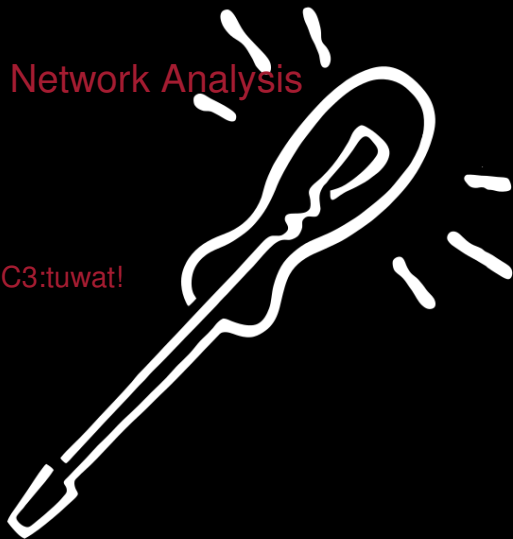# Color Based Network Analysis

34C3:tuwat!
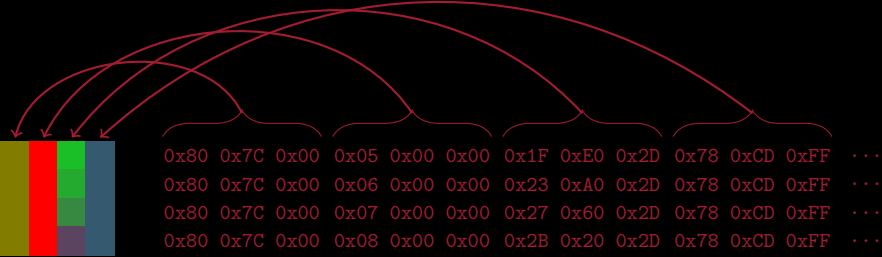
Network traffic is based on standards

https://xkcd.com/927/

Why coloring network traffic?

In the blink of an eye

"This new paper shows that the meaning of an image can be extracted even when an image is mixed up in a sequence of six or even 12 images presented at 13 milliseconds per image a rate of about 75 frames a second."[1]

---

[1] *Detecting meaning in RSVP at 13 ms per picture* by M. Potter, B. Wyble, C. Hagmann, E. McCourt

Coloring concept


```
0x80 0x7C 0x00   0x05 0x00 0x00   0x1F 0xE0 0x2D   0x78 0xCD 0xFF  ···
0x80 0x7C 0x00   0x06 0x00 0x00   0x23 0xA0 0x2D   0x78 0xCD 0xFF  ···
0x80 0x7C 0x00   0x07 0x00 0x00   0x27 0x60 0x2D   0x78 0xCD 0xFF  ···
0x80 0x7C 0x00   0x08 0x00 0x00   0x2B 0x20 0x2D   0x78 0xCD 0xFF  ···
```
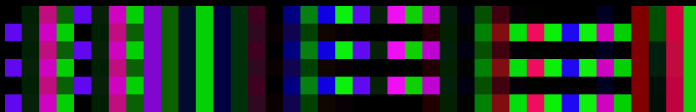
Varying the number of bits per pixel

24 Bit/Pixel

12 Bit/Pixel

1 Bit/Pixel

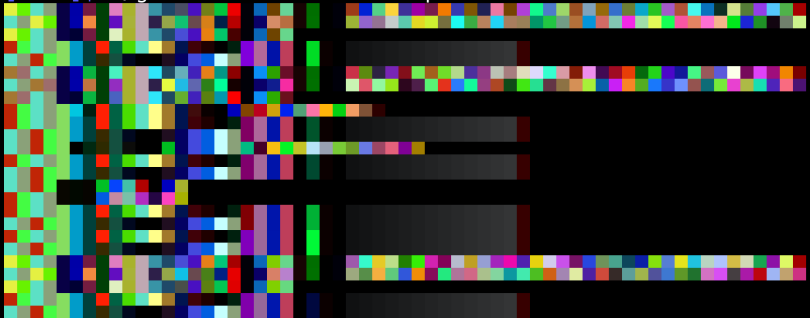# Different speech codecs

Speex with 8 kHz
sampling rate.
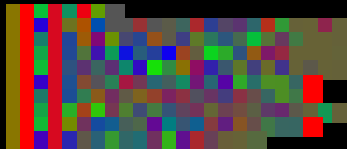
Speex with 16 kHz
sampling rate.
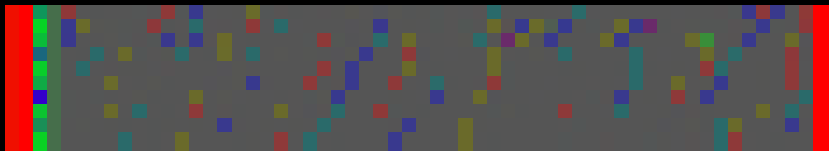
G.711 PCMA

```
[user]$ ./goNetViz -interface wlp3s0 -terminal -limit 196
```

Example: Modified ICMP packets

Thank you

Thank you for your attention.   Questions?

Get the code:
`go get -u github.com/florianl/goNetViz`