



警示

1. 实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2. 在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
3. 实验报告文件以 PDF 格式提交。

|    |          |     |       |    |  |
|----|----------|-----|-------|----|--|
| 系  | 计算机学院    | 班 级 | 保密管理班 | 组长 |  |
| 学号 | 22336090 |     |       |    |  |
| 学生 | 黄集瑞      |     |       |    |  |

## DNS 协议分析实验

### 一、第一部分：nslookup 命令

|    |  |
|----|--|
| 题号 |  |
| 1  | 请运行 nslookup 命令来获取上海交通大学网站 www.sjtu.edu.cn 的服务器 IP 地址。www.sjtu.edu.cn 的 IP 地址是什么？    |
| 答案 | IPv4 地址：202.120.2.119<br>IPv6 地址：2001:da8:8000:6fc0:102:1200:2:48                    |
| 截图 |  |
| 分析 | 具体结果如图所示   |
| 2  | 在问题 1 中，提供 nslookup 命令结果的 DNS 服务器的 IP 地址是什么？   |
| 答案 | IP 地址为 10.8.8.8  |
| 截图 |   |
| 分析 | 由于使用 nslookup 后会尝试对 dns 服务器做反向解析，如果 dns 服务器 IP 没有做 PTR 就会显示 UnKnown.                 |
| 3  | 问题 1 中 nslookup 命令的结果是来自权威服务器还是非权威服务器？   |
| 答案 | 是来自非权威服务器  |
| 截图 |  |



|    |   |
|----|---|
| 分析 | 具体结果如图所示，说明该回复是取自缓存中，而不是从权威服务器查询得到的。  |
| 4  | 请使用 nslookup 命令确定 sjtu.edu.cn 域名的权威名称服务器的名称。这个名称是什么？（如果有多个权威服务器，请提供 nslookup 返回的第一个权威服务器的名称）。如果你需要找到该权威服务器的 IP 地址，你会怎么做？  |
| 答案 | 名称： dns.sjtu.edu.cn<br>如果要找到该权威服务器的 IP 地址，我会采用 nslookup dns.sjtu.edu.cn 再去查找 IP 地址  |
| 截图 | <pre>primary name server = dns.sjtu.edu.cn responsible mail addr = hostmaster.sjtu.edu.cn  C:\Users\鸭瑞315&gt;nslookup 202.120.2.90 服务器:  UnKnown Address:  10.8.8.8  名称:     dns.sjtu.edu.cn Address:  202.120.2.90</pre> |
| 分析 | 由图片可得因为要选择返回的第一个权威服务器所以就是首要域名服务器的名称，然后因为要查找权威服务器的 IP 地址，所以再次使用 nslookup 去查找。  |

## 二、打开“dns-wireshark-trace1-1”文件，进行观察分析，回答以下问题

|    |  |
|----|--|
| 题号 |  |
| 1  | 找到解析域名 gaia.cs.umass.edu 的第一个 DNS 查询消息。该 DNS 查询消息在抓包文件中的包编号是多少？这个查询消息是通过 UDP 还是 TCP 发送的？ |
| 答案 | 编号为 15，这个查询信息是通过 UDP 发送的   |
| 截图 |  |
| 分析 | 答案如截图所示即可  |
| 2  | 现在找到与初始 DNS 查询对应的 DNS 响应。该 DNS 响应消息在抓包文件中的包编号是多少？这个响应消息是通过 UDP 还是 TCP 接收的？               |
| 答案 | 编号为 17，响应信息是通过 UDP 接收的。  |
| 截图 |  |
| 分析 | 答案如截图所示即可  |

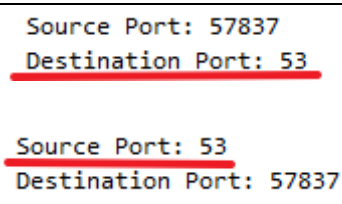


|    |  |
|----|--|
| 3  | DNS 查询消息的目标端口是什么？DNS 响应消息的源端口是什么？  |
| 答案 | 查询消息的目标端口为 53<br>响应消息的源端口也为 53   |
| 截图 |    |
| 分析 | 答案如图所示   |
| 4  | DNS 查询消息是发送到哪个 IP 地址的？   |
| 答案 | 查询地址发送到 75.75.75.75  |
| 截图 |   |
| 分析 | 答案如图所示   |
| 5  | 检查 DNS 查询消息。该 DNS 消息中包含多少个 "问题"？包含多少个 "答案"？  |
| 答案 | 包含 1 个 "问题"<br>包含 0 个 "答案"   |
| 截图 |   |
| 分析 | 由于该信息为查询信息，故自然本身不带有 "答案"   |
| 6  | 检查对初始查询消息的 DNS 响应消息。该 DNS 消息中包含多少个 "问题"？包含多少个 "答案"？  |
| 答案 | 包含 1 个 "问题"<br>包含 1 个 "答案"   |
| 截图 |   |
| 分析 | 这个是对上面查询信息的响应，由于消息类型为 A 所以便返回对应的 IPv4 地址，所以答案一般仅有一个。   |
| 7  | <p><a href="http://gaia.cs.umass.edu/kurose_ross/">http://gaia.cs.umass.edu/kurose_ross/</a> 的基础文件网页引用了位于同一服务器上的图像对象 <a href="http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg">http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg</a>。</p> <p>1) 抓包文件中首次 HTTP GET 请求基础文件 <a href="http://gaia.cs.umass.edu/kurose_ross/">http://gaia.cs.umass.edu/kurose_ross/</a> 的包编号是多少？</p> <p>2) 抓包文件中为解析 <a href="http://gaia.cs.umass.edu">gaia.cs.umass.edu</a> 以便发送此初始 HTTP 请求的 DNS 查询的包编号</p> |



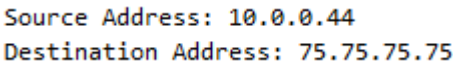
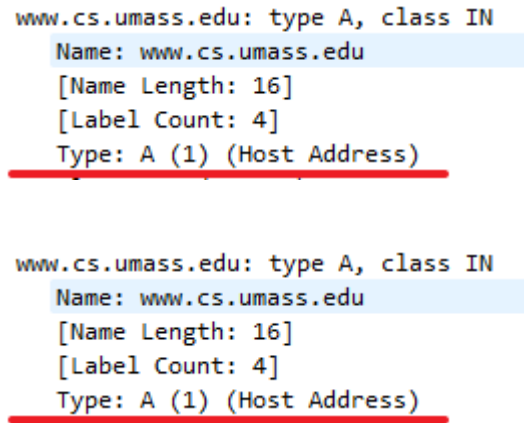
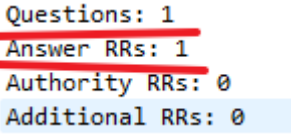
|    |  |
|----|--|
|    | <p>是多少？</p> <p>3) 抓包文件中收到的 DNS 响应的包编号是多少？</p> <p>4) 抓包文件中对图像对象 <code>http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg</code> 的 HTTP GET 请求的包编号是多少？</p> <p>5) 抓包文件中为解析 <code>gaia.cs.umass.edu</code> 以便发送第二个 HTTP 请求的 DNS 查询的包编号是多少？</p> <p>6) 讨论 DNS 缓存如何影响上一个问题的答案。</p>   |
| 答案 | <p>1. 编号为 22</p> <p>2. 编号为 15</p> <p>3. 编号为 17</p> <p>4. 编号为 205</p> <p>5. 编号仍然为 15</p> <p>6. 由于题目提到存储该图片的服务器地址与该网站的服务器地址相同，所以在一开始进行访问该网站时就先获得了该服务器地址的缓存，所以在进行第二次响应时直接从缓存中得到答案便不再进行对服务器的访问。</p>  |
| 截图 |  <p>The screenshot shows a Wireshark packet capture with four packets. Packet 22 is an HTTP GET request to 128.119.245.12. Packet 15 is a DNS query from 10.0.0.44 to 75.75.75.75. Packet 17 is a DNS response from 75.75.75.75 to 10.0.0.44. Packet 205 is an HTTP GET request from 10.0.0.44 to 128.119.245.12.</p> |
| 分析 | 答案如图所示   |

### 三、打开“dns-wireshark-trace2-1”文件，进行观察分析，回答以下问题

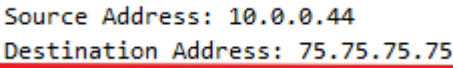
|    |  |
|----|--|
| 题号 |  |
| 1  | DNS 查询消息的目标端口是什么？DNS 响应消息的源端口是什么？  |
| 答案 | 查询消息的目标端口为 53<br>响应消息的源端口为 53  |
| 截图 |  <p>The screenshot shows the details of two DNS packets. The first packet (query) has a Destination Port of 53. The second packet (response) has a Source Port of 53.</p> |
| 分析 | 答案如图所示   |



# 计算机网络实验报告

|    |   |
|----|---|
| 2  | DNS 查询消息是发送到哪个 IP 地址的？这是你本地默认 DNS 服务器的 IP 地址吗？                                      |
| 答案 | 查询消息发送到 75.75.75.75，无法确定  |
| 截图 |    |
| 分析 | IP 地址如图所示，但是由于该抓包不是发生在本电脑上所以无法确定本地默认 DNS 服务器。                                       |
| 3  | 检查 DNS 查询消息。该 DNS 查询是哪种“类型”？查询消息中是否包含任何“答案”？  |
| 答案 | DNS 查询属于“A”类型也就是进行 IPv4 的地址查询，不包括任何“答案”   |
| 截图 |   |
| 分析 | 由于该指令类型为查询指令，自然是不会包括“答案”的；需要是 response 应答才会包含“答案”                                   |
| 4  | 检查查询消息的 DNS 响应消息。该 DNS 响应消息中包含多少个“问题”？包含多少个“答案”？                                    |
| 答案 | 该响应消息中包含 1 个“问题”，包含 1 个“答案”   |
| 截图 |  |
| 分析 | 因为该响应消息是对刚才的查询的回应，所以就是包含一个“问题”并且带有对应的一个“答案”   |

## 四、打开“dns-wireshark-trace3-1”文件，进行观察分析，回答以下问题

|    |   |
|----|---|
| 题号 |   |
| 1  | DNS 查询消息是发送到哪个 IP 地址的？这是你本地默认 DNS 服务器的 IP 地址吗？                                      |
| 答案 | 发送到 75.75.75.75 这个 IP 地址的，无法确定。   |
| 截图 |  |
| 分析 | Ip 地址如图所示，但是由于该抓包不是发生在本电脑上所以无法确定本地默认 DNS 服务器。                                       |
| 2  | 检查 DNS 查询消息。该查询包含多少问题？查询消息中是否包含任何“答案”？  |
| 答案 | 该查询包含 1 个问题，查询消息中不包含任何“答案”  |



|    |   |
|----|---|
| 截图 | <p>Questions: 1<br/>Answer RRs: 0<br/>Authority RRs: 0<br/>Additional RRs: 0</p>  |
| 分析 | <p>与上题类似，由于该指令类型为查询指令，自然是不会包括“答案”的；需要是 response 应答才会包含“答案”</p>  |
| 3  | <p>检查 DNS 响应消息（特别是类型为“NS”的 DNS 响应消息）。该响应中有多少个答案？答案中包含了什么信息？返回了多少个附加资源记录？这些附加资源记录中包含了什么额外信息（如果有返回附加信息的话）？</p>  |
| 答案 | <p>该响应中有 3 个答案<br/>答案中包含了许多信息：有消息响应的类型（NS），查询使用的类别（IN），TTL（1hour），返回的 DNS 记录数据的长度（data length）以及最重要的一查询到的权威服务器的名称（下图展示的名称为 ns1.umass.edu）<br/>返回了 3 个附加资源记录<br/>该附加信息包含了权威域名服务器的 ip 地址（IPv4 格式下的），也就是 Type= ‘A’ 的搜索结果。</p>  |
| 截图 | <p>Questions: 1<br/>Answer RRs: 3<br/>Authority RRs: 0<br/>Additional RRs: 3</p> <p>-----<br/>v umass.edu: type NS, class IN, ns ns1.umass.edu<br/>Name: umass.edu<br/>Type: NS (2) (authoritative Name Server)<br/>Class: IN (0x0001)<br/>Time to live: 3600 (1 hour)<br/>Data length: 6<br/>Name Server: ns1.umass.edu</p> <p>Additional records<br/>&gt; ns2.umass.edu: type A, class IN, addr 128.119.10.28<br/>&gt; ns1.umass.edu: type A, class IN, addr 128.119.10.27<br/>&gt; ns3.umass.edu: type A, class IN, addr 128.103.38.68</p> |
| 分析 | <p>通过 response 响应信息，我们可以得出该 DNS 响应不仅给出了 umass.edu 的权威名称服务器，还提供了这些服务器的 IP 地址信息，确保客户端能够通过网络访问这些服务器并进行域名解析。</p>  |