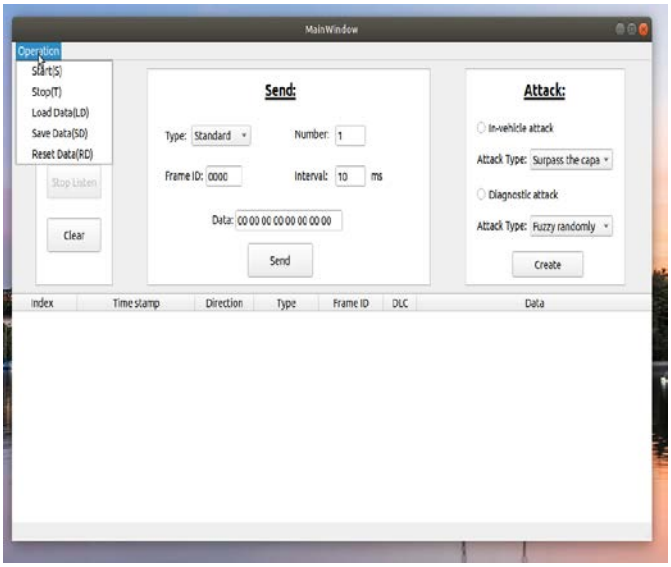
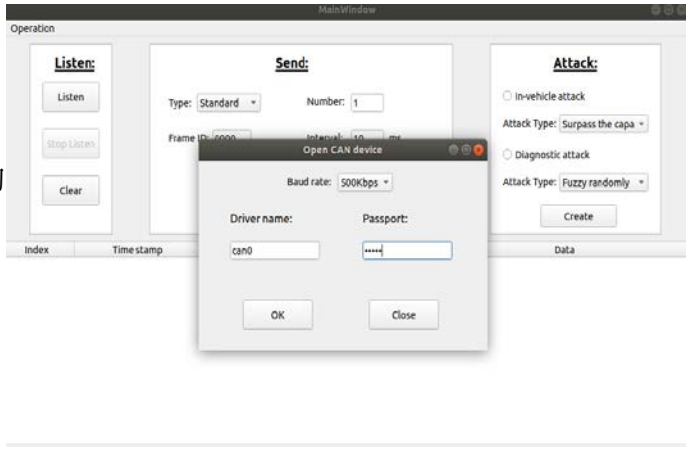
攻击工具使用 Python + PYQT5 来写的，基本的功能都已经完成了，而且所有可以选择的参数我们都给用户自己做选择。
而且我们已经在其他的 ubuntu 电脑上试验过了，生成的可执行文件在没有 QT 的环境下也可以运行。
由于图片比较大，所有我们就选择几个有特征的、普遍的界面介绍一下。

主界面：
在这个界面中可以完成一般 CAN 分析仪界面中常用的功能，就是监听 CAN 总线以及往 CAN 总线上发送消息。即 Listen 和 send 部分。最右边的 Attack 是我们所要设计的攻击部分的进入界面。

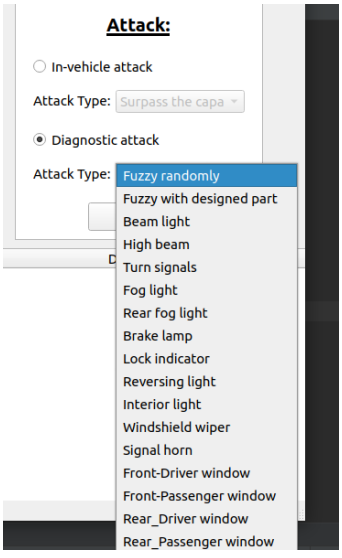


左上角有 5 个选项：
分别是建立连接、关闭连接、加载数据、保存数据和清空现有数据。加载数据和保存数据可以为后面具体的攻击所使用。

建立连接:
其中建立连接是通过 ubuntu 的命令完成连接的这也是如果需要跨平台唯一需要考虑的地方。
其中可以自由选择 CAN 接口名称，连接速度，由于需要直接创建接口，所以需要输入 sudo 的密码。

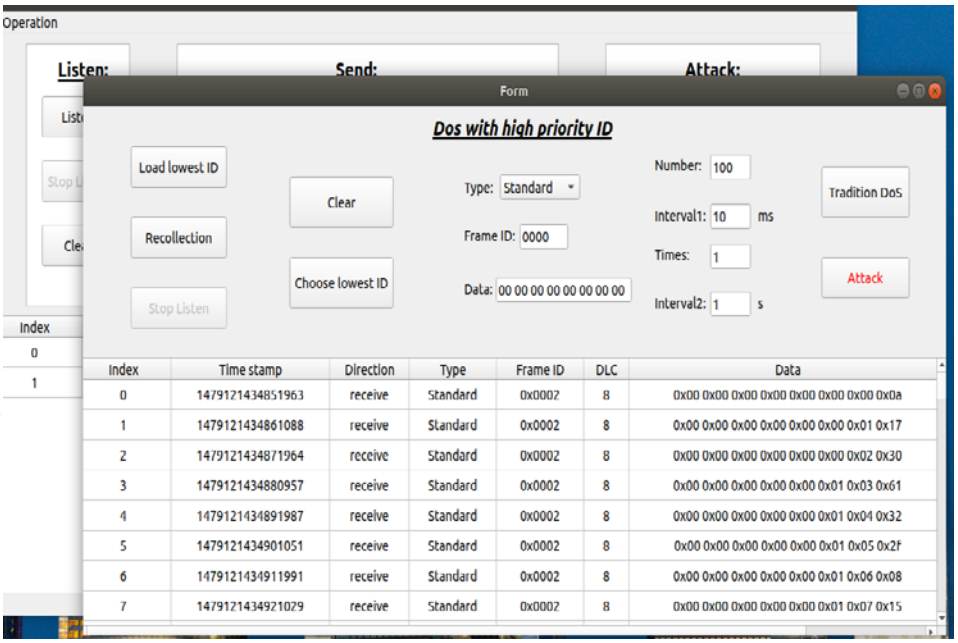


攻击选项：
接收和发送命令是使用单独的线程来完成的，这部分直接跳过。
我们通过选择不同的攻击选项，来进入不同的攻击界面。
右图中可以看到我们分为车内攻击和诊断攻击两部分。每部分又有不同的选项分类。接下来我会介绍几个典型的界面：



高优先级的 DoS

首先这里可以使用最基础的传统的 ID 为 0000 的 DoS，就是最右边的 Traditional DoS 攻击。当然，我们也可以直接修改想要的数据，例如 0x002 来做 DoS。



同时，我们也会寻找所有已经收到(包括加载的之前监听到的)和在这个界面重新收集到的数据

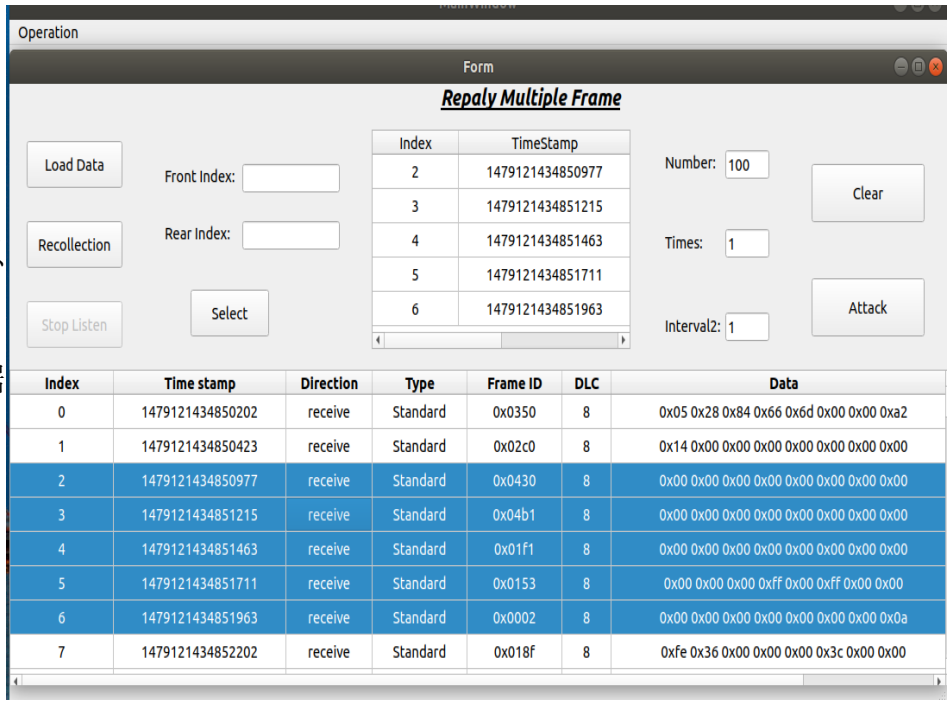
并且针对发送的攻击数据包，我们定义了发送的数量、发送的间隔、总共发送几轮以及每一轮之间需要间隔多少时间。

多帧重放

简单的单帧重放就不做赘述了。

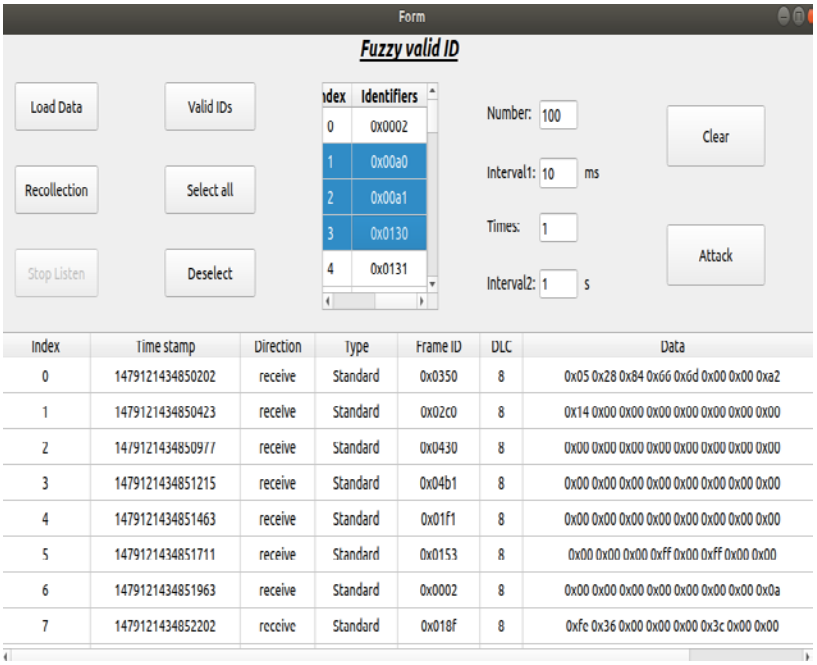
多帧重放我们首先记录的加载、监听到的数据。然后在这些数据中可以随意选择想要重放的数据(可以单独点击不连续的数据或者直接通过索引选择连续的数据)来作为攻击的数据块。

在这个攻击中，每个数据包之间的间隔是固定的，所以我们定义发送数据块的个数和轮次。



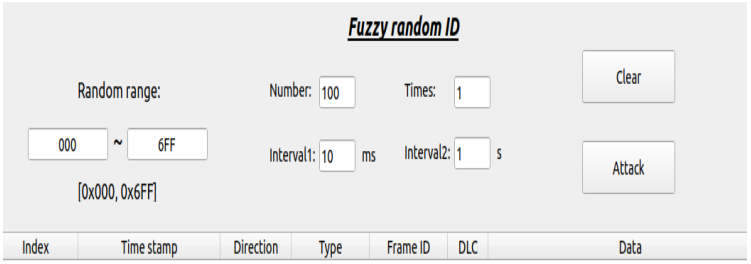
Fuzzy 有效 ID

这里会先收集所有监听和加载数据的 ID，用户可以自由地选择想要发送的随机 ID，然后根据用户自己设置好的参数来发送攻击。



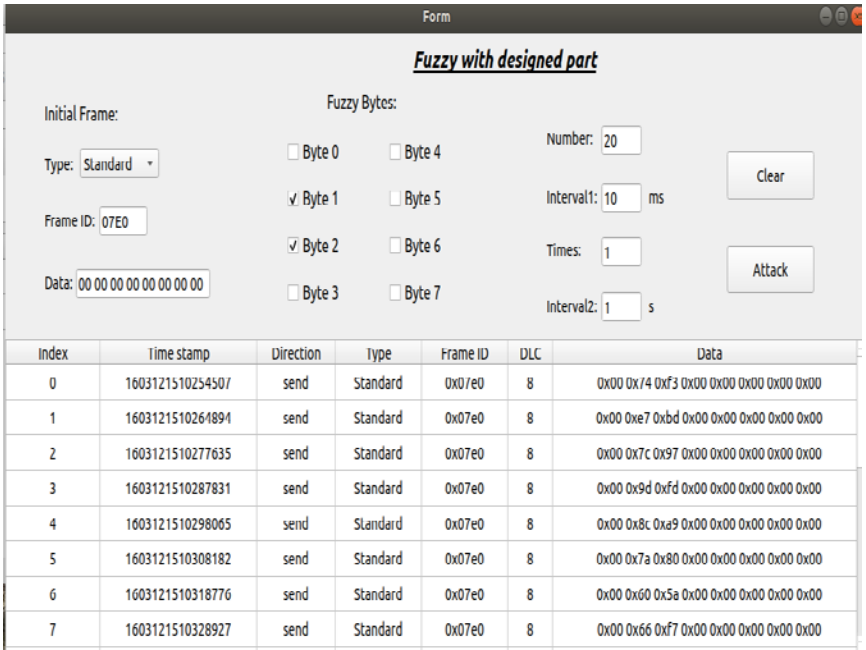
Fuzzy 随机 ID

这个攻击很简单，就是用户自己选择随机的 ID 范围和发送参数，就可以发动攻击了。



Fuzzy 诊断攻击中的特殊部分

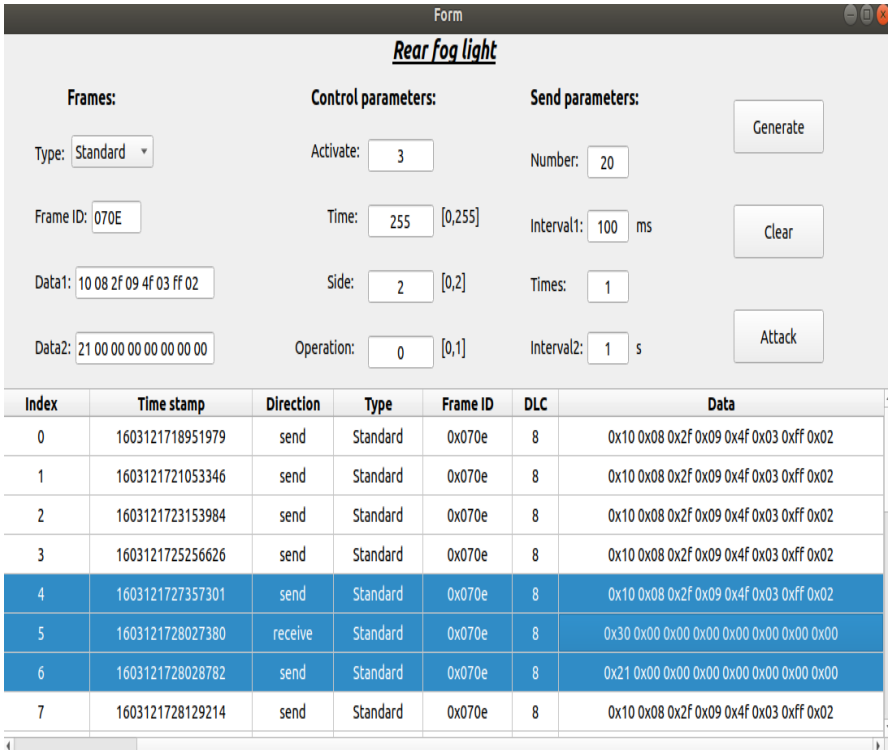
由于有些攻击这想要针对某些 ID 的特殊字节来进行 fuzzy 测试，所以我们可以直接在基础消息的基础上，直接选择想要 fuzzy 的字节。



诊断控制攻击

首先针对每一种攻击，我们都会有各种默认的攻击命令，但是同时用户可以根据自己的需求设计不同的参数，生成不同的攻击数据，然后根据发送参数发出。

诊断攻击比较特殊的地方是大部分的攻击命令都是多帧的，所以这里需要涉及特殊的多帧传输过程。以图中数据被选择的数据为例，只有当另一端发送流控帧之后，后面的多帧才能按照流控帧的指示发送。



Index	Time stamp	Direction	Type	Frame ID	DLC	Data
0	1603121718951979	send	Standard	0x070e	8	0x10 0x08 0x2f 0x09 0x4f 0x03 0xff 0x02
1	1603121721053346	send	Standard	0x070e	8	0x10 0x08 0x2f 0x09 0x4f 0x03 0xff 0x02
2	1603121723153984	send	Standard	0x070e	8	0x10 0x08 0x2f 0x09 0x4f 0x03 0xff 0x02
3	1603121725256626	send	Standard	0x070e	8	0x10 0x08 0x2f 0x09 0x4f 0x03 0xff 0x02
4	1603121727357301	send	Standard	0x070e	8	0x10 0x08 0x2f 0x09 0x4f 0x03 0xff 0x02
5	1603121728027380	receive	Standard	0x070e	8	0x30 0x00 0x00 0x00 0x00 0x00 0x00 0x00
6	1603121728028782	send	Standard	0x070e	8	0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
7	1603121728129214	send	Standard	0x070e	8	0x10 0x08 0x2f 0x09 0x4f 0x03 0xff 0x02

剩下的攻击界面都是类似的功能，所以就不在过多展示了。总共有 25 个攻击界面选项，每种攻击界面里面都为用户提供了自由的参数选择，所以攻击的自由度还是挺高的。