# 微信小程序抓包教程

0x01 准备工具

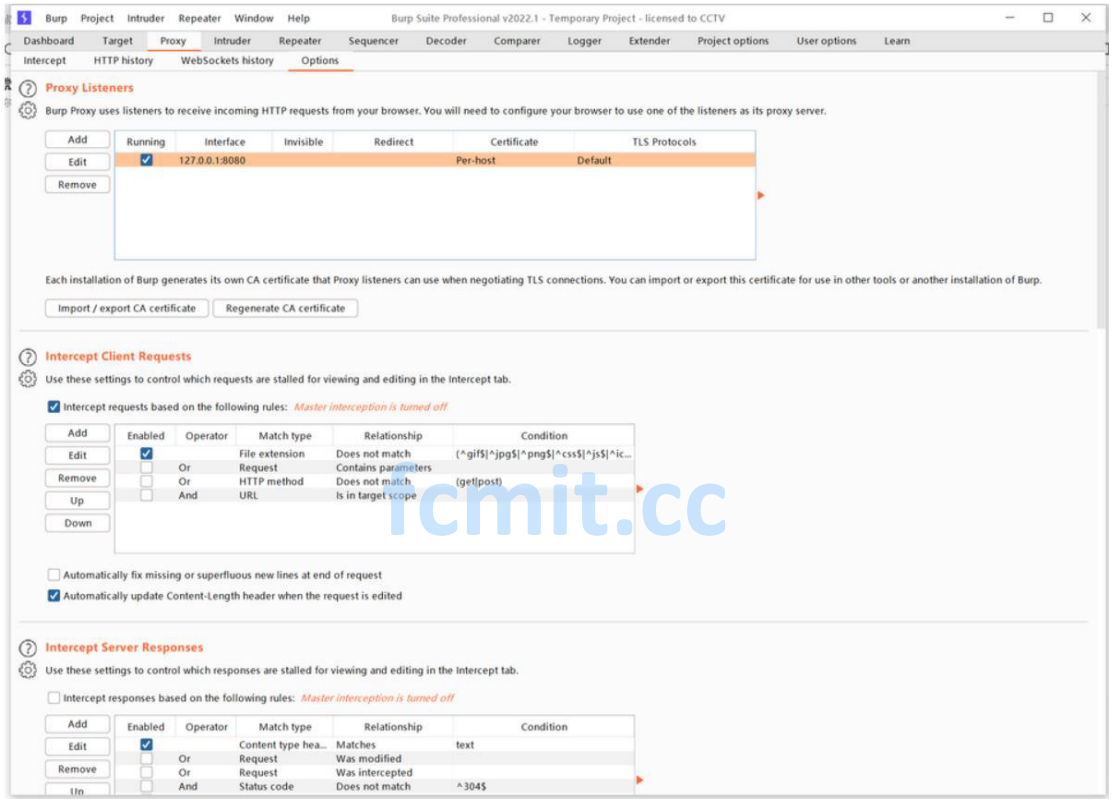
Proxifier Burpsuite

电脑端微信客户端（随便什么版本都可以）

流量走向： 电脑端微信小程序 --->通过 proxifier ---> 走到 Burpsuite

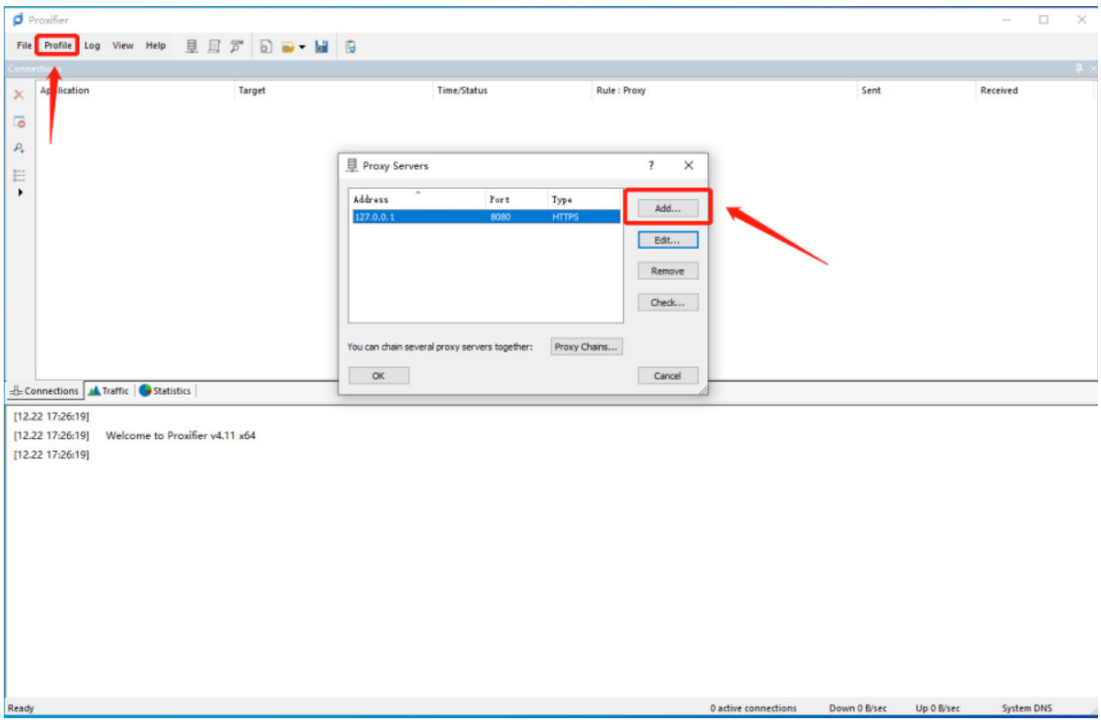
0x02 环境配置

第一步 设置 Burpsuite

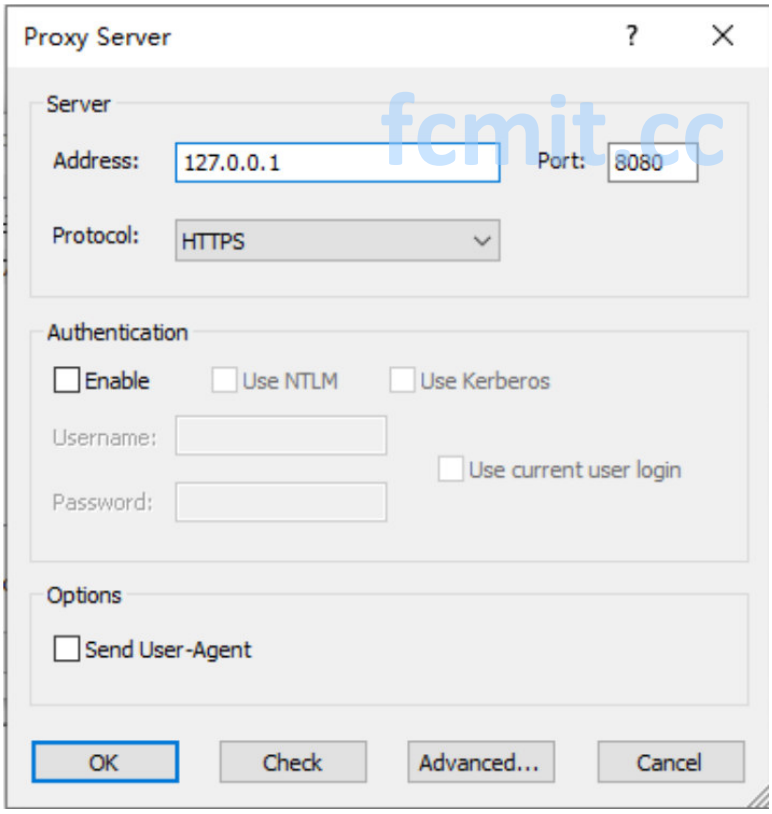



0x03 Proxifier 设置

点击 Profile (配置文件)



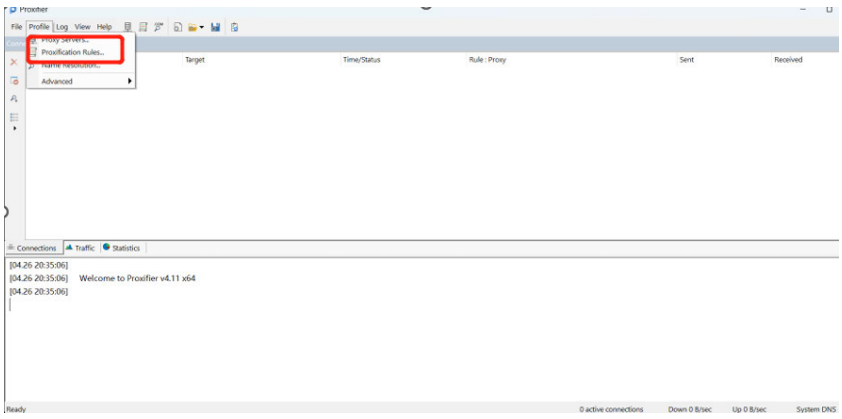

添加 Burp 的监听地址和端口

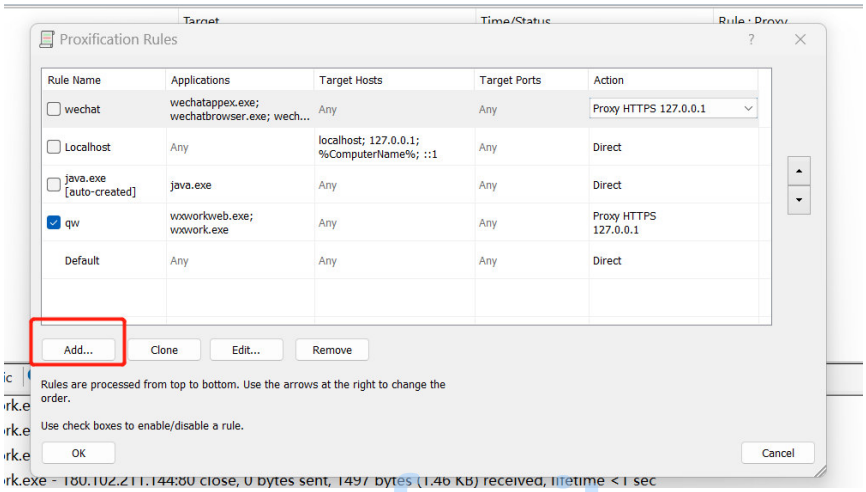


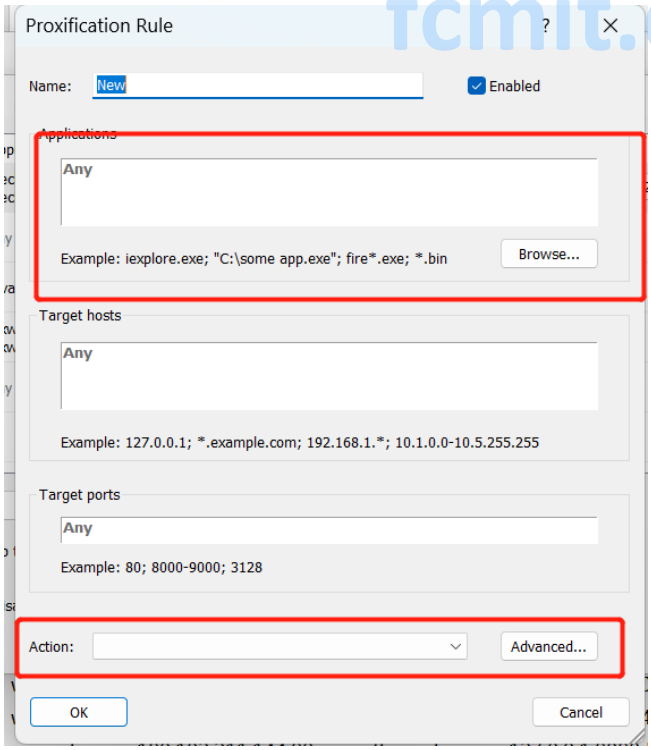

fcmit.cc

设置完记得保存

然后点击 Proxifications Rules (配置文件-代理规则)

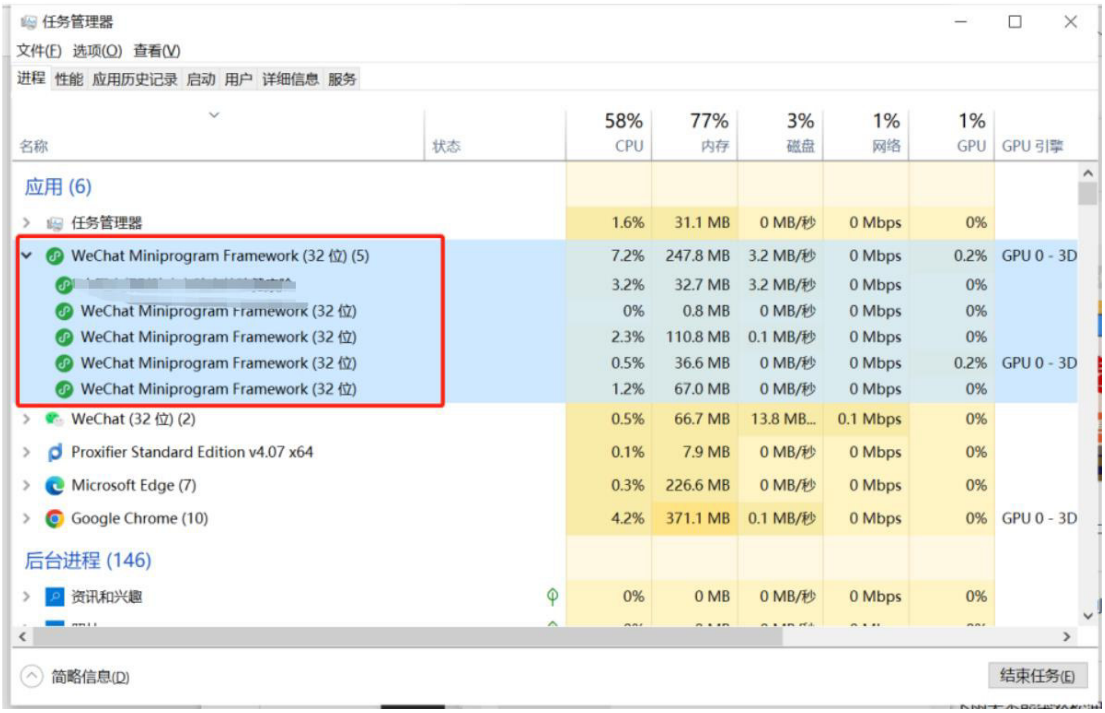


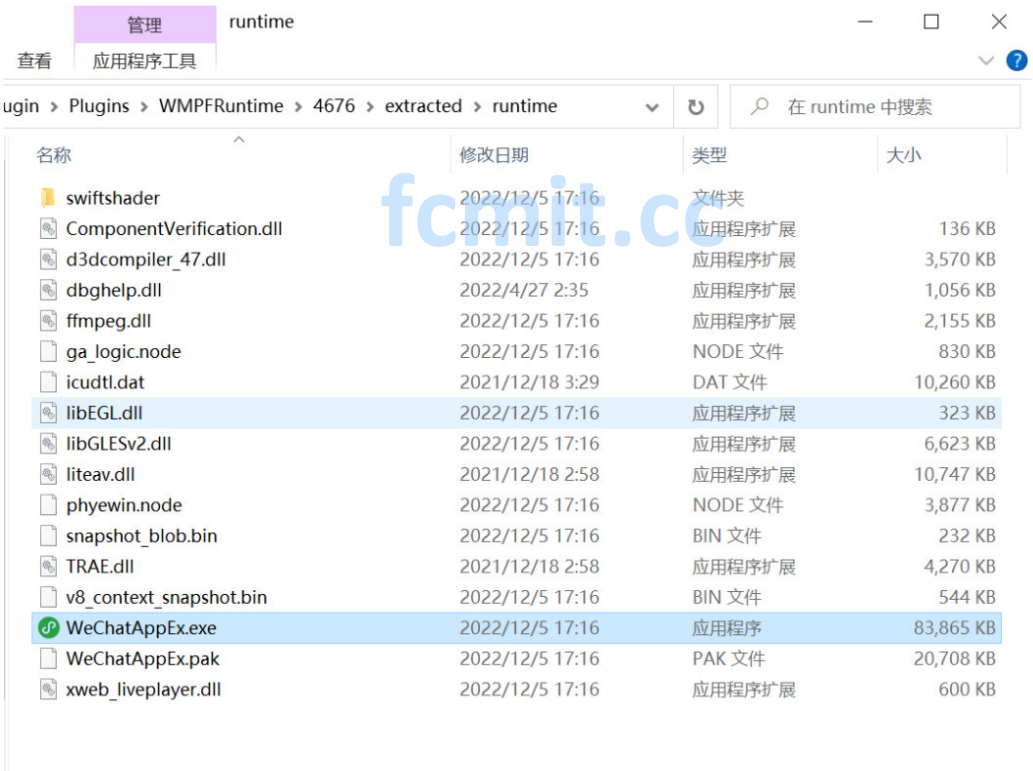




tcmit.cc

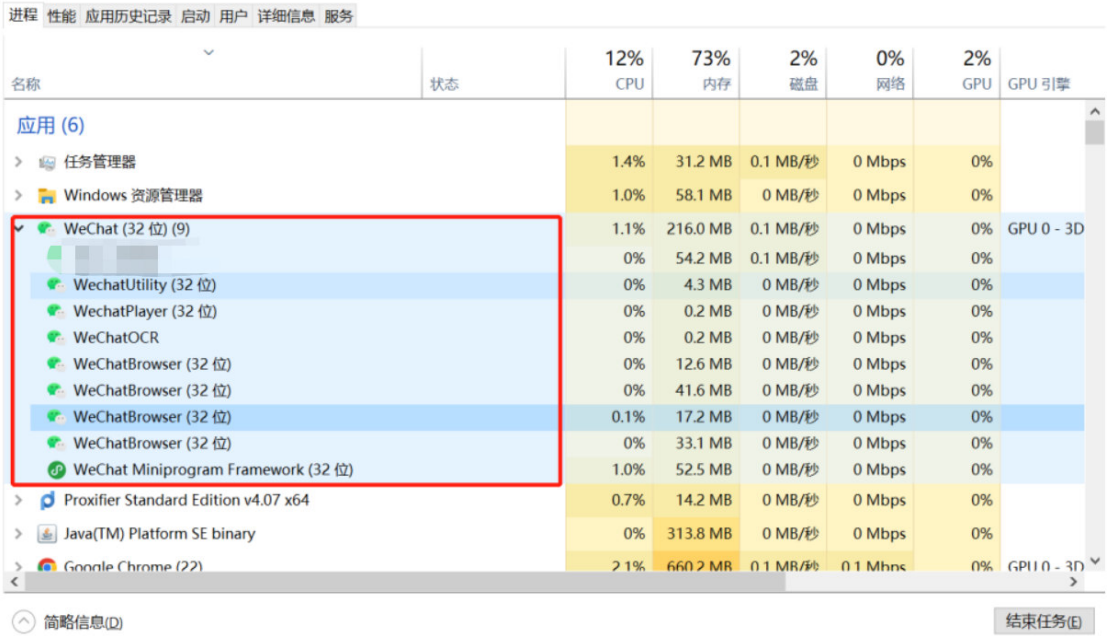
通过任务管理器可以看到
WeChatAppEx.exe 这个是电脑端小程序的名字
然后在任务管理器中右键查看文件所在位置就可以了



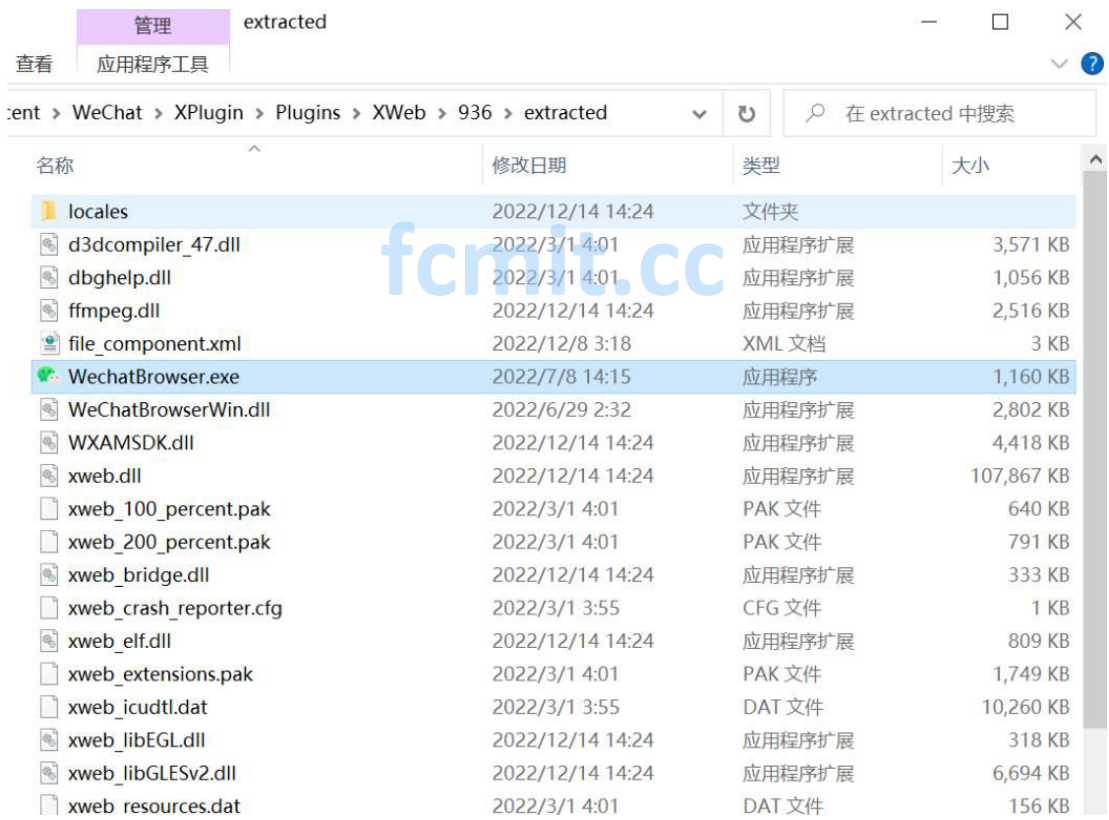

fcmit.cc

**wechatbrowser.exe 这个是电脑端微信浏览器的名字**



| 进程 性能 应用历史记录 启动 用户 详细信息 服务 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 名称 | 状态 | 12% CPU | 73% 内存 | 2% 磁盘 | 0% 网络 | 2% GPU | GPU 引擎 |
| 应用 (6) | | | | | | | |
| 任务管理器 | | 1.4% | 31.2 MB | 0.1 MB/秒 | 0 Mbps | 0% | |
| Windows 资源管理器 | | 1.0% | 58.1 MB | 0 MB/秒 | 0 Mbps | 0% | |
| WeChat (32 位) (9) | | 1.1% | 216.0 MB | 0.1 MB/秒 | 0 Mbps | 0% | GPU 0 - 3D |
| [redacted] | | 0% | 54.2 MB | 0.1 MB/秒 | 0 Mbps | 0% | |
| WechatUtility (32 位) | | 0% | 4.3 MB | 0 MB/秒 | 0 Mbps | 0% | |
| WechatPlayer (32 位) | | 0% | 0.2 MB | 0 MB/秒 | 0 Mbps | 0% | |
| WeChatOCR | | 0% | 0.2 MB | 0 MB/秒 | 0 Mbps | 0% | |
| WeChatBrowser (32 位) | | 0% | 12.6 MB | 0 MB/秒 | 0 Mbps | 0% | |
| WeChatBrowser (32 位) | | 0% | 41.6 MB | 0 MB/秒 | 0 Mbps | 0% | |
| WeChatBrowser (32 位) | | 0.1% | 17.2 MB | 0 MB/秒 | 0 Mbps | 0% | |
| WeChatBrowser (32 位) | | 0% | 33.1 MB | 0 MB/秒 | 0 Mbps | 0% | |
| WeChat Miniprogram Framework (32 位) | | 1.0% | 52.5 MB | 0 MB/秒 | 0 Mbps | 0% | |
| Proxifier Standard Edition v4.07 x64 | | 0.7% | 14.2 MB | 0 MB/秒 | 0 Mbps | 0% | |
| Java(TM) Platform SE binary | | 0% | 313.8 MB | 0 MB/秒 | 0 Mbps | 0% | |
| Google Chrome (22) | | 2.1% | 660.2 MB | 0.1 MB/秒 | 0.1 Mbps | 0% | GPU 0 - 3D |

简略信息(D) 结束任务(E)



管理 extracted

查看 应用程序工具

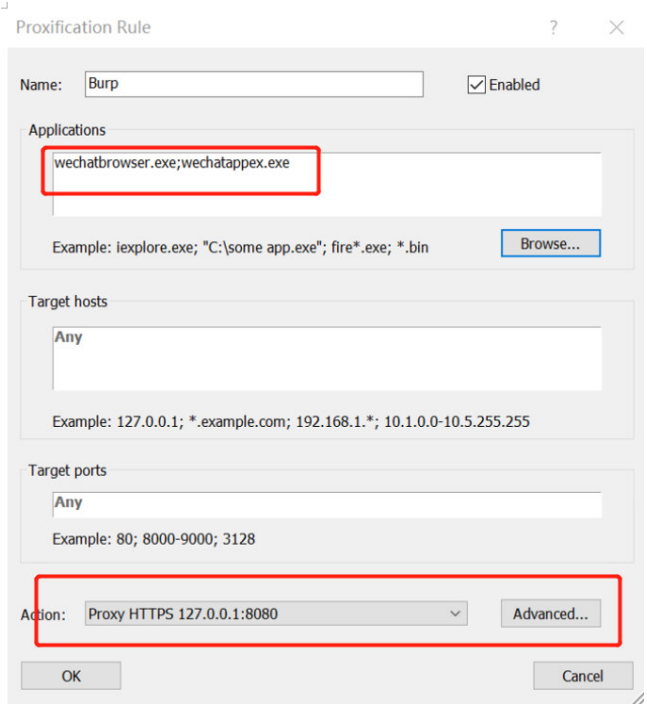
:ent › WeChat › XPlugin › Plugins › XWeb › 936 › extracted

在 extracted 中搜索

| 名称 | 修改日期 | 类型 | 大小 |
|---|---|---|---|
| locales | 2022/12/14 14:24 | 文件夹 | |
| d3dcompiler_47.dll | 2022/3/1 4:01 | 应用程序扩展 | 3,571 KB |
| dbghelp.dll | 2022/3/1 4:01 | 应用程序扩展 | 1,056 KB |
| ffmpeg.dll | 2022/12/14 14:24 | 应用程序扩展 | 2,516 KB |
| file_component.xml | 2022/12/8 3:18 | XML 文档 | 3 KB |
| WechatBrowser.exe | 2022/7/8 14:15 | 应用程序 | 1,160 KB |
| WeChatBrowserWin.dll | 2022/6/29 2:32 | 应用程序扩展 | 2,802 KB |
| WXAMSDK.dll | 2022/12/14 14:24 | 应用程序扩展 | 4,418 KB |
| xweb.dll | 2022/12/14 14:24 | 应用程序扩展 | 107,867 KB |
| xweb_100_percent.pak | 2022/3/1 4:01 | PAK 文件 | 640 KB |
| xweb_200_percent.pak | 2022/3/1 4:01 | PAK 文件 | 791 KB |
| xweb_bridge.dll | 2022/12/14 14:24 | 应用程序扩展 | 333 KB |
| xweb_crash_reporter.cfg | 2022/3/1 3:55 | CFG 文件 | 1 KB |
| xweb_elf.dll | 2022/12/14 14:24 | 应用程序扩展 | 809 KB |
| xweb_extensions.pak | 2022/3/1 4:01 | PAK 文件 | 1,749 KB |
| xweb_icudtl.dat | 2022/3/1 3:55 | DAT 文件 | 10,260 KB |
| xweb_libEGL.dll | 2022/12/14 14:24 | 应用程序扩展 | 318 KB |
| xweb_libGLESv2.dll | 2022/12/14 14:24 | 应用程序扩展 | 6,694 KB |
| xweb_resources.dat | 2022/3/1 4:01 | DAT 文件 | 156 KB |

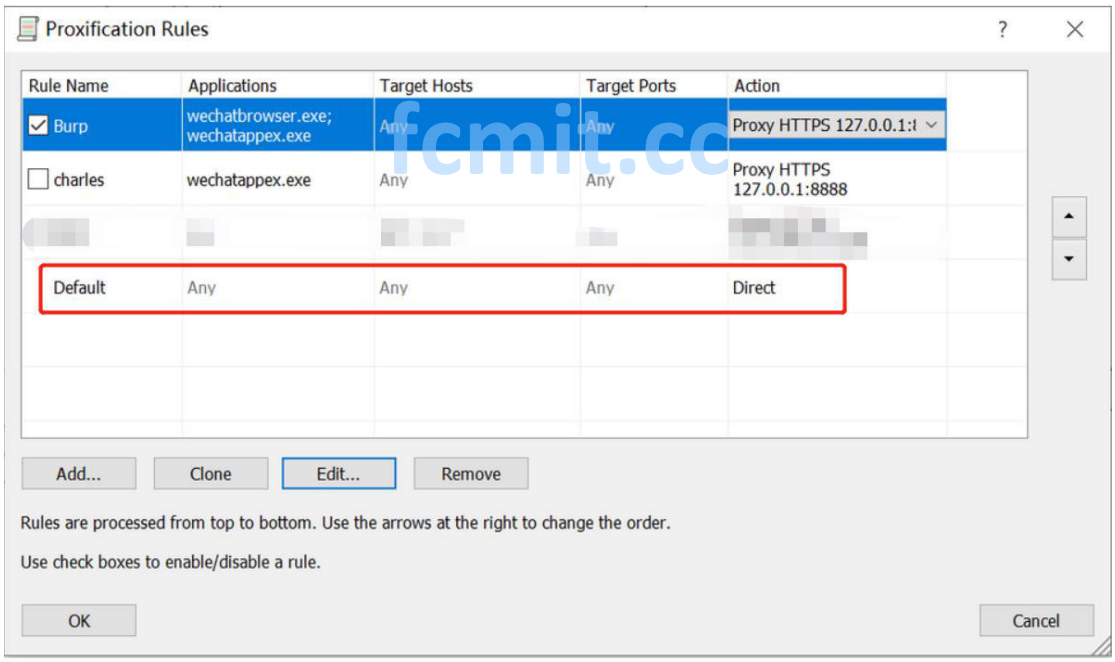
fcmit.cc

**设置 WeChatAppEx.exe 和 wechatbrowser.exe 走 Proxifier 的代理**




然后把下面设置所选代理

到这里设置就完成了，就可以去抓包了




注意最后要选 direct 不然流量出不去