背景：在一个封闭的工业互联网环境中，网络传输行为往往具有确定性的特点，即网络数据和部分业务场景为固定模式。这种“白名单”可加以挖掘利用，用于检测工业互联网中发生的网络攻击异常事件。与传统基于漏洞“黑名单”的检测方法不同，基于“白名单”的检测方法能够检测从未发生过的未知攻击。

题目：如下为某个工业互联网执行相关功能时的一段时间模拟仿真网络流量（pcap文件），请通过分析网络流量数据，提取出确定性白名单规则，用于攻击检测。检测规则示例：网络中的终端MAC地址只能是64:bc:58:b1:3c:e4和dc:fe:18:de:f9:d7，只要检测到其他MAC地址都认定为非法异常流量。

软件工具：安装wireshark打开pcap文件。

题目说明：所模拟的工业互联网流量文件中，共设计构造了若干种确定性白名单规则，该规则集合均来自于电力、航天、汽车等网络真实场景。本题一共5道小题，采用填空题的形式，选手完成所有的填空之后，将所有答案使用flag.py使用生成一个最终flag，每个答案之间使用英文逗号隔开。选手最终只需要提交由flag.py生成的md5加密后的字符串。

附：白名单规则目录（题目+答案格式，下划线部分为所填答案）

1. 题目一：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。

答案：IP地址：XX.XX.XX.XX，XX.XX.XX.XX，…，数值：XX

（补充说明：IP顺序从小到大排列，涉及的IP个数由选手自己判断）

1. 题目二：通信包数据某些字段可能为确定的，请给出确定字节数值。

答案：XX

1. 题目三：一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**）

答案：IP地址：XX.XX.XX.XX，XX.XX.XX.XX，…，数值：XX

（补充说明：IP顺序从小到大排列，涉及的IP个数由选手自己判断）

1. 题目四：一些网络通信业务存在逻辑关联性，请提供涉及的IP地址

答案：XX.XX.XX.XX，XX.XX.XX.XX，…

（补充说明：IP顺序从小到大排列，涉及的IP个数由选手自己判断）

1. 题目五：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）

答案：XXXXX，X，X

（补充说明：数据校验算法名称长度为5个字符，其中英文字母大写）