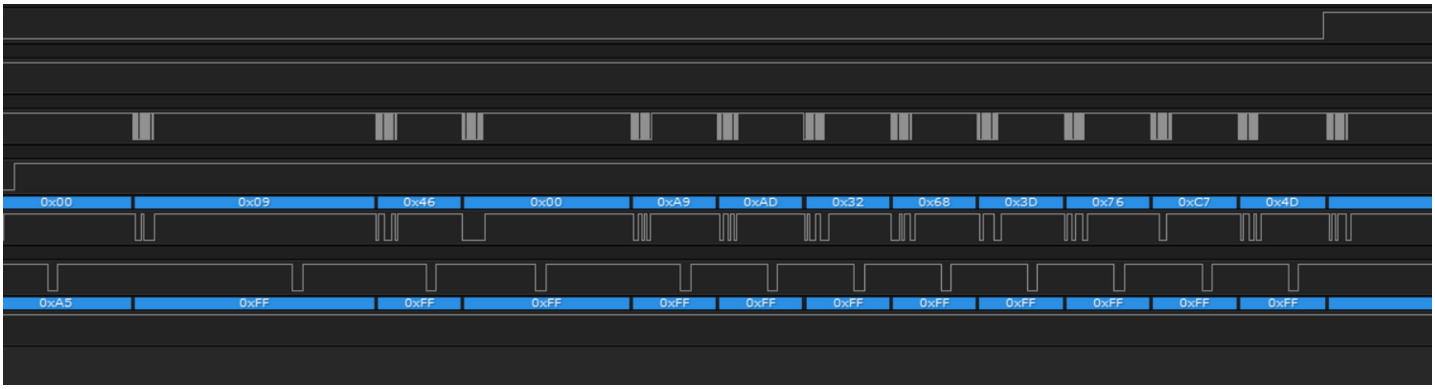
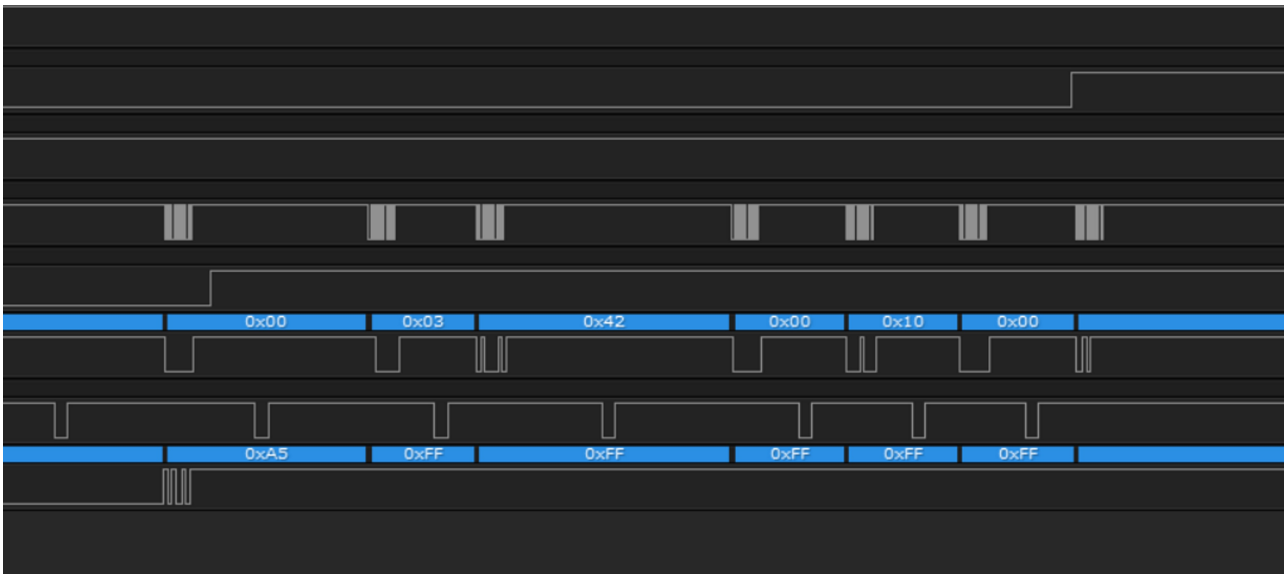
Decoding

March 15, 2019 7:53 PM

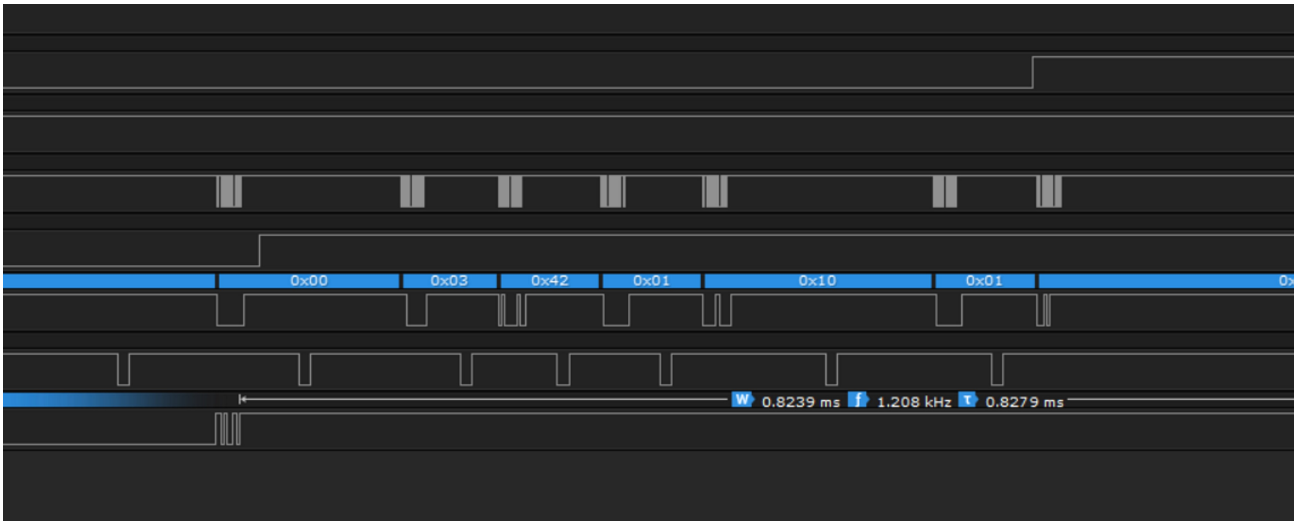


Network Key 0 this is the private Shimano key
A9-AD-32-68-3D-76-C7-4D
A9ad32683d76c74d

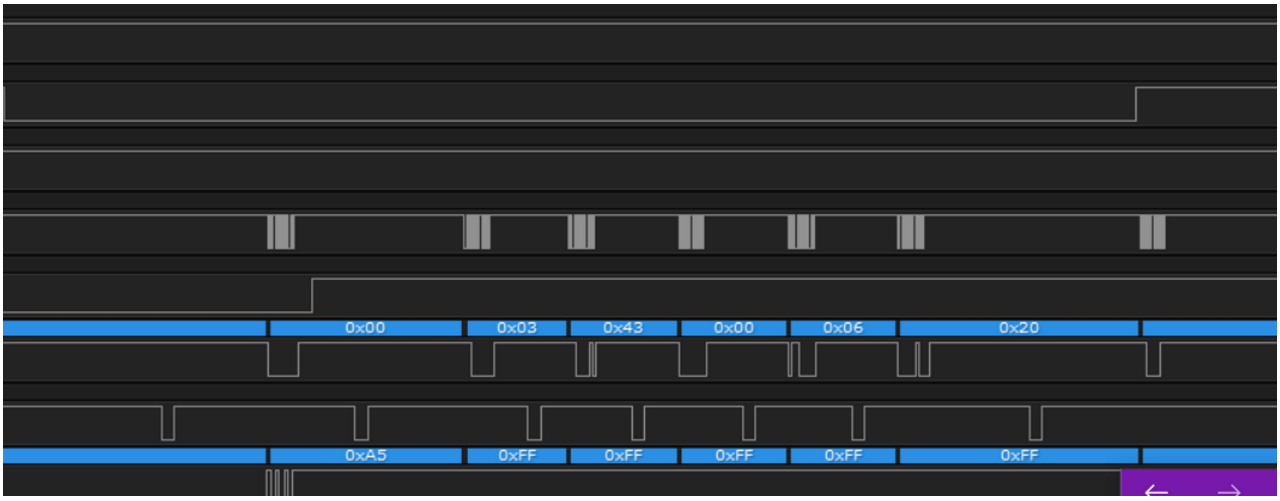
Network Key 1, this is the ANT+ key



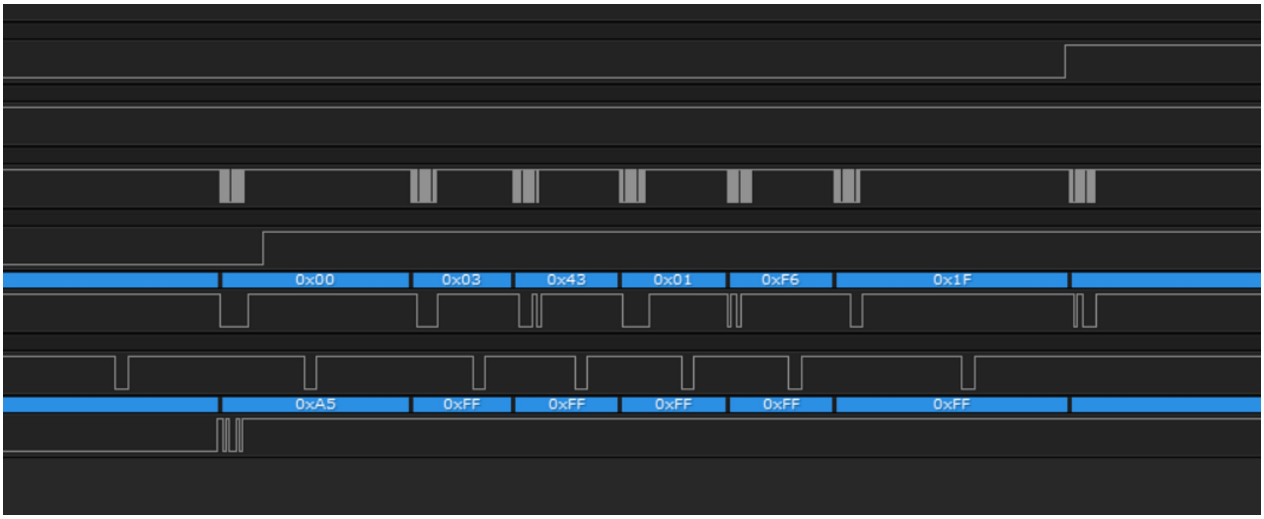
Message 42 - Assign Channel 0
Network 0
TX only
No options set for Extended assignment



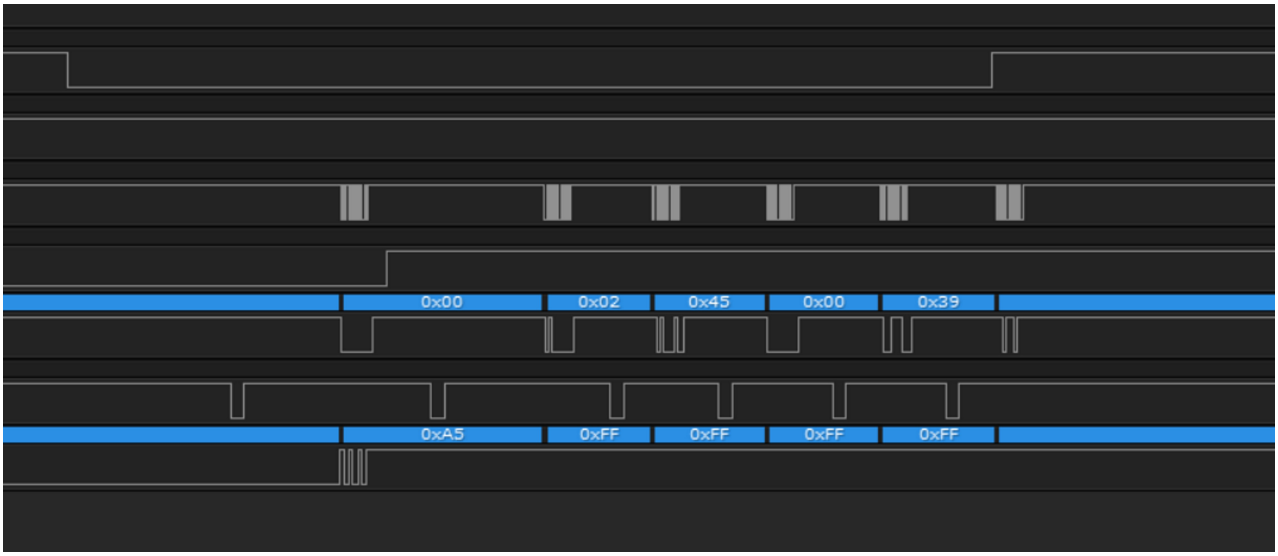
Message 42 - Assign Channel 1
Network 1
TX only
Background scanning enabled



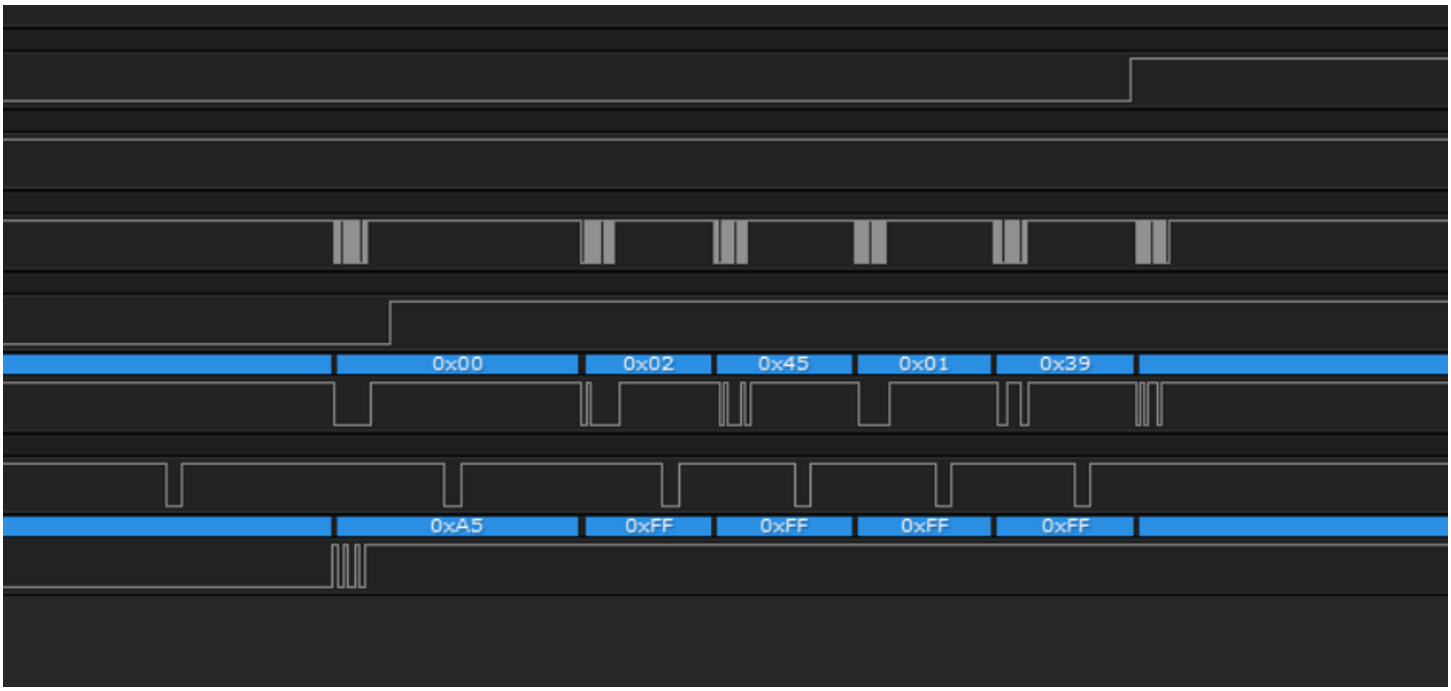
Message 43 - Set Channel 0 Messaging Period
Period 8198



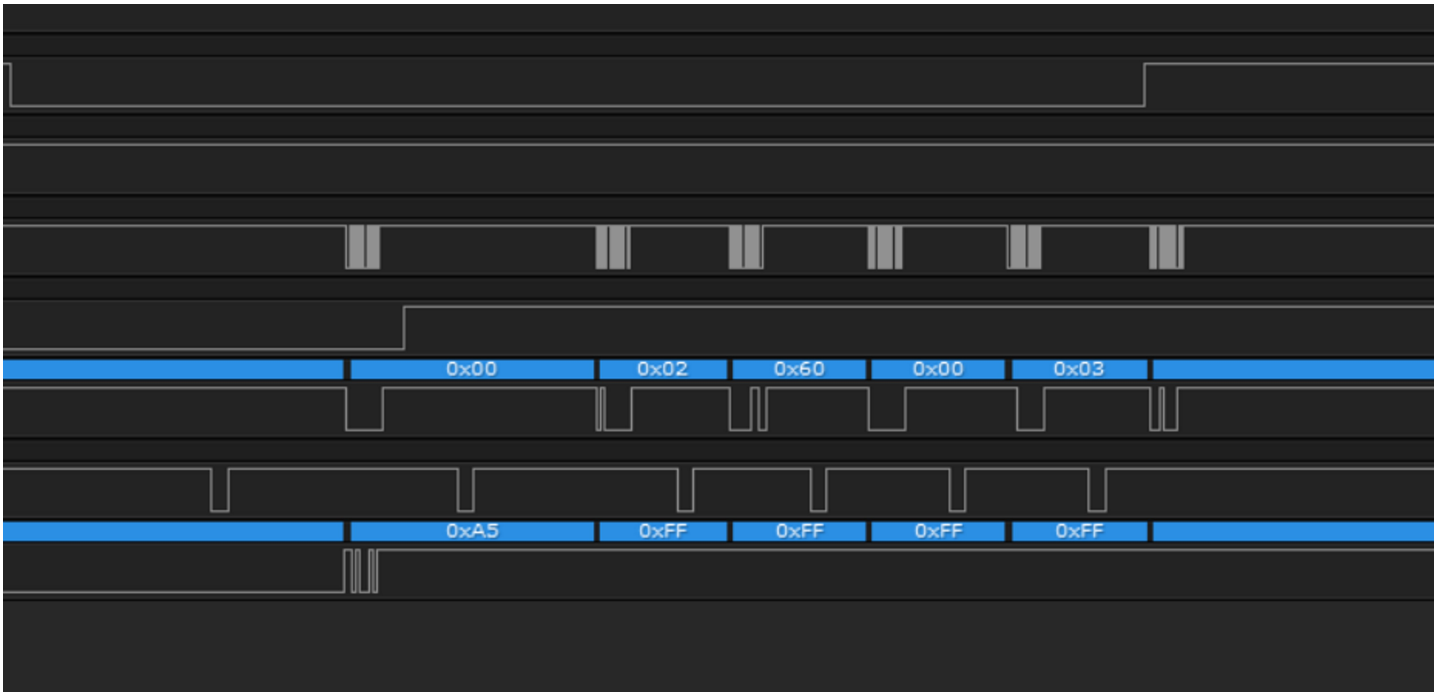
Message 43 - Set channel 1 messaging period
Period 8182



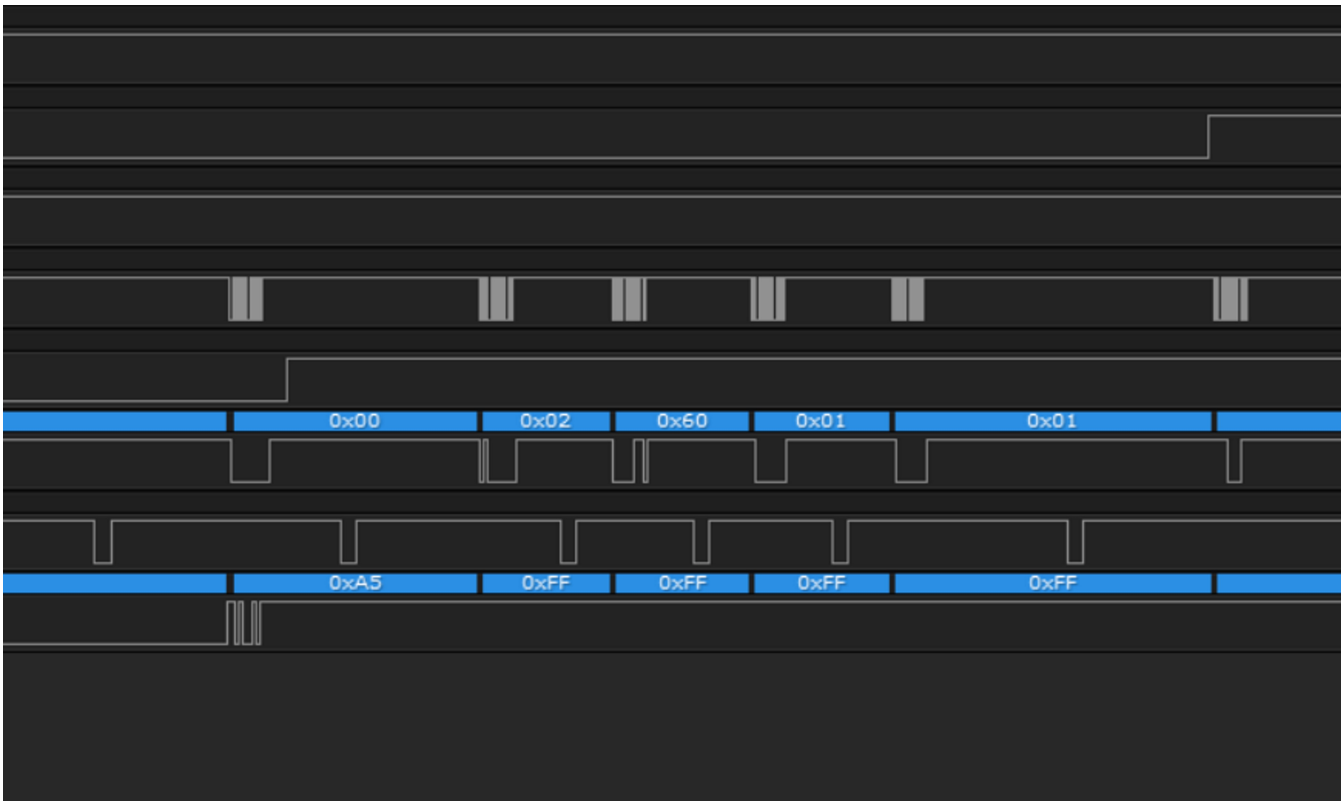
Message 45 - Set RF Frequency for channel 0
Frequency 0x39 or 57
Wait a minute, that is the frequency reserved for ANT+



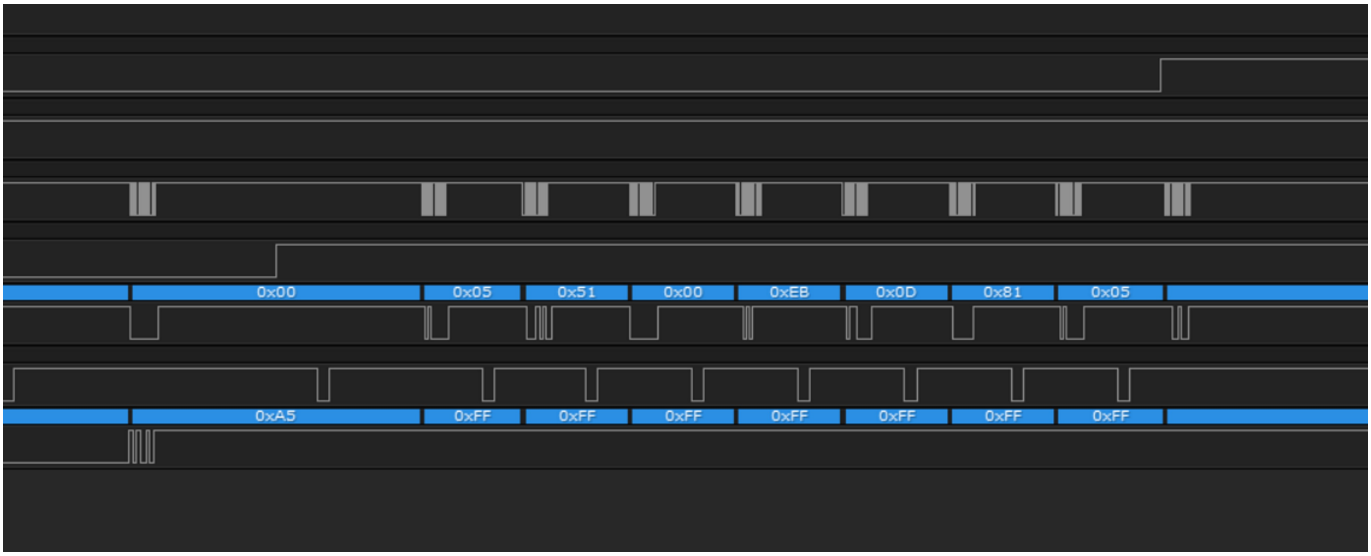
Message 45 - Set RF Frequency for Channel 1
Frequency is 0x39 or 57, but this one is using the network key for ANT+



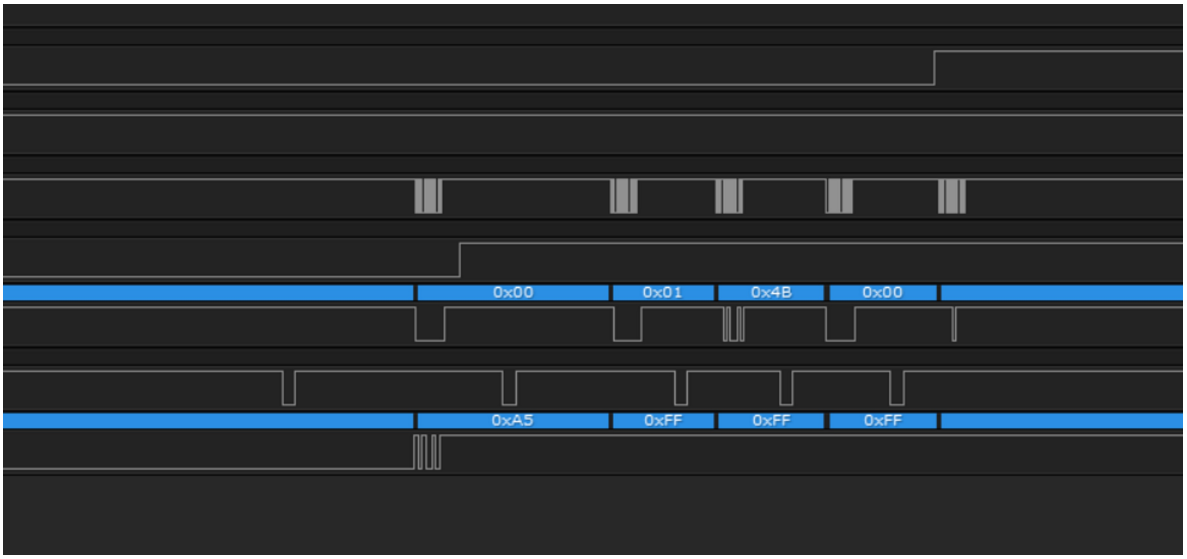
Message 60 - Set TX power channel 0 to 0dbm



Message 60 - Set TX power channel 1 to -12dbm?



Message 51
Set Channel ID of channel 0 to 0x0DEB or 3563, Device type 1 with pairing request to 1
Device type id 1
Transmission type 5



Open channel 0

Summary

Network Key: A9-AD-32-68-3D-76-C7-4D / A9ad32683d76c74d
Period 8198
Frequency 57
Device type 1
Transmission type 5

Pages

March 16, 2019 11:20 AM

Page 00
Looks like it contains the gear and the button status and battery. It struggles to fill them in and sometimes hammers the heck out of the transceiver even though it got confirmation that it was written.

[00]	[F7]	[02]	[09]	[64]	[00]	[FF]
[page]	[buttons]	[front ring]	[rear]	[?]	[?]	[?]
				Battery percent Confirmed battery Even 101% and More works		

The F7 seems to change with buttons but still needs work to reverse engineer.

Battery 100%
software version says 0.10
manufacture number says 41
model says 29241
serial says 3290598177
gears say 53-39 and 11-23

Standard ANT+ pages
Manufacturer ID page seems there

[50]	[FF]	[FF]	[01]	[29]	[00]	[39]	[72]	[D0]
page	reserved	reserved	HW rev	Mfg id lsb	Mfg id msb	Model num lsb	Model num msb	

Checks out for mfg id and model number. HW rev is just 1 I guess?

Common Data page 81, See ant docs

[51]	[FF]	[FF]	[01]	[21]	[8B]	[22]	[C4]	[FF]
page	reserved	Sw revision sup	Sw revision main	Serial lsb	Serial byte 1	Serial byte 2	Serial msb	

$W\ Revision = Main\ SW\ Revision \times 100 + Supplimental\ SW\ Revision 1000$
serial says 3290598177 so this checks out and version is .1

NO command data page 82…..

Need to setup gear page, won't show until this is sent

11	03	02	0B	FF	FF	FF	FF
page	???	Max gear front	Max back				

Transmitted with 0x4f acknowledged message. Unsure what the 03 is.

This is sent with a 4F meaning requires acknowledgement page. The page 4 only has two meaningful bytes after page. The first nibble is the type of press, and the second is the count with a roll over of 15. When you press you get an incremented count along with the code. These have to be sent until acknowledged. All acks are just 8f-FF-FF-FF-FF-FF-FF-FF it seems (except that one time byte 3 was like 81)

04	Right	Right	Left	Left	FF	FF	FF	FF	FF
page	MSB 1	LSB 1	MSB 2	LSB 2					
	1 = press	Count	1 = 1 pres s	Count					
	2 = long	1-F	2 = 2 long	1-F					
	4 = double		4 = double						
	0 = 0 release, used for long only		0 = 0 release, only used for long						
	F = Null		F=Null						

Sequence

March 17, 2019 11:30 AM

Setup

Hammers the shit out of the chip with

Type	0	FF	FF	FF	FF	00	FF	FF
0x4E	page	Button?	F gear	R gear	Battery %			

Then starts hammering this

Type	0	FF	FF	FF	64	00	FF	FF
0x4E	page	Button?	F gear	R gear	Battery %			

Then starts hammering this

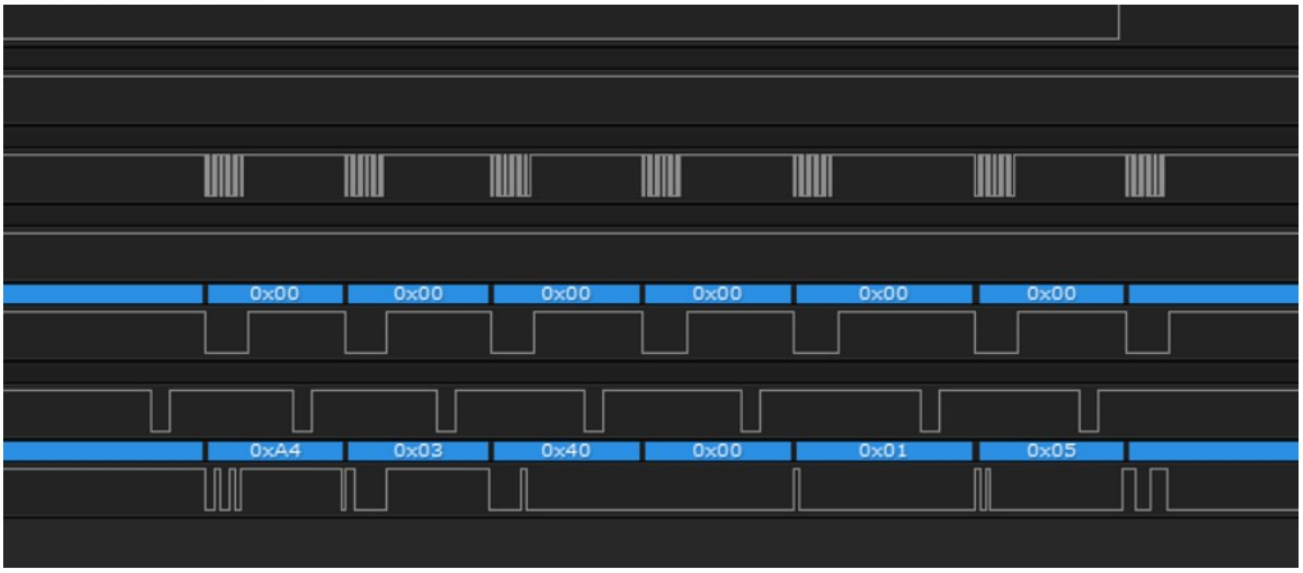
Type	00	FF	01	09	64	00	FF	FF
0x4E	page	Button?	F gear	R gear	Battery %			

0th transmission

Then after like 50ms it stops fucking hammering when it sets something for what I believe is the button field

Type	01	02	1F	01	00	00	00	FF
0x4F	page							

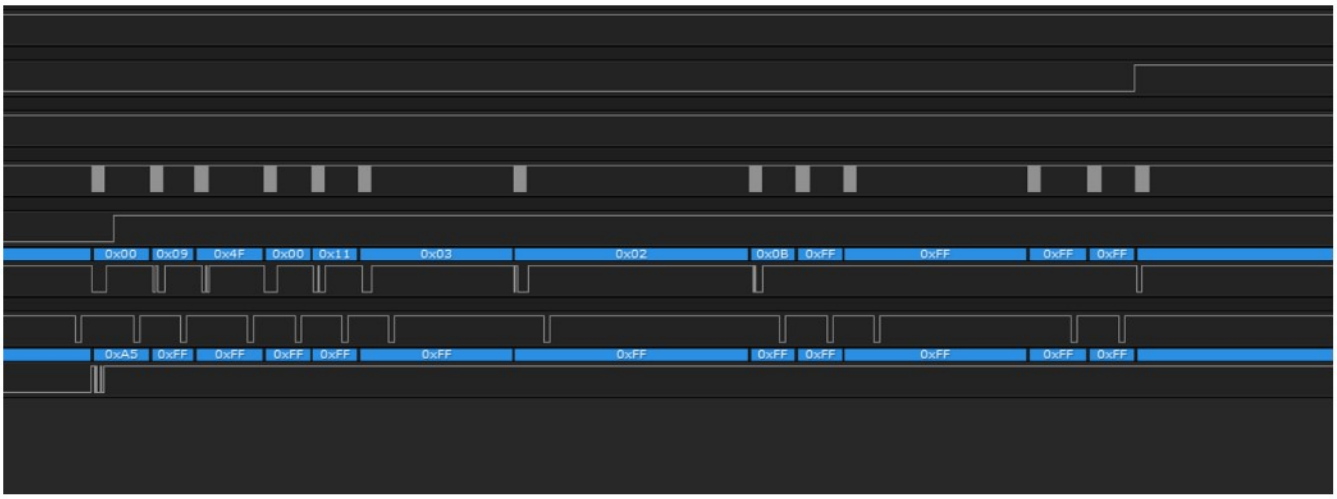
Wait a bit and then this



0x40 is channel message, the 0x00 is channel 0 so our private ANT, ~~but 0x01 is EVENT_RX_SEARCH_TIMEOUT, and that makes no sense~~
0x01 for Message ID is just an RF event, The code is the last byte so it's a normal EVENT_TRANSFER_TX_COMPLETED. We can ignore these

1st transmission

Now we set a new page to tell the cycle computer how many gears we have

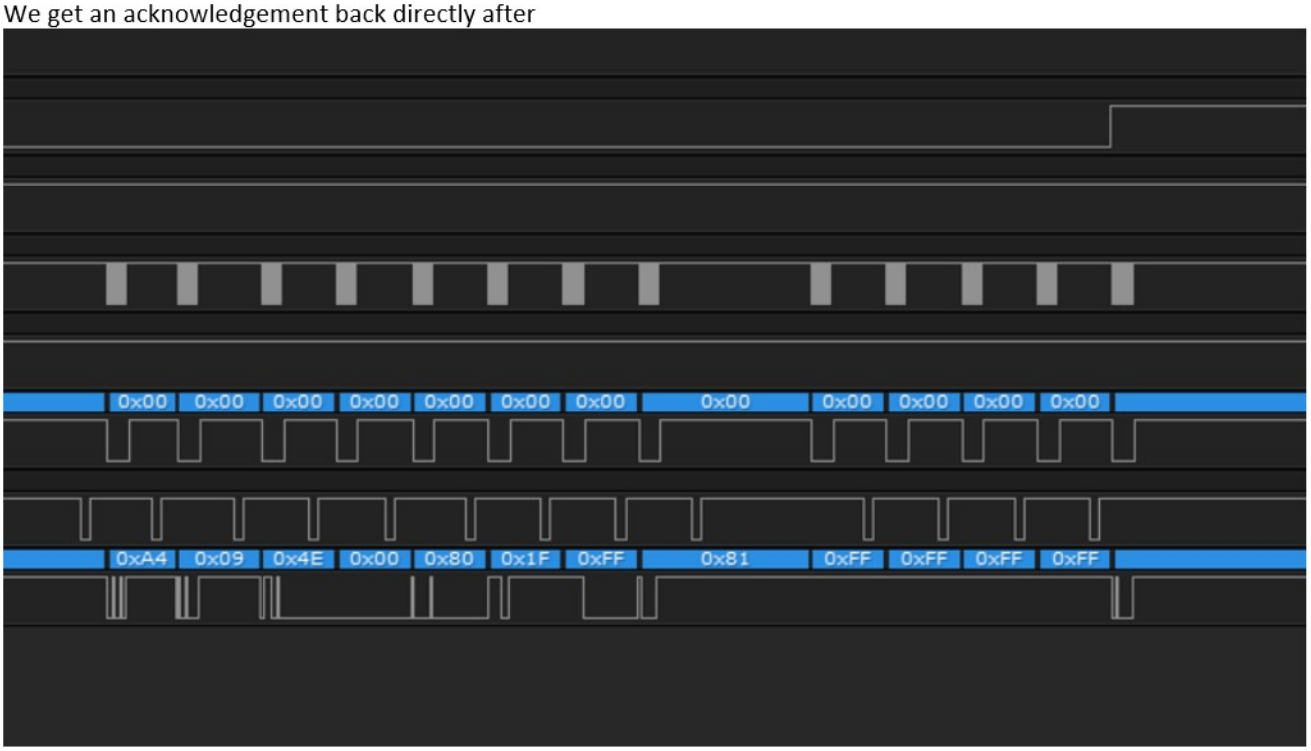


Need to setup gear page

Type	11	03	02	0B	FF	FF	FF	FF
0x4F	page	???	Max gear front	Max back				

Transmitted with 0x4f acknowledged message

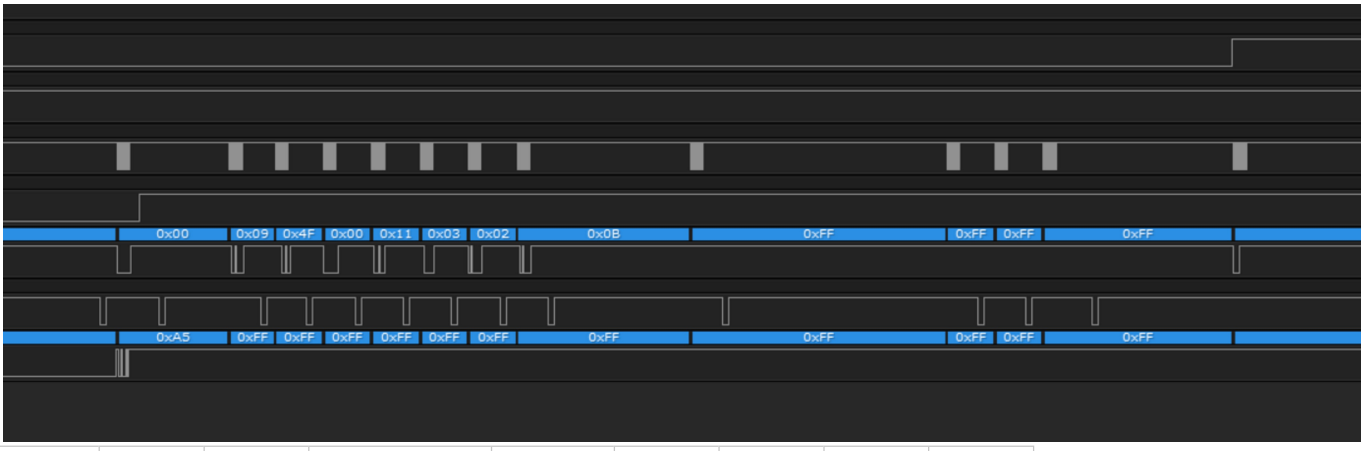
We get an acknowledgement back directly after



Type	80	1F	FF	81	FF	FF	FF	FF
0x4E	page							

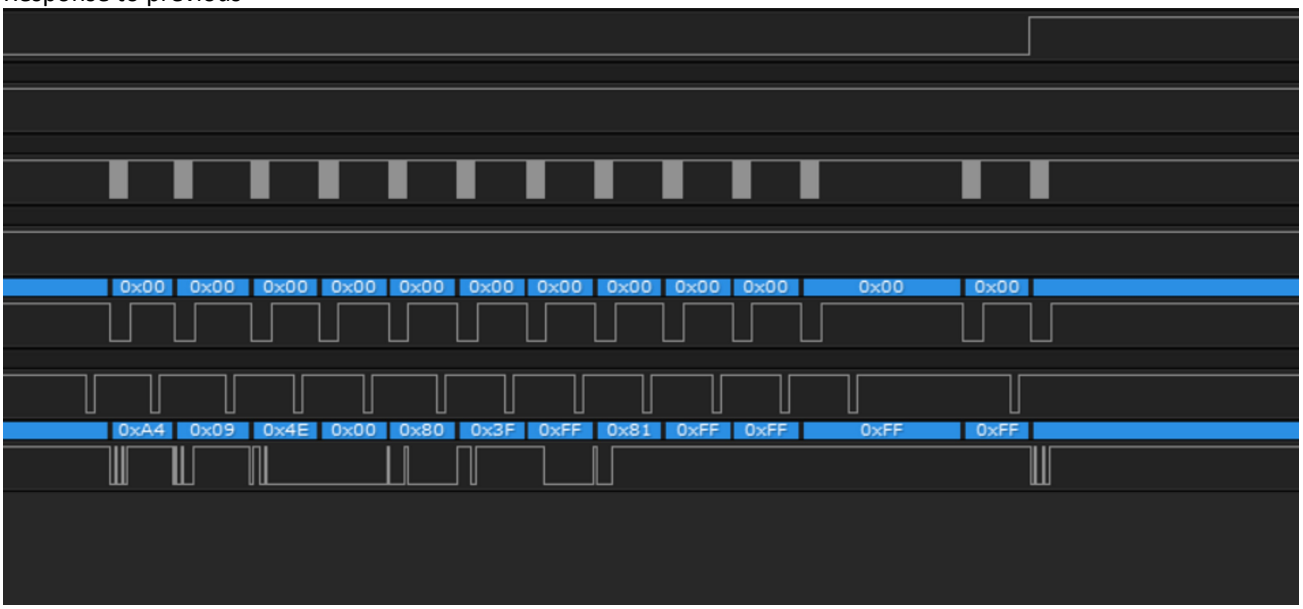
2nd Transmission

2nd ack req page for the gear setup page.



Type	11	03	02	0B	FF	FF	FF	FF
0x4F	page	???	Max gear front	Max back				

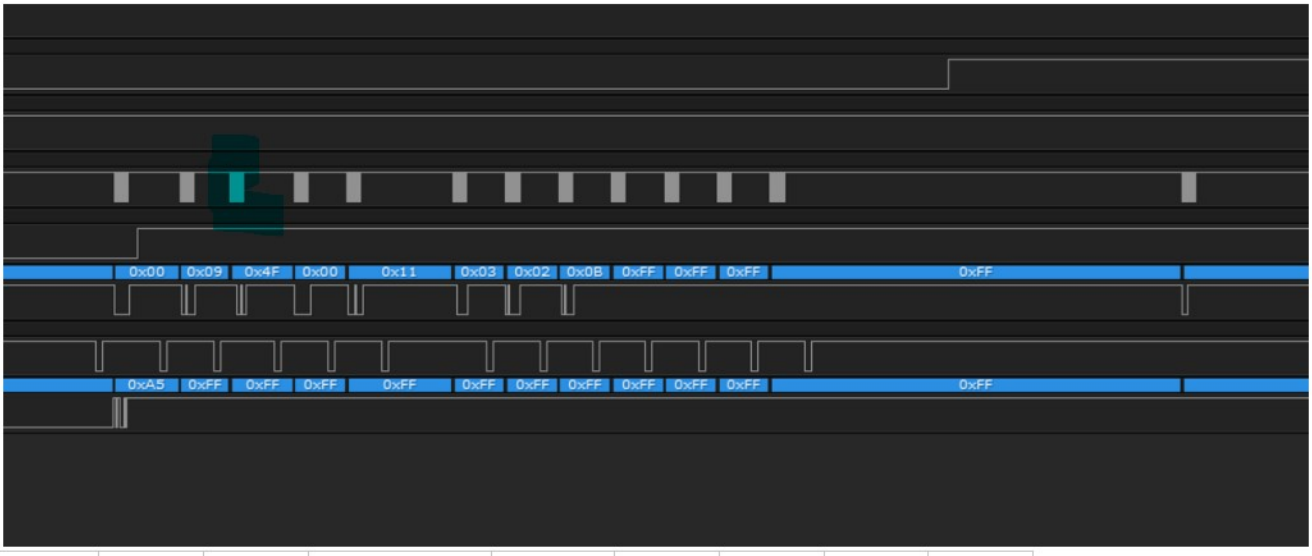
Response to previous



Type	80	3F	FF	81	FF	FF	FF	FF
0x4E	page							

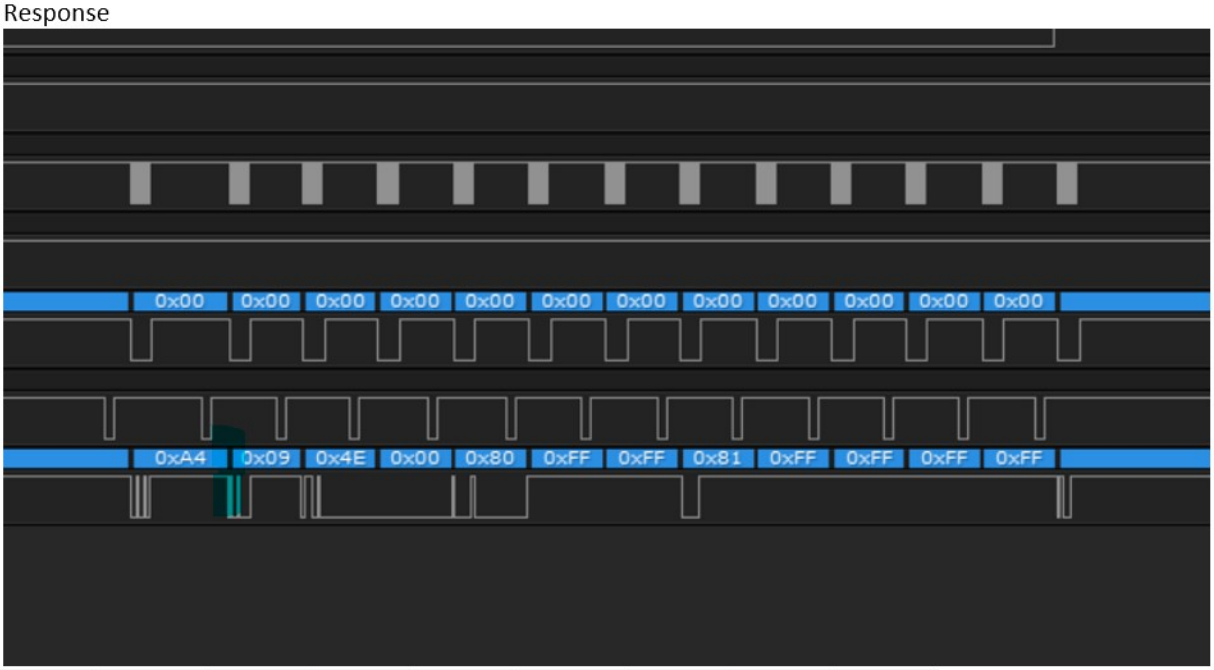
3rd transmission

Channel RF event (no image, skipped)



Type	11	03	02	0B	FF	FF	FF	FF
0x4F	page	???	Max gear front	Max back				

Response



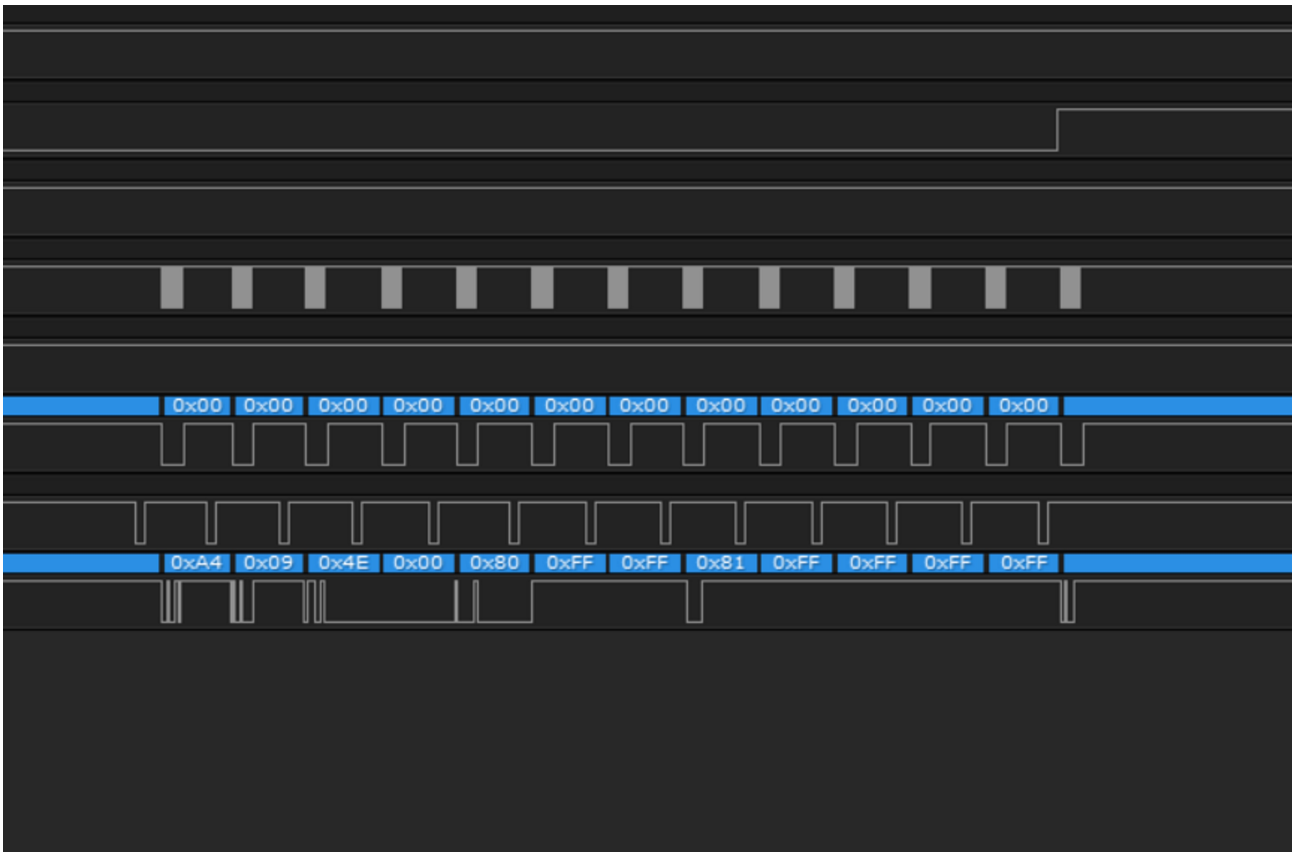
Type	80	FF	FF	81	FF	FF	FF	FF
0x4E	page	??						

Byte 1 keeps changing, 1F, 3F, now FF. It's not going up with respect to the event number

4th transmission

This is a new page, page 1? Unknown, not an ANT+ one

Type	01	02	1F	01	00	00	FF	FF
0x4F	page							



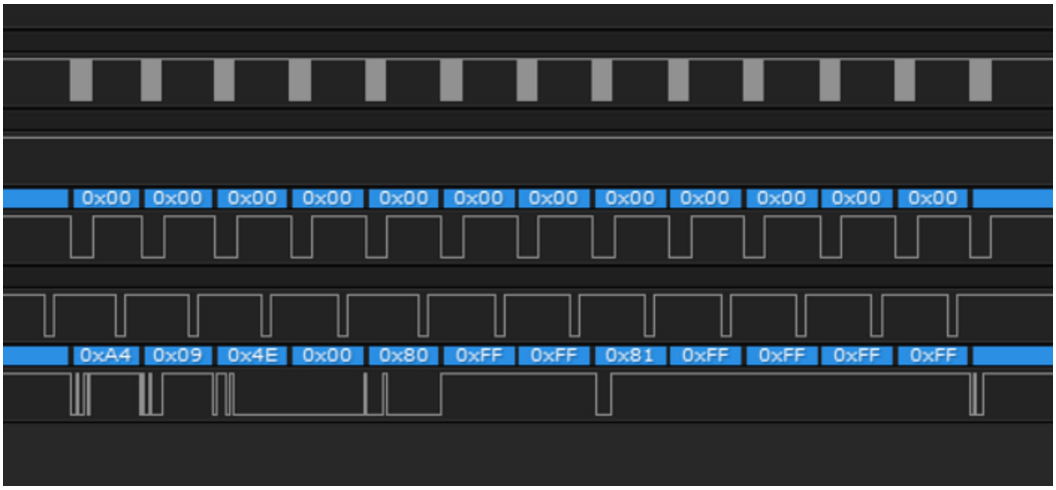
Response page looks the same?

Type	80	FF	FF	81	FF	FF	FF	FF
0x4E	page							

5 Transmission

RF success

Type	00	03	FF	FF	FF	FF	FF	FF
0x4F	page	Button?	Gear F	Gear R	Battery			



Response page looks the same?

Type	80	FF	FF	81	FF	FF	FF	FF
0x4E	page							

Talking points

March 17, 2019 10:56 AM

Shimano sets up two channels
One Private ant and one a degraded Tx -12db ANT+
Shimano uses the ANT+ frequency of 2457mhz which ANT is like NO, only ANT+