大作业

- 分组完成以下工作，每3~5人一组，提交报告时注明小组成员的姓名、学号及分工

1. 用tcpdump收集某个主机或者路由器所连接的某个物理网络上的traffic，存放到文件中以备进一步分析使用。收集流量的时间长短可以选择三种规格之一：A. 5分钟；B. 15分钟；C. 1小时
2. 编写程序处理原始数据文件，整理成你认为方便处理的数据格式（纯文本）
3. 利用Matlab或其它工具，或自行编写程序，分别就进出两个方向上的traffic，至少分析以下特征：
   1) 给出IP分组携带不同协议的载荷的饼图，分别按分组数和总数据量进行统计；
   2) 有多少IP分组是片段（fragment）？有多少IP数据报被分片？载荷为TCP和UDP的分别有多少比例的IP数据报被分片？
   3) 给出IP数据报长度的累积分布曲线，并分别比较载荷为TCP和UDP的IP数据报长度的累计分布；
   4) 分别对TCP和UDP的traffic给出端口分布的直方图，比较前10名端口上数据报长度的累计分布曲线；
   5) 对于载荷为TCP的报文，给出其中各个控制位出现的百分比。
4. 撰写一份实验报告，说明收集数据的时间、地点、工具、方法、数据结构及自行编写的程序源代码；给出所绘制的数据表格、图形及曲线，并注明分析的对象并归纳可能得到的结论；报告应包含原始数据用tcpdump不带-x参数读出的最初1000行和最末1000行作为附录。