Trustwave®

SpiderLabs®

Blinkie Lights!

Network Monitoring with Arduino

Steve Ocepek

Disclaimer

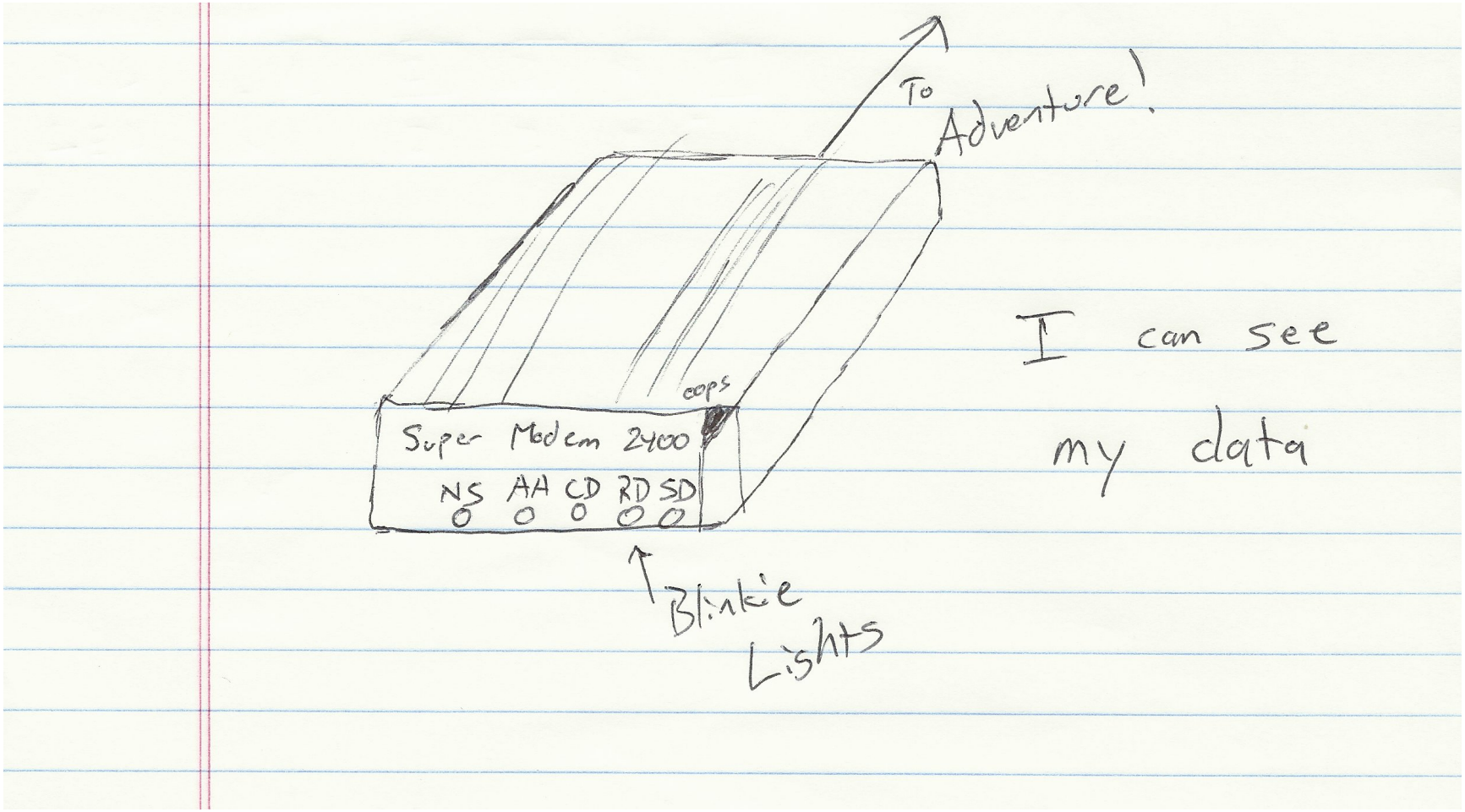
Due to legal concerns, slides containing one or more of the following have been removed:

- **Depictions of violence**
- **Dancing animals**
- **Transvestites**
- **Questionable remains of biological origin**
- **Drunk people**
- **Copyrighted images**

LEGAL APPROVED*

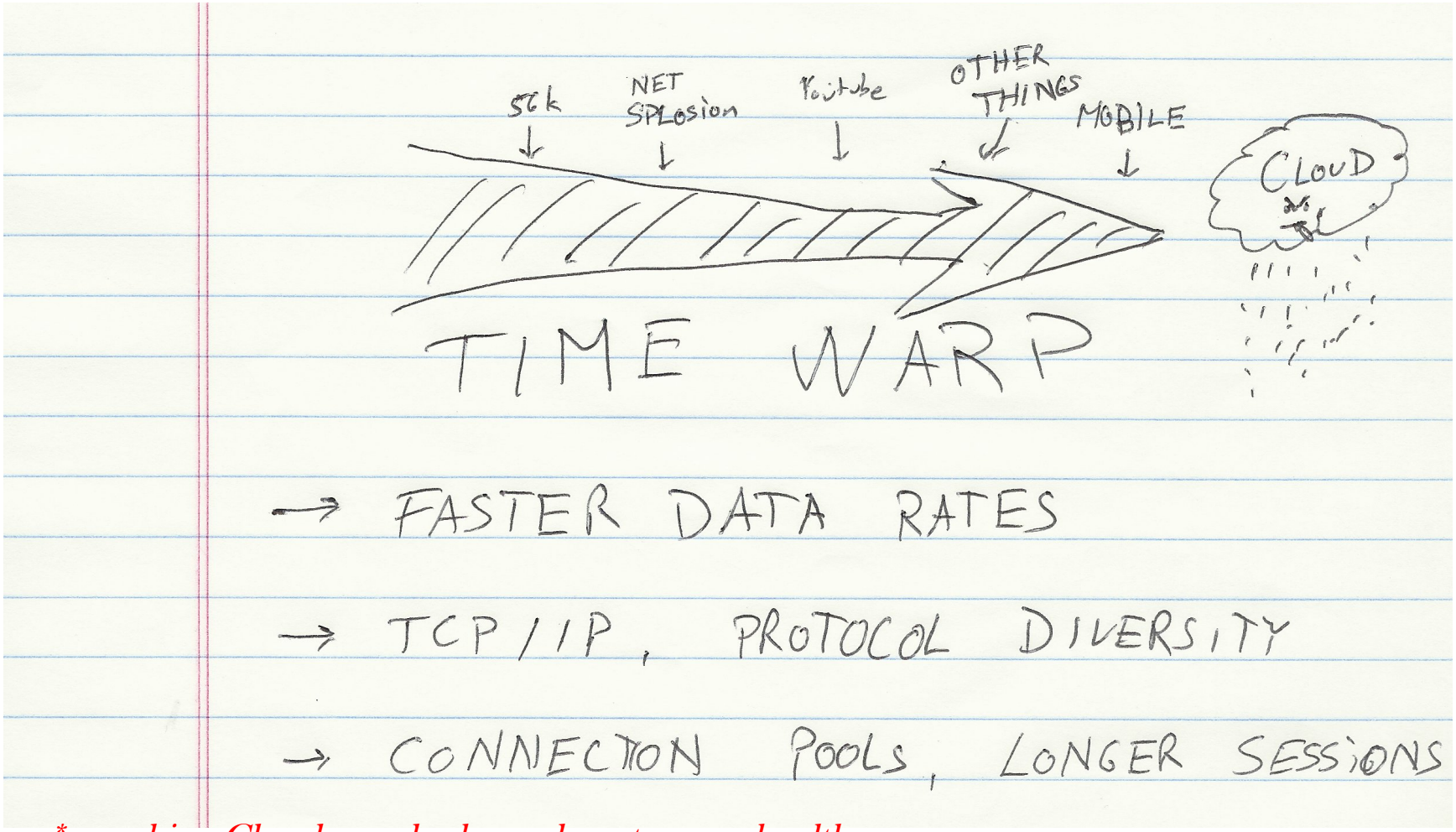
** subject to terms and conditions*

Early Market Trends



** not affiliated with Diamond Multimedia or its subsidiaries*

Industry Progression



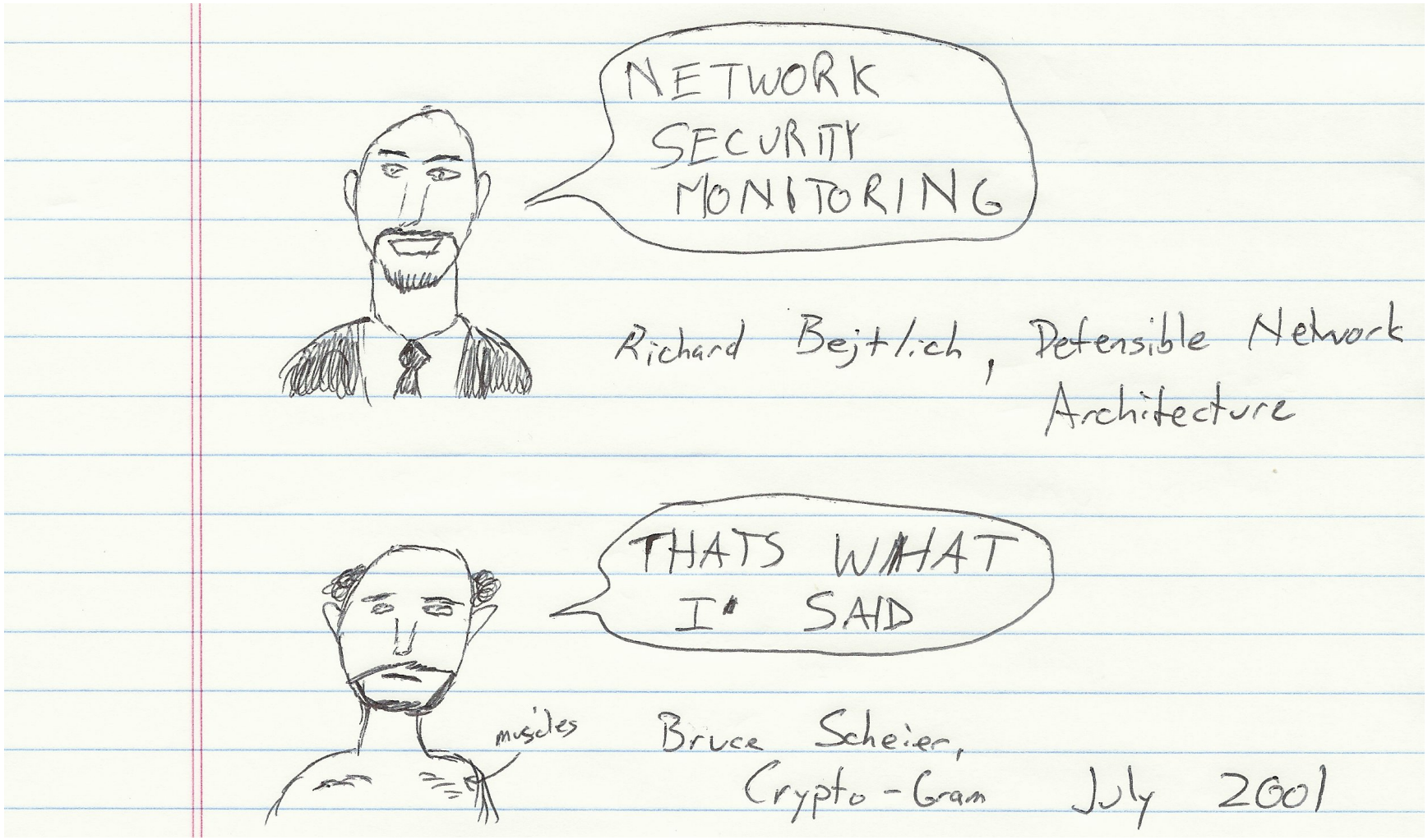
** smoking Cloud may be hazardous to your health.*

Realization

- **I don’t know what the hell my box is doing anymore**
- **I don’t know what normal looks like**
- **2 minute pcap file > 2 minute MP3**
- **My netstat hurts**

The Activity Light is Solid

Third Party Analysis



** any resemblance to real persons, living or dead is purely coincidental.*

Wait, monitoring?

#1: You mean like IDS, IPS, NAC, sniffers, scrapers, log monitors, and the theory of Atlantis?

#2: No, I mean like wtf is my box doing?

#1: Yeah try wireshark noob

#2: Just because I am a genetically enhanced 3-month-old is no reason to make this personal. Besides wireshark is for analysis, not monitoring.

#3: Can you guys keep it down? This 2-person escape pod is bad enough without your 21st century era IT debate reenactments.

Something… else

- **Like the old days, the activity lights on modems and stuff**
- **Something that makes a good excuse for Arduino and sounds good on a Defcon schedule**
- **And has freaking blinkie lights**
- **Something that provides *visibility***

Visibility vs. Visualization

- **Going for something that's more "peripheral", tap into human cognition**
- **Making up my own distinctions here**
- **Visualization**
  - Tends to be complex, static image that we stare at
- **Visibility - more tactical, realtime**
  - i.e. the military term: our ability to "see" what's there (depending on weather conditions, etc) and make decisions
- **Visualization taps into our ability to reason**
- **Visibility taps into our cognition**

Real-time Cognition

- **I only sort of know what I'm talking about here**
- **Examples:**
  - Driving
  - Video Games
  - Sports
- **Direct connection between the senses**
- **Acute perception of slight variances in stimuli**
  - Dude I made that up and it sounds awesome

Scholarly Reference

"Real-time cognition is best described not as a sequence of logical operations performed on discrete symbols but as a continuously changing pattern of neuronal activity."

Continuous Dynamics in Real-Time Cognition

Michael J. Spivey and Rick Dale

Cornell University and University of Memphis

Trustwave®

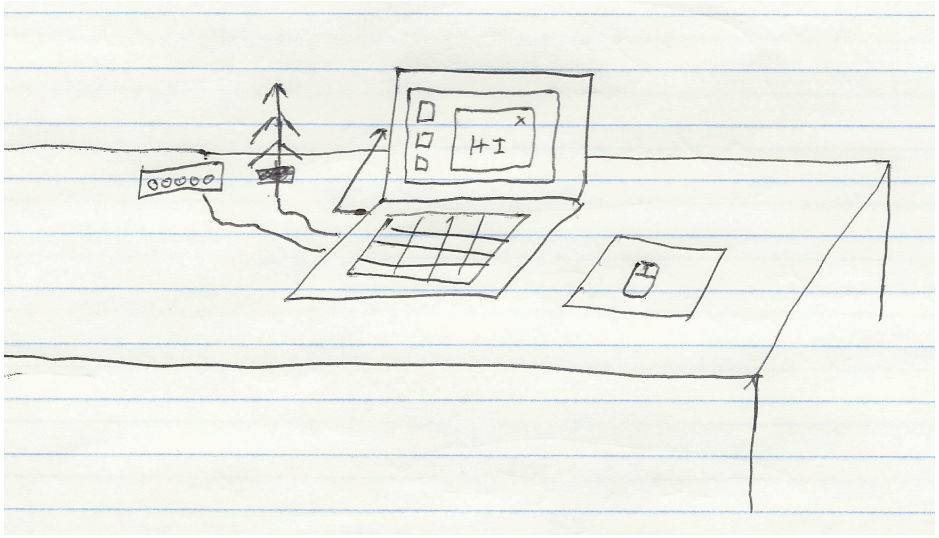
SpiderLabs®

Let's play with electronics

Peripherals

- **Screen real estate market is tapped out**
  - The maximize button
  - Widget displays such as Dashboard are on-demand only

- **USB trinkets/toys are on the rise**
  - Nerf shooter
  - Ninja detectors
  - LED Christmas trees



Crazy idea

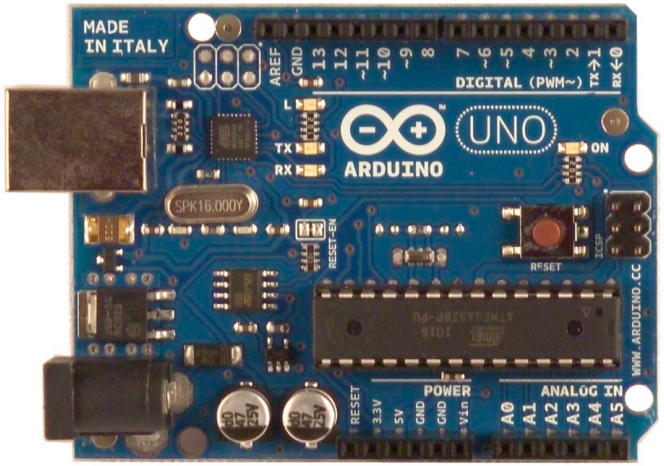
- **Render network data onto LED matrix in realtime**
- **Use color, motion, other effects to show what happening on the wire**
- **Try to get back a "feel" for what our systems are doing**
- **Tap into our natural pattern-matching ability to detect variances**

cerealbox

- **Name came from our tendency to read/interpret anything in front of us**
- **Kind of a "background" technology, something that we see peripherally**
- **Pattern detection lets us see variances without digging too deep**
- **Just enough info to let us know when it's time to dig deeper**

Arduino Uno

- **Cool little boards, based on Atmel ATMega328**
  - 8-bit RISC CPU @ 16Mhz
  - 32k flash (storage for program code / opt. static storage)
  - 2k SRAM (storage for data manipulation by program)
- **USB-powered**
- **USB-to-serial communication**
  - ATMega8U2
  - No hardware handshaking yet ☹
- **Good reference manual, easy-to-use IDE**
- **Price: ~ $30**



Colors Shield

- **Arduino "shield" that connects to header pins**
- **Makes it easy to manipulate multicolor LEDs directly**
- **iTead Studio: ~15**
- **Plus 8x8 multicolor LED Matrix: ~21**

- **Total for all parts, about $66**

Design Goals

- **Simplicity**
- **Controller on host system sends data over serial**
- **cerealbox interprets, renders to screen**
- **Minimal data retention (2k SRAM!)**
- **Minimal data processing**
  - Session based vs. packet based
- **Easy to understand, extend**

Data points

- **MAC address**
  - L2 data might let us do something about MITM
- **IP address**
- **TCP/UDP port**
  - Breakdown data by service
- **Country Code**
  - Let's take advantage of GeoIP

Language

1,00254B000102,0A000001,0050,US

1 – Command, open = 1, close = 2

MAC Address

IP Address (hex)

Port number (hex)

Country Code

Arduino code

- **Session tracker code on Defcon CD**
- **Everything is basic C – limited but "good enough"**
- **Primary tools are arrays and for loops**
- **Hashtables – possible with hacks but not native**

Arduino code

Text processing is fun

```
//"1" - add command
if (cmd[0] == 49 || cmd[0] == 50) {
  //Check validity of data
  boolean invalid = false;

  for (int x=1; x < 28; x++) {
    if ((cmd[x] >= 48 && cmd[x] <= 57) || (cmd[x] >= 65 && cmd[x] <= 90)
        || (cmd[x] == 44)) {}
    else invalid = true;
  }
```

Colorduino Library

- **C library by Lincomatic, huge help in dealing with LEDs**
- **Works with Colors Shield and Colorduino by iTead**

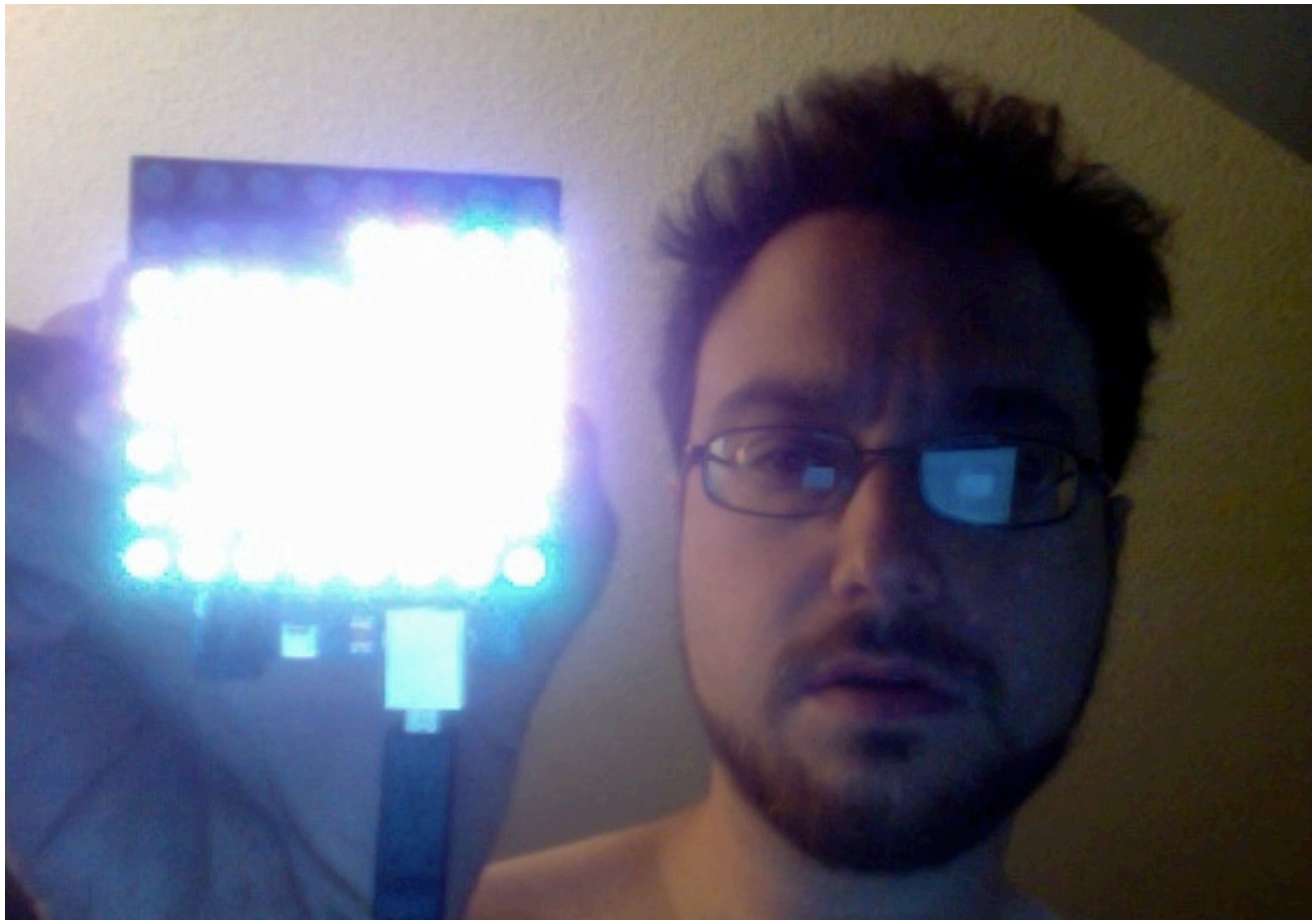
Setting an LED:

```
//Set 3,8 to Blue
Colorduino.SetPixel(3,8,0,0,255);
Colorduino.FlipPage();

//Using a pointer
PixelRGB *p = GetPixel(3,8);
p->r = 0;
p->g = 0;
p->b = 255;

// Can do p++ to increment through LEDs
```

Converting Country Code to RGB

- **Country colors are procedurally created**
  - vs. a table, which would take up SRAM/Flash
- **Arduino random is simply a long string of numbers**
  - Can use other sources for true random
  - But we actually want reproducible pseudo-random numbers
- **ASCII value of last Country Code letter is Random Seed for Red**
- **First letter -> Green**
- **Resulting Green random number is seed for Blue**

All the Colors of the Skype Rainbow



Data Storage

- **Simplified communication model = Arduino data storage**

- **Close (IP) (Port) – how does it know which LED?**
- **Store IP and Port in array**

- **9 bytes per entry**
  - RGB, IP, Port

- **128 entries ~ 1.2K**
  - OMG mah SRAM's

Array

```
//Add to array
led[pos][0] = r;
led[pos][1] = g;
led[pos][2] = b;

//pos 3-6 are ip
led[pos][3] = tohex(cmd[15])*16 + tohex(cmd[16]);
led[pos][4] = tohex(cmd[17])*16 + tohex(cmd[18]);
led[pos][5] = tohex(cmd[19])*16 + tohex(cmd[20]);
led[pos][6] = tohex(cmd[21])*16 + tohex(cmd[22]);

//pos 7-8 are port
led[pos][7] = tohex(cmd[24])*16 + tohex(cmd[25]);
led[pos][8] = tohex(cmd[26])*16 + tohex(cmd[27]);
```

Meter mode

- **Another take on the dataset**
- **Based on types of sessions being made**
- **Equalizer-ish view**
- **Give visibility to spikes, type of traffic being sent**

Performance considerations

- **9600 bps link, no handshaking**
  - Could up the speed, but be careful
- **9600 bps ~ 1200 bytes/second**
- **Message size: 32 bytes**
- **37 messages / sec, real probably about 32**

Inferno mode

- **Display limited to 128 connections**
- **Need to have a freak-out mode**
  - Throw hands up
  - Let user know that things are getting silly
- **Preferably something psychedelic**

Overload Detection

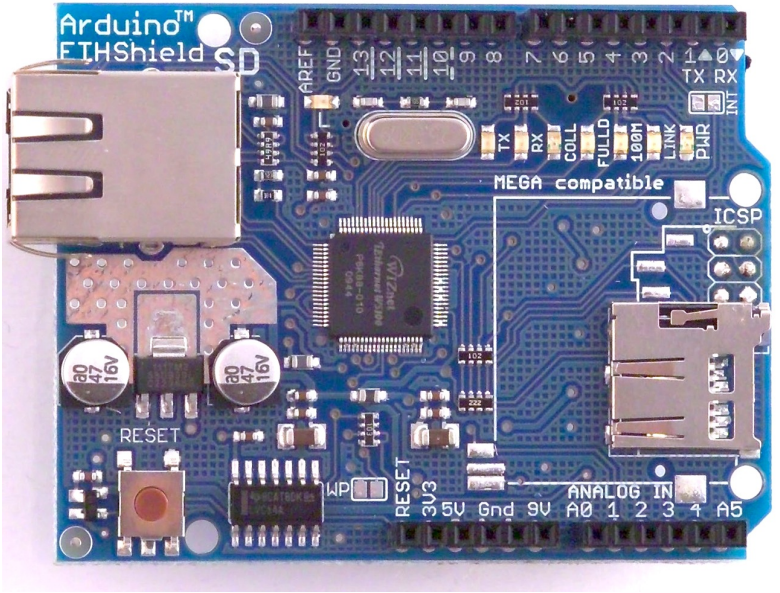
```
#define OVERLOAD 90

    if (numcmd > OVERLOAD) {
      mode = 9;
      //Delete all and start over
      while (pos > 0) {
        delete_record(pos-1);
        pos--;
      }
    }
```

Controller code

- **Perl script using Net::Pcap**
  - It works on Snow Leopard too
- **Fairly simple logic to enumerate sessions, do GeoIP**
- **Pipes over serial to Arduino**
- **2 messages, Open (1) and Close (2)**

Future Ideas

- **Ethernet Shield**
  - Eliminate need for USB/program
  - Would need 2x adapters
  - Performance would probably take a crap
- **Better host-side program**
  - Show more data behind each light
- **Bigger LEDs**
  - You know, for senior citizens



Links

- **Lincomatic's Colorduino library**
  - http://blog.lincomatic.com/?p=148
- **iTead – makers of Colors Shield and Colorduino**
  - http://iteadstudio.com
- **Arduino Uno**
  - http://arduino.cc/en/Main/ArduinoBoardUno
- **Ardunio Programming Reference**
  - http://arduino.cc/en/Reference/

Trustwave®

SpiderLabs®

Q & A