

Two-Timing Data Connectors

Kyle Osborn
kos@kos.io
@theKos

Michael Ossmann
mike@ossmann.com
@michaelossmann

2013

INFILTRATE

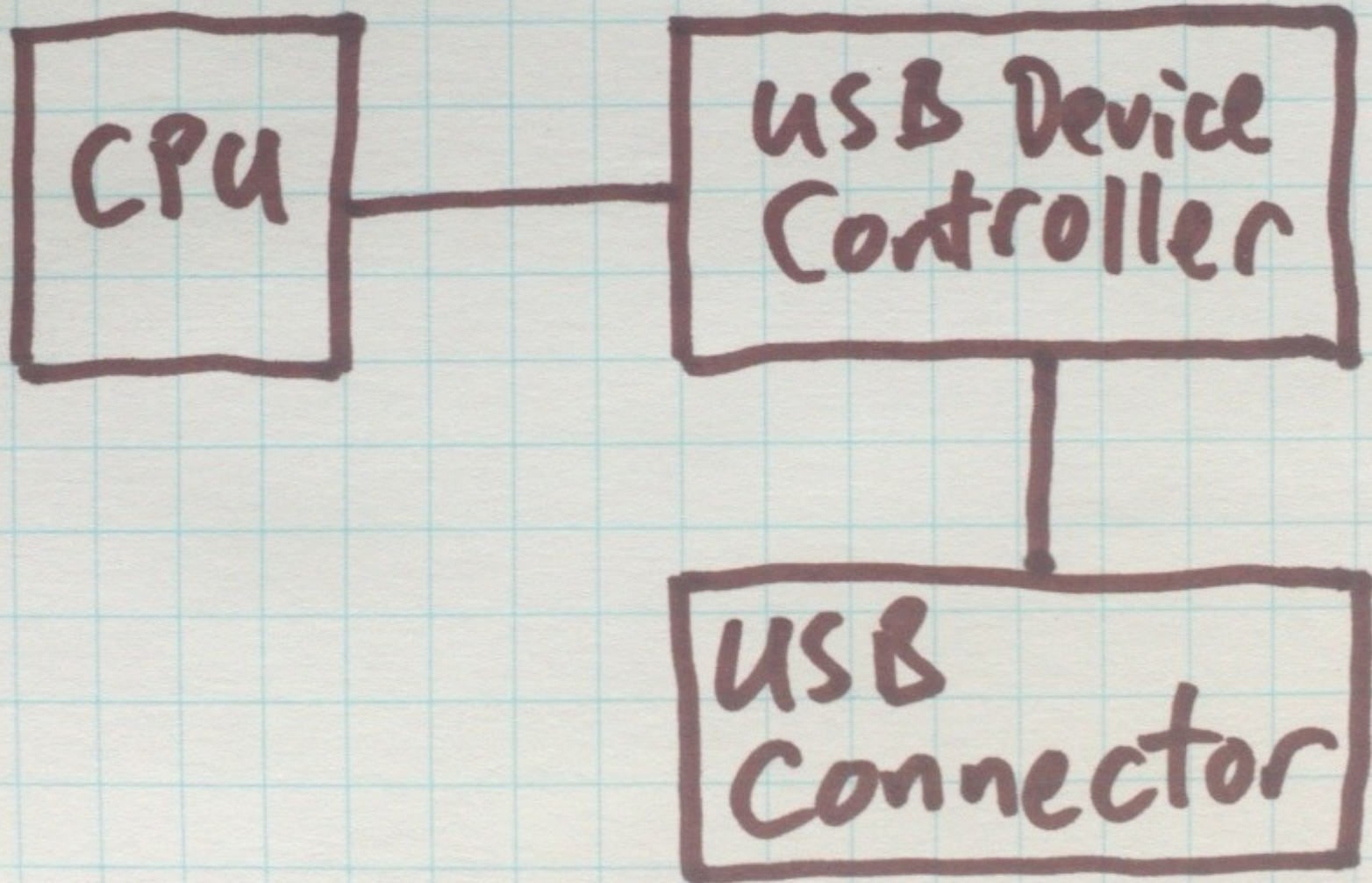
You've locked
your Android
device.

You've disabled

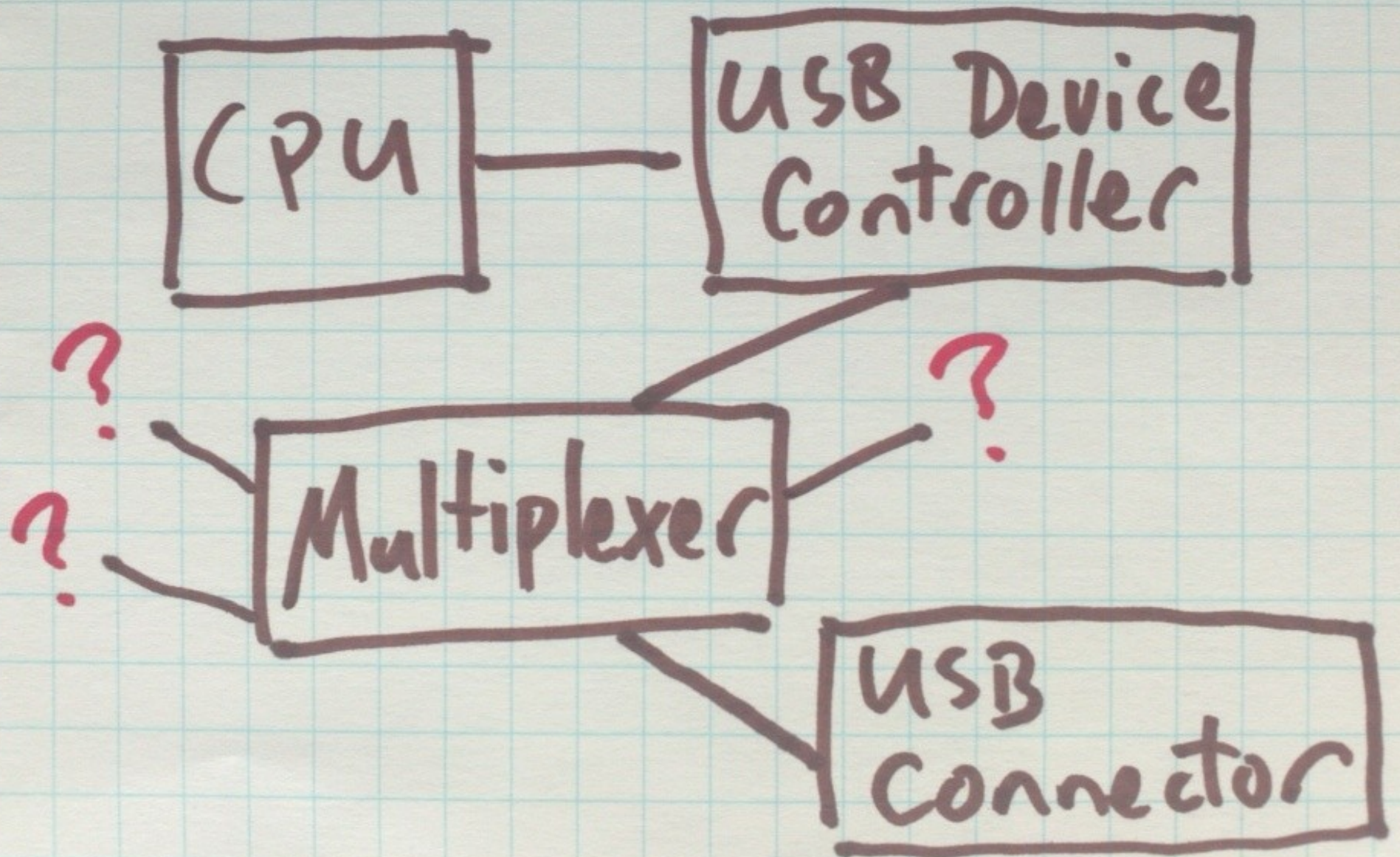
debugging (adb).

A customs officer
can still plug
into your USB
port and get a
shell.

A Typical USB Device



A Mobile Phone



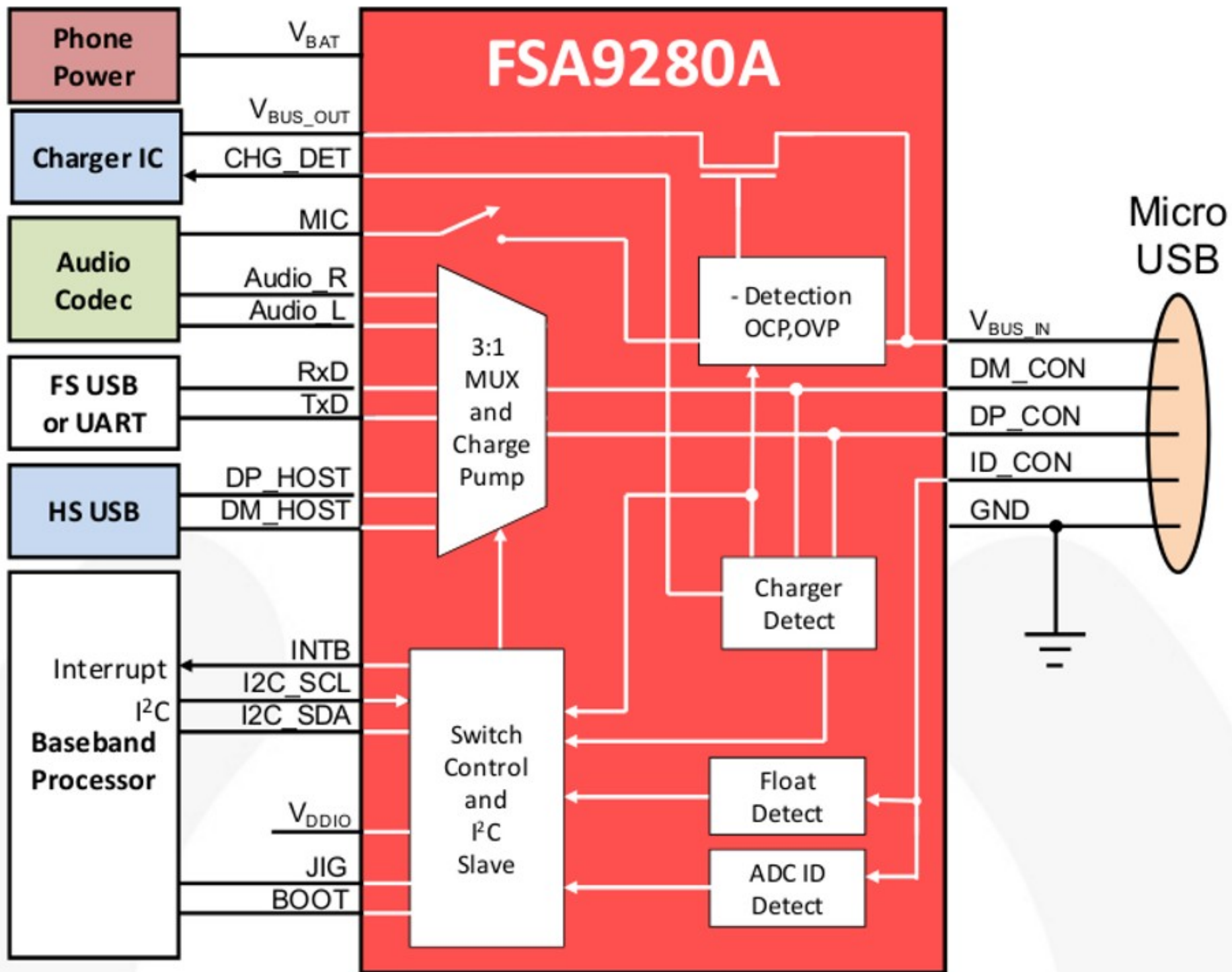


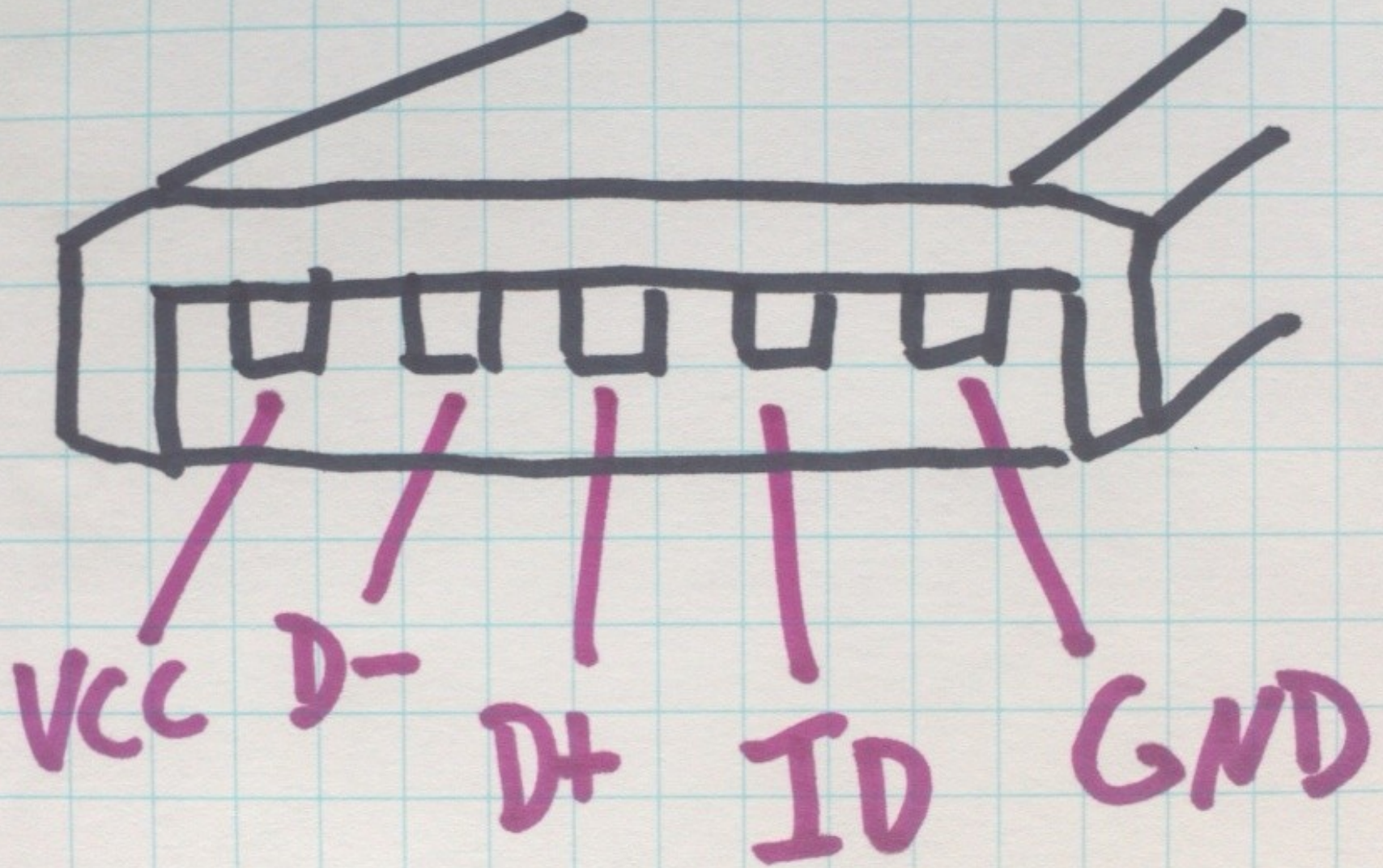
Figure 2. Block Diagram

Multiplexed Functions

USB On-the-Go (OTG)

Audio (USB Car kit)

Debug and
Programming Interfaces



Binary Value ⁽⁴⁾	ID_CON resistance to GND			Accessory Detected ⁽⁵⁾
	Min.	Typ.	Max.	
00000	GND	GND	GND	DO NOT USE
00001	1.9k Ω	2k Ω	2.1k Ω	Audio Send/End Button
00010	2.47k Ω	2.604k Ω	2.73k Ω	Audio Remote S1 Button ⁽⁶⁾
00011	3.05k Ω	3.208k Ω	3.37k Ω	Audio Remote S2 Button ⁽⁶⁾
00100	3.81k Ω	4.014k Ω	4.21k Ω	Audio Remote S3 Button ⁽⁶⁾
00101	4.58k Ω	4.82k Ω	5.06k Ω	Audio Remote S4 Button ⁽⁶⁾
00110	5.73k Ω	6.03k Ω	6.33k Ω	Audio Remote S5 Button ⁽⁶⁾
00111	7.63k Ω	8.03k Ω	8.43k Ω	Audio Remote S6 Button ⁽⁶⁾
01000	9.53k Ω	10.03k Ω	10.53k Ω	Audio Remote S7 Button ⁽⁶⁾
01001	11.43k Ω	12.03k Ω	12.63k Ω	Audio Remote S8 Button ⁽⁶⁾
01010	13.74k Ω	14.46k Ω	15.18k Ω	Audio Remote S9 Button ⁽⁶⁾
01011	16.4k Ω	17.26k Ω	18.12k Ω	Audio Remote S10 Button ⁽⁶⁾
01100	19.48k Ω	20.5k Ω	21.53k Ω	Audio Remote S11 Button ⁽⁶⁾
01101	22.87k Ω	24.07k Ω	25.27k Ω	Audio Remote S12 Button ⁽⁶⁾
01110	27.27k Ω	28.7k Ω	30.14k Ω	Reserved Accessory #1
01111	32.3k Ω	34k Ω	35.7k Ω	Reserved Accessory #2
10000	38.19k Ω	40.2k Ω	42.21k Ω	Reserved Accessory #3
10001	47.41k Ω	49.9k Ω	52.4 k Ω	Reserved Accessory #4
10010	61.66k Ω	64.9k Ω	68.15k Ω	Reserved Accessory #5
10011	76.1k Ω	80.7k Ω	84.1k Ω	DO NOT USE
10100	96.9k Ω	102k Ω	107.1k Ω	DO NOT USE
10101	115k Ω	121k Ω	127k Ω	TTY Converter
10110	143k Ω	150k Ω	157k Ω	UART Cable
10111	190k Ω	200k Ω	210k Ω	See Table 4
11000	242k Ω	255k Ω	268k Ω	Factory Mode Boot OFF-USB ⁽⁷⁾
11001	292k Ω	301k Ω	316k Ω	Factory Mode Boot ON-USB ⁽⁷⁾
11010	347k Ω	365k Ω	383k Ω	DO NOT USE
11011	419.9k Ω	442k Ω	464k Ω	See Table 4
11100	507k Ω	523k Ω	549k Ω	Factory Mode Boot OFF-UART ⁽⁷⁾
11101	588k Ω	619k Ω	650k Ω	Factory Mode Boot ON-UART ⁽⁷⁾
11110	750k Ω	1000k Ω	1050k Ω	Audio Type 1 with Remote ⁽⁸⁾
	750k Ω	1002k Ω	1050k Ω	Audio Type 1 / Only Send-End ⁽⁸⁾

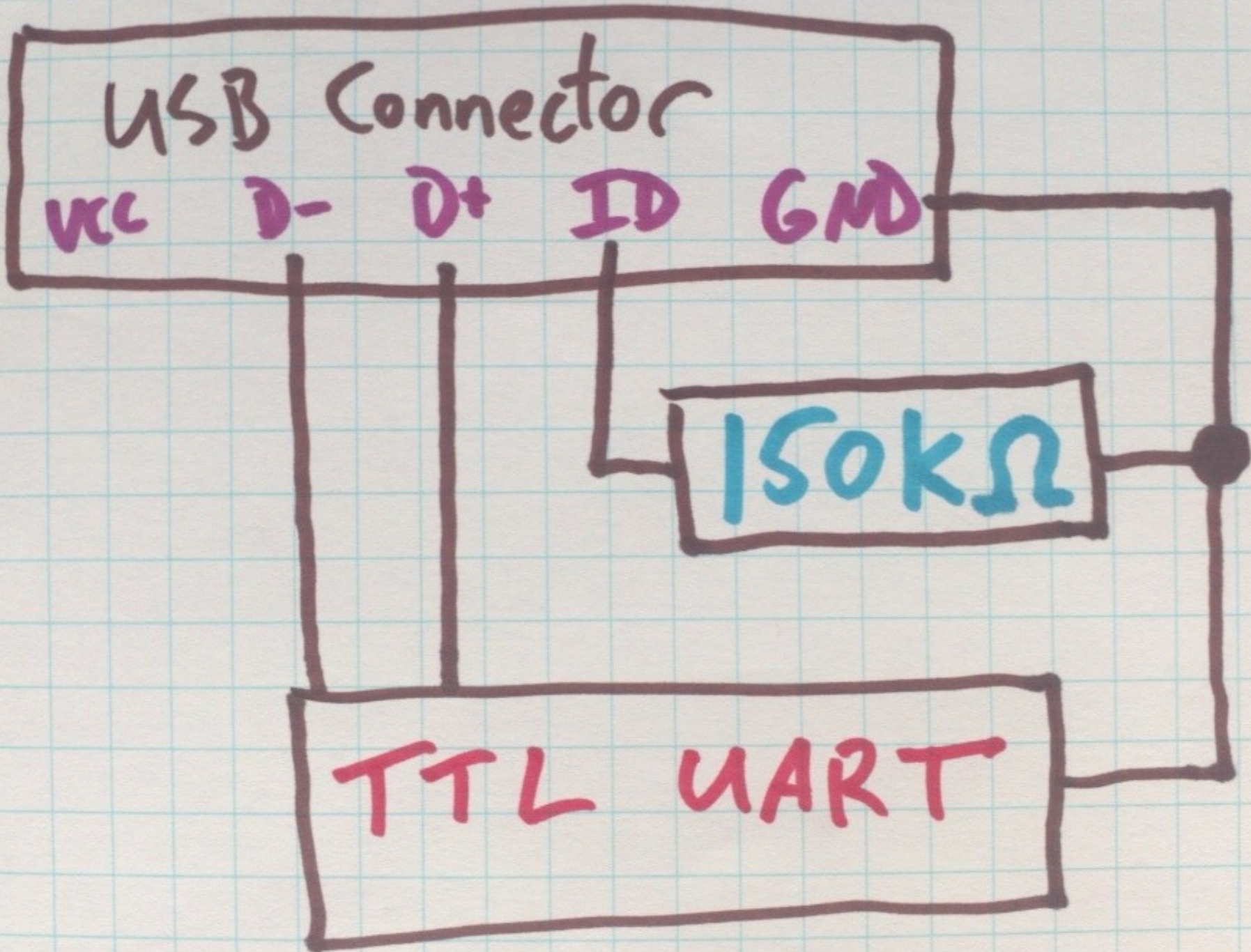
64.9kΩ	68.15kΩ	Reserved Accessory #5
80.7kΩ	84.1kΩ	DO NOT USE
102kΩ	107.1kΩ	DO NOT USE
121kΩ	127kΩ	TTY Converter
150kΩ	157kΩ	UART Cable
200kΩ	210kΩ	<i>See Table 4</i>
255kΩ	268kΩ	Factory Mode Boot OFF-USB ⁽⁷⁾
301kΩ	316kΩ	Factory Mode Boot ON-USB ⁽⁷⁾
365kΩ	383kΩ	DO NOT USE
442kΩ	464kΩ	<i>See Table 4</i>
523kΩ	549kΩ	Factory Mode Boot OFF-UART ⁽⁷⁾
619kΩ	650kΩ	Factory Mode Boot ON-UART ⁽⁷⁾
1000kΩ	1050kΩ	Audio Type 1 with Remote ⁽⁸⁾
1000kΩ	1050kΩ	Audio Type 1 with Remote ⁽⁸⁾

UART

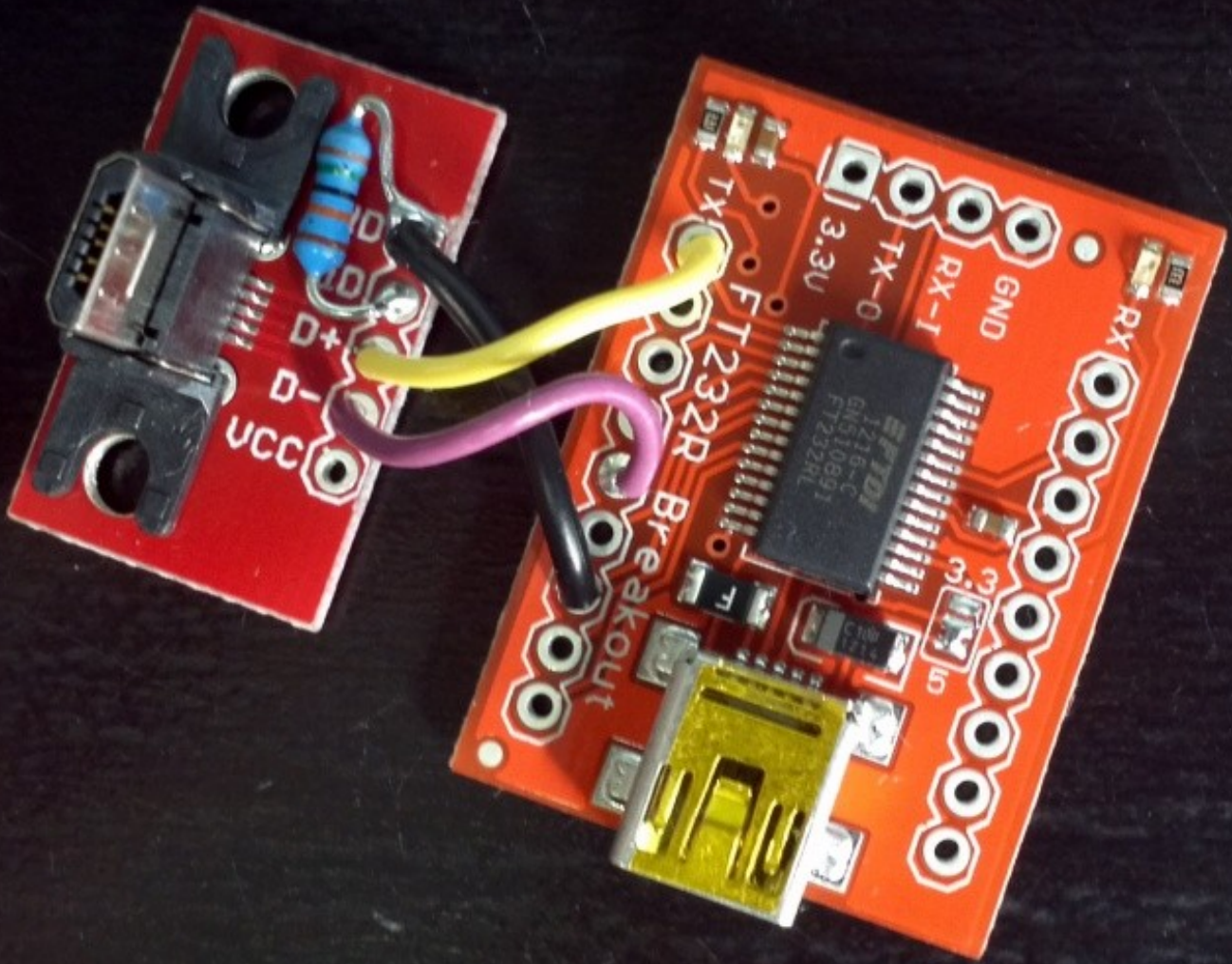
9600
19200
38400
115200
etc.

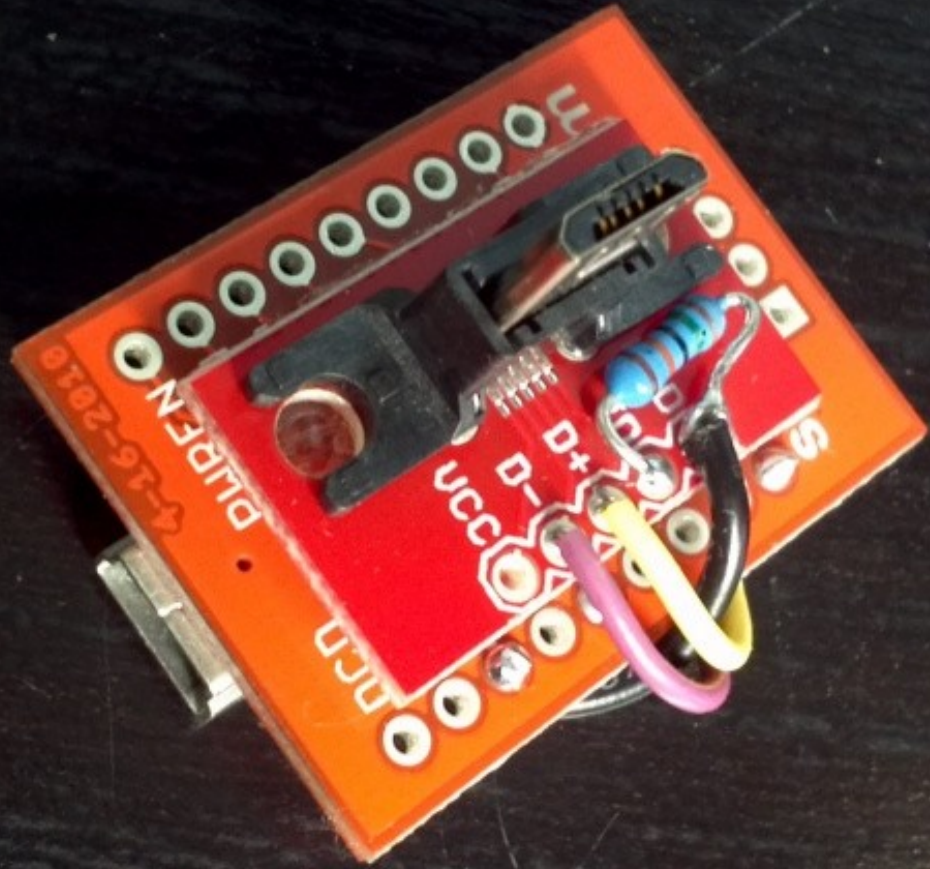
RS-232: crazy
 $\pm V$

TTL: 0 to low V



Let's build it!






```
debug>
debug>
debug>
debug> help
FIQ Debugger commands:
pc          PC status
regs        Register dump
allregs     Extended Register dump
bt          Stack trace
reboot      Reboot
irqs        Interrupt status
kmsg        Kernel log
version     Kernel version
sleep       Allow sleep while in FIQ
nosleep     Disable sleep while in FIQ
console     Switch terminal to console
cpu         Current CPU
cpu <number> Switch to CPU<number>
ps          Process list
sysrq       sysrq options
sysrq <param> Execute sysrq with <param>
debug> suspending fiq debugger
```

FIQ Debugger

arch/arm/common/fiq-debugger.c

PC

bt

kgdb*

allregs

console

* usually compiled in read-only
unprivileged mode without
kgdb

FIQ Debugger

detailed
process
information

registers
in use

console
shell

kernel
log

kernel
debugger

Let's try it!

Commercial Test Jigs

Debug interfaces
are meant to be used
by someone...

Samsung Anyway S102

Supports
many
phones
and tablets

Various
cables
available

predecessors: S100, S101

+ VBATT - + F/B - DC5V



Anyway

High Current
S102

TEST PACK

USB

UART1

UART2

No	Solution	Function		
		Mode	Off	On
1	Agere TC	Boot	Low	High
2	Hp, Vision, Infineon	SDS	O	X
3	NXP Sysol	USB	O	X
4	NXP Swift Broadcom	DBG	X	O
5	UMTS(Qualcomm)	M-USB	Use	Not Use
6	EMP	ID type	UART	USB
7	-	ID-BOOT	Boot-On	Boot-Off
8	-	-	-	-
9	-	SDS TRX	-	Loop
10	-	DBG TRX	-	Loop

O : Connect X : Disconnect

VBATT
On - Off Solution Function

Let's buy it!

GH99-36900B \$122.50

GH39-01339A \$37.15
(usb)

5V power \$5.95

total under \$200



No	Solution	Mod	BC	SC
1	Agere TC			
2	Hp, Vision, Infineon			
3	Hp, Vision, Braacomm			
4	NXP S5901 (NXP S5901)			
5	NXP S5901 (NXP S5901)			
6	EMIP			
7	UMTS/Qualcomm			
8				
9				
10				

VBATT On-Off

SAMSUNG

AnyWave

TEST PACK

+ VBATT

+ F/B



Mode	Function
Boot	Off
SDS	Low
USB	On
DBG	High
M-USB	On
ID-USB	X
ID-Type	X
ID-BOOT	Use
UART	Use
Boot-On	0
Boot-Off	0
USB	Use
Loop	Loop
Disconnect	X: Disconnect

VBATT + -
F/B + -
DC5V

USB

UART1

UART2

High Current S102



VBATT
On - Off

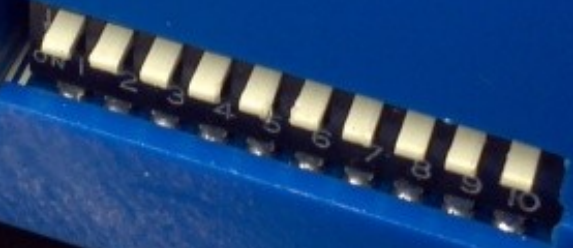
Solution

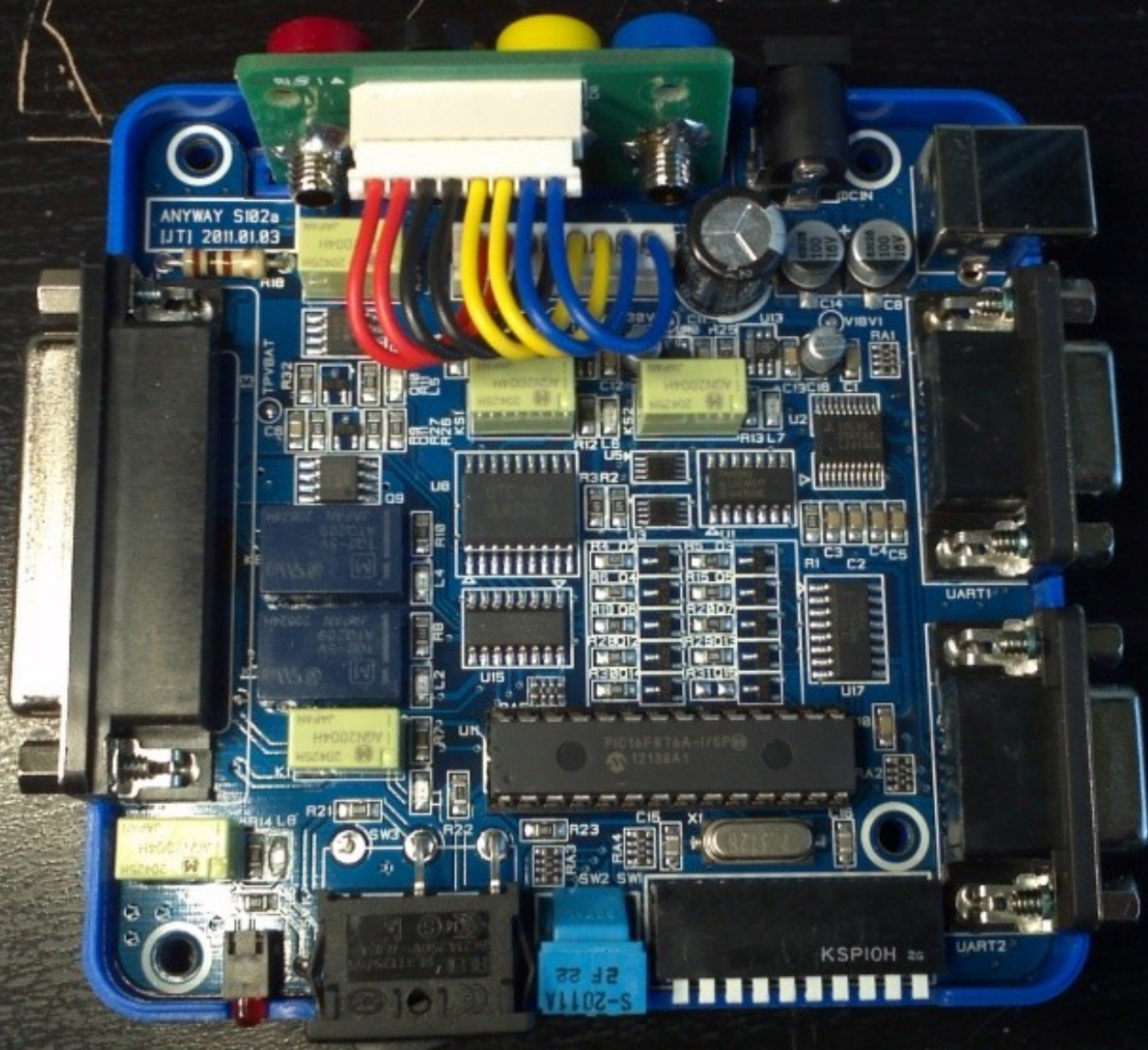
Function

7	Qualcomm	adcom	Boot	Off	Function
8	Qualcomm	adcom	SDS	Low	On
9	-	-	USB	0	High
10	-	-	DBG	0	X
	-	-	M-USB	X	X
	-	-	ID type	Use	0
	-	-	ID-BOOT	UART	Not Use
	-	-	-	Boot-On	USB
	-	-	SDS TRX	-	Boot-Off
	-	-	DBG TRX	-	-
	-	-	0 : Connect	-	Loop
	-	-	X : Disconnect	-	Loop

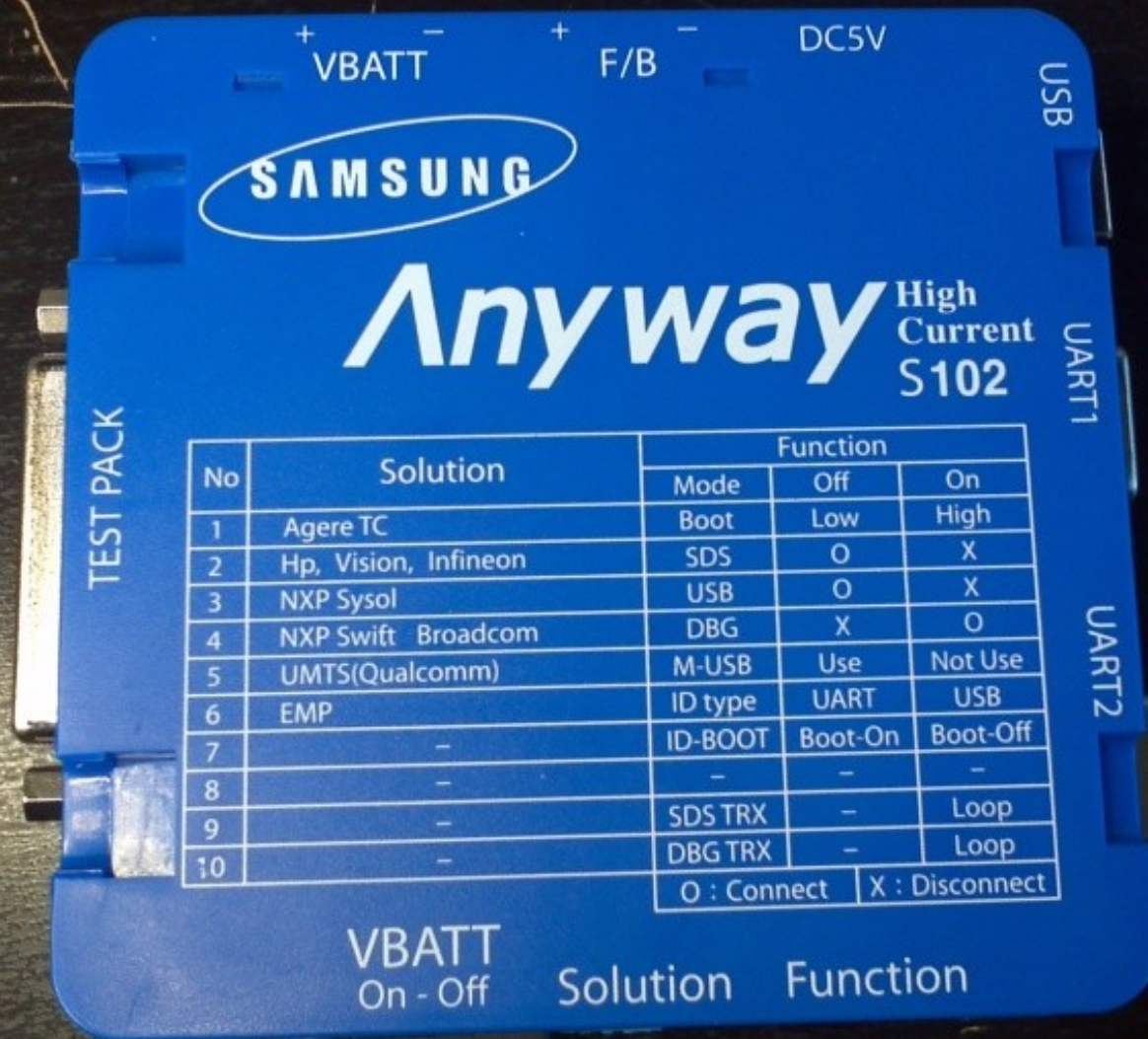
UART1

UART2





Anyway S102 Functions



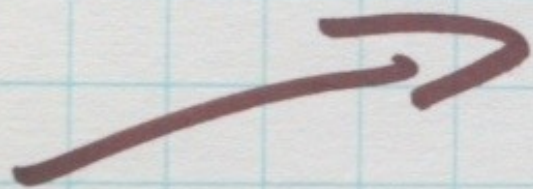
64.9k Ω	68.15k Ω	Reserved Accessory #5
80.7k Ω	84.1k Ω	DO NOT USE
102k Ω	107.1k Ω	DO NOT USE
121k Ω	127k Ω	TTY Converter
150k Ω	157k Ω	UART Cable
200k Ω	210k Ω	<i>See Table 4</i>
255k Ω	268k Ω	Factory Mode Boot OFF-USB ⁽⁷⁾
301k Ω	316k Ω	Factory Mode Boot ON-USB ⁽⁷⁾
365k Ω	383k Ω	DO NOT USE
442k Ω	464k Ω	<i>See Table 4</i>
523k Ω	549k Ω	Factory Mode Boot OFF-UART ⁽⁷⁾
619k Ω	650k Ω	Factory Mode Boot ON-UART ⁽⁷⁾
1000k Ω	1050k Ω	Audio Type 1 with Remote ⁽⁸⁾
1000k Ω	1050k Ω	Audio Type 1 with Remote ⁽⁸⁾

Let's try it!

console

/dev/tty[FIQ]

"shell" user



Same user as adb
but without the
same groups

elevate privilege?


```
ser.write("echo ""+tmpread.read()+">  
/data/local/tmp/" + filename + '\t\n\x03')
```

install APK with pm?

binary exploits
(mempodipper, etc.)?

Ever tried delivering a
payload over a slow,
unreliable serial console
that can only handle
31 input bytes at a
time?

smaller payload?

Tiniest_antiguard.apk

4.6 kB

built from previous app
called AntiGuard

17 kB → stripped functions

← compiled → decompiled to smali

← stripped more → re compiled

signed → 4.6 kB

F A I L

moving on...

no wget

no netcat

DNS TXT?

SSIDs ???

/system/bin/adb ?

- adb client on newer phones
- allows remote adb instance
- network adb pull?

other options

Select "name" and "value" columns from secure settings where "name" is equal to "new_setting" and sort the result by name in ascending order.

```
adb shell content query --uri  
content://settings/secure --projection name:value  
--where "name='new_setting'" --sort "name ASC"
```

```
data/data/com.android.provers.settings/  
databases/settings.db (sqlite)
```

content

```
Row: 18 name=screensaver_default_component, value=com.g
Row: 19 name=accessibility_display_magnification_enabled
Row: 20 name=accessibility_display_magnification_auto_up
Row: 21 name=android_id, value=1162b2e9f3616a6a
Row: 22 name=selected_spell_checker, value=com.google.a
Row: 23 name=selected_spell_checker_subtype, value=0
Row: 24 name=voice_recognition_service, value=com.google
Row: 25 name=bluetooth_name, value=Nexus 4
Row: 26 name=bluetooth_address, value=10:68:3F:D6:CA:70
Row: 27 name=bluetooth_addr_valid, value=1
Row: 28 name=masterLocationPackagePrefixBlacklist, valu
Row: 29 name=serial_blacklist, value=827,864
Row: 30 name=dropbox:data_app_anr, value=disabled
Row: 31 name=dropbox:data_app_wtf, value=disabled
Row: 32 name=ssl_session_cache, value=file
Row: 33 name=pubkey_blacklist, value=5f3ab33d55007054bc
```


context

```
Row: 41 name=wifi_on, value=0  
Row: 42 name=bluetooth_on, value=0  
Row: 43 name=adb_notify, value=0  
Row: 44 name=development_settings_enabled, value=0  
Row: 45 name=adb enabled, value=0
```

XDA Developers

public knowledge

not common knowledge

Next Steps

MOAR PHONES

headphone jacks?
other ports?

Next Steps

Custom hardware

- configurable

I/O voltage

- configurable pinout

- configurable
resistance

Questions?

<http://grantscottgadgets.com/>
infiltrate2013