MAIS UM EVENTO Flipside

REALIZAÇÃO Green Helmet

ROAD SEC 2023

O MAIOR FESTIVAL HACKER DA AMÉRICA LATINA

ROADSEC

15.07.23

ROAD SEC 2023

O MAIOR FESTIVAL HACKER DA AMÉRICA LATINA

Flipside

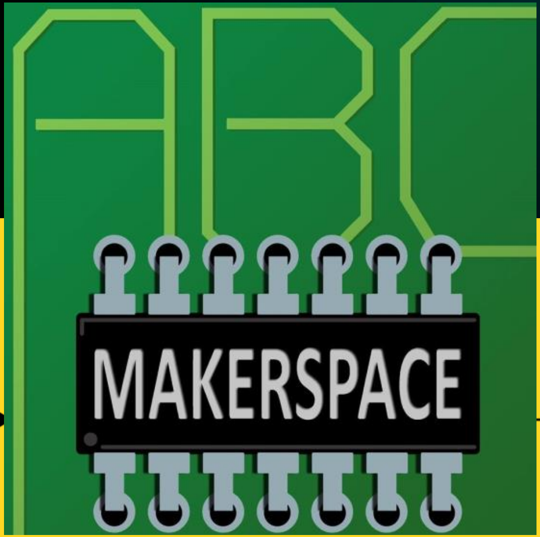
Extração de Informações via Hardware

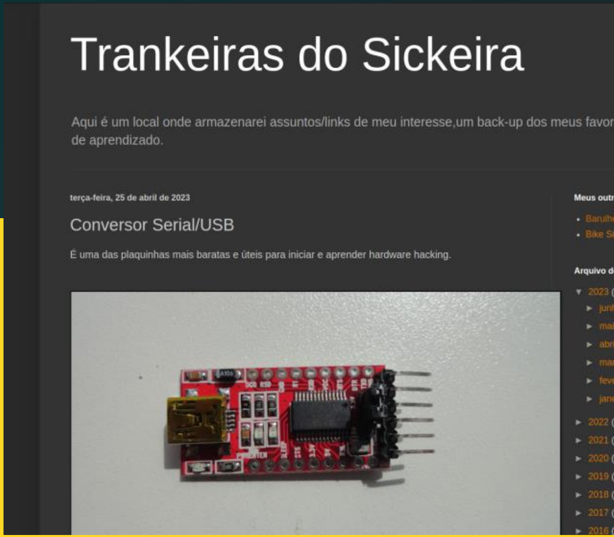
ROAD SEC 2023

O MAIOR FESTIVAL HACKER DA AMÉRICA LATINA

WhoAmI

Flipside





Trankeiras do Sickeira

Aqui é um local onde armazenarei assuntos/links de meu interesse,um back-up dos meus favor
de aprendizado.

terça-feira, 25 de abril de 2023

Conversor Serial/USB

É uma das plaquinhas mais baratas e úteis para iniciar e aprender hardware hacking.

Meus outr

- Barulh
- Bike Si

Arquivo d

- ▼ 2023 (
  - ► junh
  - ► mai
  - ► abri
  - ► mar
  - ► feve
  - ► jane
- ► 2022 (
- ► 2021 (
- ► 2020 (
- ► 2019 (
- ► 2018 (
- ► 2017 (
- ► 2016 (

ROAD
SEC
2023

WikiLab

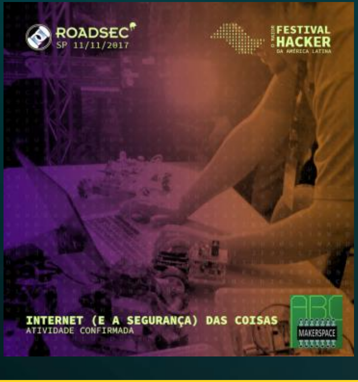
Flipside

ROAD SEC 2023

O MAIOR FESTIVAL HACKER DA AMÉRICA LATINA

ABC Makerspace na RoadSec 2016/2022

Flipside


ROADSEC SP 11/11/2017
O MAIOR FESTIVAL HACKER DA AMÉRICA LATINA
INTERNET (E A SEGURANÇA) DAS COISAS
ATIVIDADE CONFIRMADA
ABC MAKERSPACE

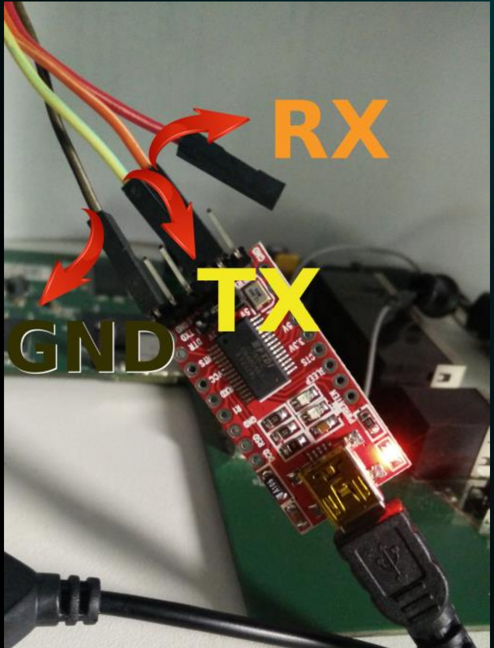
UART - Universal Asynchronous Receiver/Transmitter

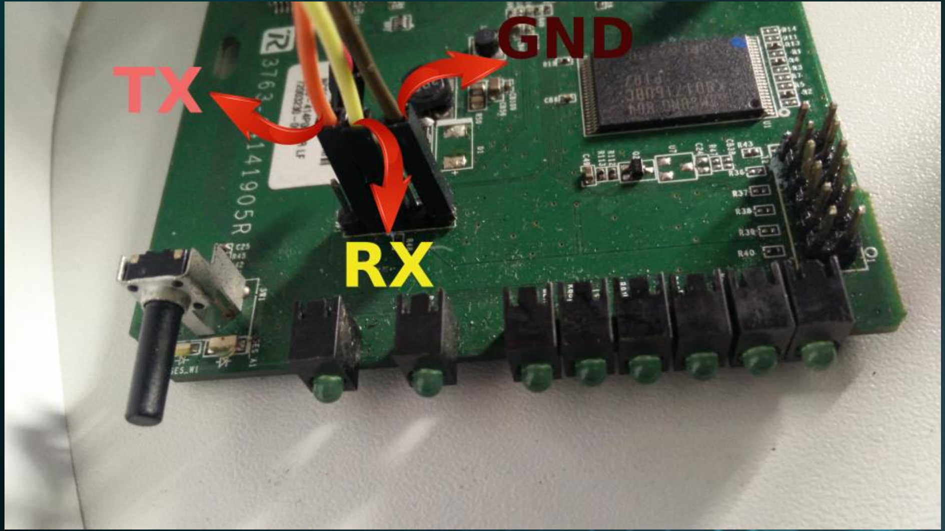
- TX - Transmissor
- RX - Receptor
- GND – Terra, carcaça, fonte e capacitor hachurado
- VCC – Tensão

ROAD SEC 2023

- Trocar o RX por TX
- Trocar o TX por RX
- Selecionar 3,3 V

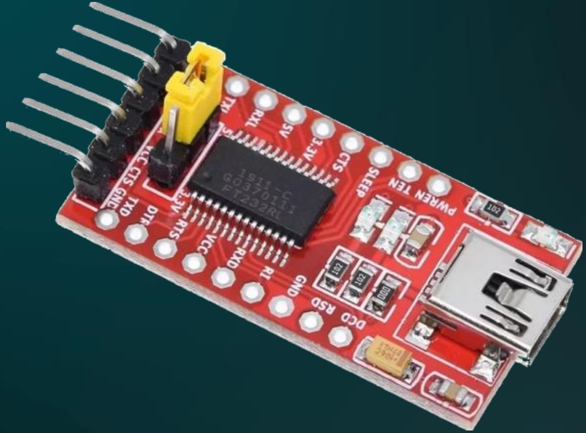
Flipside





ROAD SEC 2023

Flipside

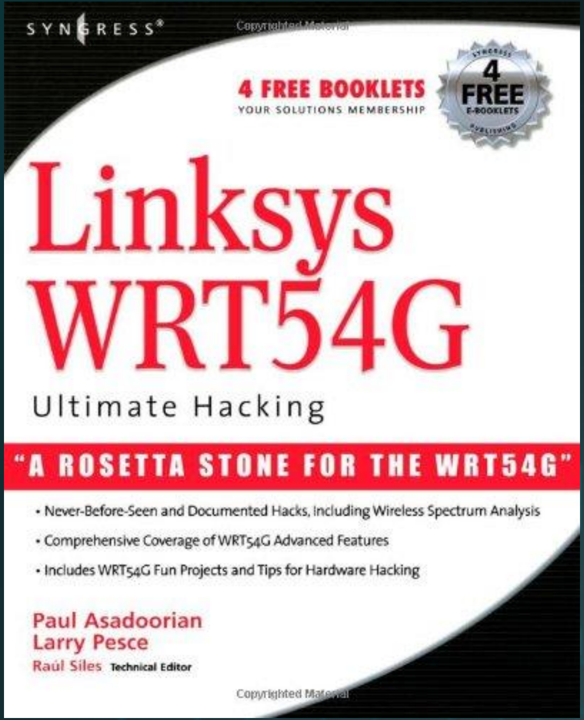


ROADSEC 2023 15.07.23

ROADSEC

Flipside

Livro: Linksys WRT54G Ultimate Hacking Edition: 1
Autores: Paul Asadoorian, Larry Pesce
Editora: Syngress
Ano: 2007
Páginas: 386
ISBN: 9781597491662; 1597491667



SYNGRESS®

Copyrighted Material

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP

4 FREE E-BOOKLETS

Linksys WRT54G

Ultimate Hacking

"A ROSETTA STONE FOR THE WRT54G"

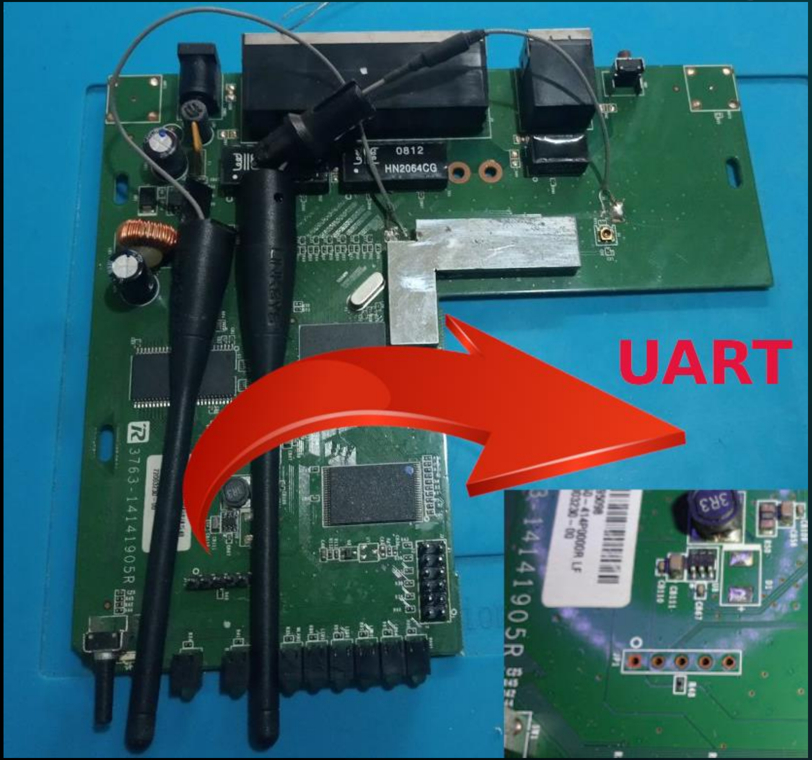
- Never-Before-Seen and Documented Hacks, Including Wireless Spectrum Analysis
- Comprehensive Coverage of WRT54G Advanced Features
- Includes WRT54G Fun Projects and Tips for Hardware Hacking

Paul Asadoorian
Larry Pesce
Raúl Siles Technical Editor

Copyrighted Material

ROAD SEC 2023

Flipside



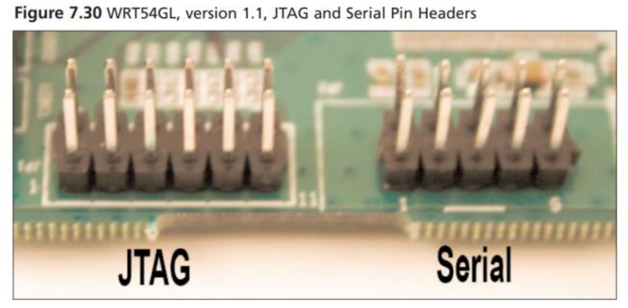


Figure 7.30 WRT54GL, version 1.1, JTAG and Serial Pin Headers

ROAD SEC 2023

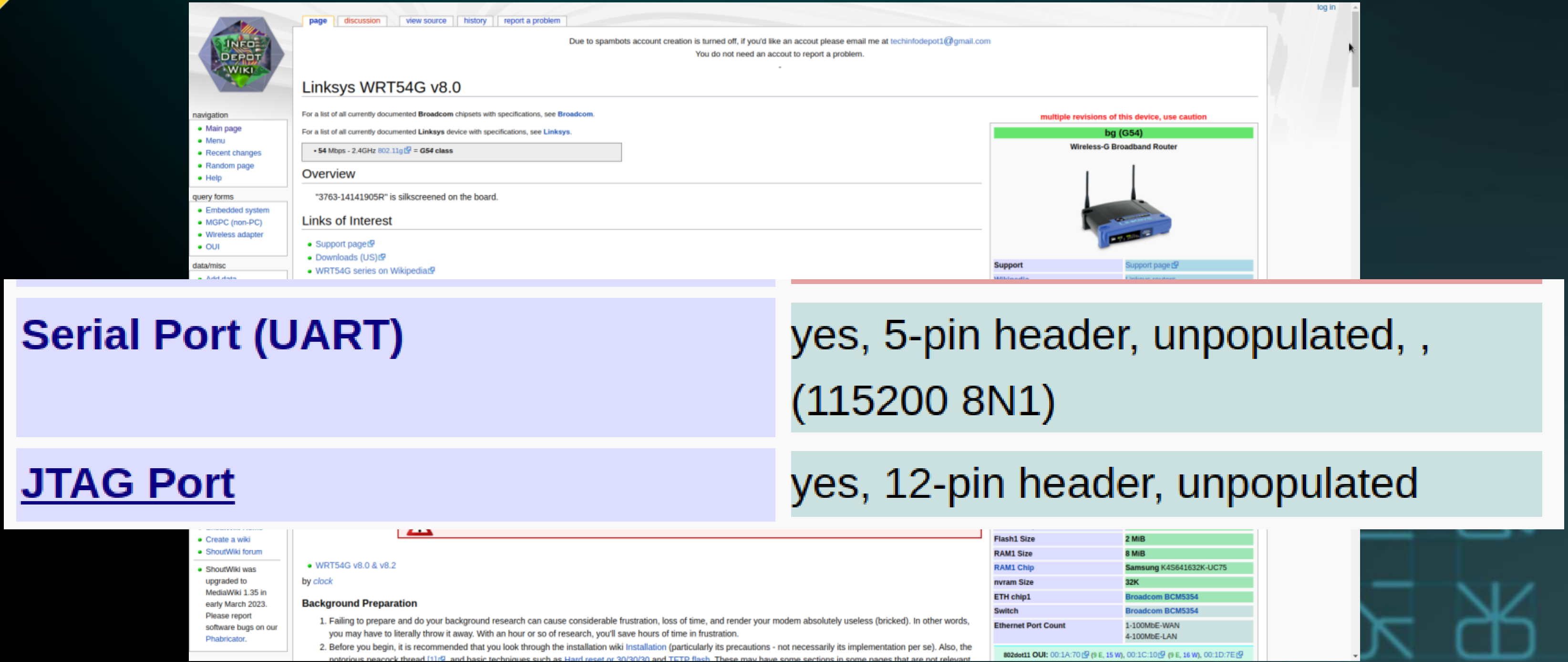
O MAIOR FESTIVAL HACKER DA AMÉRICA LATINA

Wikis de Dispositivos

Flipside

ROAD SEC 2023

Flipside



page | discussion | view source | history | report a problem

log in

Due to spambots account creation is turned off, if you'd like an accout please email me at techinfodepot1@gmail.com
You do not need an accout to report a problem.

navigation
- Main page
- Menu
- Recent changes
- Random page
- Help

query forms
- Embedded system
- MGPC (non-PC)
- Wireless adapter
- OUI

data/misc

Linksys WRT54G v8.0

For a list of all currently documented **Broadcom** chipsets with specifications, see **Broadcom**.

For a list of all currently documented **Linksys** device with specifications, see **Linksys**.

- **54** Mbps - 2.4GHz 802.11g = ***G54* class**

Overview

"3763-14141905R" is silkscreened on the board.

Links of Interest

- Support page
- Downloads (US)
- WRT54G series on Wikipedia

multiple revisions of this device, use caution

bg (G54)

Wireless-G Broadband Router

Support	Support page

Serial Port (UART)	yes, 5-pin header, unpopulated, , (115200 8N1)
JTAG Port	yes, 12-pin header, unpopulated

- Create a wiki
- ShoutWiki forum

- ShoutWiki was upgraded to MediaWiki 1.35 in early March 2023. Please report software bugs on our Phabricator.

- WRT54G v8.0 & v8.2

by *clock*

Background Preparation

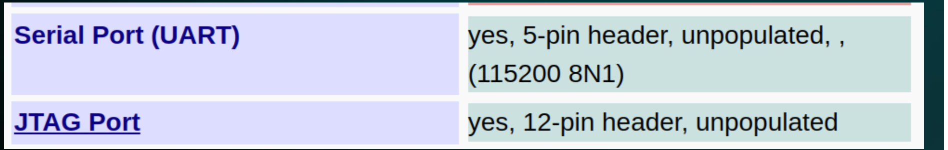
1. Failing to prepare and do your background research can cause considerable frustration, loss of time, and render your modem absolutely useless (bricked). In other words, you may have to literally throw it away. With an hour or so of research, you'll save hours of time in frustration.
2. Before you begin, it is recommended that you look through the installation wiki Installation (particularly its precautions - not necessarily its implementation per se). Also, the notorious peacock thread [1], and basic techniques such as Hard reset or 30/30/30 and TFTP flash. These may have some sections in some pages that are not relevant

Flash1 Size	**2 MiB**
RAM1 Size	**8 MiB**
RAM1 Chip	**Samsung** K4S641632K-UC75
nvram Size	**32K**
ETH chip1	**Broadcom BCM5354**
Switch	**Broadcom BCM5354**
Ethernet Port Count	1-100MbE-WAN 4-100MbE-LAN

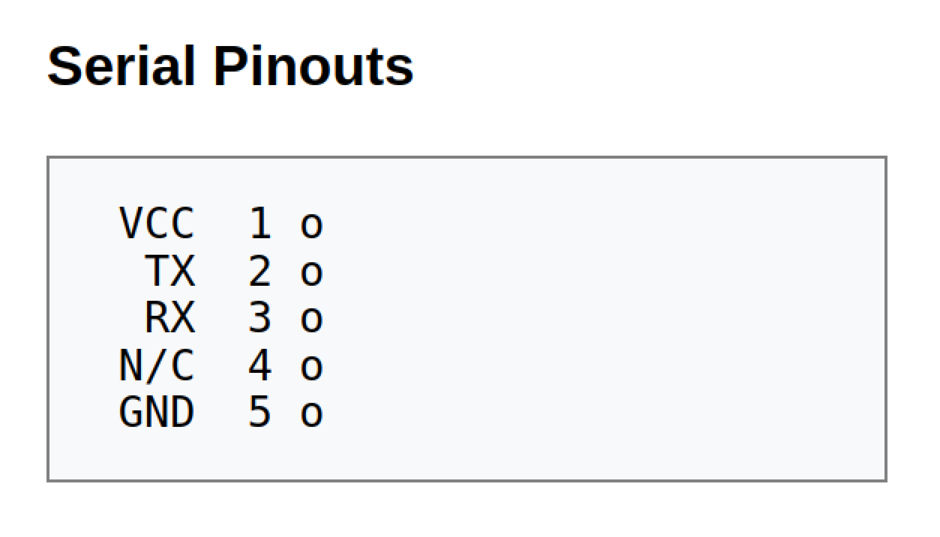
802dot11 OUI: 00:1A:70 (9 E, 15 W), 00:1C:10 (9 E, 16 W), 00:1D:7E

ROAD SEC 2023

Flipside

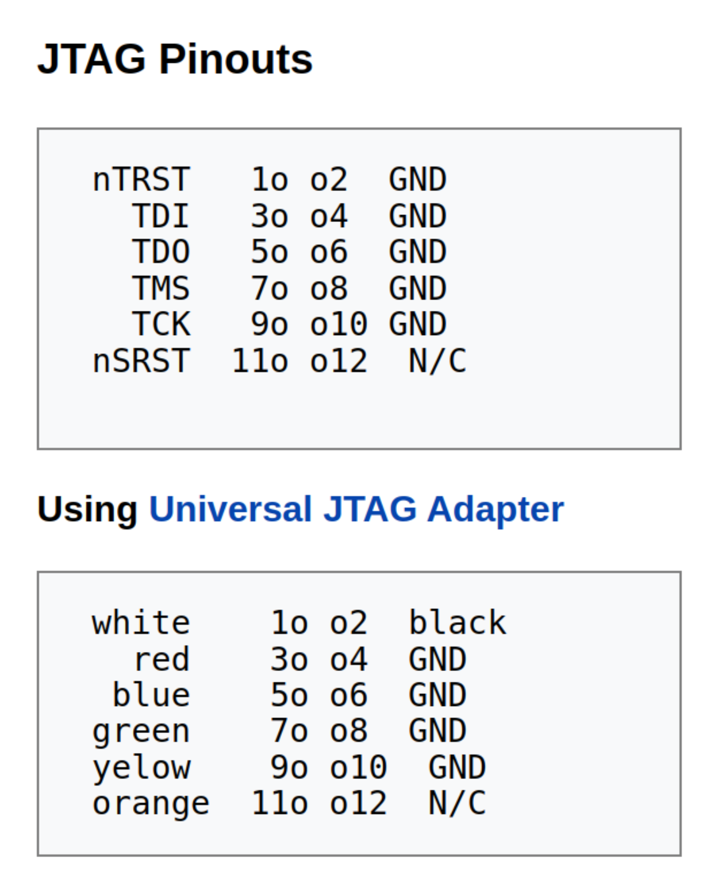


Serial Port (UART)	yes, 5-pin header, unpopulated, , (115200 8N1)
JTAG Port	yes, 12-pin header, unpopulated



Serial Pinouts

```
VCC  1 o
 TX  2 o
 RX  3 o
N/C  4 o
GND  5 o
```



JTAG Pinouts

```
nTRST    1o o2   GND
  TDI    3o o4   GND
  TDO    5o o6   GND
  TMS    7o o8   GND
  TCK    9o o10  GND
nSRST   11o o12   N/C
```

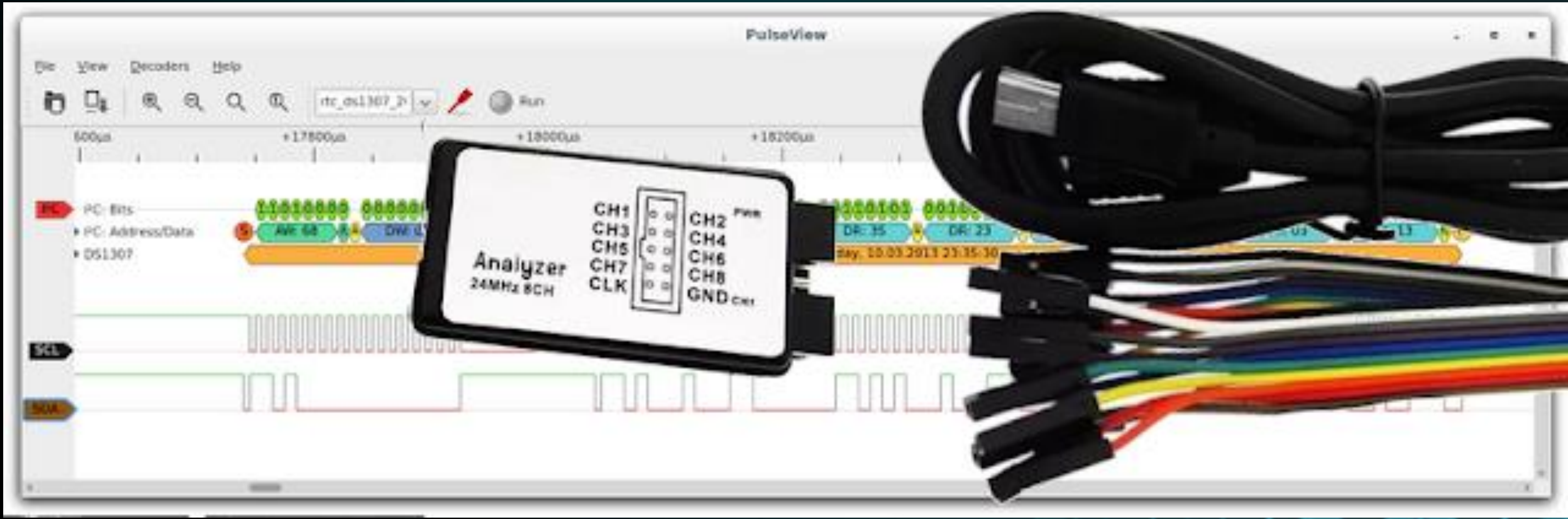
Using Universal JTAG Adapter

```
white     1o o2   black
  red     3o o4   GND
 blue     5o o6   GND
green     7o o8   GND
yelow     9o o10   GND
orange   11o o12   N/C
```

ROAD SEC 2023

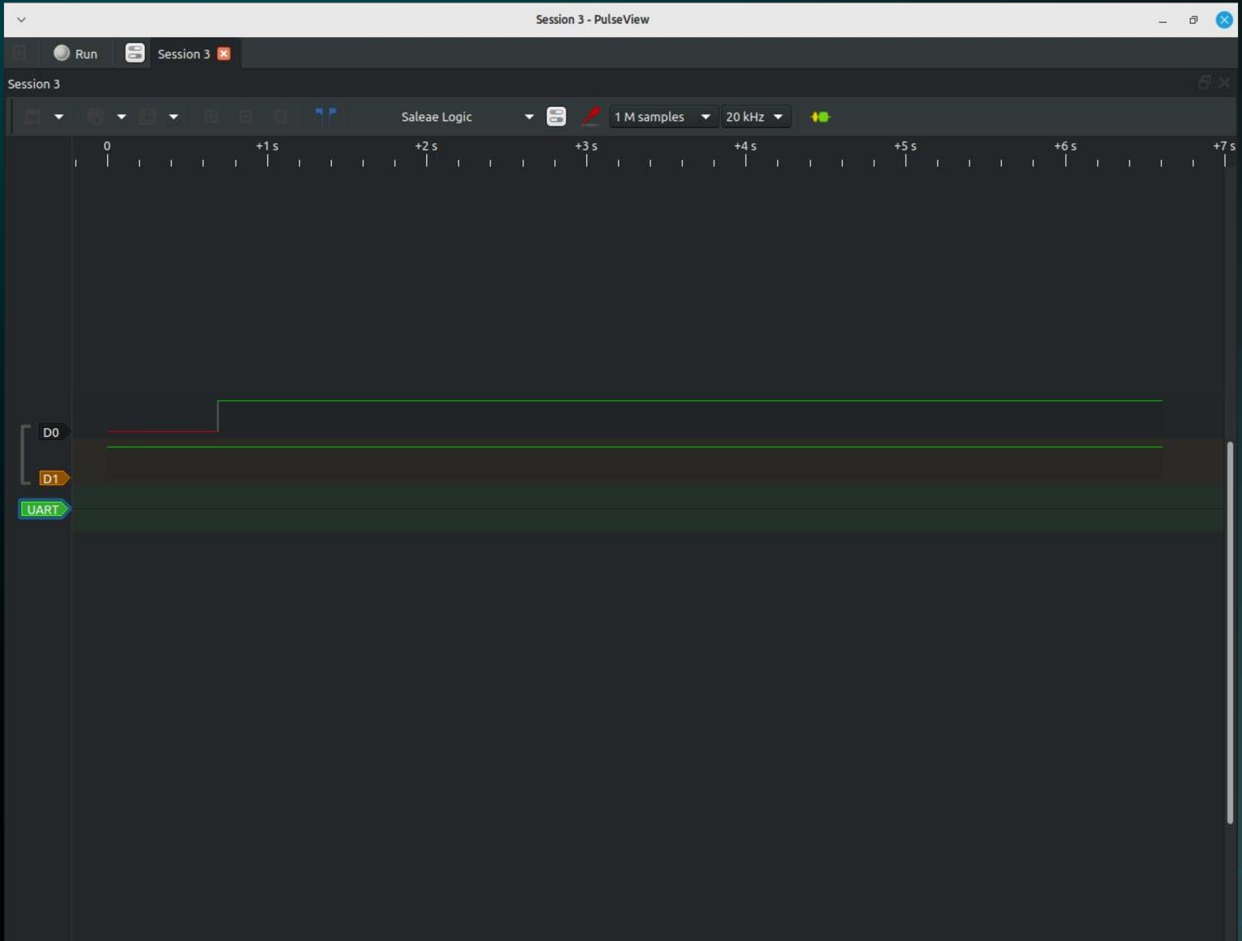
Flipside

Analisador Lógico 8 Canais



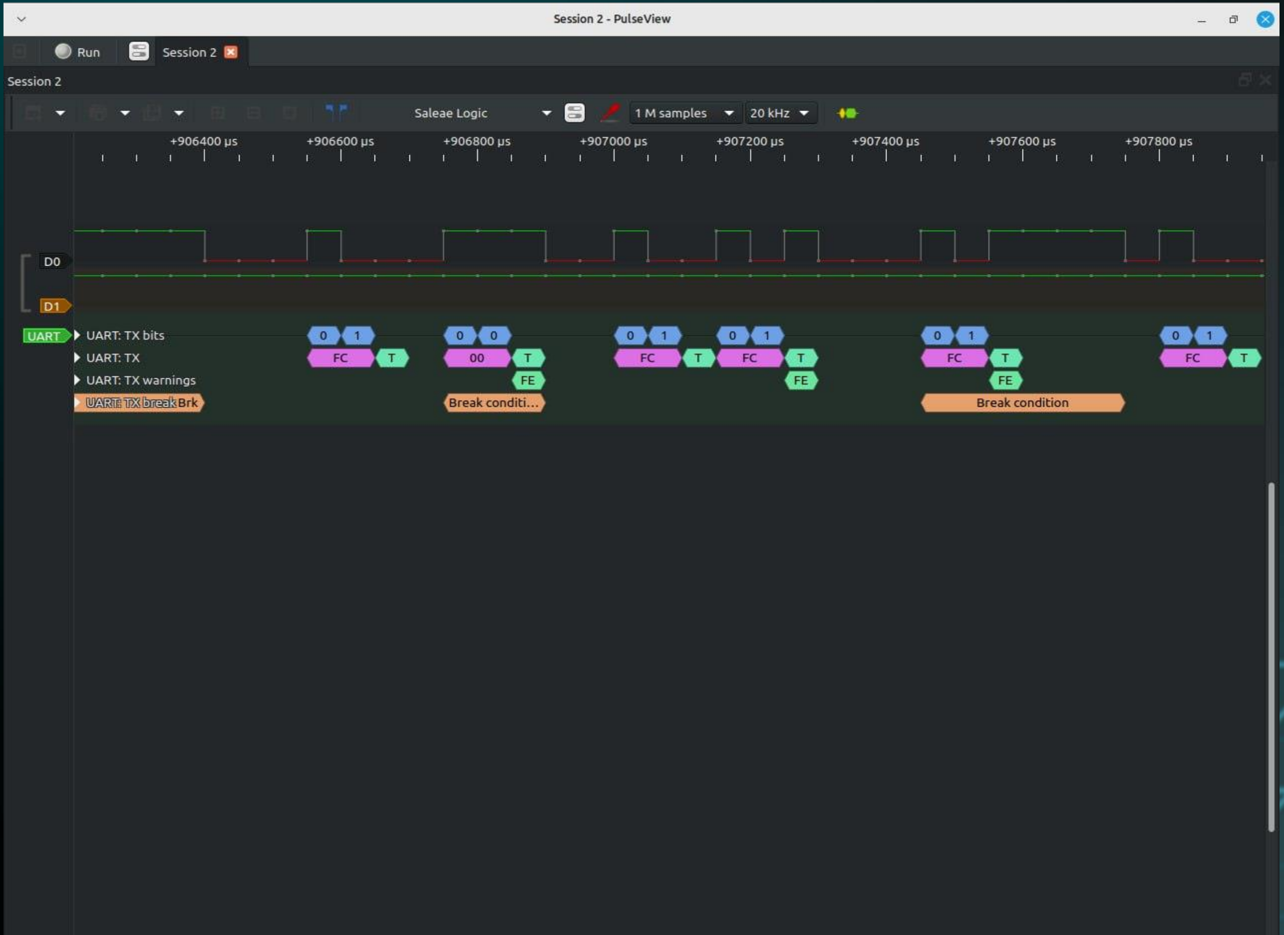
ROAD SEC 2023

Flipside



ROAD SEC 2023

Flipside



Session 2 - PulseView

Run | Session 2

Session 2

Saleae Logic | 1 M samples | 20 kHz

UART: TX bits: 0 1 | 0 0 | 0 1 | 0 1 | 0 1 | 0 1

UART: TX: FC T | 00 T | FC T | FC T | FC T | FC T

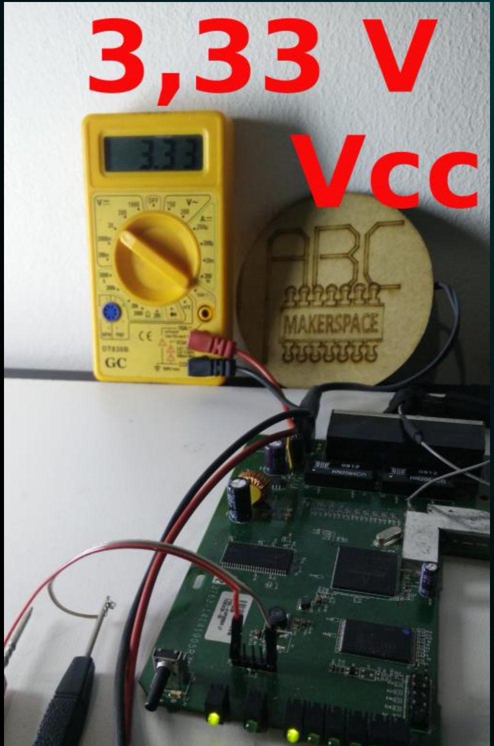
UART: TX warnings: FE | FE | FE

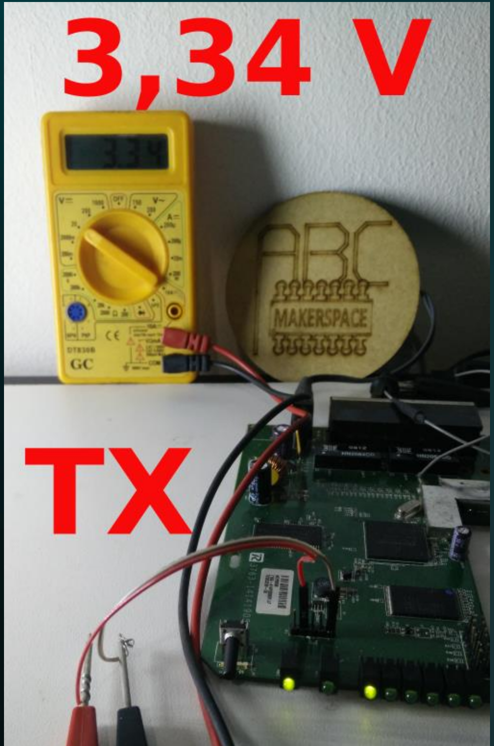
UART: TX break Brk: Break conditi... | Break condition

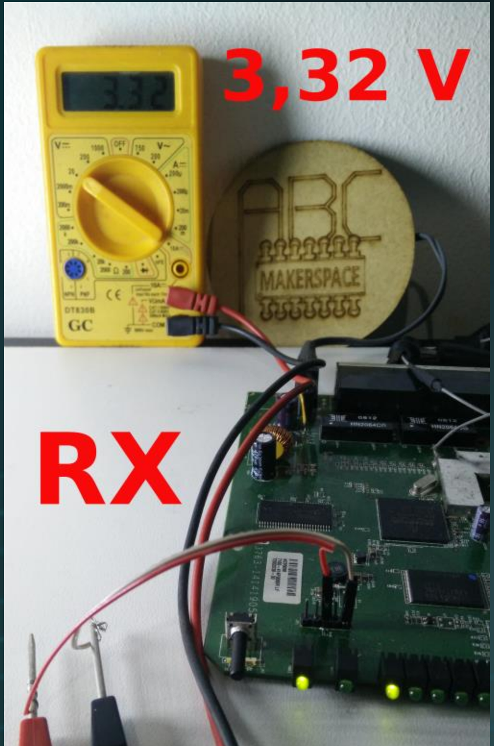
ROAD SEC 2023

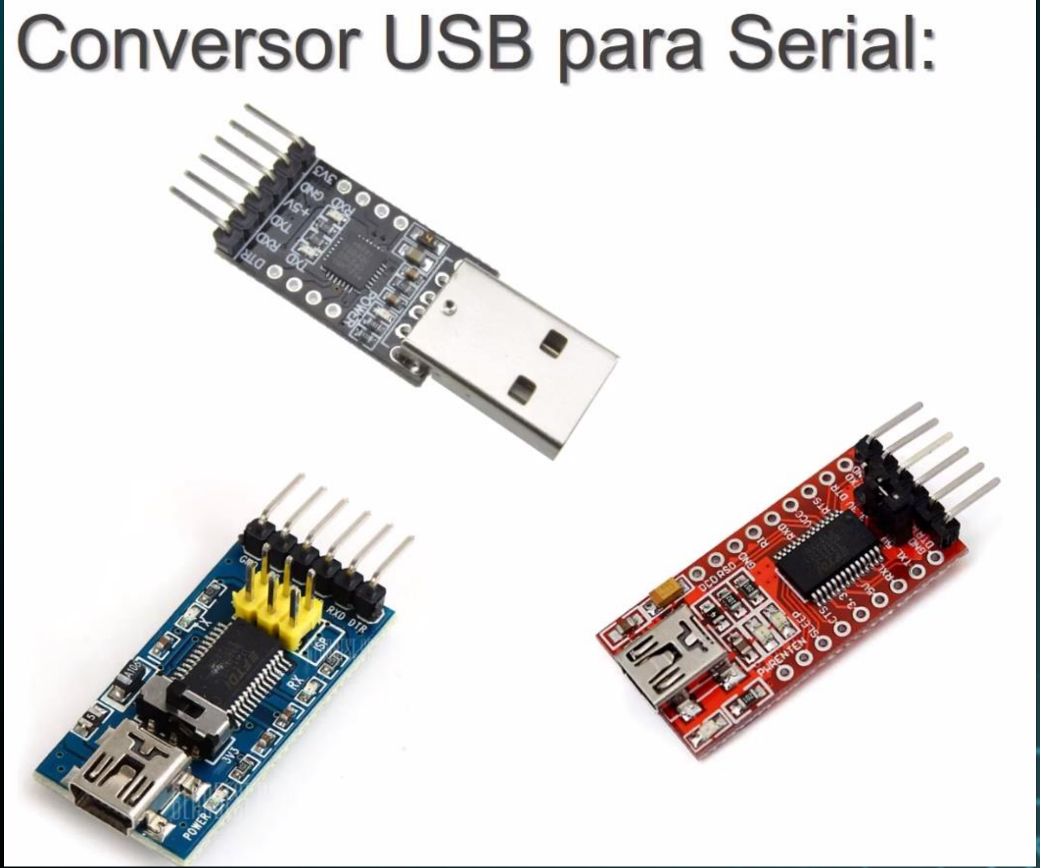
Multimetro Digital

Flipside







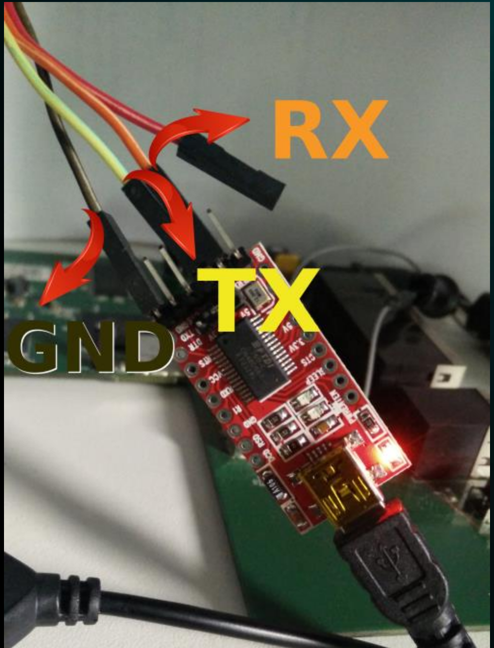


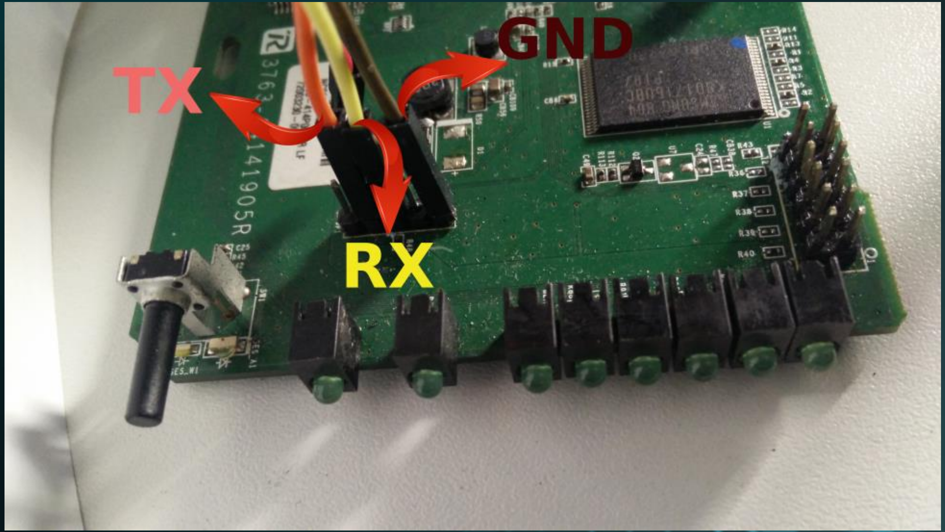
Conversor USB para Serial:

ROAD SEC 2023

- Trocar o RX por TX
- Trocar o TX por RX
- Selecionar 3,3 V

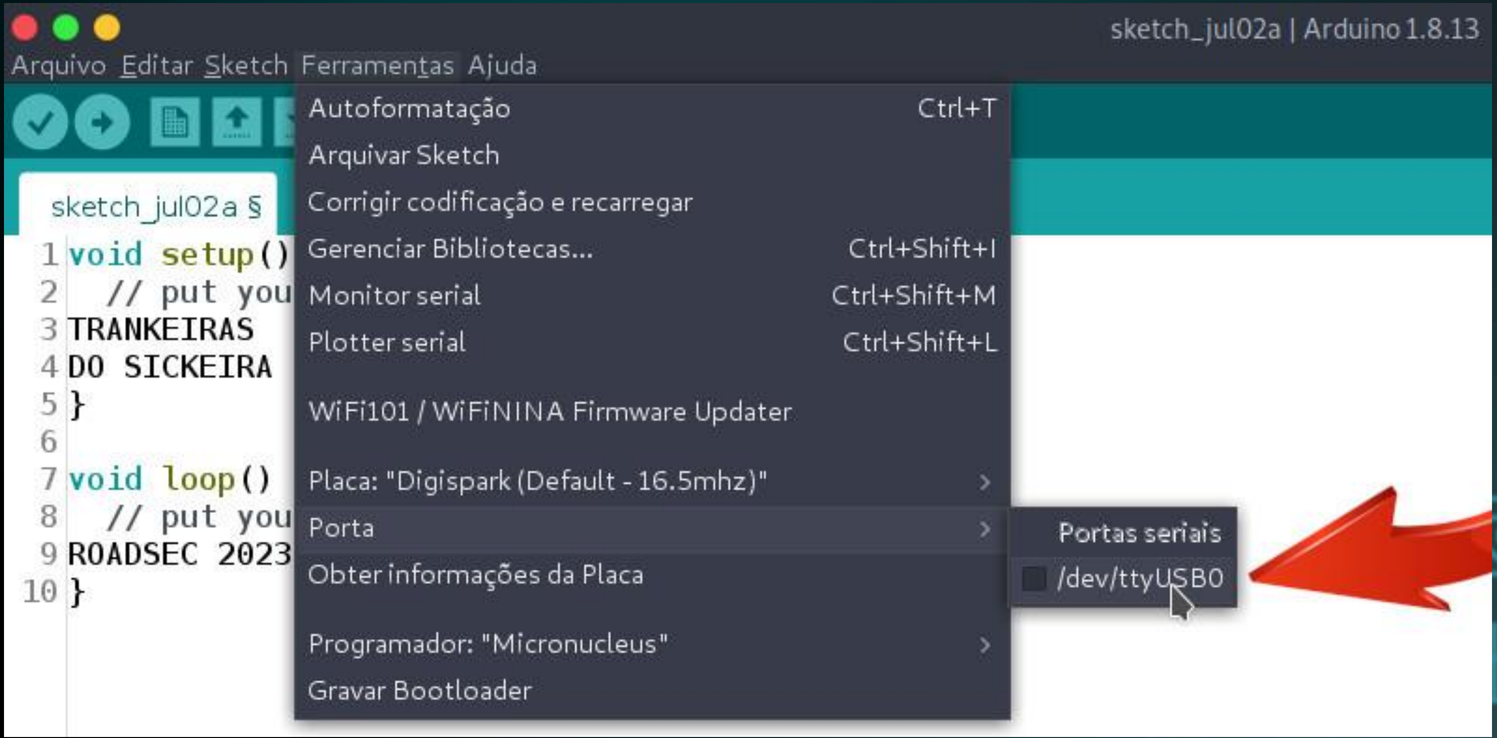
Flipside





ROAD
SEC
2023

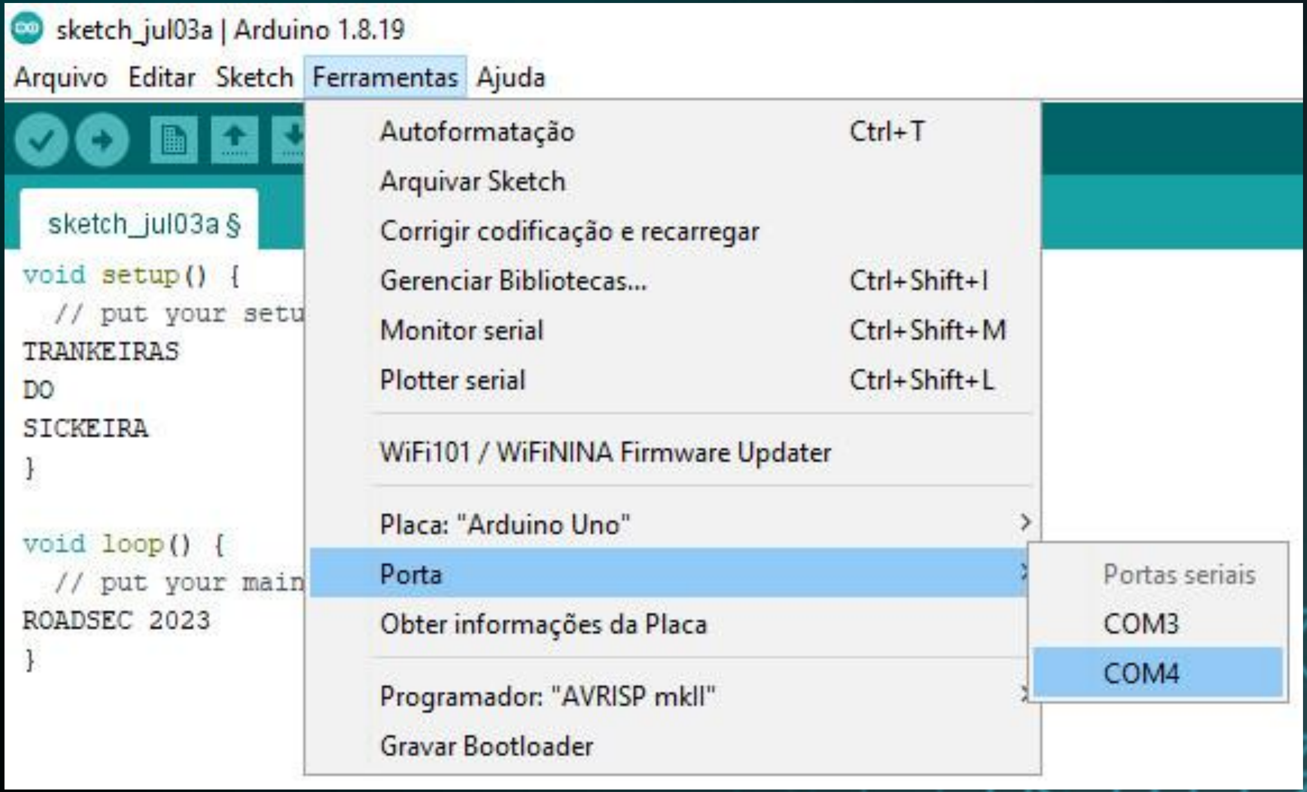
Flipside


sketch_jul02a | Arduino 1.8.13
Arquivo
Editar
Sketch
Ferramentas
Ajuda
sketch_jul02a §
Autoformatação Ctrl+T
Arquivar Sketch
Corrigir codificação e recarregar
Gerenciar Bibliotecas... Ctrl+Shift+I
Monitor serial Ctrl+Shift+M
Plotter serial Ctrl+Shift+L
WiFi101 / WiFiNINA Firmware Updater
Placa: "Digispark (Default - 16.5mhz)"
Porta
Obter informações da Placa
Programador: "Micronucleus"
Gravar Bootloader
Portas seriais
/dev/ttyUSB0

```
void setup()
  // put you
TRANKEIRAS
DO SICKEIRA
}

void loop()
  // put you
ROADSEC 2023
}
```

ROAD SEC 2023

Flipside



sketch_jul03a | Arduino 1.8.19

```
void setup() {
  // put your setu
TRANKEIRAS
DO
SICKEIRA
}

void loop() {
  // put your main
ROADSEC 2023
}
```

Placa: "Arduino Uno"

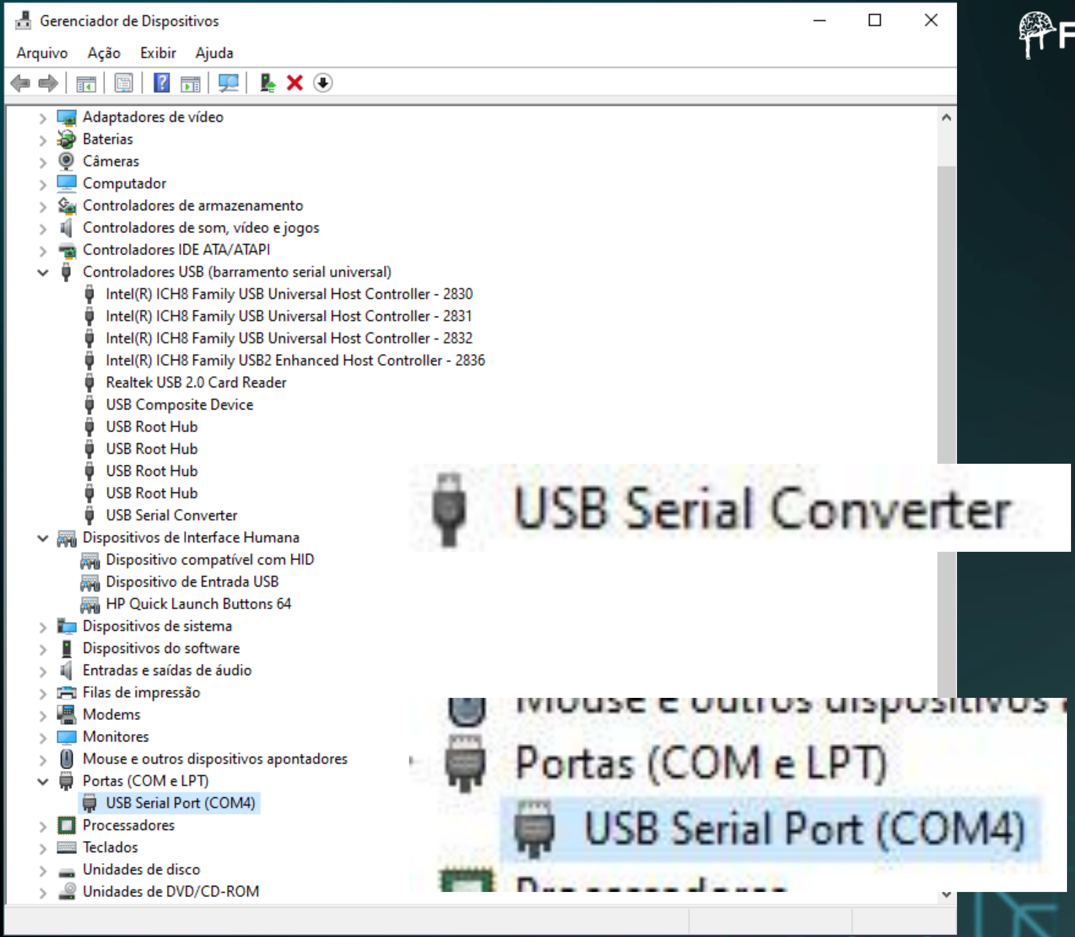
Porta: COM4

Programador: "AVRISP mkII"

Arquivo
Editar
Sketch
Ferramentas
Ajuda
sketch_jul03a §
Autoformatação Ctrl+T
Arquivar Sketch
Corrigir codificação e recarregar
Gerenciar Bibliotecas... Ctrl+Shift+I
Monitor serial Ctrl+Shift+M
Plotter serial Ctrl+Shift+L
WiFi101 / WiFiNINA Firmware Updater
Porta
Obter informações da Placa
Gravar Bootloader
Portas seriais
COM3
COM4

ROAD SEC 2023

Flipside



Gerenciador de Dispositivos

```
> Adaptadores de vídeo
> Baterias
> Câmeras
> Computador
> Controladores de armazenamento
> Controladores de som, vídeo e jogos
> Controladores IDE ATA/ATAPI
v Controladores USB (barramento serial universal)
    Intel(R) ICH8 Family USB Universal Host Controller - 2830
    Intel(R) ICH8 Family USB Universal Host Controller - 2831
    Intel(R) ICH8 Family USB Universal Host Controller - 2832
    Intel(R) ICH8 Family USB2 Enhanced Host Controller - 2836
    Realtek USB 2.0 Card Reader
    USB Composite Device
    USB Root Hub
    USB Root Hub
    USB Root Hub
    USB Root Hub
    USB Serial Converter
v Dispositivos de Interface Humana
    Dispositivo compatível com HID
    Dispositivo de Entrada USB
    HP Quick Launch Buttons 64
> Dispositivos de sistema
> Dispositivos do software
> Entradas e saídas de áudio
> Filas de impressão
> Modems
> Monitores
> Mouse e outros dispositivos apontadores
v Portas (COM e LPT)
    USB Serial Port (COM4)
> Processadores
> Teclados
> Unidades de disco
> Unidades de DVD/CD-ROM
```

USB Serial Converter

Mouse e outros dispositivos

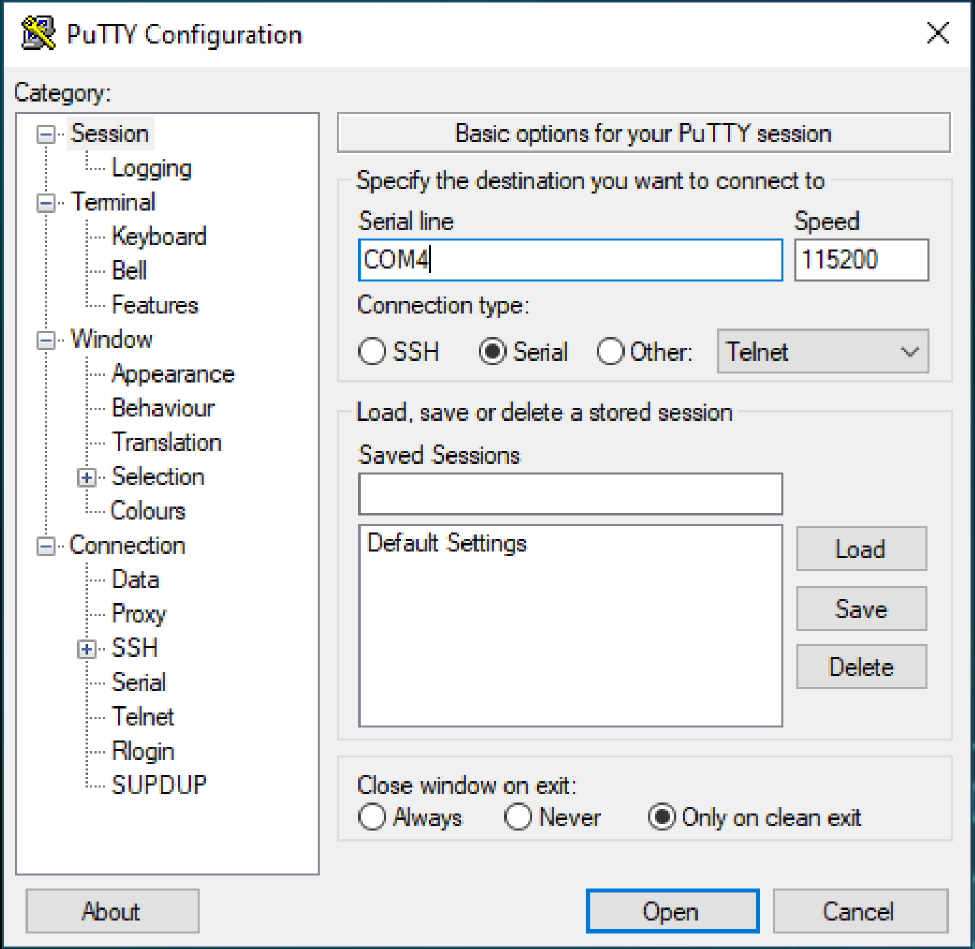
Portas (COM e LPT)

USB Serial Port (COM4)

Processadores

ROAD
SEC
2023

Flipside



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM4

Speed: 115200

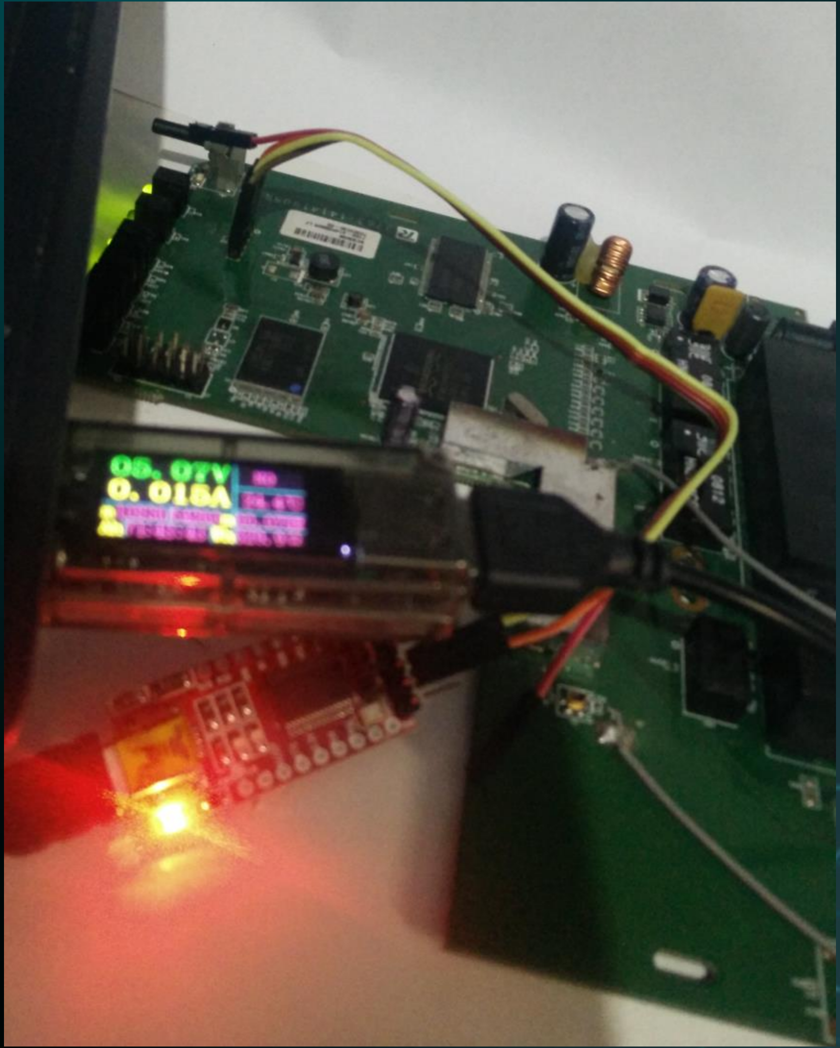
Connection type: ○ SSH ● Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions

Default Settings

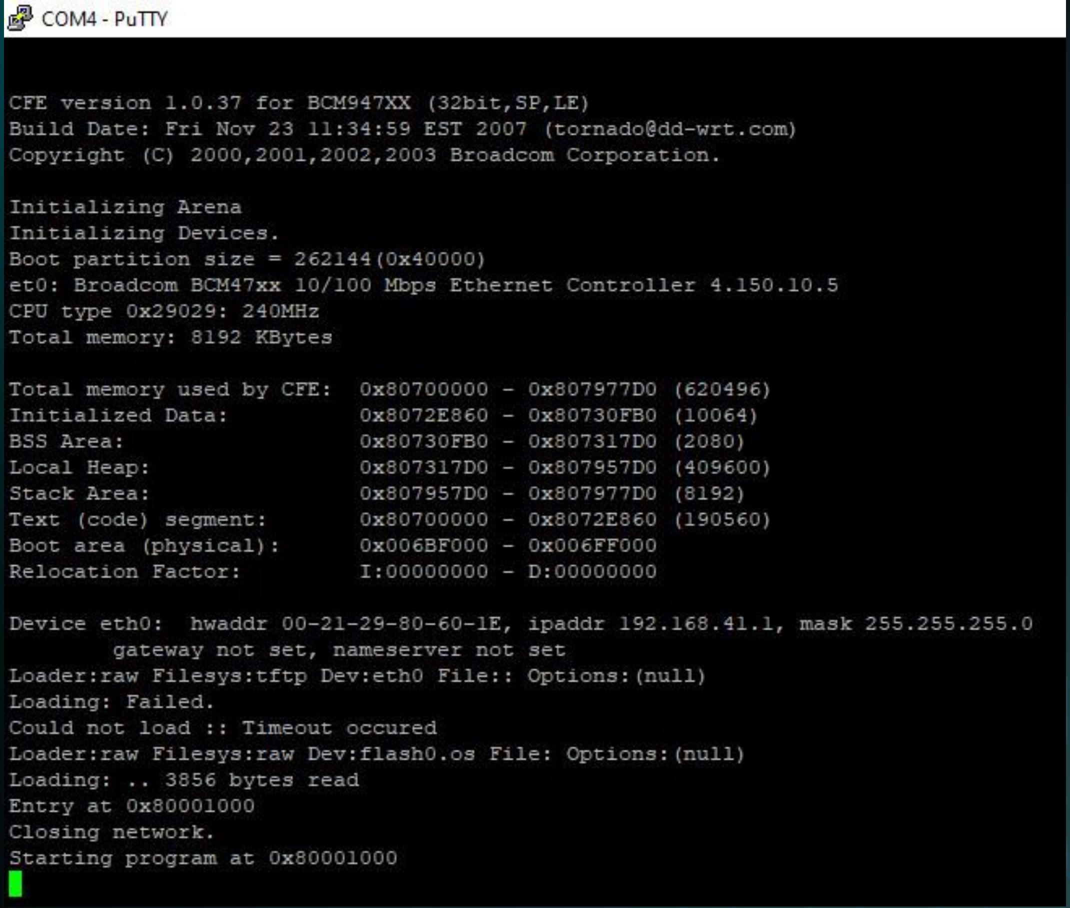
Close window on exit: ○ Always ○ Never ● Only on clean exit


05.07V
0.015A

ROADSEC 2023 15.07.23

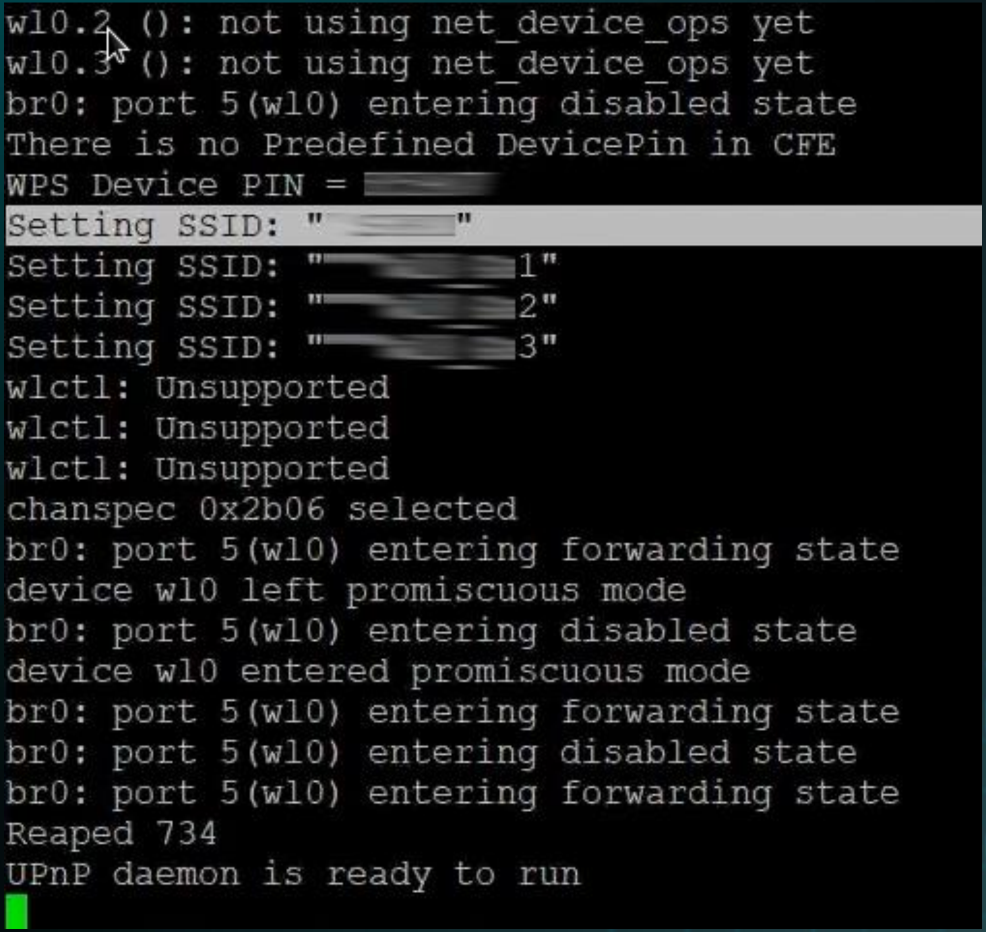
ROADSEC

Flipside



```
CFE version 1.0.37 for BCM947XX (32bit,SP,LE)
Build Date: Fri Nov 23 11:34:59 EST 2007 (tornado@dd-wrt.com)
Copyright (C) 2000,2001,2002,2003 Broadcom Corporation.

Initializing Arena
Initializing Devices.
Boot partition size = 262144(0x40000)
et0: Broadcom BCM47xx 10/100 Mbps Ethernet Controller 4.150.10.5
CPU type 0x29029: 240MHz
Total memory: 8192 KBytes

Total memory used by CFE:  0x80700000 - 0x807977D0 (620496)
Initialized Data:          0x8072E860 - 0x80730FB0 (10064)
BSS Area:                  0x80730FB0 - 0x807317D0 (2080)
Local Heap:                0x807317D0 - 0x807957D0 (409600)
Stack Area:                0x807957D0 - 0x807977D0 (8192)
Text (code) segment:       0x80700000 - 0x8072E860 (190560)
Boot area (physical):      0x006BF000 - 0x006FF000
Relocation Factor:         I:00000000 - D:00000000

Device eth0:  hwaddr 00-21-29-80-60-1E, ipaddr 192.168.41.1, mask 255.255.255.0
        gateway not set, nameserver not set
Loader:raw Filesys:tftp Dev:eth0 File:: Options:(null)
Loading: Failed.
Could not load :: Timeout occured
Loader:raw Filesys:raw Dev:flash0.os File: Options:(null)
Loading: .. 3856 bytes read
Entry at 0x80001000
Closing network.
Starting program at 0x80001000
```

ROADSEC 2023 15.07.23



```
wl0.2 (): not using net_device_ops yet
wl0.3 (): not using net_device_ops yet
br0: port 5(wl0) entering disabled state
There is no Predefined DevicePin in CFE
WPS Device PIN = [redacted]
Setting SSID: "[redacted]"
Setting SSID: "[redacted]1"
Setting SSID: "[redacted]2"
Setting SSID: "[redacted]3"
wlctl: Unsupported
wlctl: Unsupported
wlctl: Unsupported
chanspec 0x2b06 selected
br0: port 5(wl0) entering forwarding state
device wl0 left promiscuous mode
br0: port 5(wl0) entering disabled state
device wl0 entered promiscuous mode
br0: port 5(wl0) entering forwarding state
br0: port 5(wl0) entering disabled state
br0: port 5(wl0) entering forwarding state
Reaped 734
UPnP daemon is ready to run
```

ROAD SEC 2023

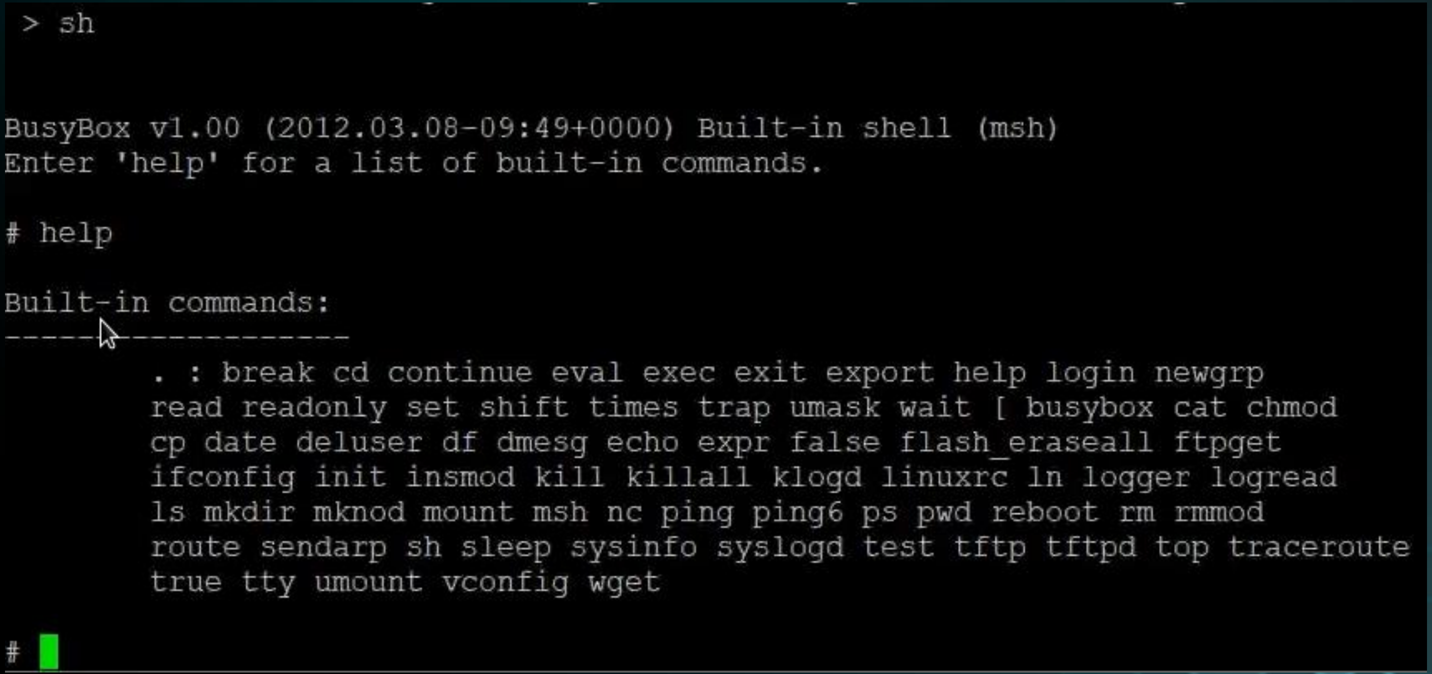
Flipside

TESTES COM ROTEADORES E DONGLE SERIAL/USB COM BUSYBOX - 01

QUARTA 05/04/2023 DAS 14H AS 19H (PODENDO SE EXTENDER A NOITE)

ROAD SEC 2023

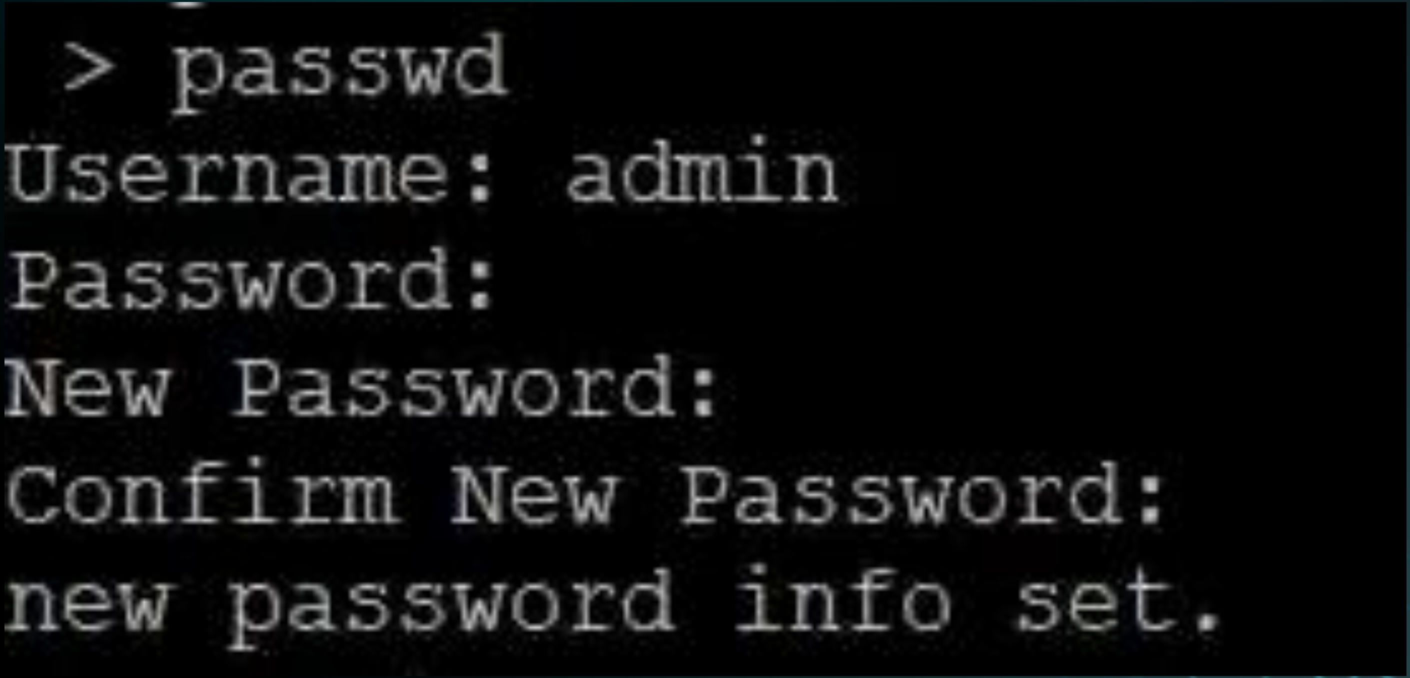
Flipside



```
 > sh


BusyBox v1.00 (2012.03.08-09:49+0000) Built-in shell (msh)
Enter 'help' for a list of built-in commands.

# help

Built-in commands:
-------------------
        . : break cd continue eval exec exit export help login newgrp
        read readonly set shift times trap umask wait [ busybox cat chmod
        cp date deluser df dmesg echo expr false flash_eraseall ftpget
        ifconfig init insmod kill killall klogd linuxrc ln logger logread
        ls mkdir mknod mount msh nc ping ping6 ps pwd reboot rm rmmod
        route sendarp sh sleep sysinfo syslogd test tftp tftpd top traceroute
        true tty umount vconfig wget

#
```

ROAD SEC 2023

Flipside



```
 > passwd
Username: admin
Password:
New Password:
Confirm New Password:
new password info set.
```

Site do ABC Makerspace - https://abcmakerspace.com.br/

Informações do Dumont Hackerspace - https://garoa.net.br/wiki/Dumont_Hackerspace_na_Campus_Party_2023

Blog do Sickeira - https://sickeira.blogspot.com/

Wikis de Dispositivos:
http://en.techinfodepot.shoutwiki.com/wiki/Main_Page
https://wikidevi.wi-cat.ru

MAIS UM EVENTO Flipside

REALIZAÇÃO Green Helmet

ROAD SEC 2023

O MAIOR FESTIVAL HACKER DA AMÉRICA LATINA

ROADSEC 15.07.23

Flipside

Sickeira

ABC Makerspace/WikiLab
Dumont Hackerspace
abcmakerspace@gmail.com

linkedin/abcmakerspace

instagram/abcmakerspace