

Décoder l'ISO7816 avec Saleae

Table des matières

Introduction.....	3
Câblage.....	3
Utilisation du logiciel.....	4
Premier enregistrement.....	9
Spécificités de T=1	10
Résolution de problèmes	11
Fréquence :	11
Installation de l'extension :	11
Pour aller plus loin	12

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 (voir [image 2](#)),
- Le logiciel Saleae Logic 2 (téléchargement : <https://www.saleae.com/fr/downloads/>).

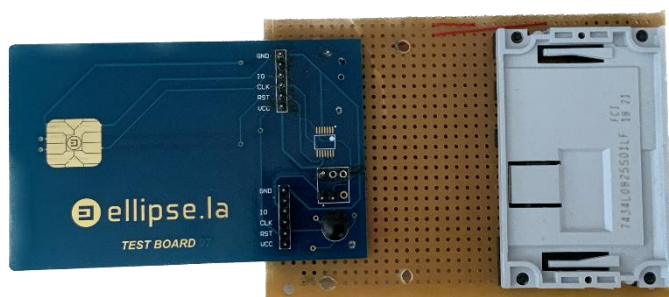


Image 1 : Bridge



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 .

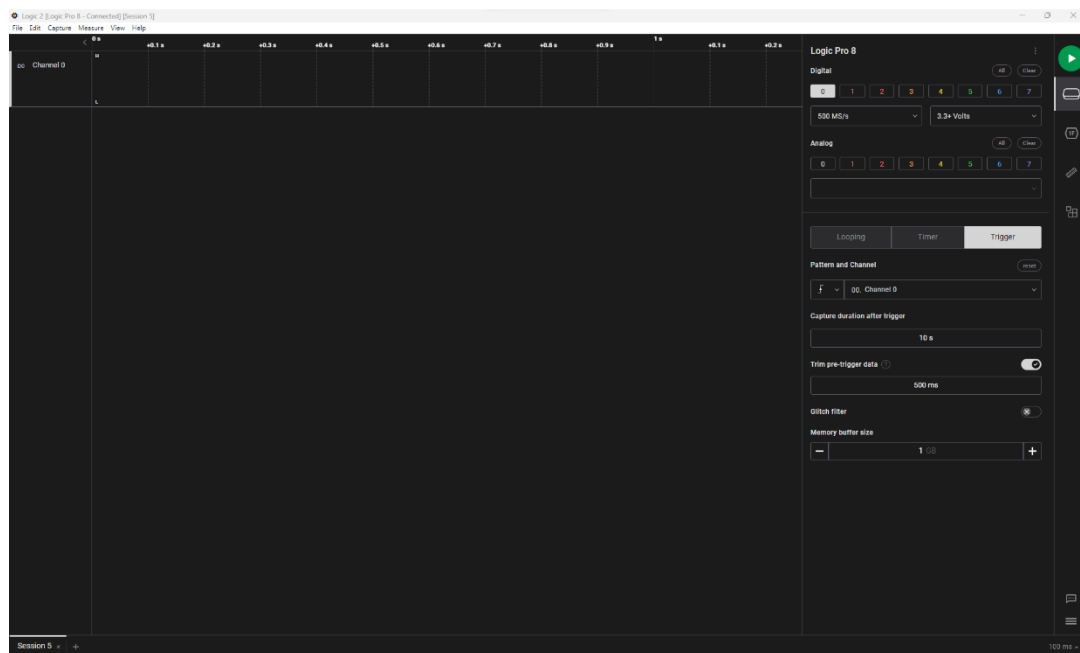


Image 4 : accueil Saleae Logic 2

- Ouvrir l'onglet « Extensions » ([Image 5](#), repère (1)).
- Rechercher l'extension « ISO7816_Hla » puis cliquez sur « INSTALL » ([image 5](#), repère (2)).

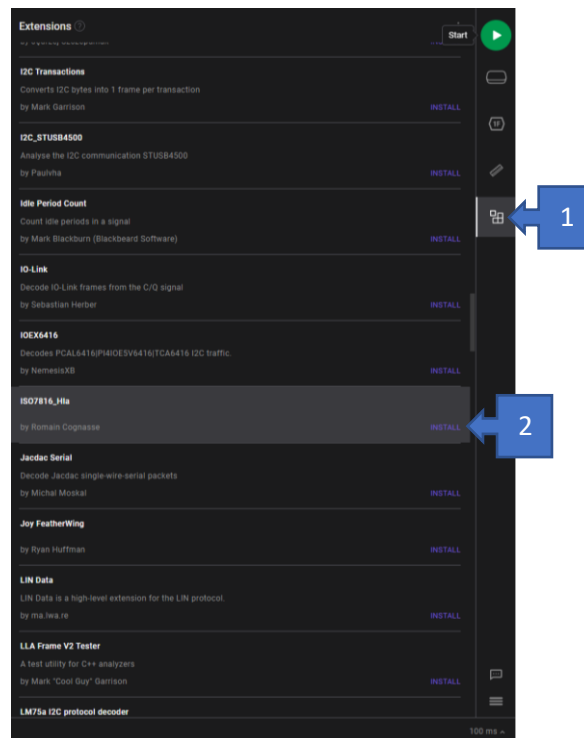


Image 5 : installer une extension

- 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 6](#).

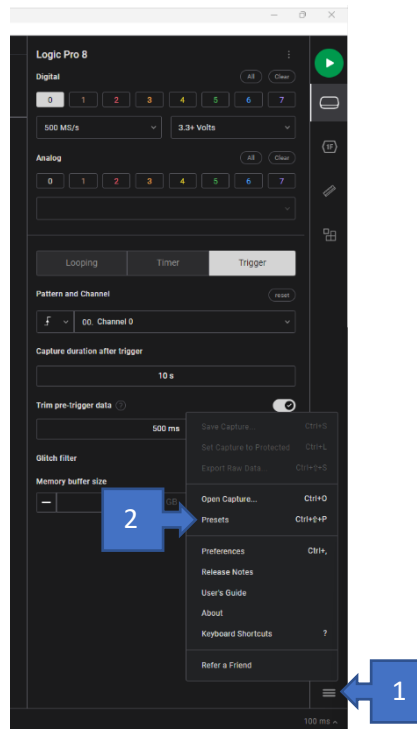


Image 6 : réglages de preset

- Cliquer sur « import », (1) sur [l'image 7](#). Puis choisir et ouvrir le fichier « ISO7816 reading preset.logic2Preset »

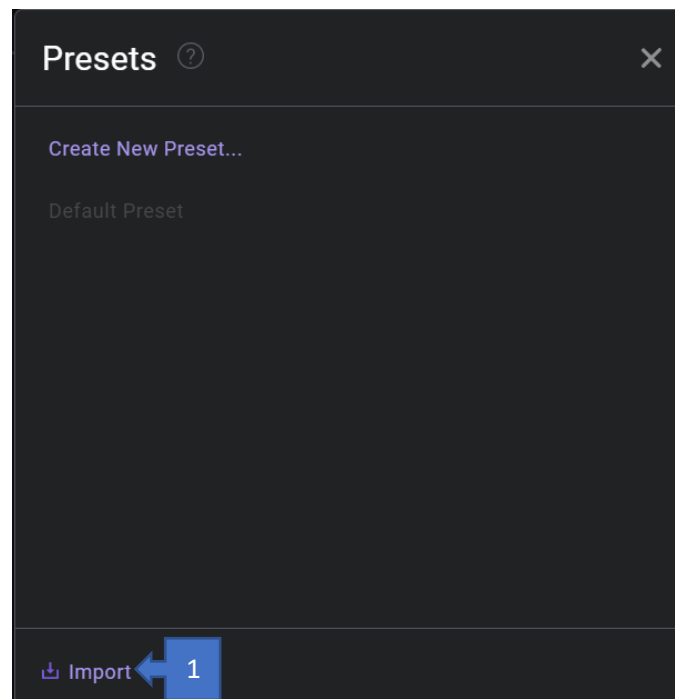


Image 7 : ajouter un preset

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

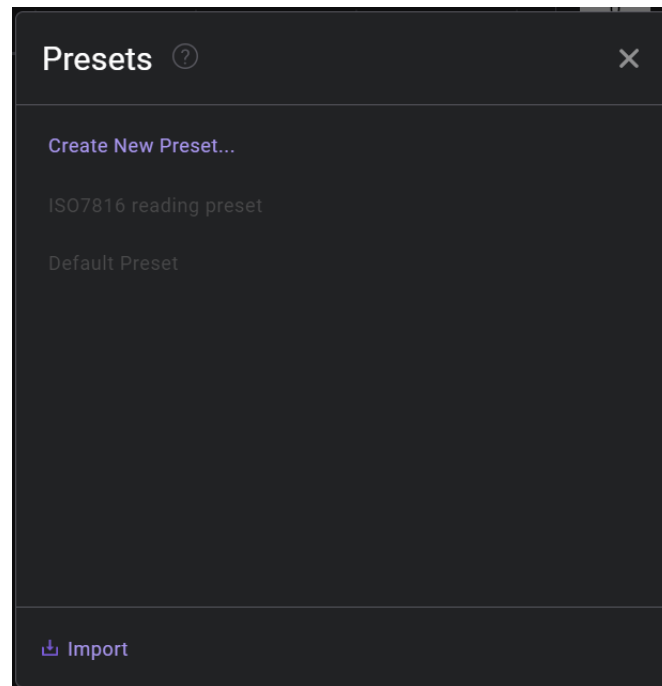


Image 8 : preset ajouté

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 [9](#), [10](#) et [11](#) montrent la page d'accueil du logiciel après le chargement du preset.

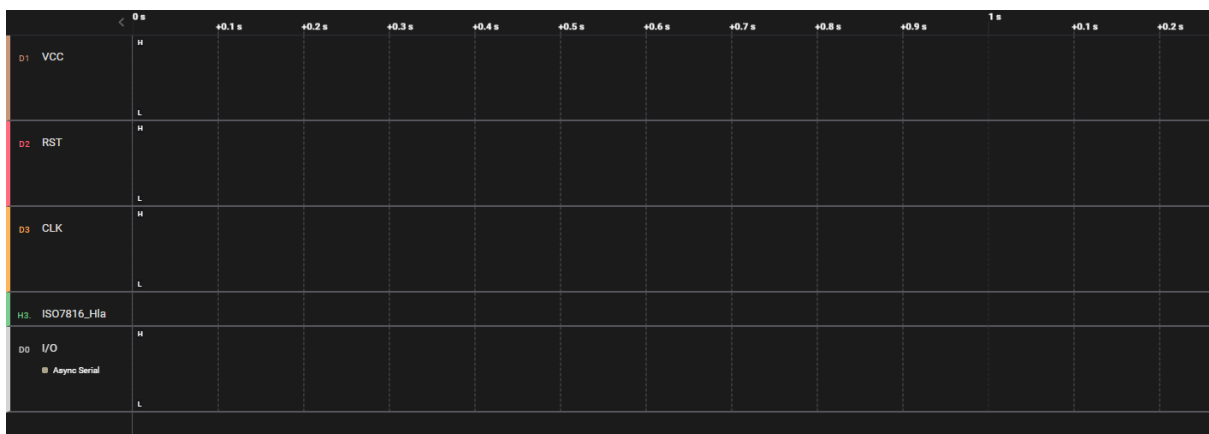


Image 9 : accueil logiciel avec preset

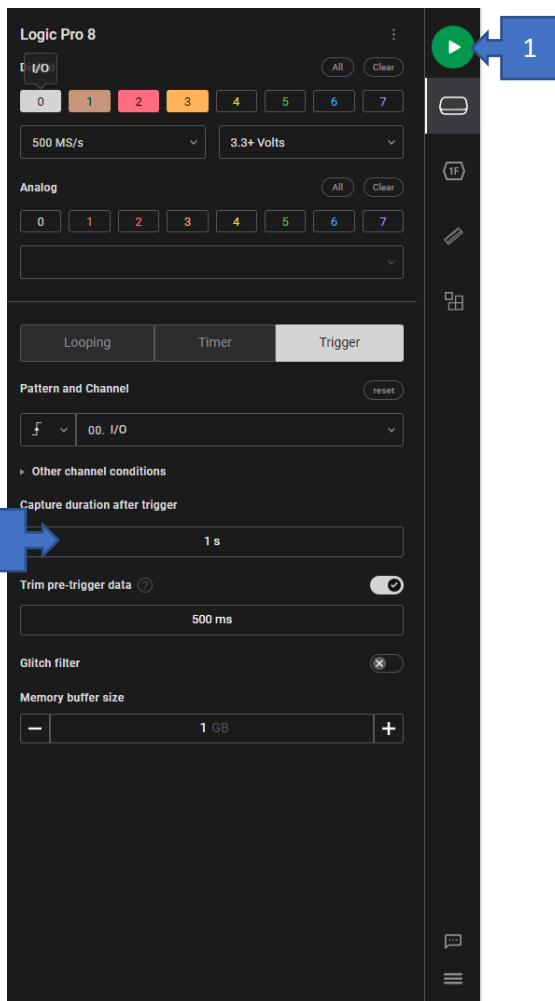


Image 10 : presets d'enregistrement

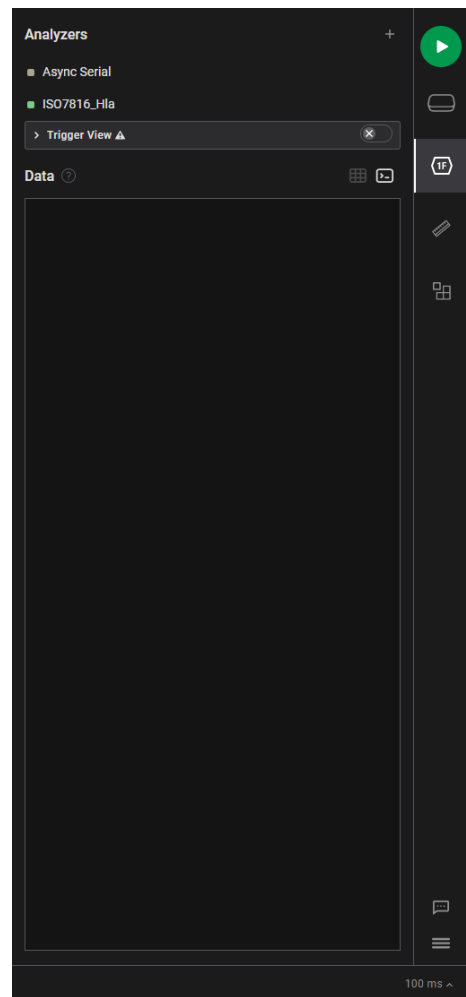
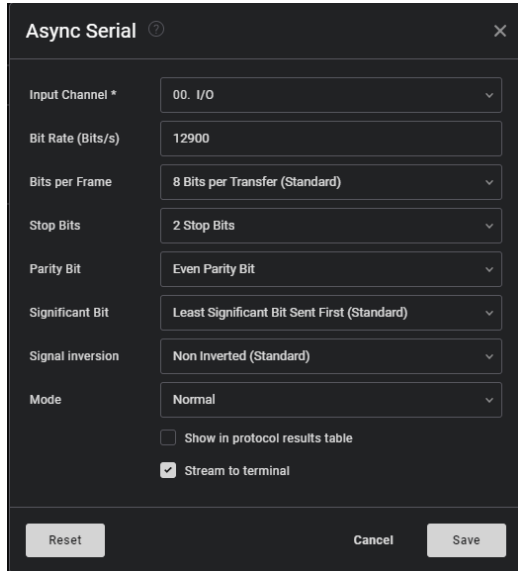


Image 11 : presets d'analyseur

Les images [12](#) et [13](#) montrent respectivement les réglages de l'analyseur Async et ISO7816_Hla, au cas où le preset n'aurait pas fonctionné.

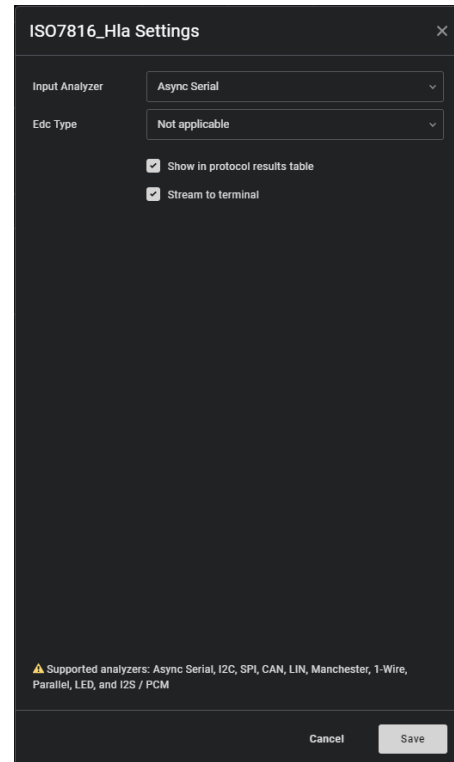


The screenshot shows the 'Async Serial' settings dialog box. It has a title bar with a question mark icon and a close button. The settings are as follows:

Setting	Value
Input Channel *	00. I/O
Bit Rate (Bits/s)	12900
Bits per Frame	8 Bits per Transfer (Standard)
Stop Bits	2 Stop Bits
Parity Bit	Even Parity Bit
Significant Bit	Least Significant Bit Sent First (Standard)
Signal inversion	Non Inverted (Standard)
Mode	Normal

At the bottom, there are two checkboxes: 'Show in protocol results table' (unchecked) and 'Stream to terminal' (checked). Below these are three buttons: 'Reset', 'Cancel', and 'Save'.

Image 12 : presets Async



The screenshot shows the 'ISO7816_Hla Settings' dialog box. It has a title bar with a close button. The settings are as follows:

Setting	Value
Input Analyzer	Async Serial
Edc Type	Not applicable

At the bottom, there are two checkboxes: 'Show in protocol results table' (checked) and 'Stream to terminal' (checked). Below these are two buttons: 'Cancel' and 'Save'.

At the very bottom, there is a small warning icon and text: 'Supported analyzers: Async Serial, I2C, SPI, CAN, LIN, Manchester, 1-Wire, Parallel, LED, and I2S / PCM'.

Image 13 : 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 10](#)). 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 10](#)).

[L'image 14](#) 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)).

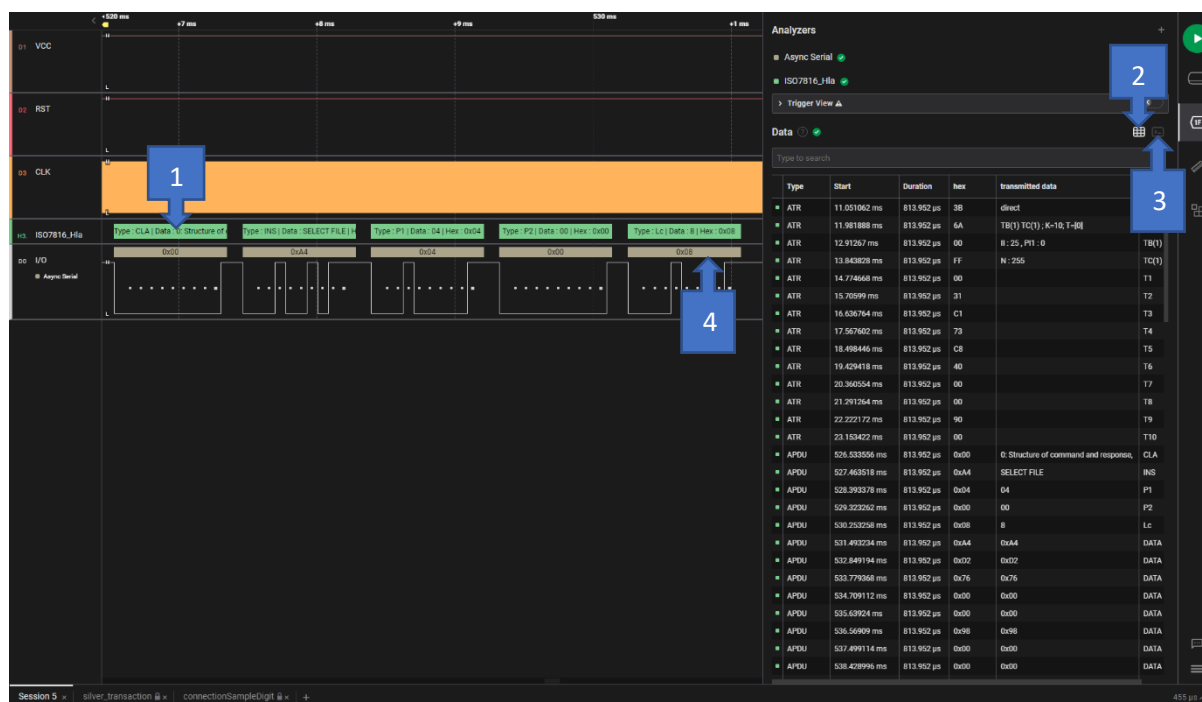


Image 14 : enregistrement iso7816, T=0

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 14](#)) 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 6](#)) : « 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 15](#)). Vous pourrez ainsi modifier ce réglage dans le champ « Edc Type » (voir [image 16](#)).

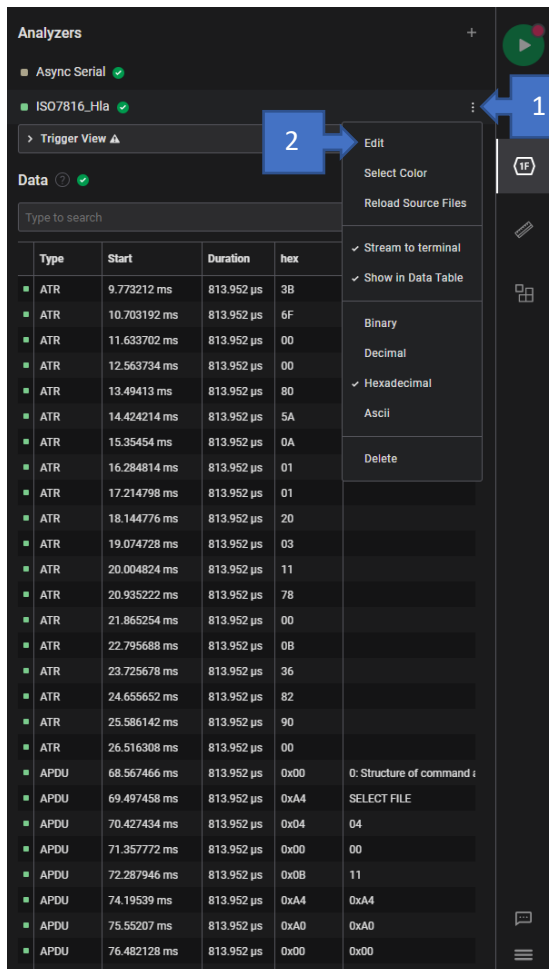


Image 15 : accéder aux réglages de l'analyseur

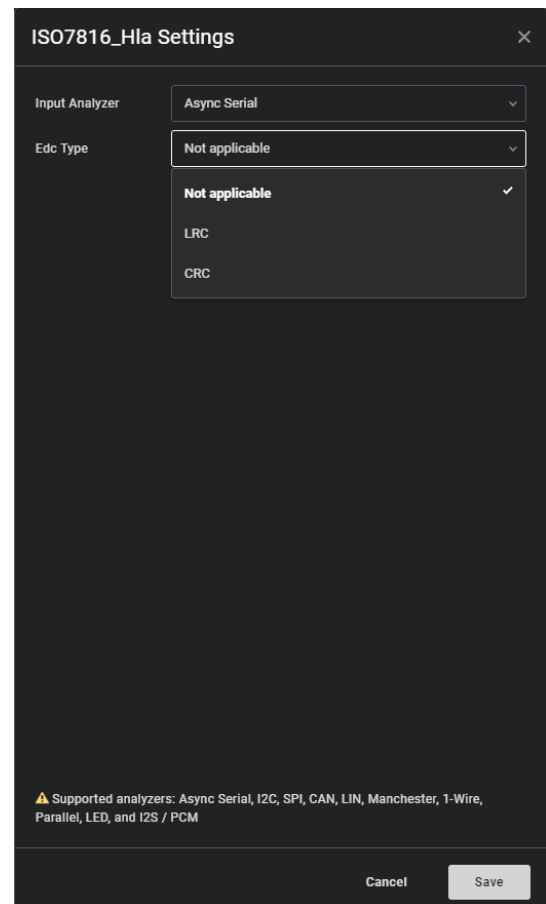


Image 16 : réglage EDC

Résolution de problèmes

Fréquence :

Si l'analyseur Async n'est pas réglé à la bonne fréquence, il se peut que l'IO soit semblable à [l'image 17](#).

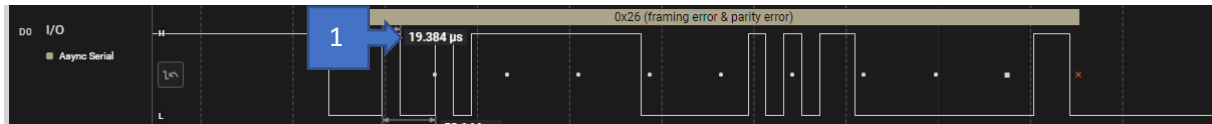


Image 17 : rectifier la fréquence 1

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 17](#)). 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 18](#), repère (1)).

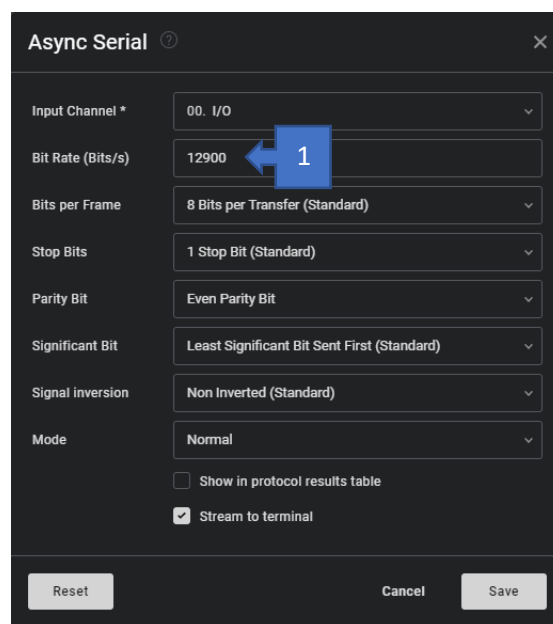


Image 18 : rectifier la fréquence 2

Cliquez sur « Save ». Si le réglage est bon, l'enregistrement devrait ressembler à celui sur [l'image 14](#).

Installation de l'extension :

Si vous ne parvenez pas à trouver l'extension dans la liste de [l'image 5](#), vous pouvez l'installer manuellement. Pour cela, suivez les indications sur le site de Saleae : <https://support.saleae.com/extensions/installing-extensions>

Le lien GitHub de l'extension est le suivant : https://github.com/SPS-R-D-RF-Organization/ISO7816_HLA

Pour aller plus loin

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

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