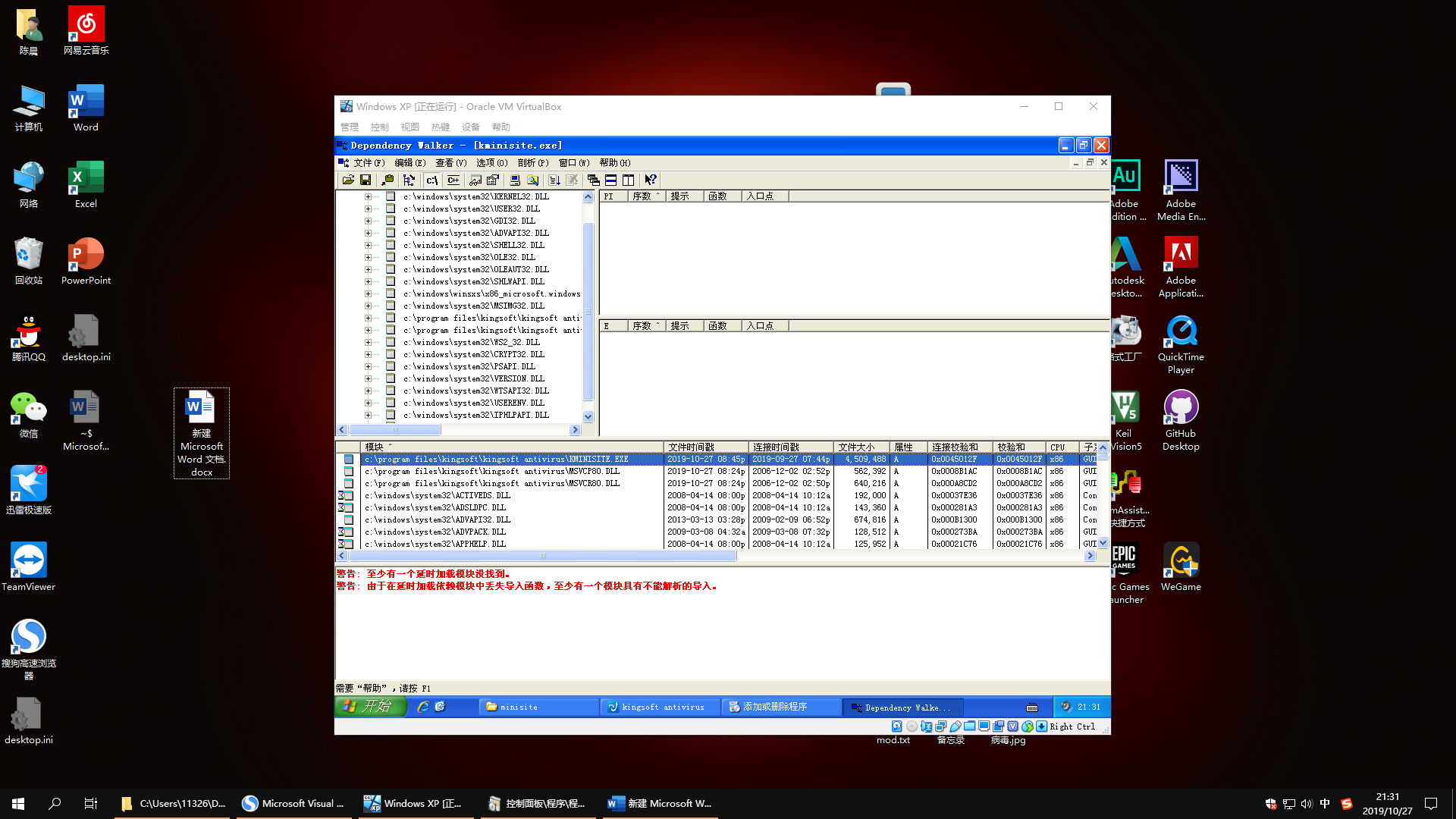
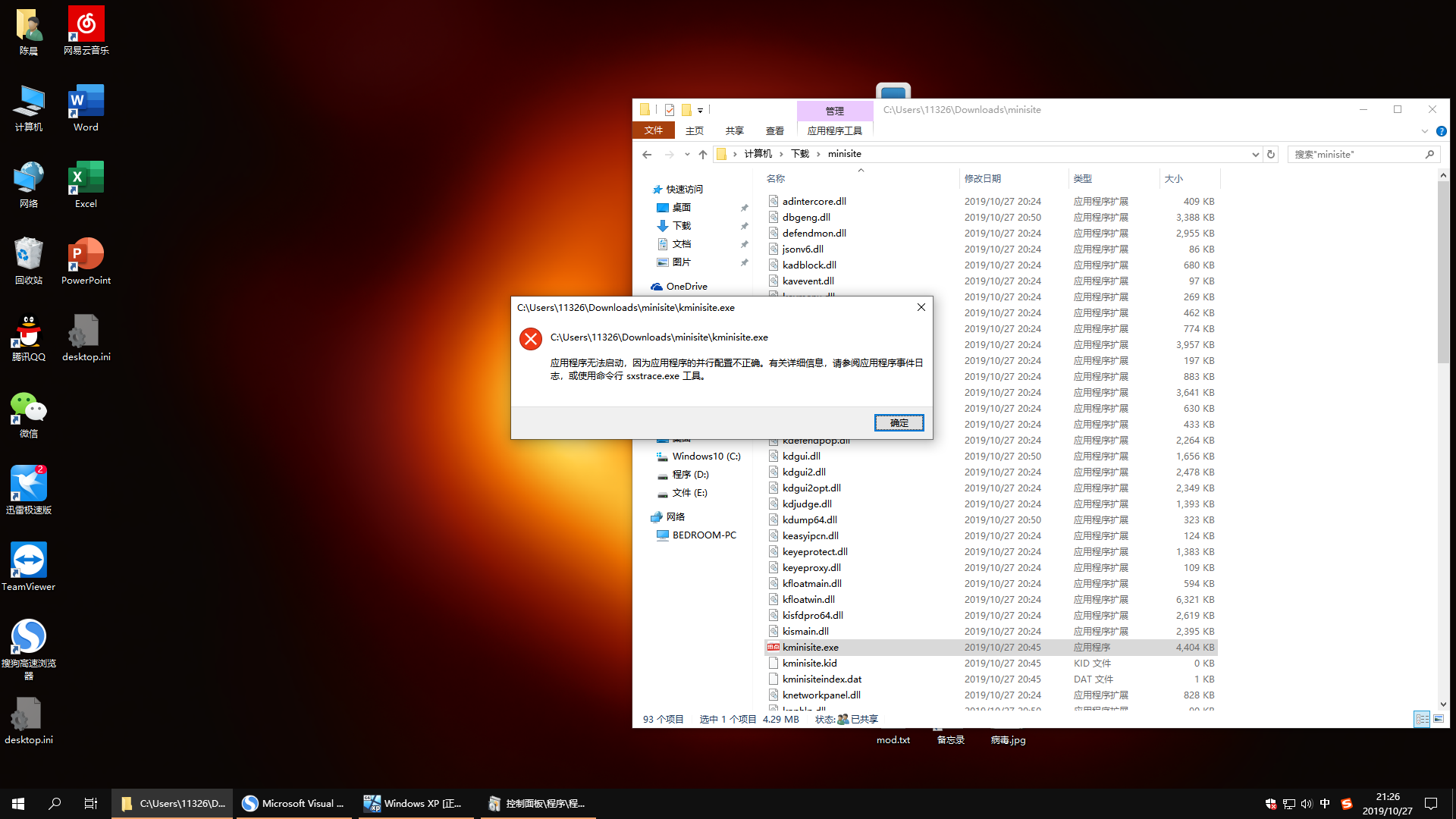
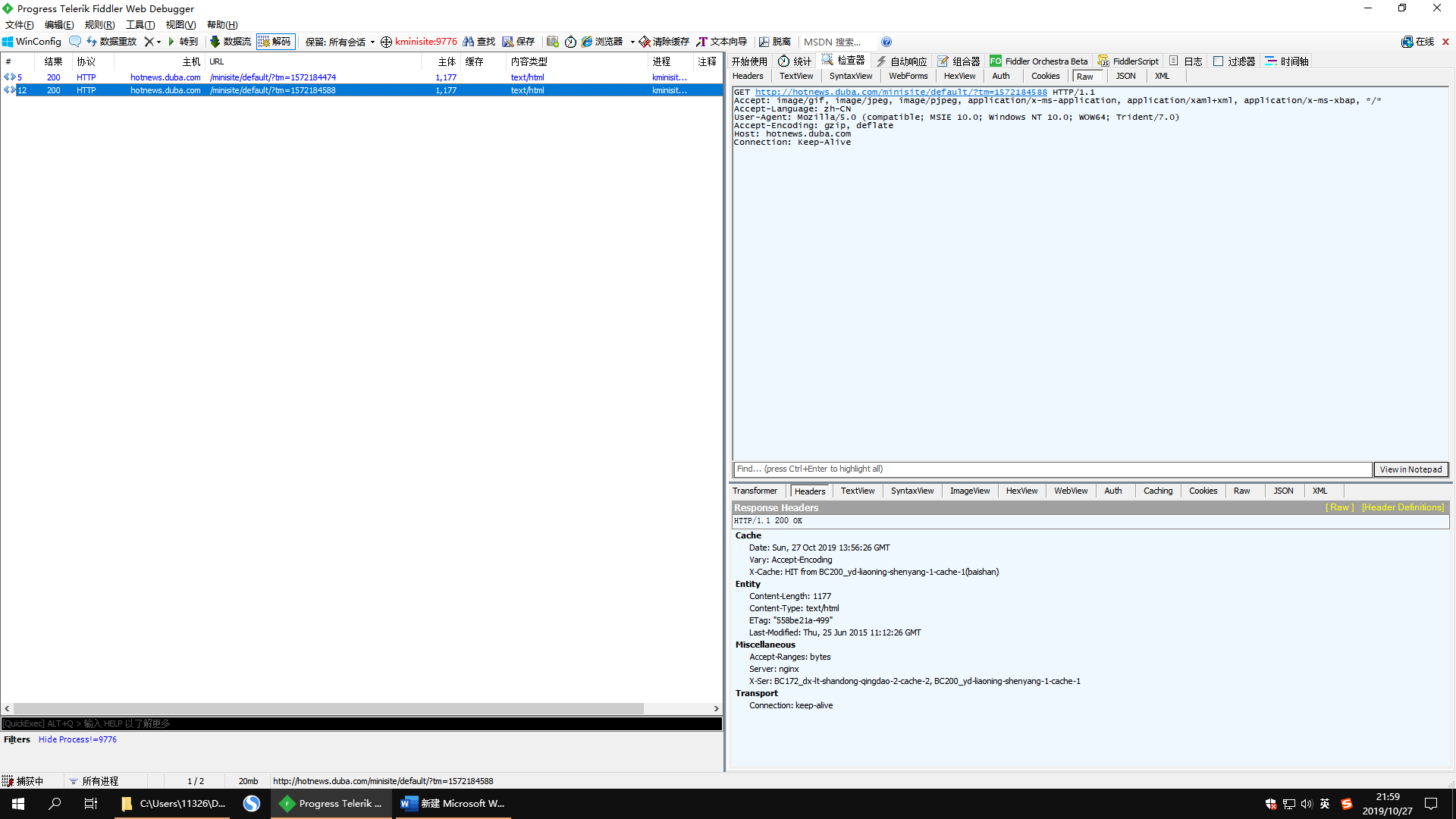
毒霸热点”入侵”记

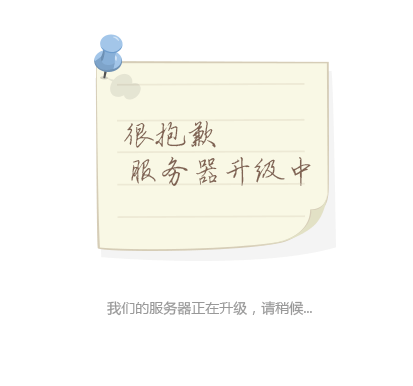
近日发现学校电脑的毒霸热点净是推送些无聊的东西,而且关还关不掉,在永吉同学的提醒下,我觉得我可以好好利用一下这个”热点”,让其发挥应有的热量.

我的计划是在本地架设伪毒霸热点服务器用来提供我的热点,然后修改hosts令热点的访问指向本地服务器,服务器用python写应该就可以,问题不大.

第一步是分析热点新闻的来源并解析其内容,为了避免金山毒霸全家桶,我选择在虚拟机(Oracle VM VirtualBox,Windows XP 32位系统)内安装金山毒霸,但虚拟机打不开,经百度得到解决方案,是由于我开启了hyper-v功能造成了冲突,使用管理员权限运行命令:bcdedit /set hypervisorlaunchtype off,然后重启即可,在忍受了极其缓慢的虚拟机后,我终于找到了毒霸热点的位置,它在金山毒霸安装目录下,文件名为kminisite.exe.我打算用抓包软件Fiddler抓包,但由于虚拟机缺.NET无法启动,那就把它拷贝出来,在实体机(Windows 10,64位)上运行,但是报错,提示应用程序的并行配置不正确,盲猜是缺动态链接库(dll),于是果断祭出Depends,单击查看完整路径,发现依赖了两个dll,是msvcp80.dll和msvcr80.dll,拷贝出来,但仍然报错,于是百度,发现这两个dll是VC++2005的,emmm,这都9102年了好吗,但是我实体机安装了VC++2005,应该没问题,最终迫不得已用了排除法,发现我没拷贝清单文件, microsoft.vc80.crt.manifest和microsoft.vc80.mfc.manifest,而且它还软依赖kdgui2.dll,Depends里没显示,真坑……,最后终于成功运行,我打开Fiddler抓包,可是毒霸热点却不显示内容,一直是该页面暂时无法显示,好在抓到了包,解析后找到了毒霸热点的网址: <http://hotnews.duba.com/minisite/default>,获取新闻时用了HTTP GET,参数tm,值是10位的数,直觉告诉我这是时间戳,百度一下,啊真是时间戳,那tm就是time的缩写了呗,但是明明返回的是200,为啥没内容呢,怀着这个疑问,我直接用浏览器访问了一下,结果……服务器升级中……恩,好吧,先睡觉,等下次放假再说







到了学校,发现毒霸新闻仍正常显示,于是在学校电脑抓包,原来这个服务器升级页面纯属骗人,经过抓包,发现一些可用的网页和其API,如下所示:

无法访问:

1334,1517,1601,8001,8003

正在维护:

https://hotnews.duba.com/minisite/default/

https://hotnews.duba.com/minisite/1338/

https://hotnews.duba.com/minisite/1516/

可用:

https://hotnews.duba.com/minisite/1335/

https://hotnews.duba.com/minisite/1337/

https://hotnews.duba.com/minisite/1509/

(精简版)https://hotnews.duba.com/minisite/1339/

API详见源码目录的\data\kminisite\_data.json

然后开始写python服务器,服务器是写完了,但是怎么能欺骗热点让它访问我的服务器呢,开始时候我想改hosts来跳转,但是我的服务器要先获取毒霸热点数据,而且python在windows下好像只能访问和增加hosts,不能删除,然后我想到了透明代理,在这个过程中还出了一点小问题,害得我调试了一晚上才发现,visual studio 2017(懒得更新) python的项目设置中的常规条目中有一个”Windows应用程序”的勾选框,我刚开始勾上没注意,然后print()就不断抛异常,调试了一晚上才明白这个应该是窗口化模式,勾上之后用pythonw.exe运行,没有命令窗口,自然没法输出,汗…所以应该是翻译错了,我觉得正确的翻译是”窗口化应用程序”,翻译给当成专有名词”Windows”了?不管这个,在配置代理时也遇到了很多问题,没有好用的代理库,只有一个mitmproxy还不错,而且能用python写脚本,经过一番配置,再写个重定向的脚本,结果…不好使,代理把我服务器的访问也给重定向了,所以造成了死循环,解决方案就是判断http头中的User-Agent,我把我的服务器的设成了”MyMinisiteServer/1.0”,问题解决.

在从学校偷过来的毒霸热点上运行正常,但新的毒霸热点好像有点问题,因为它自带一个跳转机制,我还没弄明白呢,不过现在这样就可以用了,享受吧~