

Décoder l'ISO7816 avec Saleae

Table des matières

Introduction.....	3
Câblage.....	3
Utilisation du logiciel.....	4
Premier enregistrement.....	8
Pour aller plus loin	10

Introduction

Le présent document est un tutoriel pour apprendre à décoder l'iso7816 à l'aide du matériel et du logiciel Saleae. L'extension permet de décoder les octets transmis sous les protocoles T=0 et T=1. Elle n'est cependant pas capable de gérer les changements de fréquence à la suite d'un échange PPS. En raison d'une limite logicielle, l'extension n'est pas capable de déchiffrer le dernier message APDU d'un enregistrement.

Installation nécessaire :

- La smartcard à lire,
- Un lecteur de smartcards,
- Un bridge permettant d'accéder aux contacts de la carte lorsqu'elle est branchée au lecteur (exemple sur l'image 1),
- Un boîtier type Saleae Logic Pro 8 (image 2) voir,
- Le logiciel Saleae Logic 2 (téléchargement : <https://www.saleae.com/fr/downloads/>).

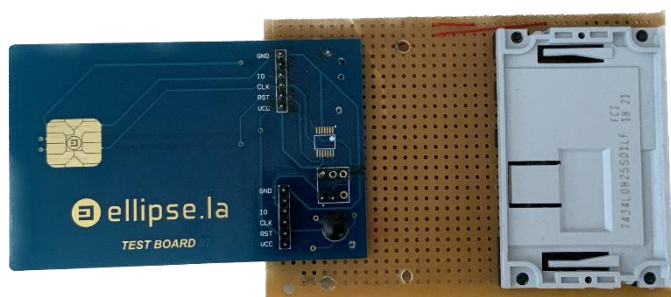


Image 1 : Bridge



Image 2 : Saleae Logic Pro 8

Câblage


Pin du Saleae	Contact de la carte	Pin sur le bridge
G (n'importe lequel)	C5	GND
0	C7	IO
1	C1	VCC
2	C2	RST
3	C3	CLK



Image 3 : pins Logic Pro 8

Il est important de réaliser ce branchement précis afin d'utiliser les pré-réglages fournis pour le logiciel. Si vous branchez autrement, il faudra configurer manuellement les réglages du logiciel. Ce ne sera pas détaillé ici.

Utilisation du logiciel

- Avant toute chose, brancher le boîtier Logic Pro 8 à l'ordinateur.
- Ouvrir le logiciel Saleae Logic 2 (logo ).

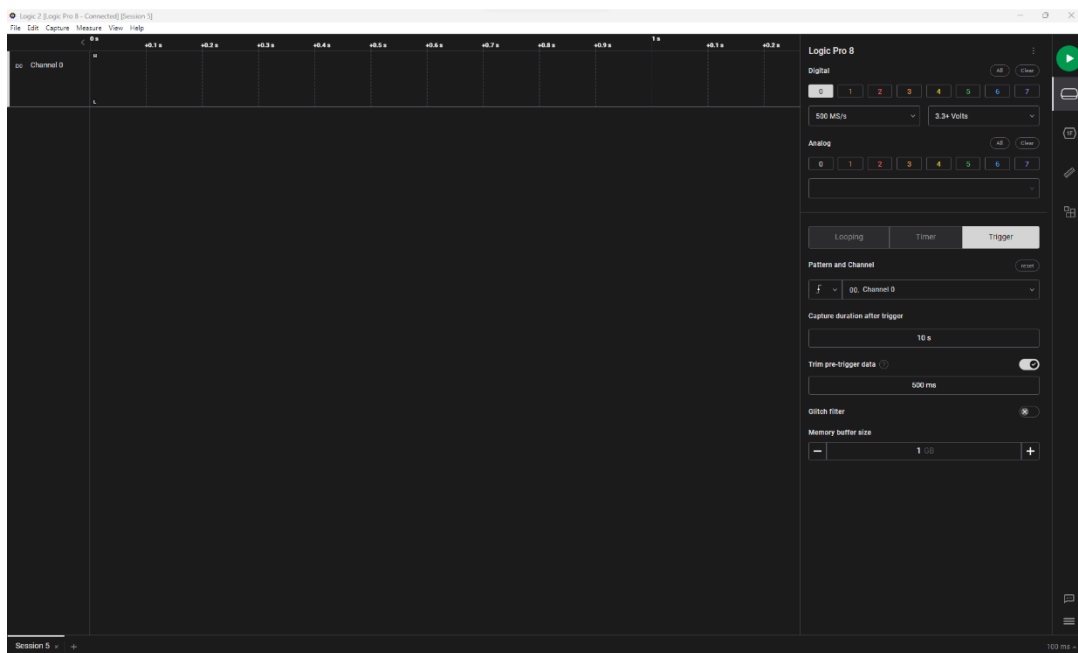


Image 4 : accueil Saleae Logic 2

- Ouvrir les réglages de preset avec le raccourci « Ctrl + ⌘ + P » ou en cliquant sur les trois barres en bas à droite puis sur « Presets ». Respectivement (1) et (2) sur l'image 5.

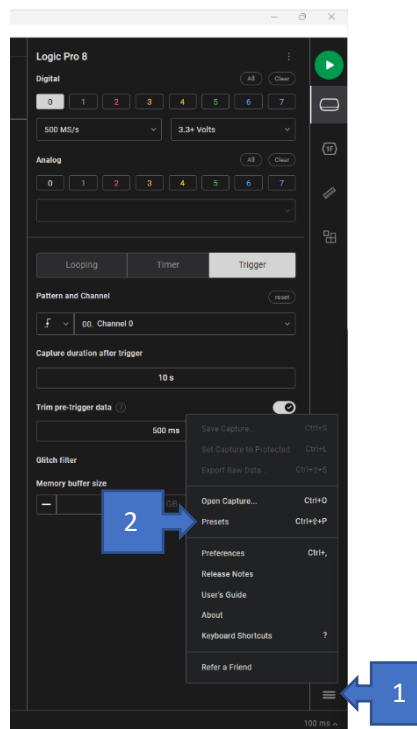


Image 5 : réglages de preset

- Cliquer sur « import », (1) sur l'image 6. Puis choisir et ouvrir le fichier « ISO7816 reading preset.logic2Preset »

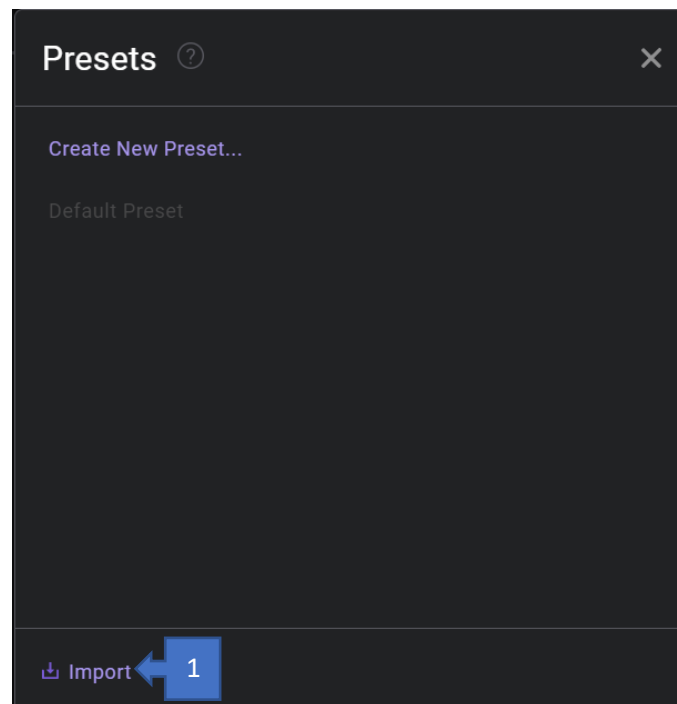


Image 6 : ajouter un preset

- Une nouvelle ligne devrait apparaître dans la fenêtre d'ajout de presets. En passant la souris sur cette ligne, « Load » apparaîtra. Cliquer sur « Load ».

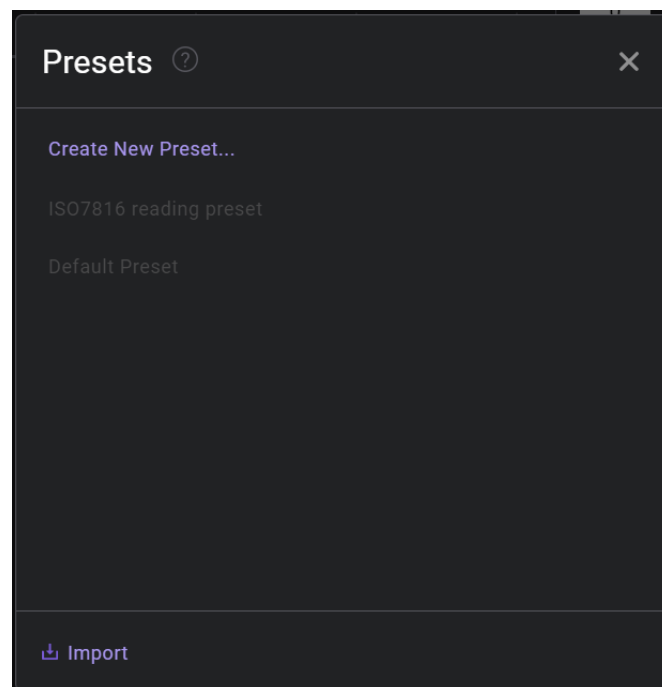


Image 7 : preset ajouté

Le preset est un ensemble de réglages permettant la capture et le traitement de signaux selon la norme iso7816. Les réglages comprennent, entre autres : les entrées à activer, le nom de chaque entrée, le mode et le temps d'enregistrement, un analyseur « Async Serial » et l'analyseur maison « ISO7816_Hla » basé sur l'Async. Charger un preset permet de configurer automatiquement tous ces réglages. Les images 8, 9 et 10 montrent la page d'accueil du logiciel après le chargement du preset.

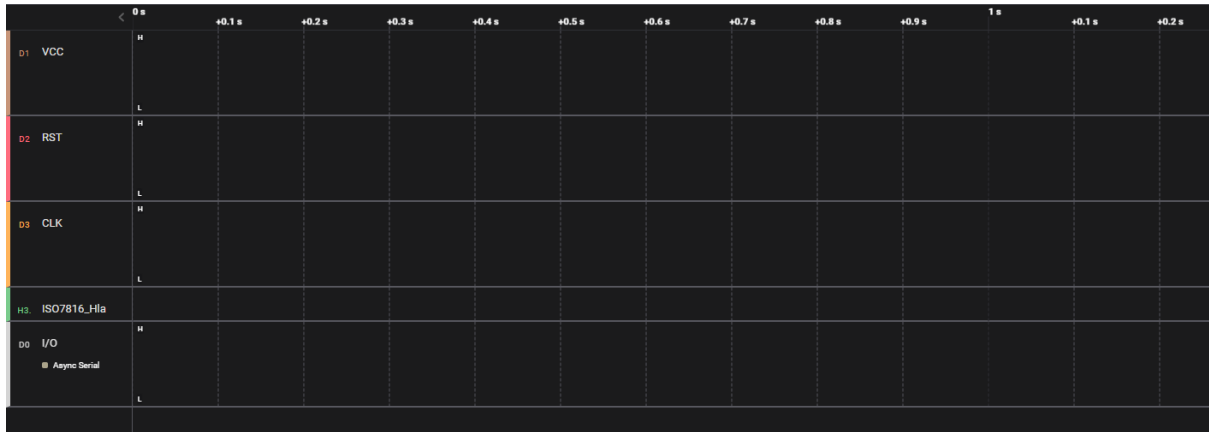


Image 8 : accueil logiciel avec preset

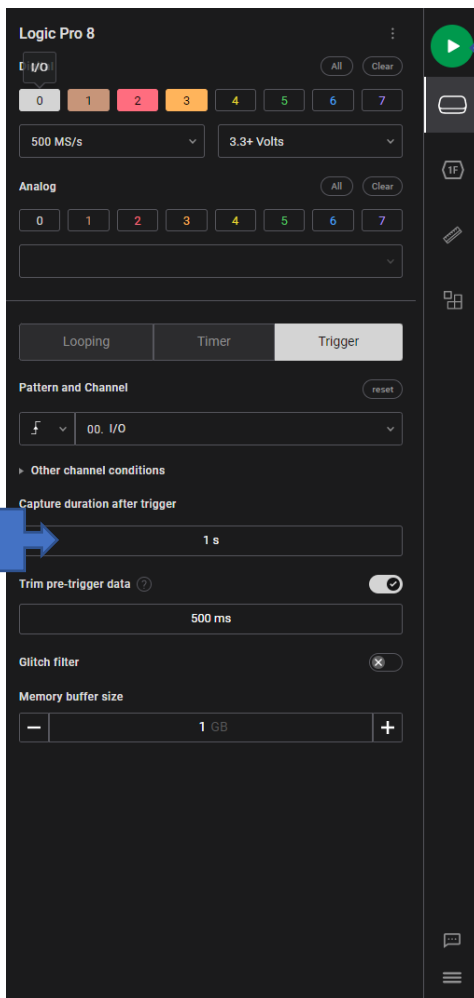


Image 9 : presets d'enregistrement

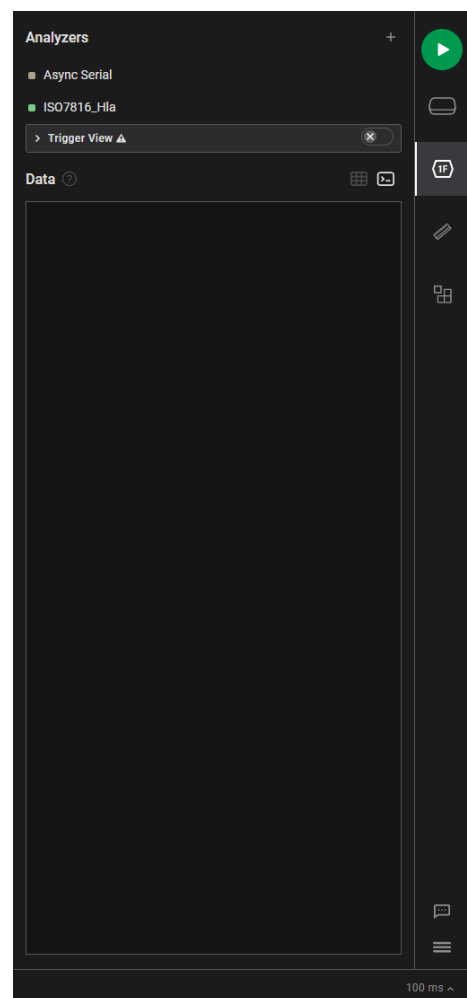
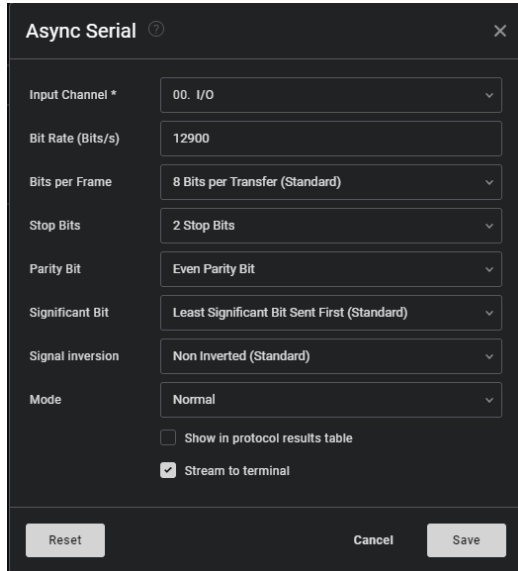


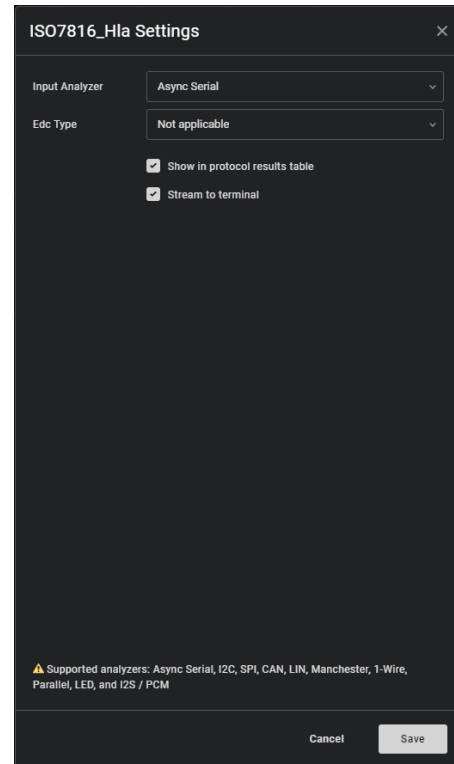
Image 10 : presets d'analyseur

Les images 11 et 12 montrent respectivement les réglages de l'analyseur Async et ISO7816_Hla, au cas où le preset n'aurait pas fonctionné.



The screenshot shows the 'Async Serial' settings window. It contains several configuration options: 'Input Channel *' set to '00. I/O', 'Bit Rate (Bits/s)' set to '12900', 'Bits per Frame' set to '8 Bits per Transfer (Standard)', 'Stop Bits' set to '2 Stop Bits', 'Parity Bit' set to 'Even Parity Bit', 'Significant Bit' set to 'Least Significant Bit Sent First (Standard)', 'Signal inversion' set to 'Non Inverted (Standard)', and 'Mode' set to 'Normal'. At the bottom, there are checkboxes for 'Show in protocol results table' (unchecked) and 'Stream to terminal' (checked). The window has 'Reset', 'Cancel', and 'Save' buttons at the bottom.

Image 11 : presets Async



The screenshot shows the 'ISO7816_Hla Settings' window. It contains two dropdown menus: 'Input Analyzer' set to 'Async Serial' and 'Edc Type' set to 'Not applicable'. Below these are two checked checkboxes: 'Show in protocol results table' and 'Stream to terminal'. At the bottom, there is a warning icon and text: 'Supported analyzers: Async Serial, I2C, SPI, CAN, LIN, Manchester, 1-Wire, Parallel, LED, and I2S / PCM'. The window has 'Cancel' and 'Save' buttons at the bottom.

Image 12 : presets ISO7816_Hla

Vous êtes prêt à réaliser votre premier enregistrement !

Premier enregistrement

Afin de réaliser votre premier enregistrement, cliquer sur le bouton « Play » (repère (1) sur l'image 9). Branchez ensuite la carte au bridge puis le bridge au lecteur. Le logiciel détectera le premier front du signal « I/O » et commencera l'enregistrement pour 1s. Si vous souhaitez réaliser un enregistrement plus long, changez la durée spécifiée dans le champ « Capture duration after trigger » (repère (2) sur l'image 9).

L'image 13 montre une partie APDU d'un enregistrement. Les rectangles verts (exemple en repère (1)) sont les informations qui ont été calculées par l'analyseur maison. La partie « Data » résume toutes ces informations dans l'onglet « matrice » (repère (2)). Des informations complémentaires, pouvant être utiles au débogage, se trouvent dans l'onglet « terminal » (repère (3)).

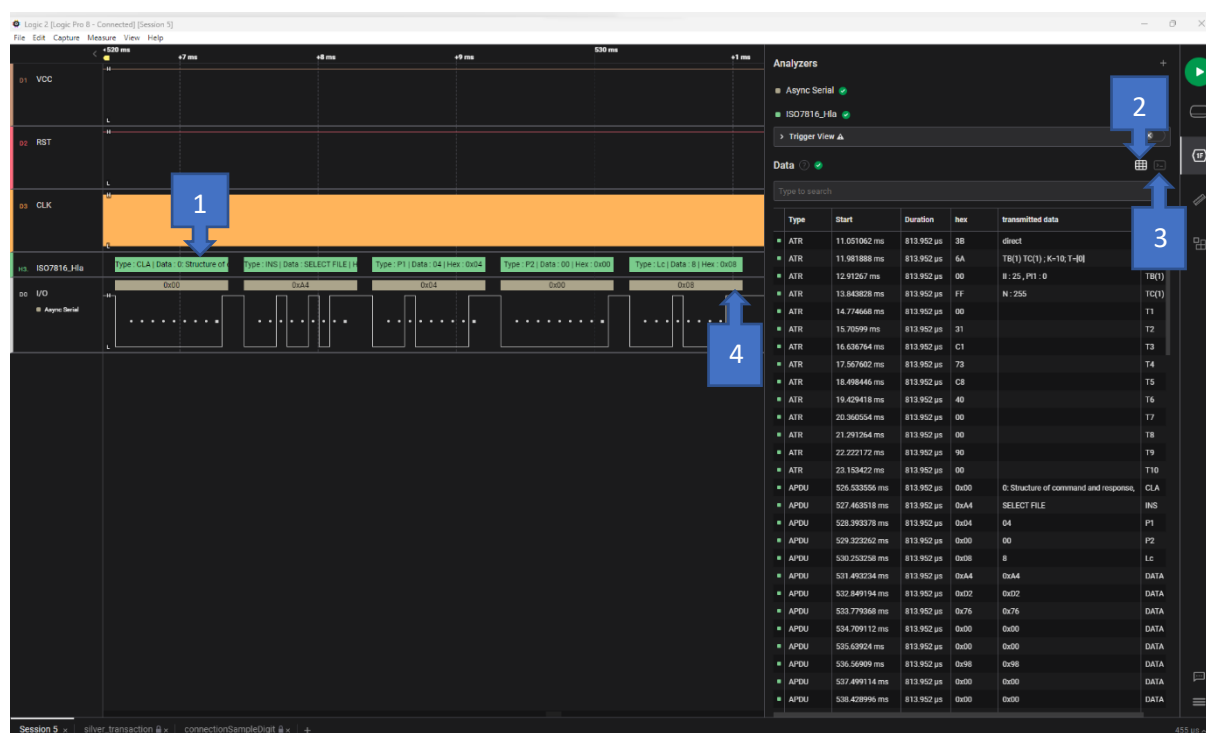


Image 13 : enregistrement iso7816, T=0

Les octets peuvent être encodés de deux manières différentes. La méthode est indiquée dans l'ATR et l'extension s'en sert pour le décodage. La « bonne » valeur hexadécimale est celle notée après « Hex : » dans les rectangles verts. La valeur notée dans les rectangles taupe (repère (4), image 13) peuvent être fausses.

Vous pouvez sauvegarder l'enregistrement avec la commande « Ctrl + S », ou dans le menu en bas à droite avec les trois barres (repère (1), image 5) : « Save capture... ».

Spécificités de T=1

Afin de décoder les octets transmis entre une carte et un lecteur selon le protocole T=1, il est nécessaire de préciser le type de caractère de contrôle utilisé. Pour cela, il faut accéder aux réglages de l'analyseur ISO7816_Hla (repères (1) puis (2), image 14). Vous pourrez ainsi modifier ce réglage dans le champ « Edc Type » (voir image 15).

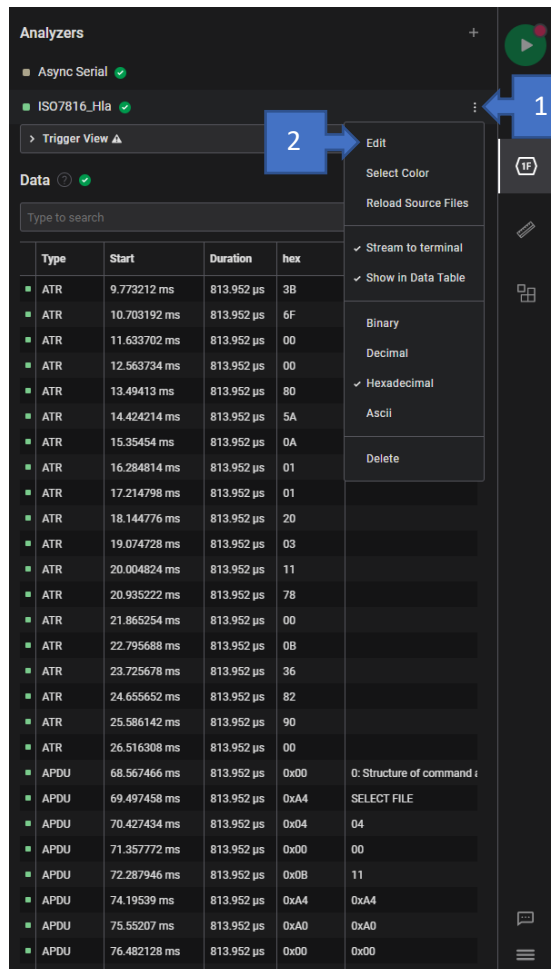


Image 14 : accéder aux réglages de l'analyseur

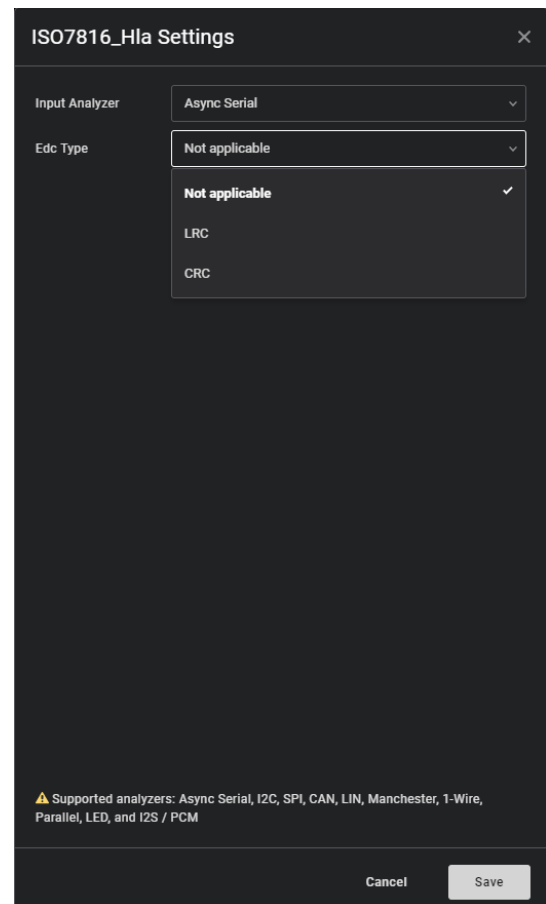


Image 15 : réglage EDC

Résolution de problèmes

Si l'analyseur Async n'est pas réglé à la bonne fréquence, il se peut que l'IO soit semblable à l'image 14.

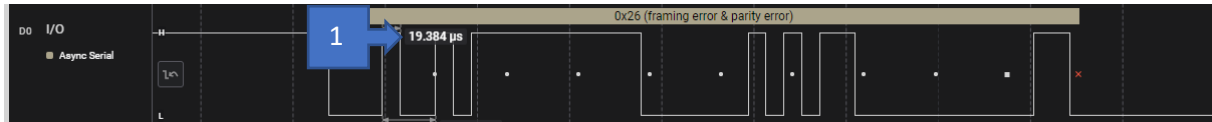


Image 16 : rectifier la fréquence 1

Il va falloir calculer la fréquence utilisée dans votre enregistrement. Pour ce faire, cherchez le bit le plus court et notez sa durée τ . Sur notre exemple, la durée est $\tau = 19.384 \mu s$ (voir repère (1), image 14). La fréquence étant l'inverse de la durée, vous devez calculer $f_1 = \frac{1}{\tau}$. Dans notre exemple, nous avons donc $f_1 = \frac{1}{19.384 \times 10^{-6}} \approx 51600 \text{ Hz}$. Ouvrez les réglages de l'analyseur Async et saisissez la fréquence calculée f_1 dans le champ « Bit Rate » (image 15, repère (1)).

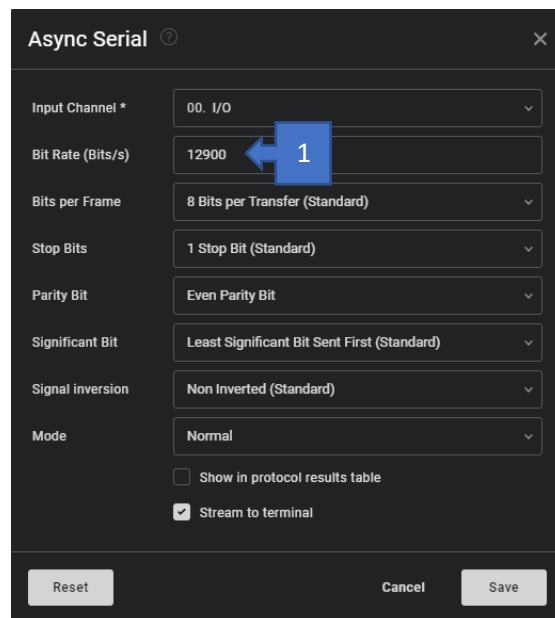


Image 17 : rectifier la fréquence 2

Cliquez sur « Save ». Si le réglage est bon, l'enregistrement devrait ressembler à celui sur l'image 13.

Pour aller plus loin

Guides utilisateur : <https://support.saleae.com/user-guide>

Guide logiciel : <https://support.saleae.com/user-guide/using-logic>