Reverse engineering

Freiraum
25.1.2018

What? Reverse engineering

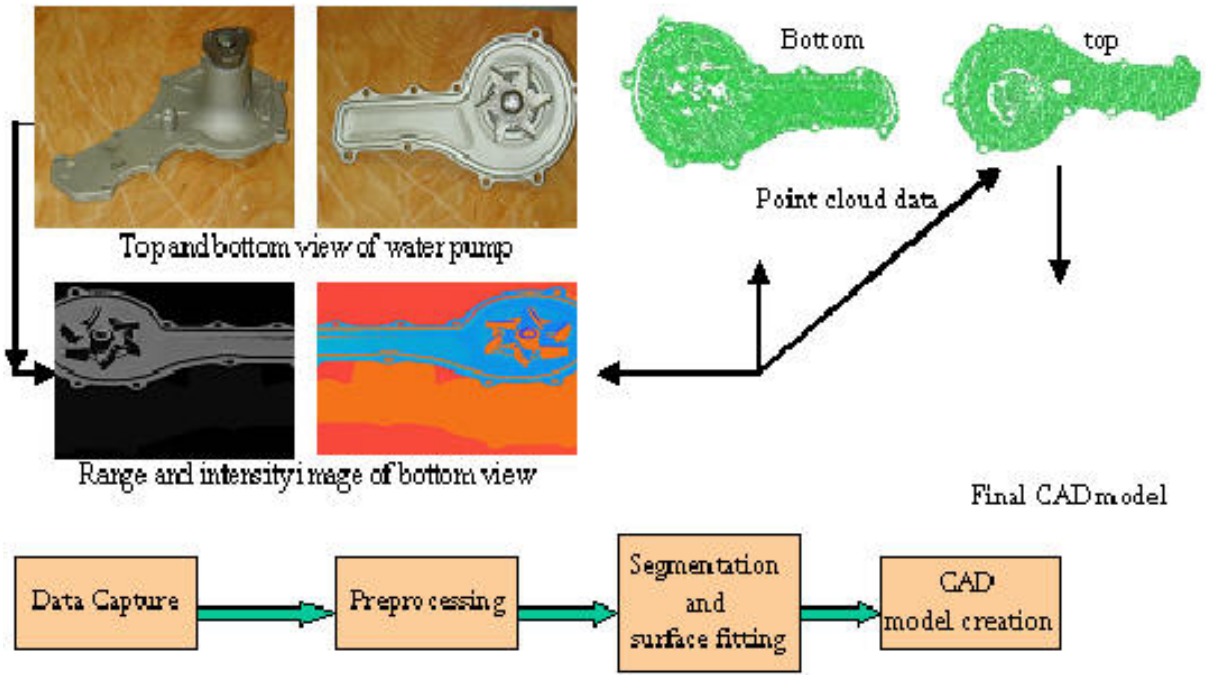
- Trying to found out how something is made
  - Usually everything is closed source
- Ready made object
  - Device, Hardware, Chemical
  - Software
- Object can be almost anything
  - Car, Router, Clock, Telephone
  - Software inside it
- How is it made?

Why?

- Curiosity, how it is made
- Trying to fix it
- Copy it
- How secure it is analysis

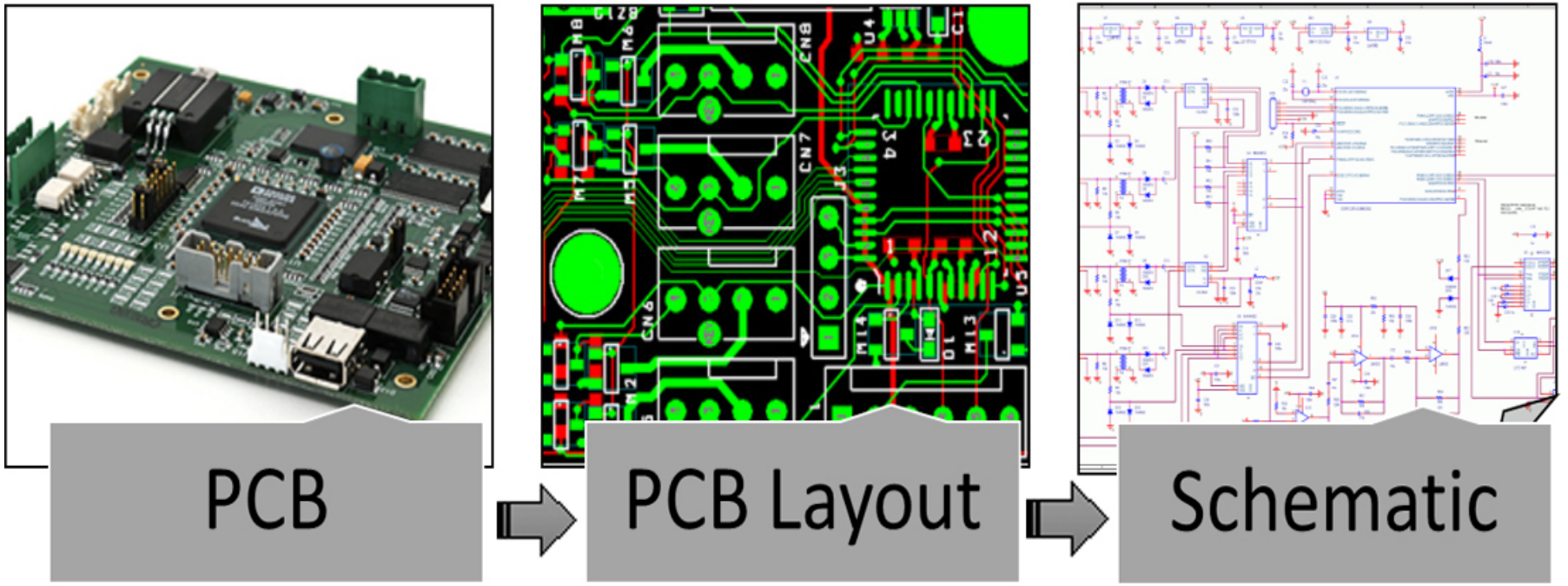
How - Mechanical

- Mechanical reversing
  - Tear down and Scanning
    - Many standard components
  - Possible to make CAD Model



How - Electrical

- Electrical (Circuit Board) Reversing
  - Many standard components
  - Possible to make Circuit Diagram (Schematic)



How - Software

- Software is in many cases the most interesting part of reversing
- Almost all devices nowadays have electronics and software
  - Look around
    - Car, Printer, Laptop, Monitor, (WLAN-)Router, Radio, Watch
    - Mobile Phone
- Software is the thing that makes difference
  - Almost always Closed Source
  - Is it secure?
  - New features?

How - Software

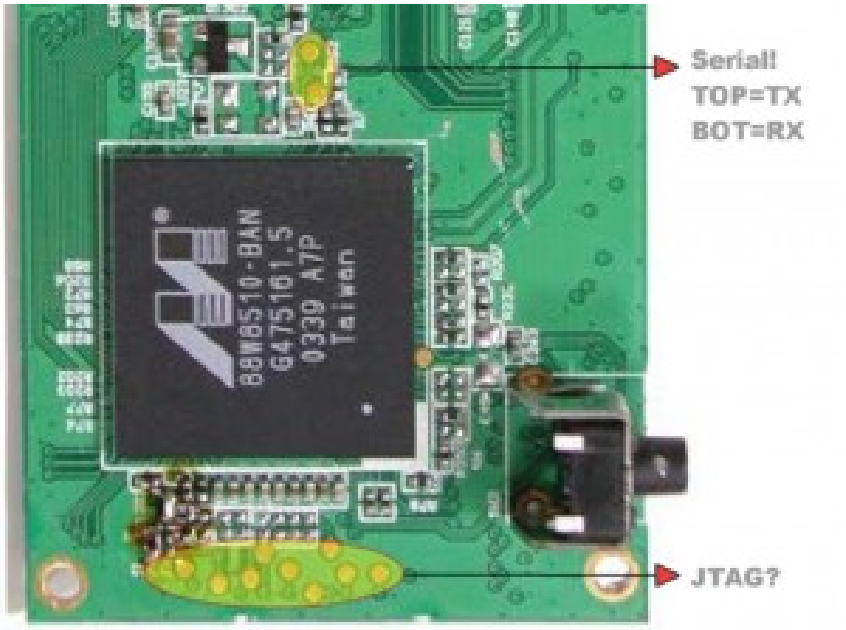
- Many Possibilities to get the software out of the device
- Interfaces
  - Usual User Interfaces
    - Display, Keys
  - Usual Data Interfaces
    - Network (Ethernet, WLAN, Bluetooth)
    - USB/Seriel
    - OBD (Cars)
  - Hidden (Usually on PCB)
    - UART
    - JTAG
    - SPI
    - BDM (Cars)

Look at PCB

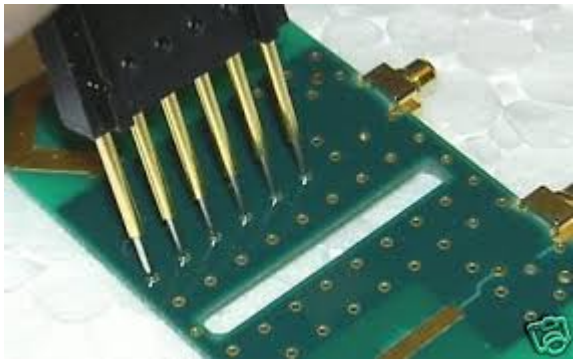
- Look for connectors
- Might be unpopulated

- Possible to solder connectors by yourself

Look at PCB



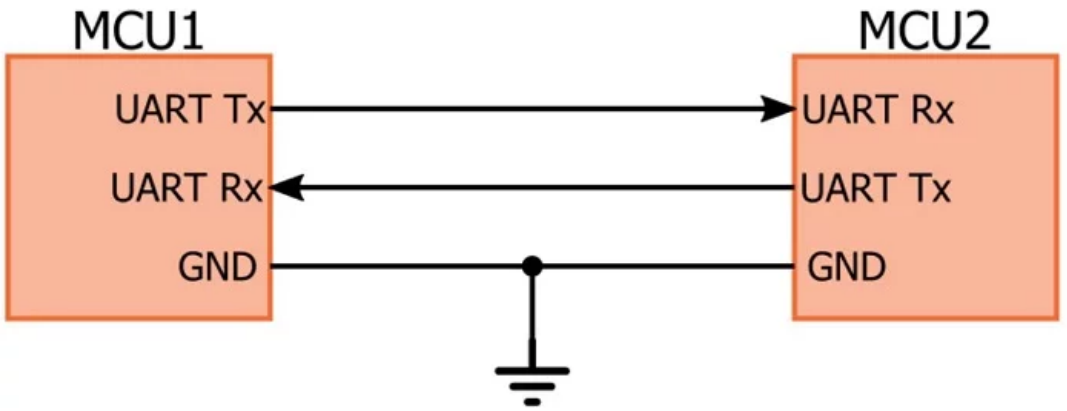
- Look for connectors
- Might be unpopulated



- Spring loaded connectors

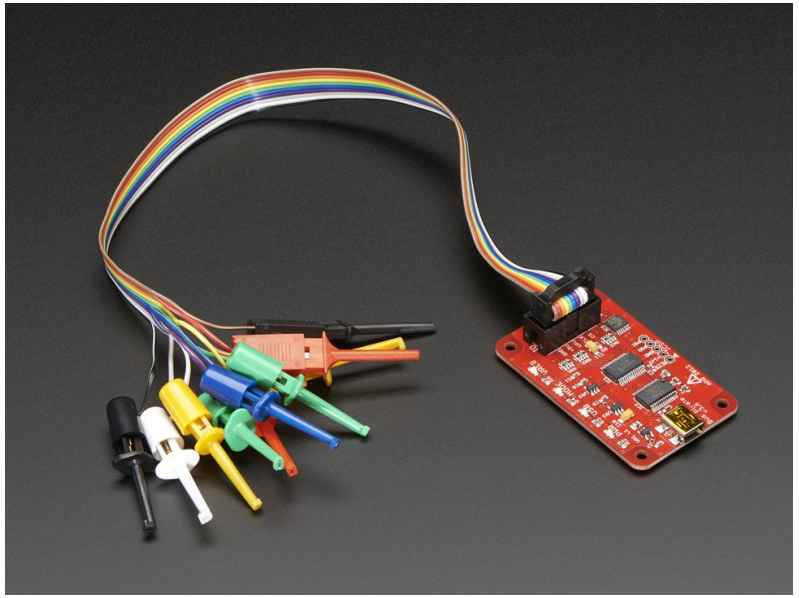
How - PCB

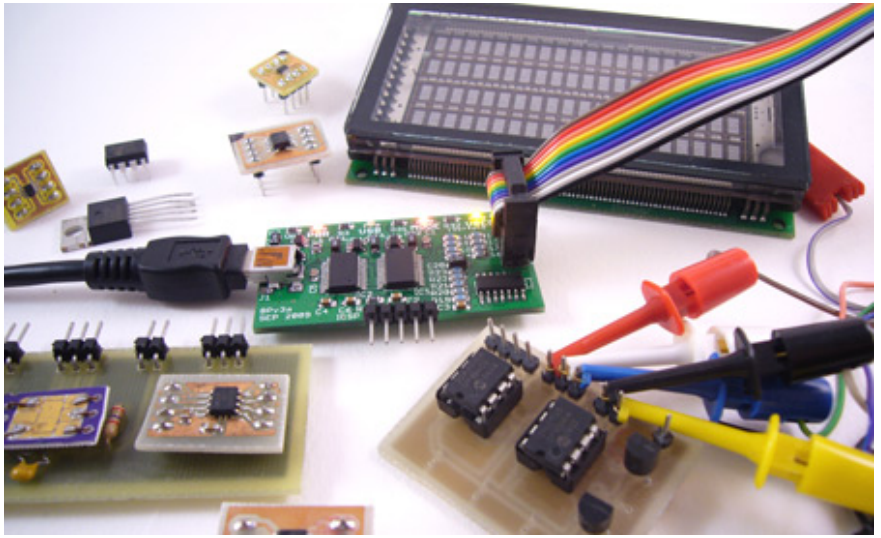
- UART / Serial Port is common
  - universal asynchronous receiver-transmitter (UART)
  - Typically console (e.g. Linux shell) over Serial/UART



UART

- Devices like Bus Pirate can be used to connect to UART





Example WRT54G

- Classical WLAN-router
- “Mother” of OpenWRT