计算机学院 计算机网络 课程实验报告

实验题目：深入理解 DNS 域名系统		学号：202200400053
日期：2024-03-22	班级： 2 班	姓名： 王宇涵
Email：1941497679@qq.com		

实验方法介绍：

1. 通过访问一些网站或执行 DNS 查询操作: 分析 DNS 查询和响应.
2. 在 Wireshark 中观察捕获的数据包，可以利用 Wireshark 的过滤器功能来过滤出与 DNS 相关的数据包，这样可以更轻松地分析 DNS 查询和响应.

实验过程描述：

一 ： nslookup

输入 nslookup www.iitb.ac.in 和 nslookup -type=NS iitb.ac.in 观察结果

```
Microsoft Windows [版本 10.0.22621.3296]
(c) Microsoft Corporation。保留所有权利。

C:\Users\Lenovo>nslookup www.iitb.ac.in
服务器:  pdns.dnspod.cn
Address:  119.29.29.29

非权威应答:
名称:    www.iitb.ac.in
Address:  103.21.124.10


C:\Users\Lenovo>nslookup -type=NS iitb.ac.in
服务器:  pdns.dnspod.cn
Address:  119.29.29.29

非权威应答:
iitb.ac.in      nameserver = dns3.iitb.ac.in
iitb.ac.in      nameserver = dns1.iitb.ac.in
iitb.ac.in      nameserver = dns2.iitb.ac.in
```

回答问题:

1. **查找获取位于印度孟买的印度理工学院 Web 服务器的 IP 地址：www.iitb.ac.in 的 IP 地址是什么?**

答 ：103.21.124.10

2. 为您提供答案的 DNS 服务器的 IP 地址是什么?

答: 119.29.29.29

3. 上述问题 1 中的命令来自权威服务器还是非权威服务器？

答: 非权威服务器

4. 使用查找命令来确定 iit.ac.in 域的权威名称服务器的名称。那名字是什么？（如果有多个权威服务器，则返回的第一个权威服务器的名称是什么？如果您必须找到该权威名称服务器的 IP 地址，您会怎么做?

```
C:\Users\Lenovo>nslookup dns3.iitb.ac.in
服务器:  pdns.dnspod.cn
Address:  119.29.29.29

非权威应答:
名称:    dns3.iitb.ac.in
Address:  103.21.127.129
```

答 ：名字为 dns3.iitb.ac.in. 若必须要找到 IP 地址则再进行一次查询即可: 返回 IP103.21.127.129

二 ： DNS cache

1. 输入命令ipconfig /flushdns清除DNS缓存，打开 Web 浏览器并清除浏览器缓存。

```
C:\Users\Lenovo>ipconfig/flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
```

2. 打开Wireshark并输入ip.addr == 172.25.241.46进入显示过滤器，使用此过滤器，

   Wireshark 将仅显示源自或发往您的主机的数据包。

在 Wireshark 中启动数据包捕获。

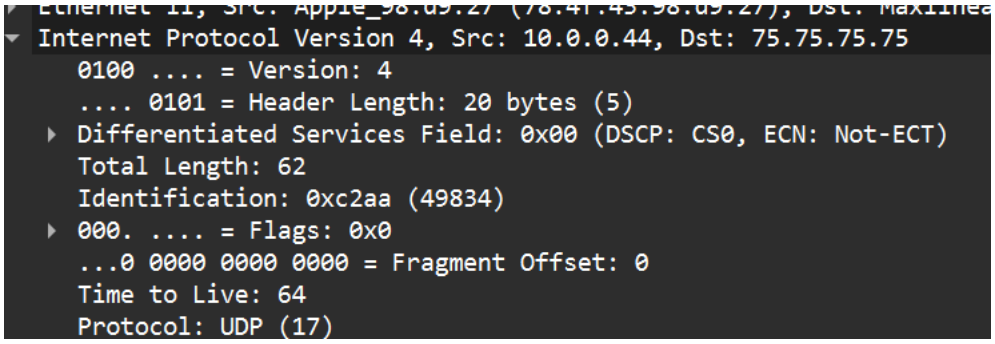
使用浏览器访问网页：http://gaia.cs.umass.edu/kurose_ross/ 停止数据

3. 使用作者捕获的包进行实验

回答问题 ：

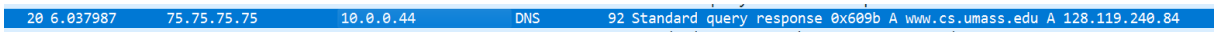
5. 找到解析名称 gaia.cs.umass.edu 的第一条 DNS 查询消息。包裹号码是多少?

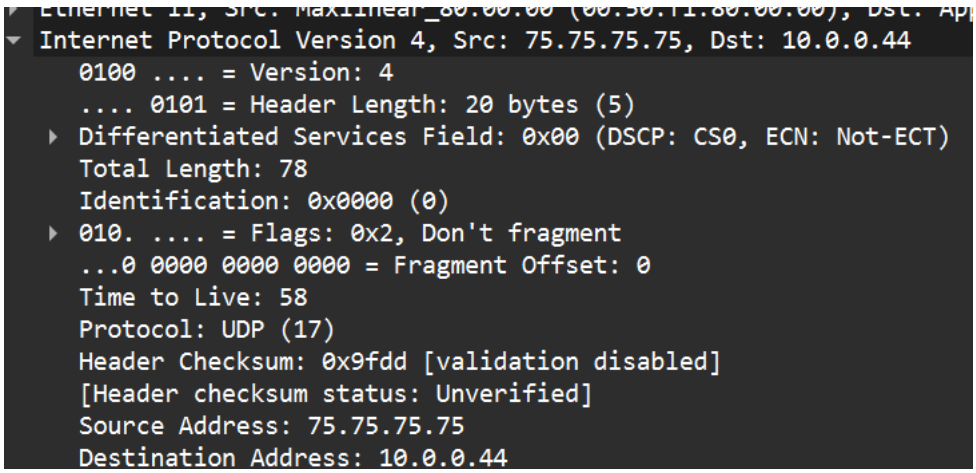
在 DNS 查询消息的跟踪中?该查询消息是通过 UDP 还是 TCP 发送的?



答: 包裹号码为19, 该消息是由UDP发送的

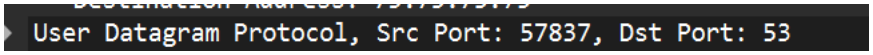
6. 现在找到对初始 DNS 查询的相应 DNS 响应。DNS 响应消息跟踪中的数据包编号是多少? 该响应消息是通过 UDP 还是 TCP 接收的?





答: 编号为 20, 由 UDP 接受的

7. DNS 查询报文的目的端口是什么?DNS 响应报文的源端口是什么?

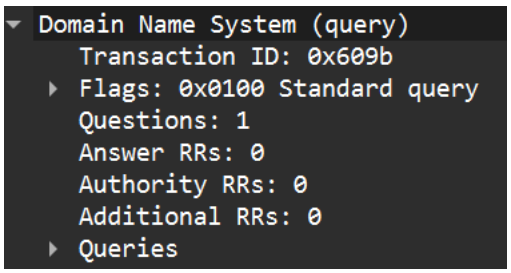


答: 均为 53

8. DNS 查询报文发送到什么 IP 地址?

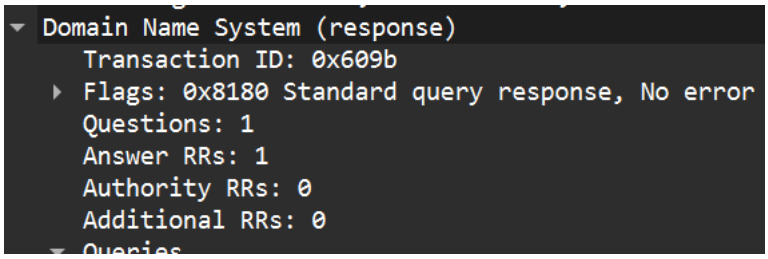
答: 75.75.75.75

9. 检查DNS 查询消息。此 DNS 消息包含多少个“问题”？它包含多少个答案？



答: 1 个问题, 0 个回答

10. 检查对初始查询消息的 DNS 响应消息。此 DNS 消息包含多少个“问题”？它包含多少个答案?

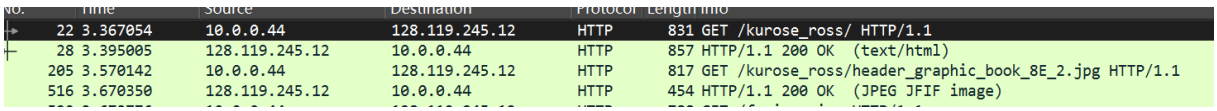


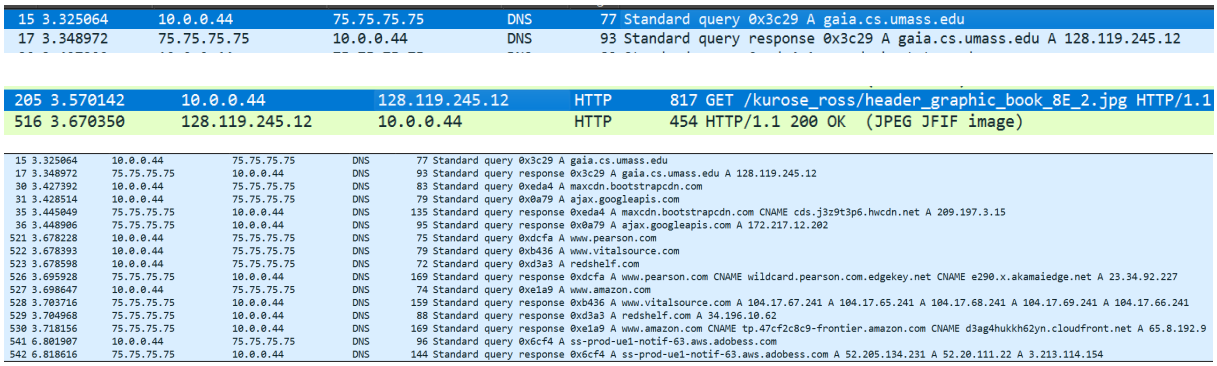
答 ：1个问题, 1个回答

11. 基本文件的网页 http://gaia.cs.umass.edu/kurose_ross/ 引用图像对象 http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg，与基本网页一样，位于 gaia.cs.umass.edu。

基本文件 http://gaia.cs.umass.edu/kurose_ross/的初始 HTTP GET 请求的跟踪中的数据包编号是多少？为了解析 gaia.cs.umass.edu 以便将此初始 HTTP 请求发送到 gaia.cs.umass.edu IP 地址而进行的 DNS 查询跟踪中的数据包编号是多少？收到的 DNS 响应跟踪中的数据包编号是多少？

图像对象 http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg 的 HTTP GET 请求跟踪中的数据包编号是多少？为了解析 gaia.cs.umass.edu 以便将第二个 HTTP 请求发送到 gaia.cs.umass.edu IP 地址，DNS 查询中的数据包编号是多少？讨论 DNS 缓存如何影响最后一个问题的答案。





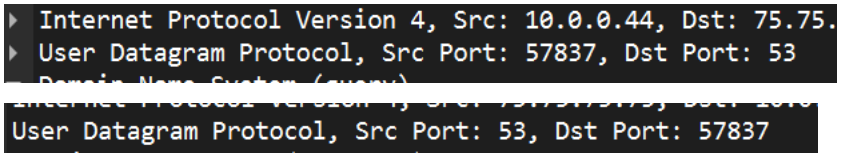
答: HTTP GET 请求的数据包编号为 22, 解析的 DNS 查询数据包编号为 15, 收到的 DNS 响应跟踪的数据包编号为 17.
图像对象的 HTTP GET 请求的数据包编号为 205, 未发现再次解析的 DNS 查询数据包编号.

原因解释 ： 当主机需要调用DNS 服务时， 该主机首先会检查所需的 DNS 记录是否驻留在该主机的

DNS 缓存中；如果找到该记录，主机甚至不会费心联系本地 DNS 服务器，而是使用此缓存的 DNS 记录, 因此再次进行 HTTP GET 请求无需解析域名.

三 ： Play With nslookup

12. DNS查询报文的目的端口是什么？DNS响应报文的源端口是什么？

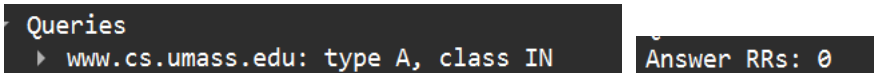


答 ： 查询目的端口为 53, 响应源端口为 53

13. DNS查询报文发送到什么IP地址？这是您默认本地 DNS 服务器的 IP 地址吗？

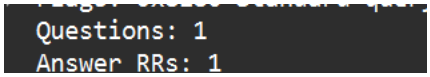
答 ： 发送到 75.75.75.75, 这应该是作者抓包时本地 DNS 服务器的 IP 地址

14. 检查 DNS 查询消息。DNS 查询是什么“类型”？查询消息中是否包含任何“答案”？



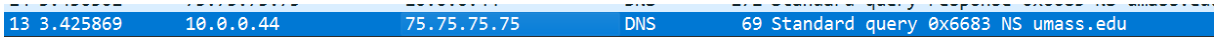
答 ： 类型 ：A 不包含任何答案

15.检查对查询消息的 DNS 响应消息。此 DNS 响应消息包含多少个“问题”？有多少个 “答案” ？



答 ：1个问题, 1个答案

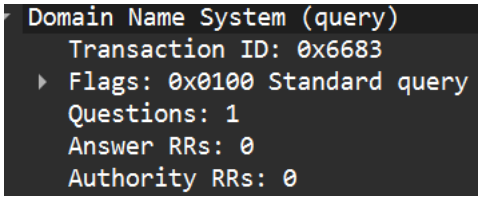
四：打开命令行输入命令 nslookup -type=NS umass.edu并抓包



16. DNS 查询报文发送到什么 IP 地址？这是您默认本地 DNS 服务器的 IP 地址吗？

答 ： 发送到 75.75.75.75，应该是本地 DNS 的 IP 地址.

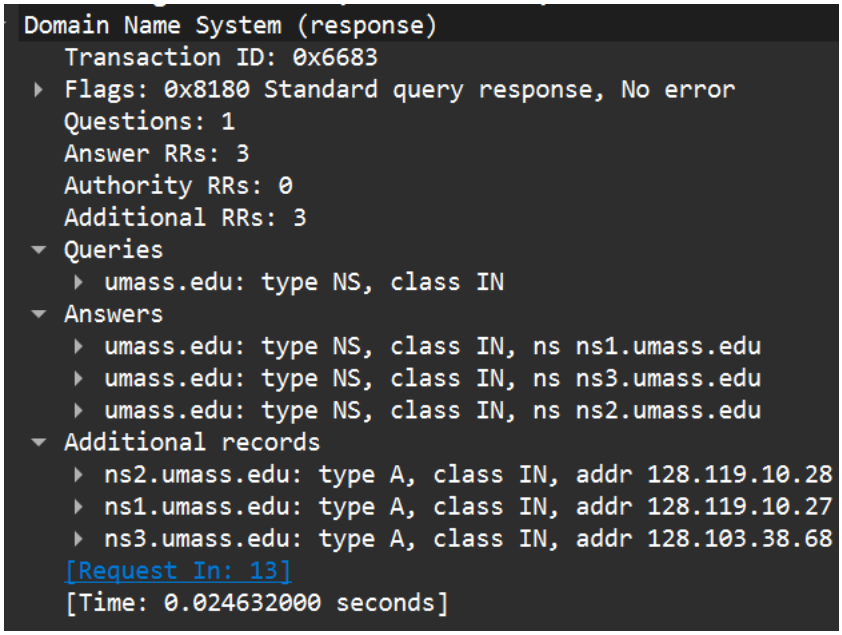
17. 检查 DNS 查询消息。该查询有多少个问题？查询消息中是否包含任何“答案”？



答 ：1 个问题，0 个回答

18. 检查 DNS 响应消息。回应有多少个答案？答案中包含哪些信息？多少额外资源记录被返回？

这些附加资源记录中包含哪些附加信息？



答：回应中有 3 个答案，答案中包含了该域的权威 DNS 服务器的主机名.
3 个额外资源记录被返回，包含这些权威 DNS 服务器的 IP 地址

结论分析：

本次实验我通过执行命令行，WireShark 抓包等操作，观察 DNS 数据包数据，从而了解 DNS 的结构层次，DNS 缓存等，更加深刻地掌握了 DNS 的多方面相关知识，收获良多.

结论：

1. 可以通过命令行进行 nslookup 域名查询操作.
2. 通过分析捕获的数据包，确定 DNS 查询的类型，例如 A 记录, MX 记录、CNAME 记录、NX 记录等.
3. DNS 缓存可以减少对 DNS 服务器的查询次数，提高域名解析的速度.
4. 可以通过分析 DNS 数据包的结构来了解 DNS 协议的工作原理，包括 DNS 报头、问题部分、回答部分、授权部分和附加部分等.