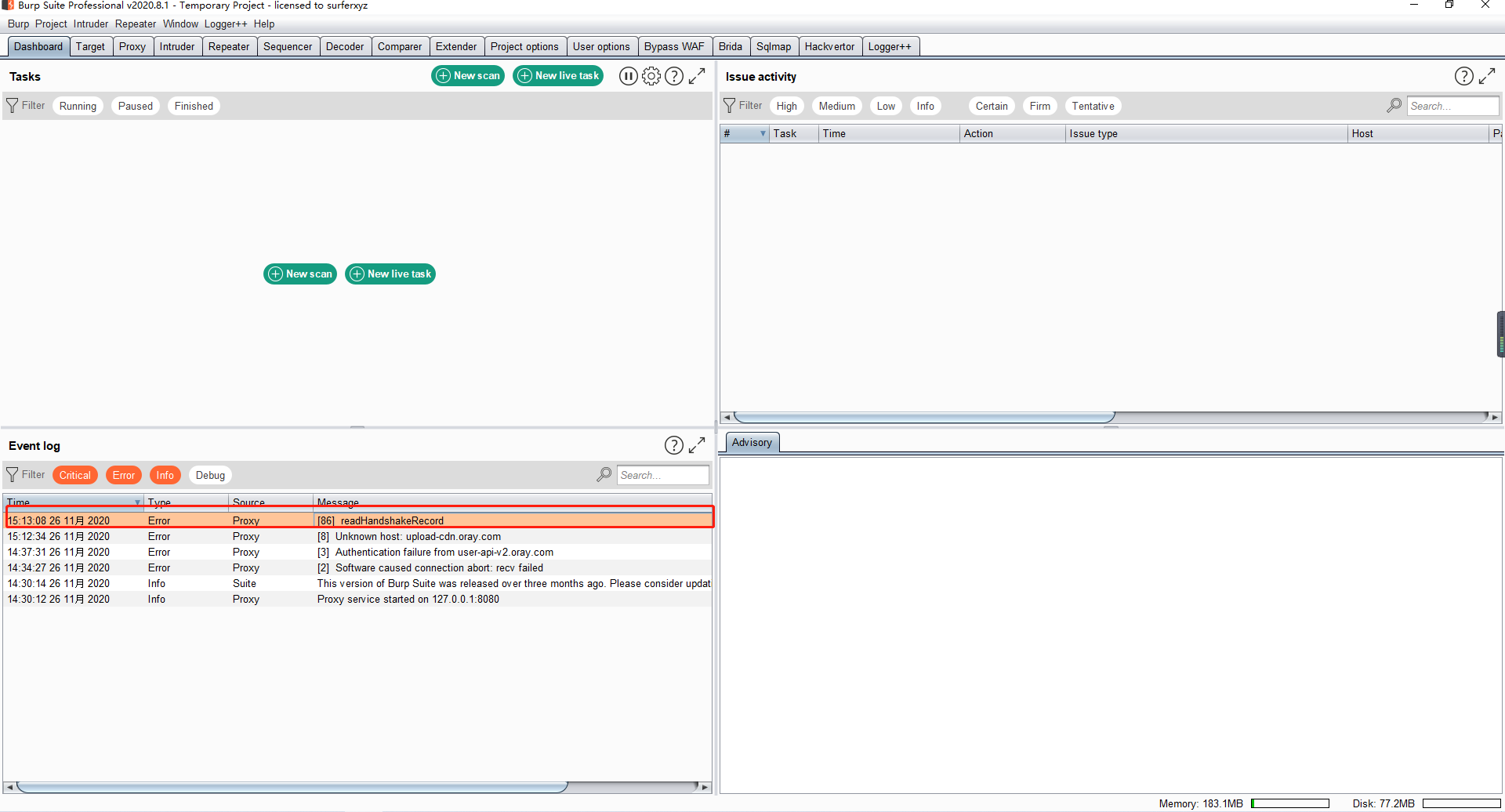
# 绕过非强制证书校验

## 缘起

尝试对某PC端远控程序进行抓包，发现无法成功，burp报错信息如下:

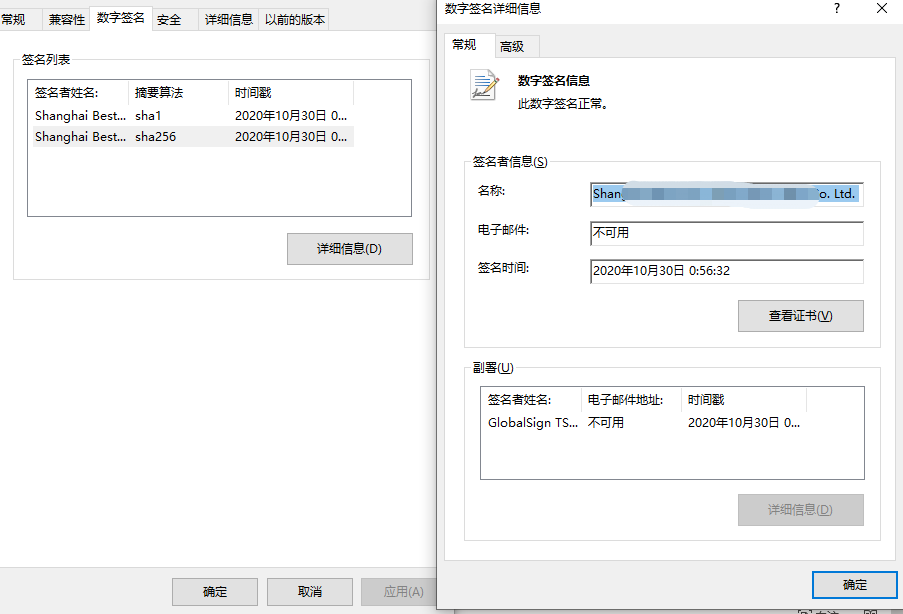


于是就想办法了解并解决该错误。

Ps:当抓包出现问题后不用盲目的去寻找各种方法，burp仪表盘给出的报错就很有用了。我之前就是因未查看该报错导致在错误的思路上花费了不少时间。

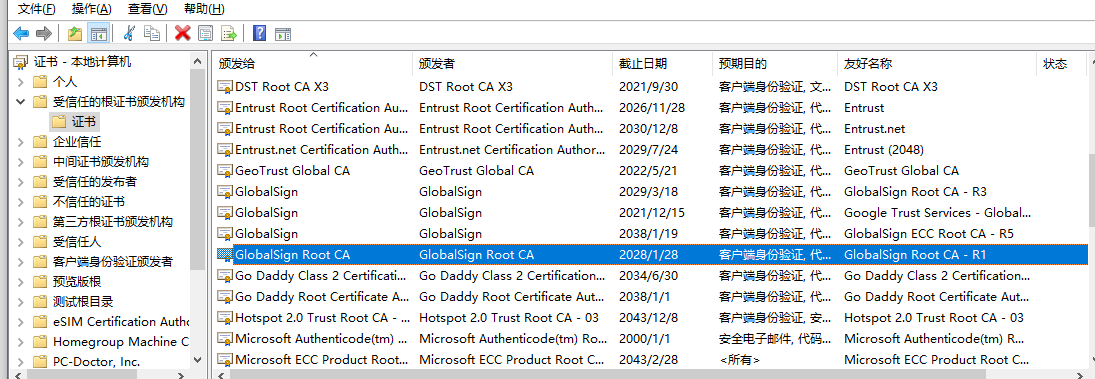
## 缘法

话不多说直接就开始讲如何进行这个非强制校验证书的exe抓包吧，对了搜索上述报错，感觉是证书问题，最后果然没理解错误。



打开程序的安装目录查看exe的属性，去找数字签名查看证书



在管理计算机证书内禁用相关证书，然后在查看证书信息：

直至这个证书状态变更为不可用为至。

然后使用proxifer等代理工具将流量传至burp即可。

## 缘灭

就这么简单的东东卡了我三天，而且还未解决强制证书校验应该如何抓包，不过我将该程序的强制校验证书关闭能抓包后，在开启该功能也能抓包，证明如果能逆向将证书或者校验逻辑更改后应该也可以抓包，不过那个一是没有普适性二是需要较高的技术水准就没有继续研究下去了。最后，就通过基础的抓包就发现自己还有很多需要学习的，且解决问题的思路千万不能跑偏。