week10: DNS报文分析

一、实验目的

- 了解系统命令`nslookup`的用法
- 学习DNS协议并掌握DNS的工作原理

二、实验任务

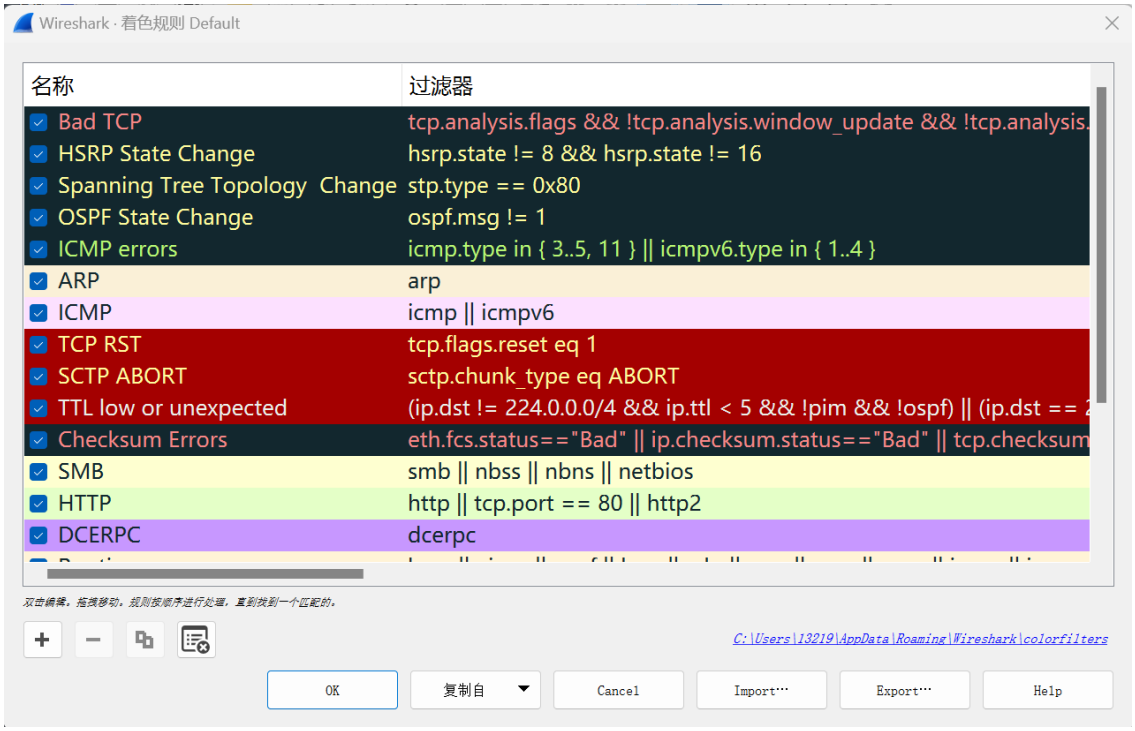
- `nslookup`命令的简单使用
- 使用Wireshark分析DNS协议

三、实验过程

3.1 Wireshark补充

- **着色规则**

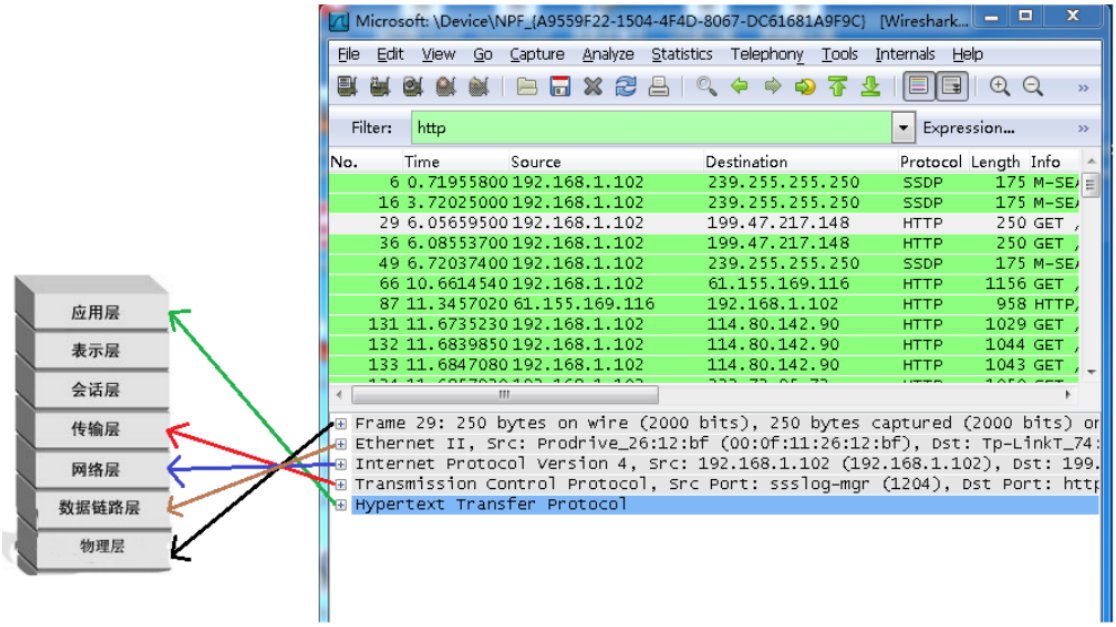
  数据包列表区中不同的协议使用了不同的颜色区分。协议颜色标识定位在菜单栏View --> Coloring Rules。如下所示：



- **Packet Details Pane(数据包详细信息)**

  在数据包列表中选择指定数据包，在数据包详细信息中会显示数据包的所有详细信息内容。数据包详细信息面板是最重要的，用来查看协议中的每一个字段。各行信息分别为：

1）Frame：物理层的数据帧概况
2）Ethernet II：数据链路层以太网帧头部信息
3）Internet Protocol Version 4：互联网层IP包头部信息
4）Transmission Control Protocol：传输层的数据段头部信息，此处是TCP
5）Hypertext Transfer Protocol：应用层的信息，此处是HTTP协议

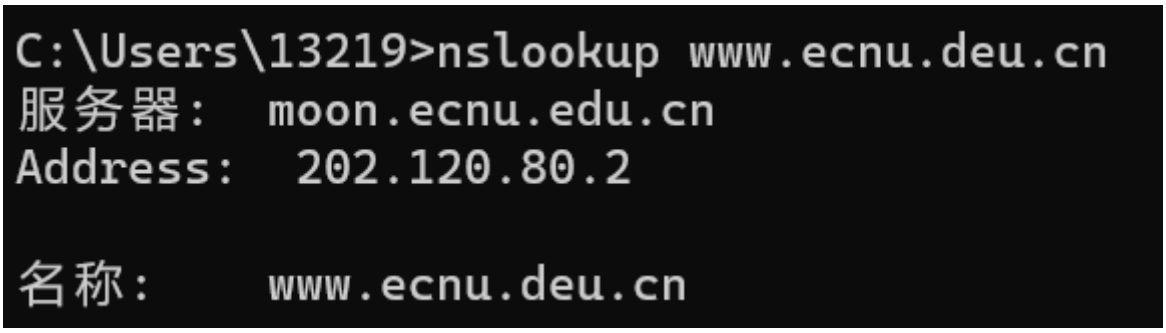


3.2 nslookup

nslookup 工具在现在的大多数 Linux/Unix 和 Microsoft 平台中都有，它允许主机查询任何指定的 DNS 服务器的 DNS 记录。DNS 服务器可以是根 DNS 服务器，顶级域 DNS 服务器，权威 DNS 服务器或中间 DNS 服务器。要完成此任务，nslookup 将 DNS 查询发送到指定的 DNS 服务器，然后接收 DNS 回复，并显示结果。

3.2.1 nslookup基本用法

下面截图显示了三个不同 nslookup 命令的结果（显示在 Mac终端，Win类似）。运行 nslookup 时，如果没有指定 DNS 服务器，则 nslookup 会将查询发送到默认的本地DNS 服务器。



- nslookup www.ecnu.edu.cn

  这个命令是说，请告诉我主机 www.ecnu.edu.cn 的 IP 地址。如上图所示，此命令的响应提供两条信息：（1）提供响应的 DNS 服务器的名称和 IP 地址；（2）响应本身，即 www.ecnu.edu.cn 的主机名和 IP 地址。虽然响应来自ecnu的本地 DNS 服务器，但本地 DNS 服务器很可能会迭代地联系其他几个 DNS 服务器来获得结果。

```
C:\Users\13219>nslookup -type=NS ecnu.edu.cn
服务器:  moon.ecnu.edu.cn
Address:  202.120.80.2

非权威应答:
ecnu.edu.cn     nameserver = xiayu.ecnu.edu.cn
ecnu.edu.cn     nameserver = liwa.ecnu.edu.cn
```

- `nslookup -type=NS ecnu.edu.cn`：查询权威DNS

  在这个例子中，我们添加了选项 `-type=NS` 和一级域名 `ecnu.edu.cn`。这将使得 `nslookup` 将 `NS（域名服务器记录，Name Server）` 记录发送到默认的本地 DNS 服务器。换句话说，“请给我发送 `ecnu.edu.cn` 的权威 DNS 的主机名”（当不使用 `-type` 选项时，`nslookup` 使用默认值，即查询 A 类记录。）上图中，首先显示了提供响应的 DNS 服务器（这是默认本地 DNS 服务器）以及两个 `ecnu` 域名服务器。这些服务器中的每一个确实都是校园主机的权威 DNS 服务器。然而，`nslookup` 也表明该响应是非权威的，这意味着这个响应来自某个服务器的缓存，而不是来自权威 ecnu DNS 服务器。

```
C:\Users\13219>nslookup www.ecnu.edu.cn liwa.ecnu.edu.cn
服务器:  liwa.ecnu.edu.cn
Address:  202.120.80.1

名称:    www.ecnu.edu.cn
Addresses:  2001:da8:8005:a492::60
          202.120.92.60
```

- `nslookup www.ecnu.edu.cn liwa.ecnu.edu.cn`

  在这个例子中，我们希望将查询请求发送到 DNS 服务器 `liwa.ecnu.edu.cn`，而不是默认的本地 DNS 服务器 。因此，查询和响应事务直接发生在我们的主机和 `liwa.ecnu.edu.cn` 之间。在这个例子中，DNS 服务器 `liwa.ecnu.edu.cn` 提供主机 www.ecnu.edu.cn 的 IP 地址信息。

- `nslookup` 语法：`nslookup -option1 -option2 host-to-find dns-server`

  一般来说，`nslookup` 可以不添加选项，或者添加一两个甚至更多选项。正如我们在上面的示例中看 到的，`dns-server` 也是可选的；如果这项没有提供，查询将发送到默认的本地 DNS 服务器。

- **task1: 运行 `nslookup` 来确定一个国外大学 (www.mit.edu) 的IP地址以及其权威 DNS 服务器，请在实验报告中附上操作截图并详细分析返回信息内容。**
- **task2: 运行 `nslookup`，使用task1中一个已获得的 DNS 服务器，来查询google服务器 (www.google.com)的 IP 地址(可直接查询)，请在实验报告中附上操作截图并详细分析返回信息内容。**

3.3 DNS协议

3.3.1 DNS协议简介

- 识别主机有两种方式：主机名、IP地址。前者便于记忆(如www.baidu.com)，但路由器很难处理(主机名长度不定)；后者定长、有层次结构，便于路由器处理，但难以记忆。
- 折中的办法就是建立IP地址与主机名间的映射，这就是域名系统DNS做的工作。
- DNS通常由其他应用层协议使用(如HTTP、SMTP、FTP)，将主机名解析为IP地址。
- 在本实验中，我们将仔细查看 DNS 报文的细节。

3.3.2 DNS报文

- **报文格式**

  DNS只有两种报文：查询报文、响应报文，两者有着相同格式，如下：

注：
查询报文仅仅包含查询部分。响应报文包含查询部分、响应部分，也可能包含其他两部分。

- **捕获的DNS报文**

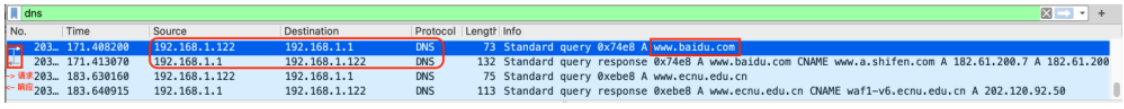
> ==实验开始前请先清空dns缓存==
> ==win: ipconfig/flushdns==
> ==mac: sudo killall -HUP mDNSResponder; sudo dscacheutil -flushcache==

1. 考虑对访问百度页面的一个操作抓包，在浏览器输入http://www.baidu.com/index.html并回车（必要时需清空浏览器缓存），首先需要将URL(**存放对象的服务器主机名和对象的路径名**)解析成IP地址，具体步骤为：

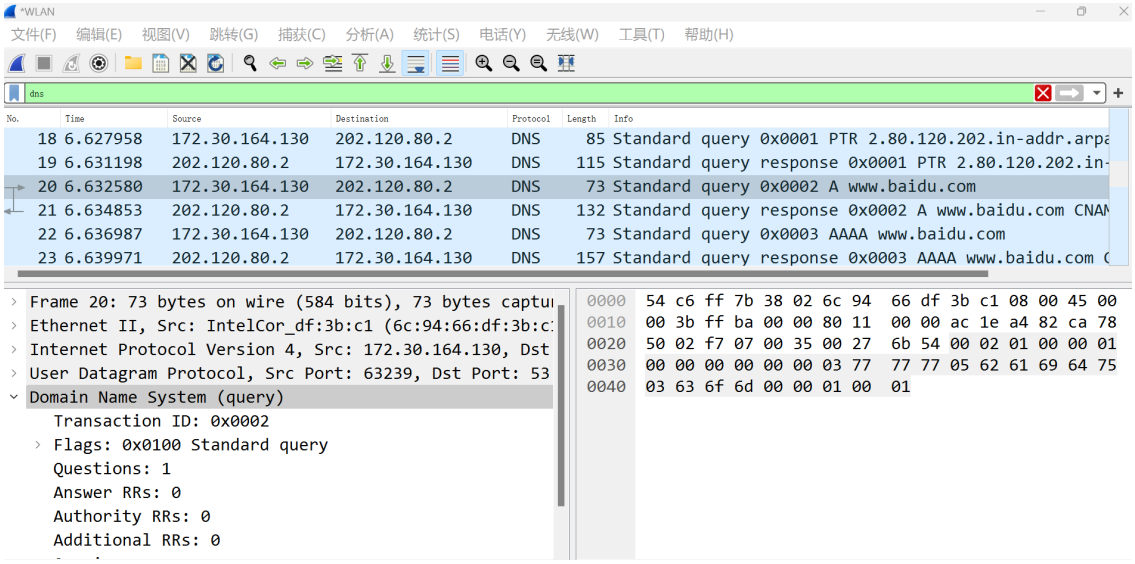
   1）同一台用户主机上运行着DNS应用的客户机端(如浏览器)
   2）从上述URL抽取主机名www.baidu.com，传给DNS应用的客户机端(浏览器)
   3）该DNS客户机向DNS服务器发送一个包含主机名的请求(DNS查询报文)
   4）该DNS客户机收到一份回答报文(DNS响应报文)，该报文包含该主机名对应的IP地址
   182.61.200.7
   5）浏览器由该IP地址定位的HTTP服务器发送一个TCP链接

2. ==或==通过命令 `nslookup www.baidu.com`

用Wireshark捕获的DNS报文如下图，第一行是DNS查询报文，第二行是DNS响应报文。



- **task3: 根据Wireshark抓取的报文信息（例，下图所示示例），分别分析DNS查询报文和响应报文的组成结构，参考上面的报文格式指出报文的每个部分（如，头部区域等），请将实验结果附在实验报告中。**



- **task4: 基于task3中得到的查询和响应报文进行分析，试问这里的查询是什么“Type"的，查询消息是否包含任何“answers"？试问这里的响应消息提供了多少个“answers”，这些“answers”具体包含什么？请将实验结果附在实验报告中。**