華北水利水電大學

North China University of Water Resources and Electric Power

计算机网络

实验六：分析网络数据包

姓　名：高树林

学　号：202018526

专　业：人工智能

院　系：信息工程学院

一、实验目的

1、DNS 是计算机网络中重要的一部分，它负责将域名解析为 IP 地址，使得各种网络应用可以被正确地转发到目标服务器。

2、通过抓包分析了解 DNS 的工作原理，同时掌握抓包分析工具的使用方法。

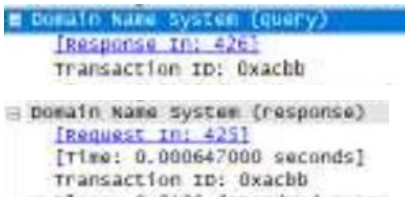
二、实验内容

1. 利用 eNSP 进行模拟实验配置
2. 利用 Wireshark 进行数据包的抓取
3. 对数据包进行分析

三、实验过程

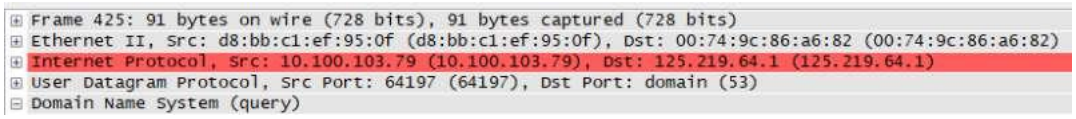
步骤 1：协议数据包窗口

从包到达的时间，顺序以及源和目的 IP 地址可知，这是一对 DNS 请求与应答报文。下图为 1 号包与 2 号包中 DNS 段的报文分析注释，由此可证明，包 1 为 DNS 请求报文，包 2 为包 1 的应答报文，请求与应答报文的到达间隔时间为 0.022177000s，它们的标识字段都为 0xf03aH，用于相互匹配。

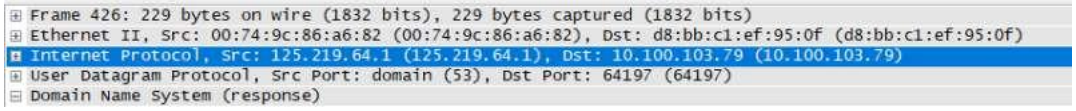


因为 DNS 请求报文的目的是请求 www.soku.com 的 IP 地址，故包 1 的源 IP 地址为本机 IP，目的 IP 地址为 DNS 服务器的 IP，包 2 与包 1 相反。

DNS 请求报文：



DNS 应答报文：



可以看出，DNS 请求报文与应答报文链路层的 MAC 地址相反，请求报文中的源物理地址为本机的物理地址，这与 IP 地址相对应。此外，DNS 请求报文与应答报文传输层中 UDP 的源端口与目的端口相反，其中请求报文 UDP 的源端口为客户机动态申请的本地端口，目的端口为 DNS 所固有的 53 号周知端口。这两点都体现了 DNS 请求报文与应答报文间的请求-应答关系。

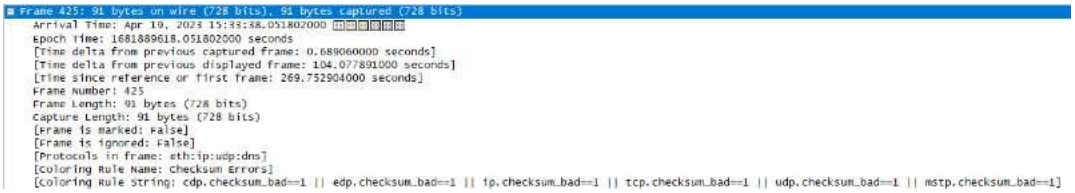
DNS 请求报文与应答报文协议树窗口显示的协议层次与网络协议的层次对应相同，如下表：

树节点名称	对应的协议层次	说明
Frame	物理层	

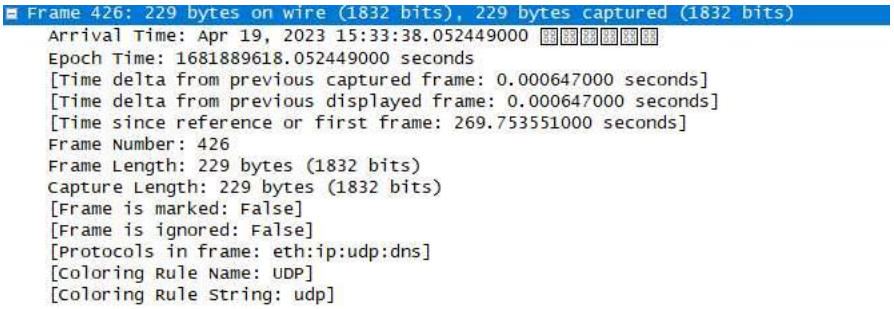
Ethernet II	数据链路层	以太网协议
Internet Protocol	网络层	IP 协议
User Datagram Protocol	传输层	UDP 协议
Domain Name System	应用层	DNS 域名系统

步骤 2：物理层节点

DNS 请求报文：



DNS 应答报文：

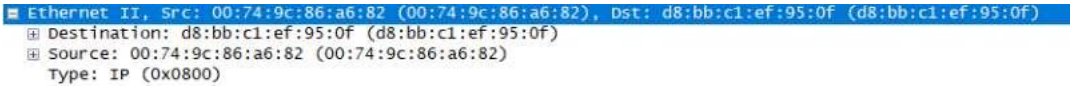


以上两张图分别给出了 DNS 请求报文与应答报文的时间参数、包号、长度与协议层次，在此不一一细说。但是，我们可以很清楚的看出，DNS 请求报文的长度为 91 字节，而应答报文的长度为 229 字节，比请求报文长得多。这是由于在 DNS 应答报文中，具有请求报文所没有的回答部分、授权部分与附加部分，在下面的应答报文分析中会具体说明。

步骤 3：数据链路层节点

DNS 请求报文：

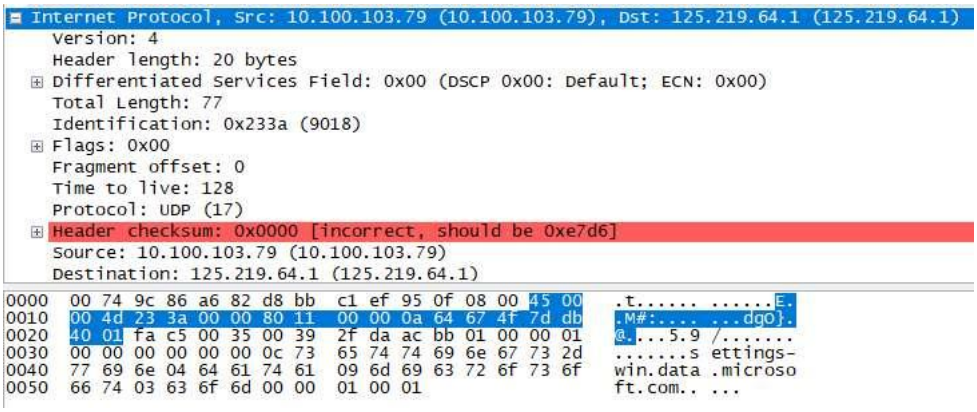
DNS 应答报文：



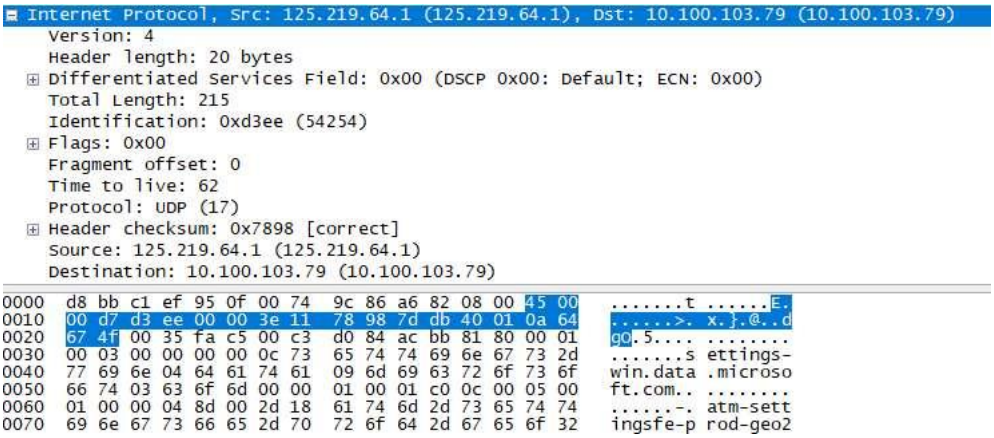
由上图可以更明显的看出，DNS 请求与应答报文的源与目的 MAC 地址的相反现象。此外，DNS 请求与应答报文以太网协议中的类型均为 IP，即在 DNS 协议层次中网络层协议为 IP，这体现了 DNS 作为 TCP/IP 协议簇中协议的特点。

3.5 IP 节点

DNS 请求报文：



DNS 应答报文：



DNS 请求与应答报文 IP 层相同点：

版本号：IPv4

首部长度：20 字节，没有其他选项

服务类型：最低优先级的一般服务

片偏移：0，无分片

协议标识：UDP（0x11H）

DNS 请求与应答报文 IP 层不同点：

数据报长度：上文已有分析。

标识不同，因为请求与应答为两个不同的报文，信源机给予的用于区分分片的标识不同。

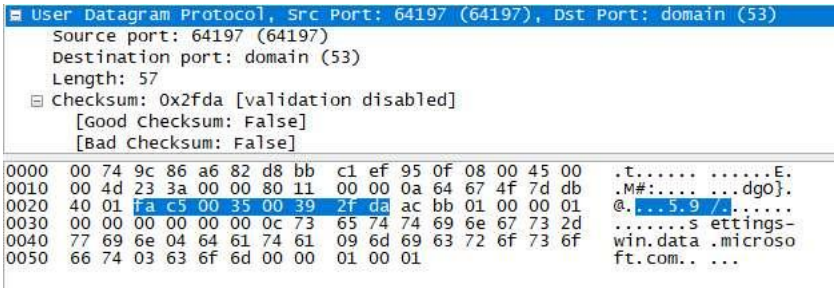
生存时间不同，请求报文为 128，应答报文为 62。

校验和不同，DNS 请求与应答报文 IP 层首部不同，故校验和不同。

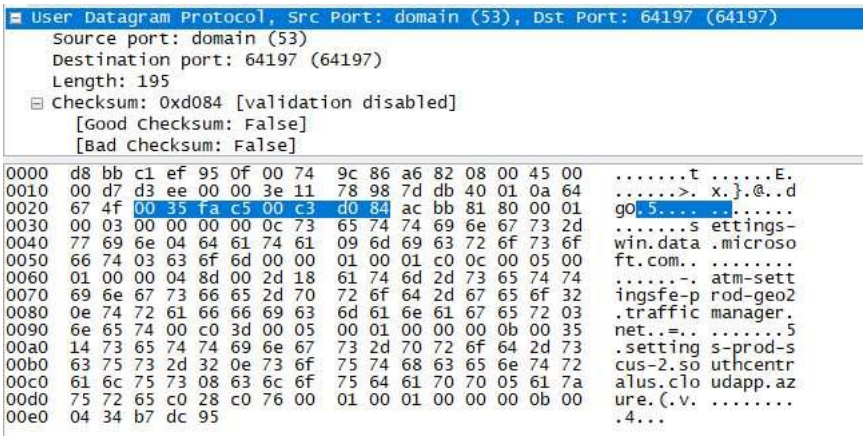
源与目的 IP 地址不同，原因在前面的分析中已经说明。

步骤 4：UDP 节点

DNS 请求报文：



DNS 应答报文：

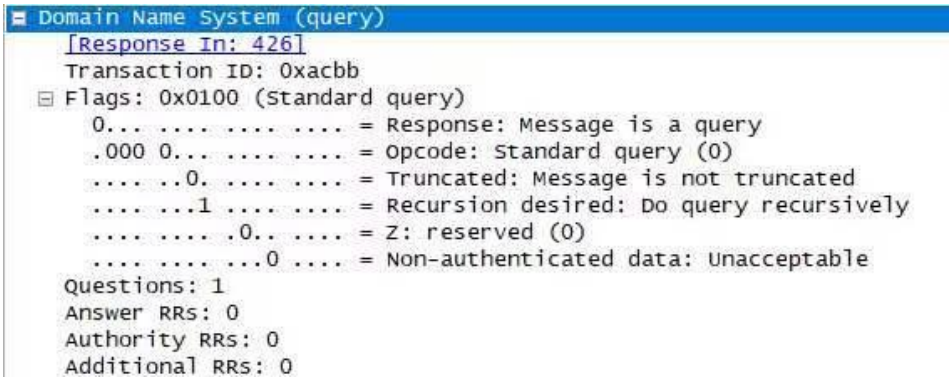


DNS 请求与应答报文的源与目的端口相反，原因在前面的分析中已经说明。
请求报文 UDP 长度为 57 字节，应答报文 UDP 长度为 195 字节。

步骤 5：UDP 节点

DNS 请求报文

首部：



标识字段：0xacbbH，用于匹配请求与响应

标志字段：0x0100H

QR：0，为请求报文

OpCode：0000（0），标准查询（正向解析）

AA：0，此字段只在服务器的响应中有效，在上图中不显示

TC：0，报文没有被截断

RD：1，请求服务器进行递归解析

RA：0，此字段只在服务器的响应中有效，在上图中不显示

3 比特保留位：000

rCode：0000，没有错误

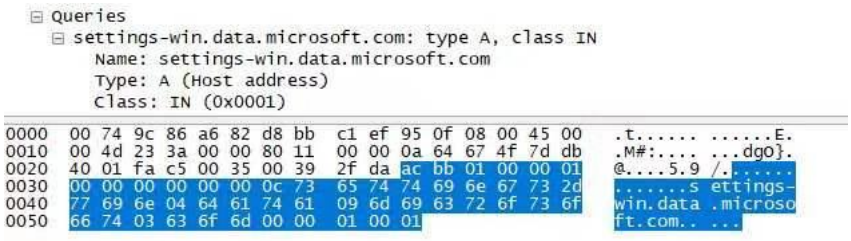
问题记录数：1

回答记录数：0（DNS 请求报文此字段为 0）

授权记录数：0（DNS 请求报文此字段为 0）

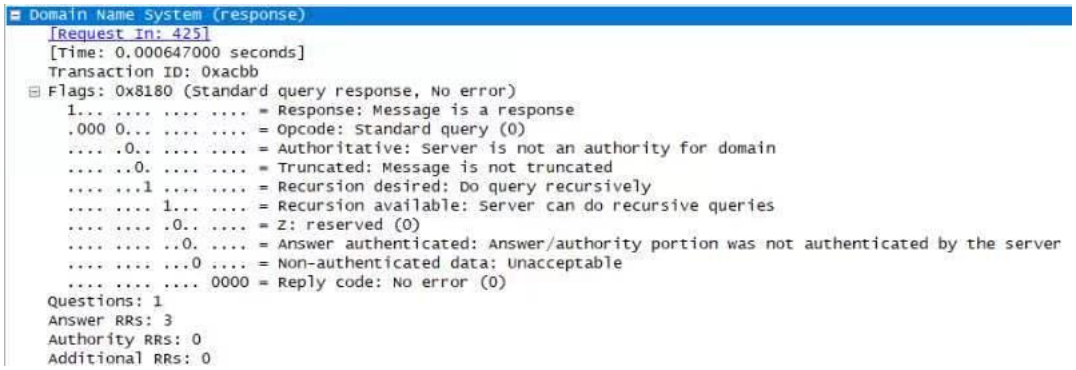
附加信息记录数：0（DNS 请求报文此字段为 0）

问题部分：



DNS 应答报文

首部：



标识字段：0xacbbH，用于匹配请求与响应，此处与 DNS 请求报文相匹配。

标志字段：0x8180H

QR：1，为应答报文

OpCode：0000（0），标准查询（正向解析）（与请求报文相同）

AA：0，回答的服务器是该域的授权服务器

TC：0，报文没有被截断

RD：1，请求服务器进行递归解析（与请求报文相同）

RA：1，服务器支持递归解析（回应 RD）

3 比特保留位：000

rCode：0000，没有错误

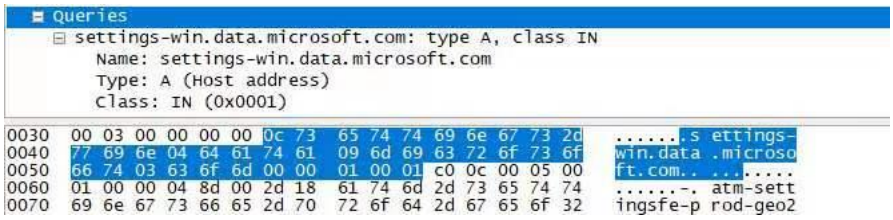
问题记录数：1

回答记录数：3

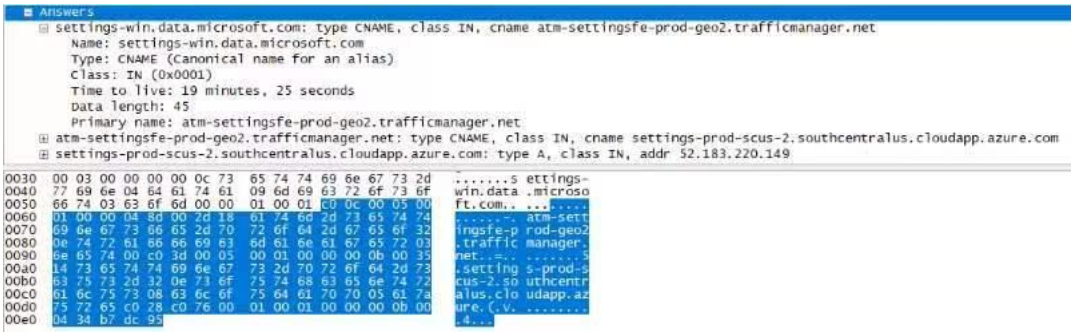
授权记录数：0

附加信息记录数：0

问题部分：



回答部分：



域名：0xC00CH，为指向问题部分询问名的指针，具体地址为 00000000001100（二进制地址）

类型：CNAME，数值为 1，记录类型为 IPv4 地址，用于域名到 IPv4 地址的转换。

类：IN，数值为 1，表示因特网协议。

生存时间：15min

资源数据长度：45 字节

四、心得体会

抓取 DNS（Domain Name System）数据包是一种分析网络通信的常见技术，可以提供有关域名解析的详细信息。以下是我对抓取 DNS 数据包的心得体会：

使用适当的工具：有许多网络抓包工具可用于捕获 DNS 数据包，如 Wireshark、tcpdump 等。选择适合你需求的工具，并熟悉其基本用法和功能。

设置过滤条件：DNS 数据包可能会非常频繁地发生，为了避免混乱和信息过载，设置适当的过滤条件非常重要。你可以根据目标 IP 地址、端口号、协议类型等设置过滤条件，以仅捕获你感兴趣的 DNS 通信。

分析数据包头部：DNS 数据包的头部包含了许多重要的信息，如查询类型（Query Type）、响应码（Response Code）、查询/响应标志位等。仔细分析这些头部字段可以帮助你了解 DNS 交互的细节和结果。

追踪域名解析过程：DNS 数据包捕获提供了一个机会，让你跟踪域名解析的整个过程。你可以看到客户端发送的查询请求、中间 DNS 服务器的转发和响应，以及最终的解析结果。这对于诊断 DNS 问题和了解域名解析性能非常有帮助。

关注时序和延迟：通过分析捕获的 DNS 数据包，你可以观察到域名解析的时序和延迟情况。你可以检查查询和响应之间的时间间隔，发现是否存在潜在的延迟问题，并根据需要采取相应的措施。

结合其他信息进行分析：DNS 数据包通常只提供了有关域名解析的信息，但结合其他相关的网络数据，如 HTTP 请求、SSL 握手等，可以获得更全面的上下文

信息，帮助你更好地分析和理解 DNS 通信。

隐私和合规性：在进行 DNS 数据包捕获和分析时，要确保遵守适用的隐私和合规性规定。确保你的操作符合相关法律法规，并且尊重用户隐私。

总的来说，抓取 DNS 数据包可以为网络管理员、安全专家和开发人员提供有价值的信息，帮助诊断问题、改善性能，并加强网络安全。然而，在进行数据包捕获和分析时，必须谨慎行事，并且遵守适用的法律和道德准则。