MAKING FRIENDS (OUT OF THIN AIR)

Impersonating Tamagotchis with Infrared

@zachr@infosec.exchange

dani.pink

What is a Tamagotchi?

- Virtual pet
- Feed it
- Play with it
- Clean up its poop

Tamagotchi Connection™ (2024 v3 re-release)

Why?

- Interest in Infrared signals from trying to reverse engineer Pixmob wristbands
- Seemed fun

PixMob (background)

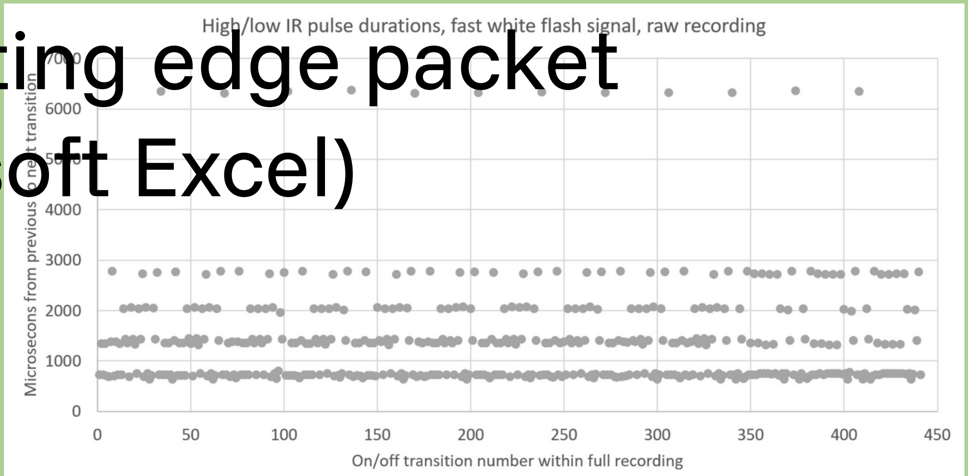
- PixMob: bracelets given out to attendees at concerts and sports events which light up in sync with the show
- Used at:
  - Taylor Swift Eras Tour
  - Coldplay Music of the Spheres Tour
  - Superbowl
  - DC Furs 2025

PixMob (background)

- We wanted to reverse-engineer the protocol to control these bracelets at home
- Recorded IR signals with Flipper Zero, and later some custom devices

PixMob (background)

- Analyzed IR codes in cutting edge packet analysis software (Microsoft Excel)
- ???????

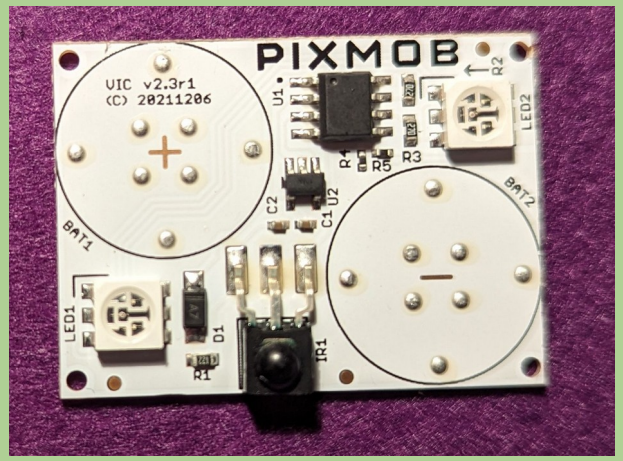


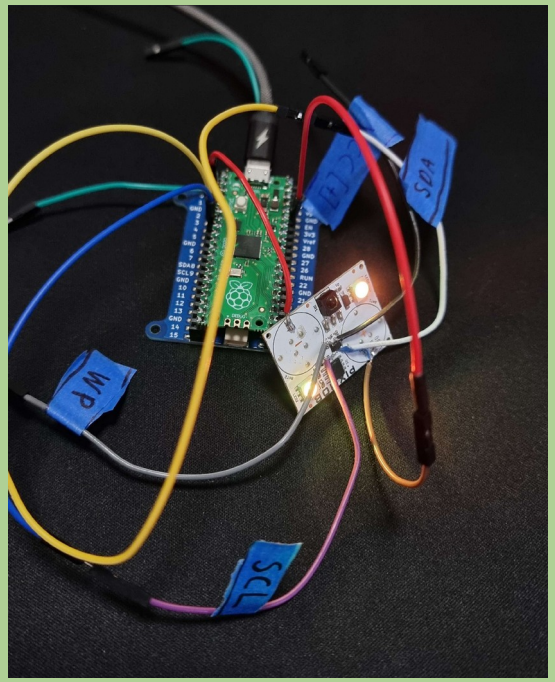
	Header and color information	Fade effect information "tail"
MAGENTA_SHARP_FLASH	1 0 1 0 1 1 0 0 1 1 0 0 0 0 1 0 0 0 1 1 0 0 0 1 0 1 0 1 1 0 0 0 1 0 1 0 0 0 1	
GREEN_SHARP_FLASH	1 0 1 0 1 1 0 0 1 1 0 0 0 0 1 0 0 1 0 1 1 0 0 1 0 0 1 1 0 0 0 0 1 1 0 0 0 0 1	
MAGENTA_FADE_IN_TAIL	1 0 1 0 1 1 0 0 1 1 0 0 0 0 1 0 0 0 1 1 0 0 0 1 0 1 0 1 1 0 0 0 1 0 1 0 0 0 1	0 0 0 1 0 1 1 0 1 0 0 0 1 0 0 0 0 1 1 0 0 0 0 1
GREEN_FADE_IN_TAIL	1 0 1 0 1 1 0 0 1 1 0 0 0 0 1 0 0 1 0 1 1 0 0 1 0 0 1 1 0 0 0 0 1 1 0 0 0 0 1	0 0 0 1 0 1 1 0 1 0 0 0 1 0 0 0 0 1 1 0 0 0 0 1
MAGENTA_FADE_OUT_TAIL	1 0 1 0 1 1 0 0 1 1 0 0 0 0 1 0 0 0 1 1 0 0 0 1 0 1 0 1 1 0 0 0 1 0 1 0 0 0 1	0 0 0 0 1 1 0 0 1 0 0 0 1 0 1 0 0 1 1 0 0 0 0 1
GREEN_FADE_OUT_TAIL	1 0 1 0 1 1 0 0 1 1 0 0 0 0 1 0 0 1 0 1 1 0 0 1 0 0 1 1 0 0 0 0 1 1 0 0 0 0 1	0 0 0 0 1 1 0 0 1 0 0 0 1 0 1 0 0 1 1 0 0 0 0 1

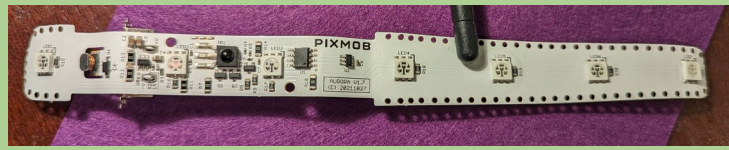
FAST_WHITE	1 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 1 0 1 1 0 0 0 0 1 0 0 1 0 0 1 0 0 0 1 1 0 0 1 0 0 0 1 1 0 0 1 0 0 0 1 1 0 0 0 0 1 0 0 0 1 0 1 0 0 0 1 1 0 0 0 0 0 1
SLOW_YELLOW	1 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 1 1 0 1 0 0 0 0 1 0 0 1 0 0 1 0 0 0 1 1 0 0 1 0 0 0 1 1 0 0 0 0 1 0 0 0 1 1 0 1 0 1 0 0 1 1 0 0 0 0 1 1 0 0 0 0 0 1

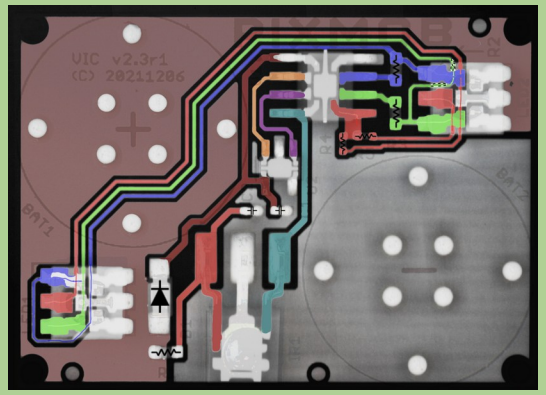
PixMob (background)

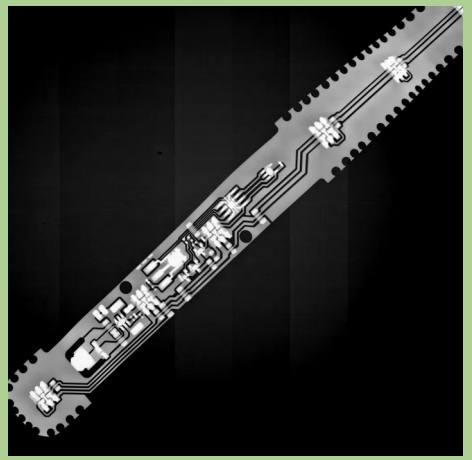
- Decided to just brute force stuff and now we can light up bracelets in fun colors











X-rays from samy.pl, pico ROM dumper from cra0

Brief overview of Infrared data transfer

Encoding and Modulating data

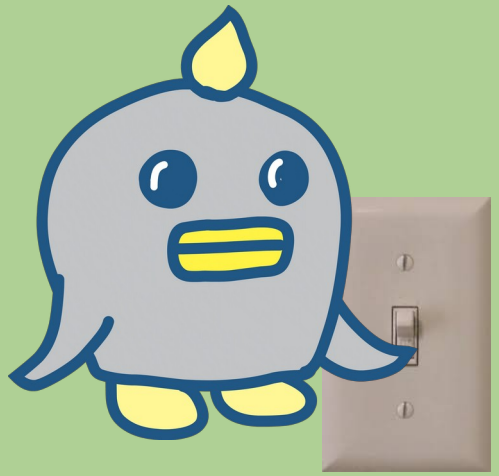
- Represent two states: 0 and 1
- How do you make a wave do two different things?

Carrier Waves

- When the light is “on” it’s actually blinking at about 38 kHz
- Mostly relevant when you’re selecting hardware
- Useful to reduce interference from any light that’s not blinking at this frequency

Encoding and Modulating data

- Lots of interesting options, but we're just going to turn the light on and off



On Off Keying (OOK)

- 1 when light is on
- 0 when light is off

Logical

- 0xFFFFFFFF…FFFFF
- 0x0000000…00000

Physical

- LED on for a long time
- LED is off for a long time

Logical

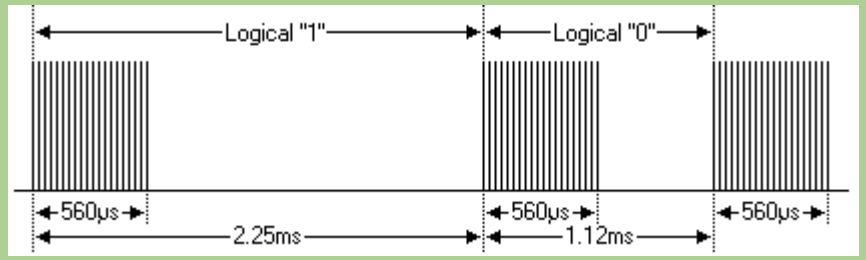
- Logical 1:
  - Represents “1”
- Logical 0:
  - Represents “0”

≠

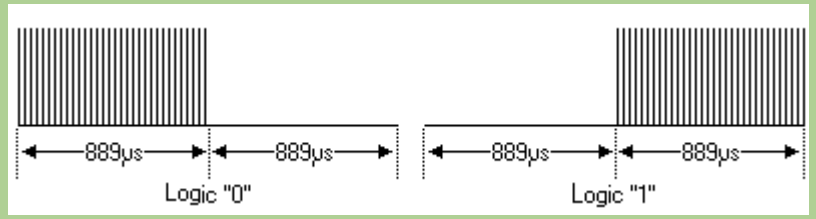
Physical

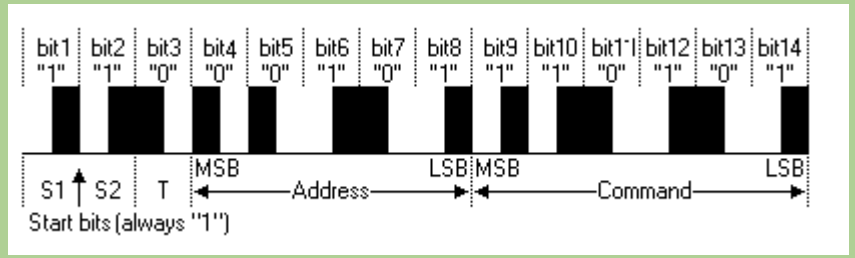
- Mark/pulse:
  - Light is on
- Space/gap:
  - Light is off

NEC - pulse distance modulation

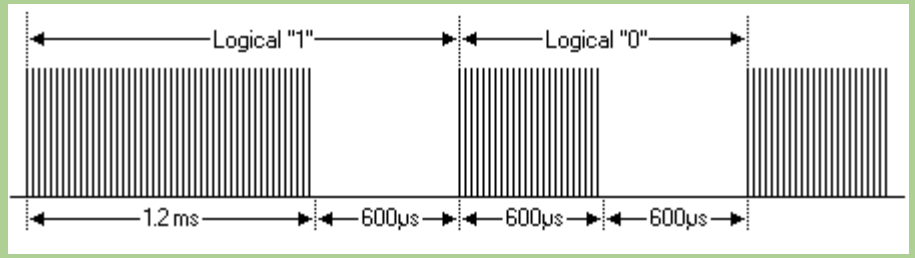


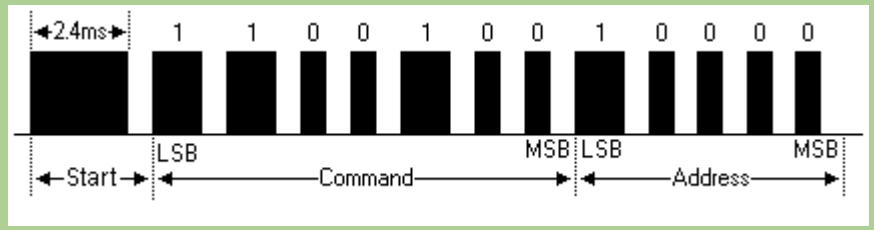
Phillips RC5 - pulse position modulation (aka Manchester)



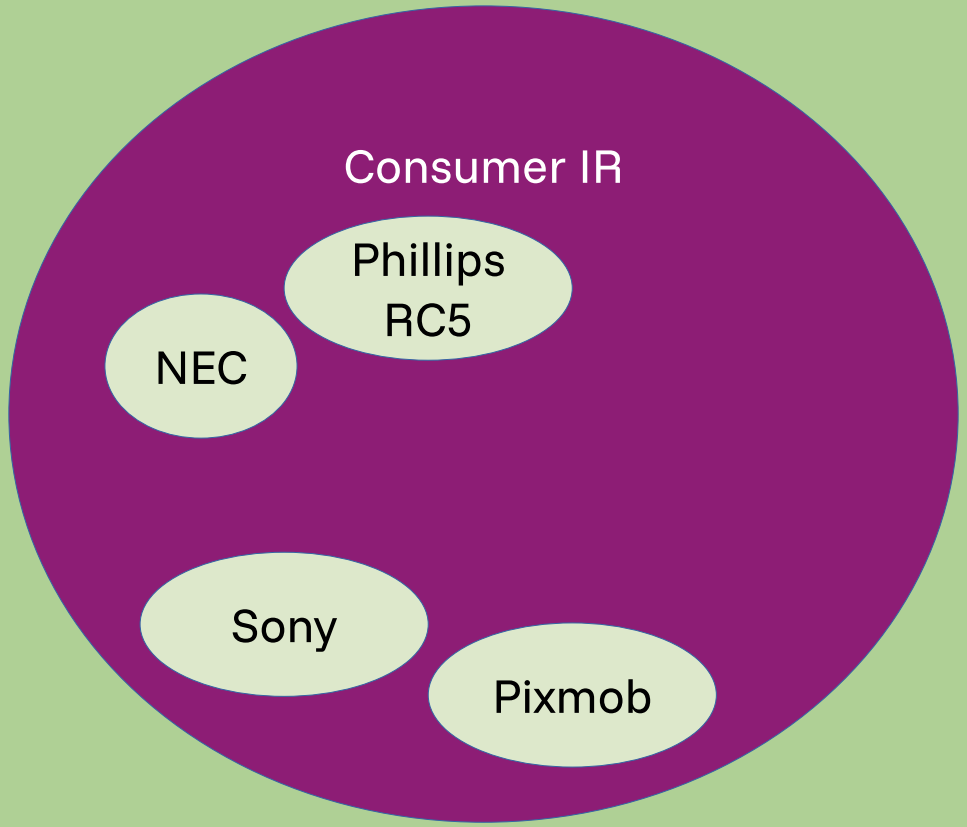


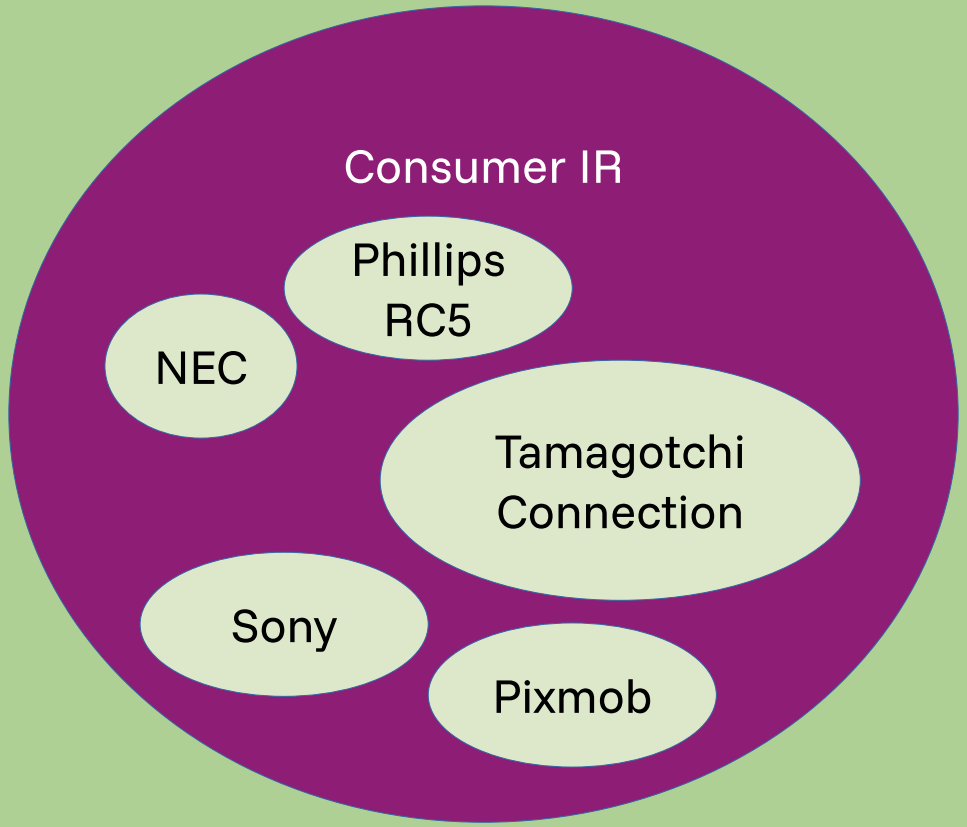
Sony - pulse width modulation

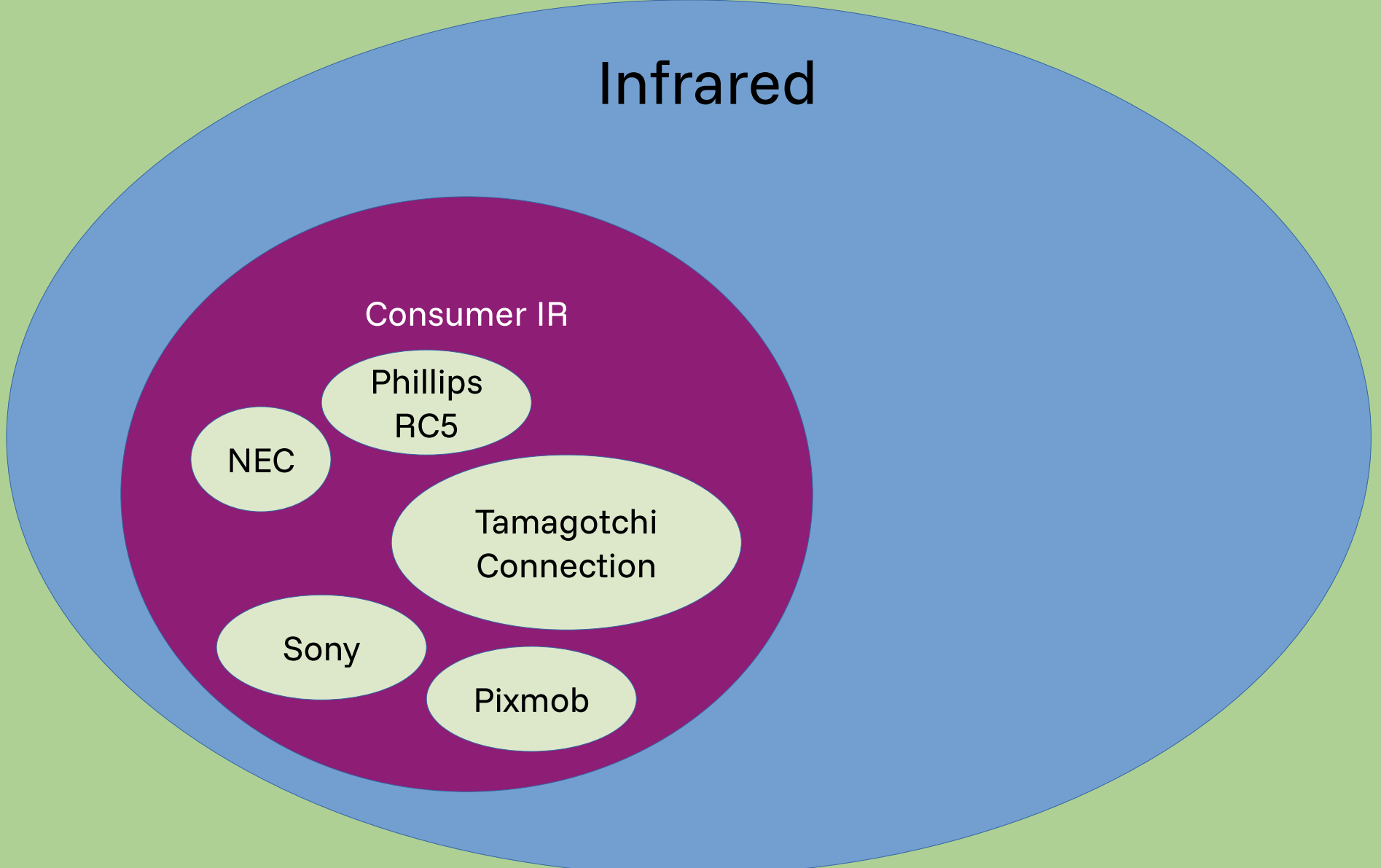




https://www.sbprojects.net/knowledge/ir/index.php

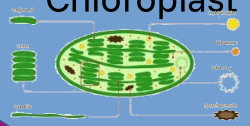

Consumer IR
Phillips
RC5
NEC
Sony
Pixmob


Consumer IR
Phillips
RC5
NEC
Tamagotchi
Connection
Sony
Pixmob


Infrared
Consumer IR
Phillips
RC5
NEC
Tamagotchi
Connection
Sony
Pixmob

Infrared

Chloroplast



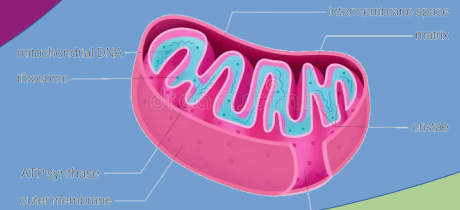
Consumer IR

- Phillips RC5
- NEC
- Tamagotchi Connection
- Sony
- Pixmob

IrDA

- SIR
- FIR
- Tamagotchi iD
- VFIR
- DC32 badge
- Palm OS

Mitochondria

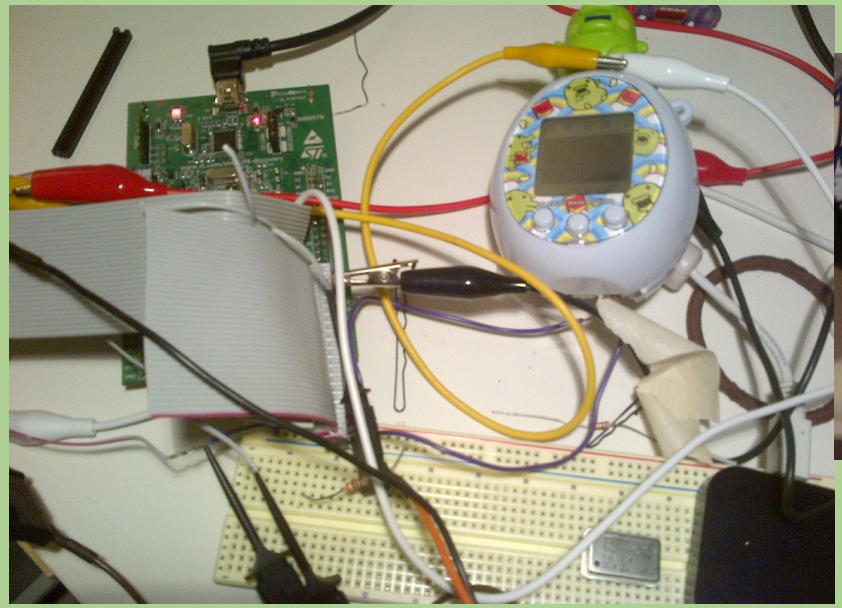


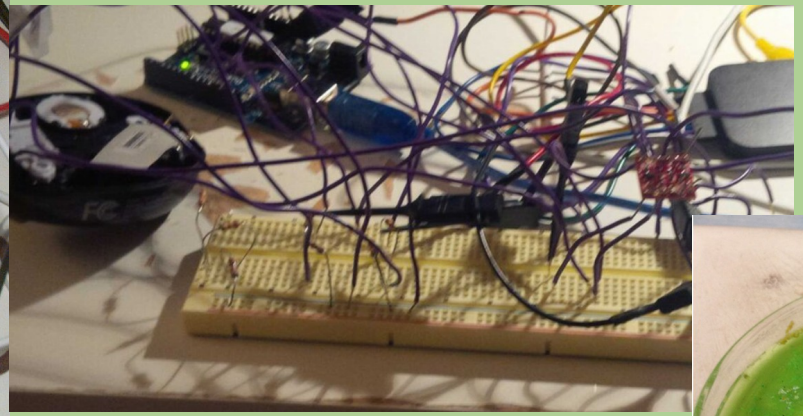
Many Tamagotchis Were Harmed

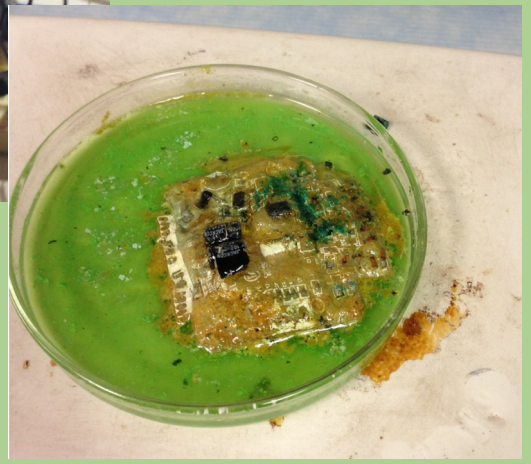
- Natalie Silvanovich gave two awesome talks about Tamagotchis at CCC
- Lots of information about the hardware

https://media.ccc.de/v/29c3-5088-en-many_tamagotchis_were_harmed_in_the_making_of_this_presentation_h264

https://media.ccc.de/v/30C3_-_5279_-_en_-_saal_1_-_201312291715_-_even_more_tamagotchis_were_harmed_in_the_making_of_this_presentation_-_natalie_silvanovich

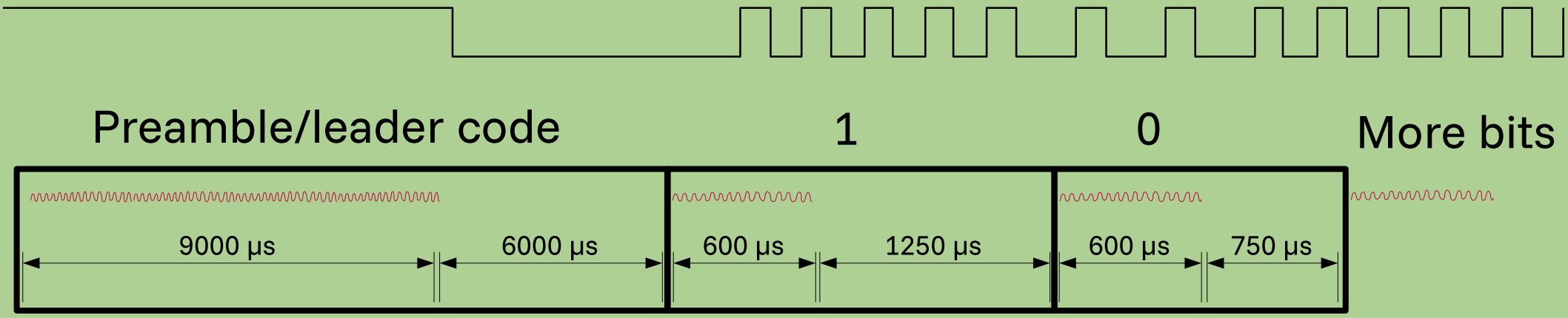


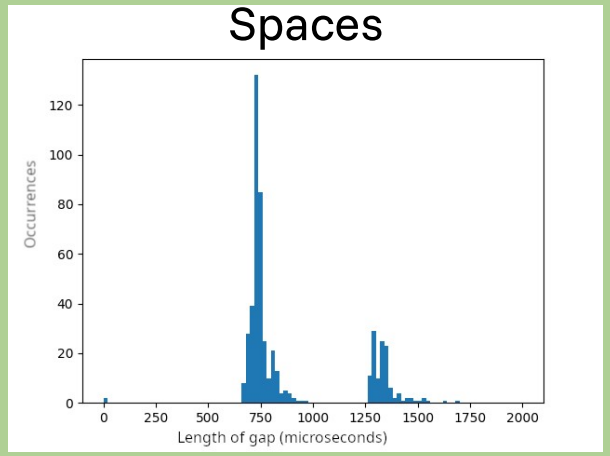


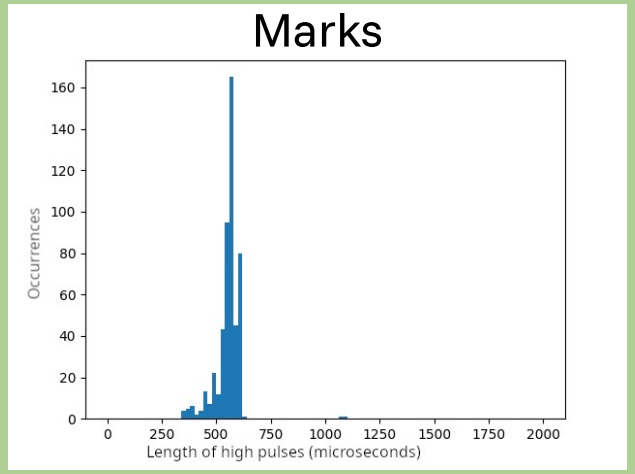


https://github.com/natashenka/Tamagotchi-Hack/blob/master/slides/recon.ppt

Tamagotchi Connection 2024 protocol





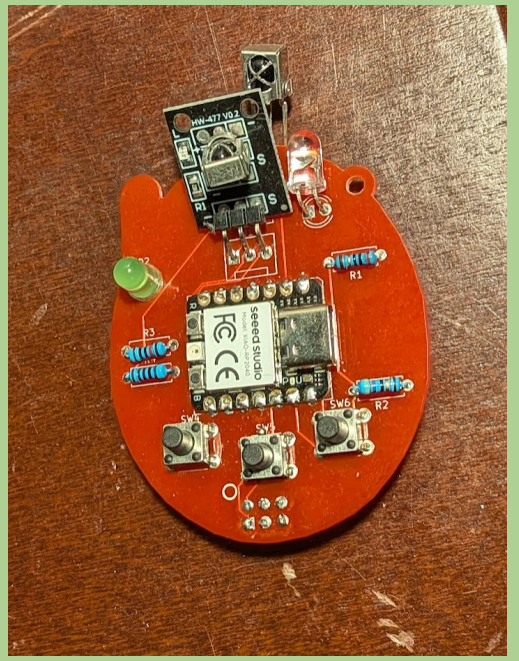


Hardware

- Tried to use the Flipper, it could only reliably get the very first message in a conversation
- Had to build my own thing
- MicroPython to the rescue
- Kinda janky though

SAO

- Dani made an SAO that can play stored recordings!



Flipper app

Now what?

OSI Model

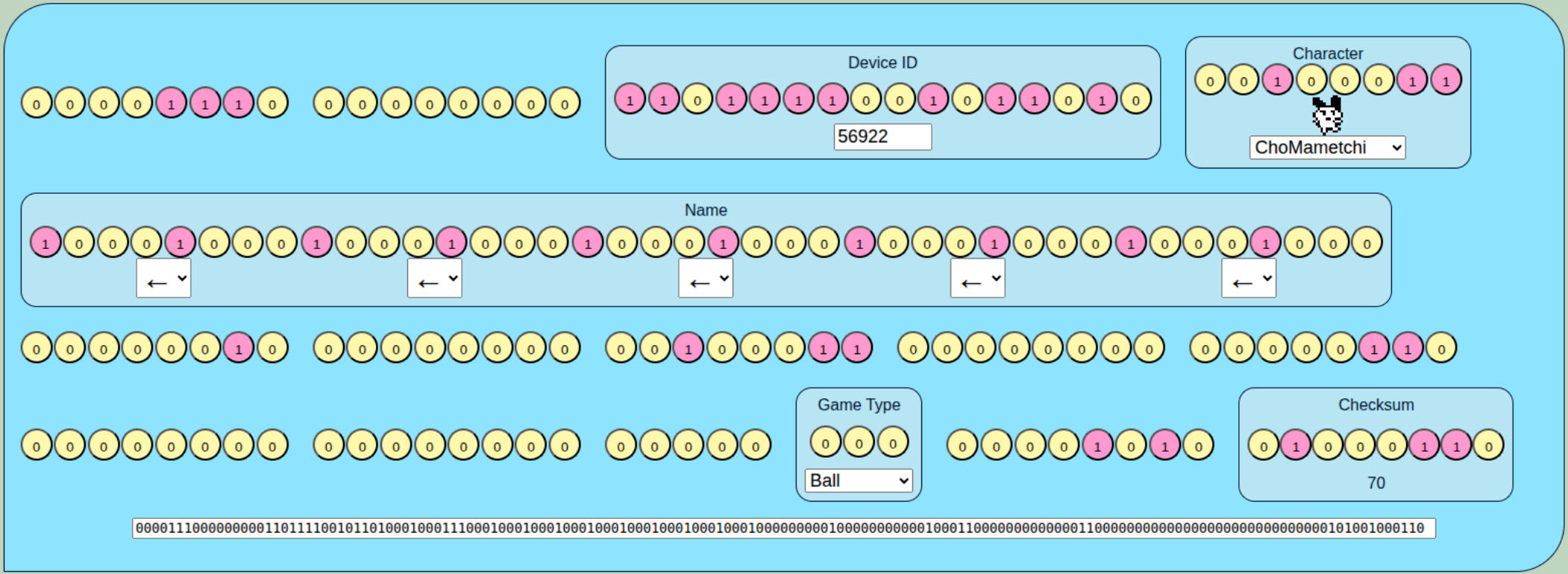
Maybe some distant cousin of the OSI Model

7. Conversation Layer

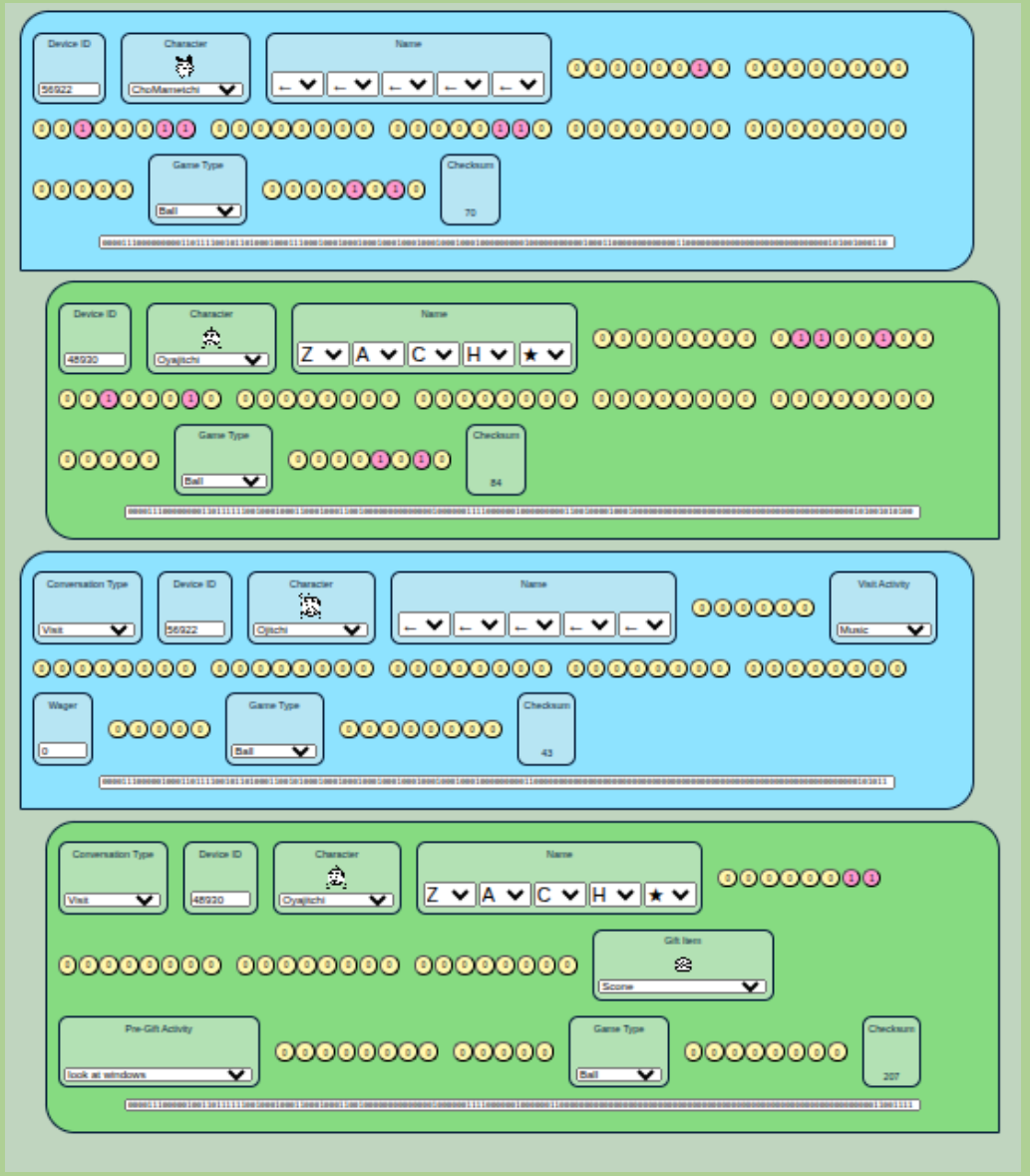
6. Message Layer

1. Physical Layer

Message Layer

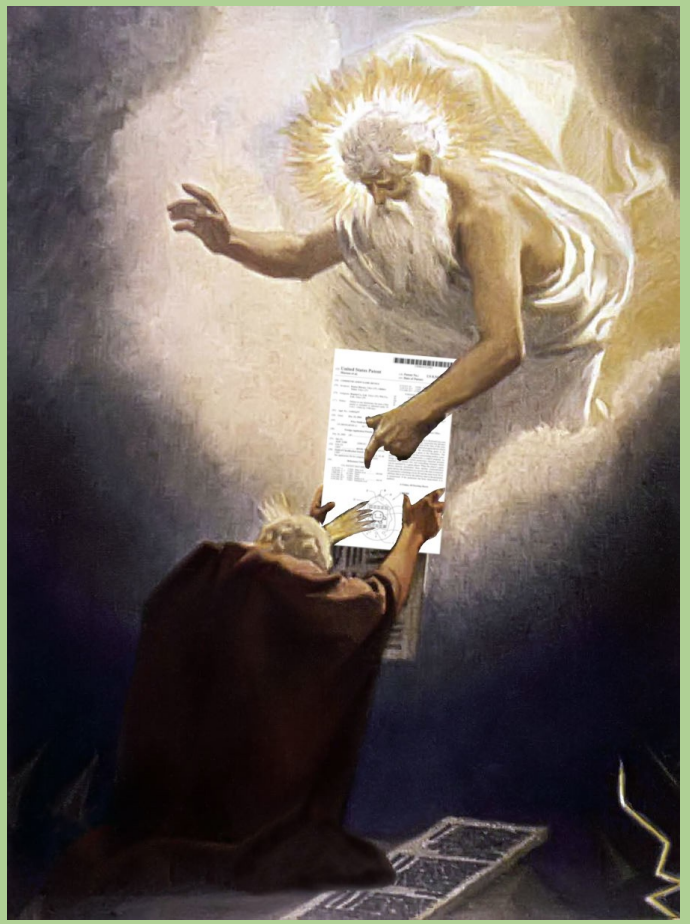


Conversation Layer



US Patent 8,545,324

- “Communication Game Device”
- Lots of information that would have been hard to figure out otherwise



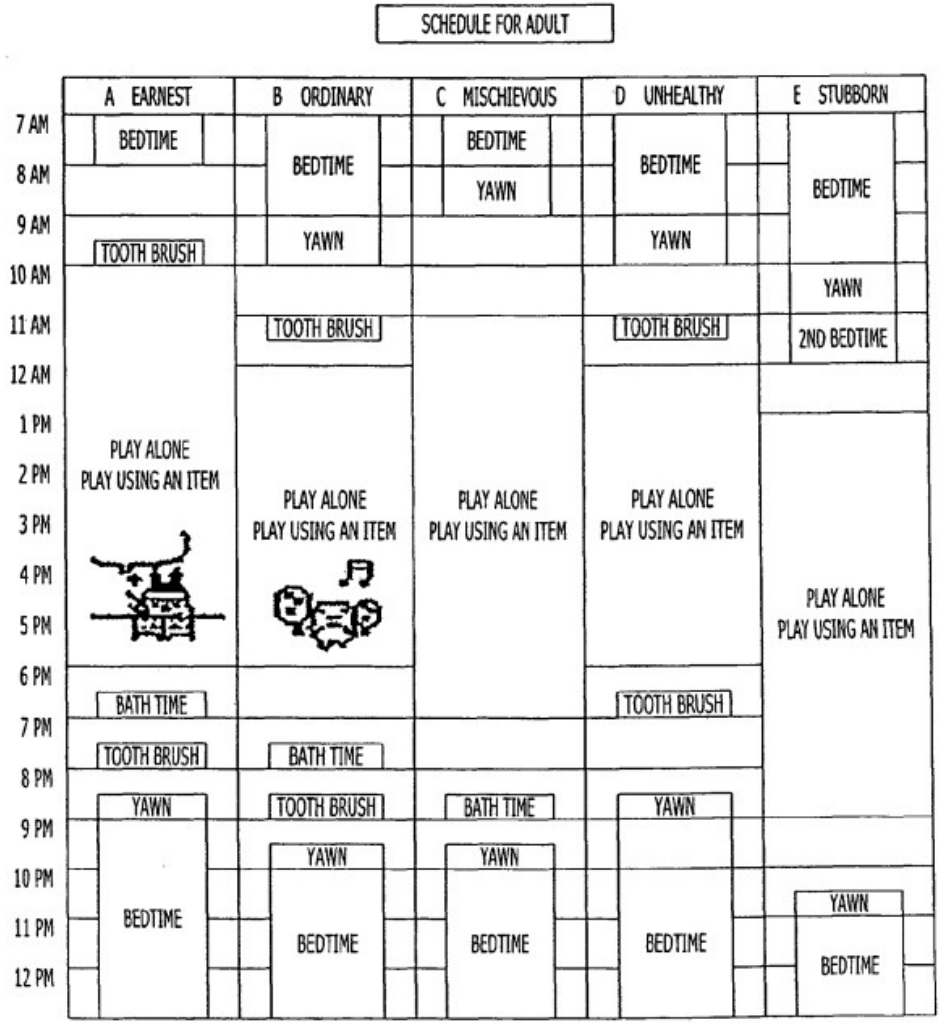

SCHEDULE FOR ADULT
A EARNEST
B ORDINARY
C MISCHIEVOUS
D UNHEALTHY
E STUBBORN
7 AM
8 AM
9 AM
10 AM
11 AM
12 AM
1 PM
2 PM
3 PM
4 PM
5 PM
6 PM
7 PM
8 PM
9 PM
10 PM
11 PM
12 PM
BEDTIME
TOOTH BRUSH
YAWN
2ND BEDTIME
PLAY ALONE
PLAY USING AN ITEM
BATH TIME

FIG. 15

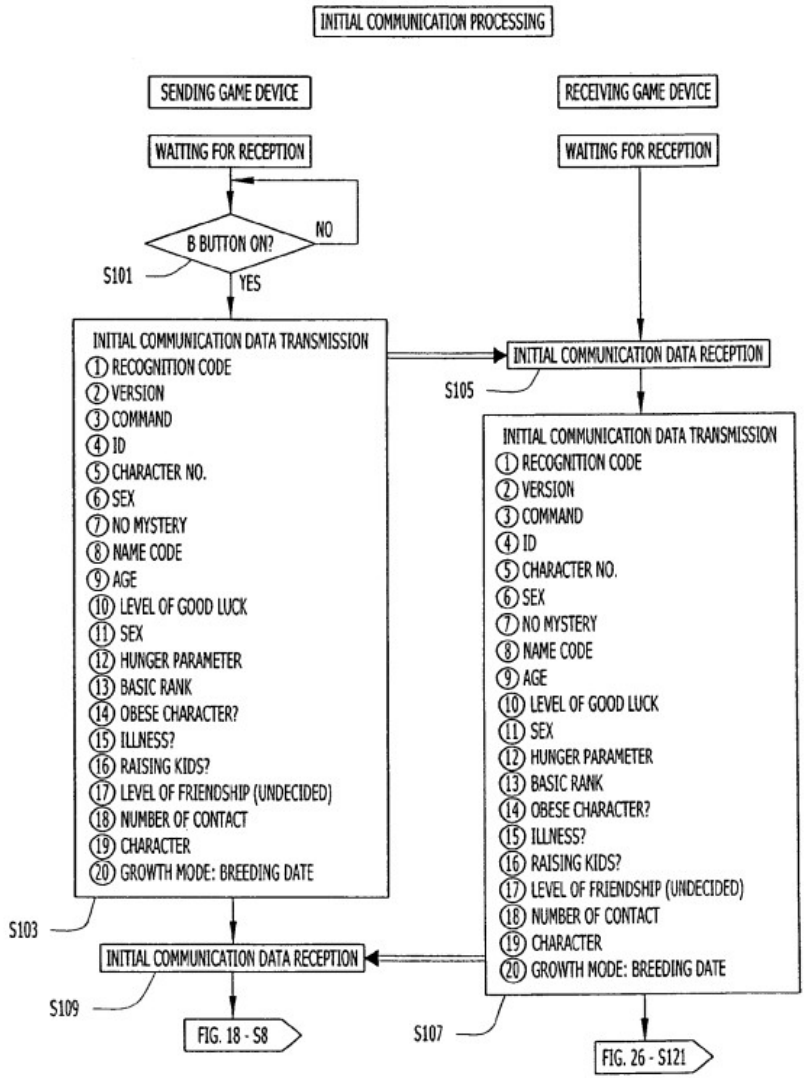

INITIAL COMMUNICATION PROCESSING
SENDING GAME DEVICE
RECEIVING GAME DEVICE
WAITING FOR RECEPTION
WAITING FOR RECEPTION
B BUTTON ON?
NO
YES
S101
INITIAL COMMUNICATION DATA TRANSMISSION
① RECOGNITION CODE
② VERSION
③ COMMAND
④ ID
⑤ CHARACTER NO.
⑥ SEX
⑦ NO MYSTERY
⑧ NAME CODE
⑨ AGE
⑩ LEVEL OF GOOD LUCK
⑪ SEX
⑫ HUNGER PARAMETER
⑬ BASIC RANK
⑭ OBESE CHARACTER?
⑮ ILLNESS?
⑯ RAISING KIDS?
⑰ LEVEL OF FRIENDSHIP (UNDECIDED)
⑱ NUMBER OF CONTACT
⑲ CHARACTER
⑳ GROWTH MODE: BREEDING DATE
INITIAL COMMUNICATION DATA RECEPTION
S105
INITIAL COMMUNICATION DATA TRANSMISSION
① RECOGNITION CODE
② VERSION
③ COMMAND
④ ID
⑤ CHARACTER NO.
⑥ SEX
⑦ NO MYSTERY
⑧ NAME CODE
⑨ AGE
⑩ LEVEL OF GOOD LUCK
⑪ SEX
⑫ HUNGER PARAMETER
⑬ BASIC RANK
⑭ OBESE CHARACTER?
⑮ ILLNESS?
⑯ RAISING KIDS?
⑰ LEVEL OF FRIENDSHIP (UNDECIDED)
⑱ NUMBER OF CONTACT
⑲ CHARACTER
⑳ GROWTH MODE: BREEDING DATE
S103
INITIAL COMMUNICATION DATA RECEPTION
S109
FIG. 18 - S8
S107
FIG. 26 - S121

FIG. 25

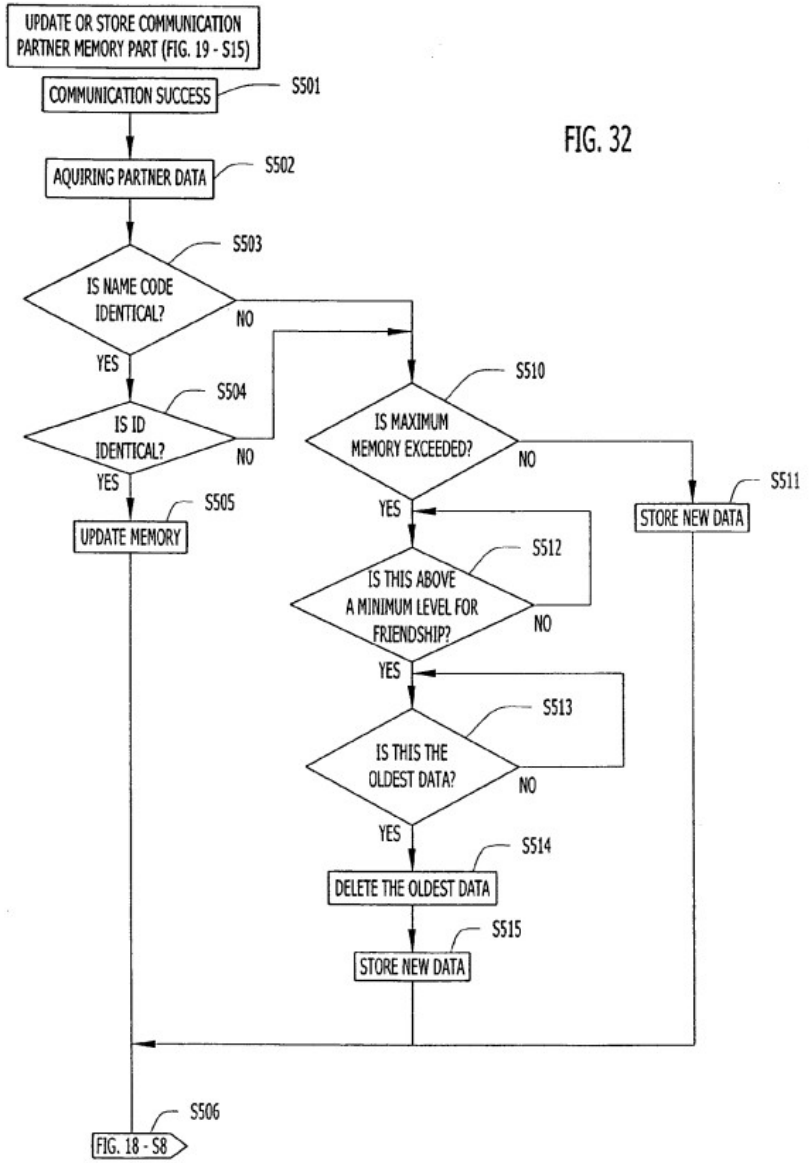


FIG. 32

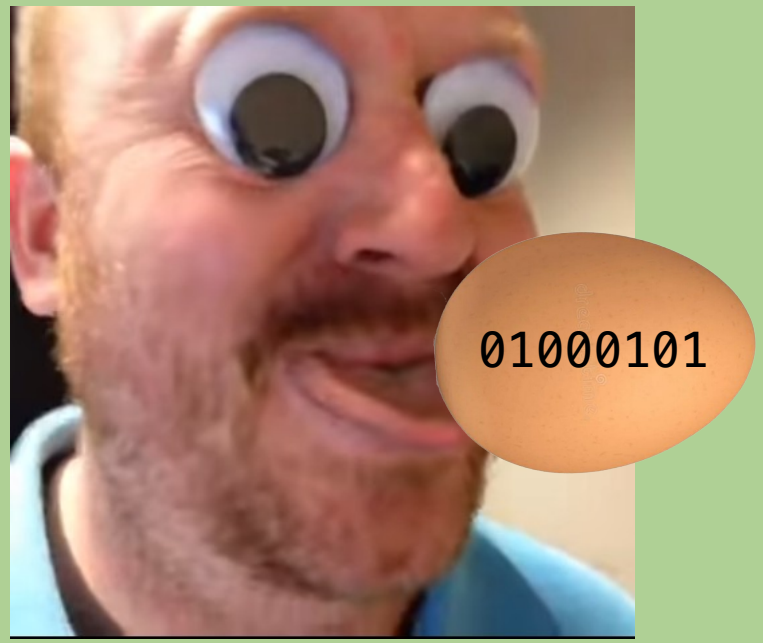
BYTE	BIT			
1	0	0	RECOGNITION CODE	(00)
	1	0		
	2	1		
	3	1		
	4	0	VERSION	VER. BIT 0 (01)
	5	0		VER. BIT 1
	6	0		VER. BIT 2
	7	0		VER. BIT 3
2	0		COMMAND	(02)
	1			
	2			
	3			
	4			(03)
	5			
	6			
	7			
3	0		ID	ID BIT0 (04)
	1			ID BIT1
	2			ID BIT2
	3			ID BIT3
	4			ID BIT4 (05)
	5			ID BIT5
	6		VERSION	VER. BIT4
	7			VER. BIT5
4	0		CHARACTER NO.	(06)
	1			
	2			
	3			
	4			(07)
	5			
	6		SEX	0 = MALE 1 = FEMALE
	7		NO MYSTERY	MYSTERY = 0 NO MYSTERY = 1
5	0		NAME 1	(08)
	1			
	2			
	3			
	4			(09)
	5			
	6			
	7			

FIG. 36A

ADDRESS		0	1	2	3	4	5	6	7
000	NAME	ID	DATE OF BIRTH(DAY)	DATE OF BIRTH(MONTH)	NAME 1	NAME 2	NAME 3	NAME 4	NAME 5
	0								
	1								
	2								
	3								
	4								
	5								
	6								
	7								
010	NAME	CURRENT MINUTES	CURRENT HOUR	PARAMETER 1	PARAMETER 2	PARAMETER 3	PARAMETER 4	INFORMATION 2	INFORMATION 3
	0			DISCIPLINE	GOOD MOOD	CARE MISTAKE	MENTAL UNDERDEVELOPMENT	ILLNESS	NUMBER OF DAYS OF BREEDING
	1							SERIOUS ILLNESS	
	2							SLEEP	
	3							DEATH	
	4			SNACKS	HUNGER	PHYSICAL UNDERDEVELOPMENT	LEVEL OF GOOD LUCK	DAYS OF RAISING KIDS	REBELLIOUS AGE CHANGES
	5								
	6								
	7								

FIG. 35A

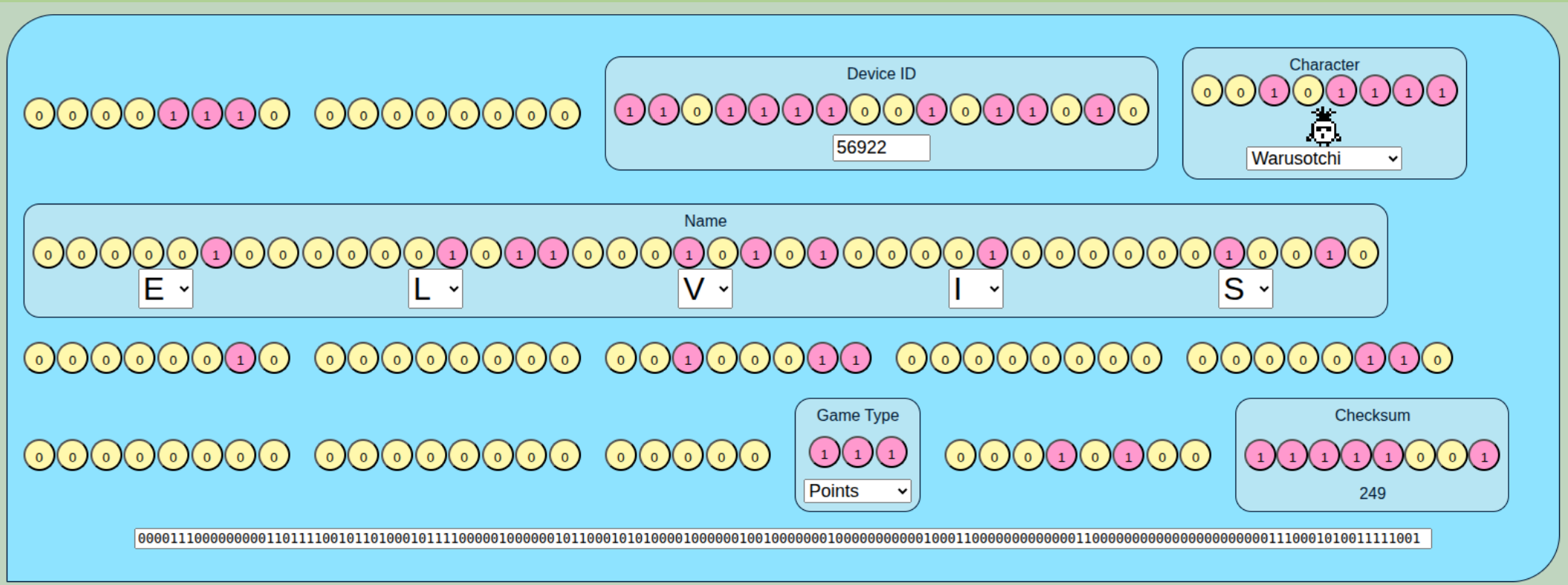
A brief mention of Endian-ness



Big Endian

Little Endian

Message Format



Tamagometer

- “Tamagometre” for any Europeans
- Record a Tamagotchi
- Edit and replay the conversation

Tamagometer

- Github pages
- Vue
- Web Serial

Tamagometer

- Github pages 🙅  💸 🍺
- Vue
- Web Serial

Tamagometer

- Github pages 🙅  💸 🍺
- Vue ☠️ 🐌
- Web Serial

Tamagometer

- Github pages 🤦 🪟 💸 🍺
- Vue ☠️ 🐌
- Web Serial
  - Chrome only 🤮

Discoveries

Infinite money!

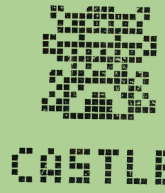
- The amount of money in the points game is 17th byte of 3rd message
- If the last bit before the checksum in 3rd message is 0, that player loses

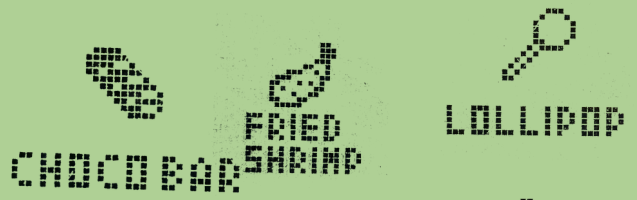
Free items!

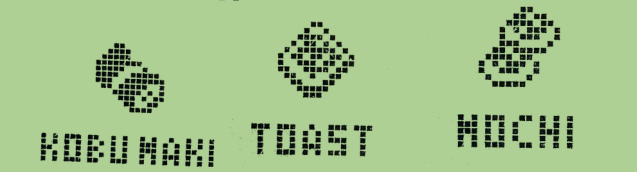
- Any item from the shop can also be sent as a gift
- Gift item is 15^{th} byte of 4^{th} message

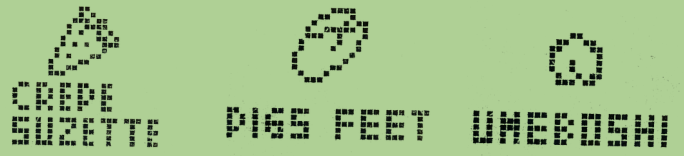
Secret items!

- Some Japanese food
- Other random foods
- Castle









Non-items stored nearby in memory (?)

- Souvenirs
  - Don’t save in inventory
- Other weird stuff

How to change a Tamagotchi’s gender

How to asexually reproduce

- Haven’t studied thoroughly
- Have successfully swapped the gender and make a baby tamagotchi with yourself