**实验二 应用层协议分析实验报告**

序号： 周一78节 姓名： 陈俊宏 学号： 20211060245

成绩：

1．实验目的：

分析HTTP协议报文的首部格式，理解HTTP协议的工作过程；分析DNS的工作过程。

2．实验环境：

（1）连入Internet的主机一台

（2）主机安装Ethereal软件

3．实验步骤：

**a.**下载一个非常简单的HTML文件（该文件不嵌入任何对象），利用Ethereal软件分析HTTP协议。

1. 启动Web browser。**清空浏览器的缓存**。
2. 启动Ethereal，开始Ethereal分组俘获。
3. 在打开的Web browser窗口中可输入下列地址之一
   * <http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html>
   * <http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file2.html>
   * <http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file3.html>
   * <http://www.ietf.org/IETF-Standards-Process.html>
   * <http://www1.cs.columbia.edu/~danr/courses/6761/Fall00/>
   * <http://www.rfc-editor.org/rfc-index.html>
   * <http://www.ietf.org/rfc/rfc959.txt>
   * <http://www.rfc-editor.org/CurrQstats.txt>
   * <http://www.ietf.org/ietf/1bof-procedures.txt>
   * <http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file4.html>

浏览器中将显示一个只有一行或多行文字的非常简单的HTML文件。

1. 停止分组俘获。在显示过滤筛选说明处输入“http”,分组列表子窗口中将只显示所俘获到的HTTP报文。将捕获结果保存为test1。
2. 根据结果回答下列问题回答实验a的问题。

**实验b.** 下载一个含多个嵌入对象的网页，利用Ethereal软件分析HTTP协议。

1. 启动浏览器，将浏览器的缓存清空。
2. 启动Ethereal分组俘获器。开始Ethereal分组俘获。
3. 在浏览器的地址栏中输入某个地址，（需要满足该地址下的网页是包含多个内嵌对象即可)。
4. 停止Ethereal分组俘获，在显示过滤筛选说明处输入“http”,分组列表子窗口中将只显示所俘获到的HTTP报文。将捕获结果保存为test2
5. 重新启动Web browser。启动Ethereal分组俘获器，进行分组捕获。在Web browser当中重新输入相同的URL或单击浏览器中的“刷新”按钮。
6. 步骤同（5）。将捕获结果保存为test3
7. 根据结果回答下列问题回答实验b的问题。

**实验c. DNS 实验**

1. 在ms-dos 下，键入ipconfig/flushdns，清理并重设定DNS客户解析器缓存的内容。
2. 打开浏览器，并清空浏览器的缓存.
3. 打开Ethereal协议分析软件，在filter一栏输入 ip.address==”本机IP地址”，则该协议分析软件仅捕获从本机发送或发送到本机的数据包.
4. 开始捕获数据
5. 在浏览器的地址一栏输入[任意一个Internet网址](http://www.google.com)
6. 停止捕获数据，并显示分析结果。将filter一栏输入DNS,即只查看DNS协议的内容。
7. 根据结果回答下列问题回答实验c的问题。

4．实验分析，回答下列问题。

**实验a**

1. 填写浏览器的输入的URL地址。

URL地址：

 **http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html** 。

1. 打开test1的捕获文件，分析请求报文

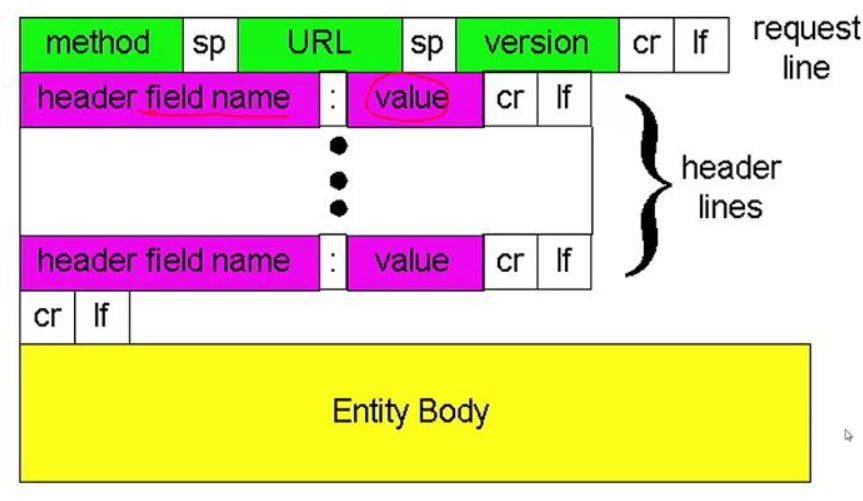
请求行字段：

|  |  |  |
| --- | --- | --- |
| Method | URL | version |
| GET | /ethereal-labs/HTTP-ethereal-file1.html | HTTP/1.1 |

首部字段：

|  |  |
| --- | --- |
| Header line : | Value: |
| Host | gaia.cs.umass.edu |
| Connection | keep-alive |
| User-Agent | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36 Edg/112.0.1722.34 |
| Accept | text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6 |

1. 画出HTTP请求消息的通用格式



（4）打开test1的捕获文件，分析响应报文

状态行字段：

|  |  |  |
| --- | --- | --- |
| Version | Status Code | Phrase |
| HTTP/1.1 | 200 | OK |

首部行字段：

|  |  |
| --- | --- |
| Header line : | Value |
| Server | Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3 |
| Content-Type | text/html; charset=UTF-8 |
| Content-Length | 126 |
| ETag | "7e-5f8f4631e5681" |
| Last-Modified | Mon, 10 Apr 2023 05:10:02 GMT |
| File Data | 126 bytes |

（5）根据捕获的报文，填写相应的内容

|  |  |
| --- | --- |
| 本机的IP地址 | 10.100.208.192 |
| 本机的浏览器运行的HTTP版本类型 | HTTP/1.1 |
| 服务器的IP地址 | 128.119.245.12 |
| 服务器的类型 | Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3 |
| 服务器运行的HTTP版本类型 | HTTP/1.1 |
| 返回到浏览器的字节数 | 126 Bytes |

**实验b.**

根据操作回答下面的问题。

1. 填写浏览器的输入的URL地址。

URL地址： **http://www.ynu.edu.cn/** 。

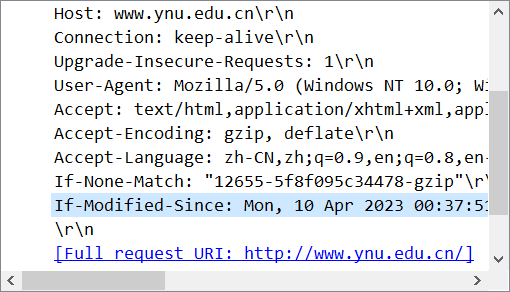
1. 分析test2的捕获文件，你的浏览器一共发出了多少个HTTP GET请求，每个GET 请求的对象是什么？这些请求被发送到的目的地的IP地址是多少？

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | GET 的对象 | 目的地的IP地址 | 与此GET请求相对应的响应报文的状态码 |
| 1 | www.ynu.edu.cn | 2001:250:2800::15:29 | 200 |
| 2 | msedge.b.tlu.dl.delivery.mp.microsoft.com\r\n | 2408:4002:1f10::41 |  |

1. 分析你的浏览器向服务器发出的第一个HTTP GET请求的内容，在该请求报文中，是否有一行是：IF-MODIFIED-SINCE？分析服务器响应报文的内容，服务器是否明确返回了文件的内容？如何获知？

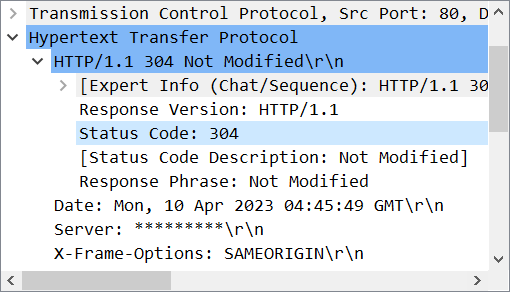
**答：没有IF-MODIFIED-SINCE。服务器明确反应了文件的内容， 因为该响应报文的状态码是200，表示请求成功，信息包含在返回的响应报文中。**

1. 分析捕获文件test3分析你的浏览器向服务器发出的第二个“HTTP GET”请求，在该请求报文中是否有一行是：IF-MODIFIED-SINCE？如果有，在该首部行后面跟着的信息是什么？



**答：有IF-MODIFIED-SINCE，该信息指的是页面的最后修改时间。**

1. 服务器对第二个HTTP GET请求的响应中的HTTP状态代码是多少？服务器是否明确返回了文件的内容？请解释。



**答：状态码：304。 服务器没有明确返回文件内容。因为返回304状态码，意思是不返回文件内容。具体原因：浏览器端缓存页面最后修改时间与服务器端时间一致，返回304状态码，客户端接到之后，就直接把本地缓存文件显示到浏览器中。**

**实验c.**

1. 填写浏览器的输入的URL地址。

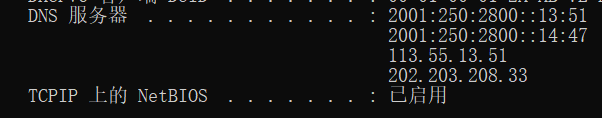
URL地址： **http：//www.ynu.edu.cn** 。

1. 定位到DNS查询报文和查询响应报文，这两种报文的发送是基于UDP还是基于TCP的？DNS查询报文的目的端口号是多少？DNS查询响应报文的源端口号是多少？

**答：这两种报文的发送基于UDP。DNS查询报文的目的端口号是（53）。DNS查询响应报文的源端口号是（53）。**

1. DNS查询报文发送的目的地的IP地址是多少？利用ipconfig命令（ipconfig/all）决定你主机的本地DNS服务器的IP地址。这两个地址相同吗？

**答：DNS查询报文的发送的目的地的IP地址是：2001:250:2800::13:51。由实验可知，这两个地址是相同的。**



1. 填写相应的DNS报文各字段的值（选择两个相对应的DNS查询和响应报文即可，没有的字段可填无）

DNS 查询报文：

|  |  |
| --- | --- |
| **Identification** | **0x226b** |
| **Flags** | **0x0100** |
| **Number of Questions** | **1** |
| **Number of answer RRs** | **0** |
| **Number of authority RRs** | **0** |
| **Number of additional RRs** | **0** |
| **Queries** | **www.ynu.edu.cn: type A, class IN** |
| **Answers** | **无** |
| **Authoritative Servers** | **无** |
| **Additional records** | **无** |

检查DNS查询报文，它是哪一类型的DNS查询？该查询报文中包含“answers”吗？

**答：该DNS查询报文是递归查询。该查询报文中不包含“answers”。**

DNS响应报文

|  |  |
| --- | --- |
| **Identification** | **0x226b** |
| **Flags** | **0x8180** |
| **Number of Questions** | **1** |
| **Number of answer RRs** | **2** |
| **Number of authority RRs** | **2** |
| **Number of additional RRs** | **4** |
| **Queries** | **www.ynu.edu.cn: type A, class IN** |
| **Answers** | **www.ynu.edu.cn: type CNAME, class IN, cname site-group.ynu.edu.cn**  **site-group.ynu.edu.cn: type A, class IN, addr 202.203.208.4** |
| **Authoritative Servers** | **ynu.edu.cn: type NS, class IN, ns secdns.ynu.edu.cn**  **ynu.edu.cn: type NS, class IN, ns pridns.ynu.edu.cn** |
| **Additional records** | **pridns.ynu.edu.cn: type AAAA, class IN, addr 2001:250:2800:2::33**  **secdns.ynu.edu.cn: type AAAA, class IN, addr 2001:250:2800:2::34**  **pridns.ynu.edu.cn: type A, class IN, addr 202.203.208.33**  **secdns.ynu.edu.cn: type A, class IN, addr 202.203.208.34** |

检查DNS查询响应报文，其中提供了多少个“answers”？每个answers包含哪些内容？

**答：由实验可得：DNS查询响应报文中提供了2个“answers”。**

**包含的内容分别是：**

**www.ynu.edu.cn: type CNAME, class IN, cname site-group.ynu.edu.cn**

**Name: www.ynu.edu.cn**

**Type: CNAME (Canonical NAME for an alias) (5)**

**Class: IN (0x0001)**

**Time to live: 120 (2 minutes)**

**Data length: 13**

**CNAME: site-group.ynu.edu.cn**

**和**

**site-group.ynu.edu.cn: type A, class IN, addr 202.203.208.4**

**Name: site-group.ynu.edu.cn**

**Type: A (Host Address) (1)**

**Class: IN (0x0001)**

**Time to live: 9722 (2 hours, 42 minutes, 2 seconds)**

**Data length: 4**

**Address: 202.203.208.4**