附件8：如何解析和破解CAN协议—未知协议（内部私有协议）

使用说明书

说明书版本：V2.03

更新日期：2018.10.24

汽车私有协议（其它工业设备私有协议的破解方法类似）

汽车CAN总线上的数据，除了部分符合ISO15765、J1939等标准协议外，其余的CAN数据基本走的是汽车厂家的私有协议（厂家在根据自身需要，内部定义使用的协议）。该协议一般只有汽车厂家掌握，一般用PDF或是DBC格式文件描述。当然，部分前装或后装市场的汽车配套设备厂家与汽车原厂有合作，也会有相应的协议在手上。对于普通客户，如汽车后装市场（导航、解码器、倒车影像、倒车雷达、360全景等厂家）需要获取汽车的档位（主要是倒档）、转向灯、双闪灯、手刹、大灯等信号，那么就需要读取到原始CAN数据，然后自行分析破解。

原始数据的获取：一般除了德系车以外，汽车上面一般都只有一条CAN总线，并且联到了汽车的OBD口CAN引脚上，波特率500K的高速CAN，这个时候可以直接在OBD口读取CAN数据。一般的德系车如大众，汽车上面有多达5-6条CAN总线，波特率100K的容错CAN与波特率500K的高速CAN都有，并且带有网关，车身数据不会在OBD口发出，所以只能到车身中的对应CAN线上读取，如：导航后是舒适CAN（100K的容错CAN）。

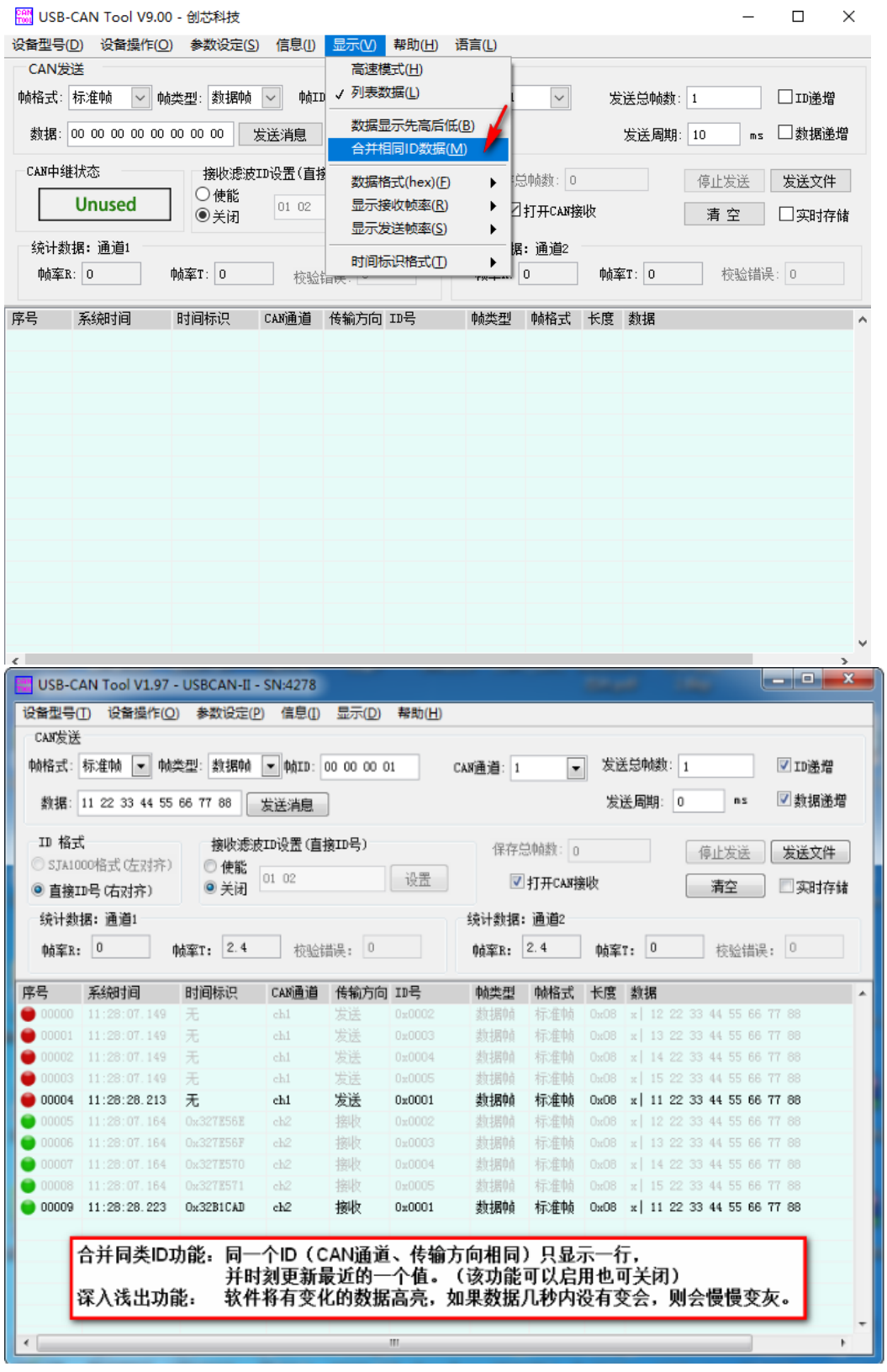
数据的处理与分析：读取到原始数据后，一般原始数据流量都比较大，要找到对应的ID与数据位比较难，本文档主要介绍几个实用的功能，辅助分析。

1、USB_CAN TOOL 原厂调试工具的合并相同 ID 与深入浅出功能

USB_CAN TOOL软件的基本操作请参考《3.USB-CAN Tool调试软件安装与使用说明书.pdf》，这里不再赘述。接收到原始CAN数据后，点击菜单上的“显示”列表下的“合并相同ID数据”选项。合并相同ID与深入浅出功能即启动。

合并同类ID功能：一个设备一般发送有限个ID数据，同ID的数据代表的意义相同，一般调试只需要关注当前（最后）的一帧数据。

深入浅出功能：运用该功能时，软件会将同一个ID有数据更新时高亮（还是黑色），对于5秒内没有变化的ID，该ID所在行会变灰。更新是指，总线上面出现ID相同的数据，不管数据位是否有变化。这对于破解未知协议时，可以帮助用户快速完成变量识别工作。



2、周立功 CANTest、CANPro 软件的变化数据“标红”功能

用户使用CANTest或CANPro1.50时，只需替换ControlCAN.dll等库文件（参考：如何兼容

使用周立功CANTest/CANpro1.50软件.pdf），并选择型号：USBCAN-2E-U即可。

CANpro1.50功能比较丰富，这里以CANpro1.50为例。

打开CANpro1.50软件，选择USBCAN-2E-U接口卡，并且选定总线的波特率（以实际波特率为准，汽车CAN总线一般为500K），点击确定并启动，启动CAN接口卡。如图2所示；

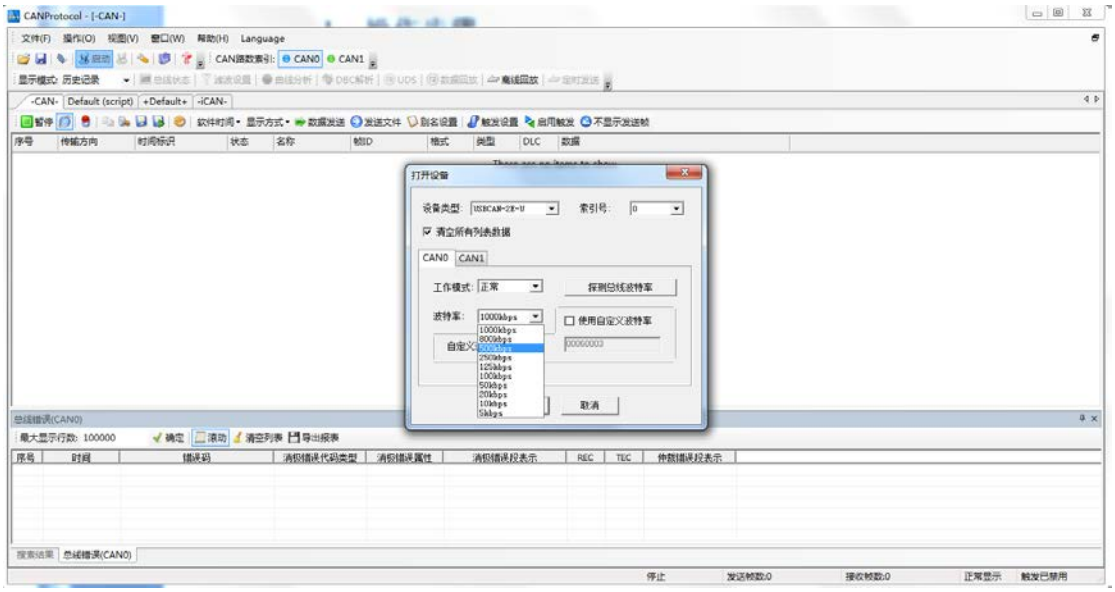


图 2 打开CANpro软件初始化

点击菜单快捷操作中的DBC解析按钮，进入DBC解析界面，如图3所示；

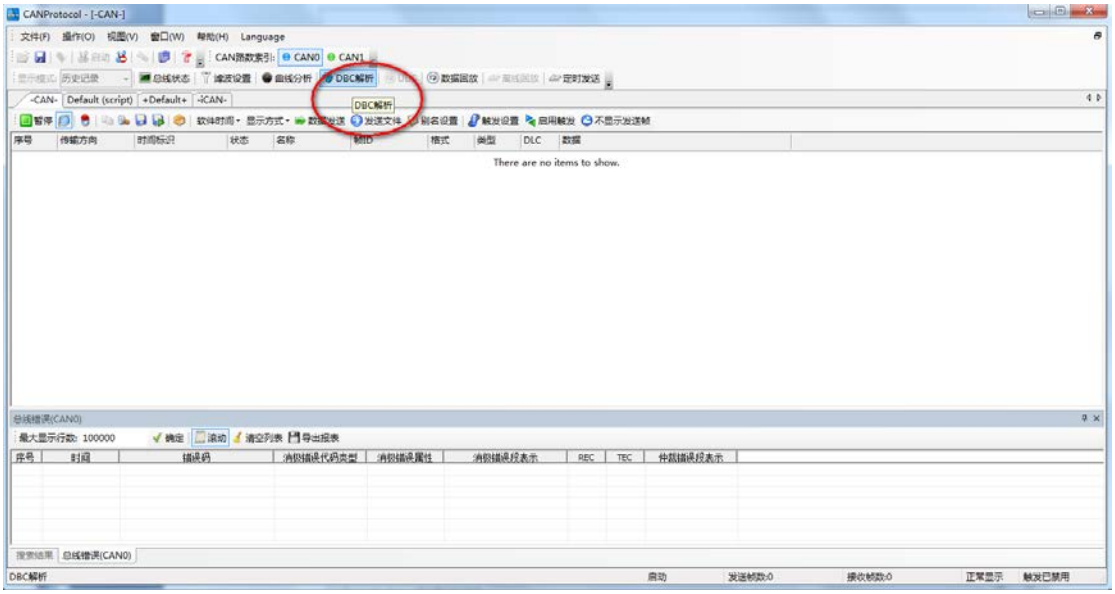


图 3 打开DBC解析

DBC解析界面中，小技巧：运用分类显示功能时，软件会将有变化的数据“标红”，这样对于破解未知协议时，可以帮助用户快速完成变量识别工作。比如，要想知道方向盘所对应CANID和数据段，即可使用此方法运行，转动方向盘，观察变红的变量，即对应。

“标红”需要启用“分类显示”功能，“标红”以字节为单位，只要该字节中任意位变化都会“标红”整个字节。

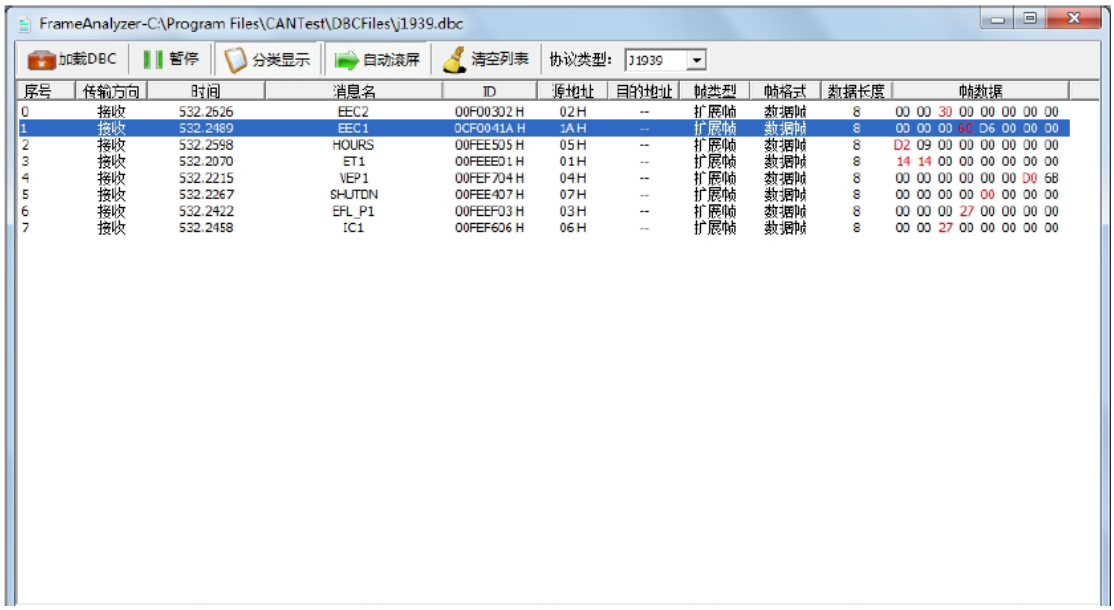


图 5 DBC协议解析结果

3、应用范围

- 工业控制测试
- 汽车电子维护维修
- 协议破解