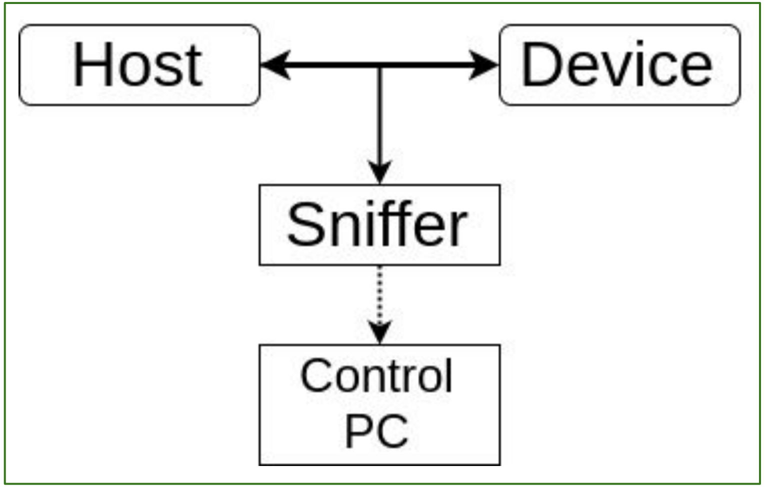
USB PHY on FPGA

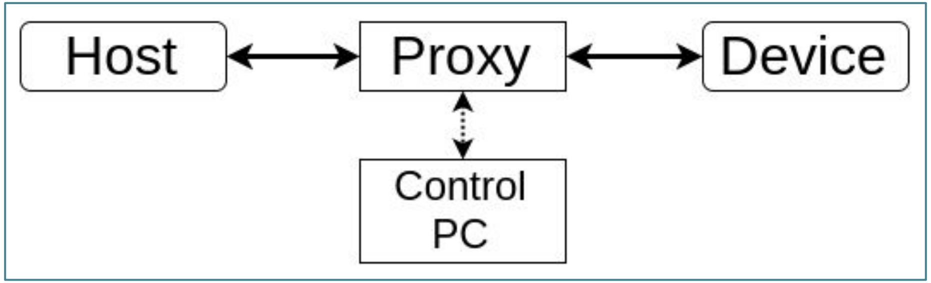


Host

Device

Sniffer

Control PC

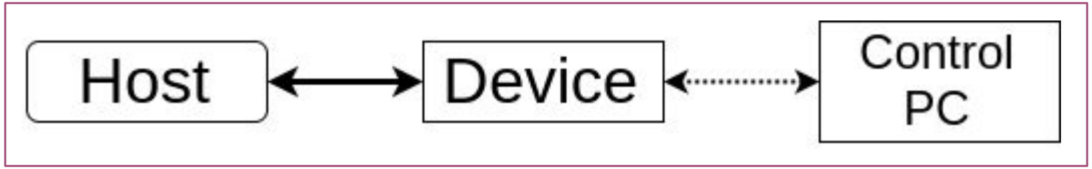


Host

Proxy

Device

Control PC

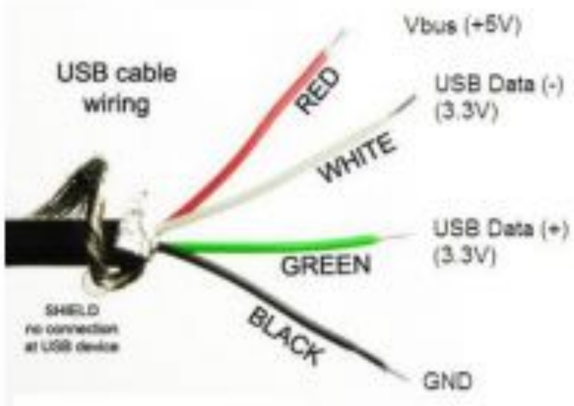


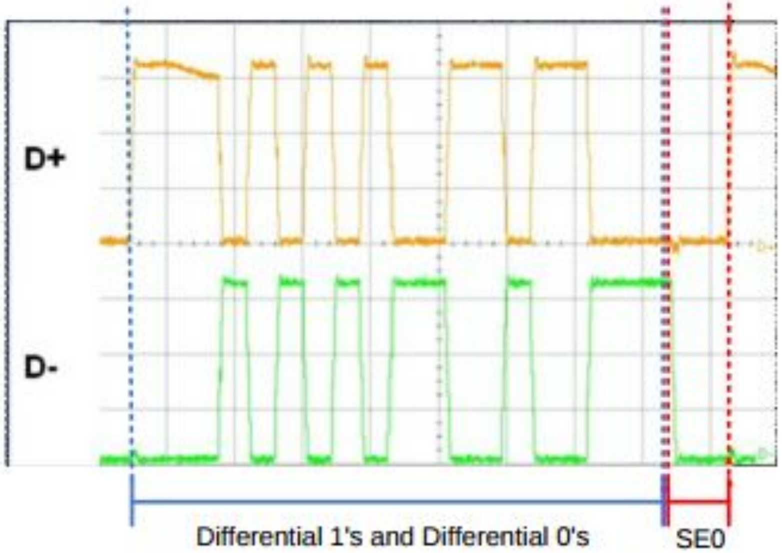
Host

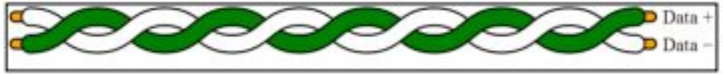
Device

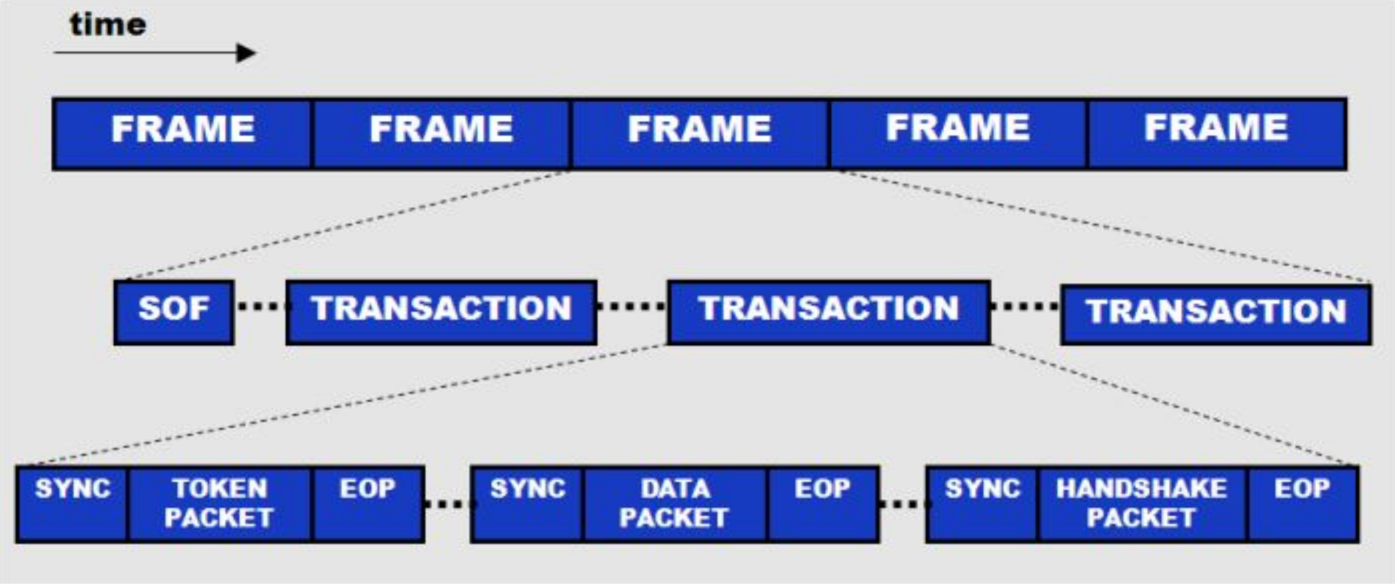
Control PC

1. Снифферы
    a. Логические анализаторы: Saleae, Dreamsource, etc.
    b. https://www.totalphase.com/products/beagle-usb12/
    c. http://openvizsla.org/
    d. MAX3421 + https://github.com/Xarlan/usbsniff
    e. Beaglebone + https://beagleboard.org/p/drinkcat-myopenid-com/usb-sniffer-ba62d2
2. Прокси
    a. Beaglebone-like usb proxy (https://github.com/dominicgs/USBProxy)
    b. Custom FPGA proxy
    c. Atmega + https://github.com/matlo/serialusb
3. Fuzzing/badUSB, etc.
    a. http://goodfet.sourceforge.net/hardware/facedancer21/
    b. Other MCU/MAX4321…


USB cable wiring
Vbus (+5V)
RED
USB Data (-) (3.3V)
WHITE
USB Data (+) (3.3V)
GREEN
BLACK
GND
SHIELD no connection at USB device

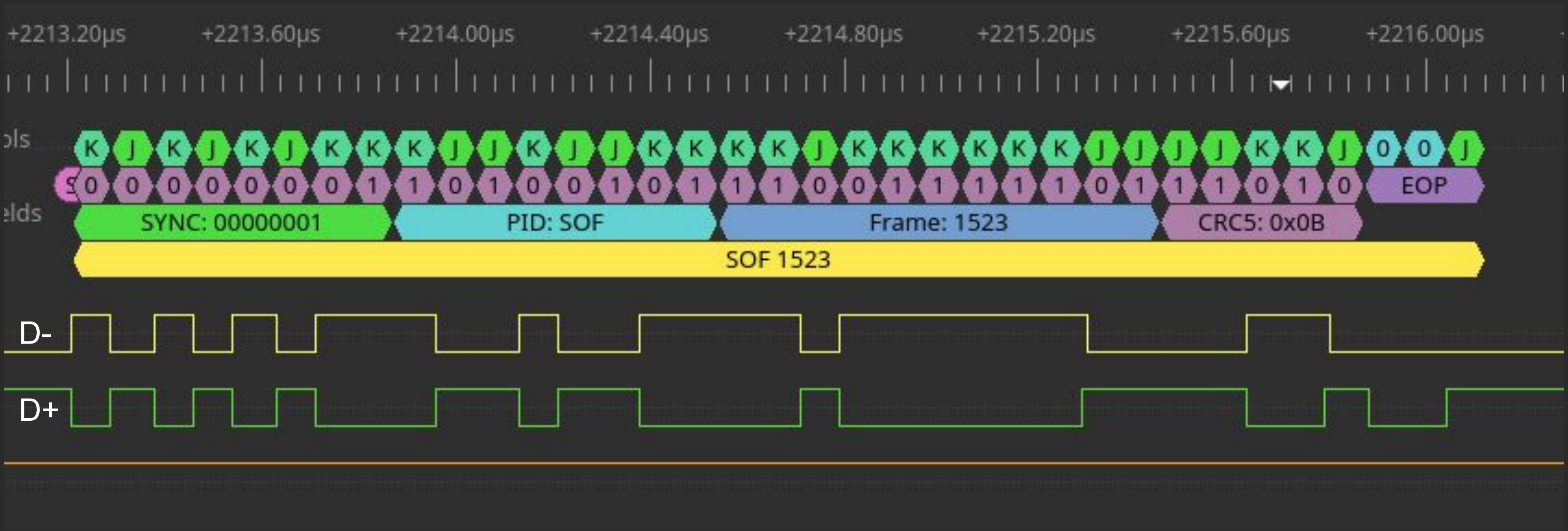

D+
D-
Differential 1's and Differential 0's
SE0


Data +
Data −

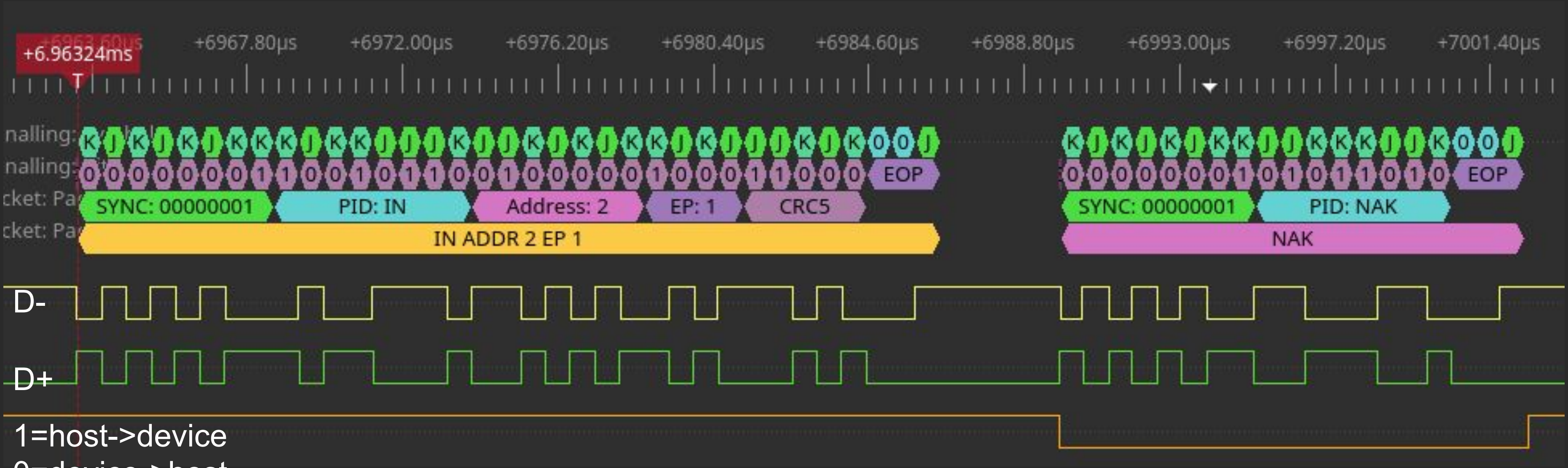


time
FRAME
FRAME
FRAME
FRAME
FRAME
SOF
TRANSACTION
TRANSACTION
TRANSACTION
SYNC
TOKEN PACKET
EOP
SYNC
DATA PACKET
EOP
SYNC
HANDSHAKE PACKET
EOP

Start Of Frame transaction

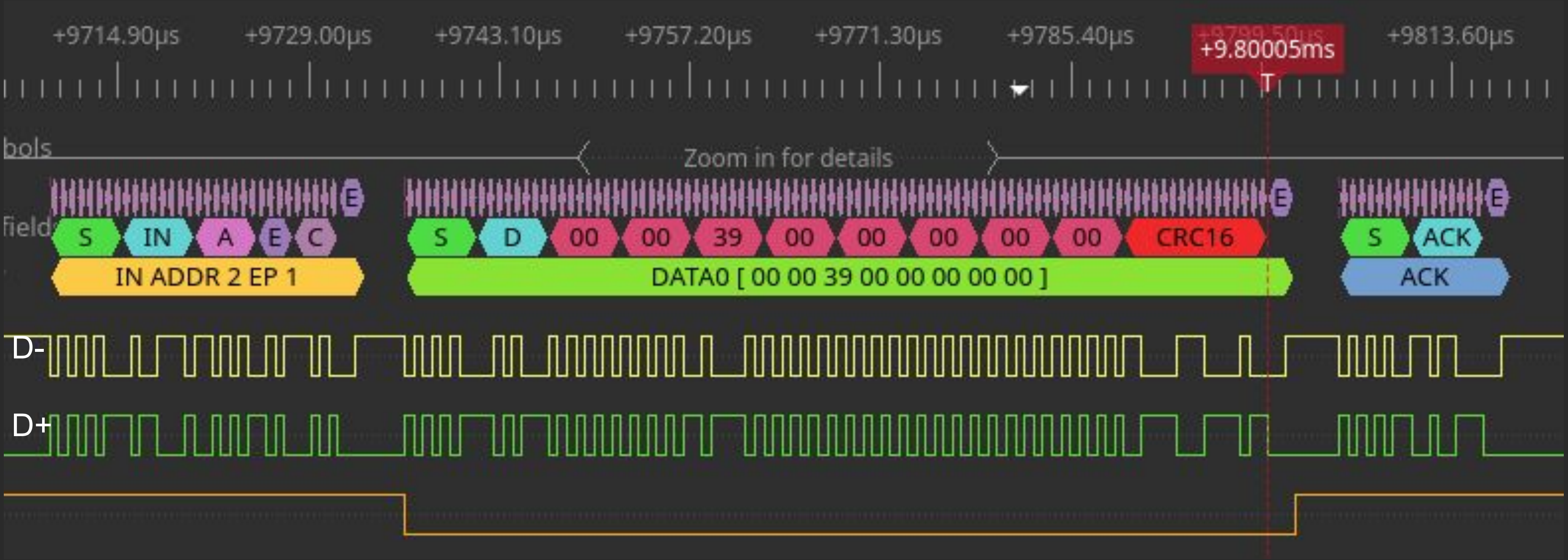


IN+NAK transaction

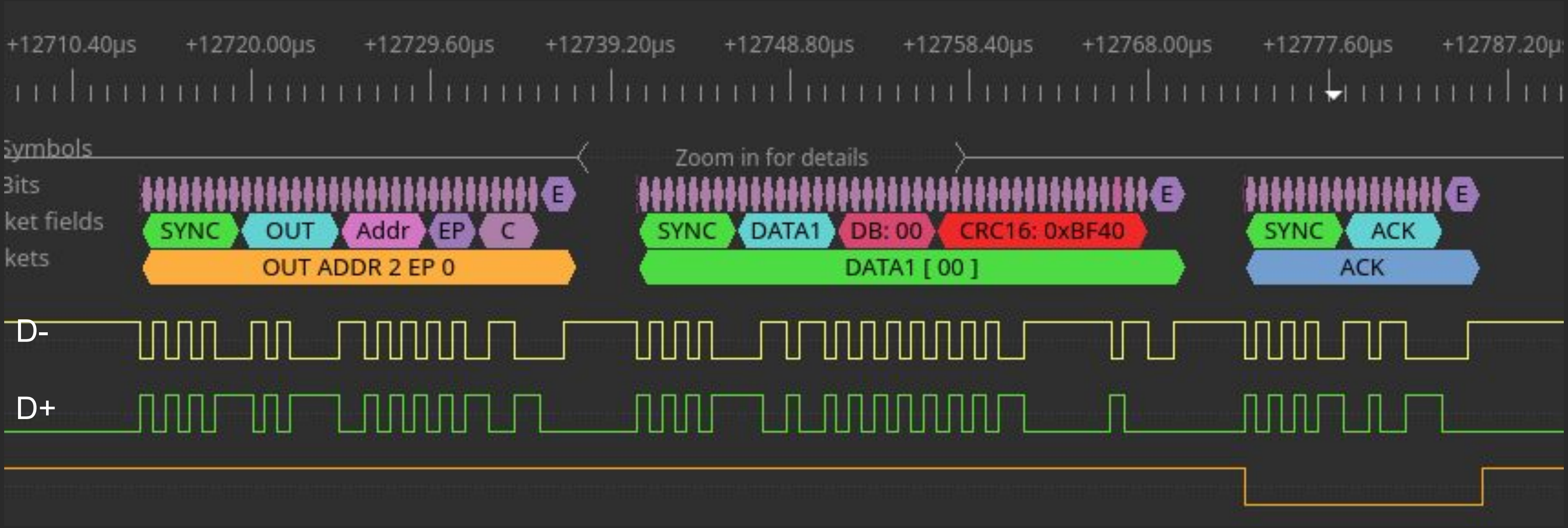


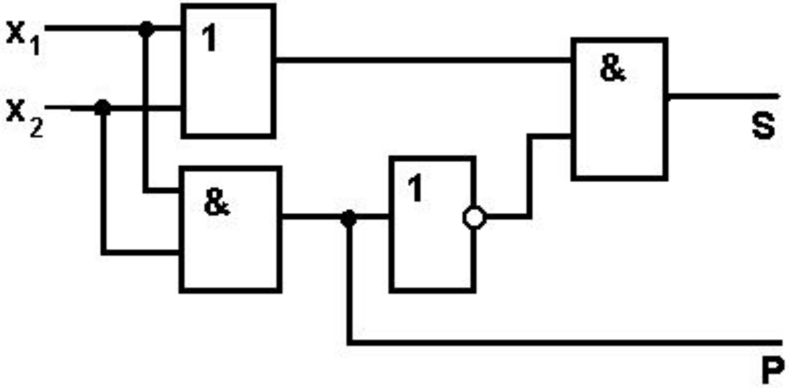
1=host->device
0=device->host

IN+DATA transaction



OUT/SETUP transaction

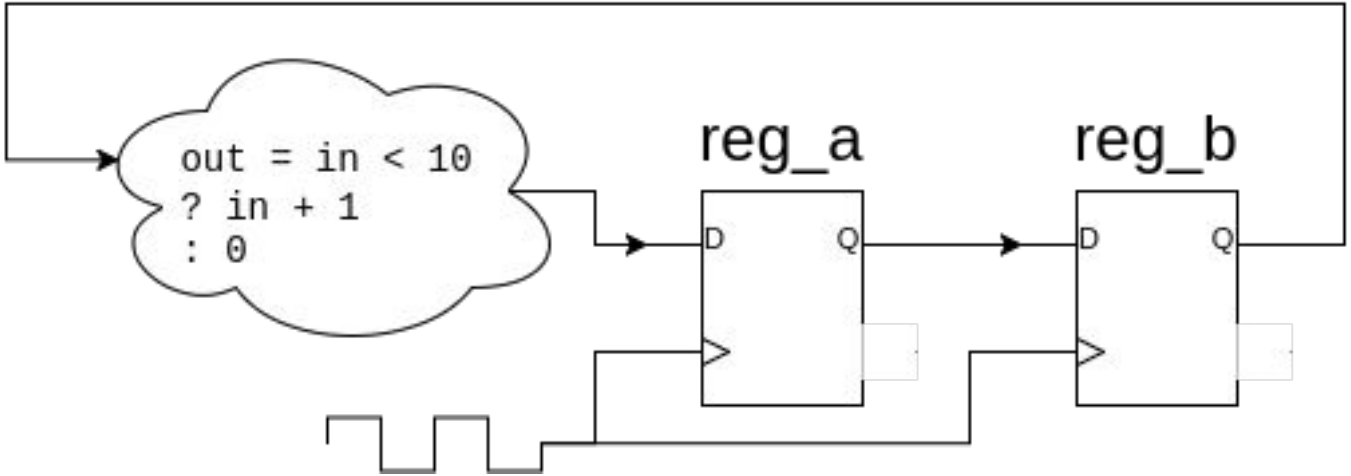




```
module(in x1, in x2, out S, out P);

assign P = x1 & x2;
assign S = (x1 | x2) & (~P);

endmodule
```



```
wire[3:0] comb_out = reg_b < 10 ?
reg_b + 1 : 0;

reg[3:0] reg_a;
reg[3:0] reg_b;

always @(posedge clk) begin
     reg_b <= reg_a;
     reg_a <= comb_out;
end
```

```
reg[3:0] reg_a;
reg[3:0] reg_b;

always @(posedge clk) begin
     if(reg_b < 10)  reg_a <= reg_b + 1;
     else reg_a <= 0;

     reg_b <= reg_a;
end
```

```
reg[3:0] reg_a;
reg[3:0] reg_b;

always @(posedge clk) begin
    reg_b <= reg_a;
    reg_a <= reg_b;
end
```

Ссылки

- https://github.com/qanper/usbproxy
- https://www.devalias.net/devalias/2018/05/13/usb-reverse-engineering-down-the-rabbit-hole/
- https://www.beyondlogic.org/usbnutshell/usb1.shtml
- http://www.cypress.com/documentation/application-notes/an57294-usb-101-introduction-universal-serial-bus-20

thx

Andrew Strokov

@aanper

https://t.me/shitsch