如何用好抓包工具wireshark————报文排序

设备管理 朱恺 2020-02-26 发表

组网及说明

用好wireshark工具的各种技巧能够帮助快速找到网络问题的种种蛛丝马迹，而数据整理中排序又是一个很关键的一步。你真的会排序吗？

问题描述

无

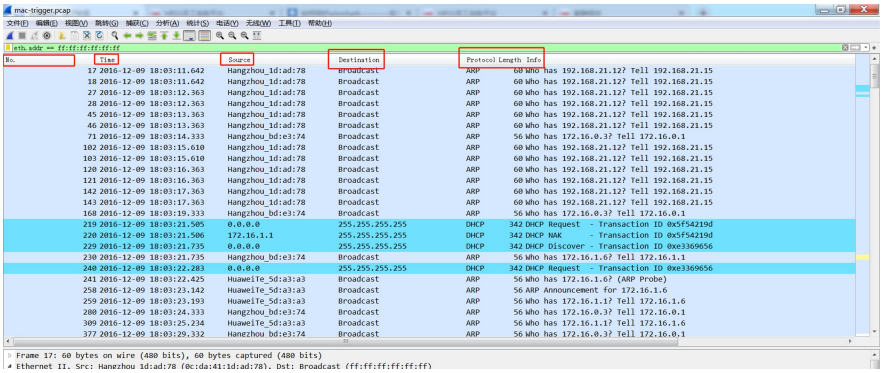
过程分析

无

解决方法

我们先来看一个默认例子：

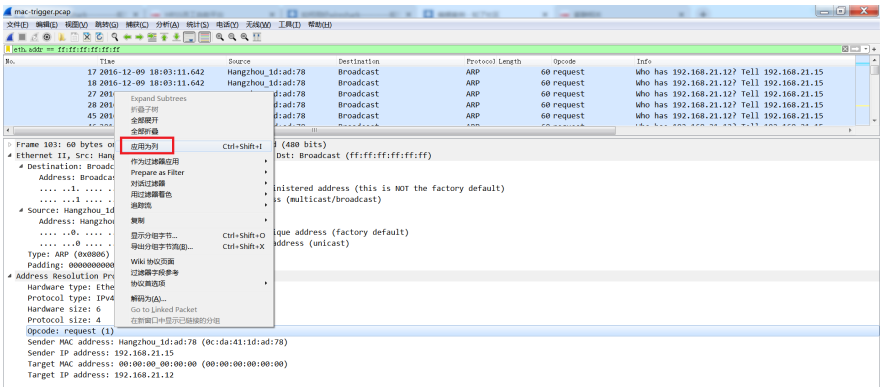
缺省的报文显示列中，有序号、时间、源地址、目的地址、协议类型、字节长度、和信息info



缺省规则是按照序号进行排序，其实也就是时间发生顺序。

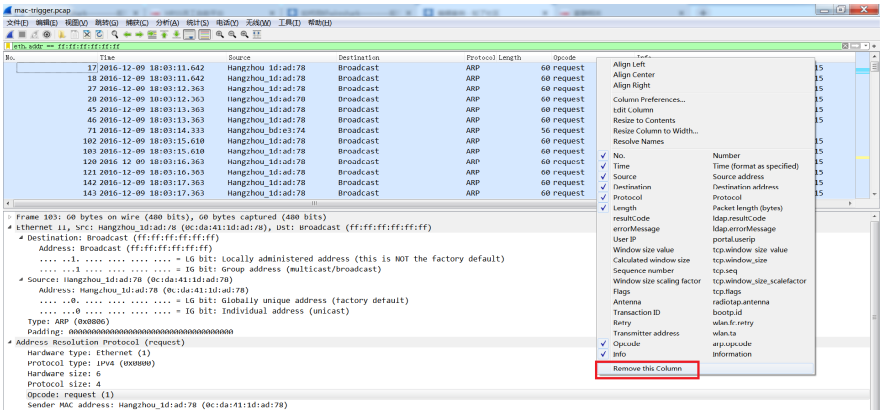
那么第一个问题：我如何增加列？

选择一个感兴趣的规则然后右键，找到应用为列。



这样就可以给自己想要加入的规则进行作为列选取排序，按照降序按照升序都可以，想要比较的数据就一目了然。

如果要删除这个列 也可以在列上右键 点击remove，有的版本wireshark也叫hidden。

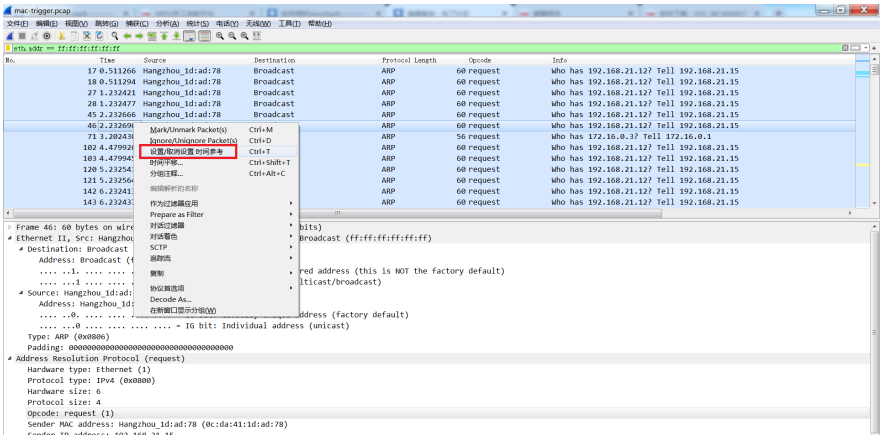


然后第二个小技巧：时间调整

图示中的时间显示为2016-12-09 然后具体时刻，我们可以在

视图→时间显示格式 里面进行选择适合自己报文分析的时间体现。时间的判断对一些问题的判断非常

重要。
当时间显示格式 选择为“自动“和”自捕获开始经过的时间“，我们还可以在报文上右键 选择设置为参考时间。



这样就能设置该时刻为参考原点，后续报文以此计算经历的时间。某些时候这个方法也能让我们分别甄别报文的顺序关系。
同时我们对特别关注的报文还能mark标记，标记后的报文就会按照颜色为黑色显示。

有了上述这些技巧，是不是感觉又有技能增长了？那么快去试试你的理解吧。