5.3 WireShark 通过 HTTP 来抓三次握手包_物联网 / 嵌入式工程师 - 慕课网

> 慕课网慕课教程 5.3 WireShark 通过 HTTP 来抓三次握手包涵盖海量编程基础技术教程，以图文图表的形式，把晦涩难懂的编程专业用语，以通俗易懂的方式呈现给用户。

- ## 一. 前言

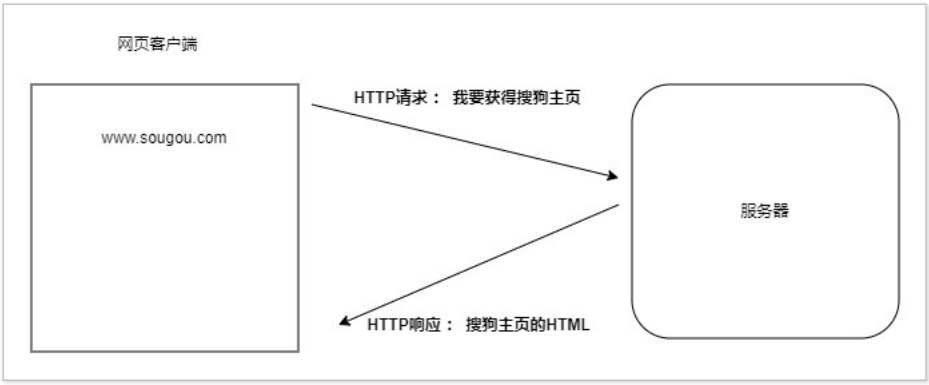
- - 介绍

- HTTP(Hyper Text Transfer Protocol)：我们称之为超文本传输协议，它是一种非常广泛的应用层的协议。该协议在传输层使用的就是 TCP 协议的数据包。本节课，我们来借助 WireShark 工具分 HTTP 协议，来查看对应的 TCP 三次握手数据包。

- - 原理

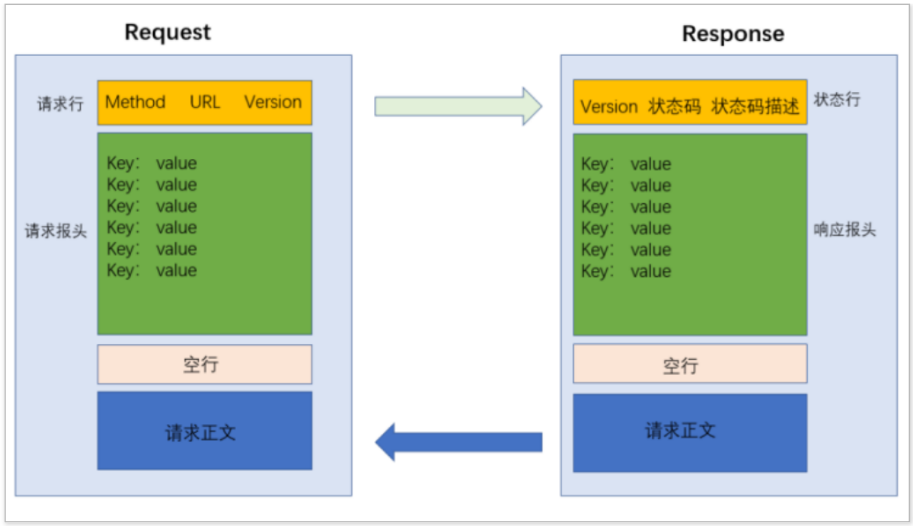
- 当我们在浏览器中输入一个“网址”, 此时浏览器就会给对应的服务器发送一个 HTTP 请求. 对方服务器收到这个请求之后, 经过计算处理, 就会返回一个 HTTP 响应。通过分析请求与相应，我们可用获得对应的 TCP 包信息。

–

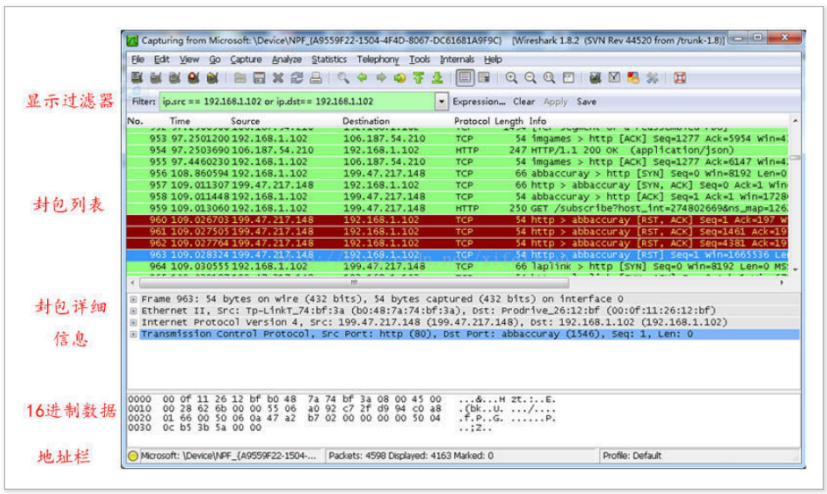


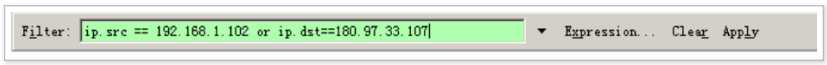
- - HTTP 协议格式

- Method： get / post

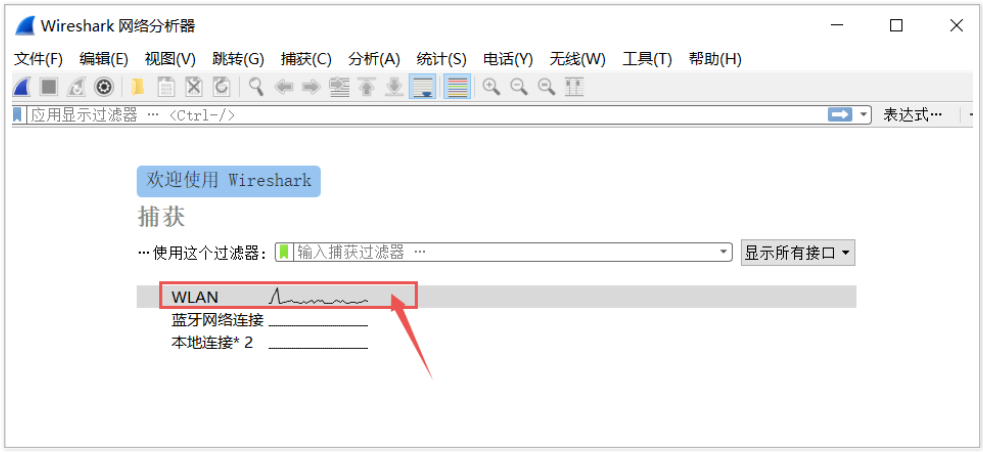


二. WireShake 常用操作介绍

- 窗口介绍
  - Display Filter(显示过滤器)， 用于过滤
  - Packet List Pane(封包列表)， 显示捕获到的封包， 有源地址和目标地址，端口号。
  - Packet Details Pane(封包详细信息), 显示封包中的字段
  - Dissector Pane(16 进制数据)
  - Miscellanous(地址栏，杂项)
  - 

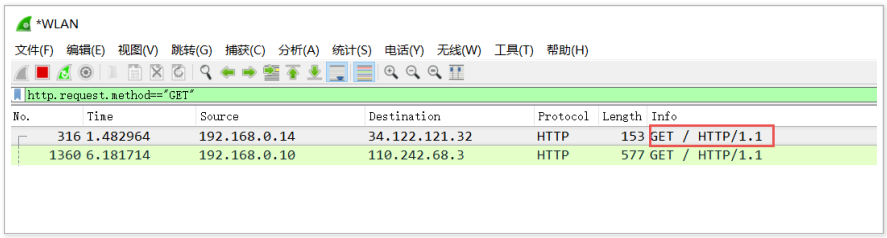
- 显示过滤
  - 

  - 过滤常用规则
    - 协议过滤
      - tcp 只显示 TCP 协议
      - udp 只显示 UDP 协议
      - http 只显示 http 协议
    - IP 过滤
      - ip.src == 192.168.0.88
      - ip.dst == 192.168.0.120
    - 端口过滤
      - tcp.port = 8000
      - udp.port = 9000
    - http 模式过滤
      - http.request.method =“GET”只显示 HTTP GET 方法。



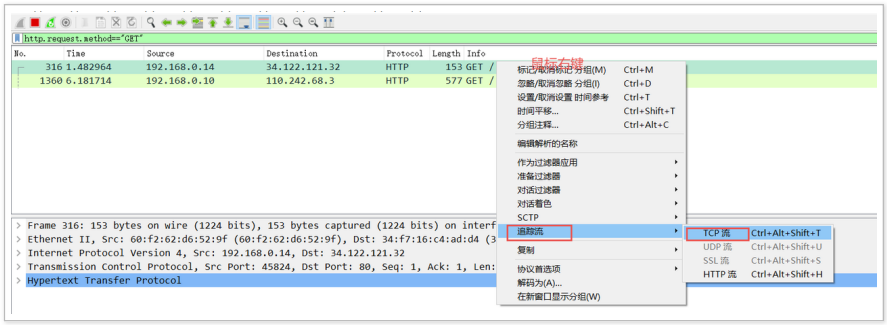

```
http.request.method == "GET"
```

之后，会出现很多 HTTP 相关协议，可以通过百度多登录几个网页，找到 HTTP/1.1 相关数据的。

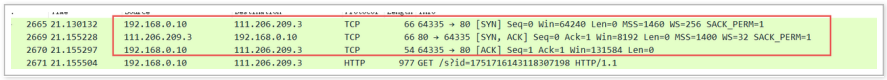


- 通过分析 HTTP 协议，来分析三次握手的数据包。选择 HTTP/1.1 相关数据。

鼠标右键——追踪流——TCP 流



说明：由于网络上的数据流比较复杂，有的时候解析出来的不一定是三次握手包。重新刷新网页，再次按照上述步骤抓取就可。



四. 课后任务

练习：大家自己利用 wireshark 通过 HTTP 协议来抓以下 tcp 三次握手包，抓到后把对应的截图上传。

全文完