Nebu1ea 韩磊 [1504895347@qq.com](mailto:1504895347@qq.com)

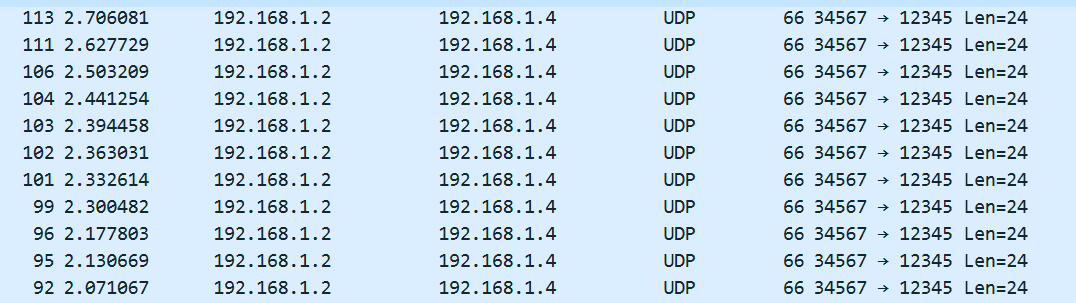
Misc:工业互联网模拟仿真数据分析

解题思路：

跟着问题一步一步来，

首先第一题：在某些网络会话中，数据包可能保持固定大小，请给出含有此确定性特征的会话IP地址和数据包字节大小值。

用wireshark打开后把ip排序寻找数据包lenth长度相同的一段包，结果找到如下：

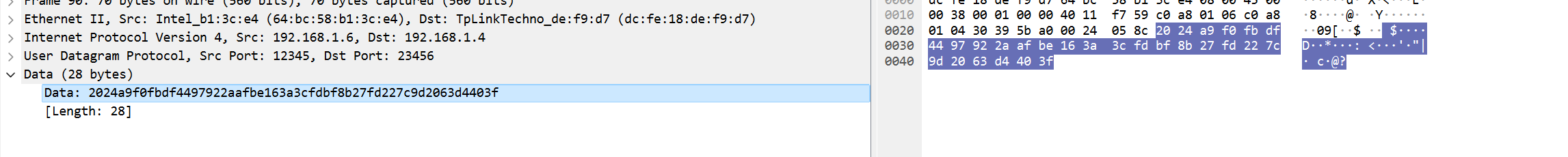


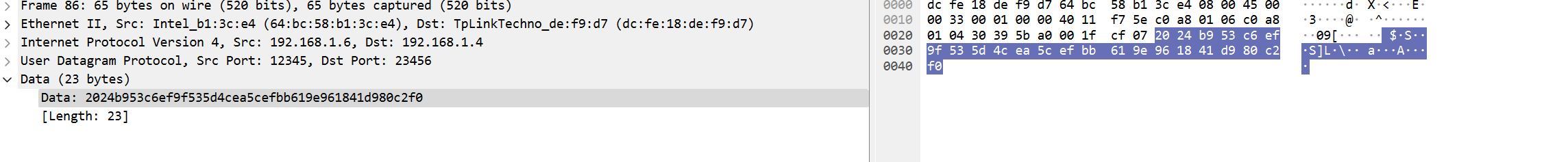
这一段就符合规则，于是第一题的答案就是：192.168.1.2,192.168.1.4,24

接着第二题:

通信包数据某些字段可能为确定的，请给出确定字节数值。

我们一个一个数据包看，发现发送的数据包中Data有嫌疑：

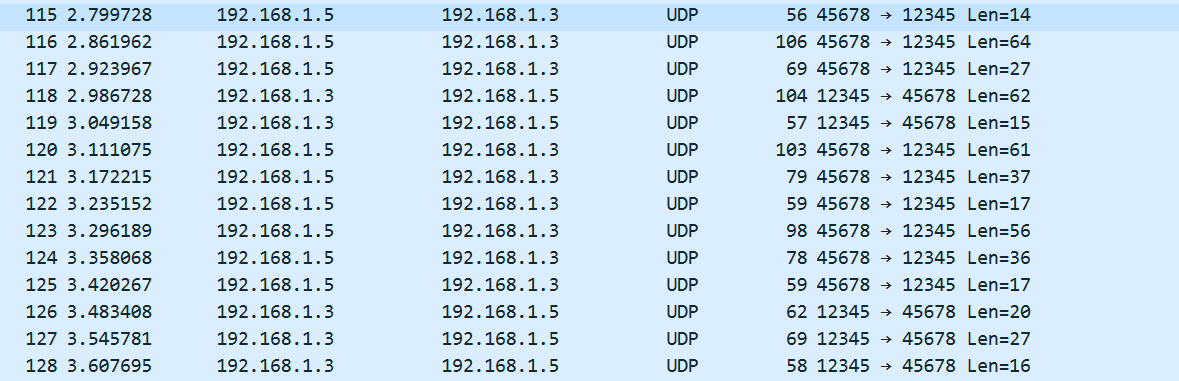




再往下慢慢看，发现data全是2024开头的，结合题目，即可推断出确定的字节数值即为2024。于是第二题的答案为2024

接着第三题: 一些网络通信业务在时间序列上有确定性规律，请提供涉及的IP地址及时间规律数值（**小数点后两位**）

正常在业务通信时的数据包一般的时间差不会太大，若是有时间规律，那大概率为等差数列规律，那我们把time给排序慢慢往下看，发现从115号包开始就有规律了：



每一个发包的间隔都稳定在0.059-0.061秒之间，去除网络误差大概是0.06秒，正好符合等差数列，那记录他们的ip即为答案。于是第三题的答案为192.168.1.3,192.168.1.5,0.06

接着第四题：一些网络通信业务存在逻辑关联性，请提供涉及的IP地址

我们把ip排序，发现192.168.1.1与192.168.1.5和192.168.1.4是单向业务管理，即一对一，不存在业务间关系，所以排除，接着看192.168.1.2，192.168.1.3，192.168.1.6之间互相传递数据包，之间的业务种类肯定大于等于2，所以理应具备逻辑关联性，所以第四题的答案是：192.168.1.2, 192.168.1.3, 192.168.1.6

最后是第五题：网络数据包往往会添加数据完整性校验值，请分析出数据校验算法名称及校验值在数据包的起始位和结束位（倒数位）

提示了数据校验算法是5个字符，英文字母大写，那就该猜到CRC16和CRC32

在经过观察测试后得出，结束位是1，起始位为4，算法为CRC16

那么第五题的答案为CRC16,4,1

最后把五道题的答案放到flag.py里跑就行了