中山大學 SUN YAT-SEN UNIVERSITY 移动网络安全技术实验报告

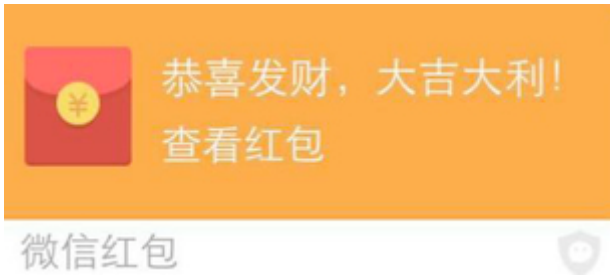
警示

1.实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2.当次小组成员成绩只计学号、姓名登录在下表中的。
3.在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
4.实验报告文件以 PDF 格式提交。

院系	数据科学与计算机学院		班 级	14M3，14C1	组长	白冰
学号	14353355	14353002				
学生	杨金华	白冰				
实验分工						
杨金华	编写抢红包安卓应用，调试验证，共同完成实验报告					
白冰	配置抓包软件环境，抓包分析数据，共同完成实验报告					

微信红包实验

【实验图标】



【实验内容】

1）通过抓包分析微信红包分发、接收的全过程，要求用抓包数据分析延迟构成、URL、红包服务器 IP 等细节内容。
2）分析群内红包发放的数据，找到红包金额分布规律、时序分布规律以及每个人多次抢到的红包金额的分布规律。
3）最后给出一个抢红包的最佳策略建议（使用数学分析方法）。
4）编写一个抢红包、拆红包的 APP。
5）如何防止外挂抢红包软件？

【实验要求】

中山大學 SUN YAT-SEN UNIVERSITY 移动网络安全技术实验报告

请根据实验内容，写出实验原理及设计方案。

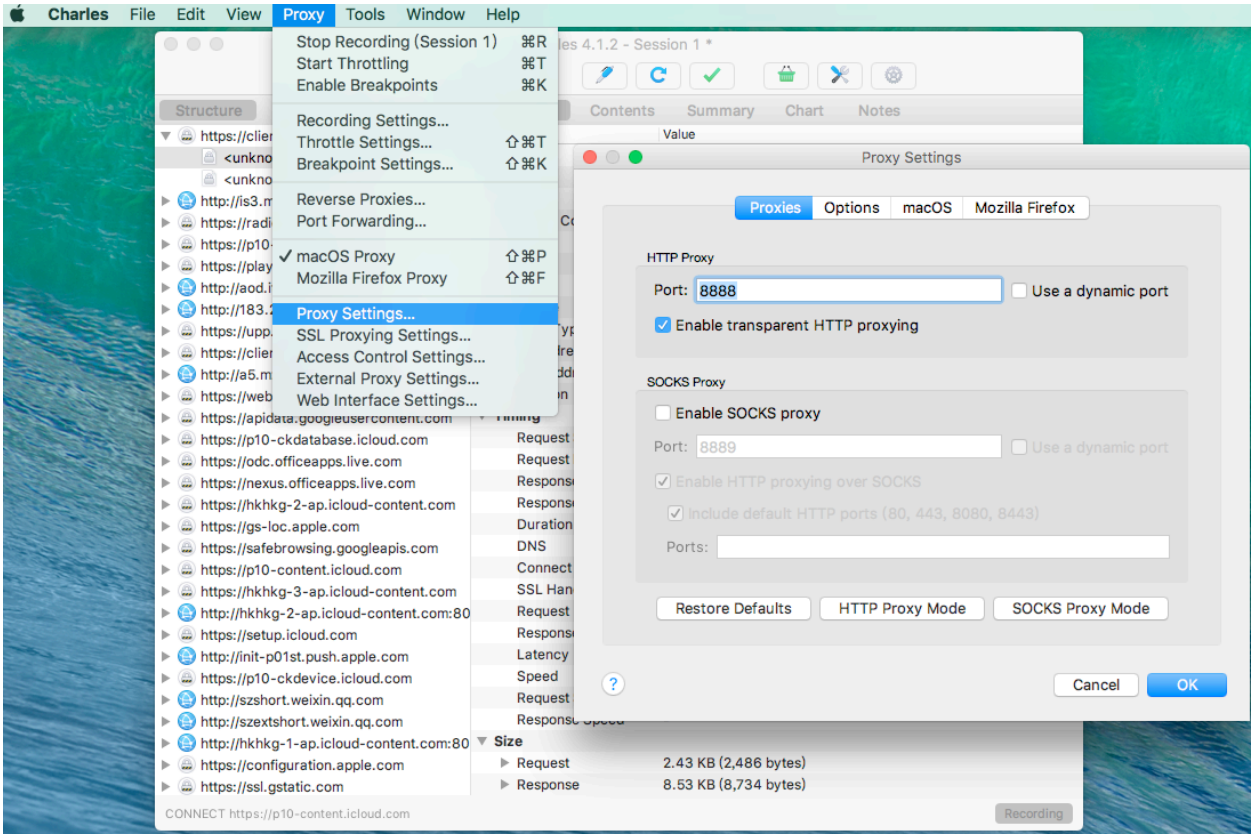
（1）使用了什么抓包工具？简述此工具的功能和抓包过程。

使用了 Charles 来抓包，
Charles 是在 Mac 或 Windows 下常用的 http 协议网络包截取工具，支持 SSL 代理，可以截取分析 SSL 的请求。

安装 Charles 的过程参考了以下博客
http://www.jianshu.com/p/9822e3f28f0a

HTTP 抓包过程：

Step 1：开启 Charleshttp 代理；



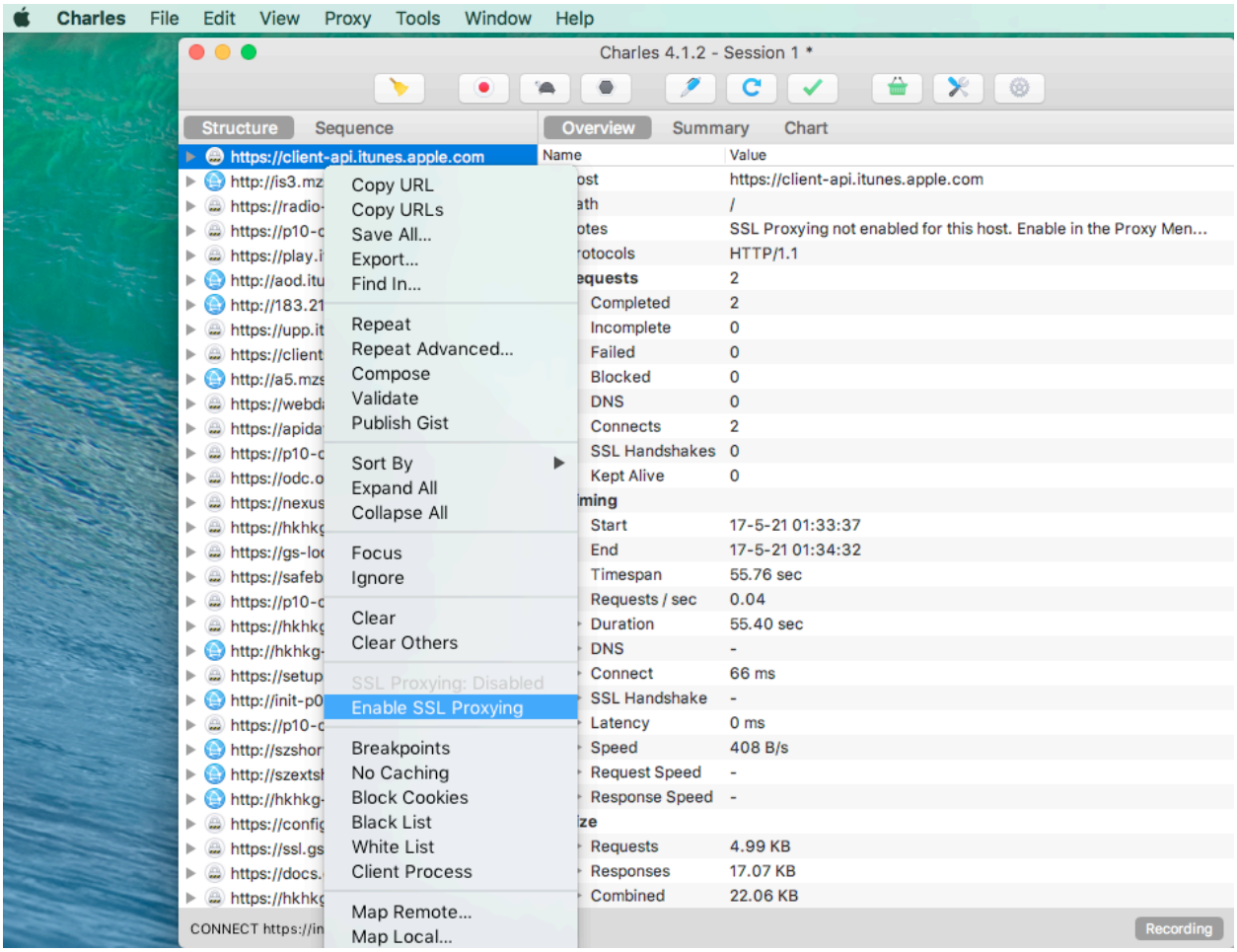
Step 2：手机端 Wifi 添加代理；
点击你所连接的 wifi，输入代理服务器的 IP 与端口，IP 即安装了 Charles 的电脑 IP 地址，端口就是前面一步设置 Charles 时所设置的端口。

Step 3：启动应用开始抓包；

Https 抓包首先需要在在手机端安装 SSL 证书：

使用 Safari 浏览器访问地址：http://www.charlesproxy.com/getssl，浏览器会下载证书并提示安装，

安装完成之后，在 Charles 中选择需要代理地址，右击，选中 Enable SSL Proxying，这样就可以抓取 HTTPS 数据包了。



Step 4：分析抓取的数据包。

（2）分析抓到包，那些数据是抢红包、拆红包的关键？请给出截图。

我请一个同学给我发红包，我在手机上的操作如下

打开微信，提醒同学发红包给我，收到红包的消息提示（图 1）；点击消息，弹出红包界面（图 2），捕获到数据包（图 4）

图 1

图 2

图 3

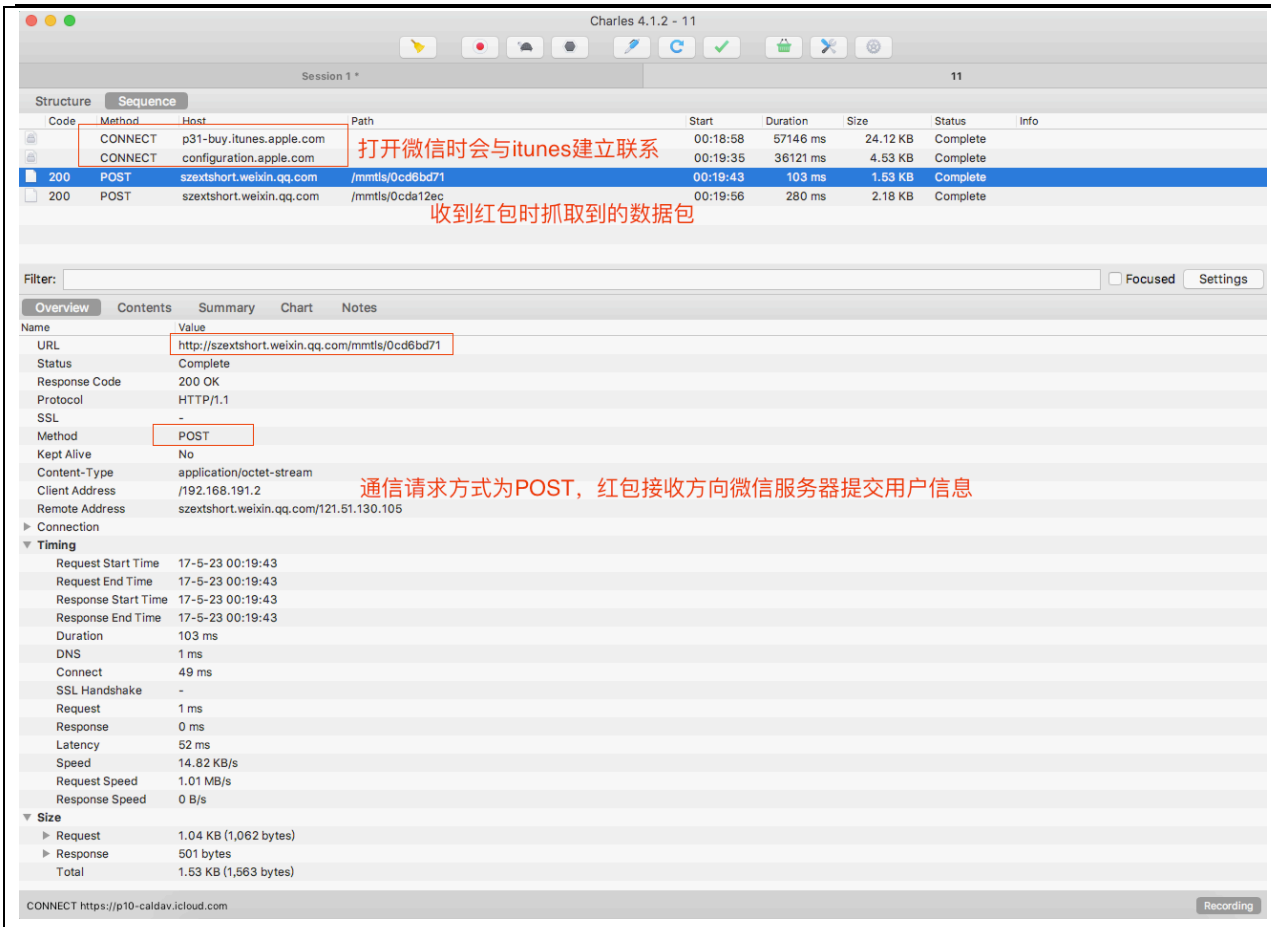


图 4

点击拆红包，出现红包金额（图 3），此时又会收到一个数据包，下图 5

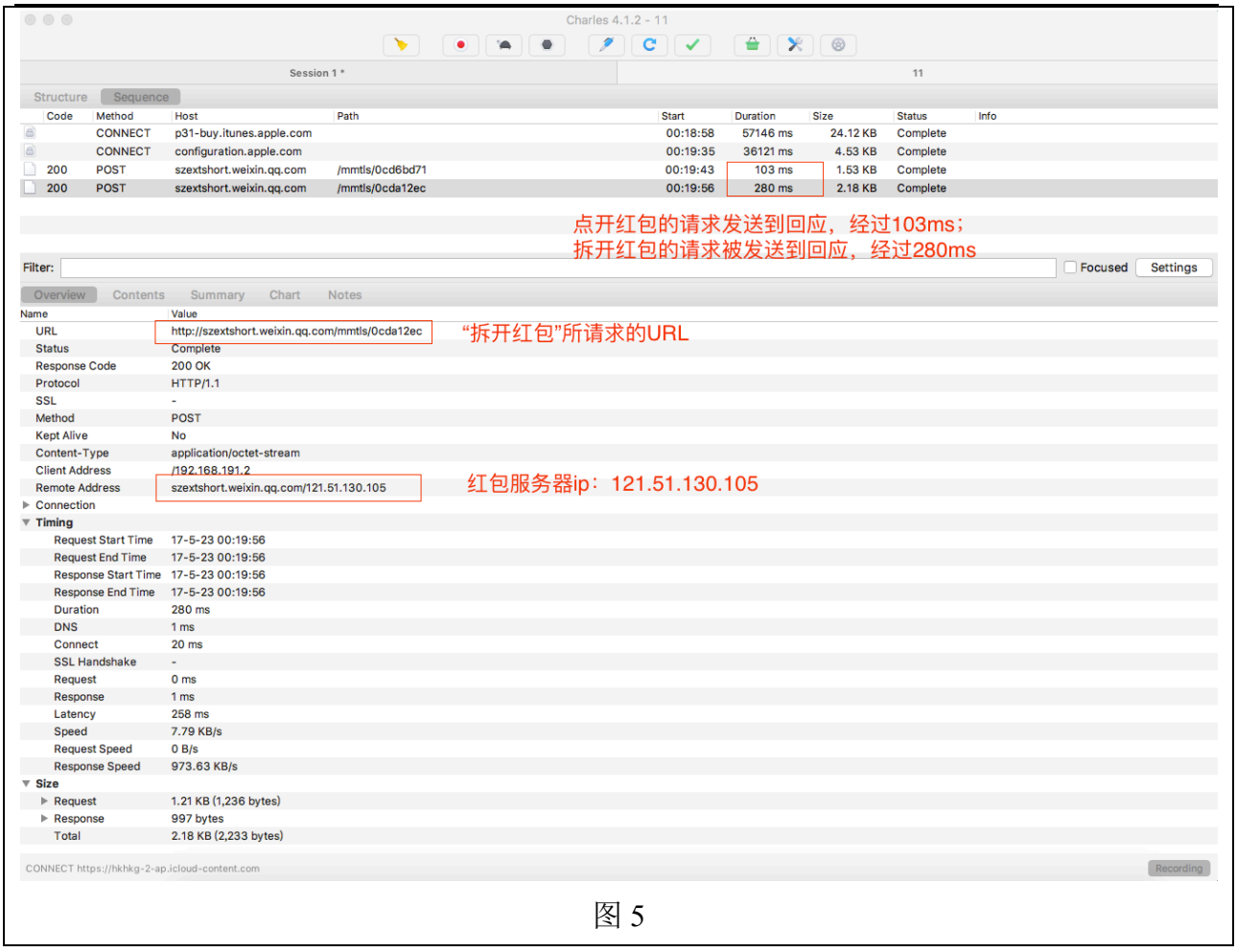
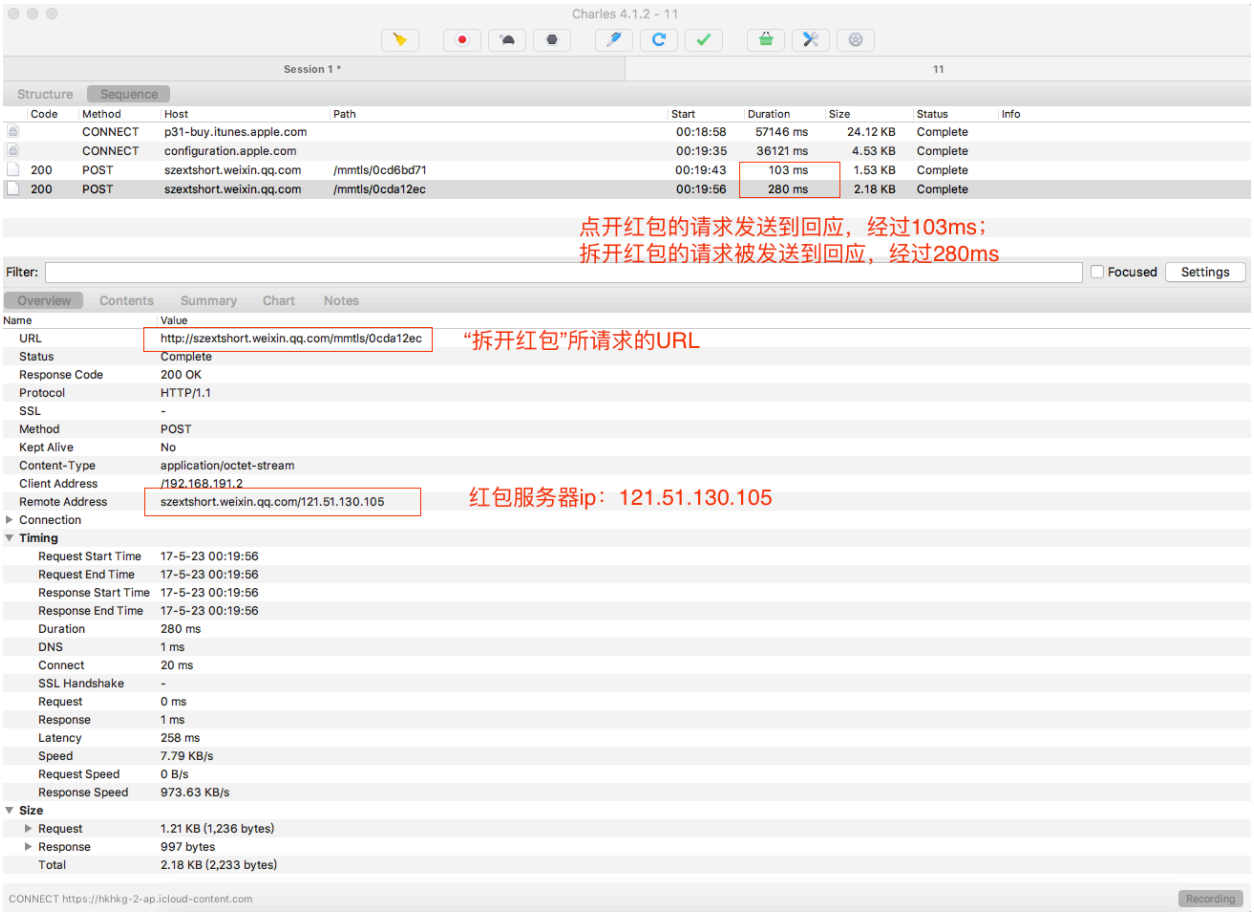


图 5

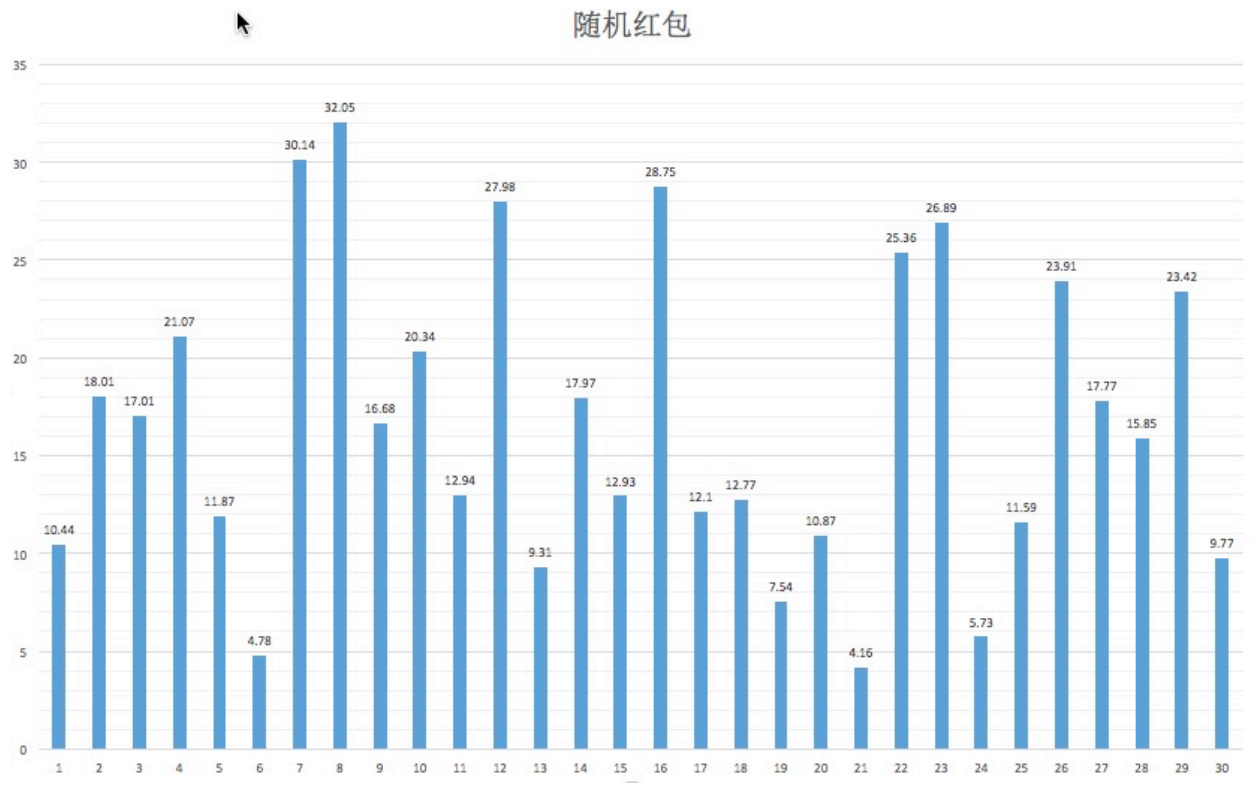
（3）分析延迟构成、URL、红包服务器 IP。请给出截图。

延迟由三部分构成，客户端延迟，线路延迟和服务器延迟。

客户端延迟主要是用户在发送请求时花费的时间，线路延迟是传输时的延迟，服务器延迟是服务器处理请求花费的时间。



（4）获取并分析抢红包、拆红包规律性，根据表格数据画出分析图。



由于分析需要比较大量的数据进行统计学分析，限于缺乏开展实验的条件，我们援引知乎用户（https://www.zhihu.com/question/22625187）对于随机红包的分析，参考他们的实验总结规律如下：

领取红包的顺序不同，获得红包的金额数学期望大致相等；

后抢的人方差大（依赖于先抢红包的人拿走的金额），波动较大，有较大概率拿到“手气最佳”；

此外，根据我们的经验，发现低于平均值的红包数量多，但是离平均值不远；有少数红包数额比平均值大很多，类似于截尾分布。

（5）根据（4）的分析结果，发一次微信红包，预测其结果，最后验证实际结果是否与预测相符并分析原因。

预测结果：大部分人获取的红包金额在平均值左右，个别人的金额较大，且较高概率出现在后抢的人手中。

验证实验结果：符合预测。尤其是在微信红包里，当发送红包金额为 0.01 元*N + 0.01 元时（N 为红包个数），最后一个人抢到的是 0.02 元，其余皆为 0.01 元。

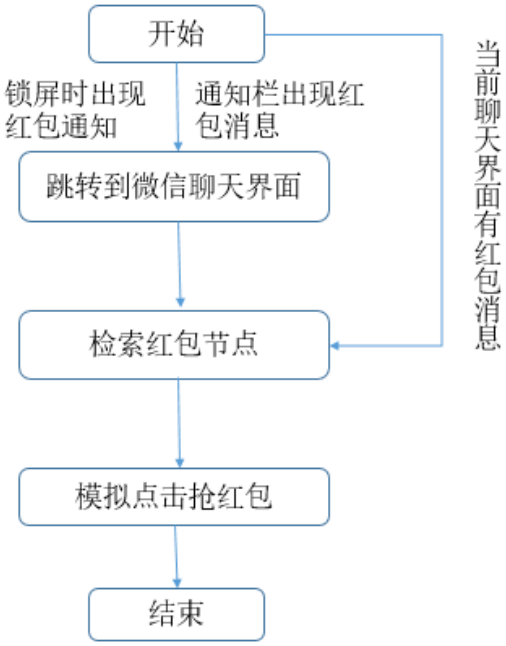
分析原因：腾讯可能采取了截尾分布，因为这样保证了大多数人的预期收益，又给抢红包的人抢到较大额红包的机会，增加了红包抽取人的积极性和游戏的公平性；

（6）如何编写抢红包、拆红包 APP？写出设计思路、画出程序流程图，给出关键代码（注意注释）。

设计思路：

捕捉手机的通知栏变动事件、使用 Android API 提供的 AccessibilityService(辅助功能)，AccessibilityService 服务会在后台运行，我们要做的就是等待系统在发生 AccessibilityEvent 事件时回调，然后根据对调的内容，判断是不是红包，搜索到红包节点，模拟点击操作。

程序流程图：



关键代码：

```java
//此方法必须重写，当通知栏消息改变时触发
public void onNotificationPosted(StatusBarNotification sbn) {
    Notification notification = sbn.getNotification();
    if (null == notification) return;

    Bundle extras = notification.extras;
    if (null == extras) return;

    List<String> textList = new ArrayList<>();
    String title = extras.getString("android.title");
    if (!isEmpty(title)) textList.add(title);

    String detailText = extras.getString("android.text");
    if (!isEmpty(detailText)) textList.add(detailText);

    if (textList.size() == 0) return;
    //for循环，遍历textList获取红包消息的notification，取到里面的PendingIntent执行
    for (String text : textList) {
        if (!isEmpty(text) && text.contains("[微信红包]")) {
            final PendingIntent pendingIntent = notification.contentIntent;
            try {
                pendingIntent.send();
            } catch (PendingIntent.CanceledException e) {
            }
            break;
        }
    }
}
```

ages Terminal

处理通知栏消息，如果出现[微信红包]则发送 PendingIntent

```
//方法重写，在不同事件下采用不同处理方式
public void onAccessibilityEvent(AccessibilityEvent event) {
    final int eventType = event.getEventType();
    //通知栏状态改变，解锁屏幕
    if (eventType == TYPE_NOTIFICATION_STATE_CHANGED) {
        unlockScreen();
        luckyClicked = false;
    }
    //窗体内容改变，抢红包
    if (eventType == TYPE_WINDOW_CONTENT_CHANGED) {
        AccessibilityNodeInfo rootNode = getRootInActiveWindow();
        if (null == rootNode) return;

        List<AccessibilityNodeInfo> list = rootNode.findAccessibilityNodeInfosByText("领取红包");
        if (null == list || list.size() == 0) return;

        AccessibilityNodeInfo parent = list.get(list.size() - 1);
        while (null != parent) {
            if (parent.isClickable() && !luckyClicked) {
                parent.performAction(ACTION_CLICK);
                luckyClicked = true;
                break;
            }
            parent = parent.getParent();
        }
    }

            //窗体状态改变，调用traverseNode()方法进行抢红包
            if (eventType == TYPE_WINDOW_STATE_CHANGED) {
                String clazzName = event.getClassName().toString();
                if (clazzName.equals(UI_RECEIVE)) {
                    traverseNode(event.getSource());
                }

                if (clazzName.equals(UI_DETAIL) && hasLucky) {
                    hasLucky = false;
                    handler.sendEmptyMessageDelayed(MSG_BACK, 1000);
                }
            }
        }
```

以上为核心代码，通过处理不同的事件（注释有具体事件）进行抢红包

（7）将编写好的 APP 安装到手机上演练，是否能达到预期效果？

预期功能：有好友发红包，能尽量快速拆开。

实验结果：当通知栏出现微信红包消息时，会自动跳转到微信抢红包，或者当在微信聊天时，有红包时也能自动抢，所以能达到预期效果。

（8）如何防止抢红包、拆红包 APP？（需具体写出措施、理由）

首先可以通过官方进行举报；
另外，由于很多抢红包 APP 都是通过匹配关键字“[微信红包]”来确定是否存在红包，所以在发红包前，我们可以发送这些文字去干扰这些 APP。

提交实验报告时，源程序以 组号_抢红包实验.cpp 或其他后缀文件提交（注意尽可能多加入注释）。

【交实验报告】

上传实验报告：ftp://222.200.180.109/ 截止日期（不迟于）：三周之内完成

上传小组实验报告。上传文件名格式：小组号_ 防火墙管理实验.pdf （由组长负责上传）

例如: 文件名“6_ 网络攻击分析实验.pdf”表示第 6 组的网络攻击分析实验报告

注意：不要打包上传！