



# Hardware Reverse Engineering Course

2019 Student Workbook

June 25, 2019

Bill Hass

<b>Welcome</b>	<b>3</b>
Covered Topics	3
Introduction	3
Basic Tools	7
Advanced Tools	9
<b>First Contact (~30 minutes)</b>	<b>10</b>
Visual Survey	11
Chip Identification	12
Passive Probing	13
<b>Hardware Modification (~30 minutes)</b>	<b>14</b>
Soldering Basics	14
<b>With Power Comes Responsibility (~90 minutes)</b>	<b>16</b>
Multimeter Probing	17
Oscilloscope and Logic Analyzer Probing	17
UART Probing	19
On-Chip Debugging - Memory Read/Write	24
<b>Extras</b>	<b>28</b>
Fun HW Hacks	28
Upgrade Bus Pirate Firmware	28
Using the FTDI Cable	30
JTAG with a Bus Pirate	30
<b>Glossary</b>	<b>31</b>

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Copyright © 2019, 2017 Bill Hass; Copyright © 2017 Russ Bielawski

# 1. Welcome

## 1.1 Covered Topics

*What topics are covered?*

In this class, we will cover the following hardware topics:

- Basic use of electronics tools:
  - Multimeter
  - Soldering iron
  - Bus Pirate
  - Oscilloscope
  - Logic analyzer
  - Serial interface device
  - On-chip debugger & programmer
- Circuit identification – The process of reconstructing knowledge about the circuitry on the printed-circuited board (PCB) of the victim hardware.
- Board modification – The process of modifying the PCB to enable breakout of interesting signals or change functionality to assist in hardware reverse engineering. For this class, this means light soldering.
- Serial data interfacing – The process of identifying interesting serial data interconnects on the victim hardware and tapping into them for inspection, analysis and, possibly, injection of commands or data.
- In-circuit debugging – The process of attaching to the built-in debugging circuitry in the board and/or processor(s) and accessing memory and controlling the processor in real-time.

*Are there CTF challenges related to this class?*

Why yes, there are! Each section will have a list of related CTF goals and their corresponding points.

## 1.2 Introduction

*What is reverse engineering?*

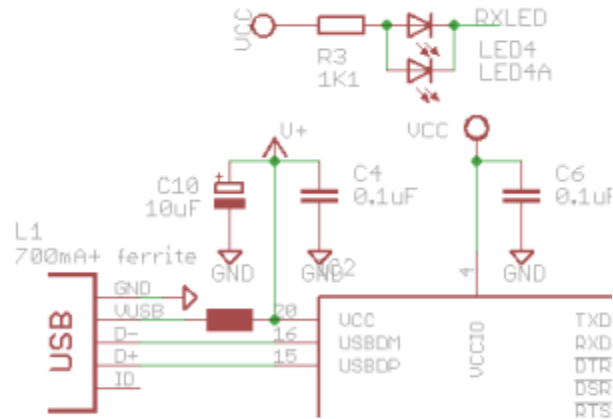
Reverse engineering (RE) is an iterative process of discovery, planning, and experimentation to learn how something is designed, built, and used to achieve a function or goal. A reverse engineer aims to answer the what, why, and how about a completely unfamiliar system.

*What is hardware engineering?*

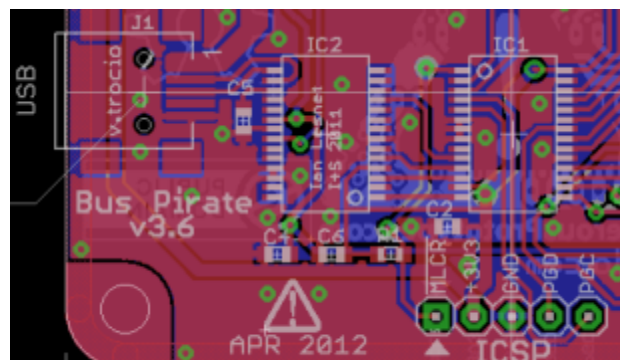
In computing, hardware engineering involves designing and constructing the physical circuitry of an electrical system to perform a task or set of tasks. Hardware engineering is often carried out by an electrical, mechanical, and/or computer engineer. Common tasks include: circuit design, layout, and

routing; active and passive component selection; circuit simulation; board fabrication and rework; and validation of assembled printed circuit boards (PCB).

- Circuit design, layout, and routing



Example circuit schematic



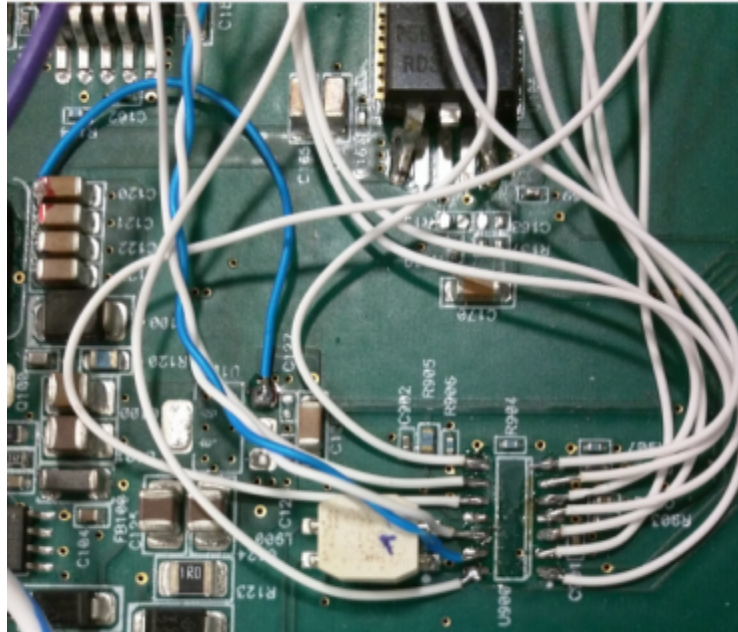
Example PCB assembly drawing

- Active and passive component selection

Component	Value	Footprint	Package	Manufacturer	Part Number	Quantity	Cost	Notes
U1	700mA+ ferrite	700mA+ ferrite	700mA+ ferrite	700mA+ ferrite	700mA+ ferrite	1	0.00	
C10	10uF	10uF	10uF	10uF	10uF	1	0.00	
C4	0.1uF	0.1uF	0.1uF	0.1uF	0.1uF	1	0.00	
C6	0.1uF	0.1uF	0.1uF	0.1uF	0.1uF	1	0.00	
R3	1K1	1K1	1K1	1K1	1K1	1	0.00	
LED4	LED4A	LED4A	LED4A	LED4A	LED4A	1	0.00	
TXD	TXD	TXD	TXD	TXD	TXD	1	0.00	
RXD	RXD	RXD	RXD	RXD	RXD	1	0.00	
DTR	DTR	DTR	DTR	DTR	DTR	1	0.00	
DSR	DSR	DSR	DSR	DSR	DSR	1	0.00	
RTS	RTS	RTS	RTS	RTS	RTS	1	0.00	

Example component selection "menu"

- Circuit simulation - to check correctness, robustness, and other parameters of circuit design
- Board fabrication and rework - solder or desolder components or wires to correct errors or temporarily bypass components



Example board rework

- Validation of assembled PCBs - to ensure circuitry behaves properly before, during, and after different software stages are flashed (e.g. bootloader, OS, and applications). Involves powering up the device and verifying power domains are at the proper levels and loading test software to ensure chip communication channels are clean and correct.

### *What is HW RE?*

Hardware reverse engineering (HW RE) is hardware engineering, but done in reverse.

#### *> Discovery*

The discovery phase is all about information gathering and documentation. During this phase, reference searches are carried out (perhaps somebody has already reverse engineered your particular device), physical components and markings are identified, and a bill-of-materials (BOM), aka component list, is created. Once finished with this phase, the HW RE engineer knows about connectors, external memory chips, microcontrollers, external and internal network interfaces, and miscellaneous/benign components on the target.

#### *> Planning*

The planning phase considers information from the discovery phase to chart a path towards a goal, consider new goals, and prioritize next steps. With the new information from the discovery

phase, you may have discovered hidden components or connectors that will make your job easier, or you may have noticed security features that dissuade you towards other low hanging fruit. At the end of this phase, the HW RE engineer has a prioritized list of interesting things to try (a plan) and has a better feeling of what might work and what won't.

#### > Experimentation

The experimentation phase executes parts of the plan to achieve a goal, aids in discovering more information, and/or verifies assumptions from the prior phases. This phase may involve powering up the unit for the first time and taking measurements. After experimentation, the HW RE engineer might know what the different power domains are, what external and internal communication interfaces are active, and/or that a particular circuit or pinout is what they thought it was.

#### *What does the HW RE engineer do?*

This HW RE course is geared towards assisting the software reverse engineering (SW RE) process. SW RE is useful in offensive security assessments for finding and exploiting vulnerabilities and in defensive security assessments for finding and fixing vulnerabilities. To reverse engineer software for a device, however, the SW RE engineer needs access to the software. HW RE techniques can be used to obtain software from a target device in their possession (It's usually better to search online for a software download first).

Embedded systems are frequently available physically to a reverse engineer (as opposed to, say, the hardware running a cloud service). By using hardware and software reverse engineering techniques, a reverse engineer can attempt to find The Ultimate Holy Grail. When there are unpatched vulnerabilities in a local device's implementation that allow for remote exploitation on other devices we call it The Ultimate Holy Grail. This is a big win and surprisingly common due to design decisions like global keys and a lack of security features.



A common exploit development workflow is depicted: HW RE yields firmware; SW RE yields a vulnerability; and a vulnerability yields a (possibly remote) exploit.

Hunting for remote vulnerabilities is not necessarily the only reason to reverse engineer a piece of hardware. Local attacks alone are often attractive to owners seeking to achieve additional or altered functionality from a device they own. Owners of video game consoles modify the hardware and software of their consoles to allow for homebrewed games (and enable piracy), owners of automobiles use hardware and software modifications to “tune” their vehicles to achieve better performance than they

were shipped with or increase the value of their vehicle by rolling back the odometer, and farmers reverse engineer their heavy agriculture vehicles so they can diagnose and make their own repairs.

Finally, a HW RE engineer provides crucial information for the rest of a comprehensive security assessment:

- Identification of key components: Micros, external memory, physical interfaces, & debug ports
- Analysis of vehicle networks: identification of “next-hop” devices (e.g. does the unit talk on any shared buses with safety or security critical modules?)
- Pin diagrams, schematics, BOM, assembly drawings and other documentation
- Ability to power-up the unit without letting the smoke out
- Establish reliable and robust connections to on-board interfaces
- Locate and bypass physical security measures

## 1.3 Basic Tools

To think about what tools might be useful, it’s important to think about the kinds of tasks that might be useful when reverse engineering.

- Determining which points on a PCB connect to one another → Multimeter
- Modifying hardware to access signals or create new circuits → Soldering Station
- Analysis of analog signals → Oscilloscope
- Analysis of digital signals → Logic Analyzer
- Decoding of encoded data transmitted on digital signals → Oscilloscope or Logic Analyzer
- Injection of commands and/or data into hardware interfaces → Many, depends on interface (e.g. USB-to-Serial, USB-to-CAN, USB-to-LIN, USB-to-I2C, and USB-to-SPI adapters)
- Real-time analysis and control of the processors (or FPGAs, etc.) on the hardware → Many, depends on hardware (e.g. JTAG, In-Circuit Serial Programmer, Serial Wire Debug).

### 1.3.1 Multimeter

A multimeter is a tool which can measure voltage and current. Most come with an auto-ranging function that automatically adjusts the order of magnitude of the measurement, but for those that don’t you will need to make a rough estimate before setting its mode. Additionally, multimeters also have an extremely useful “continuity testing” mode that beeps when there is a short circuit between both probes. This functionality is particularly useful for mapping an unknown circuit because it lets you see if two points are short-circuited (directly connected) to one another.



### 1.3.2 Soldering station

Consisting of a soldering iron, flux, solder, a wet sponge or brass sponge, a desoldering pump or wick, a helping hands, spare wire, and a good light, a soldering station is essential for modifying and building hardware. New connections can be added (e.g. repopulate a header or tap onto an existing pad so probes



can be attached) or existing connections can be removed (e.g. remove an external memory chip so it can be transferred to an external reader or disable a security circuit) greatly expanding the options available to a HW RE engineer. A soldering station should be one of the first investments of a HW RE engineer.

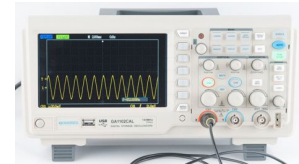
### 1.3.3 Bus Pirate

The Bus Pirate is a neat tool which can be used to perform serial data decoding and injection for several protocols including Universal Asynchronous Receiver/Transmitter (UART), Serial Peripheral Interface (SPI) and Inter-Integrated Circuit (I<sup>2</sup>C). Because JTAG and ICSP, two on-chip debugging standards, are SPI-based, the Bus Pirate can also interface with those (and other) connections to perform debugging functionality for devices with JTAG or ICSP support.



### 1.3.4 Oscilloscope

An oscilloscope is a tool used for measuring analog signals in real-time. Different oscilloscopes will have different ranges of signal frequencies that they can measure, and faster oscilloscopes are (sometimes considerably) more expensive. The oscilloscope is a great general purpose tool, and many oscilloscopes can also decode digital signals as well. Generally, however, once a digital signal has been identified and decoded with an oscilloscope, it is more useful to monitor with a logic analyzer or another digital decoding device.



### 1.3.5 Logic analyzer

A logic analyzer is like an oscilloscope, but it can only monitor digital signals. Logic analyzers are generally cheaper than oscilloscopes and usually support more channels. Most logic analyzers do not perform real-time monitoring, another difference from oscilloscopes. Rather, the only mode of operation is to set a trigger and look at what was captured after the trigger fired.



### 1.3.6 USB-to-serial adapter (a.k.a. FTDI cable)

A USB-to-serial adapter allows for decoding of serial buses on a PC as well as injecting commands. This is more useful than a logic analyzer alone, because it allows the reverse engineer to interact with the serial port directly. These devices are sometimes called “FTDI cables,” because the company FTDI has a corner on the market of USB-to-serial adapter integrated circuits.



### 1.3.7 Microcontroller-specific Debugger/Programmer

The Bus Pirate is a great Swiss Army Knife for a HW RE engineer's toolkit, but it has its limitations. One limitation is that it is often significantly slower than a specially designed debugger/programmer (e.g. 7 hours vs. 2 minutes to program a microcontroller). For this reason, it can be necessary to acquire a specialized programmer for the microcontroller





you are working with. There are a few multi-purpose microcontroller-specific debuggers/programmers to choose from that have overlapping microcontroller support. Common devices include P&E Micro MultiLink, Segger J-Link, Lauterbach Trace32, and ATMEL AVR ISP.

### 1.3.8 Miscellaneous Parts

In addition to the major tools listed above, there are a number of tools a hardware reverse engineer is bound to need:

- |                |                   |                       |                            |
|----------------|-------------------|-----------------------|----------------------------|
| • Screwdrivers | • Scissors        | • Jumper wires        | • Linux computer           |
| • Razor blades | • Electrical tape | o male-male           | • USB A, B, C, mini, micro |
| • Tweezers     | • Hot glue gun    | o male-female         | • Magnifying glass         |
| • Pliers       | • DC power supply | o female-female       | • A good light             |
| • Strippers    | o Battery         | • Headers             | • 30 AWG solder            |
| • Q-tips       | o Wall-wart       | • 30AWG wire wrap     |                            |
| • Paper clips  | o Bench-top       | • Mini grabber probes |                            |
|                | o Adjustable      | • Prototype boards    |                            |

## 1.2 Advanced Tools

The above tools are the most common tools general HW RE engineers will need, but depending on *your* goals and specific target, you may find yourself reaching for one of the advanced tools below. Besides the hot air station, the tools in this section will not be covered during the class. They are listed so you are aware that they exist and to provide pointers to where you can learn more about how they are used for HW RE.

- 1. Hot Air Station** - A handheld hair-dryer-like device that blows hot air out of a small nozzle. Used to heat up areas of a board evenly which makes it easier to solder or desolder multiple pads/pins at once. <https://learn.sparkfun.com/tutorials/how-to-use-a-hot-air-rework-station>
- 2. Solder Paste** - Tiny solder balls suspended in flux. Goes on like toothpaste. Makes surface mount soldering with a hot air station easier. <https://www.instructables.com/id/How-to-Surface-Mount-Solder-Using-Solder-Paste/>
- 3. JTAGulator** - Nifty tool that automates checking test-points, vias, and pins for on-chip debug interfaces. Does so by enumerating possible pinouts. <http://www.grandideastudio.com/jtagulator/>
- 4. Specialized Memory Sockets** - Mechanical contraptions that break out memory for you. <https://www.digikey.com/products/en/development-boards-kits-programmers/programming-adapters-sockets/798>
- 5. ChipWhisperer** - Nifty tool for side-channel analysis and glitching attacks. [https://wiki.newae.com/Getting\\_Started](https://wiki.newae.com/Getting_Started)
- 6. 3D Printer & C&C Mill** - Used to fabricate your own special purpose tools and jigs. <https://www.inventables.com/projects/pcb-milling-on-x-carve>  
<https://blog.adafruit.com/2017/06/01/3d-printed-pcb-workstation-with-needle-probes-by-giuseppe/>
- 7. XRay** - Let's you see traces within PCB layers and other hardware secrets. <https://uvicrec.blogspot.com/2015/08/xy-ray-x-ray-scanner.html>
- 8. Microscope** - Let's you look at decapped ICs. <https://seanriddle.com/decap.html>

## 2. First Contact (~30 minutes)

Before even powering up the hardware, look at the hardware itself. First contact with a new component often involves carefully taking apart the hardware or parts of the hardware to get to the circuitry to identify areas of interest. Be especially careful to avoid damaging the circuitry when attempting to physically separate components and enclosures.

### Tools Used

- Screw drivers
- Pliers
- Magnifying glass
- Razor blades
- Scissors
- Multimeter
- Tweezers
- A good light

### Section Goals

- 1) Create a BOM & assembly drawing
- 2) Identify power hookup and power domains
- 3) Identify microprocessors/microcontrollers
- 4) Locate microprocessor/microcontroller programming interface
- 5) Identify at least two interesting communication interfaces and how to connect to them

### Related CTF Challenges

Title	Description	Pts
BP3.6 IC Suppliaa rrrrrs!!	Ahoy, landlubbers! The cap'n o' this ship needs ye t' find the first 5 letters o' the three IC manufacturers o' the Bus Pirate v3.6. Report to the poop deck once ye has put the first 5 letters of the three IC suppliaa in all-caps 'n alphanumerical orderrrr, 'n don' ferget to put a '_' between each and wrap 'em in "flag{}" (Example flag for Renesas, Infineon, & NXP: "flag{INFIN_NEXTE_RENES}").	20
BP4.0 IC Suppliaa rrrrrs!!	Do ye have yer sea legs yet, scallywag? Now cap'n wants ye to get the three IC suppliaa o' the Bus Pirate v4.0. Report back to the poop deck once ye has put the first 5 letters o' th' tree IC suppliaa in all-caps, alphanumerical order, n' a '_' between 'em. O' course ye also need ta wrap 'em in "flag{}," ya hear? (Example flag for Intel, Qualcomm, & Samsung: "flag{INTEL_QUALC_SAMSU}")	20
Three Point Six Sheets to the Wind	Avast! Down yer grog 'n don spill on the datasheets. Scour every datasheet o' th' Bus Pirate v3.6 three ICs (IC1, IC2, & IC3). Yer lookin' for the "Absolute Maximum Supply Voltage" characterrrristic o' each o' the three ICs. Use 1 decimal place fer each number, -0.0 fer any IC without a minimum value listed, always include a '-' for the minimum and a '+' for the maximum, and cap'n wants 'em listed in IC orderrrr. Don' forget the '_' between each min/max pair and "flag{}" 'round the whole thing. (Example flag for IC1=-0.3v to 2v; IC2=5v; IC3=-11v to 15.15v: "flag{-0.3+2.0_-0.0+5.0_-11.0+15.1}")	50
Four Sheets to the Wind	If ye can keep yer bilge t' yerself 'n' yer sea legs steady, you'll be going on account in no time at'all. This challenge is the same as the last one, but ye need t' scour the datasheets o' th' Bus Pirate v4 three ICs (IC1, IC2, & IC3). Again, yer lookin' fer the "Absolute Maximum Supply Voltage" charrrrrracteristic o' each IC. Use 1 decimal place fer each number, -0.0 fer any IC without a minimum value listed, always include a '-' for the minimum and a '+' for the maximum, and cap'n wants 'em listed in IC orderrrr. Don' forget the '_' between each min/max pair and "flag{}" 'round the whole thing. (Example flag for IC1=-0.3v to 2v; IC2=5v; IC3=-11v to 15.15v: "flag{-0.3+2.0_-0.0+5.0_-11.0+15.1}")	50

## 2.1 Visual Survey

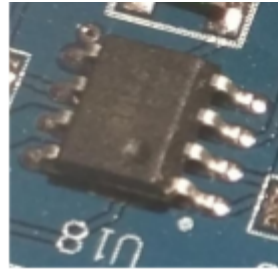
Many times, the designers of the hardware use a layer of silk screen (printing on a PCB) to mark components with identifiers and even make comments on circuits. Therefore, it is useful to look at the board to begin to get an idea of what does what. Identify the major components on the PeopleNet G3 board and try to find their manuals on the internet.

- How are components mounted?

*Through-hole is your friend. Flat pack components expose all pins. BGA is your enemy.*



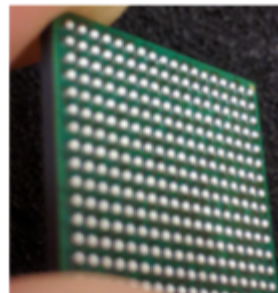
Through-Hole



SOIC

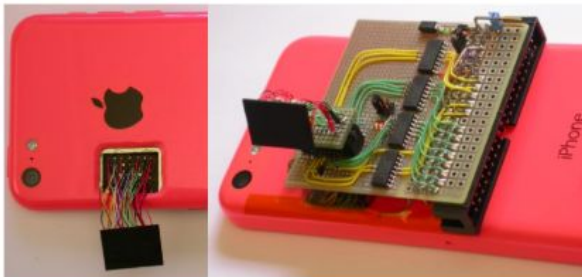


QFN



BGA

*Advanced techniques can access BGA pads, but might not be worth your time..*



© Sergei Skorobogatov from  
"The bumpy road towards iPhone 5c NAND mirroring"

- Are there barriers or protections in place?

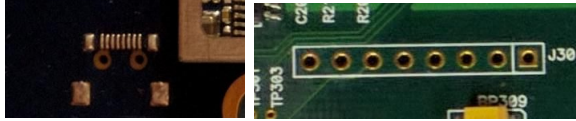
*EMF shielding, robustness coatings, and heat sinks can make our job difficult, but they can often be removed carefully.*

- What are the populated interfaces?

*Things like USB, vehicle connectors, and hidden connectors.*

- Where are interesting areas (depopulated pads, test-points, unsure)?

*Development and debug interfaces are typically depopulated before production, but they might still be supported by the software.*

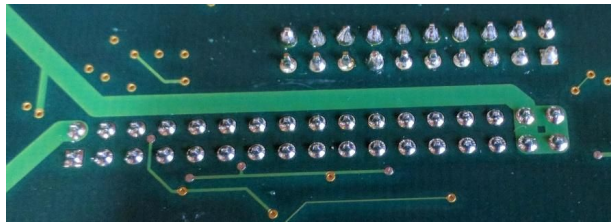


- How do components relate to one another?

*Observe general layout, components will be closest to what they interface with because that's cheaper and easier for the HW engineer.*

- How is the board powered?

*You will eventually need to power the board. Good starting point for tracing. Big traces mean big current. There's a good chance the big trace is a power or ground line.*



## 2.2 Chip Identification

Gather information about each chip on the board, build a “Bill-of-Materials” (BOM) and PCB assembly map. Useful resources: 1) <http://www.smdmark.com/en-US/>; 2) <https://duckduckgo.com/>

- What are each of the chips and what do they do?

*Identify **every** chip on the board. Draw a diagram or take a picture and work through every component from top-left to bottom-right. Note processors, FPGAs, interface controllers, and memory. The more you know the better.*

```

-----
-- Main Micro --
-----
Microchip
ATMEL ATMEGA 2560
http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel

-----
--COMMS (USB, CAN, LIN)--
-----
2: CY7C 65213 28PVXI
Cypress
USB-UART LP Bridge Controller
https://www.cypress.com/file/139881/download

3: MCP 2561E
Microchip
High-Speed CAN Transceiver
https://www.microchip.com/wwwproducts/en/MCP2561

```

Example BOM

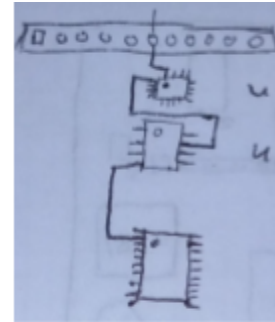


Example PCB  
Assembly Map

## 2.3 Passive Probing

Reverse engineer the circuitry to better understand the board function and zero in on areas of interest. Draw schematics by hand as you develop an understanding during this phase.

- How are inputs and outputs connected to chips?  
*Identify passive circuitry, draw it out, reason about it.*
- What chips are connected?  
*Buses between memory and MCU or between interfaces and MCU could be MITMd.*
- Where do depopulated pads and test-points connect to?  
*This can help identify JTAG or serial interfaces and areas to be repopulated.*



Example circuit drawing

### 3. Hardware Modification (~30 minutes)

#### Tools Used

- Soldering station
- Male header pins
- A good light
- Tweezers
- Magnifying glass
- Multimeter

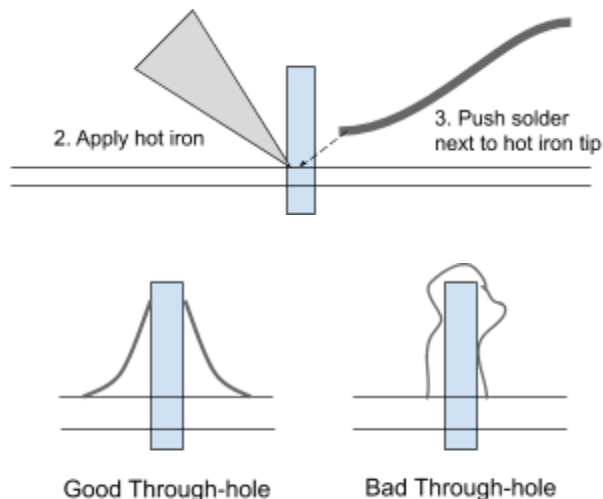
#### Section Goals

- 1) Add male header pins to unpopulated interfaces of interest

#### 3.1 Soldering Basics

Keep these tips in mind while working with the soldering station:

- Solder flows towards heat; flux helps solder flow
- Thermal equilibrium and the zeroth law of thermodynamics
  - Heat dissipates quickly through copper
  - Large contacts and planes (e.g. Vcc & Gnd) dissipate heat more quickly
  - Over time, everything heats up to match the soldering iron temp
  - A hotter iron will melt solder faster and damage sensitive components sooner
    - But too cool, and the whole circuit heats up before solder melts
- Best Practices
  1. Start with a hot iron (~350°C); if using flux, apply flux.
  2. Briefly heat target solder joint / pad / pin with hot iron
  3. Push solder onto joint / pad / pin keeping the hot iron in-place
  4. Remove hot iron and solder wick



***- Page Intentionally left blank. Use as scratch sheet. -***



## 4. With Power Comes Responsibility (~90 minutes)

*After a thorough assessment with the board unpowered, it is time to provide power to the board. In industry, this is called “smoke-testing” – give the board juice and watch for smoke. If you let out the magic smoke, you fail because the chips run on smoke and there’s no way to put it back in once it’s out.*

**Note:** *Before you power the board, check to make sure there aren’t any accidental short circuits!*

In automotive, most of the time you will find 12v DC is the proper power supply voltage because a vehicle battery is 12v DC. However, this is not always the case. First, look for markings on the case or power supply voltage in the documentation. Then, if that doesn’t help and you are completely unsure, start at a lower voltage (around 5v) and gradually work up until the board appears to be functioning properly. Having a variable power supply helps a lot here, but there are other ways to test various voltage levels (e.g. use a USB power supply to get 5v). Luckily for you, automotive electronics are usually built with robust power circuits that can tolerate poor power conditions. Therefore as long as you are within a few volts and *have enough current* (and don’t have a short circuit), the system should function properly.

Multimeter probing at the different power domains will enable you to verify the board is powered properly.

### Tools Used

- Power Supply
- Multimeter
- Bus Pirate
- Oscilloscope
- Logic Analyzer
- FTDI Cable
- Microcontroller Specific Debugger/Programmer
- Laptop/PC

### Section Goals

1. Verify power domains and pin-outs
2. Establish communication with serial port of main micro
3. Read and write internal memory of main micro
4. Establish communication with other on-board components

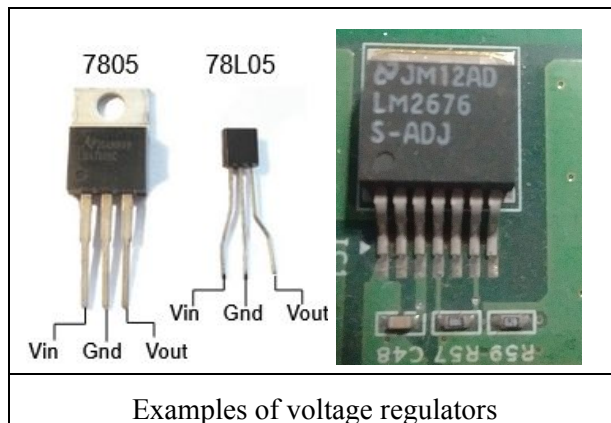
### Related CTF Challenges

Title	Description	Pts
Saleae Sea Shanty	Listen close ye scurvy dog! Do ye hear the old salt o' this ship singing an old Saleae sea shanty on SCL and SDA? Hornswaggle the flag while they're still booming about. (See attachment "CTF_HWRE_challenge_5.logicdata")	200
Keep a Weather Eye Open	Sail ho! A becalmed BPv4 merchant vessel lies ahead. Smartly now, use the spyglass up in the crow's nest to investigate the merchant ship. Shout down the flag ye see 'n if there be booty aboarrrrrd. (See attachment "CTF_HWRE_challenge_6.hex")	200
Treasure Chest	Last night I overheard the cap'n o' the BPv4 say she hides a flag in her on-board treasure chest 'n checks on it every morn'n. Follow her at dawn tomorrow n' get access however you can. Jus' don' get caught or you'll surely walk the plank n' I'll be dancin' the hempin' jig. (Requires BPv4 hardware with CTHWRE firmware installed).	500

X Marks the Spot	Ages after the captain and crew have wetted their pipes at Davy Jones' Locker for the first time, the wreckage of the BPv4 was reclaimed from the deep, dark depths. On a moist and soggy page found just below the poop deck, a smeared smattering of ink spells out this cryptic message: "Th' l _st flag, split in two ... cannot be crac __d, only found ... one piece in __ treasure chest ... the mode is one-t _e _ad ... two pieces united at last. 0x0088 marks the spot." (Requires BPv4 hardware with CTHWRE firmware installed).	800
------------------	--	-----

## 4.1 Multimeter Probing

Start at the power input connector and use the multimeter to check voltage levels at various points on the board. Focus on finding and measuring voltage regulators first, then measure voltage levels at the microprocessor.



- Verify the voltage domains.  
*Know voltage domains to interface with board later without creating smoke (e.g. whether to use a 3.3V UART vs. 5V UART).*
- Use to verify chip and connector pin-outs.  
*Sanity check what you think you know about the components. Are GND and Vdd where you expect them to be? Are they at the correct voltages based on their specs?*

**Tip:** A multimeter can also be used to find or verify digital network buses (e.g. UART or CAN).

*How? The DC voltage on a digital network bus will fluctuate rapidly while data is transmitted. Power up the board and monitor the DC voltage on a suspected digital bus.*

## 4.2 Oscilloscope and Logic Analyzer Probing

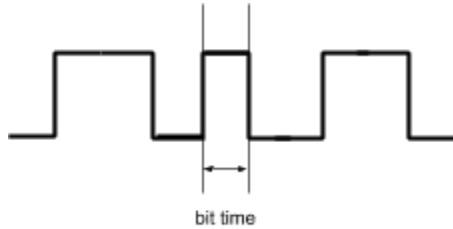
Probing with an oscilloscope or logic analyzer will give you a better picture of what is happening on the wire. Recall that an oscilloscope measures and displays an analog waveform while the logic analyzer measures and displays a digital waveform. An oscilloscope can also display a digital waveform because digital waves are actually analog waves in the real world 🤖.

- Find digital network buses.

*Although a multimeter can help with this, it is much better to use an oscilloscope or logic analyzer here. Directly monitor various test-points and pins you suspect to be a digital network bus so you can see if they're active.*

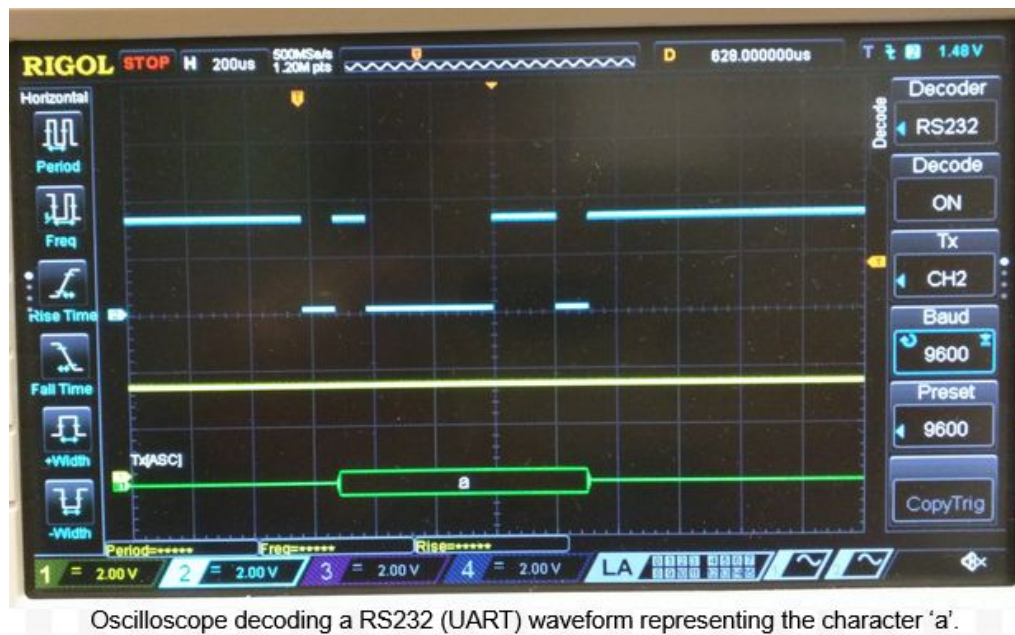
- Determine baud rates.

*When a digital network bus is found, the next question is usually: "What baud rate is it at?" To measure, look at the time spent during the **shortest** bit pattern you can see. This is called the bit time. Simply invert the bit time to get the baud rate (e.g.  $8.68\mu s \rightarrow \sim 115200\text{bps}$ ).*



- Decode signals

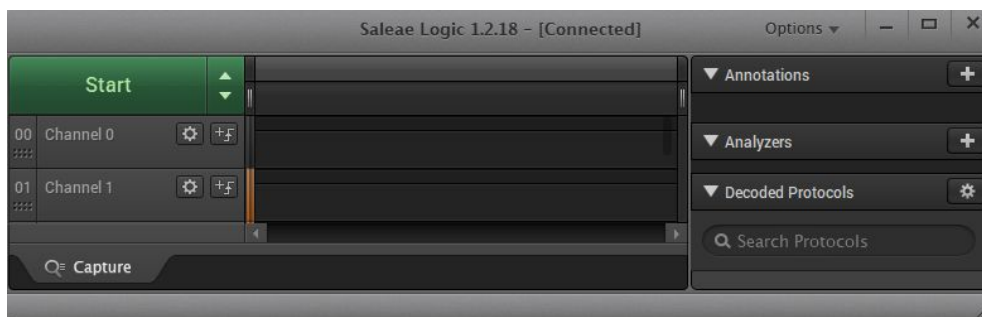
*Good oscilloscopes and logic analyzers are able to decode signals in real-time. This information could be useful.*



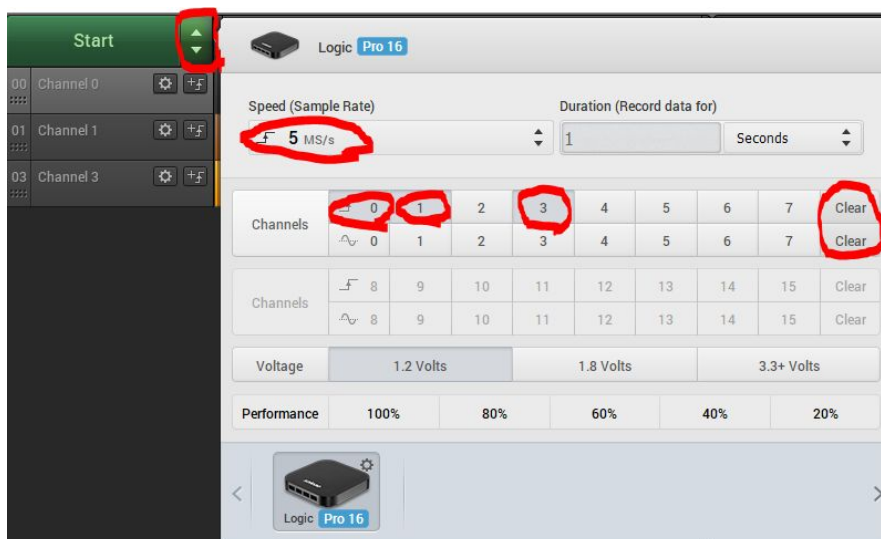
Oscilloscope decoding a RS232 (UART) waveform representing the character 'a'.

#### 4.2.1 Setup the Logic Analyzer

1. Download and install the latest Saleae Logic software from the official site:  
<https://www.saleae.com/downloads/> (Latest was version 1.2.18 at the time of writing)
2. Open the installed application and plug in the Saleae device into your PC's USB port. You should be greeted with a similar screen as below:



- Configure the logic analyzer by clicking the arrows next to the big green “Start” button to use the channels you are interested in. I have 0, 1, and 3 plugged in. Also set the sample rate to something reasonable. A large sample rate and long capture will create a lot of data, so find a balance between the settings and storage space available. I use 5MS/s and 1 second or more depending on what I am capturing.



- Press “Start” to begin the capture. If you want, set up a trigger on one of the channels to begin capturing when the voltage on one of the channels changes.

### 4.3 UART Probing

UART stands for “Universal Asynchronous Receiver/Transmitter.” SparkFun has a great write-up here: <https://learn.sparkfun.com/tutorials/serial-communication>. It suffices to say it is a defacto serial communication protocol found in embedded devices that can be used by reverse engineers to some pretty awesome stuff if it isn’t locked down depending on the target device:

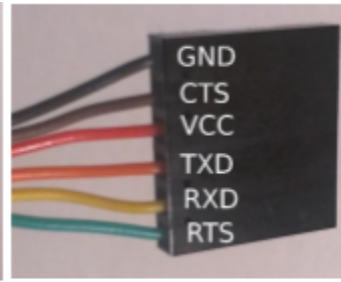
- Obtain an interactive serial console with a target platform
- Read system and debugging logs
- Upload custom software
- Modify configuration parameters
- Bypass security features

- Dump memory
- Spoof embedded components

It is easiest to use a USB-to-UART (aka “FTDI cable”) as shown below.

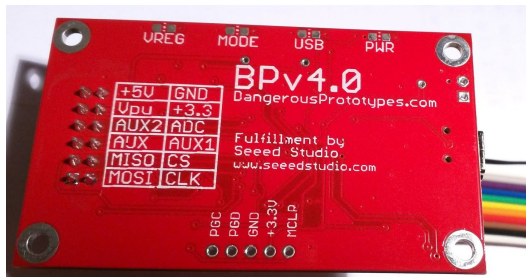


FTDI cable for UART communication



Pin-out of FTDI cable

However, if you have a Bus Pirate on hand, you can use that instead! We will be using a Bus Pirate v4 for this class.



			1-Wire	UART	I2C	SPI	JTAG	ICSP
1	MOSI	White	OWD	TX	SDA	MOSI	TDI	MOSI
2	CLK	Black		RTS	SCL	TCK	TCK	SCK
3	MISO	Brown		RX		MISO	TDO	MISO
4	CS	Red		CTS		CS	TMS	RESET
5	AUX	Orange	Auxiliary I/O, freq probe, PWM					
6	AUX1	Yellow	Auxiliary I/O1					
7	AUX2	Green	Auxiliary I/O2					
8	ADC	Blue	A/D converter, max 6V, 10b 500ksp/s					
9	Vpu	Purple	Input for pull-up resistors (0-5V)					
10	+3.3V	Gray	On-board supply, max. 150mA 150mA					
11	+5V	White	On-board supply, max. 150mA 150mA					
12	GND	Black	Ground to test circuit					

**Note:** There are two dominating hardware versions of the Bus Pirate: BPv3.6 and BPv4.0. They differ in some key ways: Number of pins (10 vs. 12), pin assignments, microprocessor, and external EEPROM in the BPv4. Make sure you are using the right pin-out diagram for your BP!

We will also be using miniature clamp probes to attach to various places on the board to enable us to interface with the components.





### 4.3.1 Class Goals

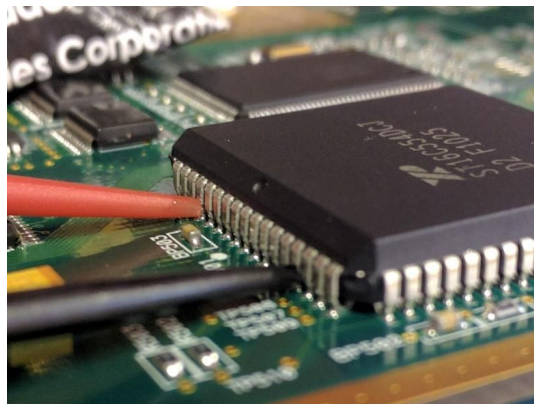
#### 4.3.1.1 Access the system serial console

Target Info Name	Target Info Value
Firmware Version	
CAN ID (Channel 32)	
CAN Data (Channel 32)	

### 4.3.2 Setup

1. Wire Bus Pirate probes to board. You don't *need* RTS and CTS for UART, but they can be helpful. Don't wire VCC. Do wire GND.

**Note:** You are supposed to figure this part out yourself! You should know from the previous stages what and where to connect. If not, check your work and come back ☺



2. Install minicom if needed:

```
$> sudo apt install minicom
```

3. Plug in the Bus Pirate USB and determine which device file descriptor was created in /dev/ using dmesg:

```
$> sudo dmesg | tail | grep tty
```

```
$ sudo dmesg | tail | grep tty
[ 1494.110513] cdc_acm 1-2:1.0: ttyACM0: USB ACM device
$
```

**Note:** Mine appears as /dev/ttyACM0, but yours might be different with a different name (e.g. /dev/ttyUSB0) or number (e.g. /dev/ttyACM1). Replace “ttyACM0” in the following steps with the proper “ttyXXXX” on your machine.

4. Give permissions to /dev/ttyACM0 and run minicom at 115200 bps:

```
$> sudo chmod o+rw /dev/ttyACM0
```

```
$> minicom -b 115200 -D /dev/ttyACM0
```

```
$ sudo chmod o+rw /dev/ttyACM0
$ minicom -b 115200 -D /dev/ttyACM0
```

```
Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on May  6 2018, 08:02:47.
Port /dev/ttyACM0, 16:51:28

Press CTRL-A Z for help on special keys

HiZ>
HiZ>
HiZ>
```

**Note:** Hit <Enter> a few times, you should be greeted with a Bus Pirate prompt: “HiZ>”

5. Type ‘i’ and hit <Enter> to display the version info and make sure the Bus Pirate firmware is updated to the “Community Firmware v7.1 - CTHWRE Edition”

```
HiZ>i
Bus Pirate v4
Community Firmware v7.1 - CTHWRE Edition [HiZ 1-WIRE
DEVID:0x1019 REVID:0x0004 (24FJ256GB106 UNK)
http://dangerousprototypes.com
HiZ>
```

**Note:** If your Bus Pirate does not have the proper version, go to Section 5 Extras > Upgrade Bus Pirate Firmware and follow the steps there before continuing.

### 4.3.3 Using Bus Pirate for UART Probing

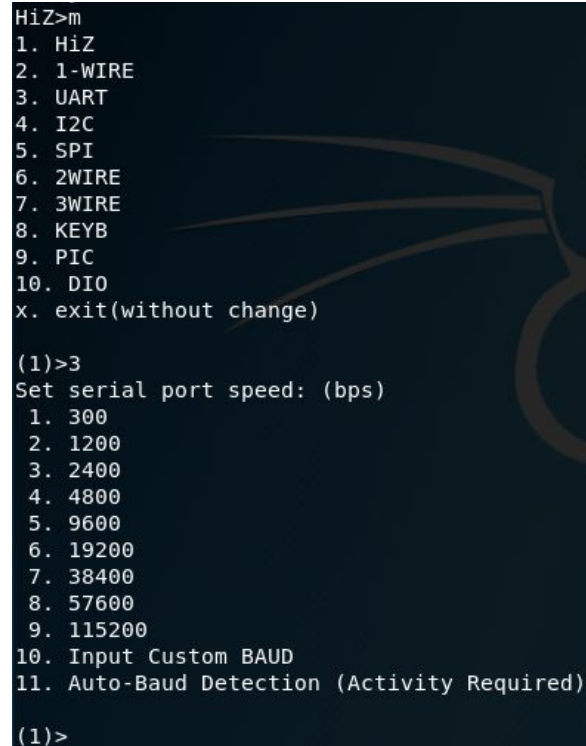
1. Put the Bus Pirate into UART mode and configure it to monitor or bridge the target’s UART interface. There’s a good overview of this mode on the official site

<http://dangerousprototypes.com/docs/UART>

- a. Set UART mode

```
HiZ> m
(1)> 3
```





```

HiZ>m
1. HiZ
2. 1-WIRE
3. UART
4. I2C
5. SPI
6. 2WIRE
7. 3WIRE
8. KEYB
9. PIC
10. DIO
x. exit(without change)

(1)>3
Set serial port speed: (bps)
1. 300
2. 1200
3. 2400
4. 4800
5. 9600
6. 19200
7. 38400
8. 57600
9. 115200
10. Input Custom BAUD
11. Auto-Baud Detection (Activity Required)

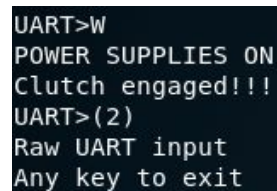
(1)>

```

- b. Set baud rate, parity bits, stop bits, and error bits. Use the measured values from earlier, or make a guess. The auto-baud detection mode doesn't work very well. When prompted, select "**Normal (H=3.3V, L=GND)**" for the output type.
- c. Start the power supplies with command 'W' then enter "live monitor" mode with "(2)"

```
UART> W
```

```
UART> (2)
```



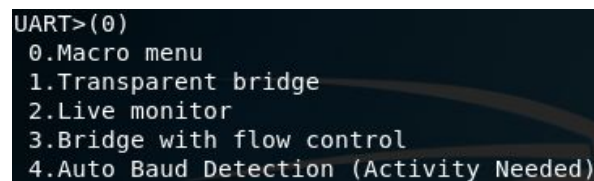
```

UART>W
POWER SUPPLIES ON
Clutch engaged!!!
UART>(2)
Raw UART input
Any key to exit

```

- d. To view the available modes, use "(0)"

```
UART> (0)
```



```

UART>(0)
0.Macro menu
1.Transparent bridge
2.Live monitor
3.Bridge with flow control
4.Auto Baud Detection (Activity Needed)

```

- e. To interact with the board, use "transparent bridge" mode with "(1)". Make sure the power supplies are on with 'W' before entering into this mode!

```
UART> W
```

```
UART> (1)
```

```
y
```

```

UART>W
POWER SUPPLIES ON
Clutch engaged!!!
UART>(1)
UART bridge
Normal to exit
Are you sure? y

```

#### Useful Minicom commands:

All commands from the main Minicom window can be accessed from the help window which can be accessed by first pressing CTRL-A followed by Z. Some have shortcuts that begin with CTRL-A followed by a single key press.

Minicom Command	Help Window Sequence	Shortcut
Help	CTRL-A, Z	
Exit	CTRL-A, Z, X	CTRL-A, X
Configure comm. Parameters (Baudrate, data bits, stop bits, parity)	CTRL-A, Z, 0	CTRL-A, P
Toggle local “echo” on/off	CTRL-A, Z, E	CTRL-A, E
Clear screen	CTRL-A, Z, C	CTRL-A, C

#### Useful Bus Pirate commands:

Bus Pirate Command	Key
Help	?
Reset	#
Change mode	m
Show version info	i
Jump to bootloader	\$

## 4.4 On-Chip Debugging - Memory Read/Write

ICSP stands for In-Circuit Serial Programming. It is a proprietary standard for on-chip debugging similar to JTAG ([https://en.wikipedia.org/wiki/In-system\\_programming](https://en.wikipedia.org/wiki/In-system_programming)). It allows you to control the chips on the board at the lowest levels.

- Write and read internal and external memory
  - o Extract firmware, modify it, write it back
  - o Modify configuration parameters
- Write and read internal registers and fuses
- Bypass security features
- Obtain an interactive debugging session with a program on the target platform

The microcontroller on the Smart Sensor Simulator (SSS) Daughter Board (DB) uses an AVR enhanced RISC instruction set architecture (ISA). Many types of Arduinos use AVR based processors, but newer ones are switching to ARM. In addition, the open-source ecosystem has mature support for the AVR

architecture. Because of this, we can use extremely inexpensive or free tools to attach to the SSS DB's ICSP port. It is often easiest to use a microcontroller specific on-chip debugger and programmer as shown below, but they can be a couple hundred dollars and only support a handful of microprocessors. As in the UART section, we will be using the Bus Pirate v4.0 here instead!



*Examples of microcontroller specific debuggers and programmers.*

#### 4.4.1 Class Goals

##### 4.4.1.1 Dump device firmware

Target Info Name	Target Info Value
Size of firmware	
16 bytes of FLASH starting at address 0x0	
16 bytes of EEPROM starting at address 0x0	

##### 4.4.1.2 Modify firmware and write it back

#### 4.4.2 Setup

We will be using the Bus Pirate v4.0 as our ICSP interface device and AVRDUDE as our interface software. AVRDUDE, once setup, will use the Bus Pirate as a protocol bridge to the AVR core running inside the Atmel ATmega 2560.

1. Download, compile, and install AVRDUDE.
  - a. Clone the latest avrdude build scripts from the arduino git repo:

```
$> git clone
https://github.com/arduino/avrdude-build-script.git
```

- b. Install dependencies

```
$> sudo apt install build-essential libtool automake
pkg-config subversion zip flex bison gperf libelf-dev
libusb-dev libftdi-dev
```

- c. Move into the repository directory and run the script to kickoff the build:

```
$> cd avrdude-build-script
$> ./avrdude-build.bash
```

- d. Move to where avrdude was built and make sure it was successful

```
$> cd avrdude-6.3
$> sudo chmod +x avrdude
$> ./avrdude -v
```

```
$ cd avrdude-6.3
$ sudo chmod +x avrdude
$ ./avrdude -v

avrdude: Version 6.3-20190610
        Copyright (c) 2000-2005 Brian Dean, http://www.bdmicro.com/
        Copyright (c) 2007-2014 Joerg Wunsch
```

- e. Copy the binary to your user binary directory so you can call it from anywhere in bash.

```
$> sudo cp avrdude /usr/local/bin/.
```

2. Wire the Bus Pirate to the ICSP pins of the Atmel microcontroller.

#### 4.4.3 Using Bus Pirate with AVRdude for ICSP Memory Read/Write

1. Use the Bus Pirate as the programmer with avrdude in terminal mode

```
$> sudo chmod o+rw /dev/ttyACM0
$> avrdude -p m2560 -P /dev/ttyACM0 -c buspirate -t
```

```
$ avrdude -p m2560 -P /dev/ttyACM0 -c buspirate -t

Attempting to initiate BusPirate binary mode...
avrdude: AVR device initialized and ready to accept instructions

Reading | ##### | 100% 0.03s

avrdude: Device signature = 0x1e9801 (probably m2560)
avrdude>
```

**Note:** If this doesn't work the first time, hit Ctrl+C to cancel, then try it again. If that doesn't work, try using Bus Pirate in bitbang mode by substituting "buspirate" with "buspirate\_bb"

**Note:** You can easily use avrdude with a microcontroller specific on-chip debugger like the avrispmkii by changing the "-c" flag to "avrispmkII" and dropping the "-P" flag.

2. Read an address in flash memory from avrdude terminal mode

```
avrdude> dump flash 0x5040 16
```

```
avrdude> dump flash 0x5040 16
>>> dump flash 0x5040 16
5040 53 6d 61 72 74 20 53 65 6e 73 6f 72 20 53 69 6d |Smart Sensor Sim|
```

3. You could read all flash this way, but it's easier to do it in one shot from the command line. Exit terminal mode then read all flash firmware into a file

```
avrdude> quit
$> avrdude -p m2560 -P /dev/ttyACM0 -c buspirate -x
serial_recv_timeout=10 -x spifreq=3 -U flash:r:sssdb_flash.bin:r
$ avrdude -p m2560 -P /dev/ttyACM0 -c buspirate -x serial_recv_timeout=10 -x spi
freq=3 -U flash:r:sssdb_flash.bin:r

Attempting to initiate BusPirate binary mode...
avrdude: AVR device initialized and ready to accept instructions

Reading | ##### | 100% 0.03s

avrdude: Device signature = 0x1e9801 (probably m2560)
avrdude: reading flash memory:

Reading | ##### | 51% 9.22s
```

4. Let's change part of the firmware and upload it back. Any strings that appear in the UART boot console are good candidates because we can ensure our changes really did take affect.

```
$> vim sssdb_flash.bin
$> avrdude -p m560 -P /dev/ttyACM0 -c buspirate -x
serial_recv_timeout=10 -x spifreq=3 -U flash:w:sssdb_flash.bin
$ vim sssdb_flash.bin
$ avrdude -p m2560 -P /dev/ttyACM0 -c buspirate -x serial_recv_timeout=10 -x spi
freq=3 -U flash:w:sssdb_flash.bin

avrdude: AVR device initialized and ready to accept instructions

Reading | ##### | 100% 0.03s

avrdude: Device signature = 0x1e9801 (probably m2560)
avrdude: NOTE: "flash" memory has been specified, an erase cycle will be perform
ed
      To disable this feature, specify the -D option.
avrdude: erasing chip
avrdude: reading input file "sssd_b_flash.bin"
avrdude: input file sssdb flash.bin auto detected as raw binary
avrdude: writing flash (261408 bytes):

Writing | ##### | 100% 48.59s

avrdude: 261408 bytes of flash written
avrdude: verifying flash memory against sssdb_flash.bin:
avrdude: load data flash data from input file sssdb_flash.bin:
avrdude: input file sssdb_flash.bin auto detected as raw binary
avrdude: input file sssdb_flash.bin contains 261408 bytes
avrdude: reading on-chip flash data:

Reading | ##### | 100% 115.14s

avrdude: verifying ...
avrdude: 261408 bytes of flash verified

avrdude: safemode: Fuses OK (E:FD, H:D8, L:BF)

avrdude done. Thank you.
```



Useful AVRDude commands:

AVRDude Command	Command
Help	?
Microcontroller info	part
Read memory (e.g. fuses, eeprom, flash)	dump
Write memory (e.g. fuses, eeprom, flash)	write

## 5. Extras

### Fun HW Hacks

<https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/december/spectre-on-a-television/>  
<https://nada-labs.net/2010/using-the-buspirate-with-a-sd-card/>  
<http://konukoi.com/blog/2018/02/13/lifting-firmware-with-the-bus-pirate/>  
[https://www.cs.cmu.edu/~dst/GeoHot/1780\\_27c3\\_console\\_hacking\\_2010.pdf](https://www.cs.cmu.edu/~dst/GeoHot/1780_27c3_console_hacking_2010.pdf)

### Upgrade Bus Pirate Firmware

Older Bus Pirate firmware versions do not support all of the features we will be using. Therefore, you must upgrade the Bus Pirate firmware. I have provided a custom firmware for the CyberTruck HW RE (CTHWRE) based on v7.1 community edition.

- Download the CTHWRE Bus Pirate firmware and updater script from the public git repo and place them in the same folder.

[https://github.com/bhass1/cthwre/cybertruck\\_2019/tools/buspirate/bpv4\\_cthwre\\_firmware\\_final.hex](https://github.com/bhass1/cthwre/cybertruck_2019/tools/buspirate/bpv4_cthwre_firmware_final.hex)  
[https://github.com/bhass1/cthwre/cybertruck\\_2019/tools/buspirate/pirate-loader\\_lnx](https://github.com/bhass1/cthwre/cybertruck_2019/tools/buspirate/pirate-loader_lnx)

**Note:** For intrepid readers at home, you can build the latest firmware from the official Bus Pirate GitHub:

[https://github.com/BusPirate/Bus\\_Pirate/blob/master/Documentation/building-and-flashing-firmware.md](https://github.com/BusPirate/Bus_Pirate/blob/master/Documentation/building-and-flashing-firmware.md)

**Note:** You'll also need to build the Bus Pirate v4.0

pirate-l[https://github.com/bhass1/cthwre/CyberTruck\\_2019/bpv4\\_cthwre\\_firmware\\_final.hex](https://github.com/bhass1/cthwre/CyberTruck_2019/bpv4_cthwre_firmware_final.hex)oad  
er if you are using a Bus Pirate v4.0. You can find the source and build-script from the official Bus Pirate GitHub here:

[https://github.com/BusPirate/Bus\\_Pirate/tree/master/package/BPv4-firmware/pirate-loader-v4-source](https://github.com/BusPirate/Bus_Pirate/tree/master/package/BPv4-firmware/pirate-loader-v4-source).

- Connect to the Bus Pirate to the USB port of the PC
- Put the Bus Pirate into bootloader mode:
  - **Bus Pirate v3.6**
    - Give permissions to /dev/ttyUSBx and connect to the Bus Pirate via minicom:

```
sudo chmod o+rw /dev/ttyUSBx
minicom -b 115200 -D /dev/ttyUSBx
```

- If the Bus Pirate prompt doesn't appear, hit enter or press '?' (help) or 'i' (version information) and hit enter and the prompt should appear (possibly after some other output).
- At the Bus Pirate prompt in screen press '\$' and, when prompted, 'y'.

```
HiZ>$
Are you sure? y
BOOTLOADER
```

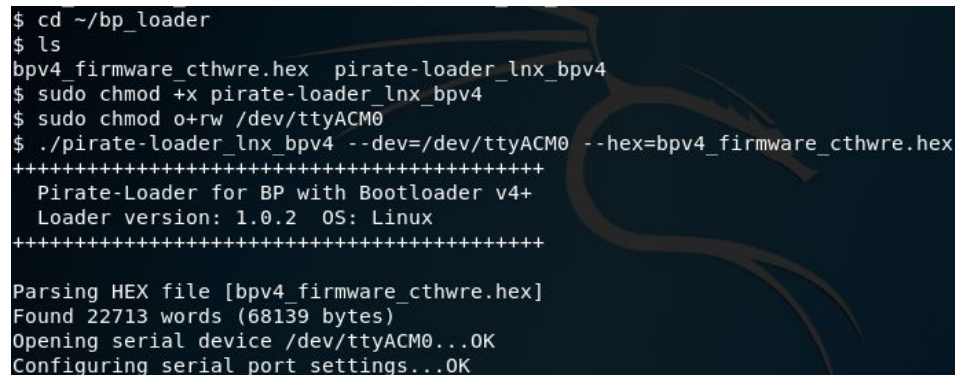
#### o Bus Pirate 4.0

- Short the PGC and PGD pins on the ICSP header. *Keep them shorted for the remaining steps.* You can solder a male header and use a female-female jumper wire or use a male-male jumper wire and wedge it into the through-holes.
- While PGC and PGD pins are shorted, press the RESET button on the BPv4.
- Finally, we're ready to update the firmware in the Bus Pirate. Open a terminal (if one isn't already open) and change the directory to where the two files in the first step were downloaded.

```
cd ~/bp_loader
```

- Set the pirate-loader\_lnx\_bp4 file we downloaded to executable and run it (both as root):

```
sudo chmod +x pirate-loader_lnx_bp4
sudo chmod o+rw /dev/ttyACM0
./pirate-loader_lnx_bp4 --dev=/dev/ttyACM0
--hex=bpv4_firmware_cthwre.hex
```



```
$ cd ~/bp_loader
$ ls
bpv4_firmware_cthwre.hex  pirate-loader_lnx_bp4
$ sudo chmod +x pirate-loader_lnx_bp4
$ sudo chmod o+rw /dev/ttyACM0
$ ./pirate-loader_lnx_bp4 --dev=/dev/ttyACM0 --hex=bpv4_firmware_cthwre.hex
+++++
Pirate-Loader for BP with Bootloader v4+
Loader version: 1.0.2 OS: Linux
+++++
Parsing HEX file [bpv4_firmware_cthwre.hex]
Found 22713 words (68139 bytes)
Opening serial device /dev/ttyACM0...OK
Configuring serial port settings...OK
```

- The pirate-loader\_lnx\_bp4 file should output some firmware update progress information. At the end, you should see the success message, "**Firmware updated successfully :)**!"



```

Writing page 51 row 408, cc00...OK
Writing page 51 row 409, cc80...OK
Writing page 51 row 410, cd00...OK
Writing page 51 row 411, cd80...OK
Writing page 51 row 412, ce00...OK
Writing page 51 row 413, ce80...OK
Writing page 51 row 414, cf00...OK
Writing page 51 row 415, cf80...OK
Erasing page 170, 2a800...OK
Writing page 170 row 1360, 2a800...(SKIPPED by bootloader)...OK
Writing page 170 row 1361, 2a880...(SKIPPED by bootloader)...OK
Writing page 170 row 1362, 2a900...(SKIPPED by bootloader)...OK
Writing page 170 row 1363, 2a980...(SKIPPED by bootloader)...OK
Writing page 170 row 1364, 2aa00...(SKIPPED by bootloader)...OK
Writing page 170 row 1365, 2aa80...(SKIPPED by bootloader)...OK
Writing page 170 row 1366, 2ab00...(SKIPPED by bootloader)...OK
Writing page 170 row 1367, 2ab80...(SKIPPED by bootloader)...OK

Firmware updated successfully :)!
$

```

- Unplug the Bus Pirate from the PC, wait a moment and reconnect the Bus Pirate. Connect with minicom and verify that the firmware is the correct version with the 'i' command:

```

sudo chmod o+rw /dev/ttyACM0
minicom -b 115200 -D /dev/ttyACM0

```

```

HiZ>i
Bus Pirate v4
Community Firmware v7.1 - CTHWRE Edition [HiZ 1-WIRE UART I2C SPI 2W
DEVID:0x1019 REVID:0x0004 (24FJ256GB106 UNK)
http://dangerousprototypes.com
HiZ>

```

## Using the FTDI Cable

1. Plug in the FTDI cable and determine which device file descriptor was created using dmesg:

```
dmesg | grep -i ttyusb
```

Mine appears as /dev/ttyUSB0, but yours might have a different number. Replace "ttyUSB0" in the following steps with the proper "ttyUSBx" on your machine.

2. Give permissions to /dev/ttyUSB0 and run minicom at 115200 bps:

```

sudo chmod o+rw /dev/ttyUSB0
minicom -b 115200 -D /dev/ttyUSB0

```

3. Turn off hardware flow control to enable sending characters:

```

CTRL-A Z
0
"Serial port setup"
F

```

4. You may be getting garbled data at this bitrate. Try using other bitrates with the -b flag when you start minicom or change the bitrate from within minicom to the proper speed.

## JTAG with a Bus Pirate

**Note:** The instructions for accessing JTAG with a Bus Pirate can be found in the CyberTruck Challenge 2017 Hardware Reverse Engineering Student Workbook and won't be covered during

*this year's class. I wanted to keep the information here for those curious who might want to use JTAG during the event.*

Joint Test Action Group (JTAG) is a standard for “boundary scan” testing and in-circuit debugging, among other things. JTAG uses Serial Peripheral Interface (SPI, pronounced “spy”) for the actual data transmission between the members of the scan chain. Because the Bus Pirate speaks SPI, it can also speak JTAG. Similar to ICSP above, JTAG will allow us to dump the processor’s memory and perform interactive control of the running program.

Interactive debugging can be more useful than static software reverse engineering. During static SW RE of a binary, a reverse engineer must attempt to follow the control flow, but during interactive debugging, the processor follows the control flow itself and the reverse engineer can hitch along for the ride. This ability enables a SW RE engineer to find interesting areas of code such as proprietary crypto algorithms, the addresses of keys, and perhaps even ephemeral security data (e.g. IoT device that only stores crypto material in RAM) even when obfuscated. This is done by setting breakpoints in interesting blocks of code then providing the proper stimulus to cause the hardware to execute the interesting security function. Once the breakpoint is hit, the debugger can read or write memory and registers at will.

The following tools can be used to interface with a JTAG port:

- Bus Pirate – The Bus Pirate is the hardware interface that attaches to the JTAG port on one side and the host PC via USB on the other.
- OpenOCD (<https://sourceforge.net/p/openocd/code/ci/master/tree/>) – OpenOCD is an open-source software tool that supports a range of hardware interfaces for JTAG as well as a wide-variety of targets.
- GDB (<https://www.gnu.org/software/gdb/>)– The GNU Debugger is a free software command line software debugger.
- Eclipse (<https://www.eclipse.org/downloads/>) – Eclipse is an open-source IDE/debugger framework, which provides a visual interface for software debugging.

## Glossary

- **Breakpoint** – A **breakpoint** is a hardware (or software) trigger to stop the processor when performing on-chip debugging.
- **Baud Rate** - The **baud rate** of a digital bus defines the number of times a signal can change on a transmission line per second. This is different from bit rate where bit rate measures the number of logical ‘0’s or ‘1’s that can be transmitted per second. Most digital communication uses two signal states (low/high) with each representing a single bit (0/1), so in those cases baud rate and bit rate are equivalent. Measured in symbols per second.
- **Bit Rate** - The **bit rate** of a digital bus defines the number of times a logical ‘0’ or ‘1’ can be sent on a transmission line per second. This is different from baud rate where baud rate measures the number of symbols that can be transmitted per second. Most digital communication uses two

signal states (low/high) with each representing a single bit (0/1), so in those cases baud rate and bit rate are equivalent. Measured in bits per second.

- **Device file** – A **device file** is a special file in Unix and Linux which represents a device connection rather than a file in the filesystem on a disk.
- **GCC** – The **GNU Compiler Collection (GCC)** is a free and open-source compiler that is part of the GNU project.
- **GDB** – The **GNU Debugger** is a free and open-source command-line software debugger that is part of the GNU project.
- **ICD/OCD** – In-circuit debugging (ICD) and on-chip debugging (OCD) are terms used for debugging hardware in-situ. The debugging circuitry is installed in the hardware inside of or alongside the microcontroller/processor.
- **JTAG** – **JTAG** stands for Joint Test Action Group. JTAG is a standard for simple hardware testing and in-situ (ICD/OCD) debugging of hardware.
- **Microcontroller** – A **microcontroller** is a (usually small and slow) system-on-a-chip (SoC) packaged as a single integrated circuit (IC) which includes one or more processor cores, read-only memory (ROM), random-access memory (RAM) and peripherals, such as those for serial communications or analog/digital conversion.
- **Multimeter** – A **multimeter** is an electronics engineering tool used for measuring simple properties like voltage and current. Unlike an oscilloscope, a multimeter generally cannot analyze time-varying signals.
- **Oscilloscope** – An **oscilloscope** is an electronics engineering tool for analyzing analog signals in real-time.
- **PCB** – A **Printed Circuit Board (PCB)** is a computer board with various electrical interconnects (called traces) laid into a single- or multi-layer substrate to form circuits connecting the discrete components, such as integrated circuits (ICs) and passives like resistors and capacitors.
- **Silk screen** – **Silk screen** is a nonfunctional annotation layer on the top and/or bottom of a PCB which often shows component identifiers and sometimes even comments.
- **Tuning** – In automotive electronics, **tuning** is the process of performing hardware and/or software modifications to the vehicle's control systems (such as an engine controller) to achieve a different performance profile than the vehicle was designed and shipped with.
- **UART** – A **Universal Asynchronous Receiver/Transmitter (UART)** is a computer peripheral technology for serial data communications, commonly employed to create a serial terminal for debugging and development.