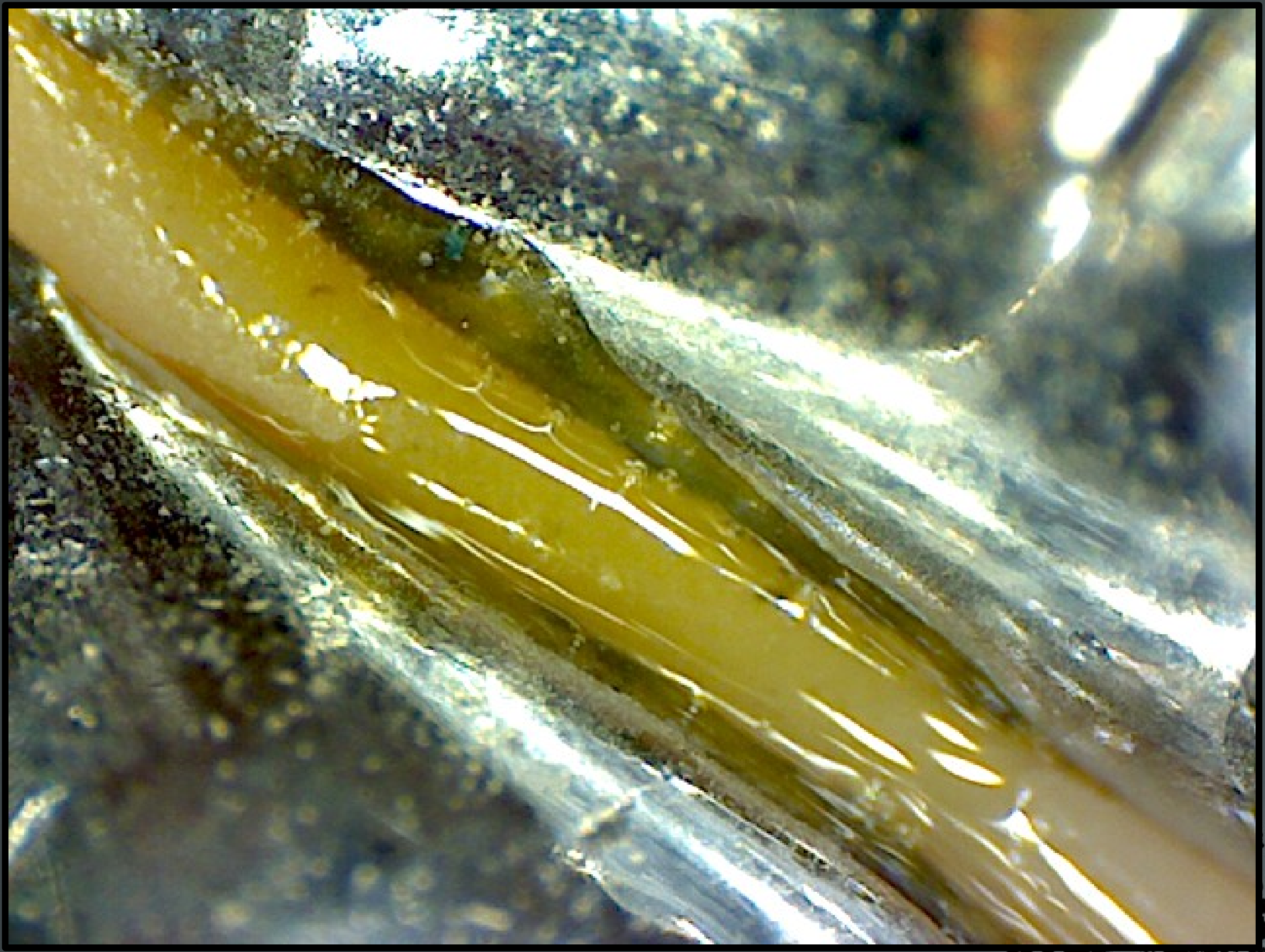
What Is This?



All Your Codes Belong To Me!!

Keith Howell

Electronics Engineer in the British Army

Network Engineer and Security Engineer for UUNET Technologies

Professional Locksmith and Access Control Technician

Security Engineer for Assurance Data Inc

Member of the local NoVaHackers group

All Your Codes Belong To Me!!

A voyage into the secrets of alarm panels and a whole new world of ”security by obscurity”

I also hope to show you how it is not too difficult for people in computer security to adapt their skills and explore the field of physical security

Starting the Investigation

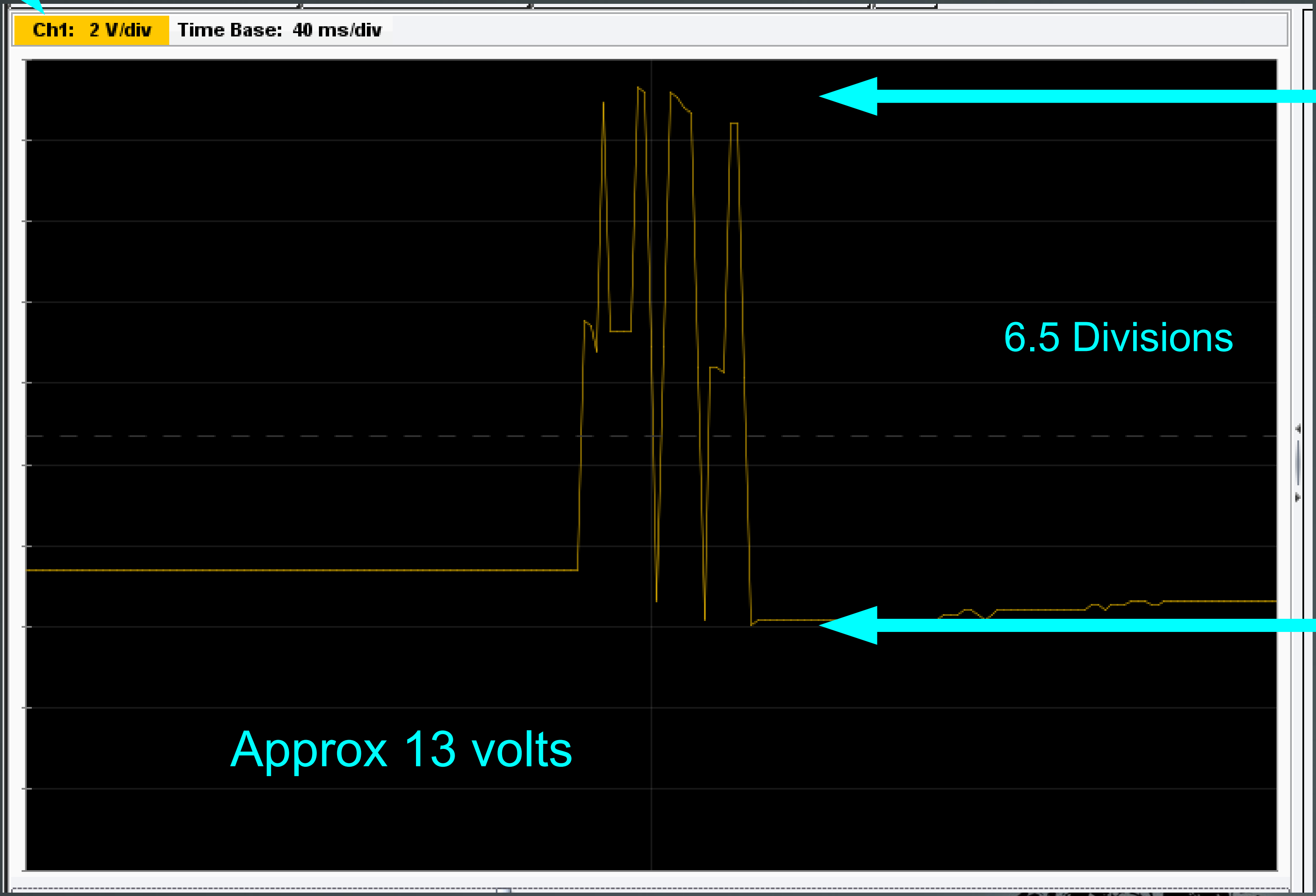
Alarm system uses a 4 wire bus between the panel and additional devices such as keypads:

Ground	(black wire)
Power	(red wire)
Data In	(green wire)
Data Out	(yellow wire)

First Look At The Bus

- How?
  - Unknown Voltage
  - Unknown Protocol
- Oscilloscope
  - High Impedance
  - Voltage Isolated
  - Simple Measuments

First Look At The Bus



Ch1: 2 V/div Time Base: 40 ms/div

6.5 Divisions

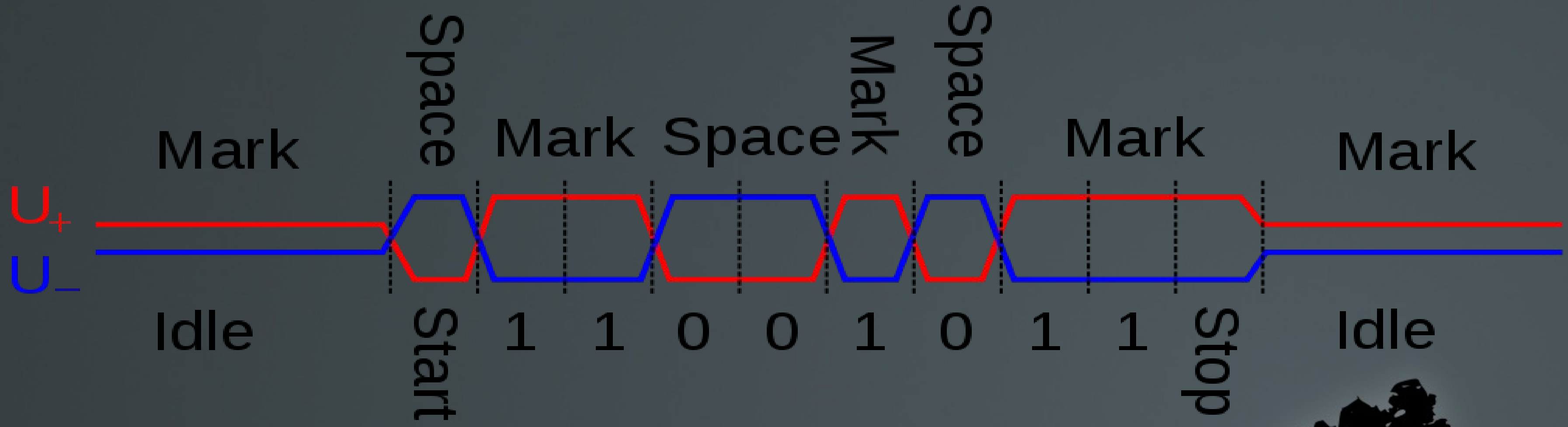
Approx 13 volts

What is the bus?

RS-485

Does not use differential signaling

Wrong voltages (-7v to +12v)

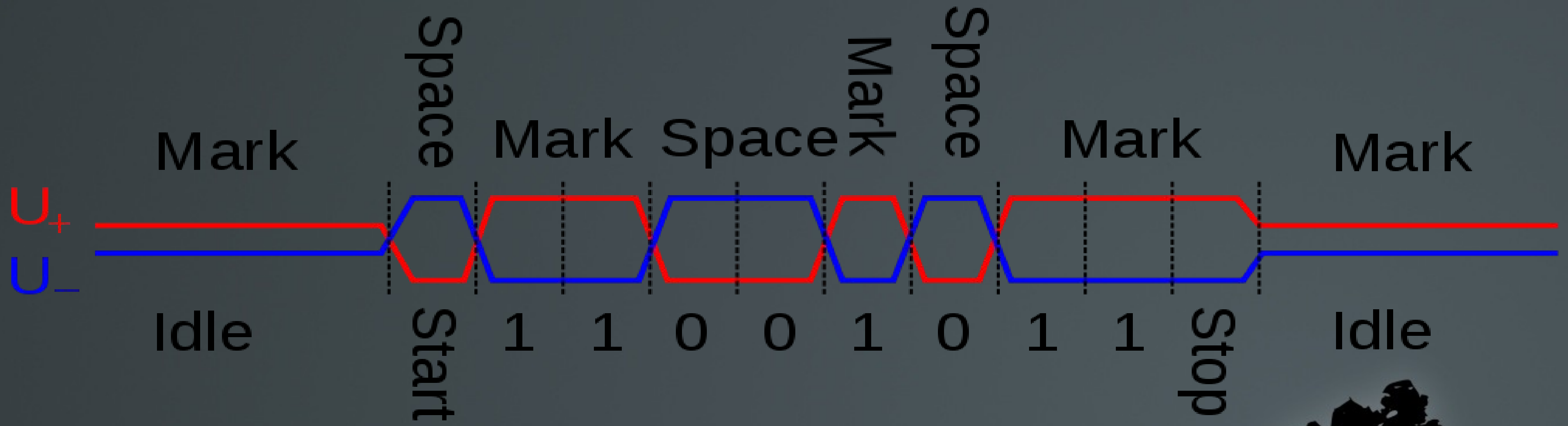


What is the bus?

RS-422

Does not use differential signaling

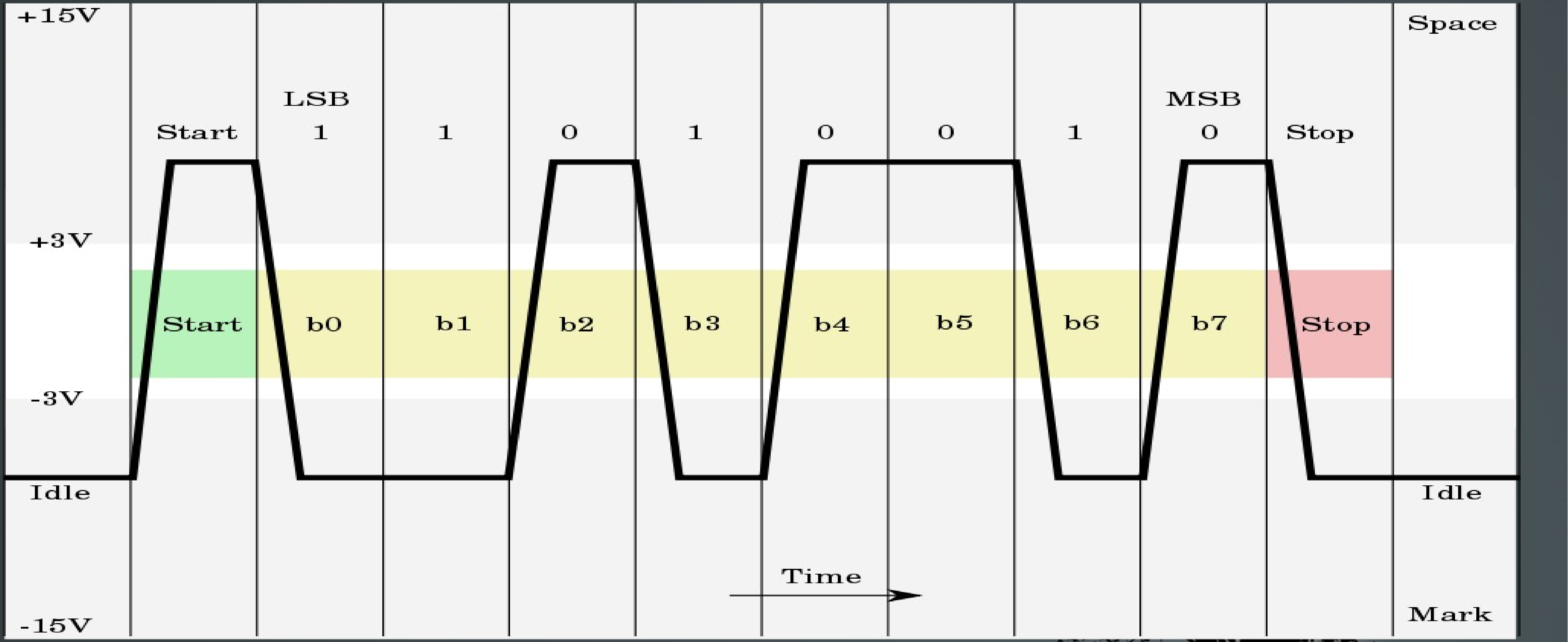
Wrong voltages (-6v to +6v)



What is the bus?

RS-232

There is no negative voltage on the data lines



What is the bus?

Protocol information and images from:

http://en.wikipedia.org/wiki/Rs485

http://en.wikipedia.org/wiki/Rs422

http://en.wikipedia.org/wiki/Rs232

What is the bus?

What now?

- Search the internet of course!!

http://www.google.com/patents/US6868493

System and method for panel linking in a security system

Not much use on the protocol, but some interesting block diagrams on the contents of data packets

What is the bus?

More reading of patents for clues

In patents US20090232307 and US20090083828, there is the same diagram with the wording:

ECP bus (proprietary protocol) RS232 like protocol

What Next?

RS-232 spec is rather flexible in the voltage needed

12v tolerant on the I/P pins

Lets try a PC Serial interface!

miniterm.py

Simple python terminal program included in the 2.6 package

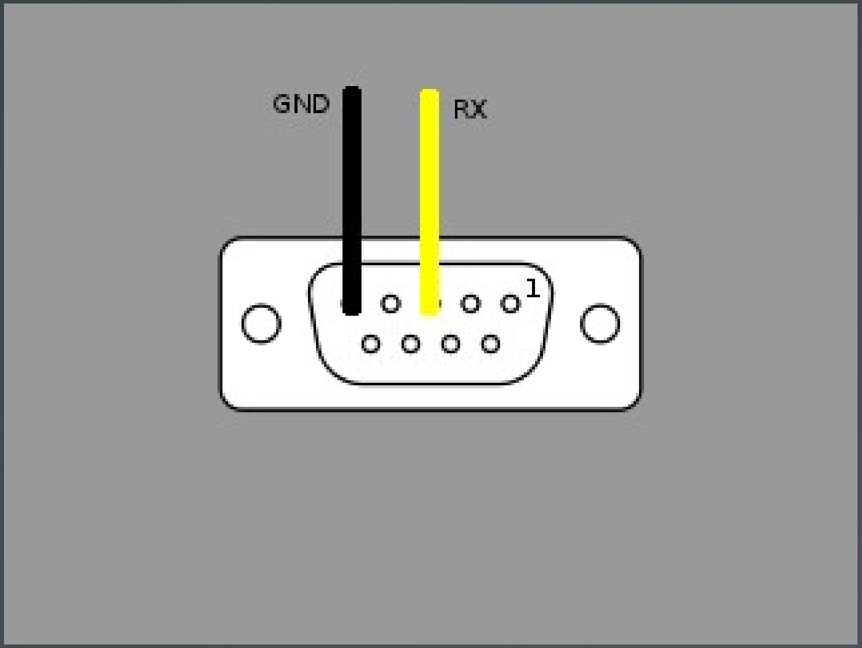
Using miniterm.py

```
Usage: miniterm.py [options] [port [baudrate]]

Miniterm - A simple terminal program for the serial port.

Options:

  -h, --help            show this help message and exit

  -p PORT, --port=PORT  port, a number or a device name

  -b BAUDRATE, --baud=BAUDRATE

                        set baud rate, default 9600

  --parity=PARITY       set parity, one of [N, E, O, S, M], default=N
```

Using miniterm.py

Physical wiring

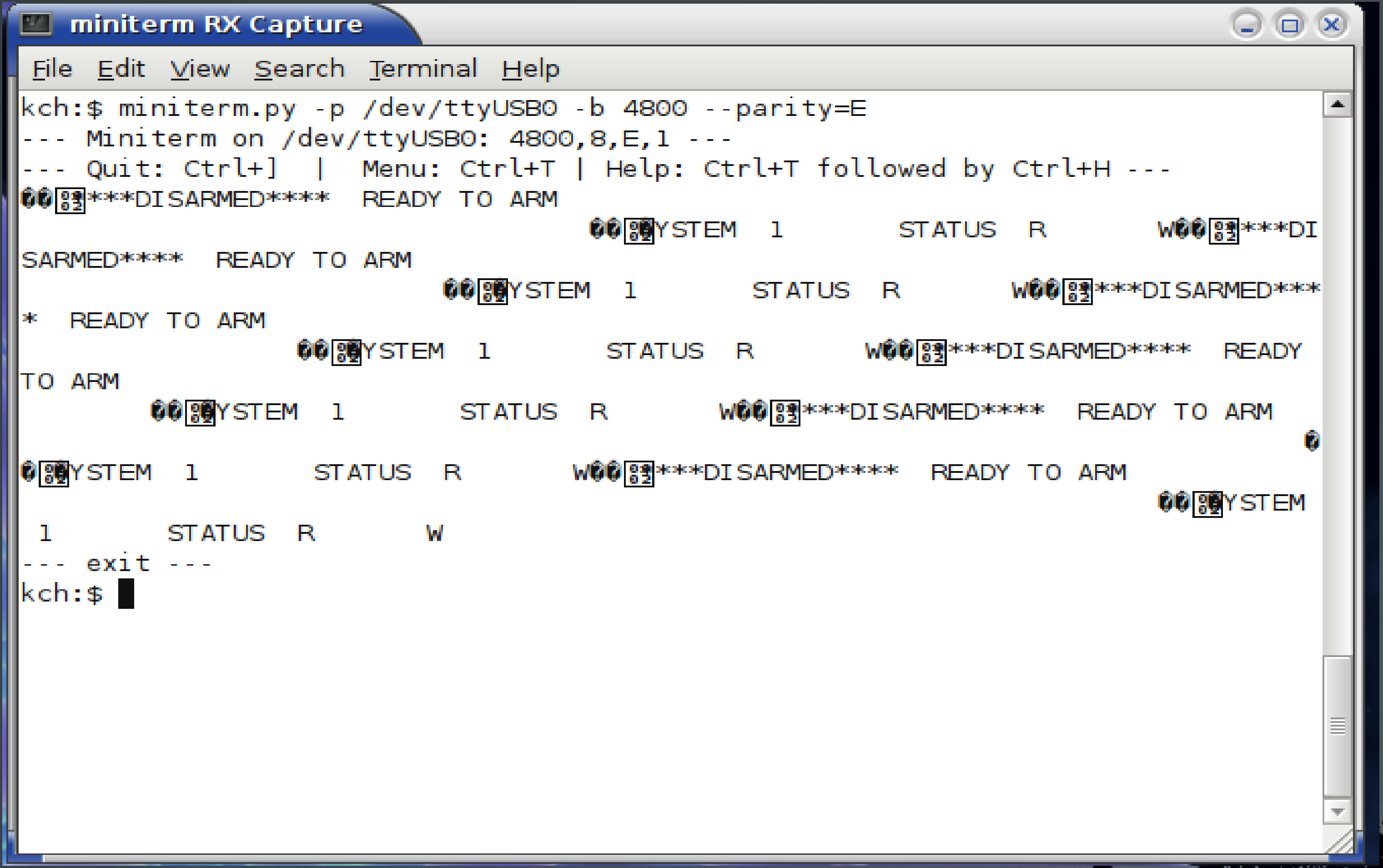
- Pin 3 – Receive
- Pin 5 - Ground



```
kch:~$ miniterm.py /dev/ttyUSB0 4800
```

Using miniterm.py

Live Demo!!!



```
kch:$ miniterm.py -p /dev/ttyUSB0 -b 4800 --parity=E
--- Miniterm on /dev/ttyUSB0: 4800,8,E,1 ---
--- Quit: Ctrl+]  |  Menu: Ctrl+T | Help: Ctrl+T followed by Ctrl+H ---
��□***DISARMED*****  READY TO ARM
                                   ��□YSTEM  1       STATUS  R       W��□***DI
SARMED*****  READY TO ARM
                          ��□YSTEM  1       STATUS  R       W��□***DISARMED***
*  READY TO ARM
                 ��□YSTEM  1       STATUS  R       W��□***DISARMED*****  READY
TO ARM
        ��□YSTEM  1       STATUS  R       W��□***DISARMED*****  READY TO ARM
                                                                               �
�□YSTEM  1       STATUS  R       W��□***DISARMED*****  READY TO ARM
                                                                      ��□YSTEM
 1       STATUS  R       W
--- exit ---
kch:$ 
```

Investigating Further

So what is the next step?

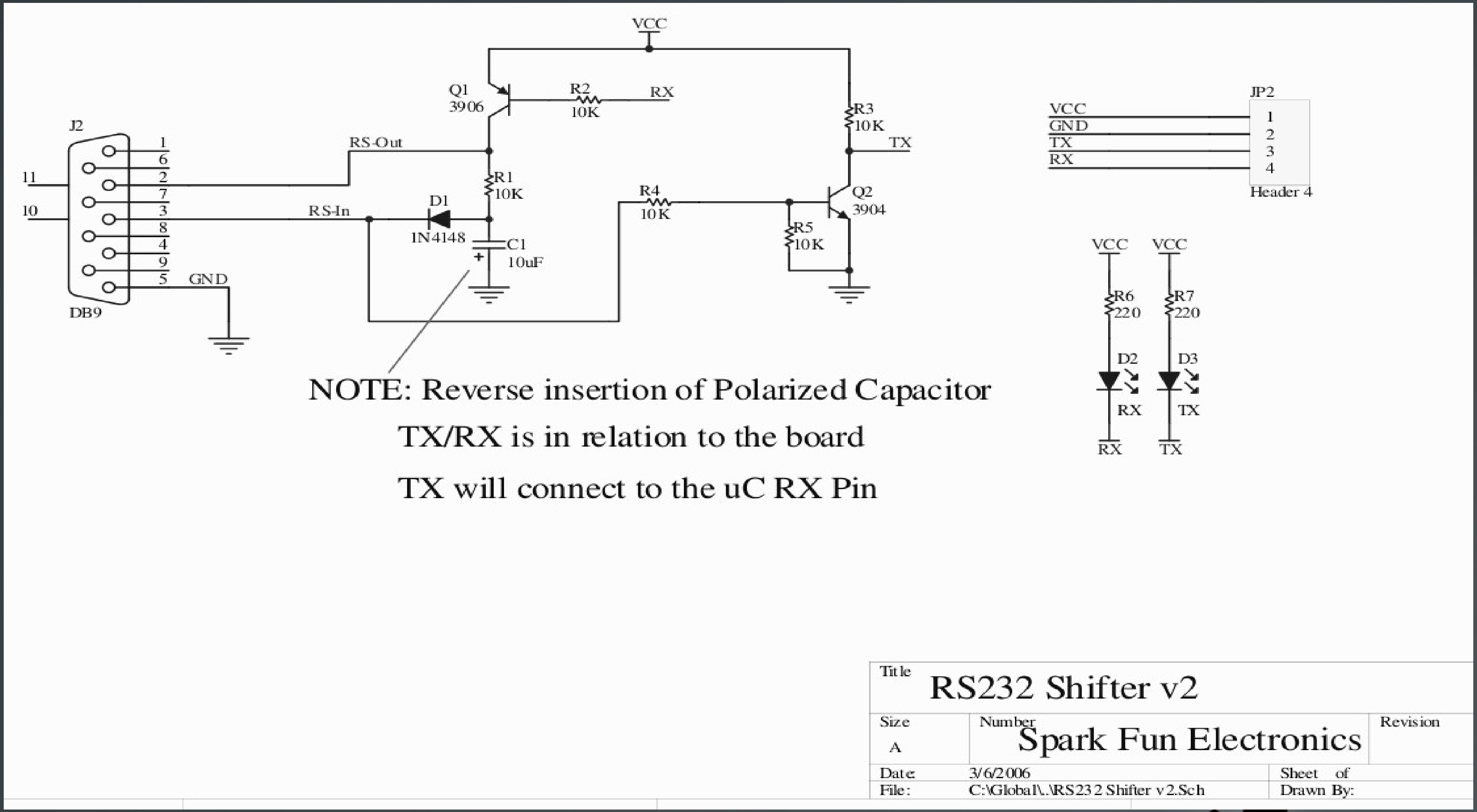
Logic Analyser

- only designed for 5v max level!

(don't let the blue smoke moster out!!)

Solution – RS232 level shifter

Investigating Further



NOTE: Reverse insertion of Polarized Capacitor

TX/RX is in relation to the board

TX will connect to the uC RX Pin

Title RS232 Shifter v2

Size A

Number Spark Fun Electronics

Revision

Date 3/6/2006

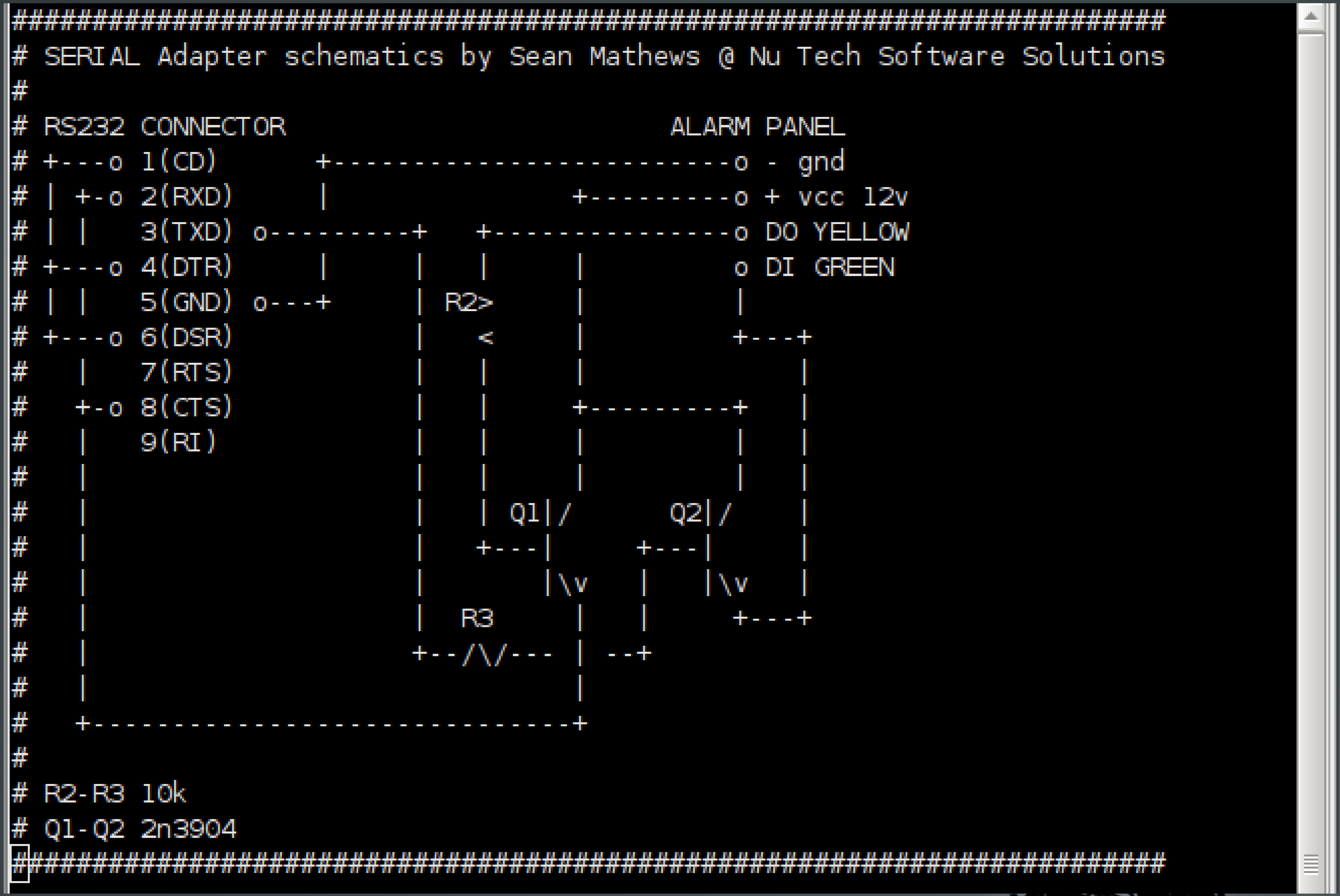
Sheet of

File: C:\Global\..\RS232 Shifter v2.Sch

Drawn By:

http://www.sparkfun.com

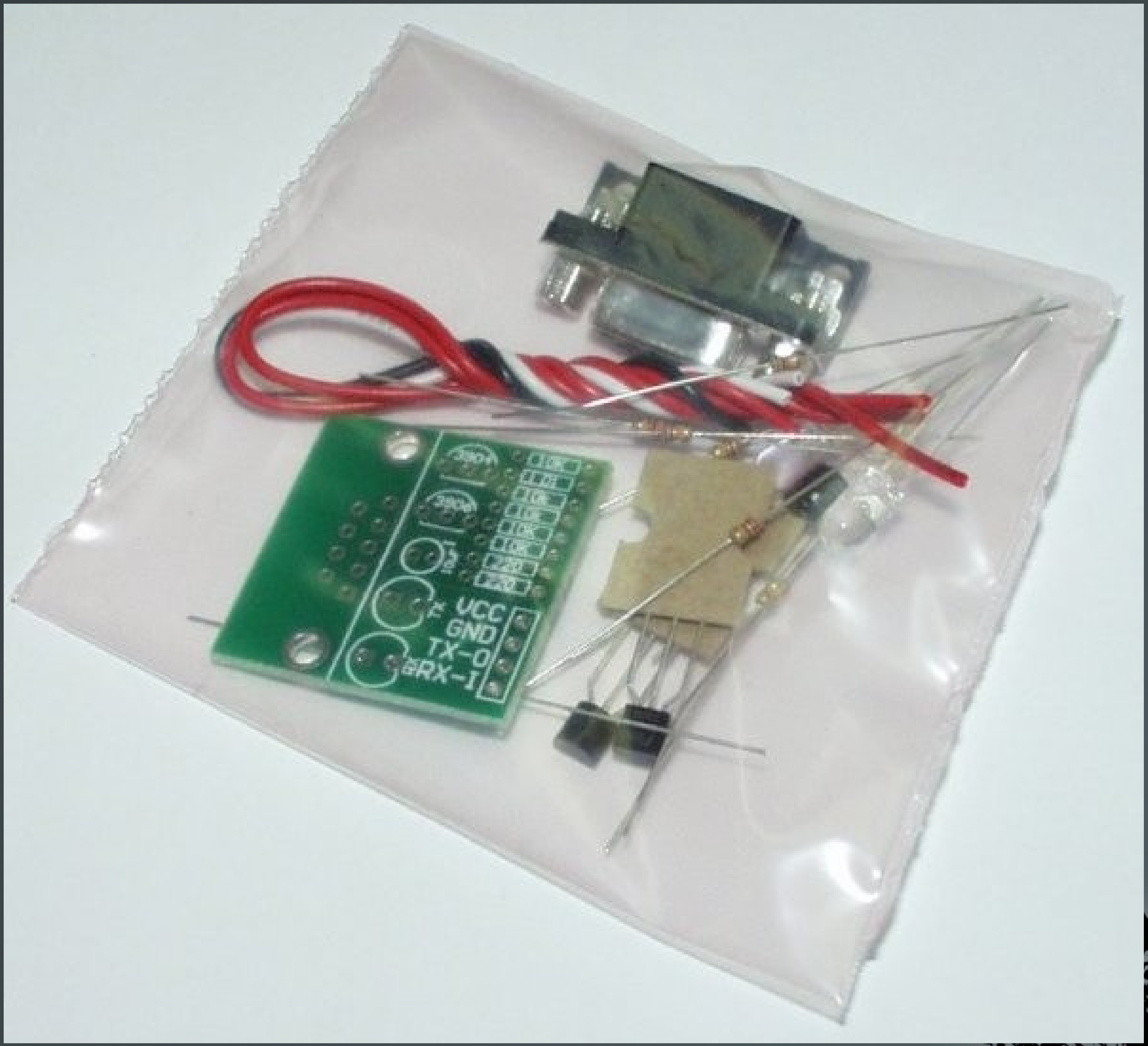
Investigating Further



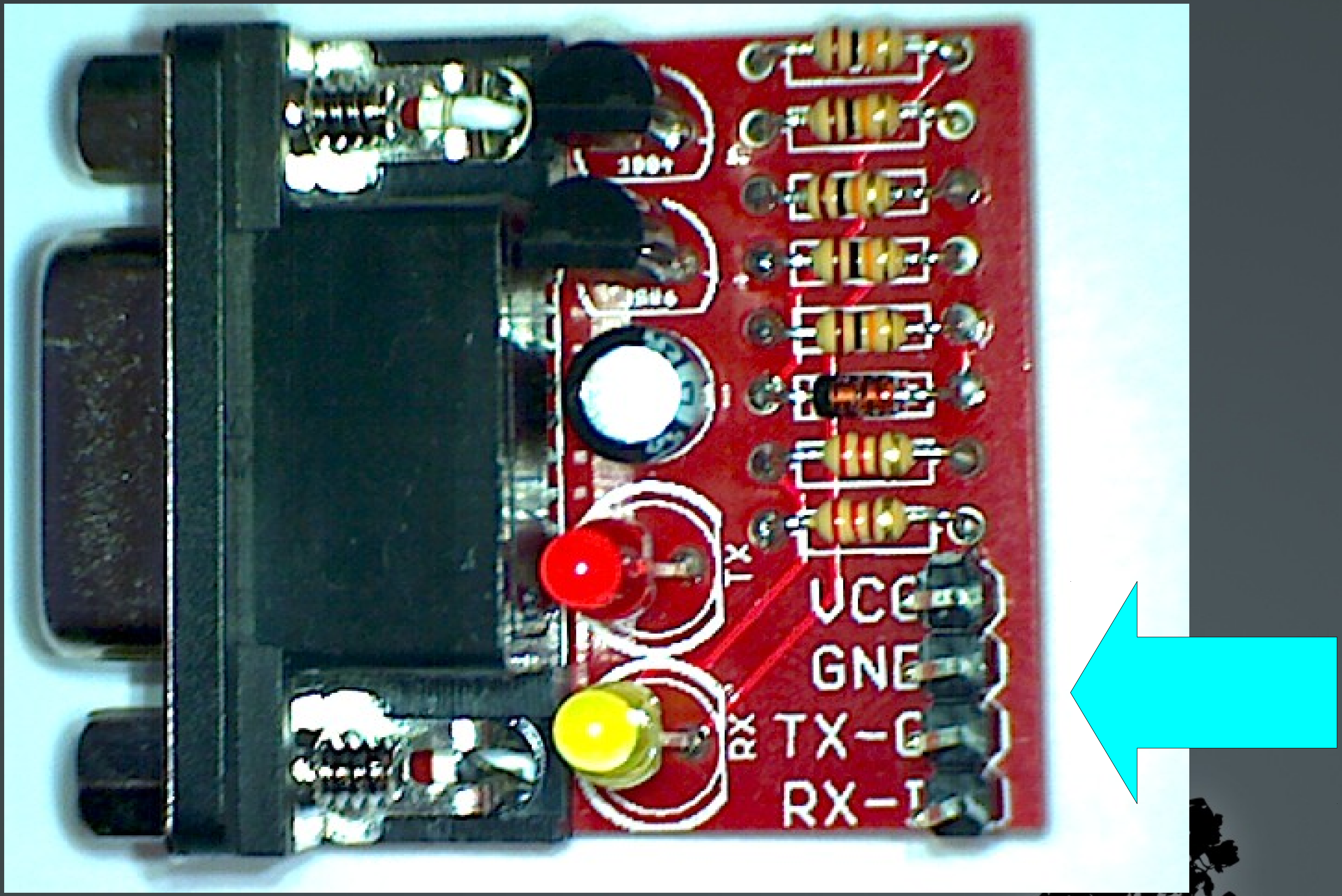
```
########################################################################
# SERIAL Adapter schematics by Sean Mathews @ Nu Tech Software Solutions
#
# RS232 CONNECTOR                        ALARM PANEL
# +---o 1(CD)      +-------------------------o - gnd
# | +-o 2(RXD)     |               +---------o + vcc 12v
# | |   3(TXD) o---------+   +---------------o DO YELLOW
# +---o 4(DTR)     |     |   |     |         o DI GREEN
# | |   5(GND) o---+     | R2>     |         |
# +---o 6(DSR)           |   <     |         +---+
#   |   7(RTS)           |   |     |             |
#   +-o 8(CTS)           |   |     +---------+   |
#   |   9(RI)            |   |     |         |   |
#   |                    |   |     |         |   |
#   |                    |   | Q1|/      Q2|/    |
#   |                    |   +---|     +---|     |
#   |                    |       |\v   |   |\v   |
#   |                    |  R3     |   |     +---+
#   |                    +--/\/--- | --+
#   |                              |
#   +------------------------------+
#
# R2-R3 10k
# Q1-Q2 2n3904
########################################################################
```

http://www.diysecurityforum.com

Investigating Further



Investigating Further



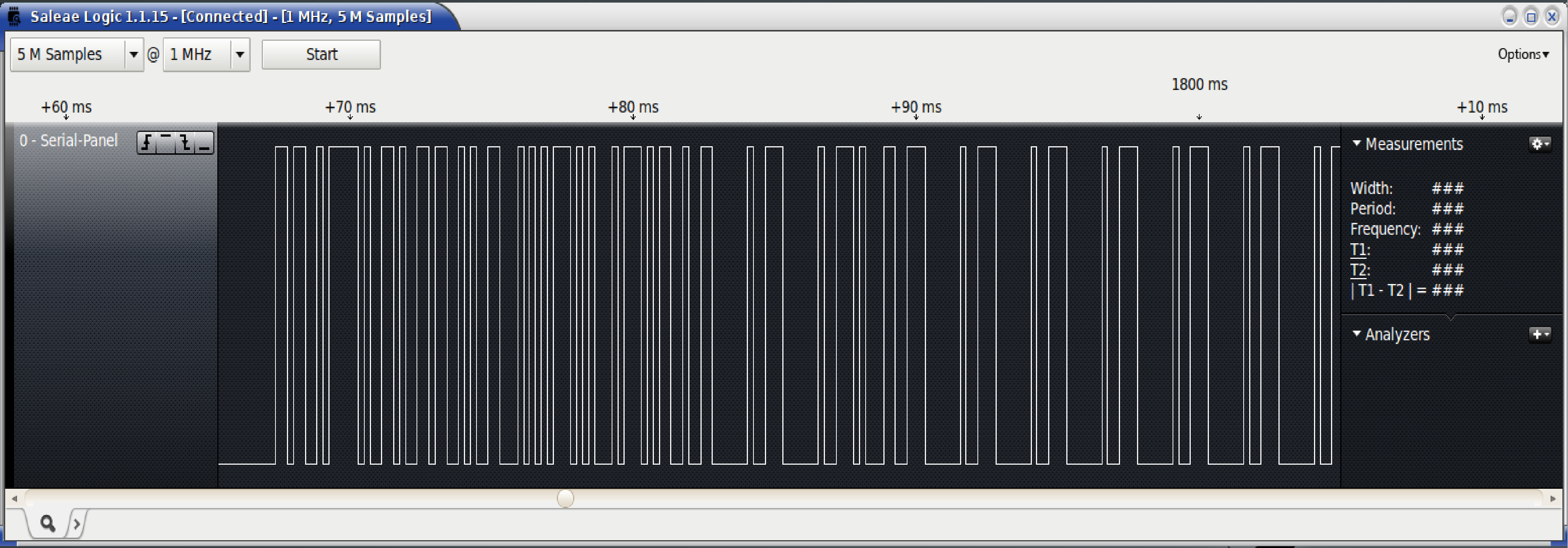
Investigating Further

Logic Analyzer

http://www.saleae.com/Logic

Investigating Further

Live demo time again



Width: ###
Period: ###
Frequency: ###
T1: ###
T2: ###
| T1 - T2 | = ###

Investigating Further

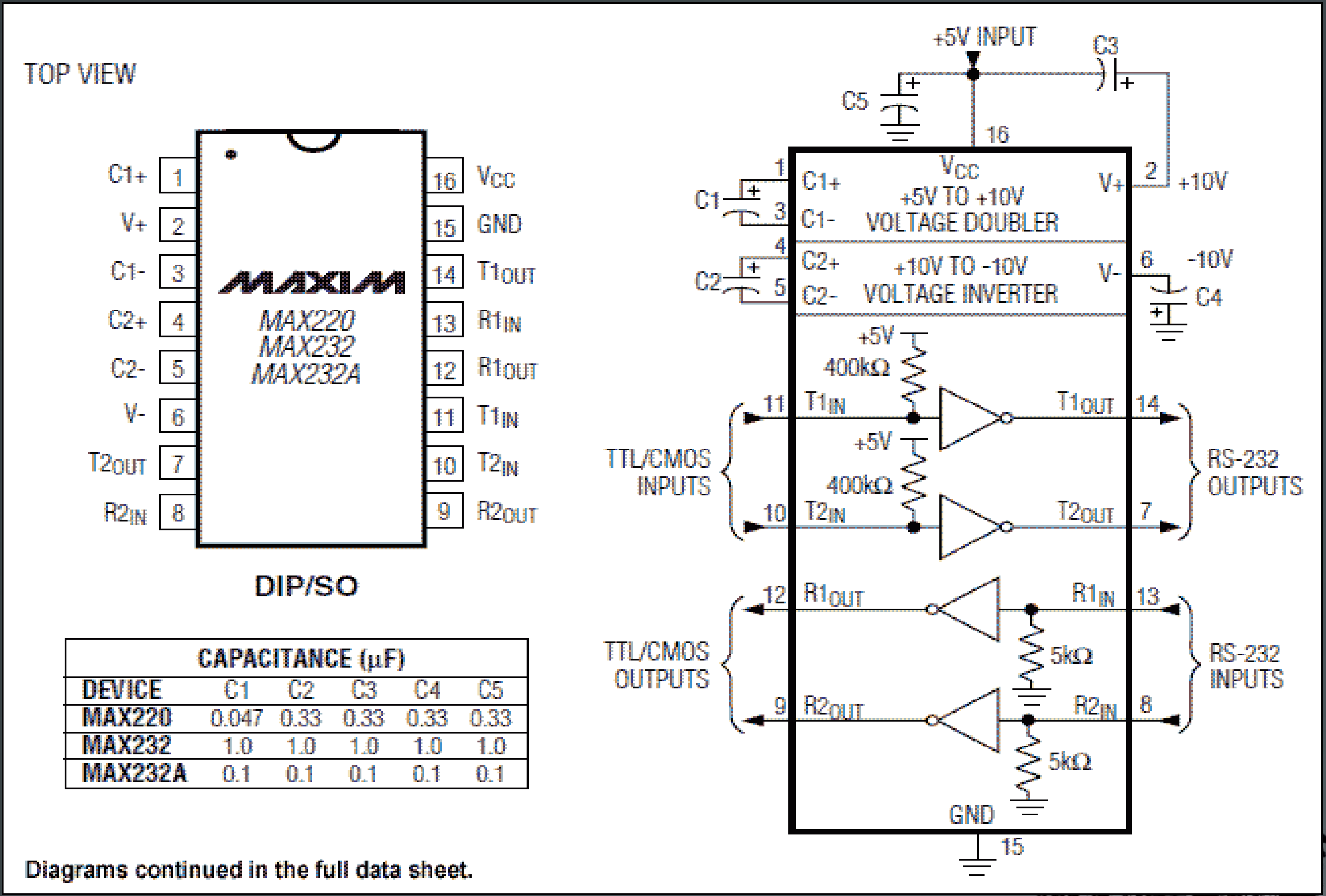
Serial port shifter designed for RX and TX interface to a microcontroller

only 'reads' one line at a time

to monitor both lines needs two level shifters

Investigating Further

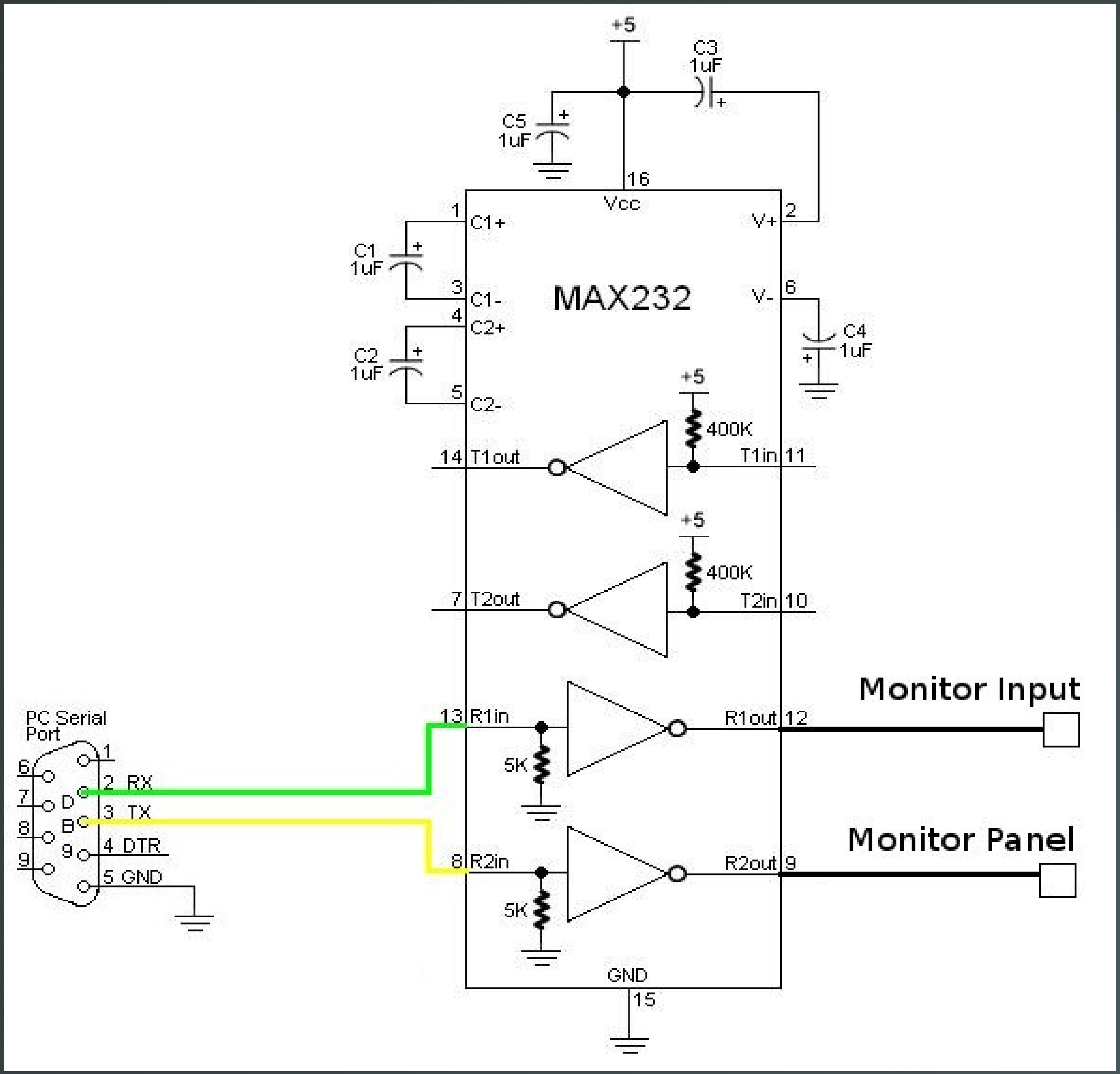
Maxim MAX232 chip to the rescue



CAPACITANCE (μF)					
DEVICE	C1	C2	C3	C4	C5
MAX220	0.047	0.33	0.33	0.33	0.33
MAX232	1.0	1.0	1.0	1.0	1.0
MAX232A	0.1	0.1	0.1	0.1	0.1

Diagrams continued in the full data sheet.

MAX232 Circuit

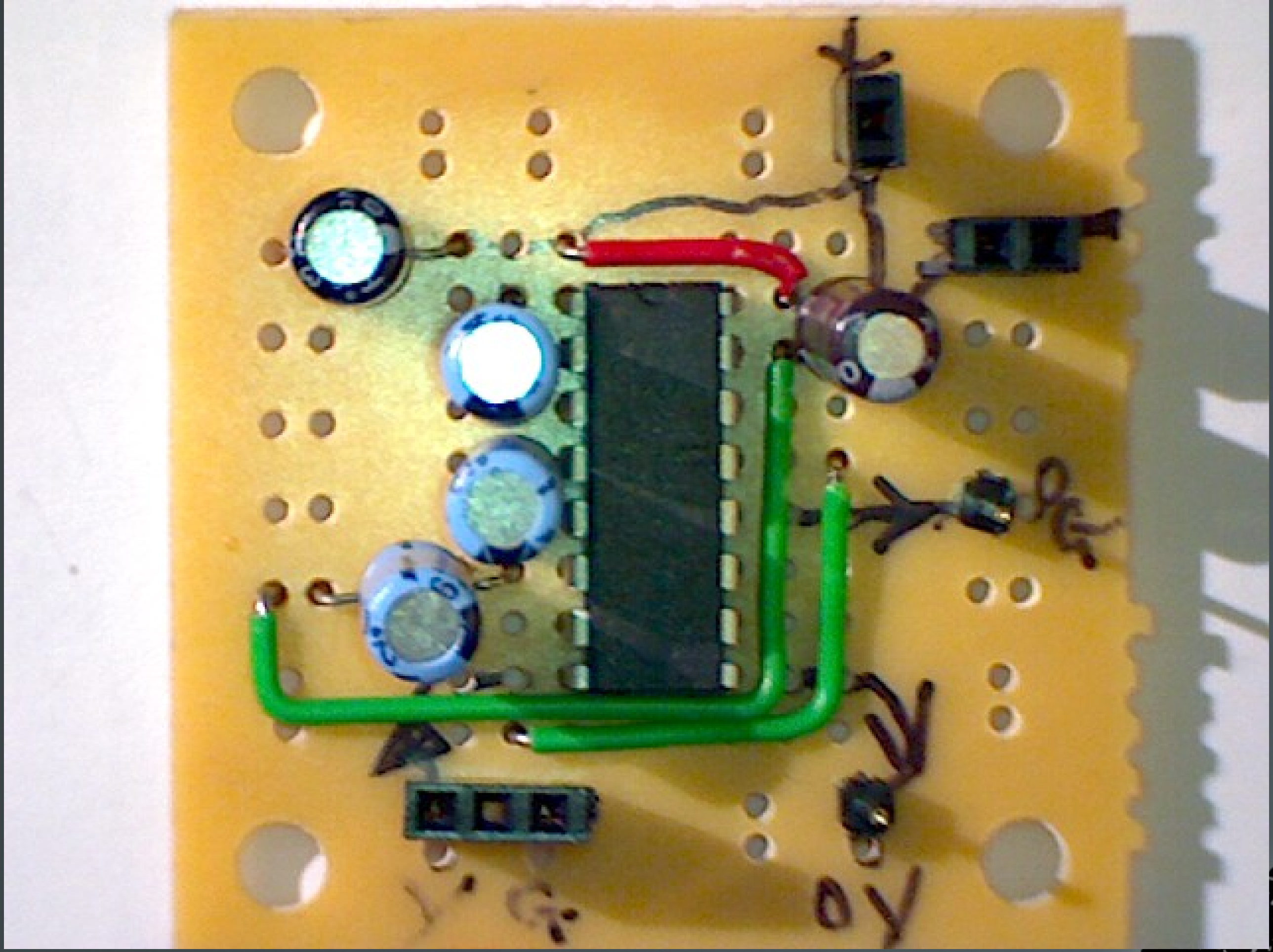


MAX232 very common

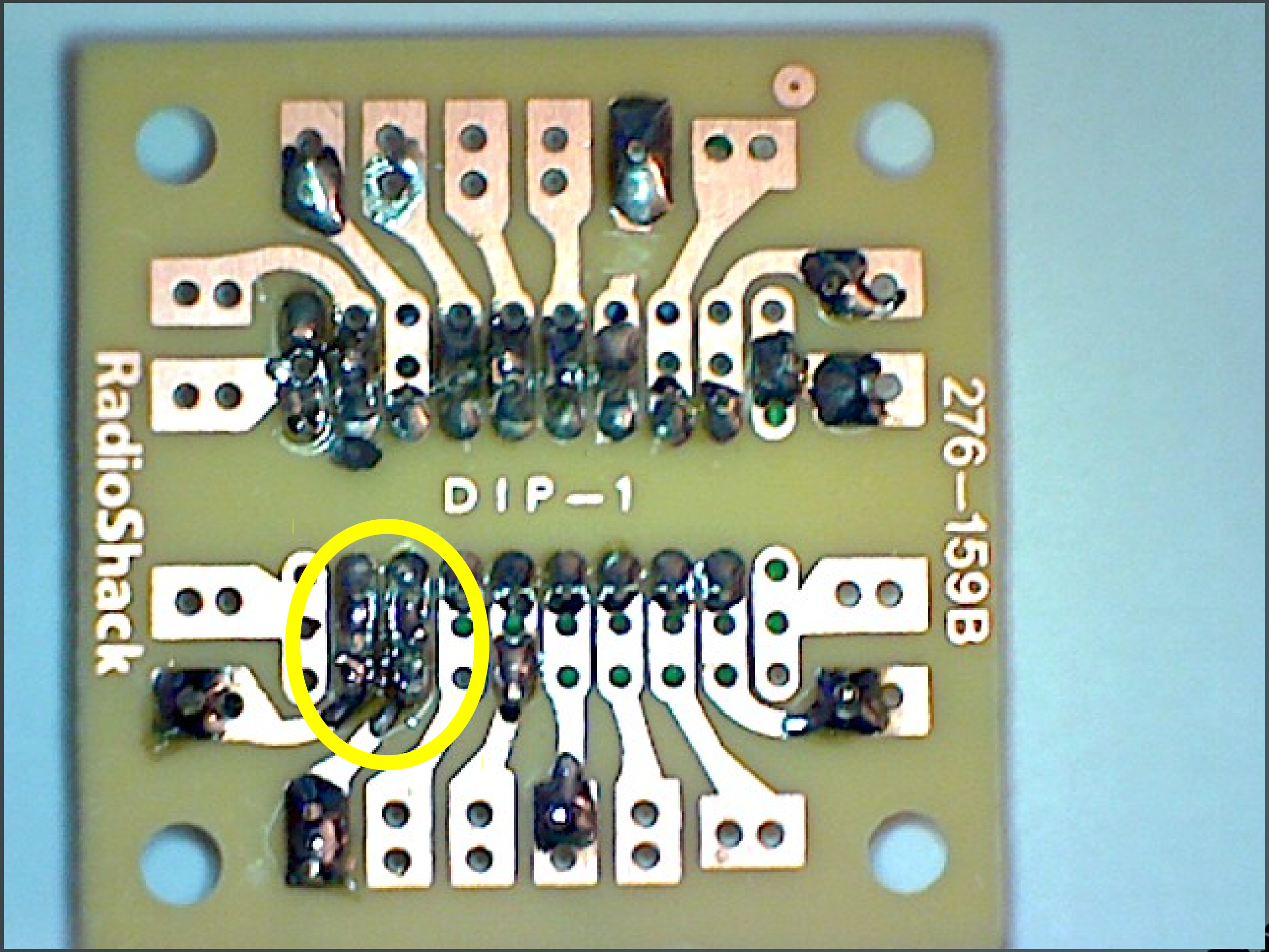
capacitors easy to get

simple to solder up

MAX232 Circuit



What Was That?



Analyzing the Bus Traffic

Demonstration.

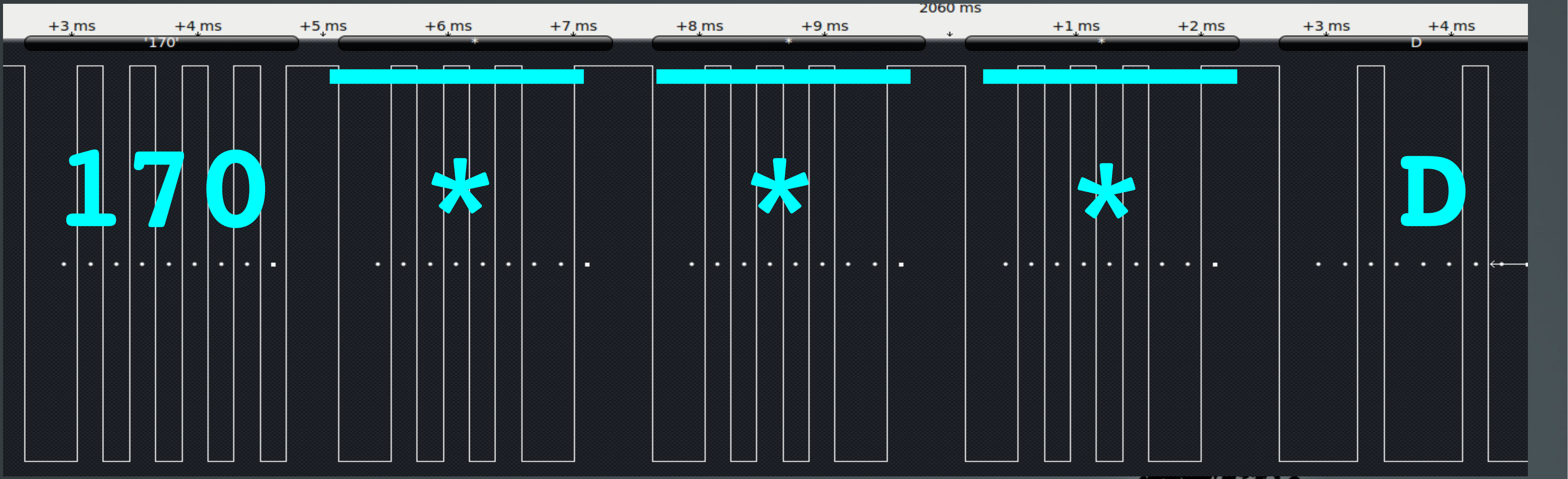
Capture of both data lines using the max232

Analyzing the Bus Traffic

Decoding still is not 100%. Message should be

`****DISSARMED****`

Missing '*' at the start



More Research on Bus Traffic

More research needed

- back to the internet

article from ”Circuit Cellar” magazine issue 201

Reverse-Engineered ECP Bus

http://www.circuitcellar.com

More Research on Bus Traffic

Author Miguel Sanchez details:

- Problems with protocol violations
- Timing issues trying to send data from perl
- Using a RCM3710 Microprocessor Core

http://www.rabbitsemiconductor.com

More Research on Bus Traffic

While doing more research:

http://www.diysecurityforum.com/index.php?topic=10480

Someone else has solved the problem!

More Research on Bus Traffic

NuTech Software Solutions

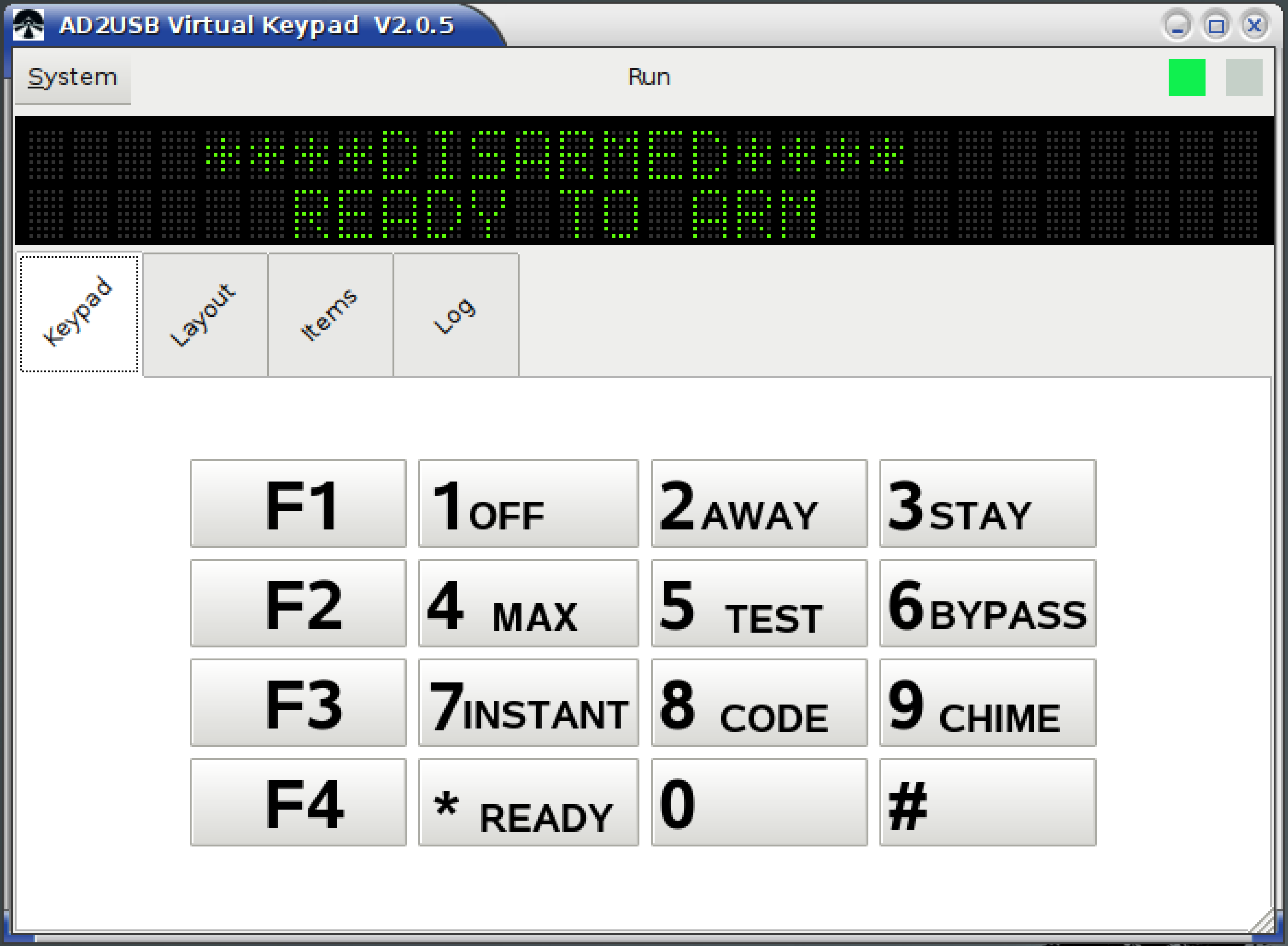
AD2USB Adapter

- PIC microcontroller with ECP and USB interfaces
- Virtual Keypad software
- Standard FTDI usb chip used (should be Linux friendly)
- No more converter, just connect and go!

http://www.nutech.com/online-store/4.html

The AD2USB Adapter

The Virtual Keypad



```
****DISARMED****
  READY TO ARM
```

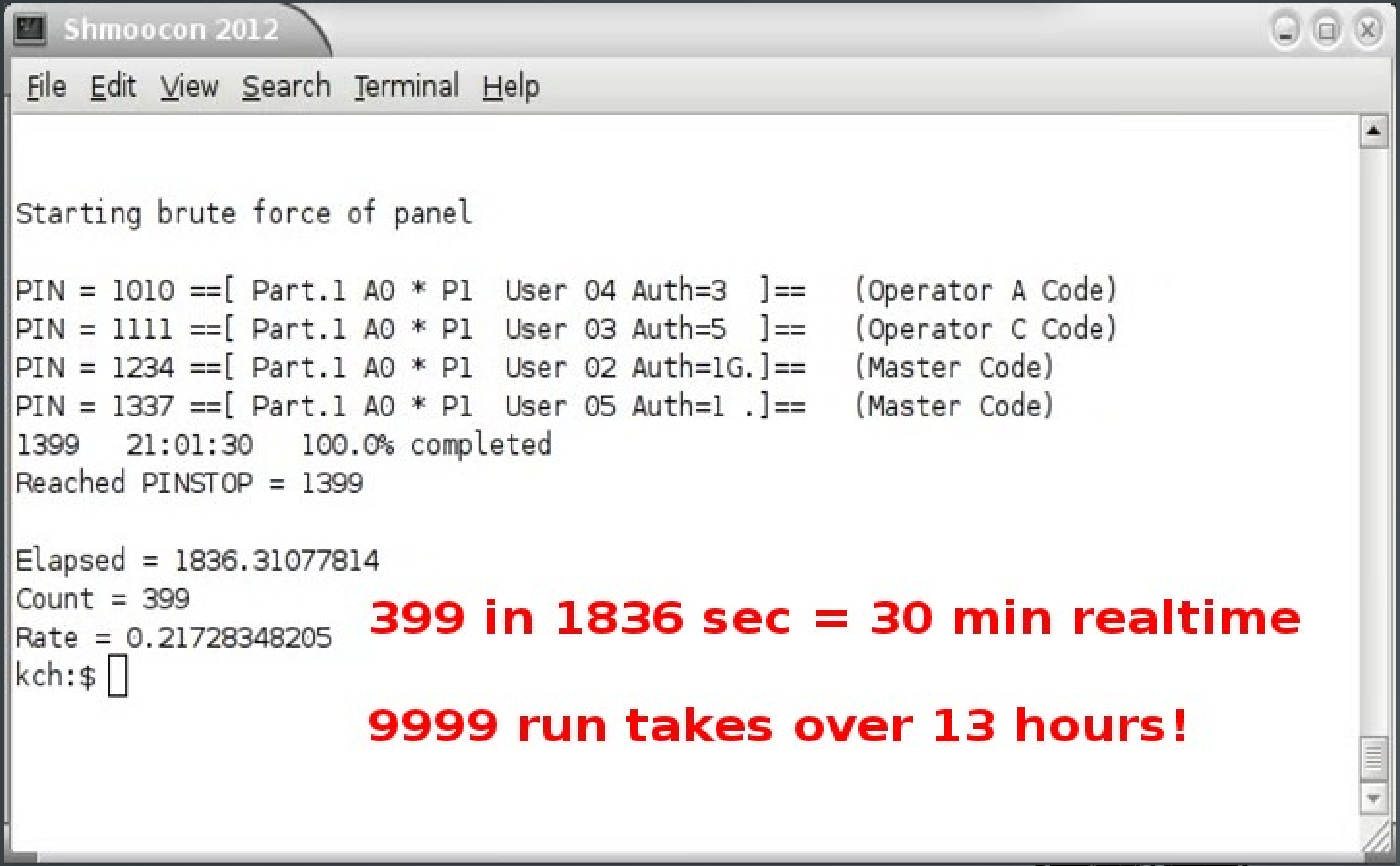
What Can It Do?

- Full interface to the ECP Bus
- Interfaces correctly with the TX and RX data
- Uses standard ascii text to send data
- Converts keystrokes to data transmission packet
- A simple python program can do the rest!

What Can It Do?

Video Clip.

What Can It Do?



```
Starting brute force of panel

PIN = 1010 ==[ Part.1 A0 * P1  User 04 Auth=3  ]==   (Operator A Code)
PIN = 1111 ==[ Part.1 A0 * P1  User 03 Auth=5  ]==   (Operator C Code)
PIN = 1234 ==[ Part.1 A0 * P1  User 02 Auth=1G.]==   (Master Code)
PIN = 1337 ==[ Part.1 A0 * P1  User 05 Auth=1 .]==   (Master Code)
1399   21:01:30   100.0% completed
Reached PINSTOP = 1399

Elapsed = 1836.31077814
Count = 399
Rate = 0.21728348205
kch:$
```

399 in 1836 sec = 30 min realtime

9999 run takes over 13 hours!

Some ”Gotcha's”!

- different panels have different features
- could trigger ”duress” codes!
- Police/Fire/EMS might show up if you try this on a live panel!
- could be logged by the panel (if configured_ – but I was not blocked on the panel I tried it on

The technique I used on the panel I have also worked when the panel was armed!!!

There Must Be A Better Way?

How about sniffing the wire?

Yes. Not with the stock firmware though.

Many thanks to Sean Mathews the designer of the AD2USB for a debug enabled version of the firmware.

I wrote a keystroke sniffing module for the virtual keypad

Demonstration Time

Other Devices

- How did any other devices communicate?
- Was this also in plain text?
- Turns out – No. Not quite.
- The data sent to the panel uses bit-fields packed into bytes
- This is the same type of data I interpret to read the keystrokes

Data Communications

Keypad sending 1234

```
(fe)(c0)(02)(01)(3d)
(fe)(00)(02)(02)(fc)
(fe)(40)(02)(03)(bb)
(fe)(80)(02)(04)(7a)
```

Data Communications

`(fe)(c0)`	Header
`(02)`	Number of bytes
`(01)`	Data byte(s)
`(3d)`	Checksum

Unknown Data!

Data appears in my logs when I am not doing anything!

RF receiver is picking up *any* device in range

Most sensors are 'supervised' and send out regular ”check-in” messages to the panel

Unknown Data!

```
(fb)(02)(51)(82)(66)(7f)
(80)
(c6)

!RFX:0157311,80
```

Unknown Data

RFX:0000264
RFX:0008248
RFX:0027768
RFX:0039424
RFX:0039616
RFX:0040192
RFX:0040256
RFX:0040320
RFX:0040384
RFX:0049290
RFX:0067584
RFX:0067600
RFX:0067616
RFX:0067632
RFX:0133136
RFX:0133379
RFX:0157311
RFX:0251840
RFX:0267813
RFX:0272005
RFX:0288708
RFX:0393296
RFX:0572636

Where is it coming from?

Data is sent by the RF receiver

Only 0027768 is my sensor

Must be other devices in the area

I guess my neighbors use compatible devices!!

Some of it is me!

```
1/25/2012 9:02:32 PM !DBG:(fb)(02)(51)(80)(6c)(78)
1/25/2012 9:02:32 PM !RFX:0027768,a0
1/25/2012 9:02:32 PM !DBG:(a0)(a9)(fb)(02)(54)(82)(09)(03)
1/25/2012 9:02:32 PM !RFX:0133379,00
1/25/2012 9:02:33 PM !DBG:(00)(1c)(fb)(02)(51)(86)(00)(50)
1/25/2012 9:02:33 PM !RFX:0393296,20
1/25/2012 9:02:36 PM !DBG:(20)(b7)

1/25/2012 9:02:36 PM !DBG:(fb)(02)(54)(80)(6c)(78)
1/25/2012 9:02:36 PM !RFX:0027768,80
1/25/2012 9:02:37 PM !DBG:(80)(c6)(fb)(02)(51)(82)(08)(10)
1/25/2012 9:02:37 PM !RFX:0133136,1c
1/25/2012 9:02:39 PM !DBG:(1c)(f7)
```

Activity Around The Con

RFX:0000270

RFX:0002716

RFX:0012112

RFX:0012608

RFX:0020454

RFX:0022118

RFX:0023788

RFX:0025194

RFX:0027710

RFX:0027768

RFX:0029252

RFX:0063944

RFX:0112424

RFX:0128563

RFX:0134582

RFX:0349026

RFX:0363444

RFX:0400730

RFX:0478161

RFX:0483563

RFX:0527492

RFX:0638358

RFX:0819607

RFX:0922035

RFX:1022140

RFX:1026268

RFX:1040738

RFX:1040760

Tracking a Sensor

```
1/28/2012 3:37:47 PM !RFX:0819607,80        Loop 1 triggered

1/28/2012 3:37:49 PM !RFX:0819607,00        Loop 1 reset

1/28/2012 3:40:23 PM !RFX:0819607,80        Loop 1 triggered

1/28/2012 3:40:25 PM !RFX:0819607,00        Loop 1 reset

1/28/2012 3:56:45 PM !RFX:0819607,80        Loop 1 triggered

1/28/2012 3:56:47 PM !RFX:0819607,00        Loop 1 reset

     [computer off-line, no logging]

1/28/2012 7:38:15 PM !RFX:0819607,04        Loop 1 supervisor check

1/28/2012 7:51:18 PM !RFX:0819607,80        Loop 1 triggered

1/28/2012 7:51:19 PM !RFX:0819607,00        Loop 1 reset

1/28/2012 9:00:54 PM !RFX:0819607,04        Loop 1 supervisor check
```

What Good Is All This?

Offense

- Intelligence gathering
- Covert entry

Defense & Auditing

- Checking for bad PIN numbers
- Logging alarm panel to internal servers
- Activity tracking without alarms

Any Suggestions?

Work in Progress

Currently working on

- Decoding header in more detail
- Analyzing more of the RF messages
- Additional RF device testing
- What can be learned without physical access?

Assumptions...

- Transmitter is sending out panel status
- Wireless keypads transmit keystrokes

Thank You To

Sean Matthews	http://www.nutech.com
	http://diysecurityforums.com
Adafruit Industries	http://www.adafruit.com
Sparkfun Electronics	http://www.sparkfun.com
Saleae Electronics	http://www.saleae.com
Miguel Sanchez	http://www.circuitcellar.com
Matt Morrison	http://www.assurancedata.com

Any Questions?