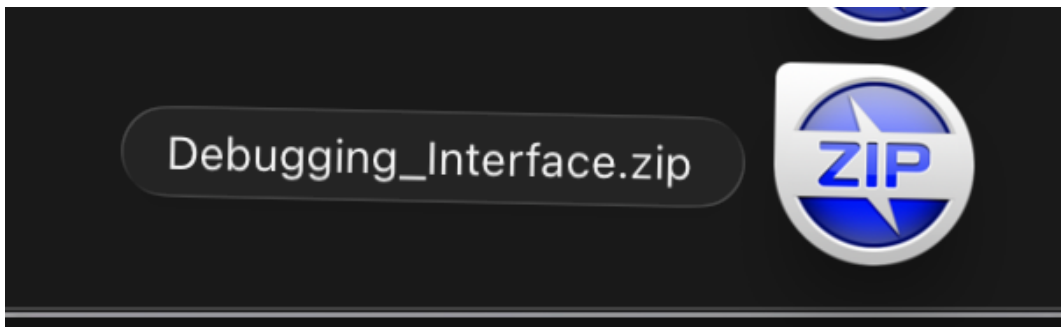


[HackTheBox] Hardware Hacking - Debugging Interface

The screenshot shows the 'Debugging Interface' challenge page on HackTheBox. At the top, there's a 'Back' button. The challenge title 'Debugging Interface' is followed by 'Very Easy' difficulty, a 4.8 star rating from 715 users, 10 points, and a bar chart for 'User-Rated Difficulty'. Below this is a navigation bar with 'Play Challenge' (active), 'Challenge Info', 'Reviews', 'Activity', and 'Changelog'. The 'Challenge Scenario' section describes the task: decoding messages from an asynchronous serial debugging interface. A file 'Debugging_Interface.zip' (10 KB) is available for download. The 'Submit challenge Flag' section contains a text input with 'HTB{s0me_t3xt}', a 'Submit Flag' button, a 'Submit flag difficulty rating' dropdown, and a 'Submit Rating' button. At the bottom, it shows 'Blood taken by dim1119' with a timer at '0H 12M 6S', 'Released on 9th April, 2021', and 'Created by diogt'.

- HackTheBox의 HardWare 영역의 워게임 문제인 Debugging Interface 문제를 풀어보도록 하겠다.

This block shows a close-up of the file download section. It includes a file icon, the filename 'Debugging_Interface.zip', the size '10 KB', a green 'Download Files' button with a dropdown arrow, and a key icon.



Debugging_Interface.zip	10KB	Zip 아카이브	오늘 오후 3:12
debugging_interface_signal.sal	10KB	Saleae Capture	오늘 오후 3:12

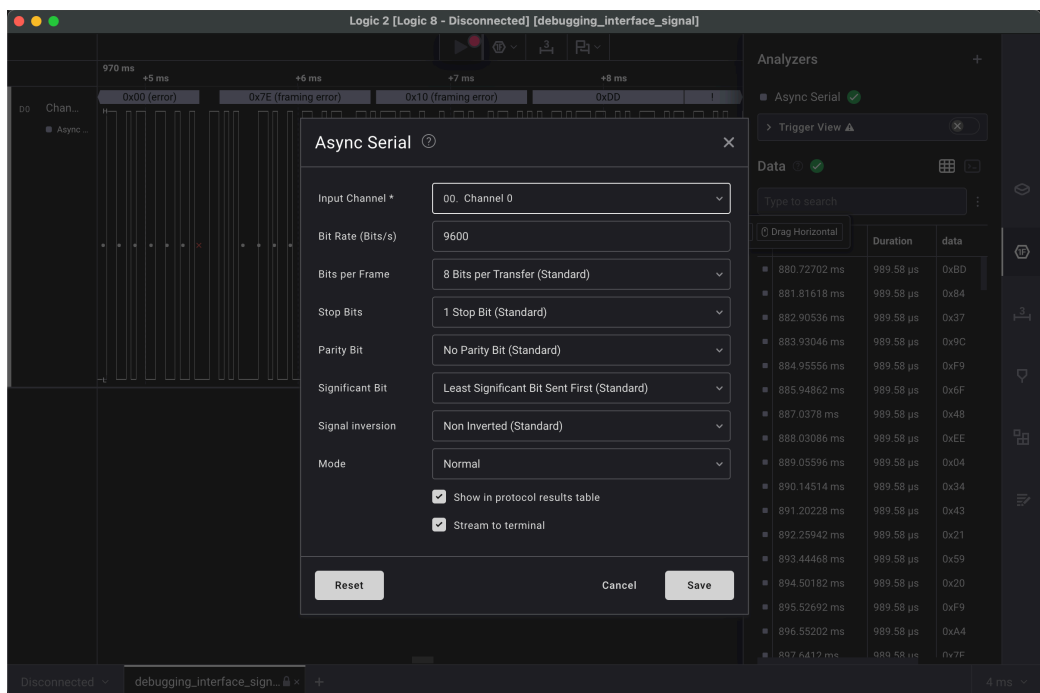
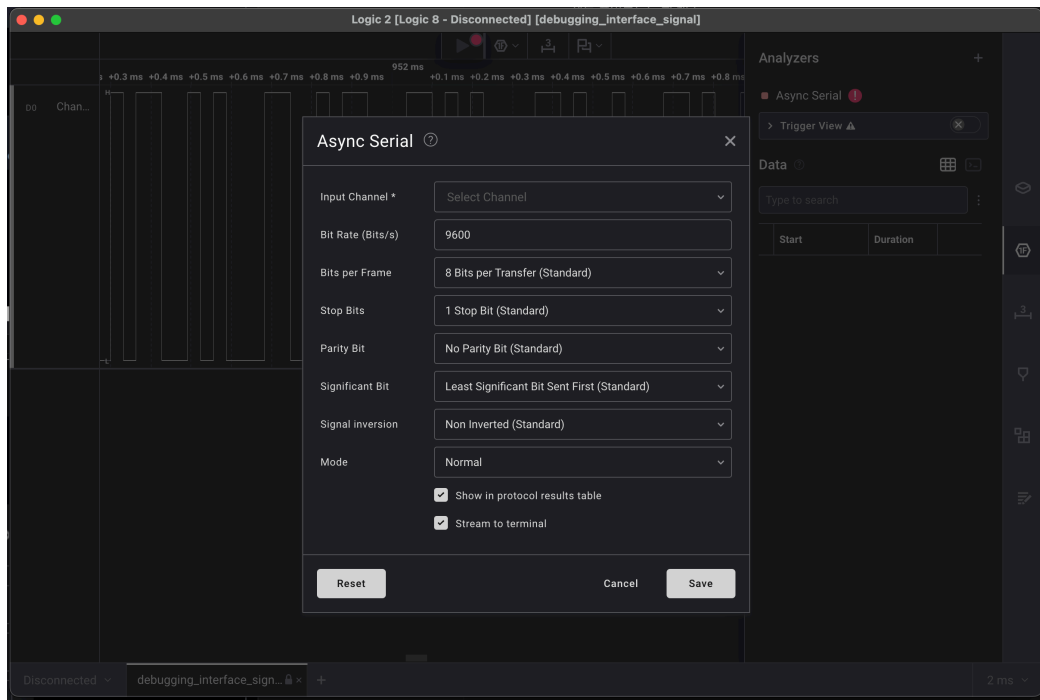
- 문제 파일을 다운로드 한 후, 압축 해제를 하면, debugging_interface_signal.sal 파일이 있는 것을 확인할 수 있다.
- file 명령어를 이용하여 파일 형식을 확인해보겠다.

```
~/Downloads
~/Downloads file debugging_interface_signal.sal ok | system node | at 15:14:29
debugging_interface_signal.sal: Zip archive data, at least v2.0 to extract, compression method=deflate
```

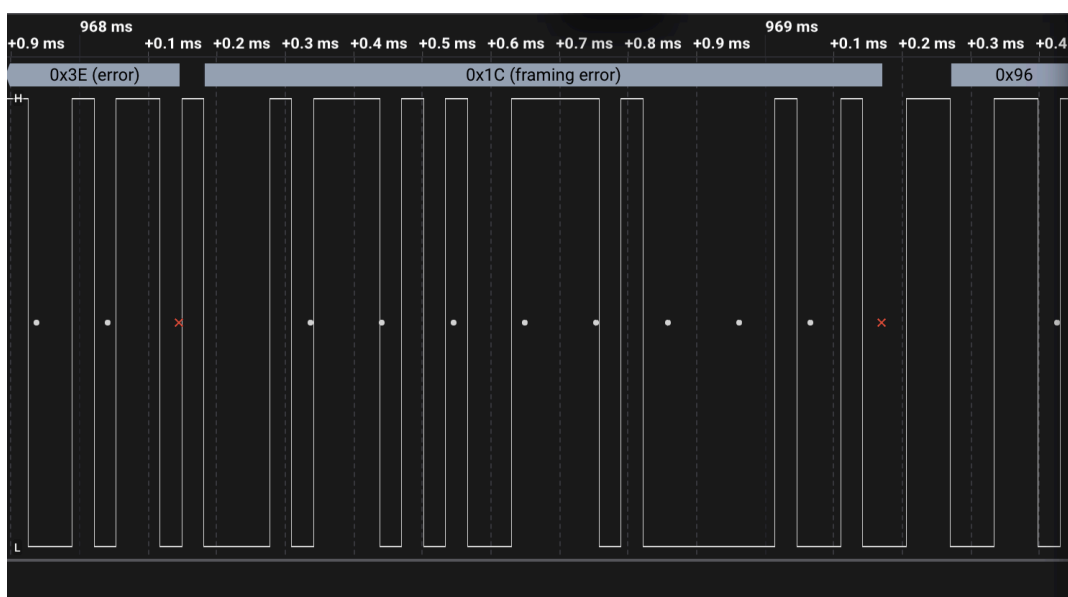
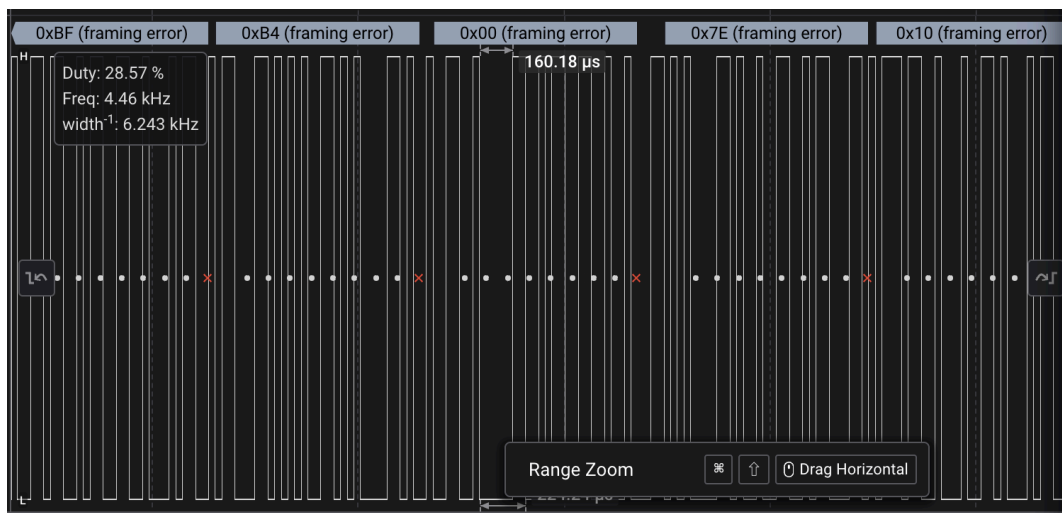
- 이제 다음으로 확장자가 .sal이므로, Saleae 로직 분석기를 사용해서 분석해보도록 하겠다.

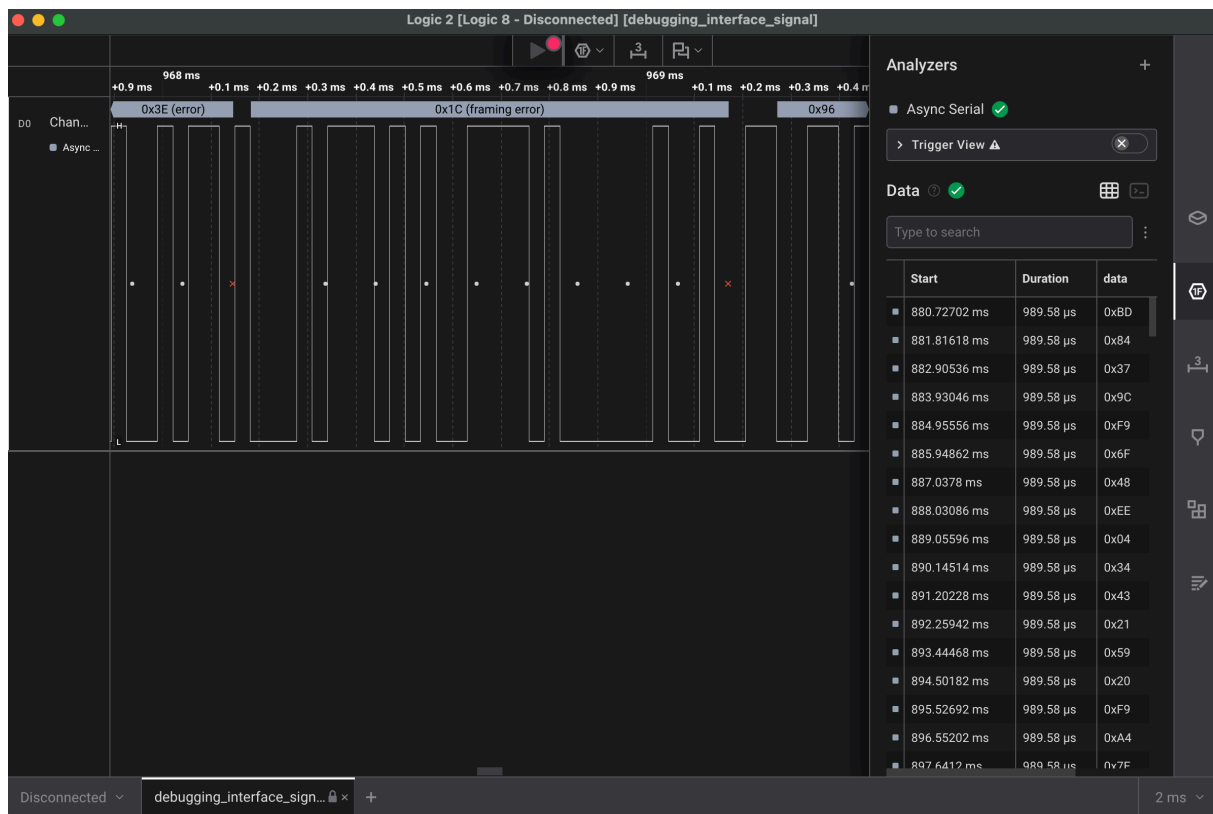


- 이제 Analyzer 탭을 선택한 다음에 Async Serial을 클릭해본다.



- 저장을 클릭한 다음 확인해보면, 프레임 (프라이밍) 오류가 많다는 것을 확인할 수 있다. (빨간색 표시)





Analyzers

☒ Async Serial

> Trigger View

Data

Type to search

	Start	Duration	data	error	
	880.72702 ms	989.58 μs	0xBD	framing	
	881.81618 ms	989.58 μs	0x84	framing	
	882.90536 ms	989.58 μs	0x37	framing	
	883.93046 ms	989.58 μs	0x9C	framing	
	884.95556 ms	989.58 μs	0xF9		
	885.94862 ms	989.58 μs	0x6F	framing	
	887.0378 ms	989.58 μs	0x48		
	888.03086 ms	989.58 μs	0xEE	framing	
	889.05506 ms	989.58 μs	0x04	framing	
	891.20228 ms	989.58 μs	0x34	framing	
	891.20228 ms	989.58 μs	0x43	framing	
	892.25942 ms	989.58 μs	0x21	framing	
	893.44468 ms	989.58 μs	0x59	framing	
	894.50182 ms	989.58 μs	0x20	framing	
	895.52692 ms	989.58 μs	0xF9	framing	
	896.55202 ms	989.58 μs	0xA4	framing	
	897.6412 ms	989.58 μs	0x7E	framing	

- 위의 데이터 표현 방식을 ASCII로 바꾸어보자.

Analyzers

☒ Async Serial ✔
⋮

▼ Trigger View ⚠

Async Serial

Query

Holdoff

Data ? ✔

Type to search

	Start	Duration	data	error
■	880.72702 ms	989.58 μs	0xBD	framing
■	881.81618 ms	989.58 μs	0x84	framing
■	882.90536 ms	989.58 μs	0x37	framing
■	883.93046 ms	989.58 μs	0x9C	framing
■	884.95556 ms	989.58 μs	0xF9	
■	885.94862 ms	989.58 μs	0x6F	framing
■	887.0378 ms	989.58 μs	0x48	
■	888.03086 ms	989.58 μs	0xEE	framing
■	889.05596 ms	989.58 μs	0x04	framing
■	890.14514 ms	989.58 μs	0x34	framing
■	891.20228 ms	989.58 μs	0x43	framing
■	892.25942 ms	989.58 μs	0x21	framing
■	893.44468 ms	989.58 μs	0x5D	framing

Edit...

Select Color

Restart

Delete

☒ Stream to Terminal

☒ Show in Data Table

Binary

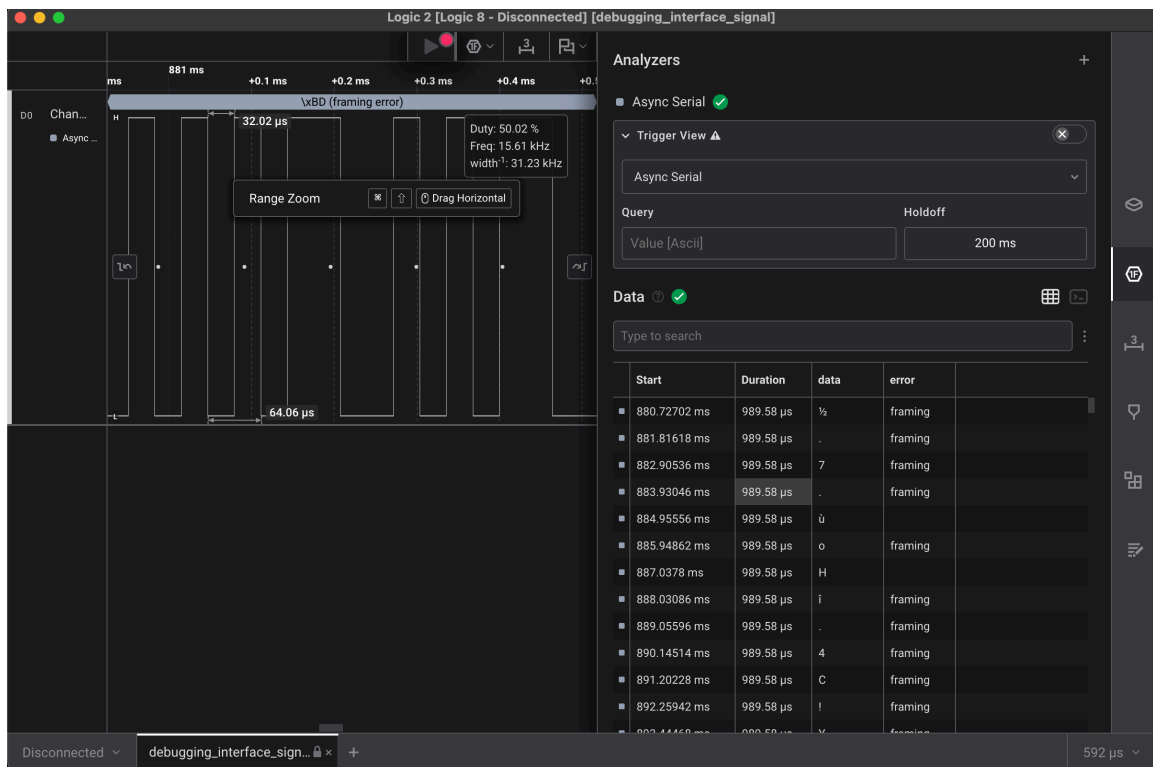
Decimal

☒ Hexadecimal

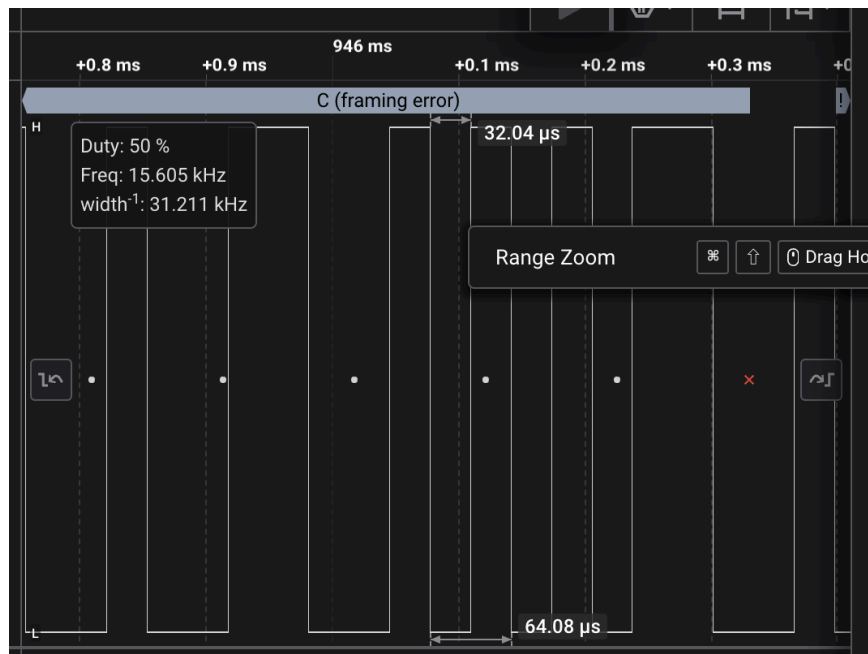
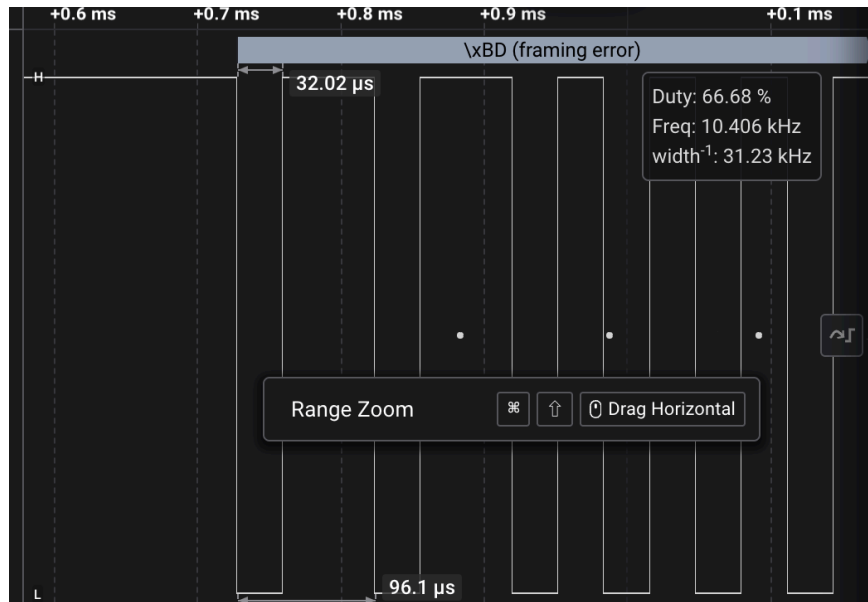
Ascii

Export to TXT/CSV

592 μs ▼



- ASCII 코드로 바꾸고 난 후, 훨씬 더 읽기 쉬워진 것을 확인할 수 있다.
 - 이제 프레임 (프라이밍) 오류를 해결해야만 한다.
 - 프레임 (프라이밍) 오류는 읽는 비트의 속도가 너무 빠르거나 너무 느릴 때 발생한다.
 - 비트를 너무 빠르게 읽거나, 너무 느리게 읽으면 비트가 서로 다른 값 을 나타낸다.
 - 즉, 프레임 (프라이밍) 오류를 수정하려면 각 최단 간격을 찾기만 하면 된다.



- 마우스를 가져다대면서 확인해보면, 최단 간격은 32.02라는 것을 알 수 있다.
- 따라서, 실제 비트 전송률을 계산하기 위해 아래와 같은 공식을 적용할 수 있다.

$$\text{비트 전송률 (bps)} = \frac{\text{파일 크기 (바이트)} \times 8}{\text{파일 전송 시간 (초)}}$$

Actual Bit Rate = $1 / (32.02 * 10^{-6}) \rightarrow 312.30.480949406621$

- 읽어야 할 비트 수에 소수점 자리가 없으므로, 소수점을 제외할 수 있다. (즉, 반올림을 하여 계산하면 된다.)
 - Async Serial의 편집 버튼을 클릭한 다음, 비트 전송률 값을 변경한다.
(31230)으로 변경하였다.
(312.30.xxxx이기 때문)

Analizers

■ Async Serial ✓

▼ Trigger View ⚠

Async Serial

Query

Value [Ascii]

Data ⓘ ✓

Type to search

	Start	Duration	data	err
■	880.72702 ms	989.58 μs	½	fra
■	881.81618 ms	989.58 μs	.	fra
■	882.90536 ms	989.58 μs	7	fra
■	883.93046 ms	989.58 μs	.	fra
■	884.95556 ms	989.58 μs	ù	
■	885.94862 ms	989.58 μs	o	framing
■	887.0378 ms	989.58 μs	H	
■	888.03086 ms	989.58 μs	î	framing
■	889.05596 ms	989.58 μs	.	framing
■	890.14514 ms	989.58 μs	4	framing
■	891.20228 ms	989.58 μs	C	framing
■	892.25942 ms	989.58 μs	!	framing
■	893.44468 ms	989.58 μs	Y	framing

Filter

Find More Analyzers

SPI

Async Serial

I2C

Midi

Intel MCS-04 bus

Atmel SWI

MDIO

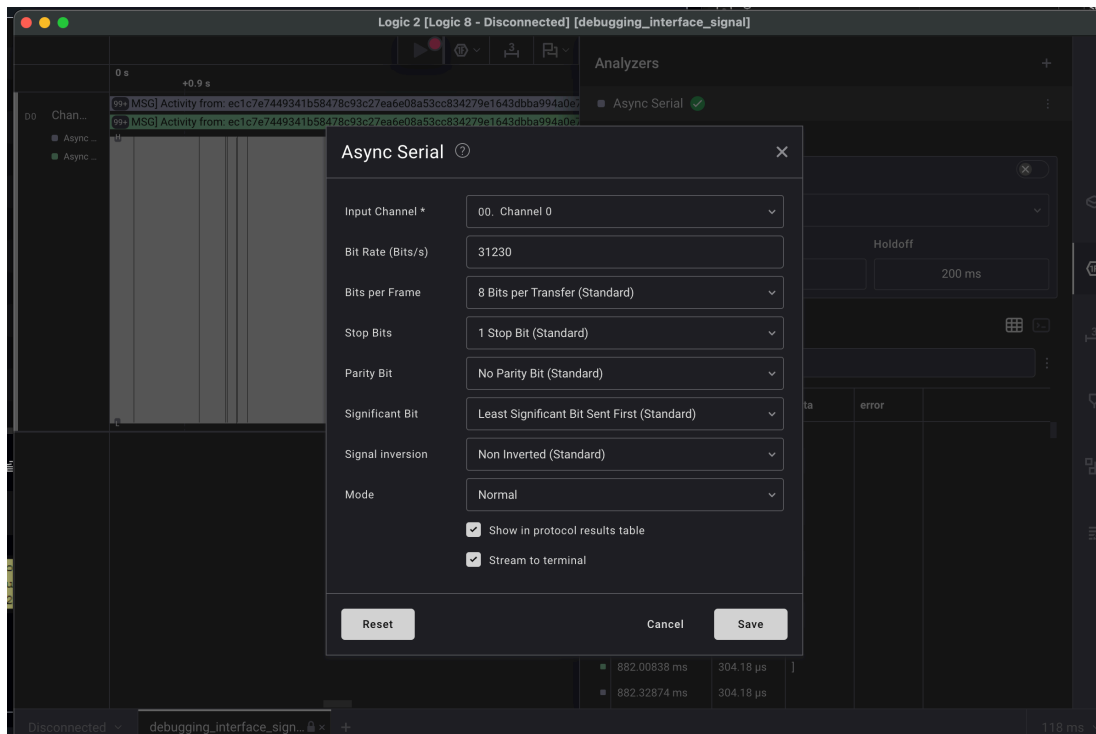
HDMI CEC

SWD

PS/2 Keyboard/Mouse

Manchester

884 μs ▼



- 그리고 난 후, 저장을 클릭하면, 프레임 (프라이밍) 오류가 해결된 것을 확인할 수 있다.

■ Async Serial [1] ✓

> Trigger View ▲
✕

Data ? ✓
 📊 >_

⋮

	Start	Duration	data	error	
■	880.72702 ms	304.18 μs	[
■	880.72702 ms	304.18 μs	[
■	881.04736 ms	304.18 μs	M		
■	881.04736 ms	304.18 μs	M		
■	881.3677 ms	304.18 μs	S		↩
■	881.3677 ms	304.18 μs	S		
■	881.68804 ms	304.18 μs	G		
■	881.68804 ms	304.18 μs	G		
■	882.00838 ms	304.18 μs]		
■	882.00838 ms	304.18 μs]		
■	882.32874 ms	304.18 μs			
■	882.32874 ms	304.18 μs			
■	882.64908 ms	304.18 μs	A		
■	882.64908 ms	304.18 μs	A		
■	882.96942 ms	304.18 μs	c		

- 데이터 결과를 터미널로 변경해서 확인하면 플래그를 확인할 수 있다.

Data ? ✓



```
468f8f5dab8a7ad0
[MSG] Activity from: 36257a19934b71cea753da3df9be8ae8ca49ee843b72b1c5
468f8f5dab8a7ad0
[MSG] Activity from: HTB{d38u991n9_1n732f4c35_c4n_83_f0und_1n_41m057_
3v32y_3m83dd3d_d3v1c3!!52}
[MSG] Activity from: ec1c7e7449341b58478c93c27ea6e08a53cc834279e1643d
bba994a0e7f3ea43
[MSG] Activity from: 003b9434a45f0eecd2d35bcc78129aa3edc363f802ae5abd
d161c4f421ca49a7
[MSG] Activity from: 65ec312325f43f40107dfcba651cab2d1afb6df54578065f
1d8bba89801d3ef2
[MSG] Activity from: 223e634cea203ba2c7d4e7931a2dafdf0d452309c1a1eb1a
28fc2fae057df400
[MSG] Activity from: 431d591c6eed3b6e793b316d7bf6ce2e3be51aa707680b6f
14511fbc9dae9e32
[MSG] Activity from: 65ec312325f43f40107dfcba651cab2d1afb6df54578065f
1d8bba89801d3ef2
[MSG] Activity from: 65ec312325f43f40107dfcba651cab2d1afb6df54578065f
1d8bba89801d3ef2
[MSG] Activity from: ebb2b5d1dfbbb8174f5fb1fd15230540aea77772d3a65482
def3d978f6caf152
[MSG] Activity from: f7fab4b591754a190be32cb607f257f436fa3f325d71edf4
1b6179c5330cd75a
[MSG] Activity from: 476bdcaf166385371f49c54ba74d275cfdfa5c70c255ea45
363e3795cbc11ae5
[MSG] Activity from: 63681fa3c03451c49f9fc2ab9be43bea7f069069c1c472f6
a41e3ef3a761de50
[MSG] Activity from: 36257a19934b71cea753da3df9be8ae8ca49ee843b72b1c5
468f8f5dab8a7ad0
[MSG] Activity from: 36257a19934b71cea753da3df9be8ae8ca49ee843b72b1c5
468f8f5dab8a7ad0
[MSG] Activity from: HTB{d38u991n9_1n732f4c35_c4n_83_f0und_1n_41m057_
3v32y_3m83dd3d_d3v1c3!!52}
```



```
468f8f5dab8a7ad0
[MSG] Activity from: 36257a19934b71cea753da3df9be8ae8ca49ee843b72b1c5
468f8f5dab8a7ad0
[MSG] Activity from: HTB{d38u991n9_1n732f4c35_c4n_83_f0und_1n_41m057_
3v32y_3m83dd3d_d3v1c3!!52}
[MSG] Activity from: ec1c7e7449341b58478c93c27ea6e08a53cc834279e1643d
bba994a0e7f3ea43
[MSG] Activity from: 003b9434a45f0eecd2d35bcc78129aa3edc363f802ae5abd
d161c4f421ca49a7
[MSG] Activity from: 65ec312325f43f40107dfcba651cab2d1afb6df54578065f
1d8bba89801d3ef2
[MSG] Activity from: 223e634cea203ba2c7d4e7931a2dafdf0d452309c1a1eb1a
28fc2fae057df400
[MSG] Activity from: 431d591c6eed3b6e793b316d7bf6ce2e3be51aa707680b6f
14511fbc9dae9e32
[MSG] Activity from: 65ec312325f43f40107dfcba651cab2d1afb6df54578065f
1d8bba89801d3ef2
[MSG] Activity from: 65ec312325f43f40107dfcba651cab2d1afb6df54578065f
1d8bba89801d3ef2
[MSG] Activity from: ebb2b5d1dfbbb8174f5fb1fd15230540aea77772d3a65482
def3d978f6caf152
[MSG] Activity from: f7fab4b591754a190be32cb607f257f436fa3f325d71edf4
1b6179c5330cd75a
[MSG] Activity from: 476bdcaf166385371f49c54ba74d275cfdfa5c70c255ea45
363e3795cbc11ae5
[MSG] Activity from: 63681fa3c03451c49f9fc2ab9be43bea7f069069c1c472f6
a41e3ef3a761de50
[MSG] Activity from: 36257a19934b71cea753da3df9be8ae8ca49ee843b72b1c5
468f8f5dab8a7ad0
[MSG] Activity from: 36257a19934b71cea753da3df9be8ae8ca49ee843b72b1c5
468f8f5dab8a7ad0
[MSG] Activity from: HTB{d38u991n9_1n732f4c35_c4n_83_f0und_1n_41m057_
3v32y_3m83dd3d_d3v1c3!!52}
```



