# 如何用好抓包工具wireshark————装载插件

设备管理 朱恺 2020-03-04 发表

## 组网及说明

Wireshark是一款开源的抓包软件，同时该软件能够显示很多常见的通用协议，是因为内置了常见协议的解析器。
没错Wireshark就是依靠解析器来分析各种报文。但是如果遇到一些私有开发的报文，wireshark就没办法很好的正常显示了。
这个时候为了方便理解报文，我们可以尝试自己构建解析器。下面我们就来理解一下基本操作和举例。

## 问题描述

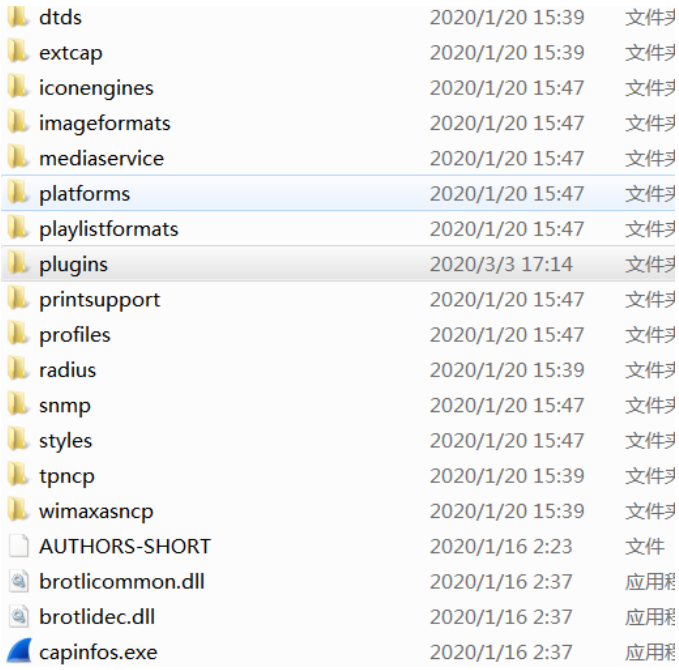
无

## 过程分析

无

## 解决方法

首先我们检查一下wireshark的安装目录，我们可以发现存在一个叫plugins的文件夹，如下：




进入plugins目录，你会发现都是由一些dll文件组成。这些就是wireshark缺省携带的通用解析器。wireshark除了支持dll方式的插件装载，也支持LUA文件的插件装载。LUA是一个简单化轻量级的类似python语言，主要用于可扩展性的程序，wireshark对其有一些些自定义的语法函数规范。一些官方链接介绍：
https://wiki.wireshark.org/Lua
https://www.wireshark.org/docs/wsdg_html_chunked/wsluarm.html
笔者目前也是在尝试接触当中，在能力所及的范围内做了一个关于portal的分析插件。
众所周知，portal协议并不是全球公认的协议标准，在中国主导是CMCC标准，同时每个厂商都有一些私有化的定制，各种属性扩展各有含义和表达方式。在本文的附件中，本人上传了H3C目前采用的标准做的解析器，主要目的是方便问题的排查和报文的解读，存在部分字段暂时值格式问题，不过不妨碍使用理解。
使用方法：把portal.lua放在wireshark安装目录下的plugins就可以了
比如D:\Program Files\Wireshark\plugins。
然后重新启动wireshark软件。

安装完成之后，你就可以通过wireshark去解析portal类型的报文，并且能够解读其中的报文含义。当然这只能用作辅助定位，因为不同厂商的赋值方式可能有所区别。
有能力有兴趣的 还可以参考上诉的官方文档和我的附件插件给其他协议做同样的类比方法，希望通过这款软件能更快更准确的帮助一些网络问题的理解。

**附件下载：** portal插件.rar