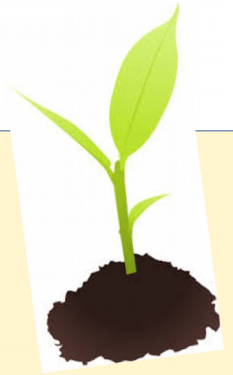
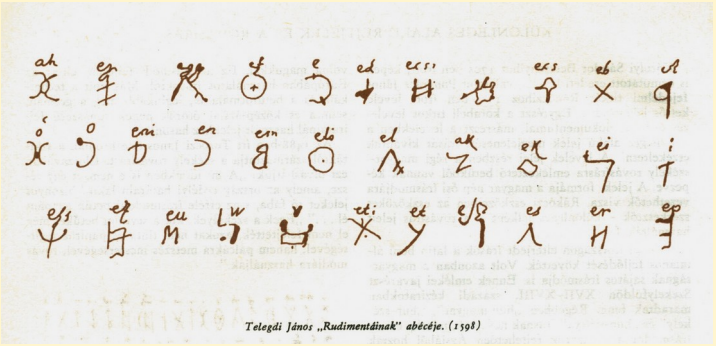
A brief introduction to firmware extraction

Pauline Bourmeau
@ko97551819

Who am I ?



- IT background
- Linguistics
- Use to be a teacher
- Passionate about human thinking and history



About Entry level tutorials serie

- Entry level
- Writing tutorials from field
- Publication
- Contribute
- Development
- A cycle

Our session today

1) Hardware care and tools
2) How to gather information about the hardware ?
3) Tooling for extraction
4) Software and configuration
5) Perform the extraction
6) Do the analysis
7) Prepare files for emulation

Our session today

1) Hardware care and tools
2) How to gather information about the hardware ?
3) Tooling for extraction
4) Software and configuration
5) Perform the extraction
6) Do the analysis
7) Prepare files for emulation

Hardware care and tools

- Target (NetGear router)
- Adapter UART-to-USB
- PC with Linux

My list of essentials:

Hearders

Soldering kit

Cables

Multimeter

Set of screwdrivers

Adhesive

A dentist appointment

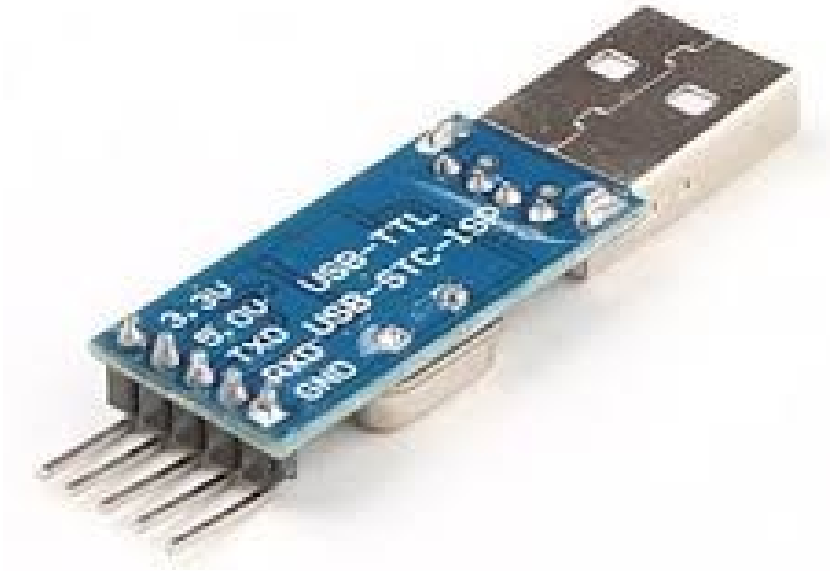
The target

- Netgear D300 router

?

UART-USB (TTL) adapter
SPI
Serial Port Interface

(Universal asynchronous receiver-transmitter)



Expl : Cost around 2 euros on eBay

UART

http://www.circuitbasics.com/basics-uart-communication/

- Universal Asynchronous Receiver Transmiter
- Transfert data over the data bus
- For Minicom configuration :
  - Bits of data
  - Parity bits
  - Stop bits
  - Baudrate

Our session today

1) Hardware care and tools
2) How to gather information about the hardware ?
3) Tooling for extraction
4) Software and configuration
5) Perform the extraction
6) Do the analysis
7) Prepare files for emulation

Netgear router

No usb

Simple home router (30€)

2 times for information gathering :

- By searching the Internet
- By opening it

1/2 Information gathering

Among some ideas :

Vendors website : Manual, documentation, pilotes

Search for any references, serial numbers, dates …

- Production informations
- Gives you other informations (pivoting)

With refs :

datasheets

technical descriptions (protocol implementations, versions, updates)

Commercial communication : expected device capabilities

Key-word search for similar research done: other works

1/2 Information gathering

Examples :

Production rules :

FCC (https://www.fcc.gov) - Federal Communications Commision

Community shared knowledge :

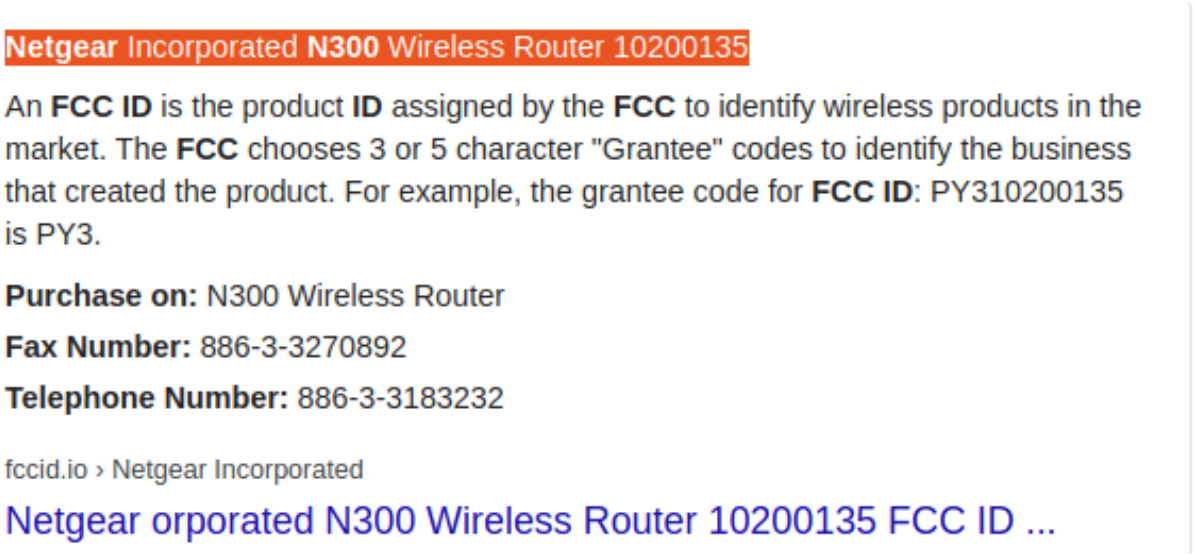
Dig Chip (https://www.digchip.com/) Electronic components databases

Open-source projects :

Open WRT (https://openwrt.org/) Free and opensource firmware for routers

FCC example

Google « Netgear N300 fcc id »



Go on fcc.gov

https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm

https://www.fcc.gov/oet/ea/fccid

FCC example

Pivoting : Google search --> FCC number --> Product code research → all about the device

OET Exhibits List

12 Matches found for FCC ID PY310200135

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
Attestation Statement Ad Hoc Declaration	Attestation Statements	09/15/2010	pdf	09/15/2010
Confidentiality Request	Cover Letter(s)	09/15/2010	pdf	09/15/2010
Cover Letter Agent Authorization	Cover Letter(s)	09/15/2010	pdf	09/15/2010
External Photos	External Photos	09/15/2010	pdf	09/15/2010
Label	ID Label/Location Info	09/15/2010	pdf	09/15/2010
Label Location	ID Label/Location Info	09/15/2010	pdf	09/15/2010
Internal Photos	Internal Photos	09/15/2010	pdf	09/15/2010
Operational Description	Operational Description	09/15/2010	pdf	09/15/2010
RF Exposure Info	RF Exposure Info	09/15/2010	pdf	09/15/2010
Test Report	Test Report	09/15/2010	pdf	09/15/2010
Test Setup Photos	Test Setup Photos	09/15/2010	pdf	09/15/2010
User Manual	Users Manual	09/15/2010	pdf	09/15/2010

For Software defined radio devices, search by Frequency

What about Europe ?

Our session today

1) Hardware care and tools
2) How to gather information about the hardware ?
3) Tooling for extraction
4) Software and configuration
5) Perform the extraction
6) Do the analysis
7) Prepare files for emulation

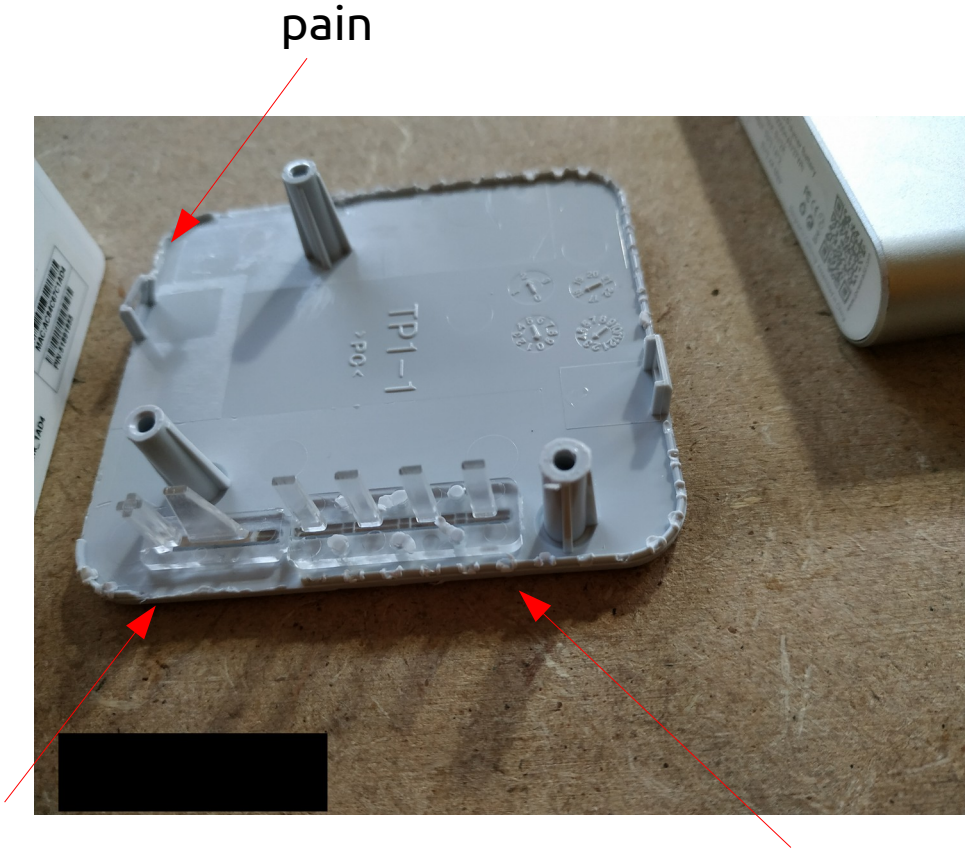
2/2 Information gathering

- Open, inspect, take pictures of components
  - More serial numbers for information collection
  - Is there any differences ? Versions by country ?
- Identify components and relations :
  - read the PCB
  - Search for serial pins

- Global understanding

Opening the box 1/3

Opening the box 2/2



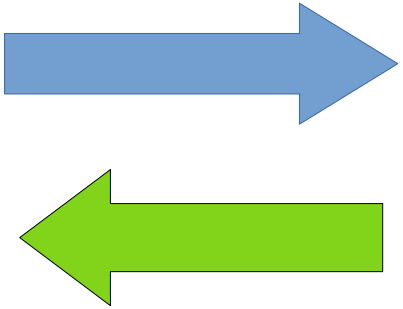
Our session today

1) Hardware care and tools
2) How to gather information about the hardware ?
3) Tooling for extraction
4) Software and configuration
5) Perform the extraction
6) Do the analysis
7) Prepare files for emulation

Serial communication interface

Hardware level

1 bit at a time, device to computer, here for debug purpose



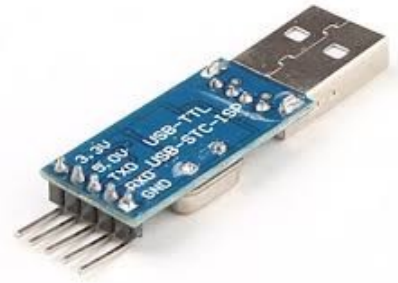
Transmit is TX, or TX0, TX1...

Receive is RX, RX0, RX1...

Or something else ! :)

Use TTL – as TTL Serial communication (transistor to transistor logic)

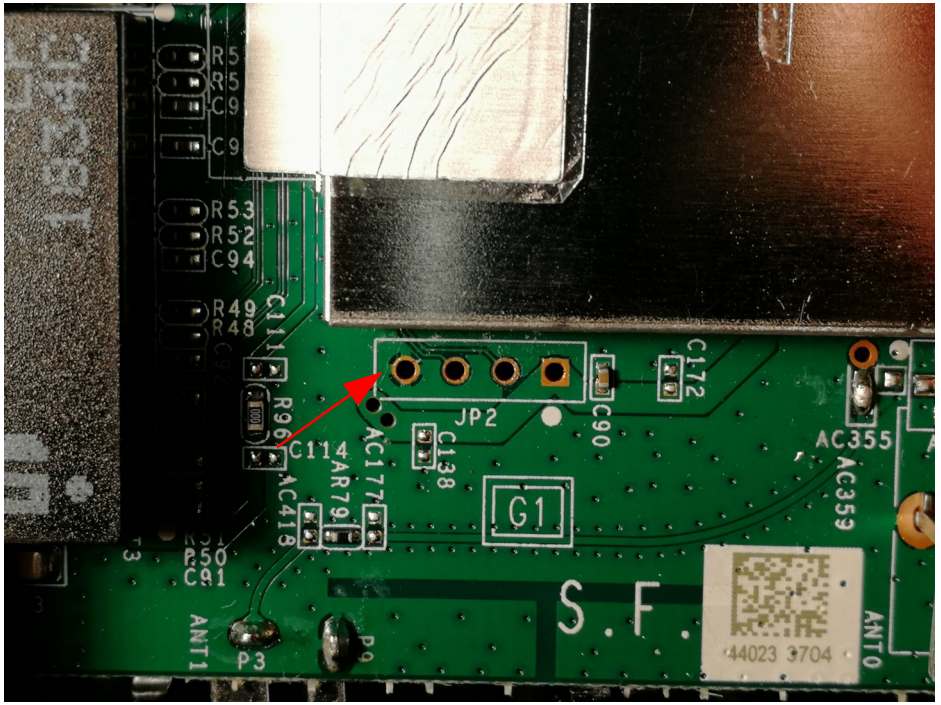
Need an Adapter :

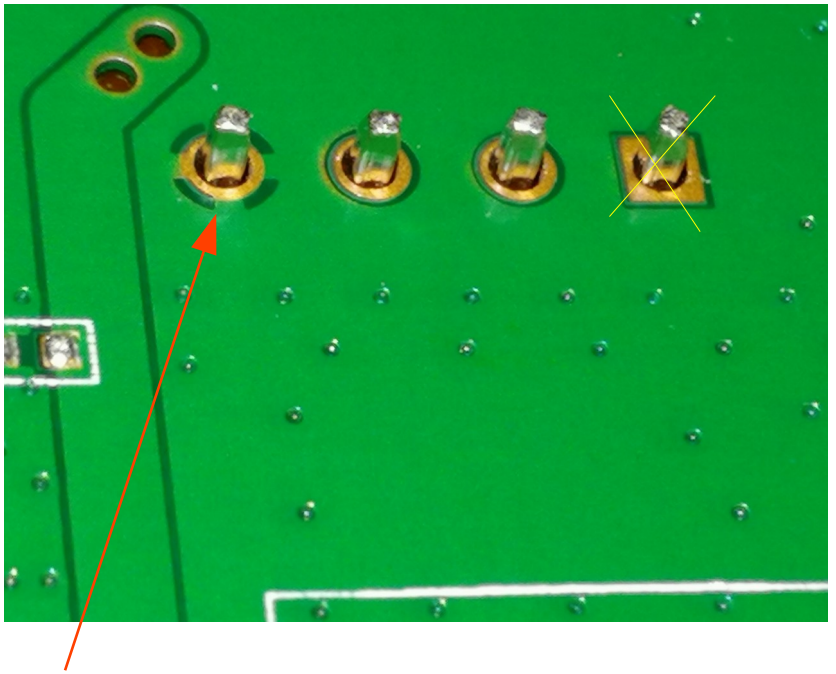


RX into TXD and TX into RXD

Find, identify, test, solder

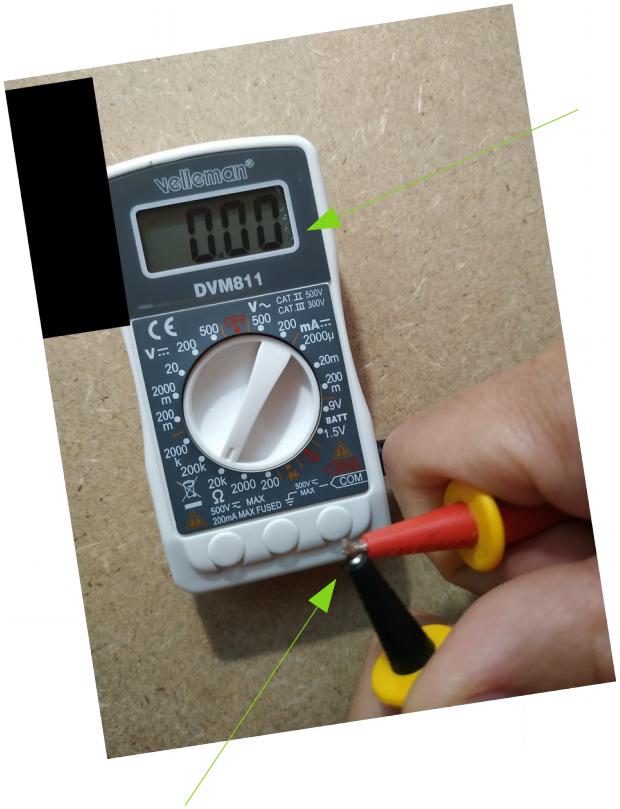
- Ground
- RX
- TX

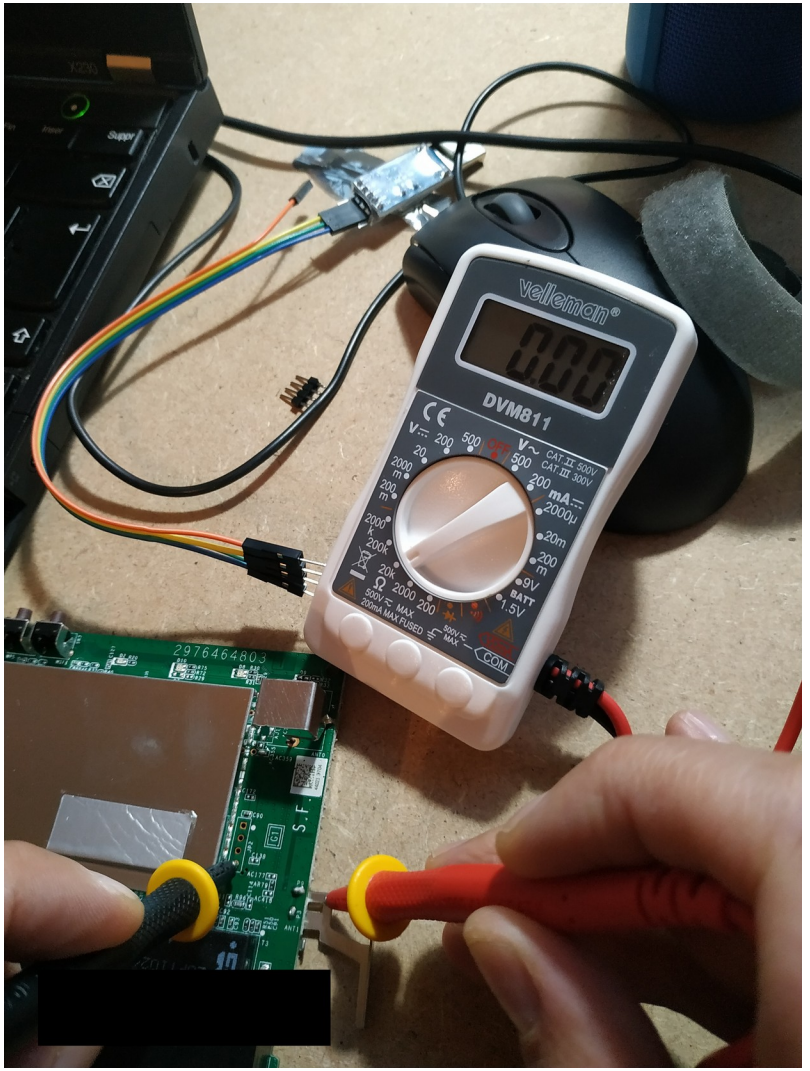




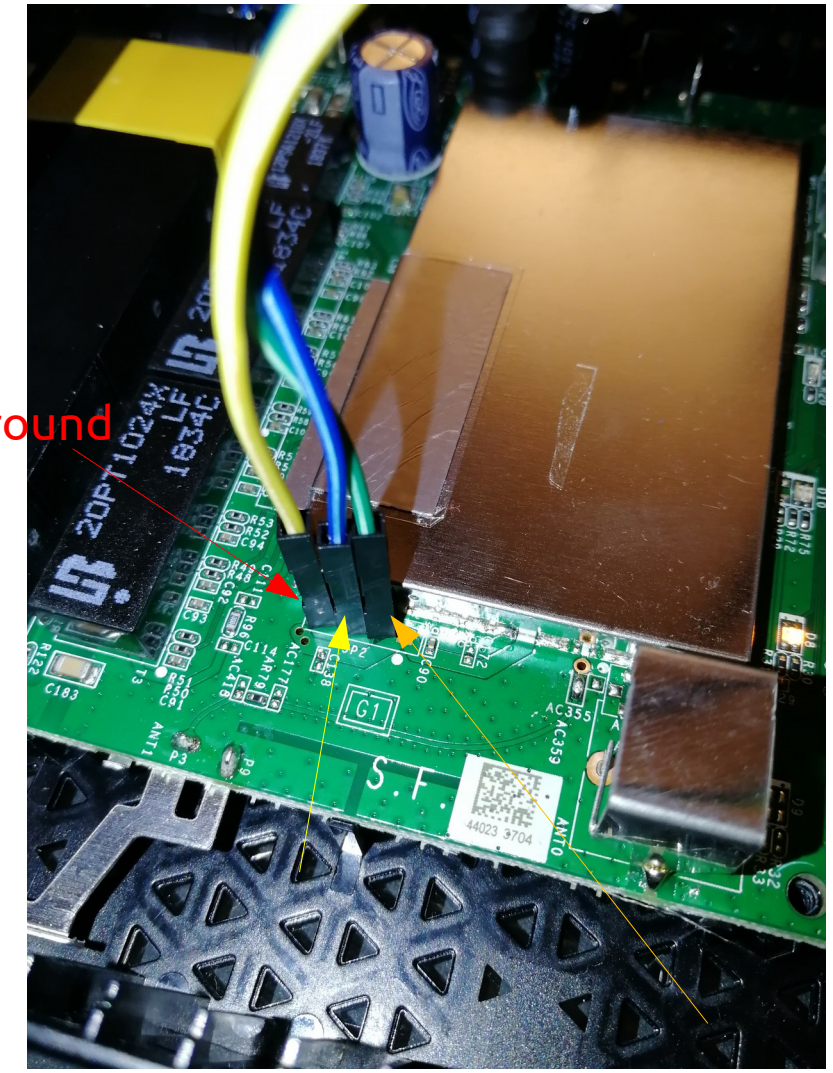
Find, identify, test, solder

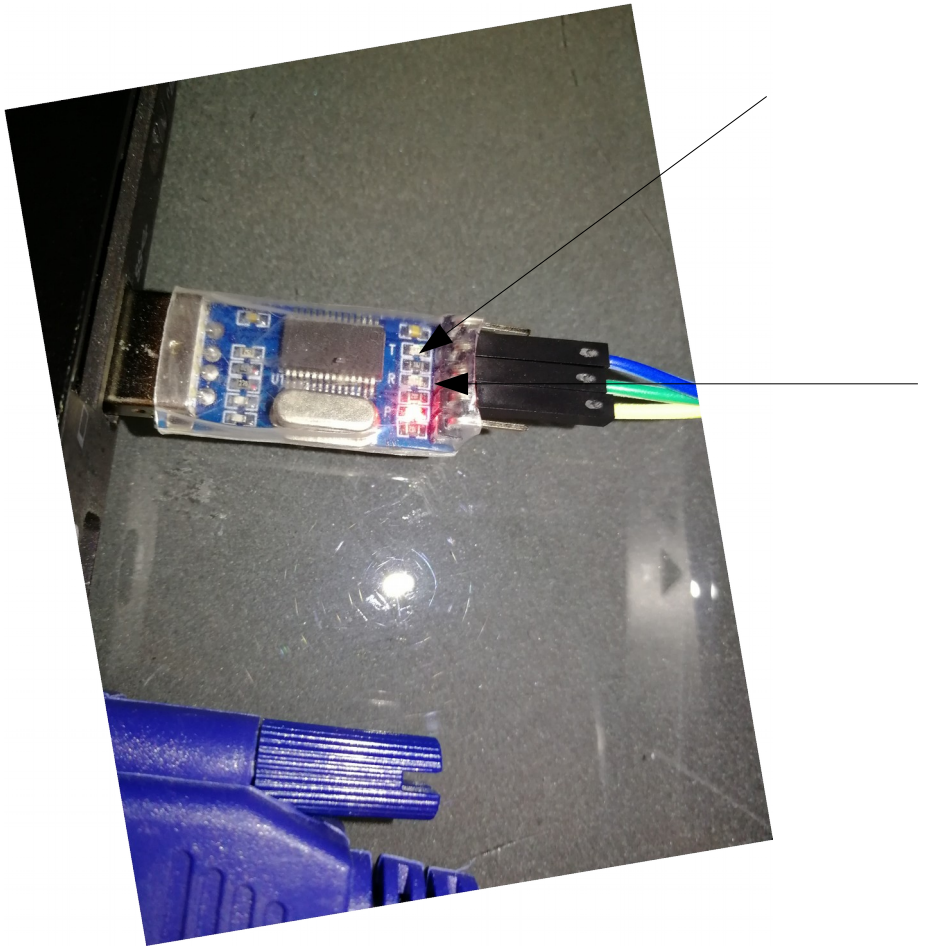
- Continuity test





connecting



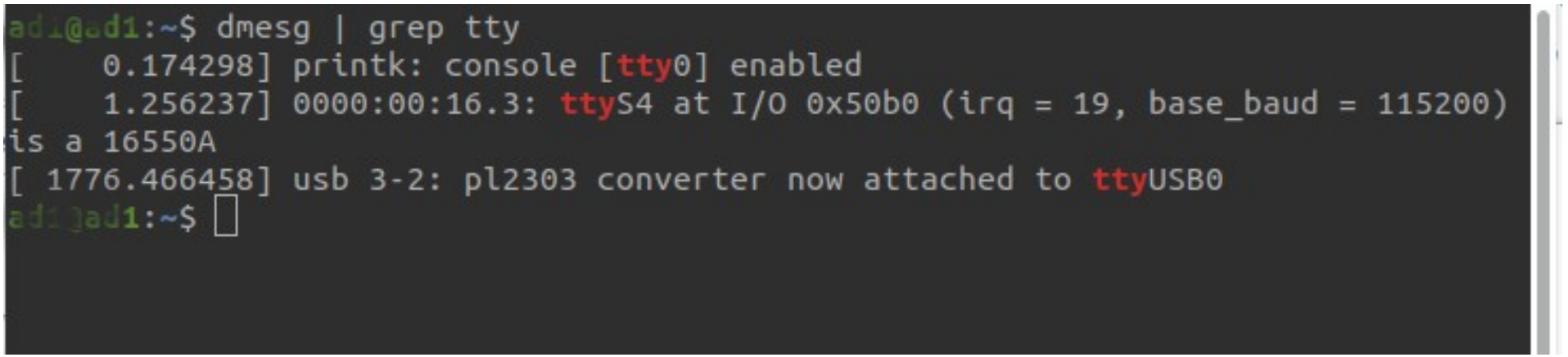


Our session today

1) Hardware care and tools
2) How to gather information about the hardware ?
3) Tooling for extraction
4) Software and configuration
5) Perform the extraction
6) Do the analysis
7) Prepare files for emulation

Is serial well connected ?

- Simple run dmesg command
- $ dmesg | grep tty
- Ls -l */dev/*tty*



Minicom

- Setting up a (remote) serial console
- Menu and options
- Runs in terminal
- Connect to embed linux (like) systems

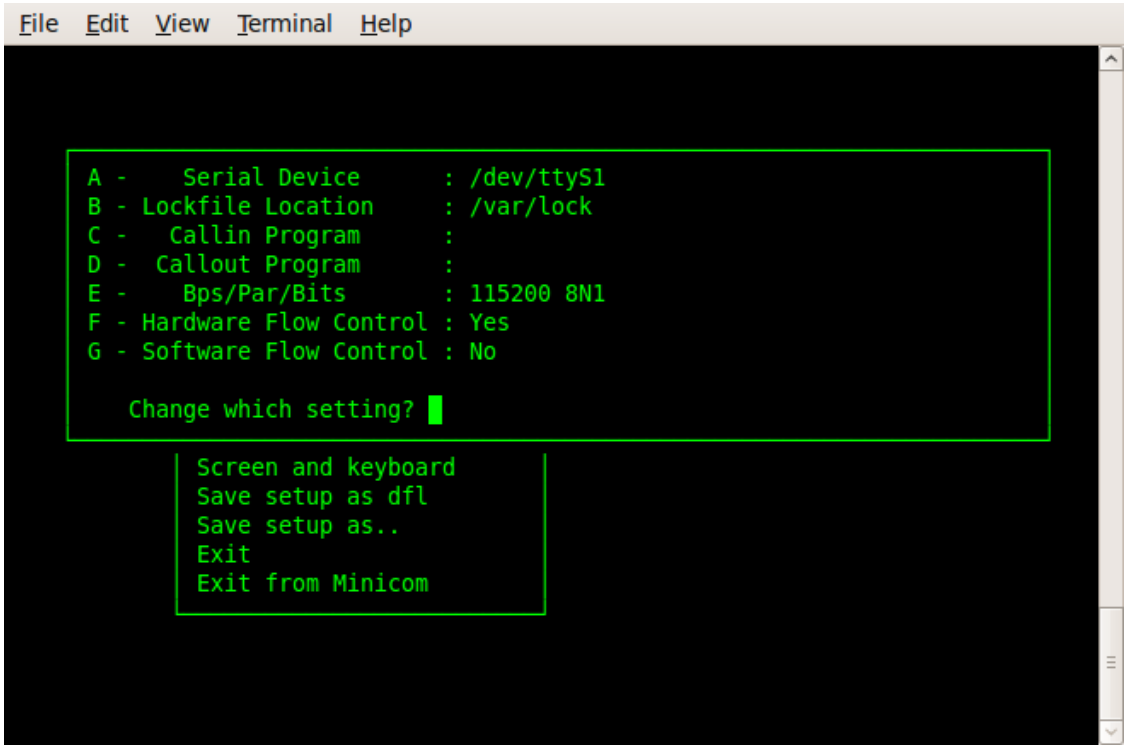


Image youtube.com

Transmission parameters

- Baudrates :
  - 38 400 baud
  - 57 600 baud
  - 115 200 baud

  Tranmission parameters are set over :
  - minicom [option]

- How fast the data is send over serial
- Test for most common
- Python script for this also :

  https://github.com/devttys0/baudrate

Our session today

1) Hardware care and tools
2) How to gather information about the hardware ?
3) Tooling for extraction
4) Software and configuration
5) Perform the extraction
6) Do the analysis
7) Prepare files for emulation

Extraction

- sudo minicom -b 115200 -D /dev/ttyUSB0
- Booting up, initialize
- Press Enter

  troubleshooting :
  - Nothing on the console ? Is the wiring ok ?
  - Nothing happen when press Enter ?
    - Check Minicom options (Control+A and O)

root@WNR2000v5:/#

Explore : what is there ?

- pwd
- cd
- ls -l
- mount
- ps

- cat */proc*/cmdline
  - Where is rootfs ?
- Cat *proc*/version

Take a look at mtdblocks :

- Cat */proc/partitions*
  - *Ls /dev/mtdblock**

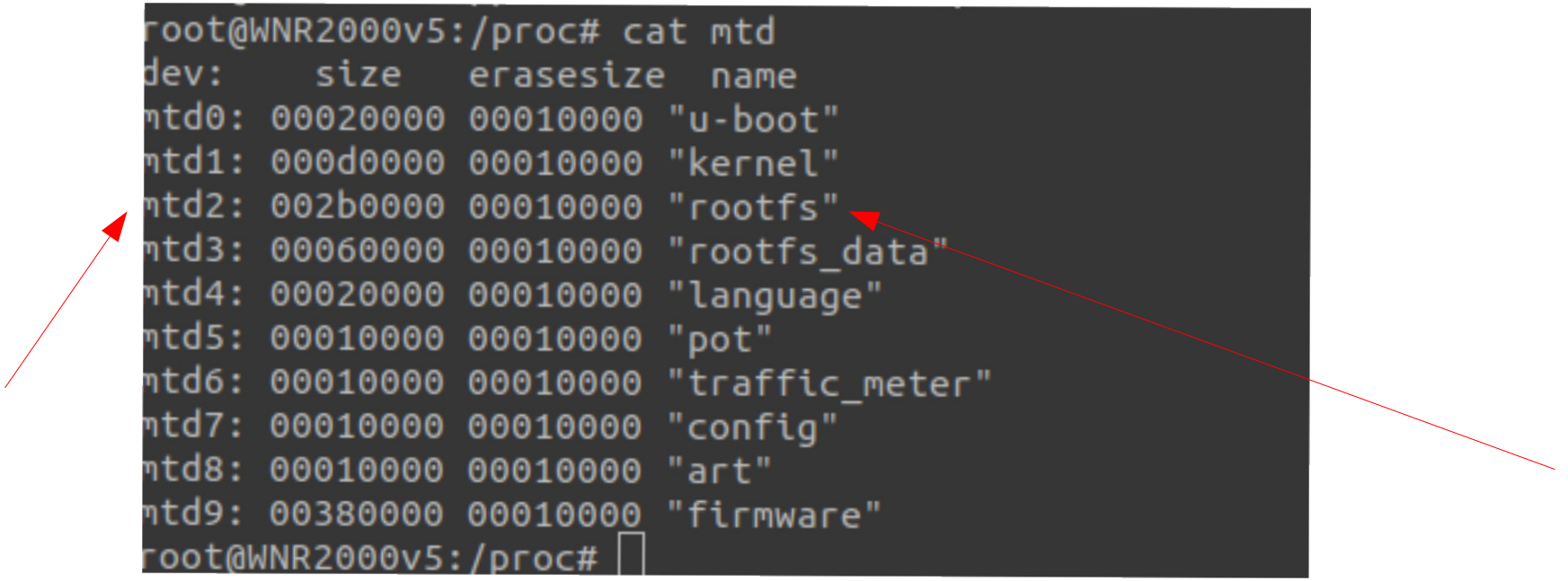
Flash memory

Mtdblock : Memory Technology Device subsystem for Linux
« emulate » block devices over MTD

Each block is « mounted »
/dev/mtdblock0

Searching for mtdblocks

- What are the names of mtdblocks we found ?
  - Cat */proc/*mtd
- What mtdblock do we want ?
- Remember where to find it ?



grabbing mtdblocks

How to extract mtdblocks?

How do extract

- Via USB
- Via the Network (wifi or Ethernet)

- Searching for binaries to run on the router : anything useful ?
- dd, nc are all I need
- No nc or netcat binary !

Well...

An old schooler

- TFTP
- Send to Target a netcat binary

Host ip 192.168.1.2, received via dhcp

Victim1 ip 192.168.1.1 (minicom), default ip address

On host

- On the target directory you want, copy the binaries you'll need :
  - Statically linked netcat binary (MIPS)
  - a TFTP Server (x86 statically linked binary also)

- Chmod +x tftpserver
- Run the server on port 6969
  - sudo ./tftpserver . 6969

On Target

- Connect to the target
- Go to /tmp directory
- Get the netcat binary
  - Tftp -g -r netcat 192.168.1.2:6969
  - Ls -la
  - Is there ?
    - Yes, chmod +x netcat

Transferring mtdblocks over UART

nc -nvv -l -p 4444 > mtdblock2.bin

/target
(where mtdblocks will arrive)
mtdblock2.bin

dd if=/dev/mtdblock2 | /*tmp*/netcat 192.168.1.2 4444

Did it work ?

```
[redacted]/Desktop/WORKSHOP/victim1$ ls -l
total 3056
-rw-rw-r-- 1 ad1 ad1 2818048 oct.  19 23:38 mtdblock2.bin
-rw-rw-r-- 1 ad1 ad1   65536 oct.  19 23:39 mtdblock7.bin
-rw-rw-r-- 1 ad1 ad1  177974 oct.  19 23:23 netcat
-rwxrwxr-x 1 ad1 ad1   58748 oct.  18 21:06 tftpserv
drwxrwxr-x 2 ad1 ad1    4096 oct.  19 22:49 tmp
[redacted]/Desktop/WORKSHOP/victim1$
```

Now analyse

Our session today

1) Hardware care and tools
2) How to gather information about the hardware ?
3) Tooling for extraction
4) Software and configuration
5) Perform the extraction
6) Do the analysis
7) Prepare files for emulation

Uncompress the filesystem

- File mtdblock2.bin
- Strings mtdblock7.bin
- Root unsquashfs mtdblock2.bin
  - Quick install of unsquashfs-tools with apt

- Ls
  - New folder : /squashfs-root !

And « voila ! »

```
:~/Desktop/WORKSHOP/victim1/squashfs-root$ ls -l
total 88
drwxr-xr-x  2 root root  4096 juil. 12  2018 bin
-rw-r--r--  1 root root    11 juil. 12  2018 default_language_versi
drwxr-xr-x  2 root root  4096 juil. 12  2018 dev
drwxr-xr-x 15 root root  4096 juil. 12  2018 etc
-rw-r--r--  1 root root     1 juil. 12  2018 firmware_region
-rw-r--r--  1 root root    10 juil. 12  2018 firmware_version
-rw-r--r--  1 root root    10 juil. 12  2018 hardware_version
drwxr-xr-x  2 root root  4096 juil. 12  2018 jffs
drwxr-xr-x  8 root root  4096 juil. 12  2018 lib
drwxr-xr-x  2 root root  4096 juil. 12  2018 mnt
-rw-r--r--  1 root root    10 juil. 12  2018 module_name
drwxr-xr-x  2 root root  4096 juil. 12  2018 proc
drwxr-xr-x  2 root root  4096 oct.  10  2017 rom
drwxr-xr-x  2 root root  4096 juil. 12  2018 root
drwxr-xr-x  2 root root  4096 juil. 12  2018 sbin
drwxr-xr-x  2 root root  4096 juil. 12  2018 sys
drwxrwxrwx  2 root root  4096 juil. 12  2018 tmp
drwxr-xr-x  7 root root  4096 juil. 12  2018 usr
lrwxrwxrwx  1 root root     4 juil. 12  2018 var -> /tmp
drwxr-xr-x  8 root root 16384 juil. 12  2018 www
~/Desktop/WORKSHOP/victim1/squashfs-root$
```

Identify the firmware

binwalk vs File : Bruteforce the file and find all headers
- risk of false flags
- give offsets (for copy)

file reads the header

mmls : list blocks and gives offsets

binwalk -e [file] : will extract

Mount -o loop,offset [filename] [mountpoint]

Our session today

1) Hardware care and tools
2) How to gather information about the hardware ?
3) Tooling for extraction
4) Software and configuration
5) Perform the extraction
6) Do the analysis
7) Prepare files for emulation