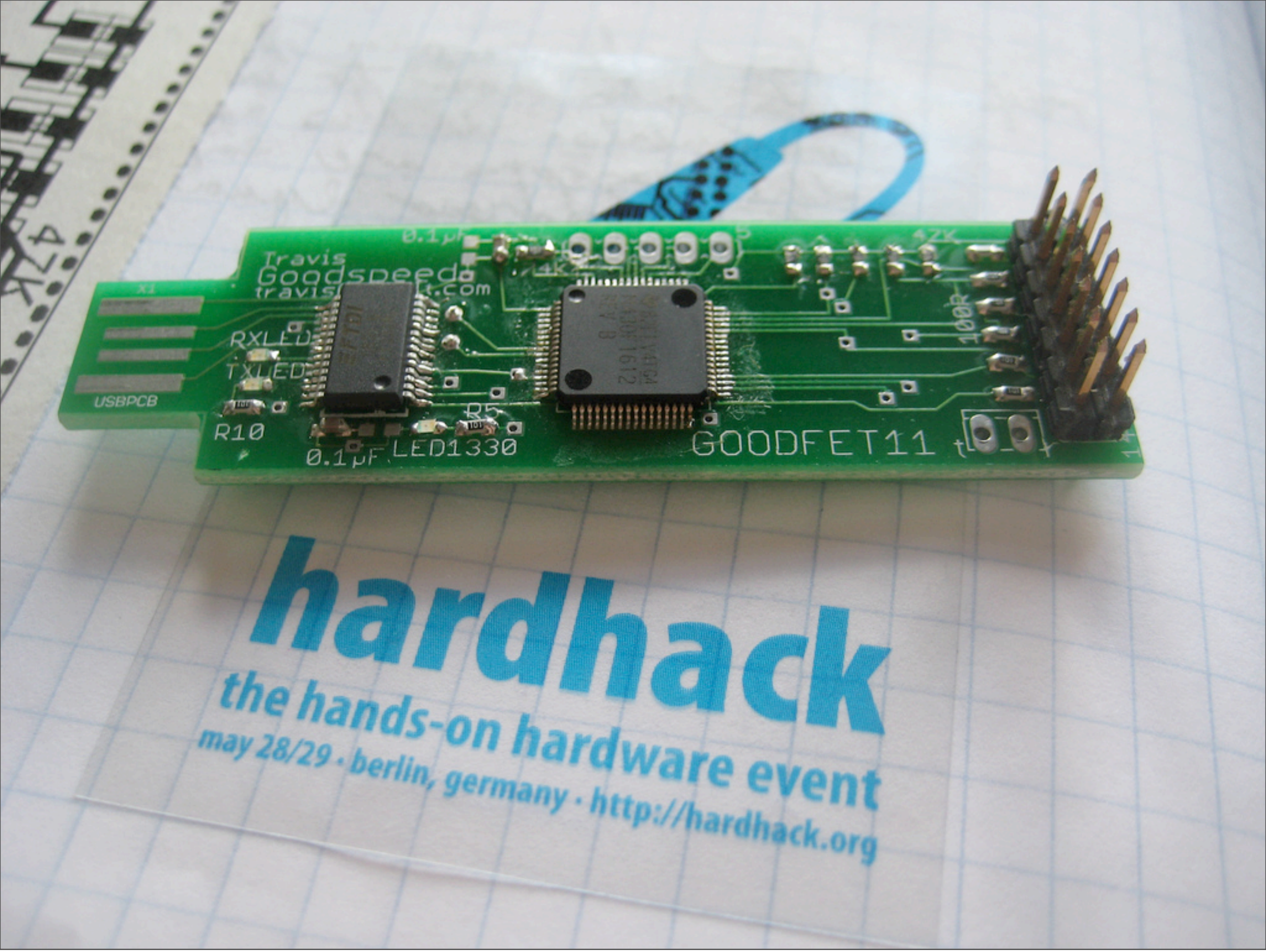
802.11 Packets in Packets

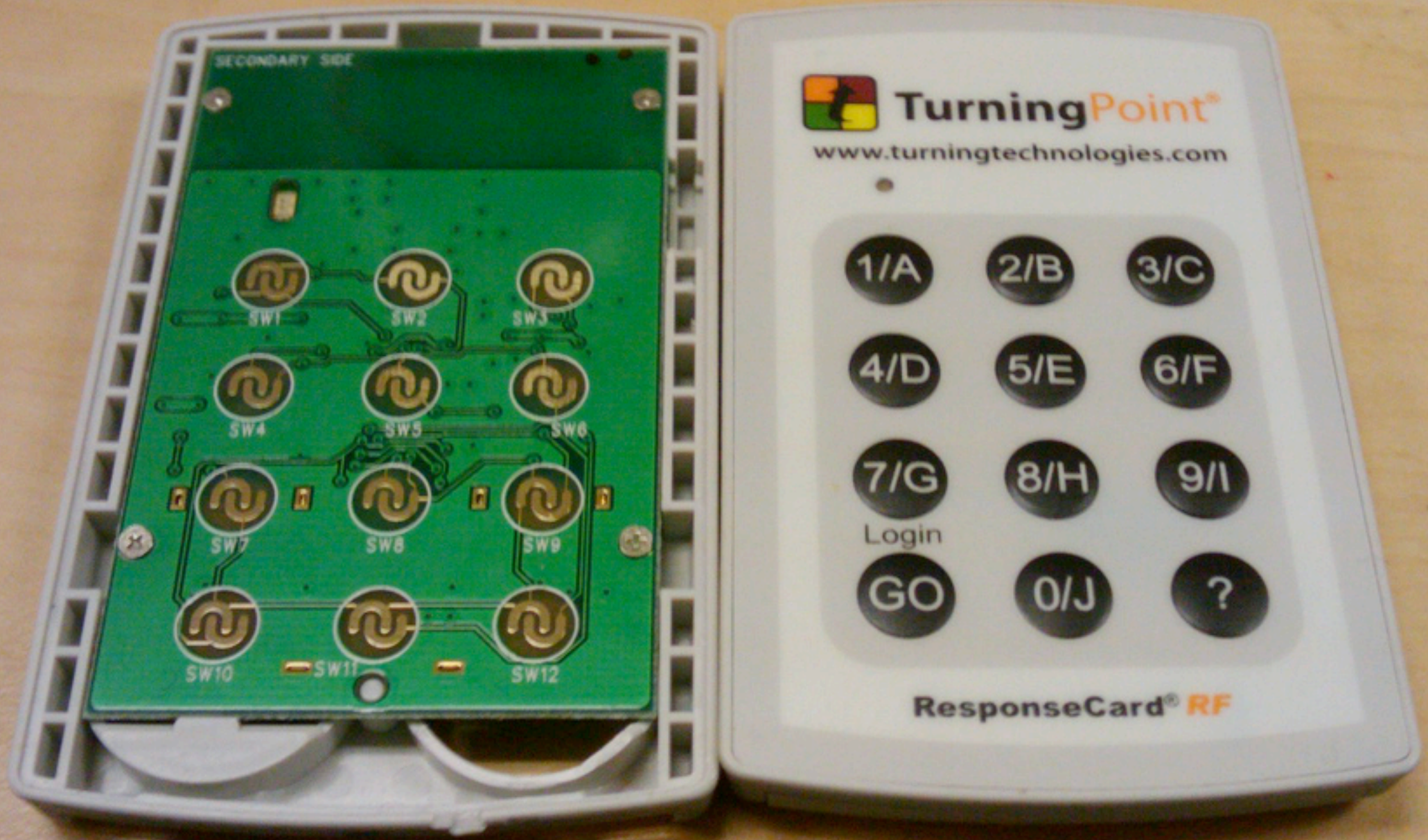
Standard-Compliant PHY Exploits

T. Goodspeed; S. Bratus
University of Pennsylvania; Dartmouth College

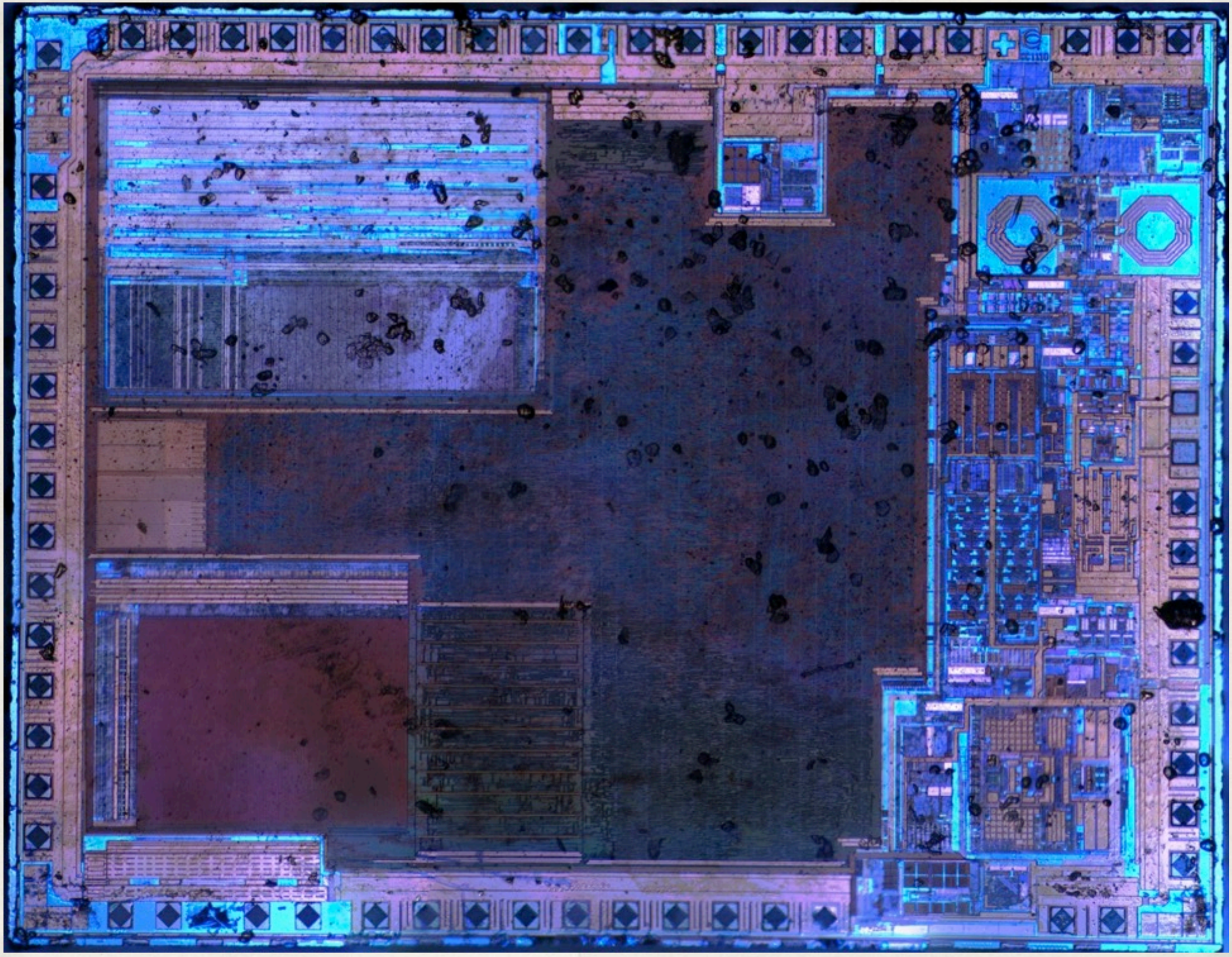
28th Chaos Communications Congress

27 December, 2011; Berlin, Germany


Travis
Goodspeed
travis@goodspeed.com
RXLED
TXLED
USBPCB
R10
R5
0.1µF
LED1330
GOODFET11
hardhack
the hands-on hardware event
may 28/29 · berlin, germany · http://hardhack.org

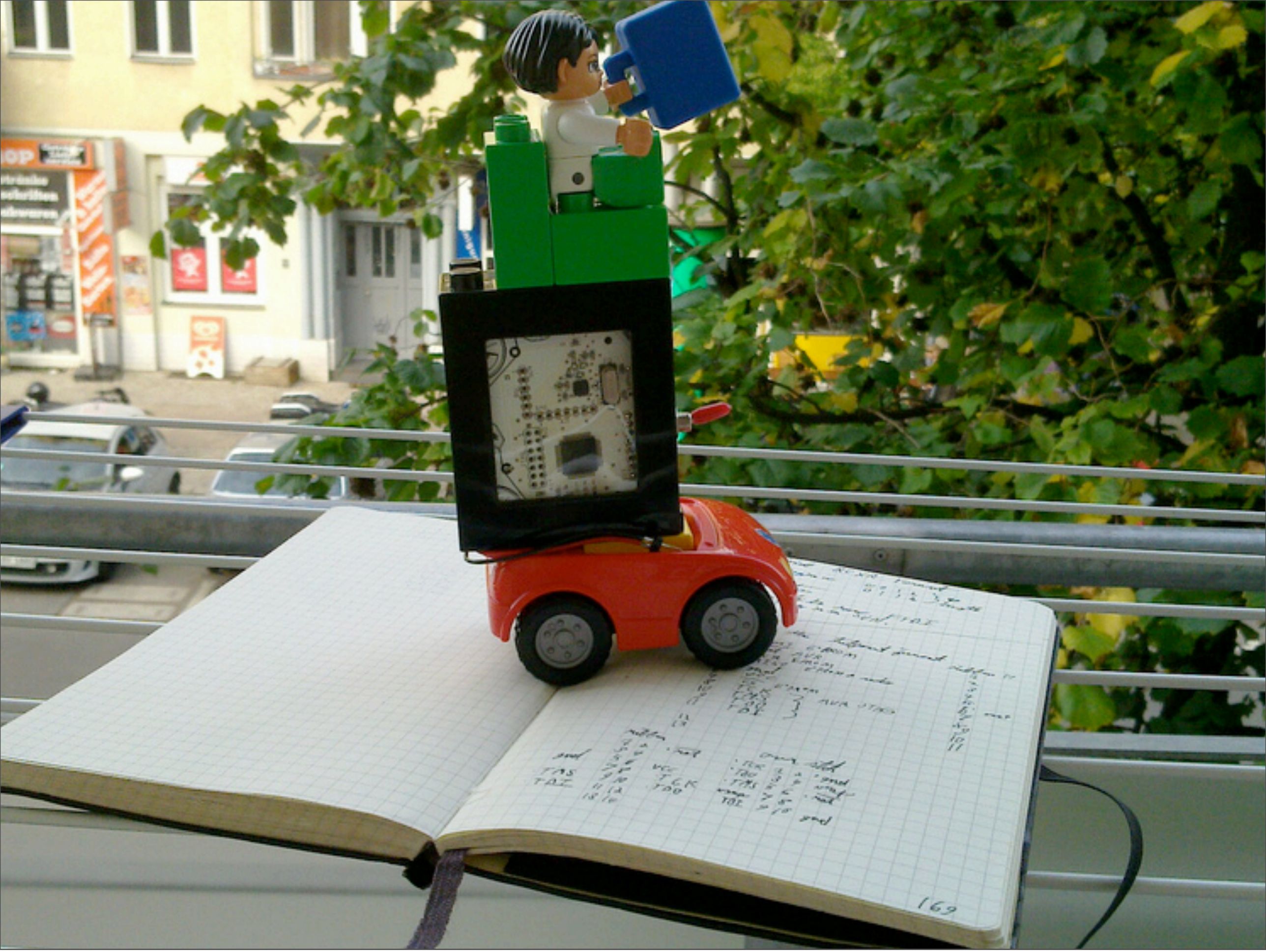


Tuesday, December 27, 2011




CC1110

Tuesday, December 27, 2011



Tuesday, December 27, 2011

Tuesday, December 27, 2011

Tuesday, December 27, 2011

802.11 Packets in Packets

Standard-Compliant PHY Exploits

T. Goodspeed; S. Bratus
University of Pennsylvania; Dartmouth College

28th Chaos Communications Congress

27 December, 2011; Berlin, Germany

RTFP

Packets in Packets:
Orson Welles' In-Band Signaling Attacks for Modern Radios

Travis Goodspeed
University of Pennsylvania

Sergey Bratus
Dartmouth College

Ricky Melgares
Dartmouth College

Rebecca Shapiro
Dartmouth College

Ryan Speers
Dartmouth College

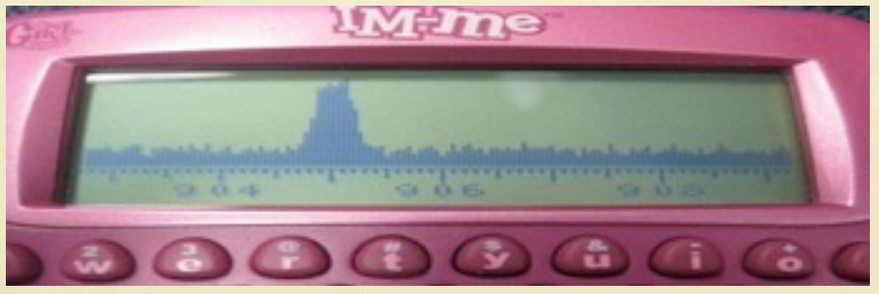
How it happened

Toor 2005, BH 2006: 802.11 L2 drivers suck

+

PLLP preamble (12 symbols)	Rate (4 b)	Reserved (1 b)	Length (12 b)	Parity (1 b)	Tail (6 b)	Service (16 b)	PSBU (payload)	Tail (6 b)	Pad

?



!


PLLP preamble
(12 symbols)
Pad

?

!


Ettus Research
USRP2

$$$$$?


Ettus Research
USRP2


IM-me

!

Remote PHY-Layer Injection

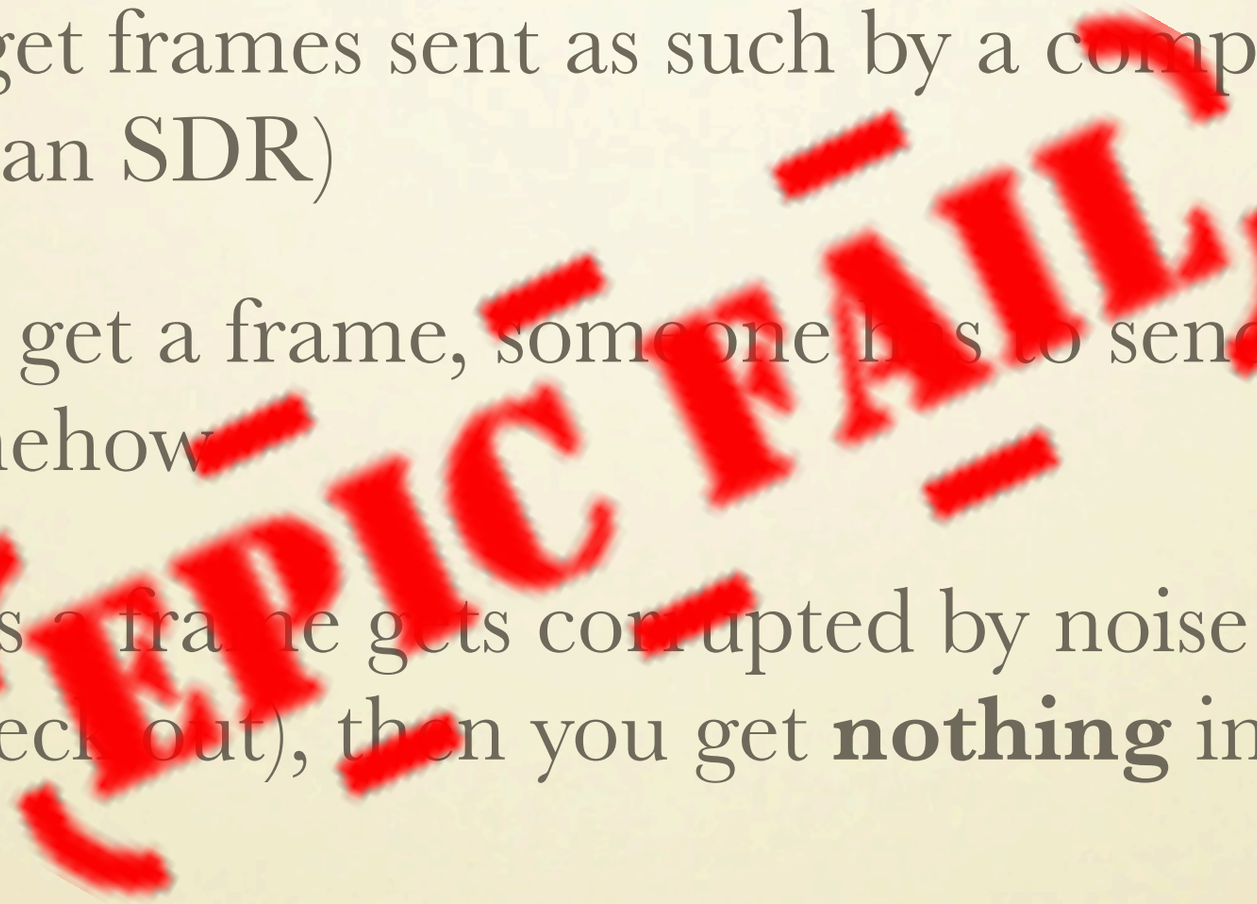
- Mallory wants to attack Bob, but
  - 1) She has no radio. All packets must be forwarded through Alice.
  - 2) Alice filters packets, stopping Mallory's favorite exploit.
- Packet-in-Packet Injection
  - 1) Mallory sends a specially crafted string in Layer 7.
  - 2) By a radio error, this string *becomes a packet* at Layer 1.
- **Impossible**?

What I believed about Digital Radio

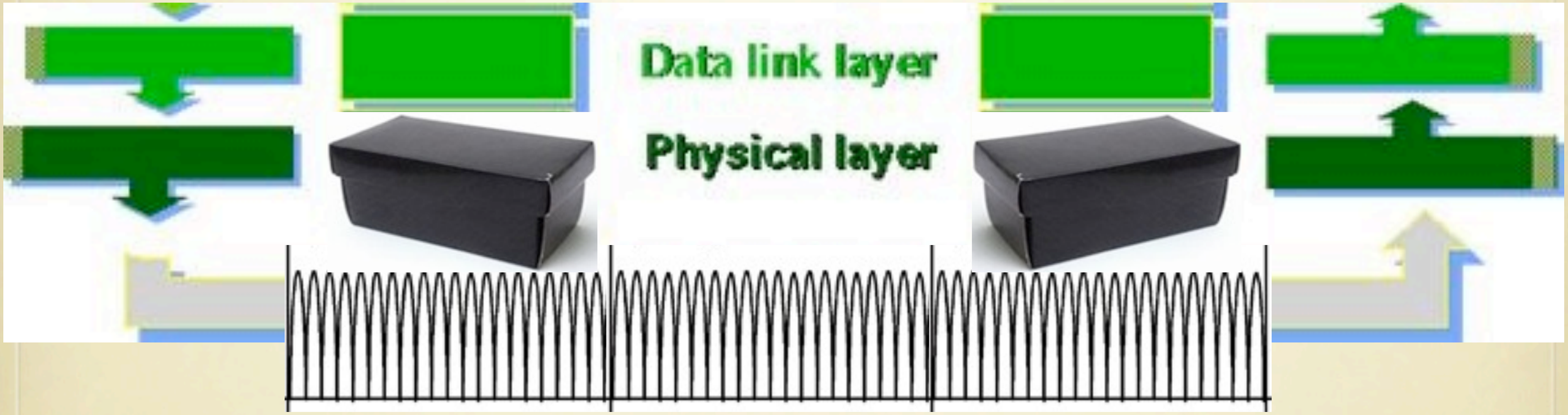
- You only get frames sent as such by a compatible device (or an SDR)
- For you to get a frame, someone has to send this **exact** frame somehow
- Sometimes a frame gets corrupted by noise (FCS doesn't check out), then you get **nothing** in normal mode
- Barring SDRs, you get in PHY only what comes from someone's compatible radio's Link layer

What I believed about Digital Radio

- You only get frames sent as such by a compatible device (or an SDR)
- For you to get a frame, someone has to send this **exact** frame somehow
- Sometimes a frame gets corrupted by noise (FCS doesn't check out), then you get **nothing** in normal mode
- Barring SDRs, you get in PHY only what comes from someone's compatible radio's Link layer

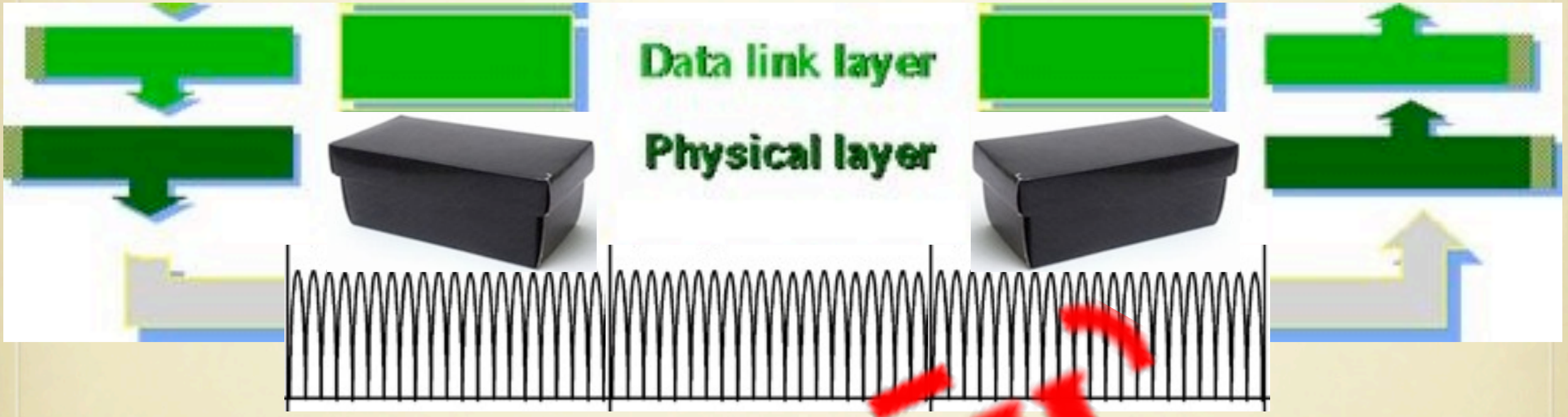


“A Black Box PHY”



- “The black box will deliver only valid or almost-valid (slightly noise-damaged) frames”

“A Black Box PHY”

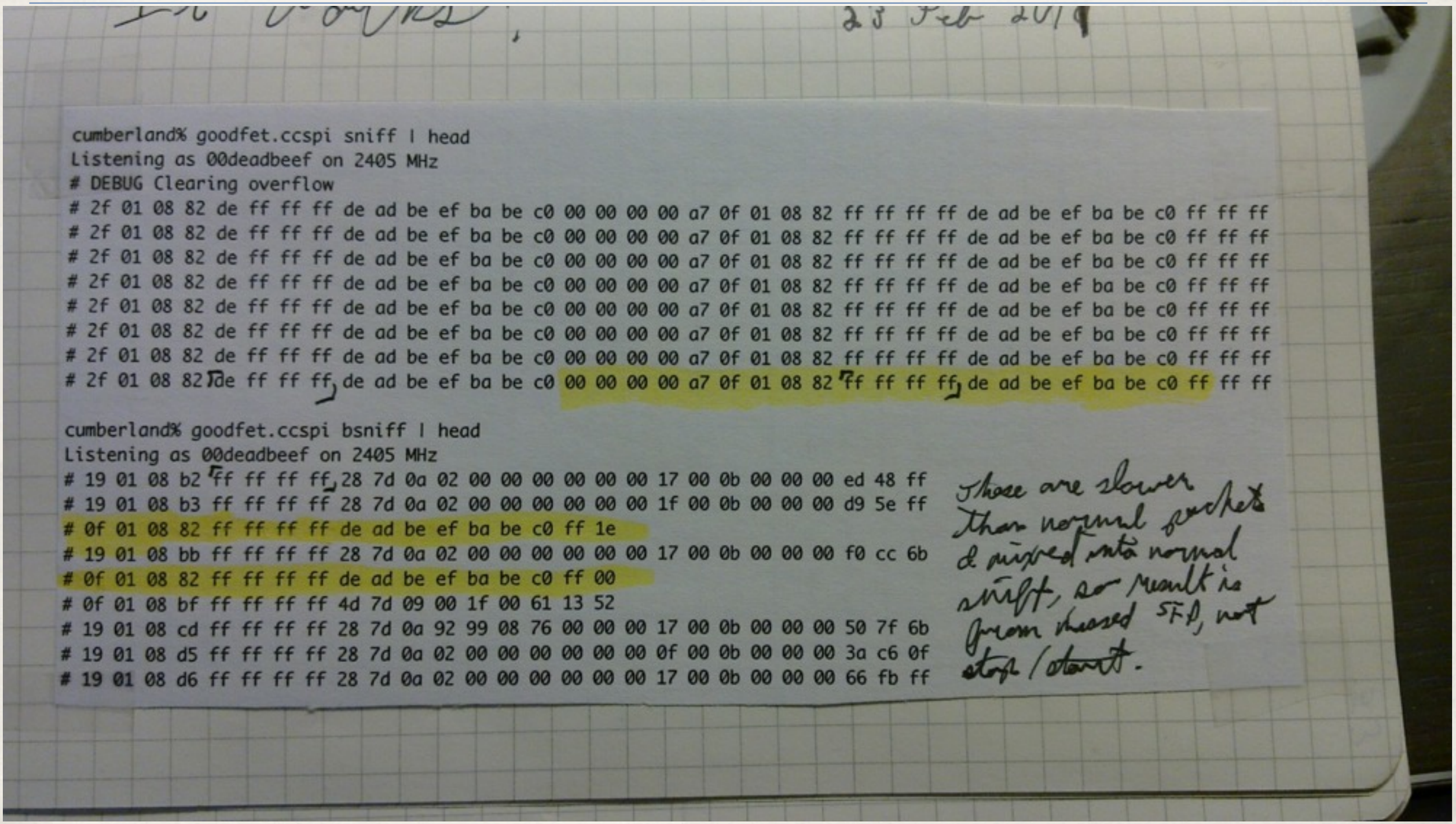


- “The black box will deliver only valid or almost-valid (slightly noise-damaged) frames”

A Packet, in a Packet

Outer	Hex	Inner
Preamble	00 00 00 00	
Sync	a7	
Body	19	
	01 08 82	
	ca fe ba be	
	00 00 00 00	Preamble
	a7	Sync
	0a 01 08 82 ff ff ff ff c9 d1	Body
	15 e8	

It Works!



23 Feb 2019

```
cumberland% goodfet.ccspi sniff | head
Listening as 00deadbeef on 2405 MHz
# DEBUG Clearing overflow
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff

cumberland% goodfet.ccspi bsniff | head
Listening as 00deadbeef on 2405 MHz
# 19 01 08 b2 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 ed 48 ff
# 19 01 08 b3 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 1f 00 0b 00 00 00 d9 5e ff
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 1e
# 19 01 08 bb ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 f0 cc 6b
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 00
# 0f 01 08 bf ff ff ff ff 4d 7d 09 00 1f 00 61 13 52
# 19 01 08 cd ff ff ff ff 28 7d 0a 92 99 08 76 00 00 00 17 00 0b 00 00 00 50 7f 6b
# 19 01 08 d5 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 0f 00 0b 00 00 00 3a c6 0f
# 19 01 08 d6 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 66 fb ff
```

These are slower than normal packets & mixed into normal stuff, so result is from biased SFD, not start/stop.

packet format

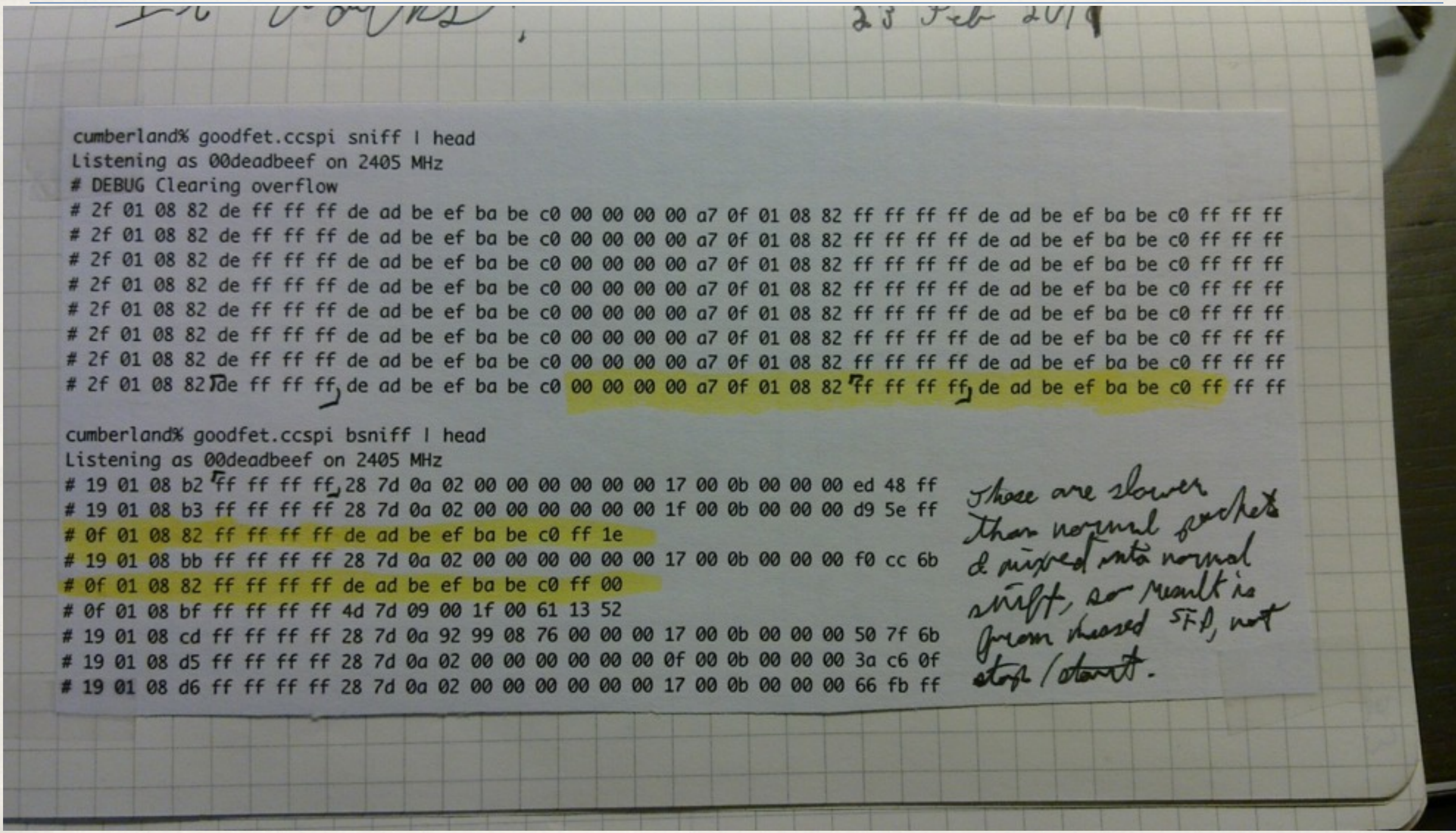
variable length

optional: whitening, FEC, Manchester

A Packet, in a Packet

Outer	Hex	Inner
Preamble	00 00 00 00	
Sync	a7	
Body	19	
	01 08 82	
	ca fe ba be	
	00 00 00 00	Preamble
	a7	Sync
	0a 01 08 82 ff ff ff ff c9 d1	Body
	15 e8	

It Works!



```
cumberland% goodfet.ccspi sniff | head
Listening as 00deadbeef on 2405 MHz
# DEBUG Clearing overflow
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff

cumberland% goodfet.ccspi bsniff | head
Listening as 00deadbeef on 2405 MHz
# 19 01 08 b2 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 ed 48 ff
# 19 01 08 b3 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 1f 00 0b 00 00 00 d9 5e ff
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 1e
# 19 01 08 bb ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 f0 cc 6b
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 00
# 0f 01 08 bf ff ff ff ff 4d 7d 09 00 1f 00 61 13 52
# 19 01 08 cd ff ff ff ff 28 7d 0a 92 99 08 76 00 00 00 17 00 0b 00 00 00 50 7f 6b
# 19 01 08 d5 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 0f 00 0b 00 00 00 3a c6 0f
# 19 01 08 d6 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 66 fb ff
```

These are slower than normal packets & mixed into normal sniff, so result is from shared SFD, not stop/start.

packet format

variable length

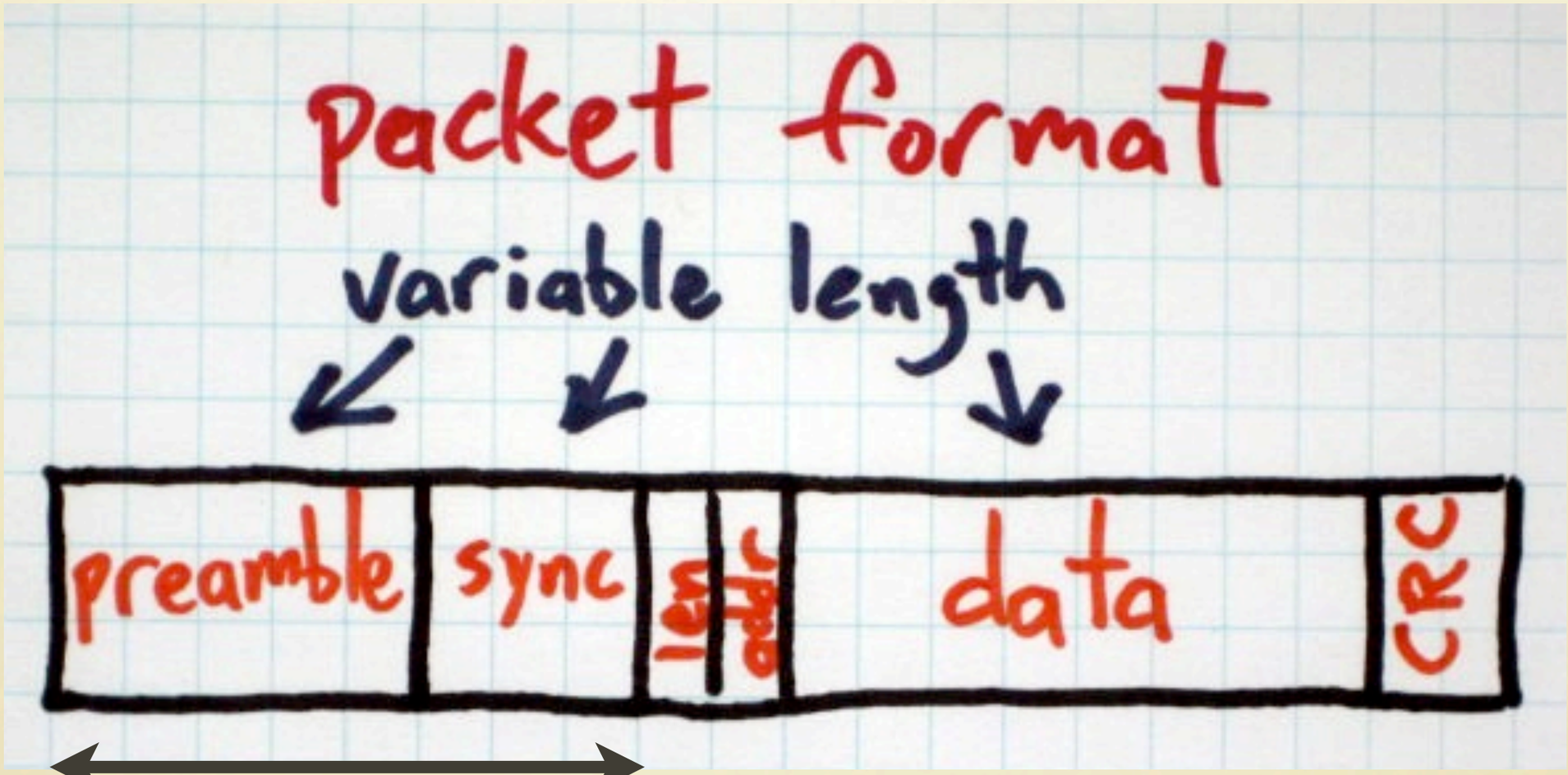
Radio Drama

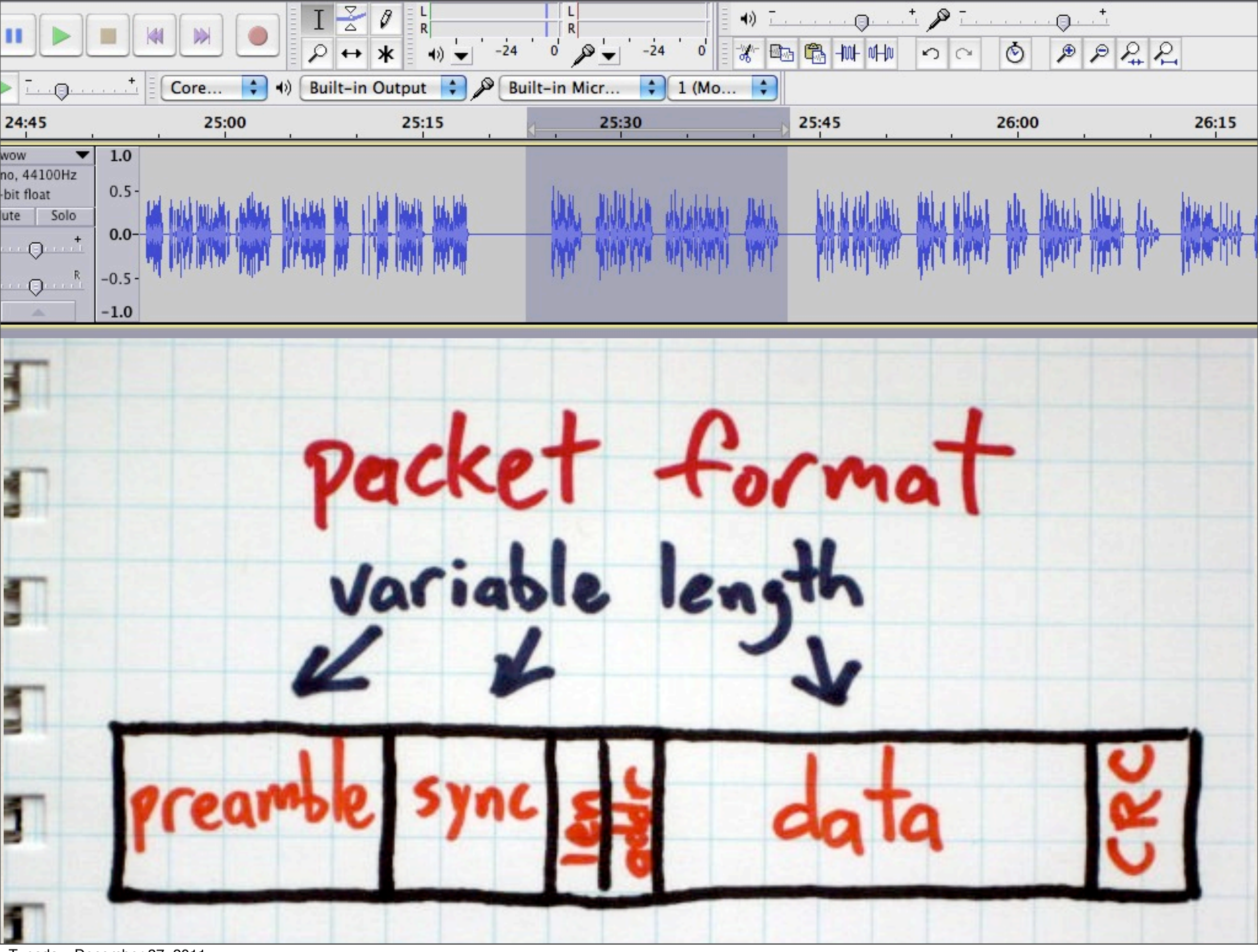
optional: whitening, FEC, Manchester

Prior Art: Orson Welles, 1938

- "**The War of the Worlds**" broadcast
- **2 min 20 sec** long **intro** (during a popular show on another station)
- **38 min** of 1st Act, starting with a fake weather report and a music concert, interrupted by fake news, interviews, eyewitness reports, and so on
- Listeners who missed the intro believed they were listening to **real** news of a Martian invasion

A packet is a packet is a packet




Core...
Built-in Output
Built-in Micr...
1 (Mo...
24:45
25:00
25:15
25:30
25:45
26:00
26:15
1.0
0.5
0.0
-0.5
-1.0
Solo
packet format
variable length
preamble
sync
data
CRC

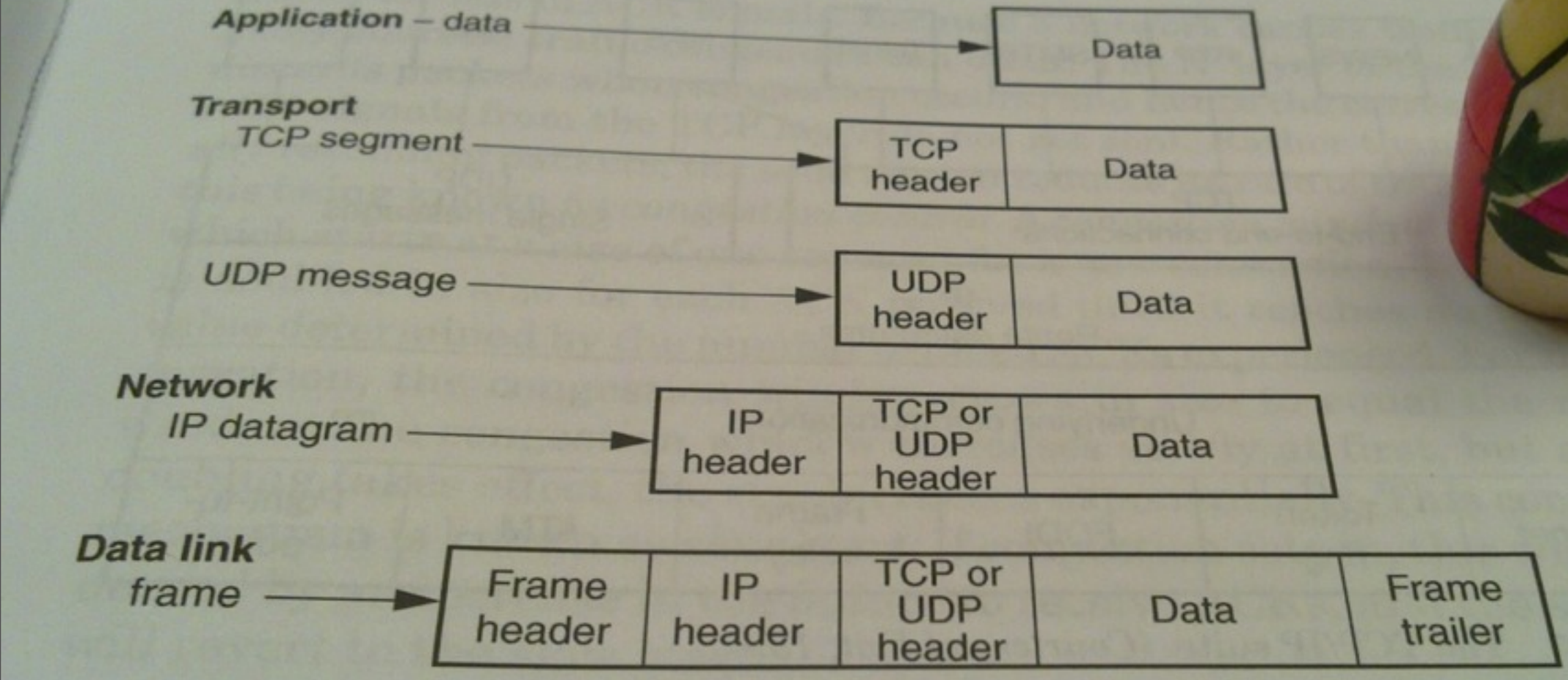


Figure 15.11 Packet terminology. (*Courtesy of Feit, 1997.*)

Sergey

referre packet comprising the TCP header, and the data

Encapsulation in Practice

Reality:
Encapsulation, in Presence of Errors

wow

Core... | Built-in Output | Built-in Micr... | 1 (Mo...

24:45 | 25:00 | 25:15 | 25:30 | 25:45 | 26:00 | 26:15

wow
Mono, 44100Hz
32-bit float
Mute | Solo

1.0 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0.0 -0.1 -0.2 -0.3 -0.4 -0.5 -0.6 -0.7 -0.8 -1.0

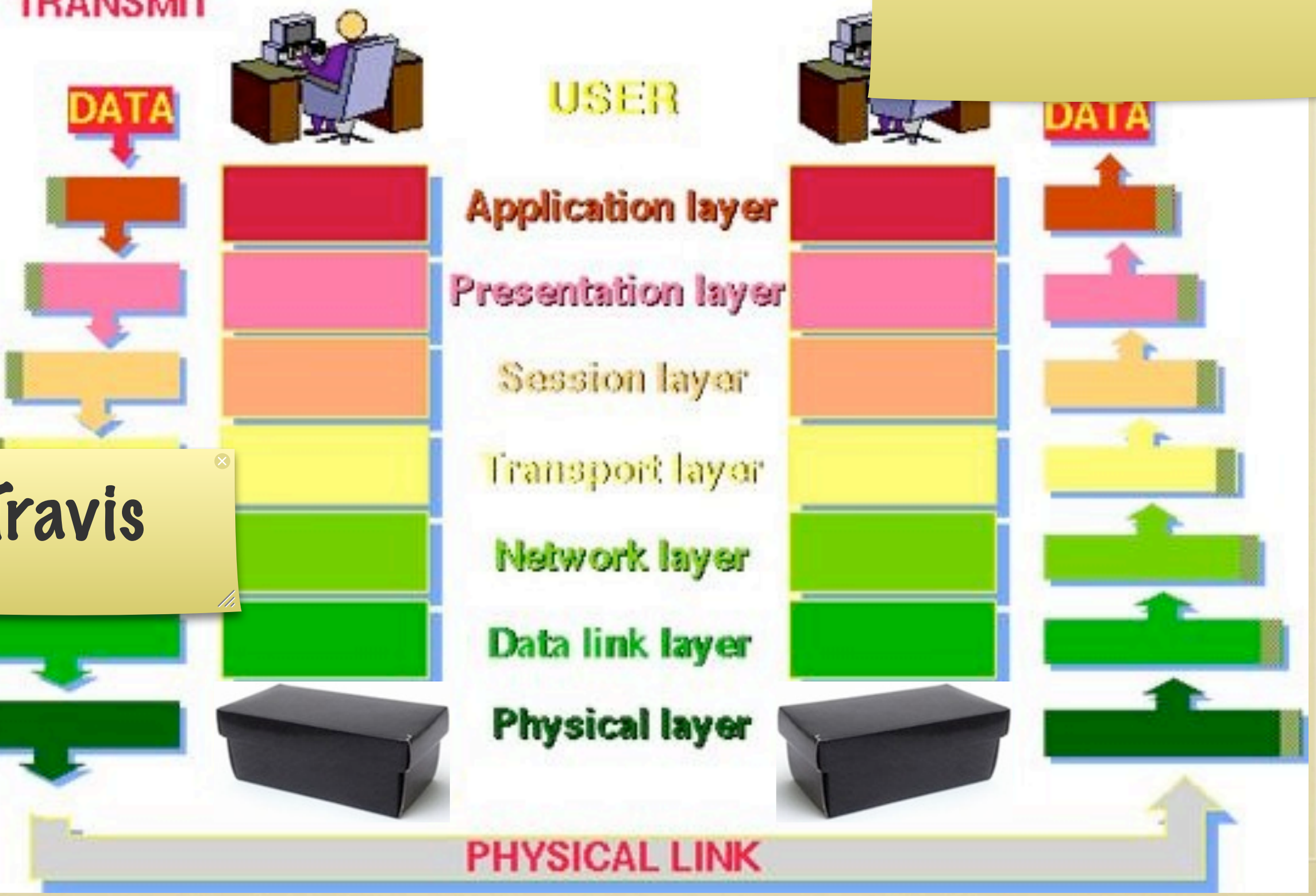
Project Rate (Hz): 44100 | Snap To | Selection Start: 00 h 25 m 22 s | End | Length 00 h 00 m 19 s | Audio Position: 00 h 00 m 00 s

Click and drag to select audio

Actual Rate: 44100

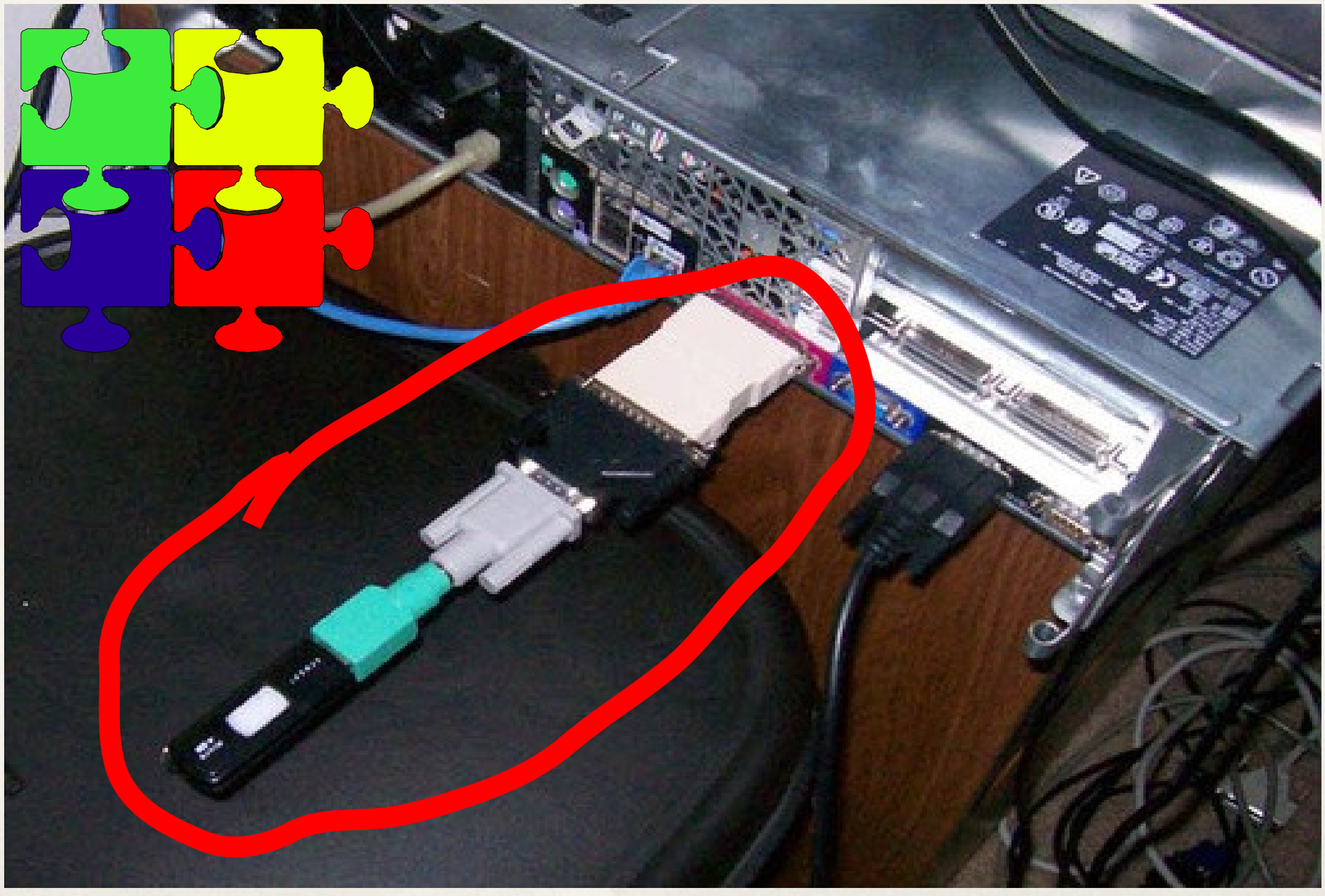
Repeat prior movement here, focusing on the urge to use parts without understanding them or their interactions.

THE 7 LAYERS OF



Travis

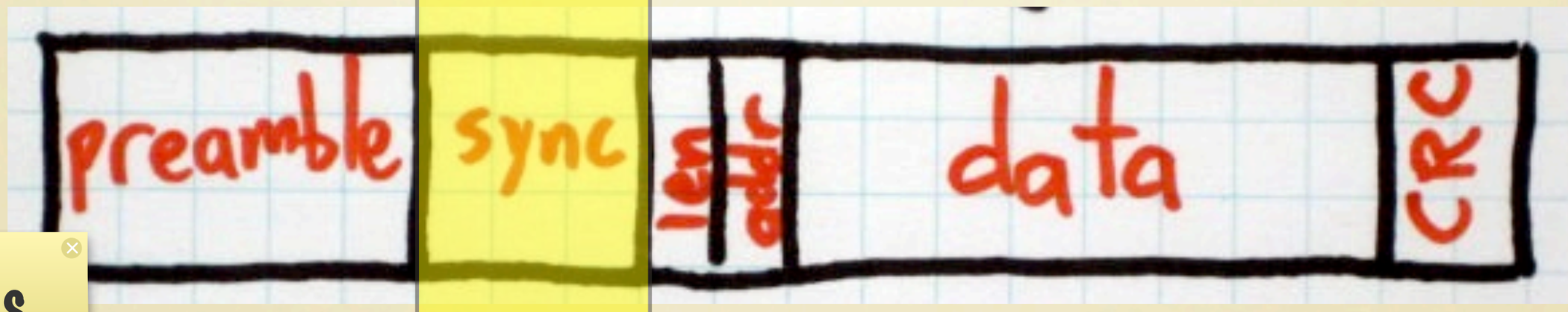
Misunderstanding Interaction



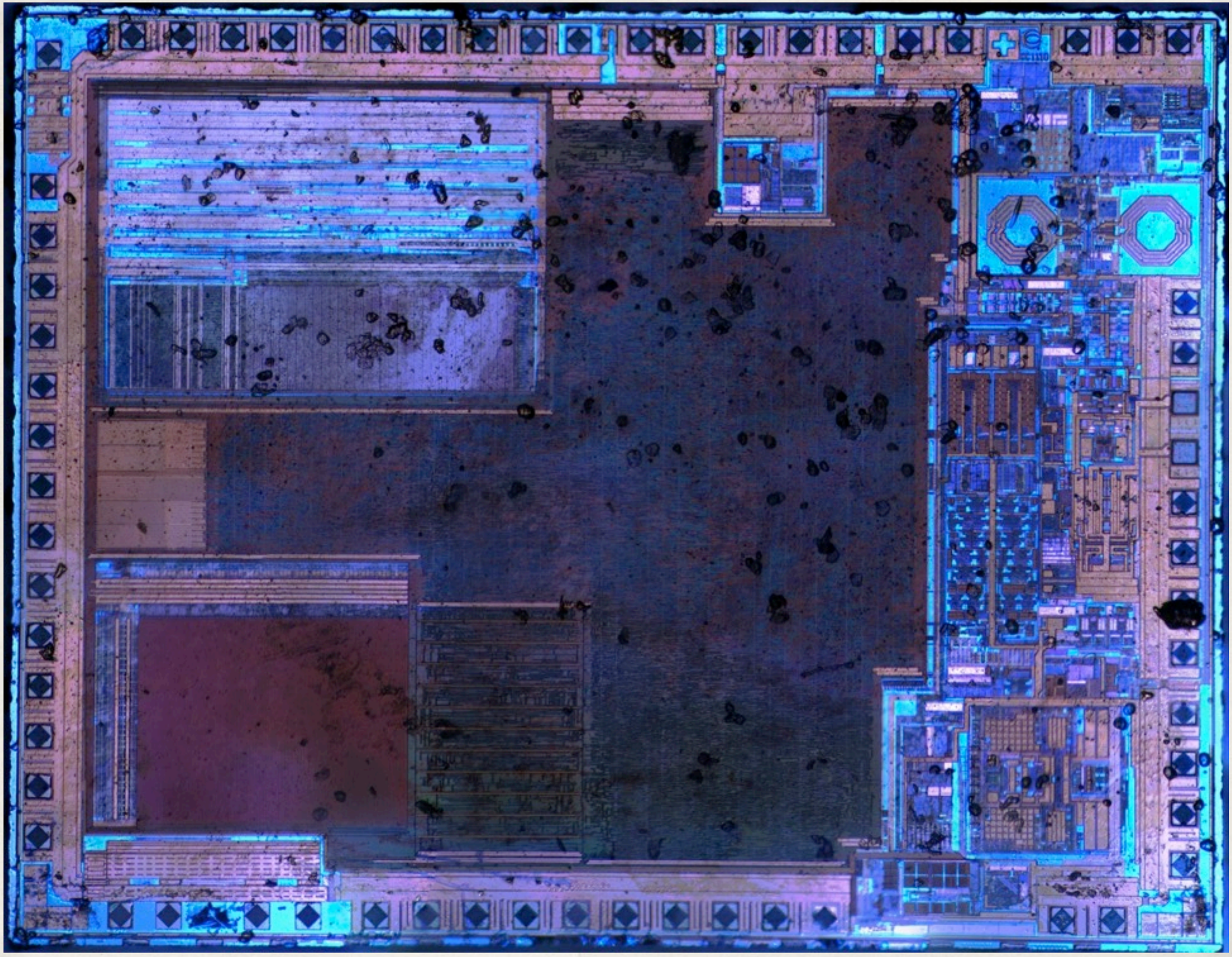
Composition Kills

"Don't trust the black box"

- It's just a bit-shift register FSM that matches SYNC
- That FSM + CRC logic cannot provide any sort of "encapsulation validation" in the presence of noise.
- "Packet is wherever/whenever a SYNC is"

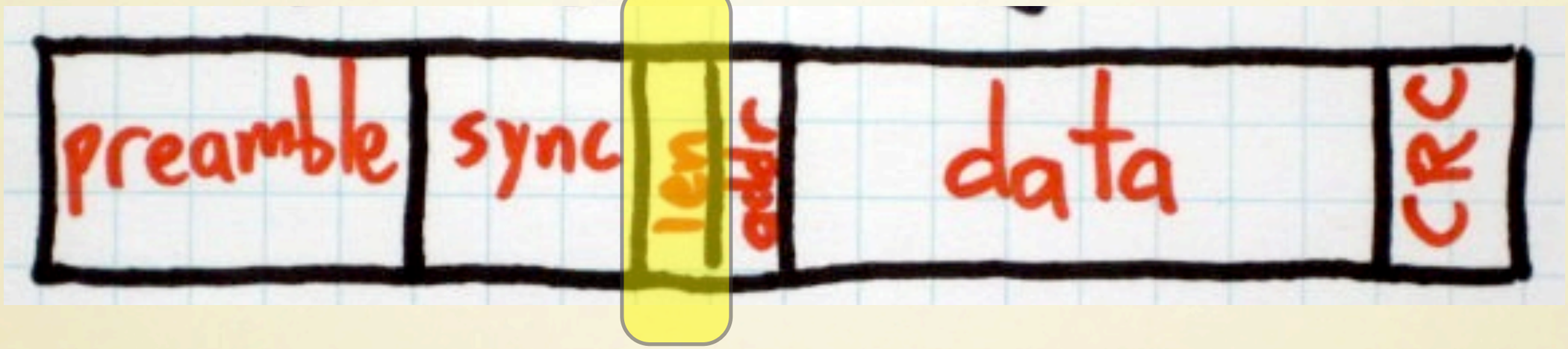


Travis




CC1110

"Length fields considered harmful"



- Parser can't tell **data** from **metadata** without context
- Makes packets a "**context-sensitive language**" -- this is BAD for parsers and input handlers
- Watch "Towards a Formal Theory of Computer Insecurity: a Language-theoretic Approach", by Len Sassaman & Meredith L. Patterson

Sergey

Complications

- Whitening
- Symbol Alignment
- Differential Signaling
- Inter-frame Gap

Complications

- Bluetooth uses Sync as Address.
- Wifi varies the data rate within a packet.
- Wifi varies encoding within a packet.

Complications

None of these are a deal-breaker.

- GSM uses Time Division Multiple Access
- 3G uses Code Division Multiple Access

End Part 1

- PIP Injection is Easy in 802.15.4
  - Prefix packet with “\x00\x00\x00\x00\xA7”.
- General Pattern
  - Include Layer 1 bytes inside of an upper layer.
  - Wifi is a lot harder.

Begin Part 2

- What does 802.11B look like?
- How the hell do we work with it?

802.11b Packet

- PLCP Header
  - First half is always 1Mbps.
  - Second half is 1 or 2 Mbps.
- PSDU Body
  - 1, 2, 5.5, or 11 Mbps

802.11b Packet

- Three data rates.
  - Three PHY standards.
  - We can only inject from the fastest.
- Final rate varies with signal strength, packet loss.

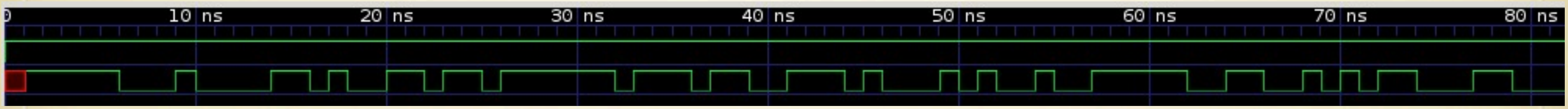
How slow is the Fastest?

- Injecting from 1Mbps BPSK
  - As easy as Zigbee/802.15.4.
  - Some networks can't drop this low.
- 2Mbps QPSK
  - 1Mbps can be recreated.
  - Requires guessing a 7-bit scrambler state.

Other Rates

- 5.5Mbps and 11Mbps 802.11B
- 802.11G
  - Different body rates, but same header rate.

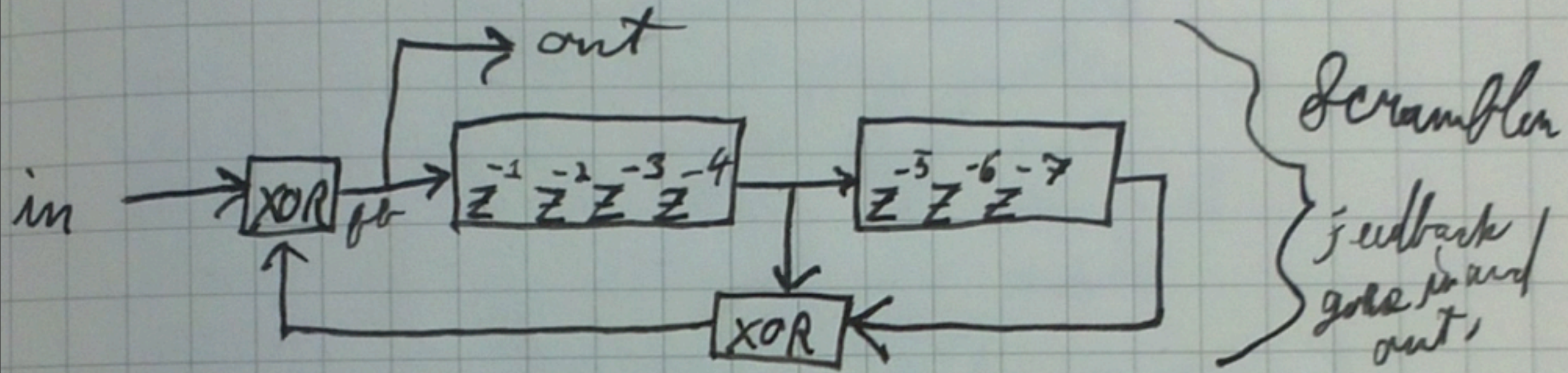
Scrambled Preamble

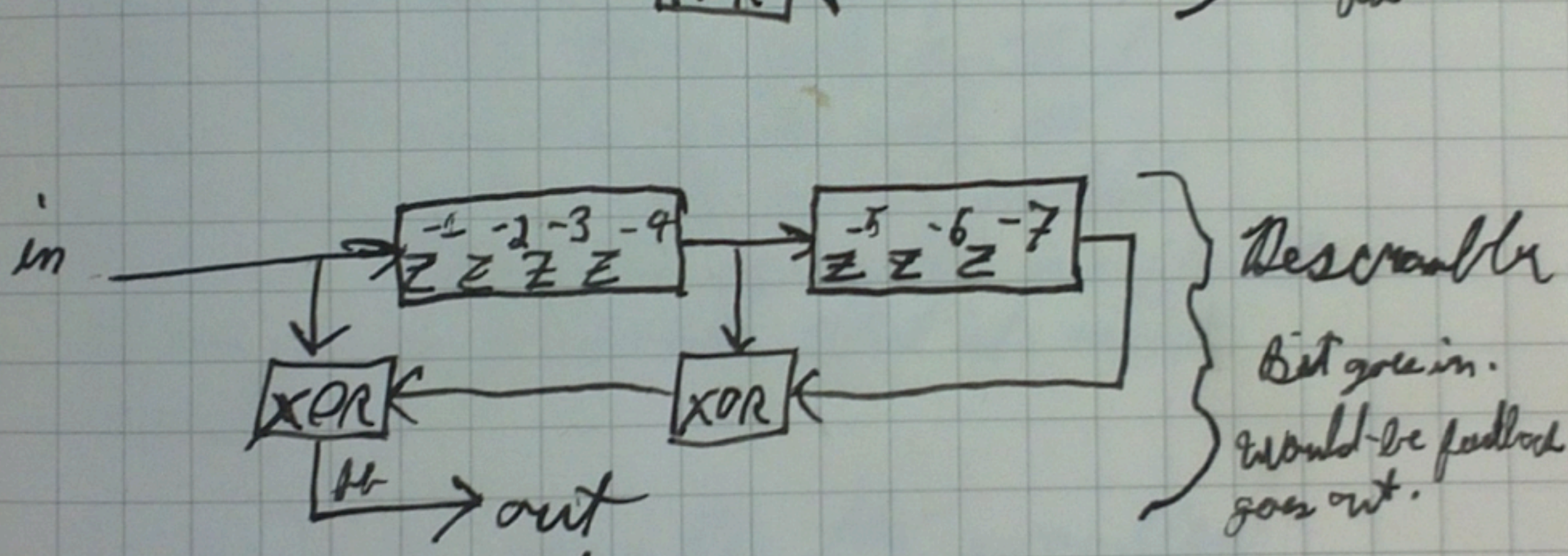


- FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
  FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
- Scrambled from any state but 7b1111111.

The scrambler design follows, initialized to anything but all one's.

$$G(z) = z^{-7} + z^{-4} + 1$$





Scrambler

- 7-bit LFSR
- Initialized to anything but 7b1111111
  - No requirement that it's random.
- Must be predicted in order to inject across rates.

Scrambler/ Descrambler

- Scrambler randomizes the appearance of each packet.
  - 127 different preamble patterns.
  - 128 different Start-Frame Delimiters.
- Descrambler self-synchronizes.
  - State recoverable from past 7 bits.
  - Attacker can’t observe these bits.

1 Mbps to 1 Mbps

- Same symbol set, same rate, corrected scrambler.
- Just like ZigBee, put the right bytes in the right order.
- Prefix is just the PLCP.
  - 128 bits of 1's
  - F3A0 -- Start Frame Delimiter
  - 0A0000C0EADA -- Flags, rate, CRC.

2Mbps to 1Mbps

- Symbol rate is the same: 1MS/s
- Symbol set changes:
  - 1Mbps -- 0, π
  - 2Mbps -- 0, π/2, π, 3π/2
- All the 1Mbps symbols exist in 2Mbps traffic!

2Mbps to 1Mbps

BPSK	QPSK	Phase Change
0	00	0
	01	pi/2
1	11	pi
	10	3pi/2

- 2Mbps symbols can recreate 1Mbps symbols.

2Mbps to 1Mbps

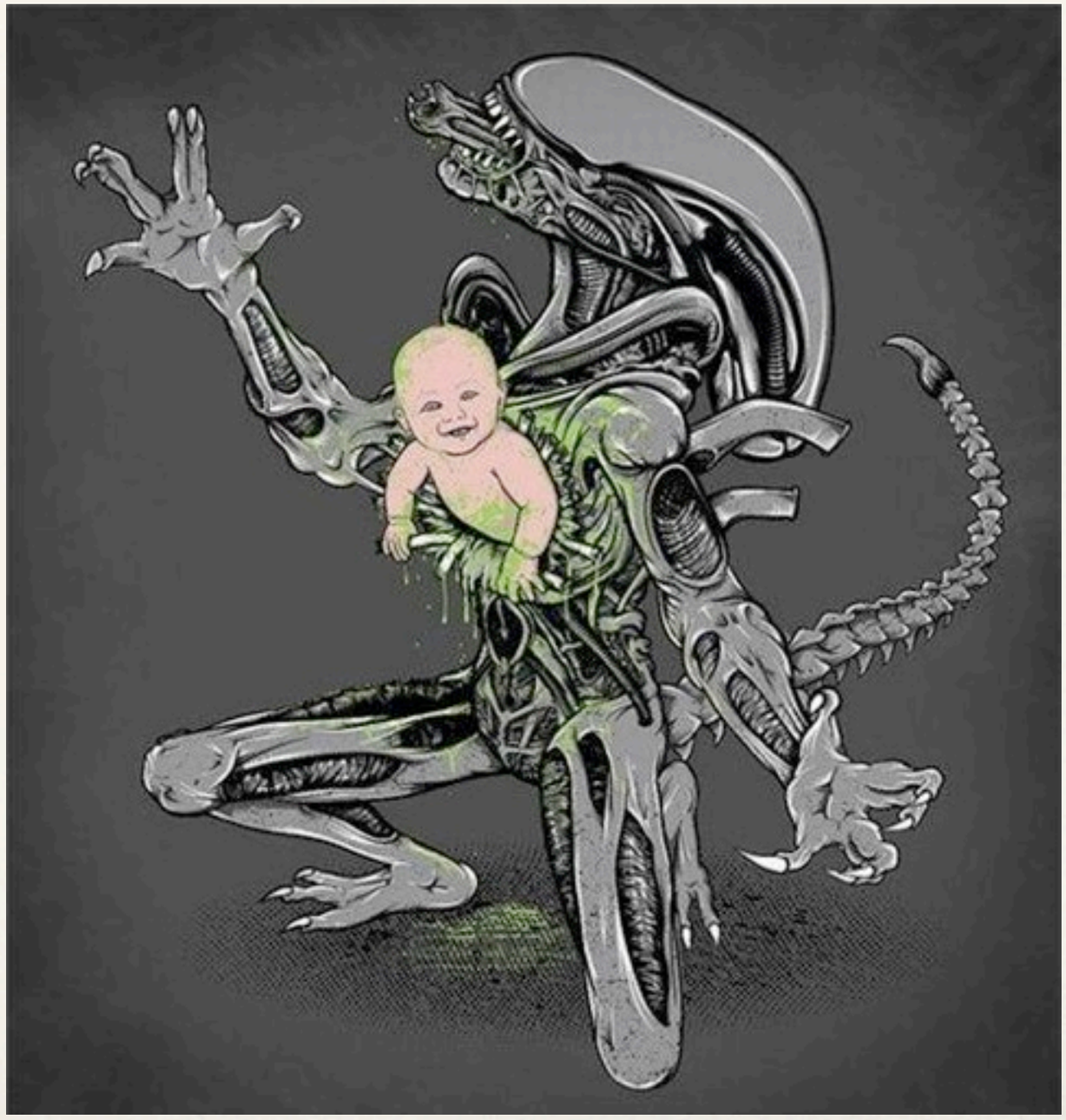
- Scrambler no longer self-corrects, so we need to guess.
  - Verilog at https://github.com/travisgoodspeed/
  - 7-bit state only reduces our odds 128 times.

State of PIP in Wifi

- 802.11B is vulnerable to PIP injection.
  - At 1Mbps and 2Mbps.
  - When the transmission network is cleartext.

Layers of Abstractions Become Boundaries of Competence

Questions?



802.11 Packets in Packets

Standard-Compliant PHY Exploits

T. Goodspeed; S. Bratus
University of Pennsylvania; Dartmouth College

28th Chaos Communications Congress

27 December, 2011; Berlin, Germany