



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。

院系		班 级		组长	
学号					
学生					

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	202.120.2.119; 2001:da8:8000:6fc0:102:1200:2:48
截图	
分析	应答给出了 www.sjtu.edu.cn 的 IPv4 和 IPv6 地址
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	10.8.8.8
截图	同上
分析	
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	非权威服务器
截图	同上
分析	
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	dns.sjtu.edu.cn; 输入 nslookup dns.sjtu.edu.cn



截图	<pre>C:\Users\黄倩怡>nslookup -type=NS www.sjtu.edu.cn 服务器: UnKnown Address: 10.8.8.8 sjtu.edu.cn primary name server = dns.sjtu.edu.cn responsible mail addr = hostmaster.sjtu.edu.cn serial = 2410052204 refresh = 10800 (3 hours) retry = 3600 (1 hour) expire = 604800 (7 days) default TTL = 3600 (1 hour)</pre>
分析	

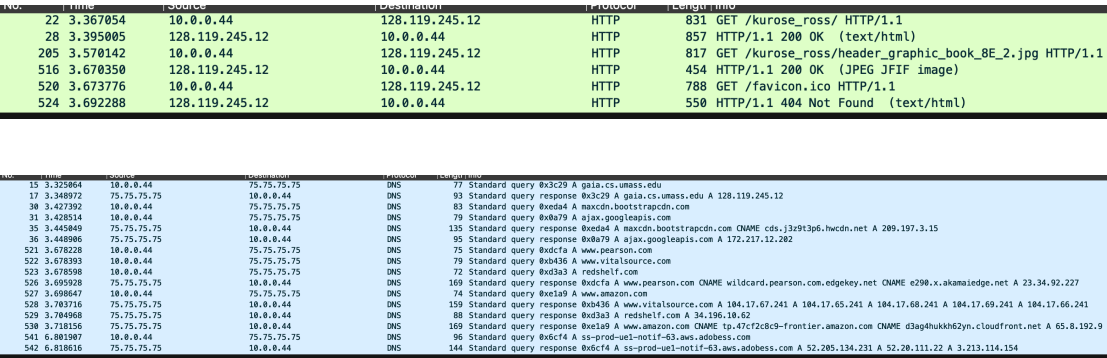
二、打开“dns-wireshark-trace1-1”文件，进行观察分析，回答以下问题

题号	
1	找到解析域名 <code>gaia.cs.umass.edu</code> 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	15; UDP
截图	<pre>> Frame 15: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface en0, id 0 > Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinear_80:00:00 (00:50:f1:80:00:00) > Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75 > User Datagram Protocol, Src Port: 58350, Dst Port: 53 > Domain Name System (query)</pre>
分析	查看使用的传输层协议
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	17; UDP
截图	<pre>> Frame 17: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface en0, id 0 > Ethernet II, Src: Maxlinear_80:00:00 (00:50:f1:80:00:00), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27) > Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.44 > User Datagram Protocol, Src Port: 53, Dst Port: 58350 > Domain Name System (response)</pre>
分析	查看使用的传输层协议
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	53; 53
截图	同上两图
分析	UDP 数据段头部包含源端口号和目的端口号
4	DNS 查询消息是发送到哪个 IP 地址的？
答案	75.75.75.75



截图	<pre>> Frame 15: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface en0, id 0 > Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinear_80:00:00 (00:50:f1:80:00:00) > Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75 > User Datagram Protocol, Src Port: 58350, Dst Port: 53 > Domain Name System (query)</pre>
分析	IP 数据包头部含有目的 IP 地址
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	1; 0
截图	<pre>> Frame 15: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface en0, id 0 > Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinear_80:00:00 (00:50:f1:80:00:00) > Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75 > User Datagram Protocol, Src Port: 58350, Dst Port: 53 v Domain Name System (query) Transaction ID: 0x3c29 > Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 > Queries [Response In: 17]</pre>
分析	根据应用层数据中的 "Questions" 和 "Answer RRs" 得到
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	1; 1
截图	<pre>> Frame 17: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface en0, id 0 > Ethernet II, Src: Maxlinear_80:00:00 (00:50:f1:80:00:00), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27) > Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.44 > User Datagram Protocol, Src Port: 53, Dst Port: 58350 v Domain Name System (response) Transaction ID: 0x3c29 > Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0 > Queries > Answers [Request In: 15] [Time: 0.023908000 seconds]</pre>
分析	同上
7	<p>http://gaia.cs.umass.edu/kurose_ross/ 的基础文件网页引用了位于同一服务器上的图像对象 http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg。</p> <ol style="list-style-type: none">1) 抓包文件中首次 HTTP GET 请求基础文件 http://gaia.cs.umass.edu/kurose_ross/ 的包编号是多少?2) 抓包文件中为解析 gaia.cs.umass.edu 以便发送此初始 HTTP 请求的 DNS 查询的包编号是多少?3) 抓包文件中收到的 DNS 响应的包编号是多少?4) 抓包文件中对图像对象 http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg 的 HTTP GET 请求的包编号是多少?



	5) 抓包文件中为解析 gaia.cs.umass.edu 以便发送第二个 HTTP 请求的 DNS 查询的包编号是多少? 6) 讨论 DNS 缓存如何影响上一个问题的答案。
答案	22; 15; 17; 205; 没有发送查询包; 由于 DNS 缓存中记录了 http://gaia.cs.umass.edu 的 IP 地址, 第二次 HTTP 请求时直接从 DNS 缓存中查询, 无需发送 DNS 查询包。
截图	
分析	(1)(4)见图 1, (2)(3)(5)见图 2

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	53;53
截图	
分析	
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	75.75.75.75;不是
截图	



分析	
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	type A; 不包含答案
截图	<div><div><div>Domain Name System (query)</div><div>Transaction ID: 0x609b</div><div>> Flags: 0x0100 Standard query</div><div>Questions: 1</div><div>Answer RRs: 0</div><div>Authority RRs: 0</div><div>Additional RRs: 0</div><div>Queries</div><div>> www.cs.umass.edu: type A, class IN</div><div>[Response In: 20]</div></div></div> <div><div>Domain Name System (query)</div><div>Transaction ID: 0x1462</div><div>> Flags: 0x0100 Standard query</div><div>Questions: 1</div><div>Answer RRs: 0</div><div>Authority RRs: 0</div><div>Additional RRs: 0</div><div>Queries</div><div>> cc-api-data.adobe.io: type A, class IN</div><div>[Response In: 32]</div></div>
分析	
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	第一个响应消息包含 1 个问题; 1 个答案 第二个响应消息包含 1 个问题; 8 个答案



截图	<pre>✓ Domain Name System (response) Transaction ID: 0x609b > Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0 ✓ Queries > www.cs.umass.edu: type A, class IN > Answers [Request In: 19] [Time: 0.034183000 seconds]</pre>
	<pre>✓ Domain Name System (response) Transaction ID: 0x1462 > Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 8 Authority RRs: 0 Additional RRs: 0 > Queries > Answers [Request In: 31] [Time: 0.017970000 seconds]</pre>
分析	

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	75.75.75.75；不是
截图	<pre>> Frame 13: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface en0, id 0 > Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinear_80:00:00 (00:50:f1:80:00:00) > Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75 > User Datagram Protocol, Src Port: 59963, Dst Port: 53 > Domain Name System (query)</pre>
分析	从网络层信息可得
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	1 个问题；不包含答案
截图	<pre>✓ Domain Name System (query) Transaction ID: 0x6683 > Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 > Queries [Response In: 14]</pre>
分析	
3	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）？
答案	3 个答案；答案包含查询的域名、DNS，权威服务器的域名等；附加资源记录包含权威服务器的 IP 地址等。
截图	<pre>✓ Domain Name System (response) Transaction ID: 0x6683 > Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 3 Authority RRs: 0 Additional RRs: 3 > Queries ✓ Answers > umass.edu: type NS, class IN, ns ns1.umass.edu > umass.edu: type NS, class IN, ns ns3.umass.edu > umass.edu: type NS, class IN, ns ns2.umass.edu ✓ Additional records > ns2.umass.edu: type A, class IN, addr 128.119.10.28 > ns1.umass.edu: type A, class IN, addr 128.119.10.27 > ns3.umass.edu: type A, class IN, addr 128.103.38.68 [Request In: 13] [Time: 0.024632000 seconds]</pre>
分析	