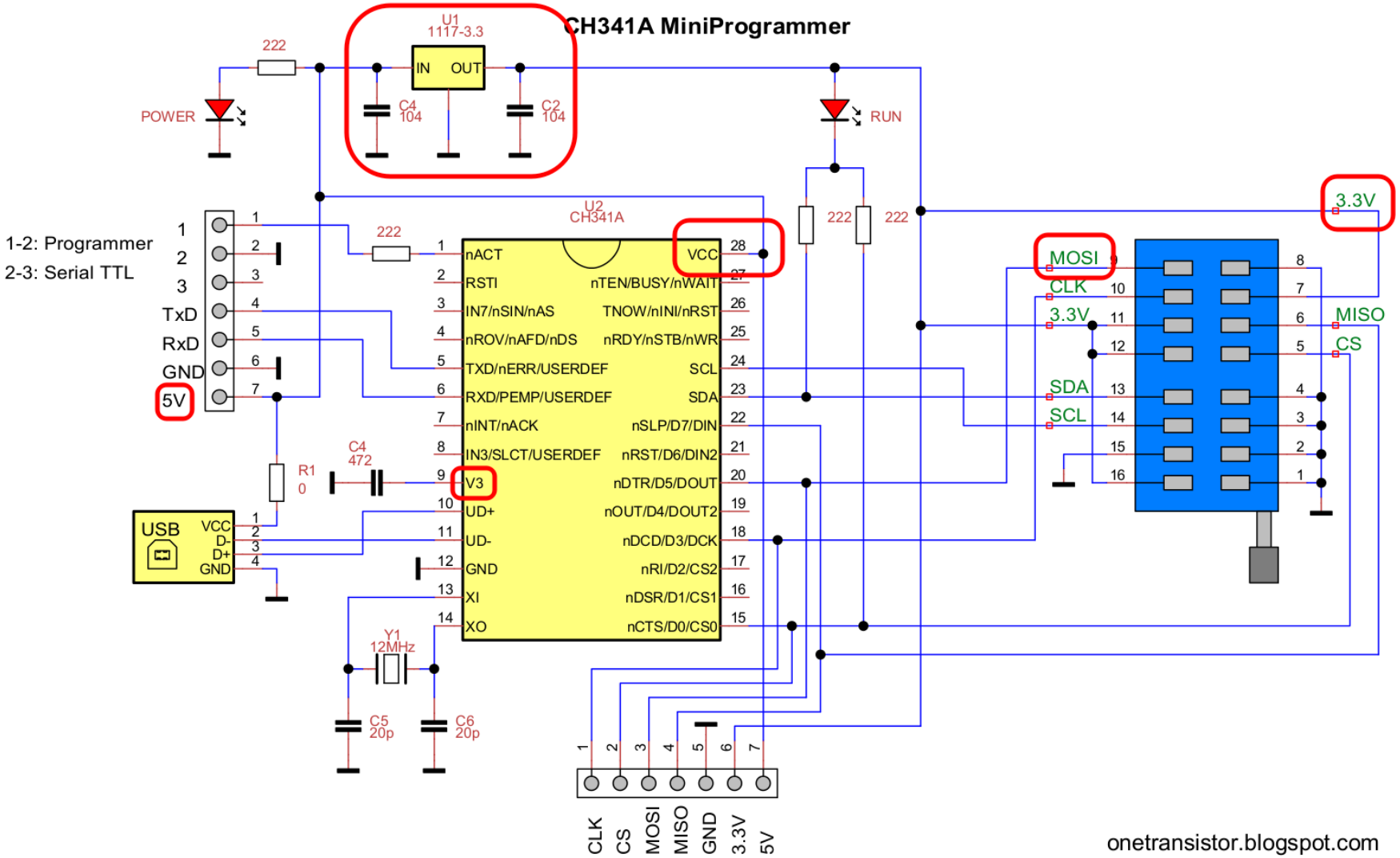
6.2. Electrical parameter (test conditions: TA=25℃, VCC=5V, excluding pin connection of USB bus)

(If the source voltage is 3.3V, multiply 40% of the current parameter)

Name	Parameter note		Min.	Typical	Max.	Units
VCC	Source voltage	V3 doesn't connect to VCC	4.5	5	5.3	V
		V3 connect to VCC	3.3	3.3	3.6	V

CH341a : datasheet

SYNACKTIV



Credits: onetransistor.eu

CH341a : patch

SYNACKTIV

Author | **Topic: CH341A Serial Memory Programmer Power Supply Fix**

johnmx
Frequent Contributor

Posts: 277
Country:

CH341A Serial Memory Programmer Power Supply Fix
« **on:** October 14, 2017, 12:29:37 pm »

I bought one cheap chinese CH341A serial memory programmer black PCB (see attached picture).

Someone already did the schematic of this board (atached). Source: https://www.onetransistor.eu/2017/08/ch341a-mini-programmer-schematic.html

All Vcc connections in the ZIF socket are 3.3V but the CH341A is powered at 5V.
So all I2C and SPI signals are 5V while the external memory is powered at 3.3V.
There are no limiting series resistors on those signals.

One simple solution to fix this issue is to simply bypass the 1117-3.3V regulator.
I can use the hot air station to remove the 1117 and then short-circuit the input with the output.

My question is, is it safe to just do the short-circuit without removing the 1117 linear regulator?

Ian.M
Super Contributor
Posts: 12813

Re: CH341A Serial Memory Programmer Power Supply Fix
« **Reply #3 on:** October 14, 2017, 03:16:21 pm »

No track cuts, just lift pin 28 (easy because its near the board edge with nothing in the way) and run a wire from the lifted pin across to pin 9, and on to the 3.3V regulator output.

WattsThat
Frequent Contributor
Posts: 764
Country:

Re: CH341A Serial Memory Programmer Power Supply Fix
« **Reply #21 on:** February 16, 2020, 05:05:54 am »

For any new players out there intending to do this mod, the OP's bodge wire modification shown in reply #4 is done correctly. What is wrong is the original schematic, it lists C4 twice. The 104 value C4 shown on the the 1117 input is in reality C1.

Forum source

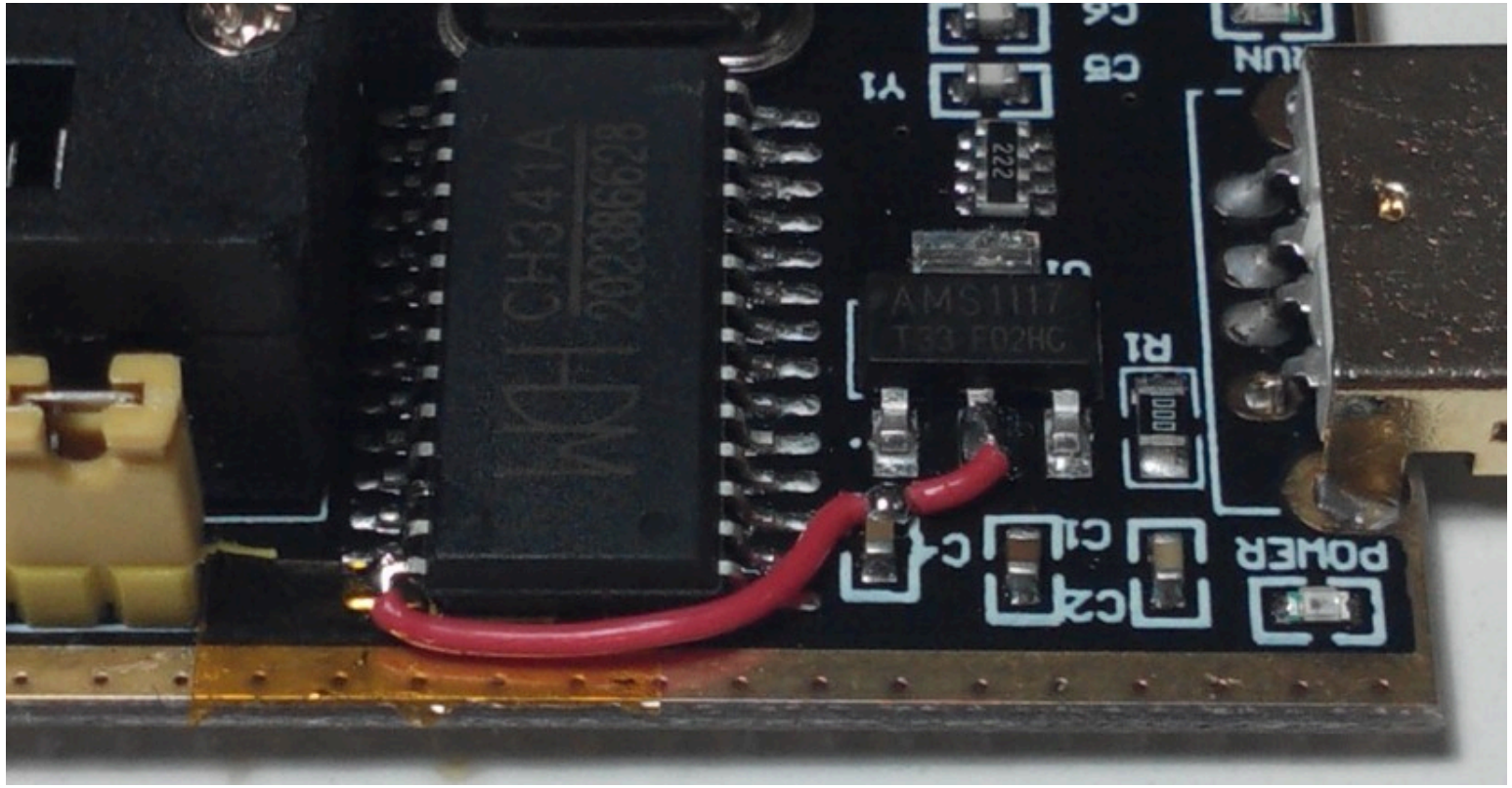
CH341a : datasheet

SYNACKTIV

CH341 support 5V and 3.3V source voltage. When working on 5V source voltage, the VCC input 5V power from outside, and V3 connects to 4700pF or 0.01uF decoupling capacitance. If the work power is 3.3V, connect V3 to VCC, input 3.3V source voltage. The voltage of other circuit which is connected to CH341 is no pass than 3.3V.

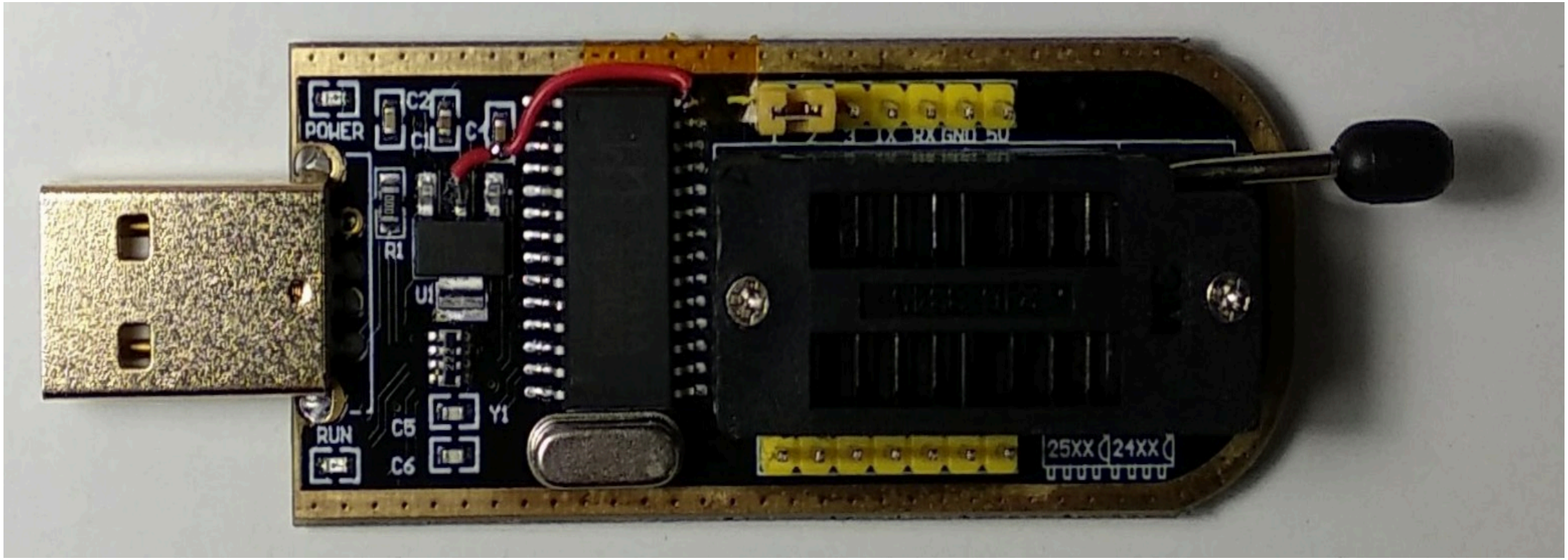
CH341a : patch

SYNACKTIV



CH341a : patch

SYNACKTIV



Conclusions

SYNACKTIV

- De tout et de rien en matériel
- Bien lire la doc (s'il y en a) du matériel...
- ... sinon "faisez vos recherches !"
- *captain obvious* → relation prix/qualité ?
- `Utiliser autre chose que le CH341a` → *board* utilisant un FT2232h

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com