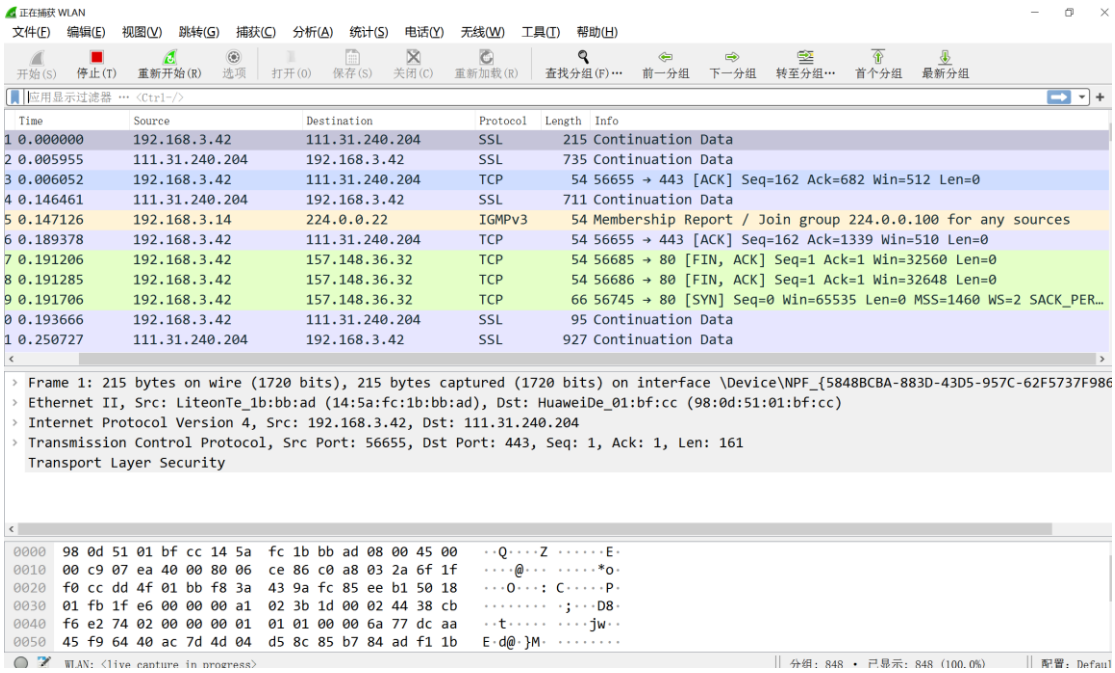
关键词：wireshark，QQ，编辑器（winhex),同一子网，图片文件，捕获。

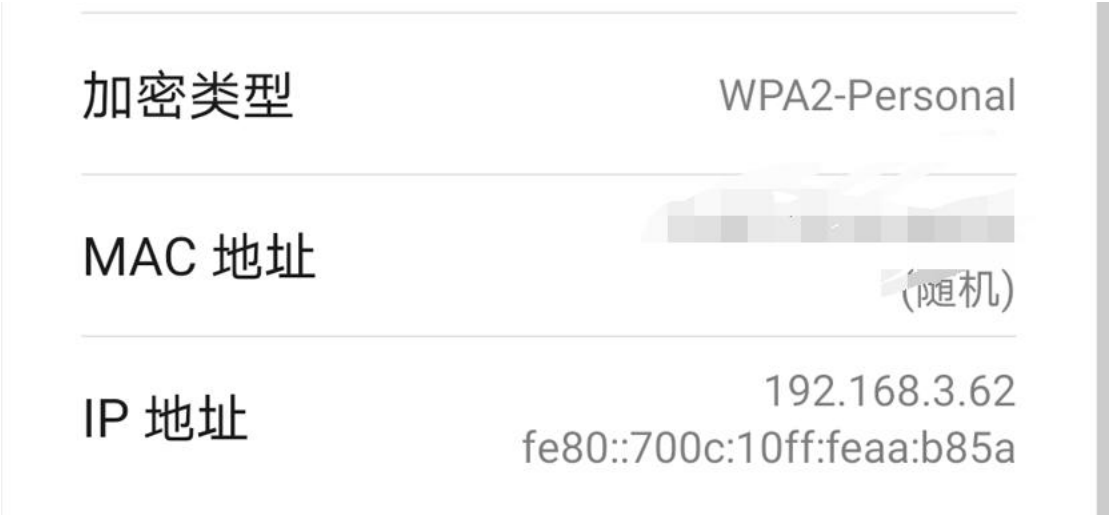
概述：在同一子网下，手机通过聊天软件（QQ）给【我的电脑】发送一张图片(同一子网下是为未加密的)，发送过程通过 wireshark 捕获相关流量，交由 16 进制编辑器 winhex 打开进行编辑，最后还原图片内容。

具体步骤：

1. **打开 wireshark 待命**



2. **查看图片发送端（手机）的 IP 地址：192.168.3.62**



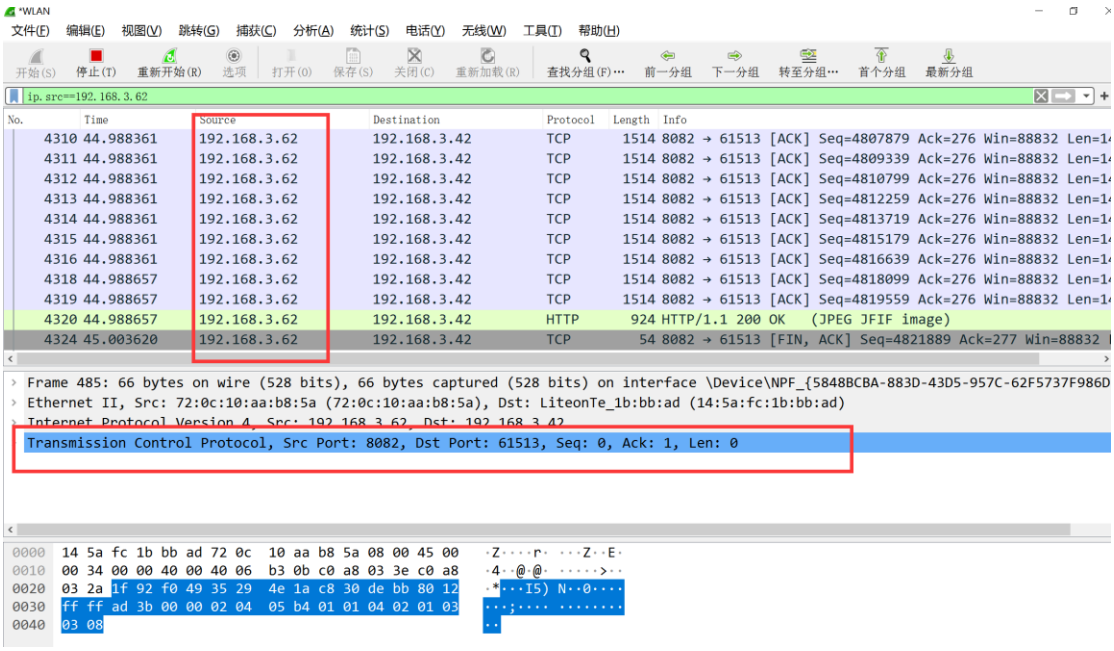
3. 使用 wireshark 显示过滤器，选出源地址为【192.168.3.62】的流量信息

命令语法【ip.src==192.168.3.62】

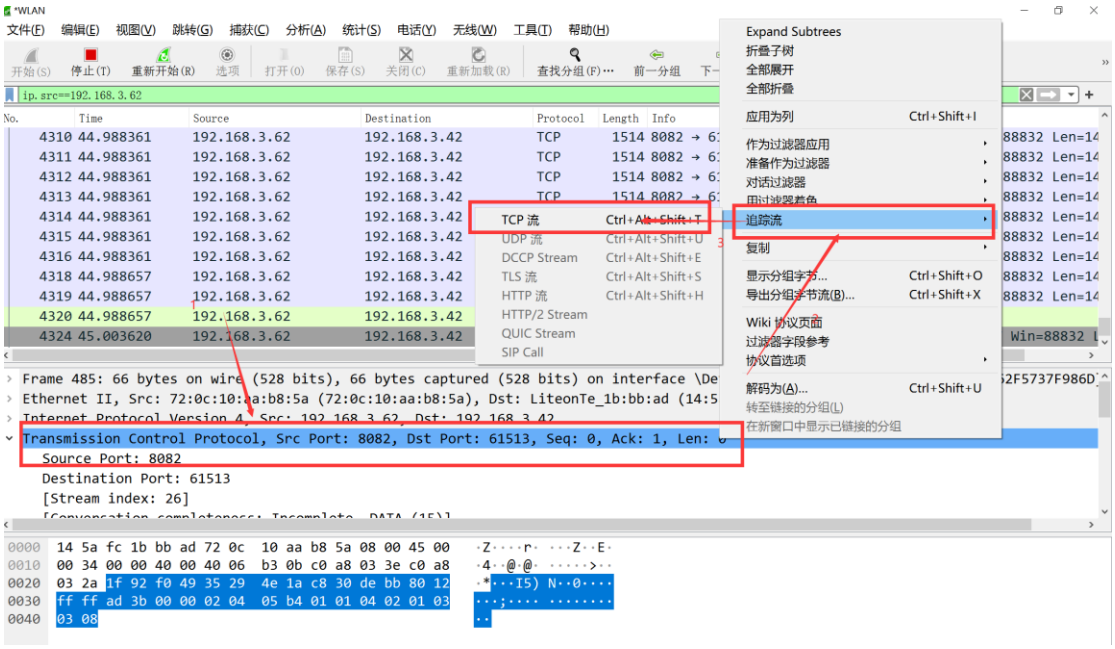
此时我关闭了先前捕获（初始化了），手机未给电脑发送图片，所以没有任何源 IP【192.168.3.62】的流量信息。

4. 手机通过 QQ 给电脑发送一张图片、wireshark 捕获到相关信息

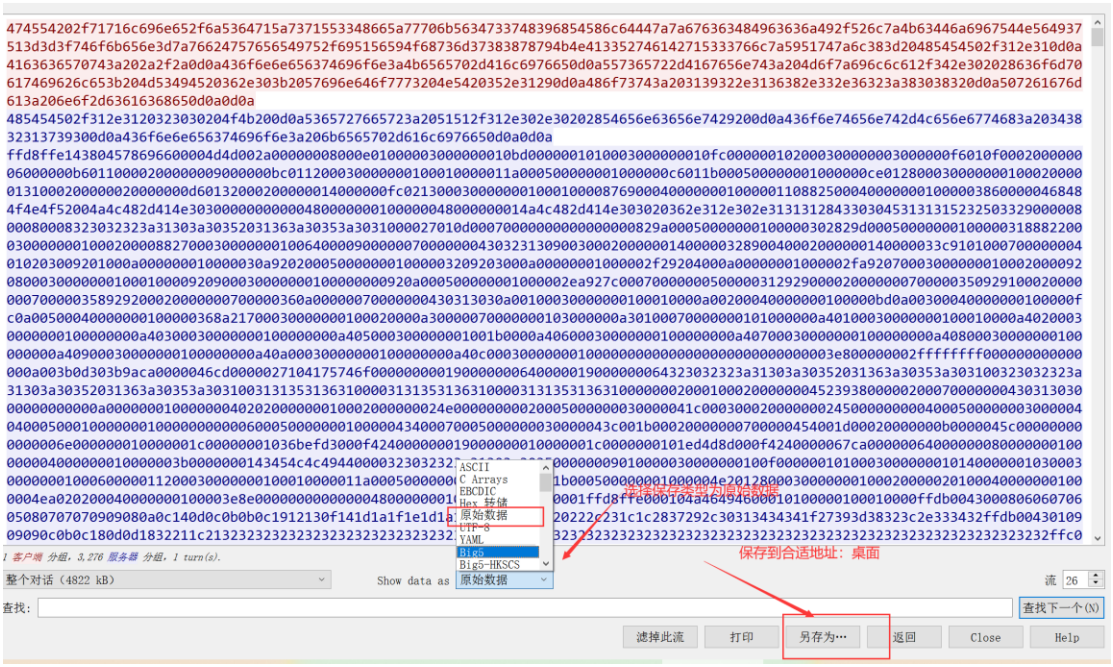
!!! 发送一张新图片，旧图片（先前发过的）可能会捕获不到（我就出现这种情况，通过尝试发送不同图片得以解决）



5.根据传输协议 TCP 选择相应的 TCP 流



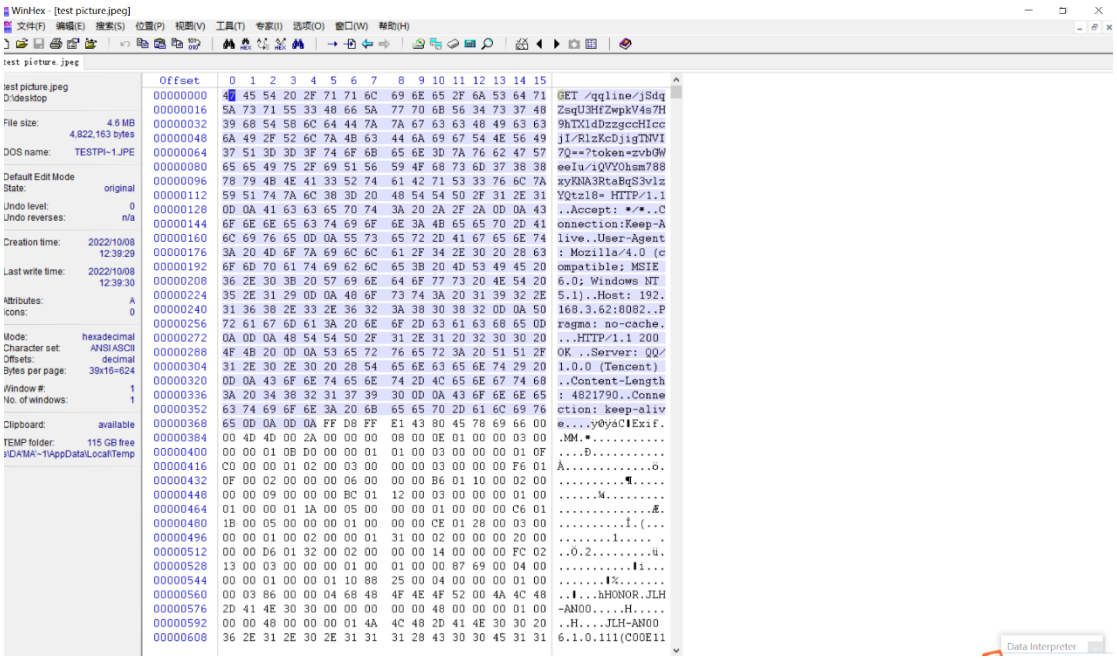
6.将流量信息以原始数据的形式保存到桌面



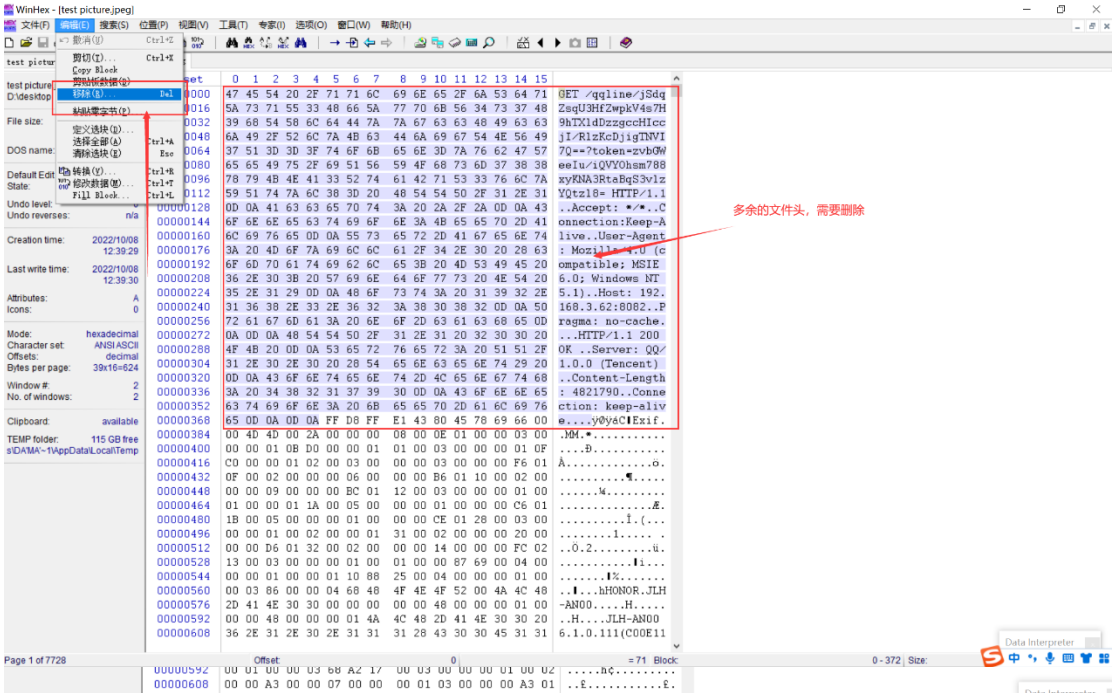
7.发现用 photos 打不开,猜测可能图片格式（JPEG）的文件头存在问题

test picture.jpeg

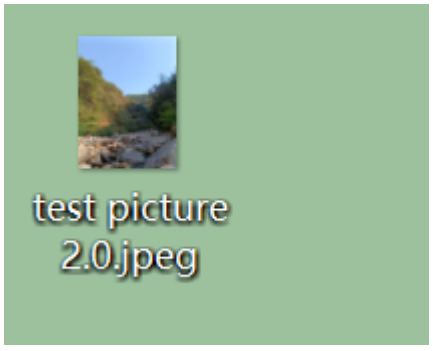
8. 用 16 进制编辑器打开后发现在 JPEG 的文件头【FF D8 FF】存在其他 16 进制编码，造成 JPEG 文件头错误（似乎文件头被一堆 16 进制乱码隐藏了），所以用 photos 打不开【格式错误：文件后缀名与文件不符】。



9．此时果断将 JPEG 文件头【FF D8 FF】前多余部分删除，紧接着保存至合适地方：桌面



11.==========画面豁然开朗==========



用 photos 打开后。。。。。。。。。。。。。。。。。

对比之后。。。。。。。。。。。

猜测正确：图片文件头的问题

猜想：在同一个子网下，两机通过 QQ 传送图片时图片并没有加密，只是隐藏了文件头。

附：