开发一个wireshark离线包分析工具的具体需求。

=============分隔符，下面是需求=========================

（基于wireshark定制脚本的实现方式，红色字体标注部分需要重点做些前期方案的调研和设计，作为关键功能实现方案需要讨论需求）

1. 针对用户行为的分析：

可做：终端平台类型的统计；浏览器类型的统计；

不可做：基于IP的在线用户统计；基于URL关键字段匹配的统计，以及相关过滤条件；

在线用户个数随时间变化；用户平均在线时长随时间变化；用户GET请求到达率随时间变化；TCP会话达到率随时间变化。（不可做原因：因为在本地抓包分析，所以没有多用户访问的概念，所以这部分需求不可做）

二、针对HTTP业务流程的分析：

可做：区分针对单个网页的多个Get请求及其TCP连接会话，作为一个网页访问session，统计从第一个GET请求到最后一个200响应达到的时间差异；

针对网页访问session为单位，进行SP响应时延（从单个get请求到达到对应200响应回复）的统计，上下行流量，以及相关过滤条件（不是很清楚这个需求的意思）；

识别浏览器的pipelining和multipart优化机制使用占比、相关参数（pipelining并发度、调度方式）的统计，结合终端平台类型和浏览器类型进行关联统计，以及相关过滤条件。

识别浏览器的并发TCP连接个数，pipelining并发度、multipart并发度。

识别网页session资源的分布模型（文本、图片、视频的种类统计、个数统计、大小统计），及其过滤条件。

不可做：用户访问次数

请求到达速率随时间变化的统计（不可做原因：同上，因为在本地抓包分析，所以没有多用户访问的概念，所以这部分需求不可做）

1. 针对流量模型的分析：

可做：针对上述过滤条件的上下行流量使用和瞬时速率统计。

针对TCP会话的持续时间，全部数据和有效数据（去除连接建立和连接拆除）流量使用、瞬时速率和时间占用比例统计。

针对网页访问session的持续时间，（上下行）全部数据和有效数据（去除协议头）流量使用、瞬时速率和时间占用比例统计。

针对协议类型（应用层和传输层）的（上下行）流量使用、瞬时速率统计。

1. 针对拥塞控制的分析：

可以做：针对TCP初始窗口大小；

针对TCP会话的丢包率、RTT、数据重传概率、重传流量占比的统计；

针对链路层的包错误率、单跳时延、帧重传概率、重传流量占比的统计。

不确定：针对PCN功能标识的统计（哪些终端支持PCN拥塞控制，是否存在实际使用的PCN拥塞标识）；（不确定是因为在本地抓包分析的时候，没有大量的包去分析哪些终端支持pcn，只能知道本终端是否使用pcn标识）

**【我们的分析：下面这个是非功能性需求，应该可以满足！】**

四、实现要求：

* 基于wireshark定制脚本方式，提供源码；
* 所有统计要求，提供平均数值、最小值、最大值、Mean值的统计表格（excel表格）和图形化界面；
* 部分统计要求，提供间隔10%为步长的概率分布统计表格（excel表格）和图形化界面；
* 确保提供处理海量数据的能力，或者提供数据分段整合的解决方案。