10.5.3 学到的知识

看完这个「犯罪剧」，你一定学到了很多关于调查网络通信问题的知识。当「犯罪」发生后，侦探开始问讯受害者。找到线索，顺藤摸瓜，直到找到罪魁祸首。

在这个场景中，我们一开始先查看了受害者（工作站），然后找到了 DNS 通信问题这个线索。这个线索将我们带到分支 DNS 服务器，然后又到中心 DNS 服务器，最终找到路由器，也就是问题的来源。

在分析时，请尝试从数据包中找出线索。线索不一定能告诉你谁是「罪犯」，但通常它们最终能帮你找出来。