Décoder l’ISO7816 avec Saleae

Table des matières

[Introduction 3](#_Toc141261911)

[Câblage 3](#_Toc141261912)

[Utilisation du logiciel 4](#_Toc141261913)

[Premier enregistrement 9](#_Toc141261914)

[Spécificités de T=1 10](#_Toc141261915)

[Résolution de problèmes 11](#_Toc141261916)

[Fréquence : 11](#_Toc141261917)

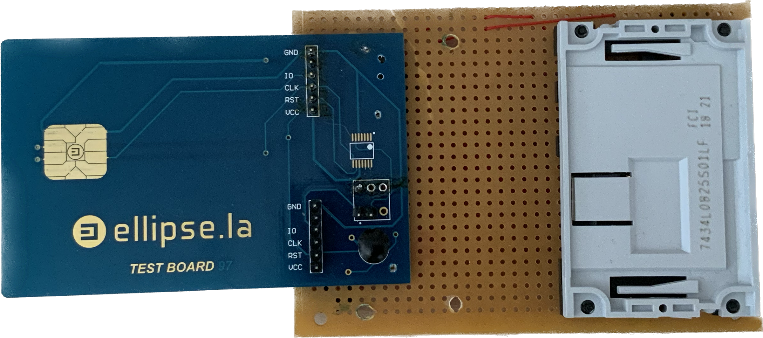
[Installation de l’extension : 11](#_Toc141261918)

[Pour aller plus loin 12](#_Toc141261919)

# 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](#Image1_bridge)),
* Un boitier type Saleae Logic Pro 8 (voir [image 2](#image2)),
* Une image contenant Appareils électroniques, Appareil électronique

  Description générée automatiquementLe 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 |

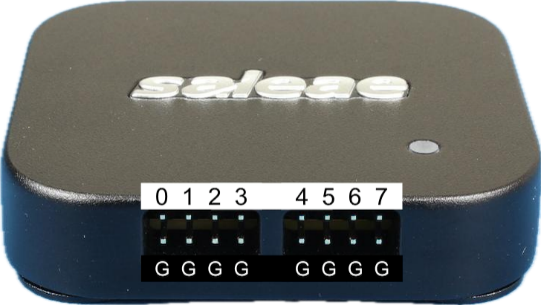


Image 3 : pins Logic Pro 8

Il est important de réaliser ce branchement précis afin d’utiliser les préréglages 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 boitier Logic Pro 8 à l’ordinateur.
* Ouvrir le logiciel Saleae Logic 2 (logo ).

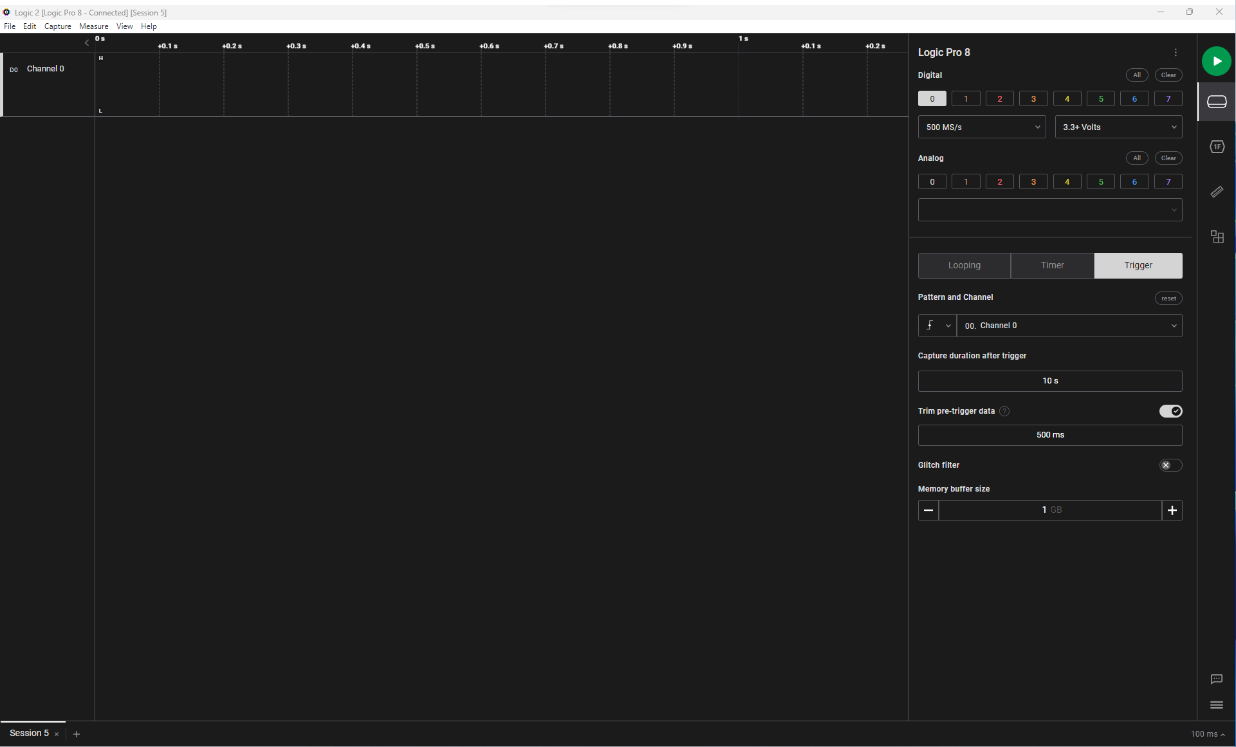


Image 4 : accueil Saleae Logic 2

* Ouvrir l’onglet « Extensions » ([Image 5](#image5), repère (1)).
* Rechercher l’extension « ISO7816\_Hla » puis cliquez sur « INSTALL » ([image 5](#image5), repère (2)).

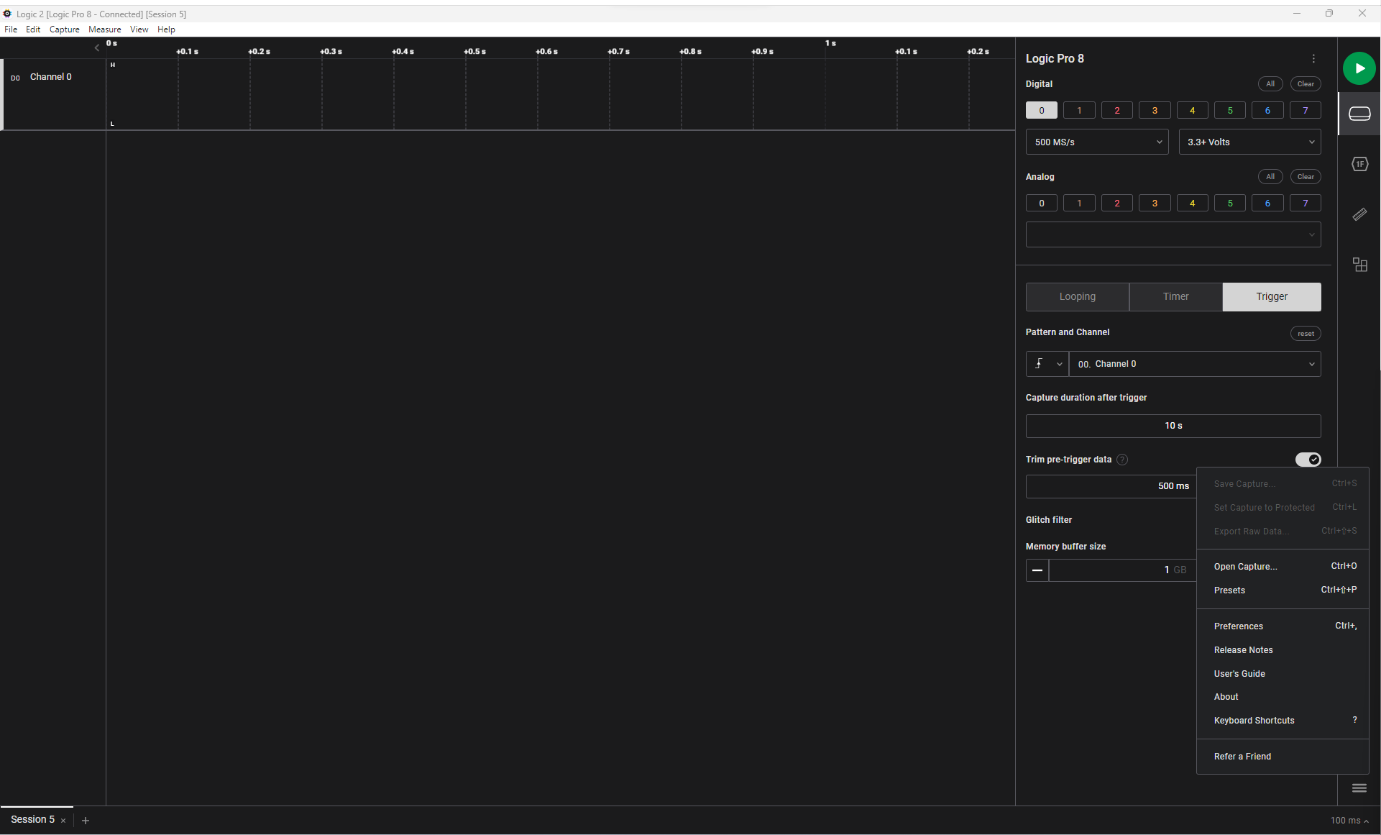
Image 5 : installer une extension

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

2

1

* 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](#image6).

1

2

Image 6 : réglages de preset

* Cliquer sur « import », (1) sur [l’image 7](#image7). Puis choisir et ouvrir le fichier « ISO7816 reading preset.logic2Preset »

Une image contenant texte, capture d’écran

Description générée automatiquement

Image 7 : ajouter un preset

1

* Une nouvelle ligne devrait apparaitre dans la fenêtre d’ajout de presets. En passant la souris sur cette ligne, « Load » apparaitra. Cliquer sur « Load ».

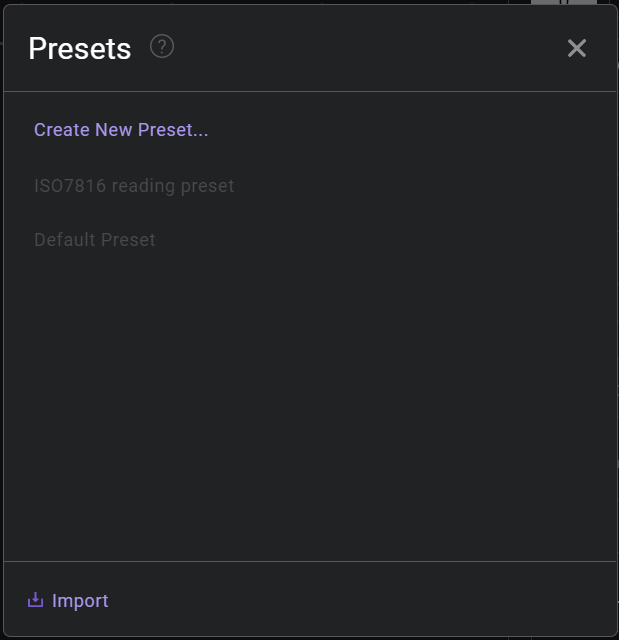


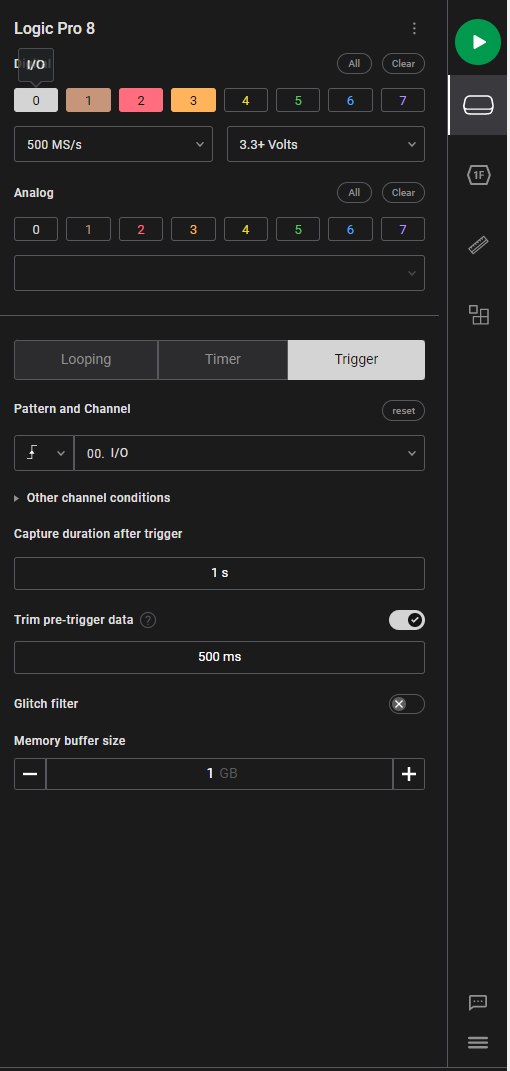
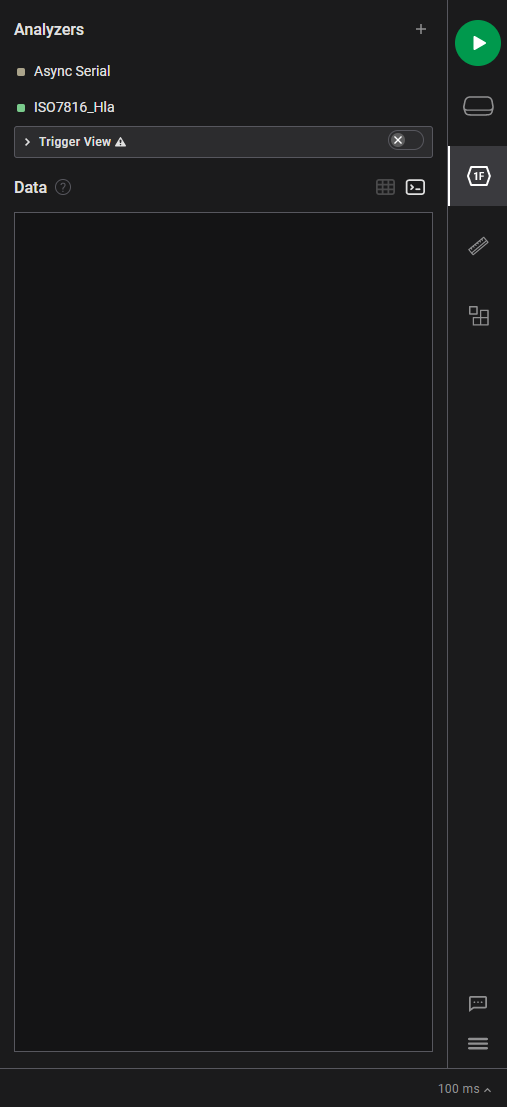
Image 8 : preset ajouté

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](#image9), [10](#image10) et [11](#image11) montrent la page d’accueil du logiciel après le chargement du preset.

Une image contenant capture d’écran, texte, ligne

Description générée automatiquement

Image 9 : accueil logiciel avec preset

2

1

Image 11 : presets d’analyseur

Image 10 : presets d’enregistrement

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquementUne image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement Les images [12](#image12) et [13](#image13) montrent respectivement les réglages de l’analyseur Async et ISO7816\_Hla, au cas où le preset n’aurait pas fonctionné.

Image 13 : presets ISO7816\_Hla

Image 12 : presets Async

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](#image10)). 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](#image10)).

[L’image 14](#image14) 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)).

Une image contenant capture d’écran, texte, logiciel, Logiciel multimédia

Description générée automatiquement

3

2

4

1

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](#image14)) 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](#image6)) : « Save capture… ».

# Spécificités de T=1

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquementUne image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement 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](#image15)). Vous pourrez ainsi modifier ce réglage dans le champ « Edc Type » (voir [image 16](#image16)).

2

1

Image 16 : réglage EDC

Image 15 : accéder aux réglages de l’analyseur

# 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](#image17).

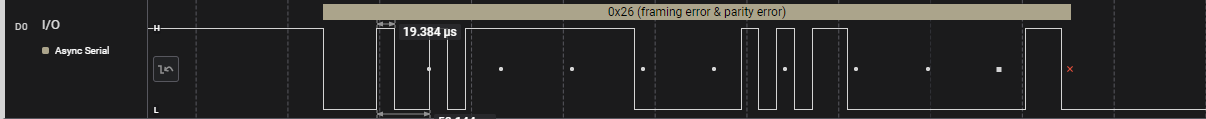


Image 17 : rectifier la fréquence 1

1

Une image contenant texte, capture d’écran, Police

Description générée automatiquement Il va falloir calculer la fréquence utilisée dans votre enregistrement. Pour ce faire, cherchez le bit le plus court et notez sa durée . Sur notre exemple, la durée est (voir repère (1), [image 17](#image17)). La fréquence étant l’inverse de la durée, vous devez calculer . Dans notre exemple, nous avons donc . Ouvrez les réglages de l’analyseur Async et saisissez la fréquence calculée dans le champ « Bit Rate » ([image 18](#image18), repère (1)).

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](#image14).

## Installation de l’extension :

Si vous ne parvenez pas à trouver l’extension dans la liste de [l’image 5](#image5), 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>