

Hardware Hacking for the Masses (and you!)



BusesCanFly

```
buses@slides:~$ cat ./boring_disclaimer.txt
```

- I am not a lawyer
- This presentation is just my view/experiences and those of friends around me
- We're all noobs!
- Be responsible and hack your own stuff
- Links for where to find the images used are in the last slide
- Have fun, don't be dumb, cite your sources.
- I am not a lawyer

buses@slides:~\$ whoami

- Just a noob exploring what I find fun
- {Embedded, Automotive} hardware hacker
 - Mostly a hobby
- Student
- Love rock climbing, quadcopter flying, and messing with electronics



```
buses@slides:~$ cat ./overview.txt
```

- What is hardware hacking?
 - What is hacking?
 - Making stuff do what it's not supposed to!
 - Dumping and learning all the secrets!
 - ~~General and absolute chaos~~
 - Very general idea with different areas
 - Some common ideas/concepts



In short, whatever you want it to be! If you can touch it, hack it, and have fun it's hardware hacking.

buses@slides:~\$ head -n 12 ./questions.*

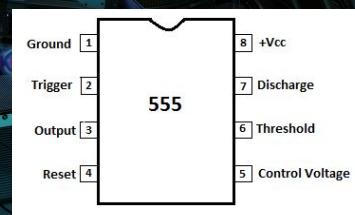


- Isn't hardware hacking hard?
 - No! ...yes?
 - (As with everything, it depends on what you do)
 - There is something for everyone
- Can I hack hardware?
 - **YES!**
- What do I need to get started?
 - Stay right where you are and you'll find out :)
- Is hardware hacking expensive?
 - A lot is possible for very little money

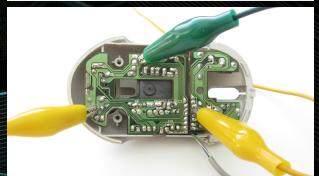
ebay

buses@slides:~\$ tail -n 10 ./how2learn

- Projects!
 - Arduino's
 - Raspberry pi's + similar SBC's
 - General electronics
 - Soldering
- Books
- Web resources
 - Youtube ([GreatScott!](#), [Electroboom](#))
 - Forums (Adafruit, Sparkfun)

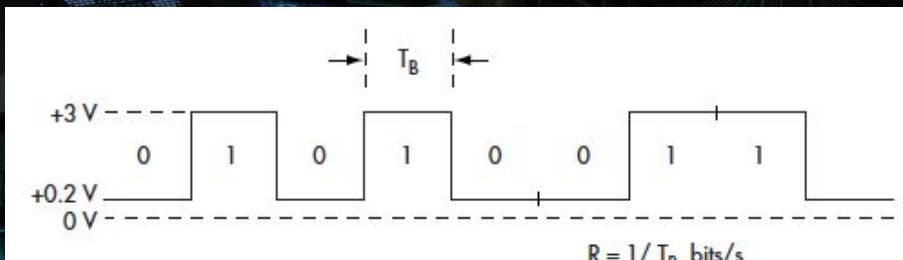
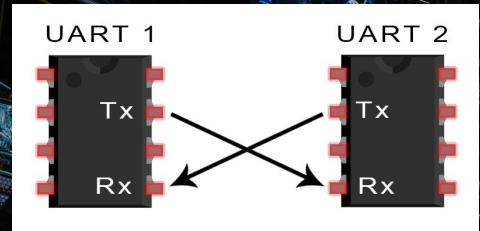


<https://makezine.com/projects/diy-hacks-how-tos-rapid-fire-mouse-button/>



buses@slides:~\$ tac ./things2know.txt | tac

- Baud rate
 - “The baud rate is the rate at which information is transferred in a communication channel.”
 - <https://www.setra.com/blog/what-is-baud-rate-and-what-cable-length-is-required-1>
 - 4800, 9600, 19200, 38400, 57600, 115200 (bits/sec)
- Common electronics terms
- Vcc: “voltage at the common collector.” (AKA power, (+), voltage)
- GND: Ground, (-)
- Rx: Receive
- Tx: Transmit



buses@slides:~\$ more ./RTFM.txt

- Incredible amount of information online
 - Datasheets (IC's, processors, etc.)
 - Schematics
 - FCC documents (!)
 - <http://fcc.io/>
 - RF information, internal pictures, specifications, etc.
 - Firmware (can also be dumped off hardware)

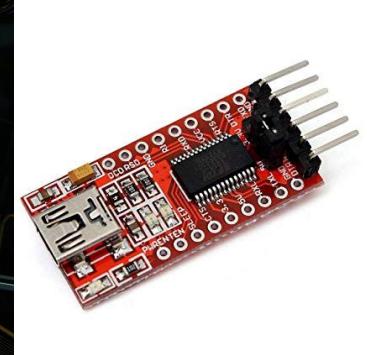
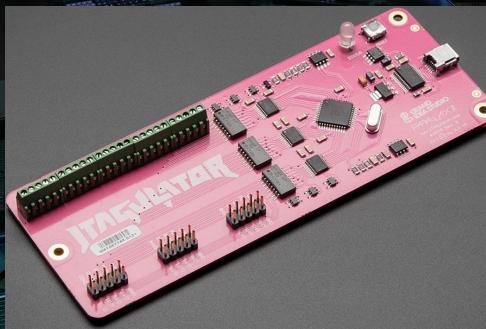
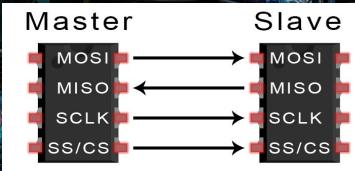


- Inspecting the hardware...



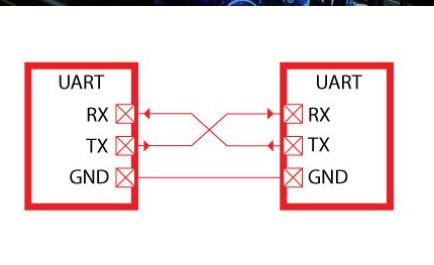
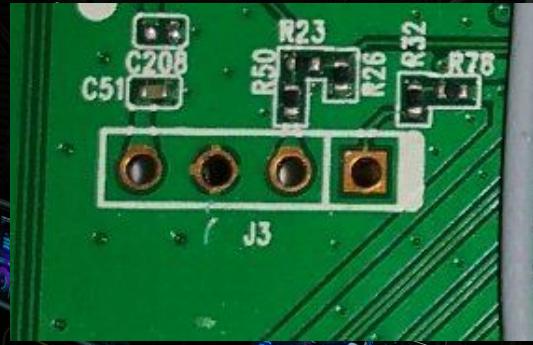
buses@slides:~\$ #What do I look for?

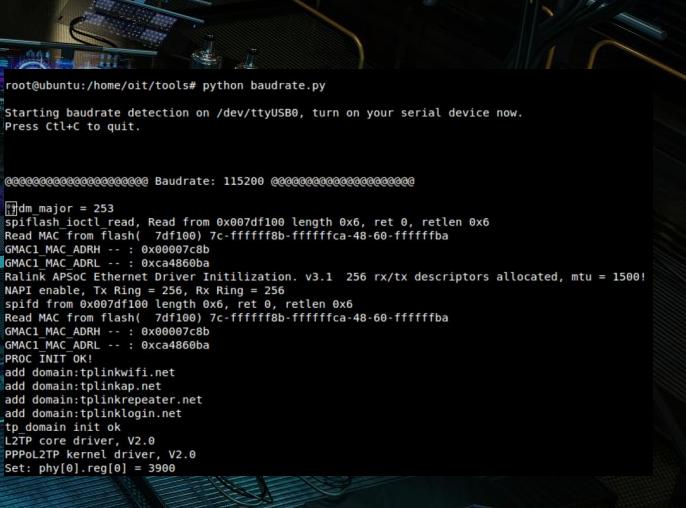
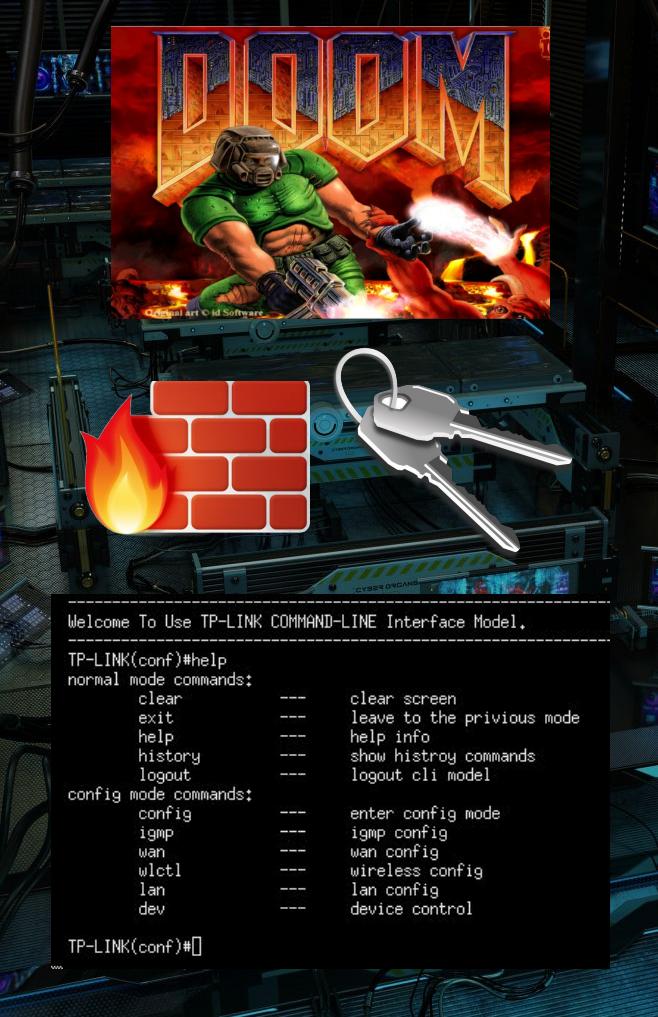
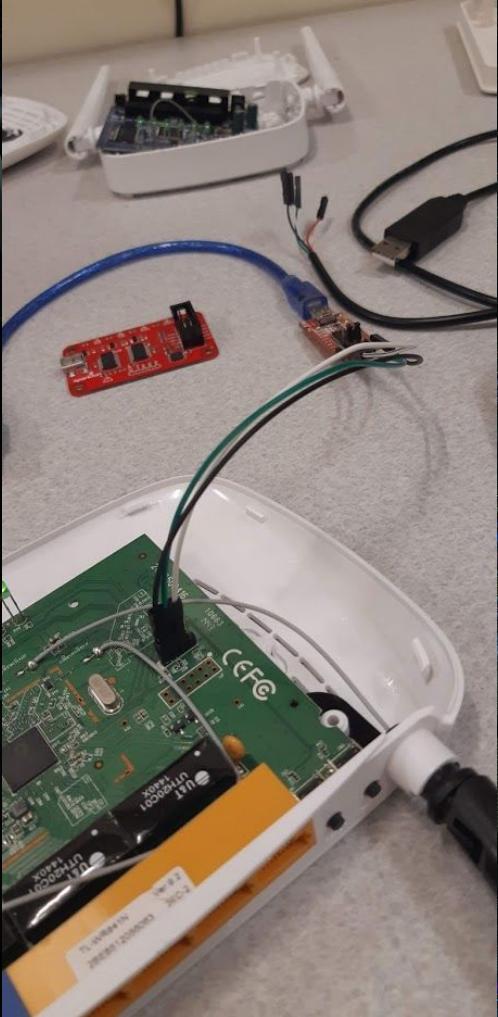
- “Debug interfaces”
 - Code has to be loaded somehow!
 - Devs need a way to see information or interact with the devices
 - Busybox? Limited shell? Custom sh? Root shell? ...Arch?
- How can we get the information?
 - UART, JTAG (pin layouts/hardware)
 - SPI, I2C/I²C, ... (communication protocols)
 - “Common” interfaces:
 - USB
 - Ethernet
 - Screen, Minicom, Miniterm, PuTTY
 - Need to know Baud Rate



buses@slides:~\$ more ./UART.txt

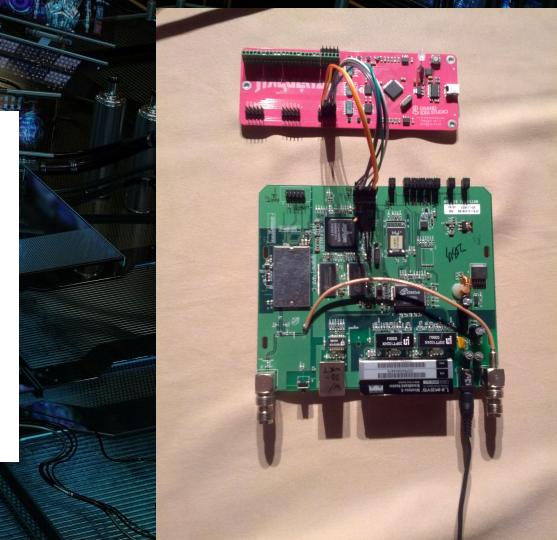
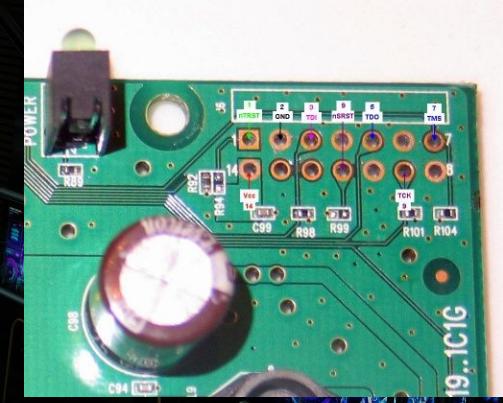
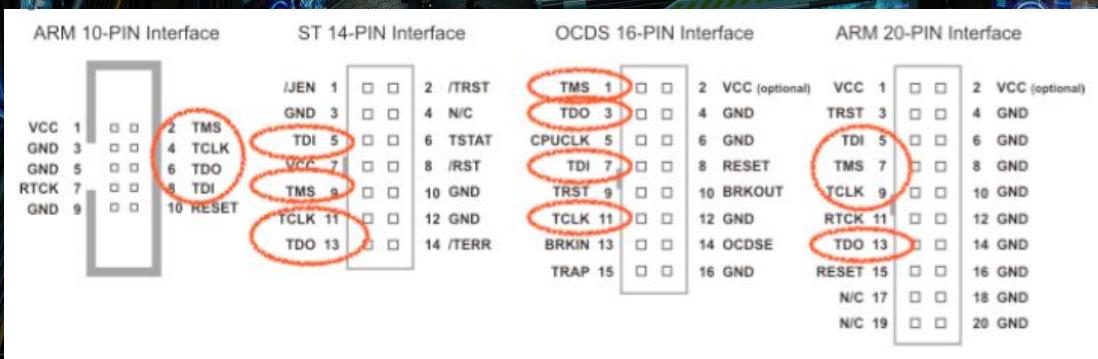
- “Universal Asynchronous Receiver/Transmitter”
 - Very common, and easy to use!
 - Generally 4 pins
 - ...but generally* don't connect Vcc
 - How do we identify them?
 - Trial and error
 - Small tricks
 - Ground is usually square (shared across board)
 - Vcc trace slightly thicker
 - Rx/Tx just guess
 - Oscilloscope
 - Logic analyzer

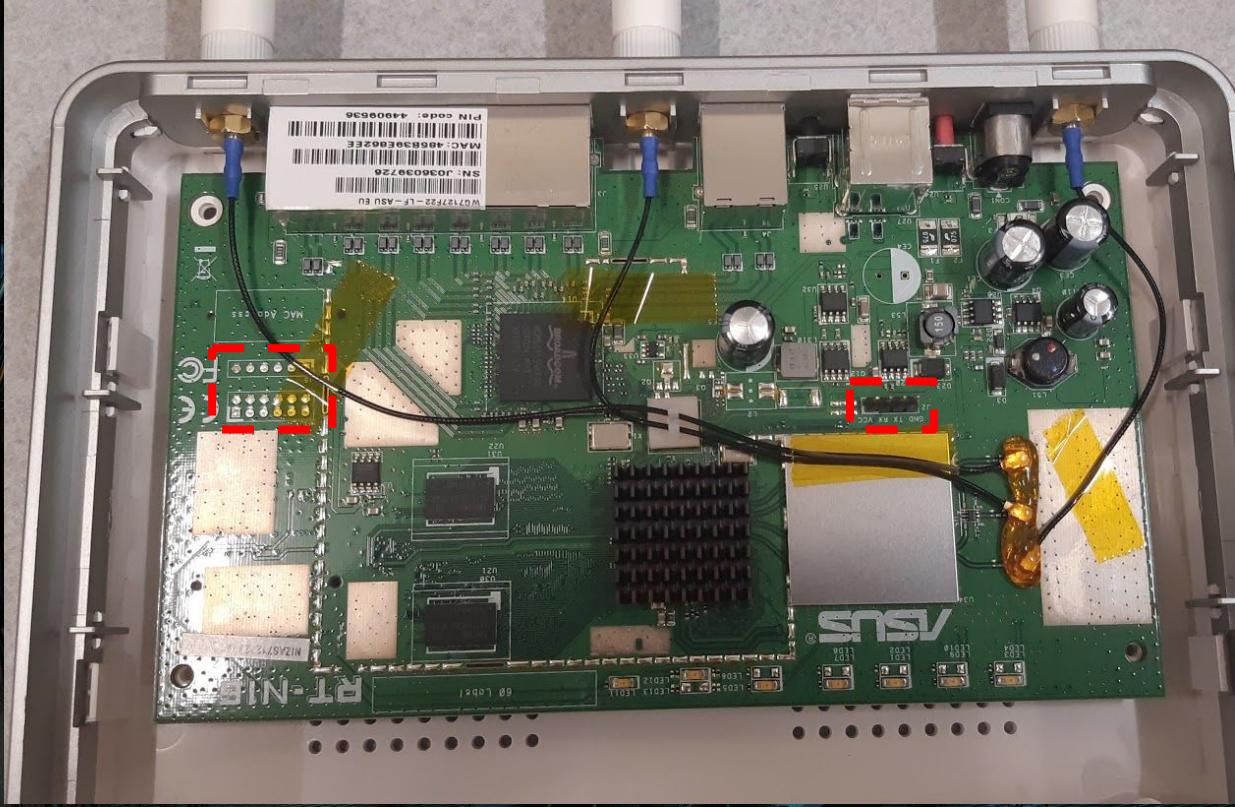




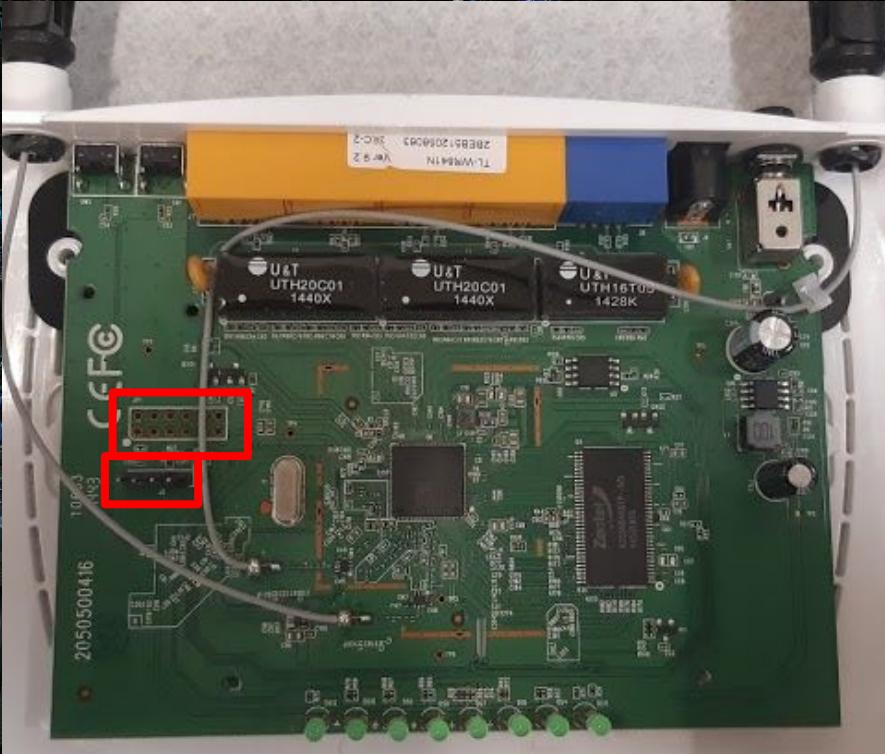
buses@slides:~\$ less ./JTAG.txt

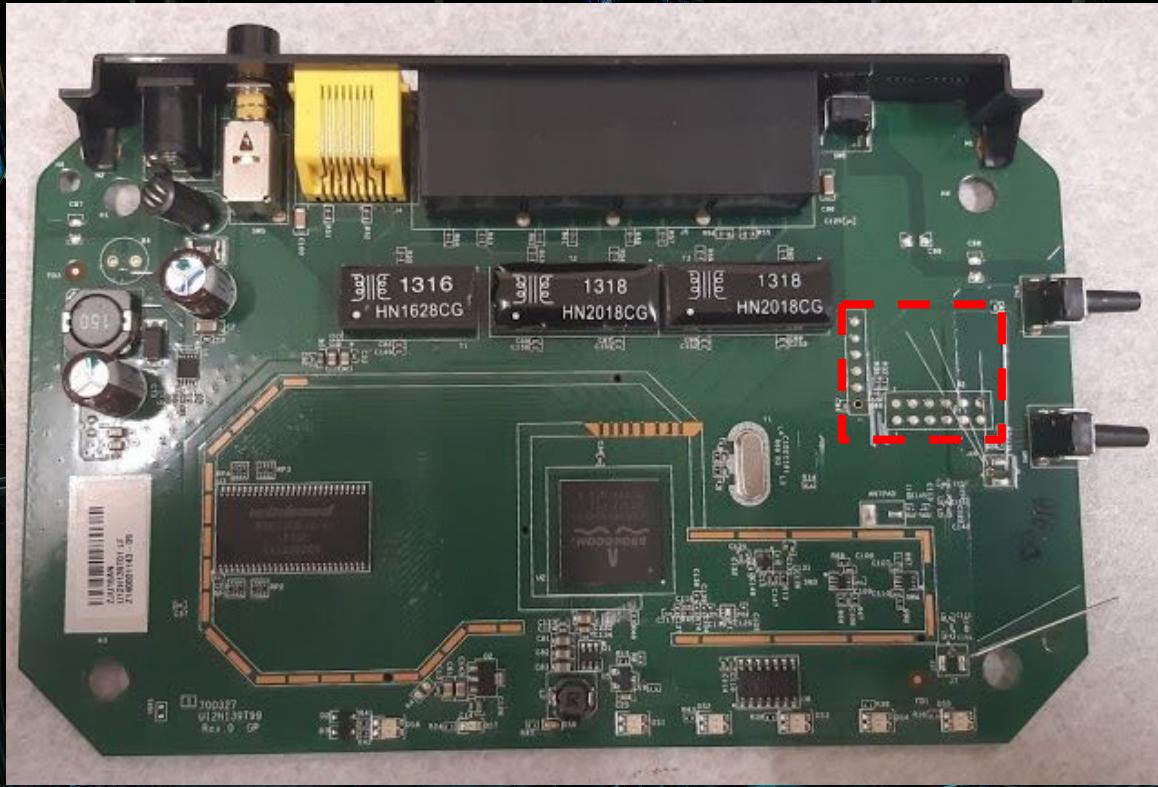
- “Joint Test Action Group”
- Pin count can vary but core ones stay the same
- Can be secured* with a key/password
- Hit or miss





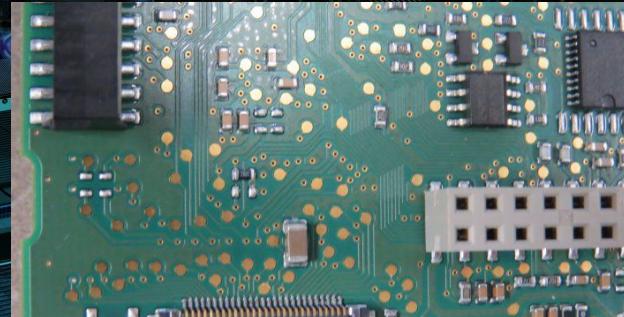
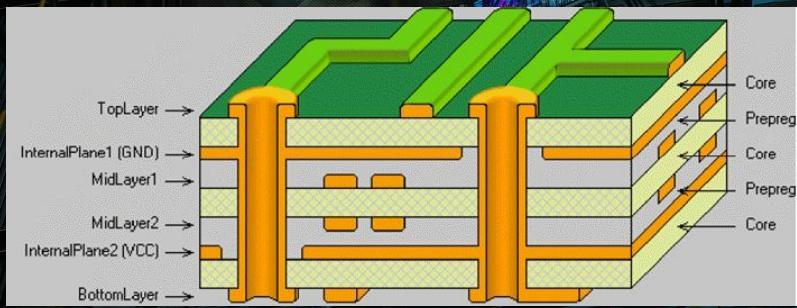
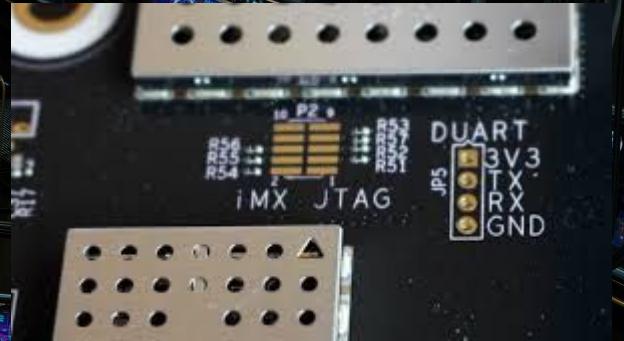






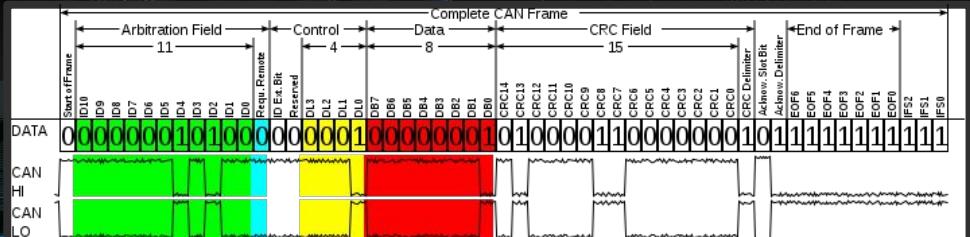
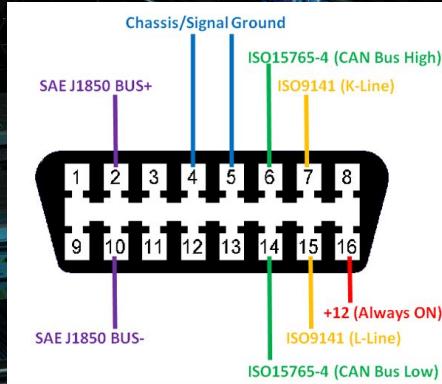
buses@slides:~\$ xdg-open ./weird/

- Lots of PCB standards/techniques
- Different formats and standards for interfaces
- Learn through experience!



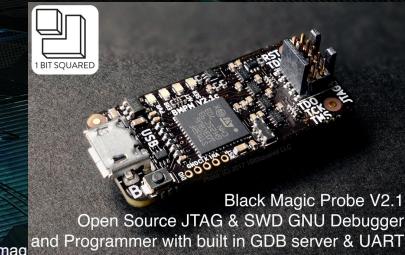
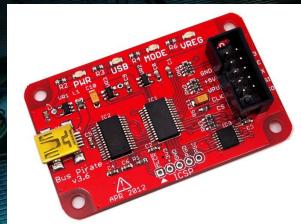
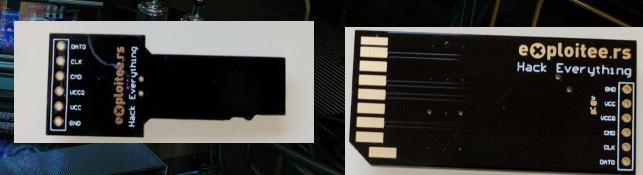
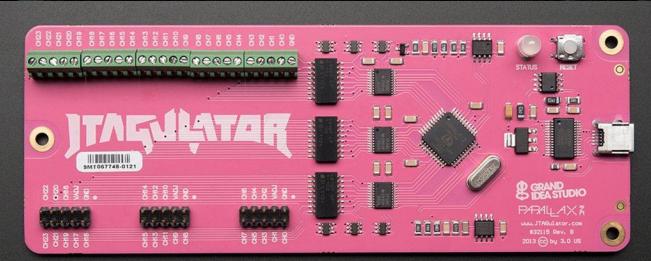
```
buses@slides:~$ cat ./explore.txt
```

- Automotive/Car hacking
 - IoT devices
 - ICS/SCADA equipment
 - Planes? Trains? Predator Drones?
 - Car chargers
 - Voting machines
 - Cell phones



buses@slides:~\$ open -t Tools.txt

- Connecting to all the things...
 - [Black Magic Probe](#) (JTAG/SWD adapter)
 - [JTAGulator](#) (Best friend for JTAG)
 - [Bus Pirate](#) (Hardware connection multi-tool)
 - [The Shikra](#) (Similar to bus pirate)
 - [UART cable\(s\)](#) (Cheap but trusty, very useful)
 - [Chip Whisperer](#) (For glitching and side channel attacks)
 - [greatFET](#) (Great video [here](#))
 - Logic analyzer [[Salea](#) is the god tier]
 - [bitmagic](#)
 - [CANable](#) [or [CANTact](#)] (Need an adapter cable to connect to OBDII ports)



Black Magic Probe V2.1
Open Source JTAG & SWD GNU Debugger
and Programmer with built in GDB server & UART

Imag

buses@slides:~\$ perl ./resource1.sh

- Getting started:

- <https://learn.adafruit.com>
- <https://learn.sparkfun.com/tutorials/where-do-i-start/all>
- <http://konukoii.com/blog/2018/02/16/5-min-tutorial-root-via-uart/>
- <https://blog.senr.io/blog/itaq-explained>
- <http://www.nicolascollins.com/texts/originalhackingmanual.pdf>
- <http://security.cs.rpi.edu/courses/hwre-spring2014/>

- Books:

- <https://nostarch.com/catalog/hardware-and-diy>
- <https://hackaday.com/2016/12/16/books-you-should-read-the-hardware-hacker/>
- <https://nostarch.com/hardwarehackerpaperback>
- https://books.google.com/books/about/Hardware_Hacking_Handbook.html?id=DEqatAEACAAJ



buses@slides:~\$ perl ./resource2.py

- Presentation/Talks/Slides...
 - Getting started with car hacking:
 - <https://www.youtube.com/watch?v=56LB7pTyax4>
 - Hardware hacking Defcon talks
 - Exploiters DC talks (!)
 - <https://youtu.be/S9MxbC0PO10>
 - <https://www.youtube.com/watch?v=h5PRvBpLuJs>
 - <https://www.defcon.org/images/defcon-12/dc-12-presentations/Fullam/dc-12-fullam.pdf>
 - <https://www.youtube.com/watch?v=l8yVaYpWDxE>
 - <https://www.youtube.com/watch?v=B8DjTcANBx0>
 - Samy Kamkar's hardware hacking talk:
 - <https://www.youtube.com/watch?v=tlwXmNnXeSY>



buses@slides:~\$ perl ./resource3

- IfNotPike's collection of SDR/radio/RF resources
 - <https://github.com/notpike/SDR-Notes>
- Samy Kamkar's array of projects
 - <https://samy.pl>
 - <https://www.youtube.com/user/s4myk>
- BLE ctf:
 - https://github.com/hackgnar/ble_ctf
- MG's amazing work:
 - <https://github.com/O-MG/DemonSeed>
- UART examples:
 - <https://www.davidsopas.com/using-uart-to-connect-to-a-chinese-ip-cam/>
 - <https://www.blackhillsinfosec.com/how-to-hack-hardware-using-uart/>



buses@slides:~\$ Shout-outs

- My amazing friends, family, teachers...
- The [@thugcrowd](#) crew
- The [SAE Cyberauto](#) event
- The car hacking village
- Bugcrowd
- Rqu, Specters, Soups, Deker, Eiais, DocProfSky, Butterfli
- You know who you are



THUGCROWD RADIO | TUESDAYS AT 9:30 PM EST



TWITCH | TWITTER | GITHUB | THU.GG | PATREON | INSTAGRAM | PERISCOPE | SNAPCHAT

Join us every week for live discussions on hacking, phreaking, and everything that DOESNT SUCK in infosec!

Images

- <https://commons.wikimedia.org/wiki/File:Arduino-uno-perspective-transparent.png>
- <http://pluspng.com/raspberry-pi-png-4298.html>
- <https://www.tp-link.com/us/support/faq/46/>
- <http://www.repeater-builder.com/motorola/qp68/qp68-overview.html>
- <https://fccid.io/M9MRDR6X8X/Label/FCC-ID-Label-1281984>
- https://www.adafruit.com/product/954?gclid=EA1aiQobChMizMfKnMiE5QIVTuDICh2RUg-iEAQYAIABEgKvyPD_BwE
- http://www.flupzor.nl/2015/04/30/root_on_ac750.html
- <http://konukoii.com/blog/2018/02/16/5-min-tutorial-root-via-uart/>
- <https://www.pond5.com/stock-footage/10749013/zapping-exploding-electronic-circuit-board.html>
- https://hackaday.com/2013/08/04/def-con-tamper-evidence-contests-and-embedded-talks/img_20130803_183741/
- <https://blog.senr.io/blog/jtag-explained>
- <https://www.mattcarrier.com/post/hacking-the-winkhub-part-1/>
- <https://electronics.stackexchange.com/questions/79224/what-parts-would-one-typically-use-for-automated-pcb-testing>
- <https://www.allaboutcircuits.com/technical-articles/which-via-should-i-choose-a-guide-to-vias-in-pcb-design/>
- <https://components101.com/connectors/obd2>
- <https://www.polygon.com/2018/12/10/1813430/sigil-doom-sequel-john-romero-release-date-price>
- <https://www.agcnetworks.com/in/a-guide-to-choosing-the-right-firewall-2/>
- <https://boingboing.net/2019/09/27/dumpster-fires-r-us.html>