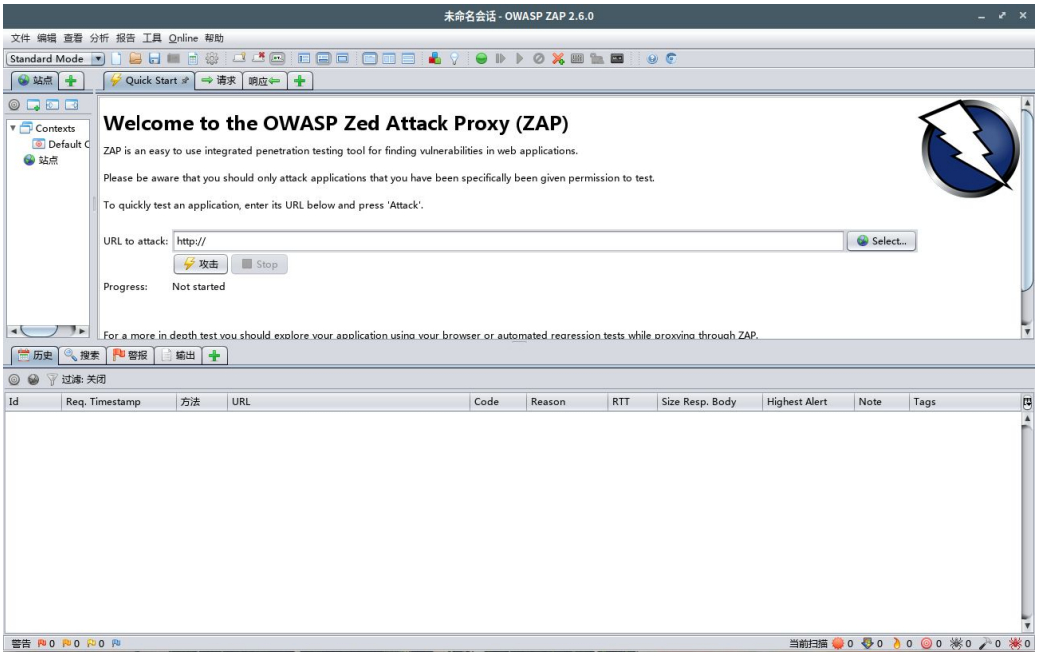
Task2.2 ZAP代理抓包

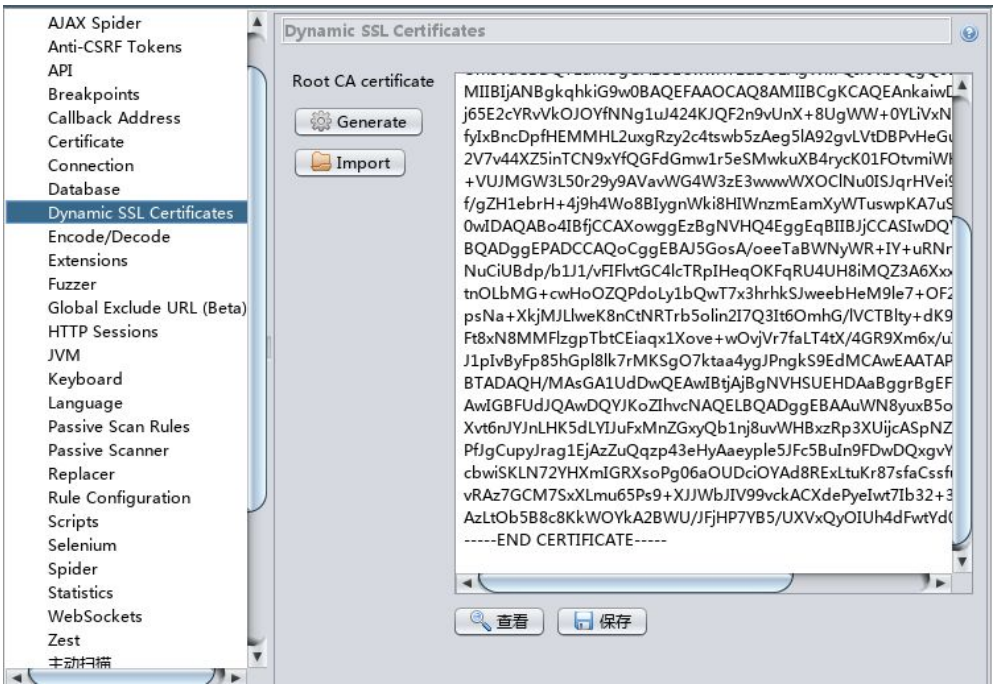
1.ZAP 安装

zap下载地址:
https://github.com/zaproxy/zaproxy/releases/download/2.6.0/ZAP_2.6.0_Linux.tar.gz
安装: tar xvzf ZAP_2.6.0_Linux.tar.gz
运行: 进入ZAP_2.6.0目录，命令行运行./zap.sh
（无法启动图形化界面时，更新下java版本）

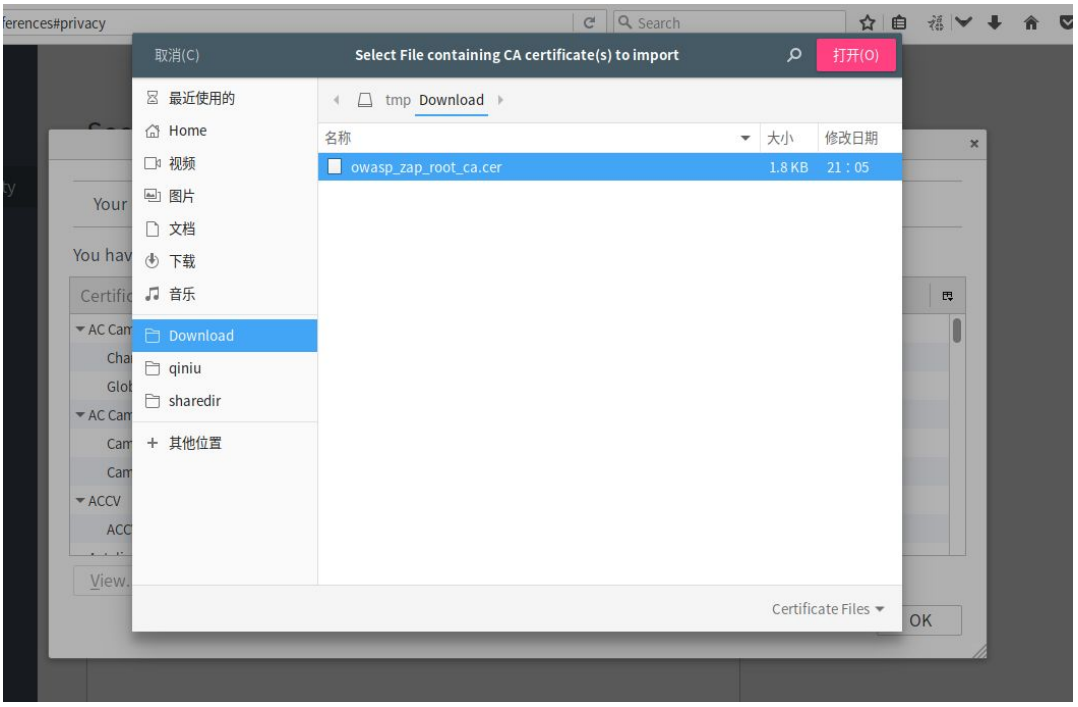


2.Zap 使用

为了能够抓取到https流量，首先要在在ZAP生成证书并导入浏览器中，点击工具->选项->Dynamic SSL Certificates

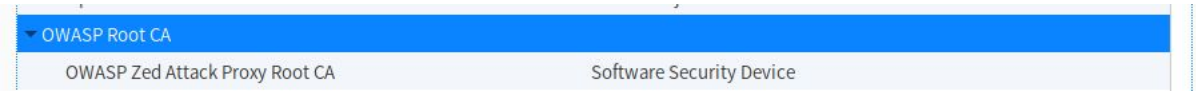


点击保存，保存到本地。接着导入证书以firefox为例，点击Preference->Privacy&Security->View Certificates->Import

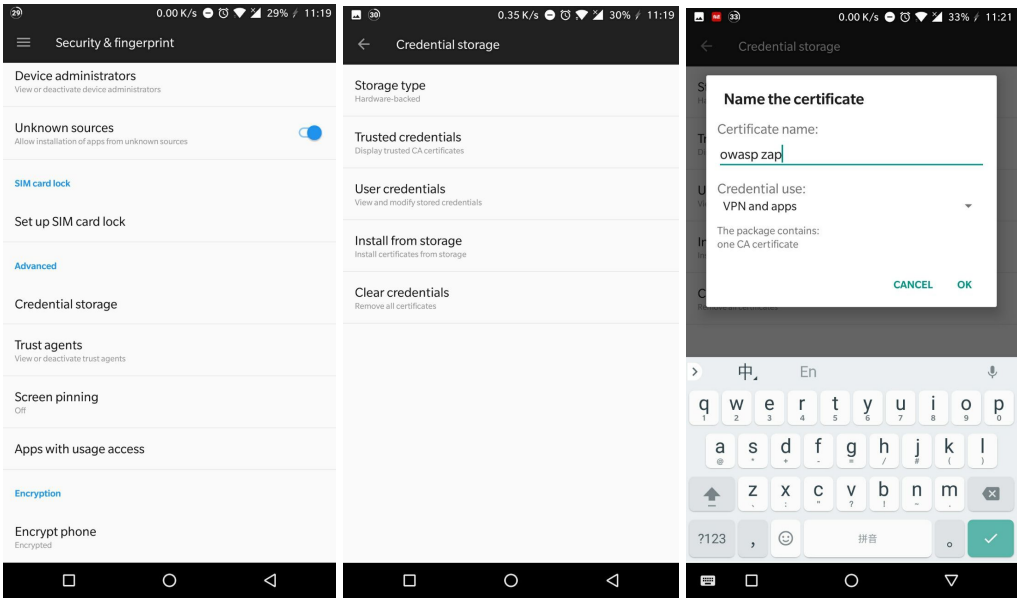


选择刚刚导入的证书

确定

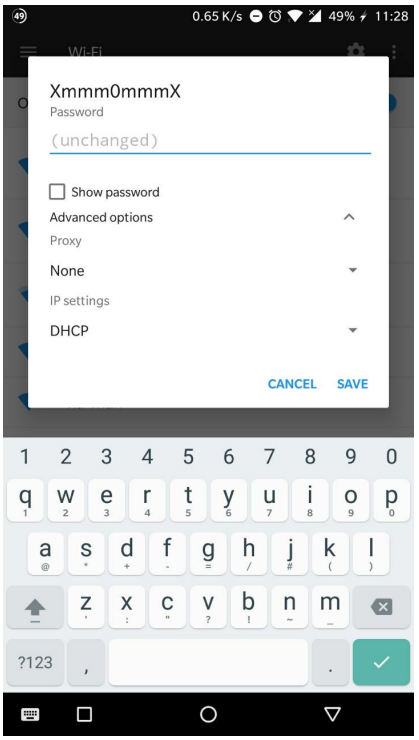


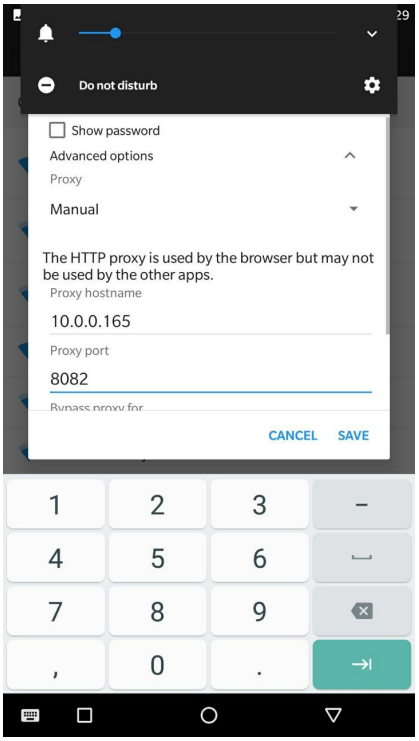
导入成功。要抓取手机的app的http数据包，可以将证书传到手机上，在手机中设置->安全中将证书安装:



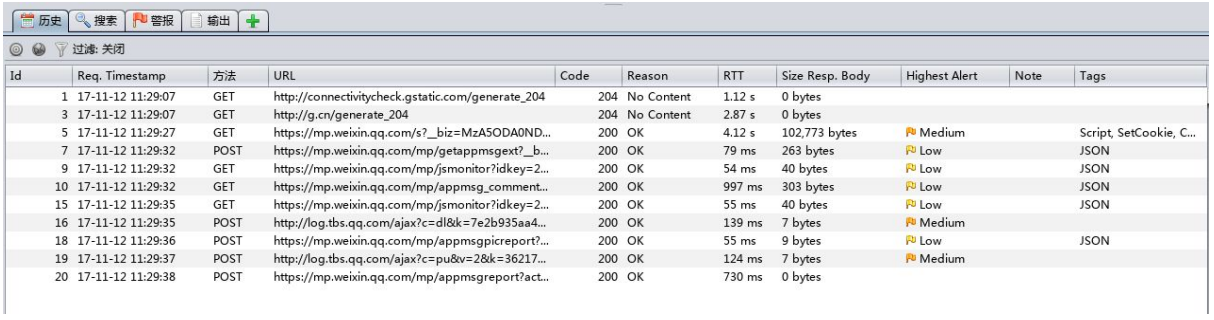
接着可以让手机和zap(电脑?)在同一局域网中，有以下几种方法：连同一wifi，该wifi可以自己创建或连stu-xdwlan，手机和电脑都连stu-xdwlan可能两者会ping不同，可能由于校园网配置的原因，此时可以电脑拨号，而手机连无线；或者电脑创建无线，手机连电脑反之也行。下面测试为电脑拨号，手机连stu：首先电脑拨号，查看ip地址，接着打开zap 设置zap监听ip地址为0.0.0.0，端口为8082，查看电脑在校园网下的ip地址，如下

手机上连接wifi(stu-xdwlan)，设置代理服务器地址:



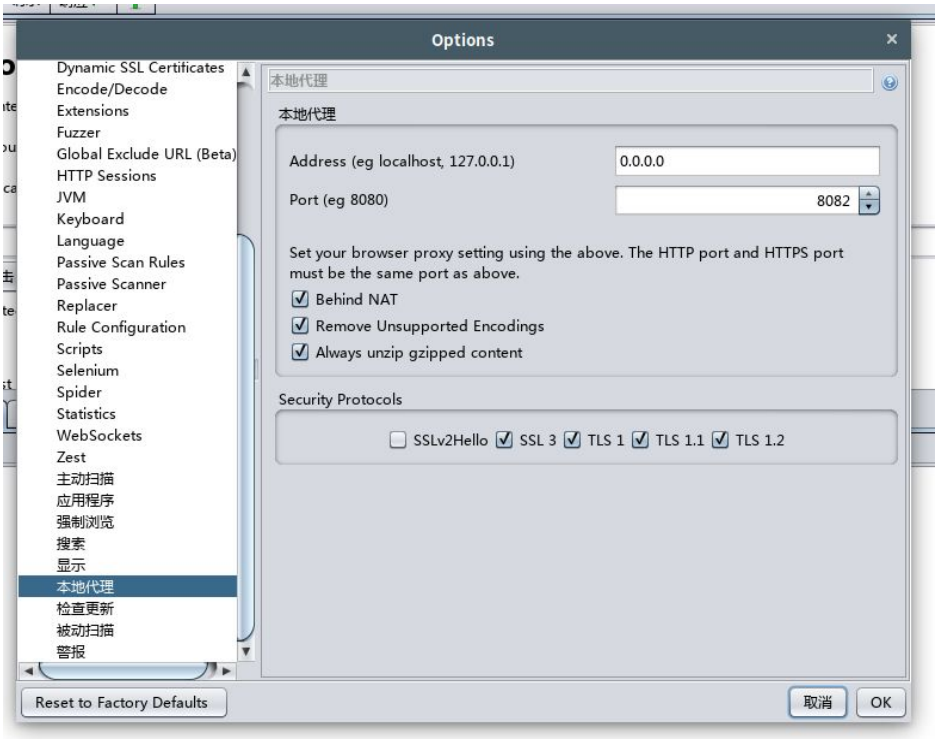


在微信下操作，查看历史栏能够看到http和https的数据包:



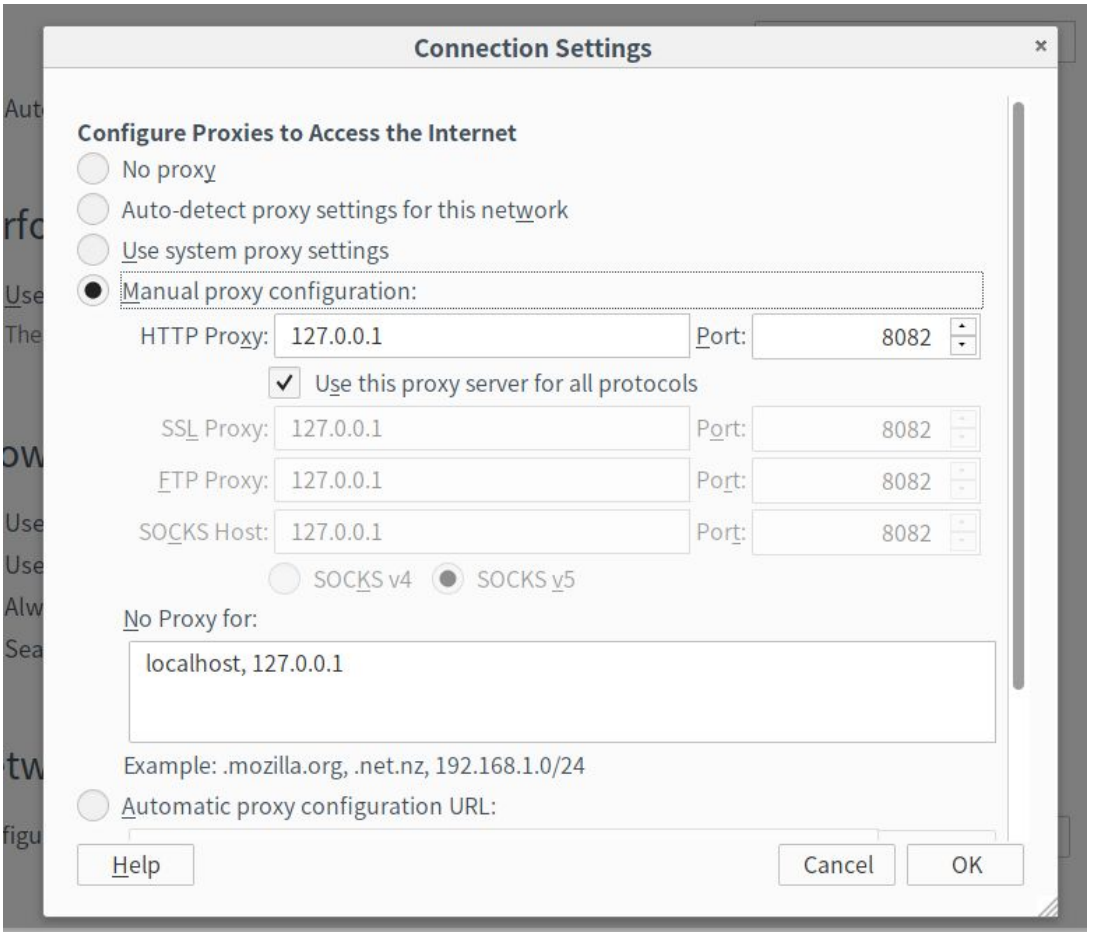
Id	Req. Timestamp	方法	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	17-11-12 11:29:07	GET	http://connectivitycheck.gstatic.com/generate_204	204	No Content	1.12 s	0 bytes			
3	17-11-12 11:29:07	GET	http://g.cn/generate_204	204	No Content	2.87 s	0 bytes			
5	17-11-12 11:29:27	GET	https://mp.weixin.qq.com/s?__biz=MzA5ODA0ND...	200	OK	4.12 s	102,773 bytes	Medium		Script, SetCookie, C...
7	17-11-12 11:29:32	POST	https://mp.weixin.qq.com/mp/getappmsgext?__b...	200	OK	79 ms	263 bytes	Low		JSON
9	17-11-12 11:29:32	GET	https://mp.weixin.qq.com/mp/jsmonitor?idkey=2...	200	OK	54 ms	40 bytes	Low		JSON
10	17-11-12 11:29:32	GET	https://mp.weixin.qq.com/mp/appmsg_comment...	200	OK	997 ms	303 bytes	Low		JSON
15	17-11-12 11:29:35	GET	https://mp.weixin.qq.com/mp/jsmonitor?idkey=2...	200	OK	55 ms	40 bytes	Low		JSON
16	17-11-12 11:29:35	POST	http://log.tbs.qq.com/ajax?c=dl&k=7e2b935aa4...	200	OK	139 ms	7 bytes	Medium		
18	17-11-12 11:29:36	POST	https://mp.weixin.qq.com/mp/appmsgpicreport?...	200	OK	55 ms	9 bytes	Low		JSON
19	17-11-12 11:29:37	POST	http://log.tbs.qq.com/ajax?c=pu&v=2&k=36217...	200	OK	124 ms	7 bytes	Medium		
20	17-11-12 11:29:38	POST	https://mp.weixin.qq.com/mp/appmsgreport?act...	200	OK	730 ms	0 bytes			

接着将zap设置成代理服务器，在zap中工具->选项->本地代理中，设置zap作为代理服务器监听的端口和地址。这里设置监听地址为0.0.0.0:8082，这在所有本地地址上都监听(127.0.0.1、...)，可以设置成127.0.0.1:8082等，只在127.0.0.1:8082上监听。

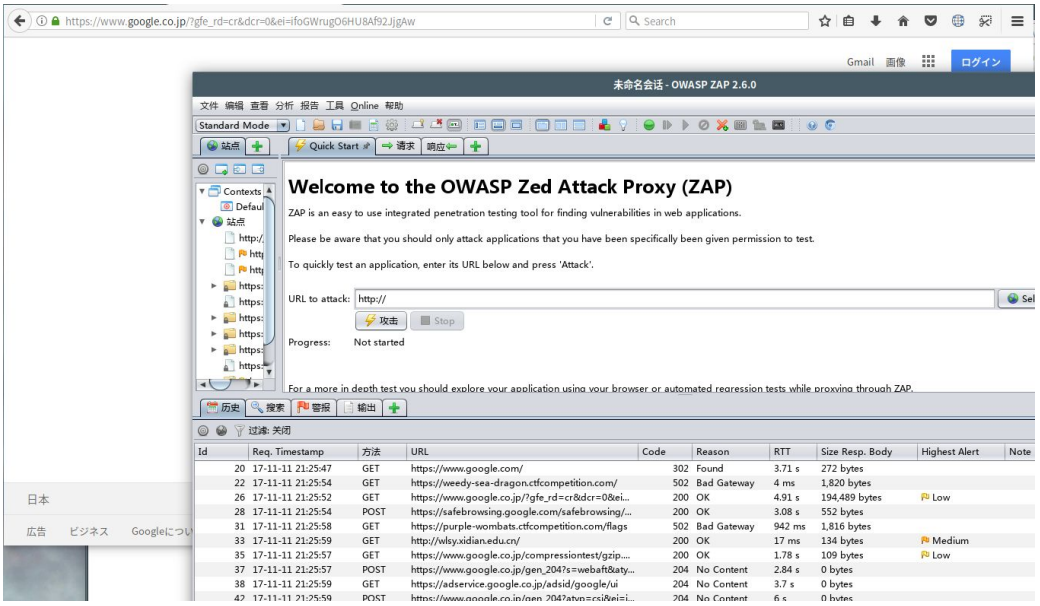


然后在浏览器上设置代理服务器的地址，在firefox中Preference->General->Network Proxy->Setting

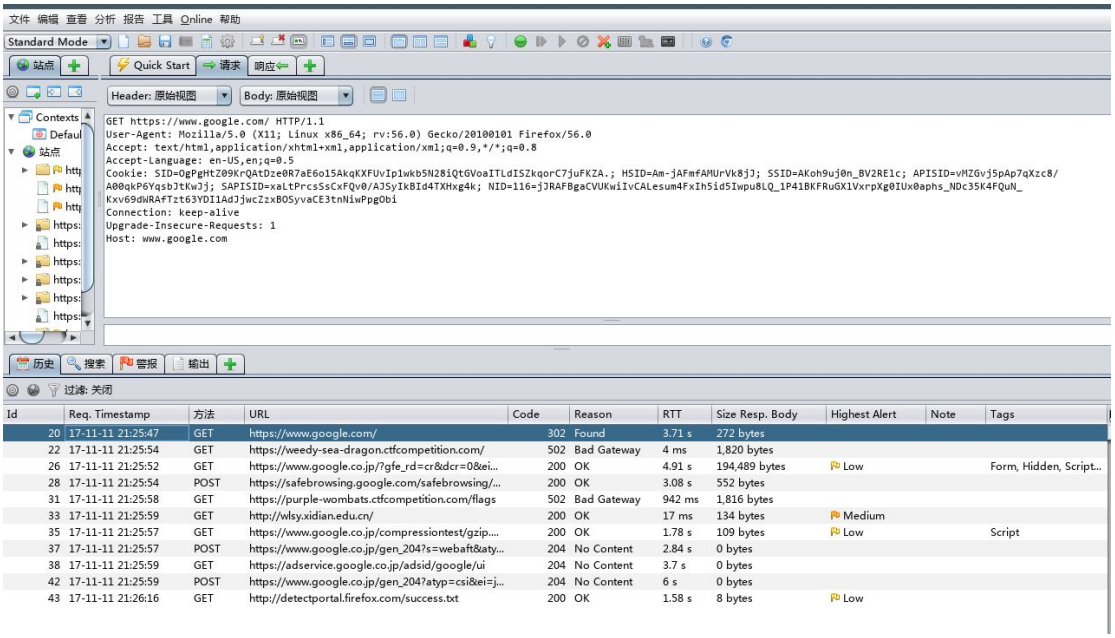
设置HTTP代理地址为127.0.0.1:8082



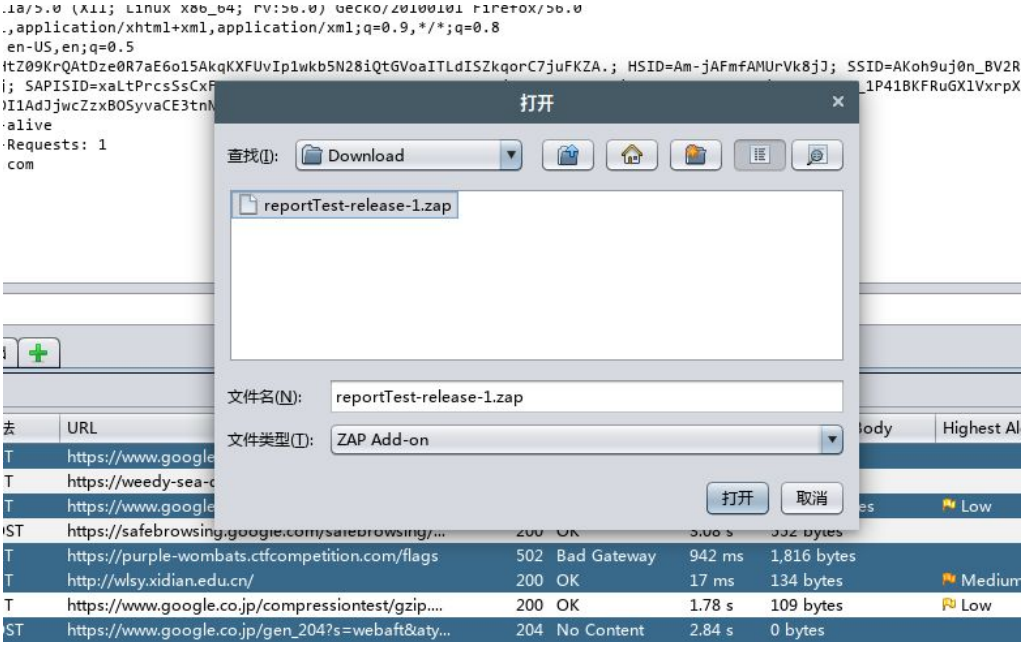
设置好后访问网站进行测试:



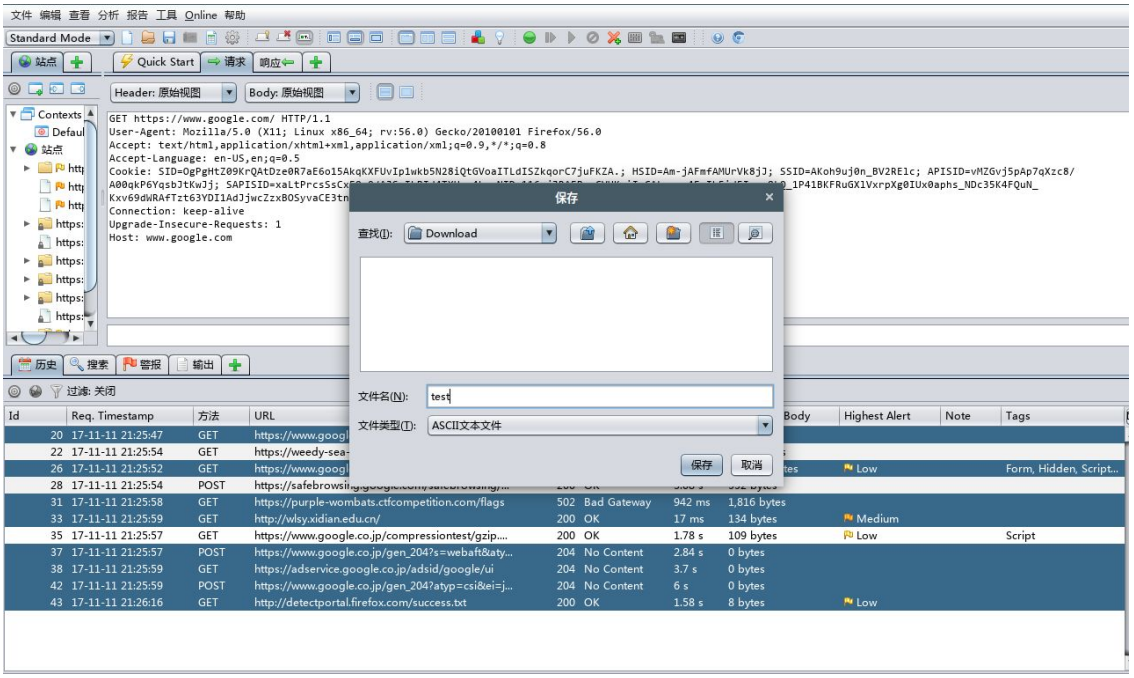
在历史中可以看到通过zap代理服务器的http数据包
点击http数据包可以看到其请求响应



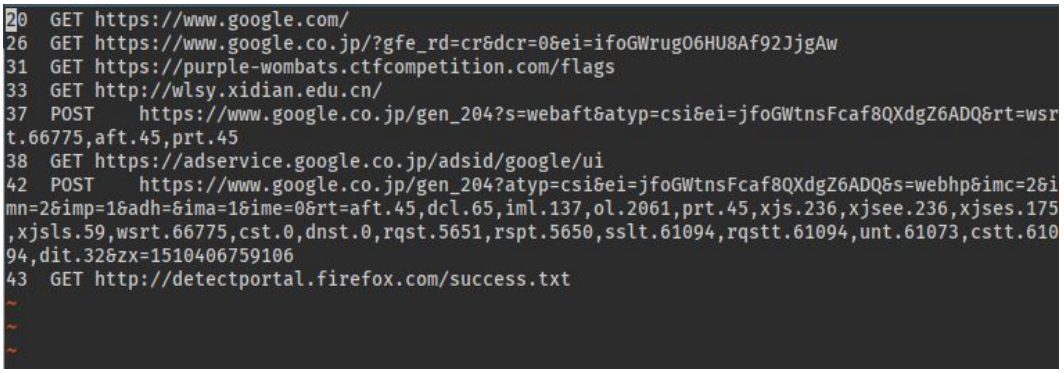
接着将收集到的接口导出，首先安装结果导出插件，在zap中文件->Load Add-on File选择[reportTest-release-1.zap]打开。



在历史栏中选择要导出的结果，报告->Report Test，将结果导出，插件中有相应的去重规则所以一些本来在历史栏中有的结果会被去掉，正常的这是。



导出结果如下



问题：

1. 打开http://weather.news.sina.com.cn 收集该页面结果并导出
2. 在zap的历史栏中找到1.中根据城市获取天气情况的api修改参数(如城市)重新发送
3. 在zap中添加相应的过滤规则，使得对于https://www.baidu.com 域名下的接口都不收集，及在历史栏下没有对应接口url(总之就在工具->选项下探索探索)
4. 尝试收集手机app http和https流量（自己要截取手机端收集http流量的app图标一张即可）