LAB 2\_Jinbo Li

Statement: I (We) have read and understood the course academic integrity policy.

Q1: Run nslookup to obtain the IP address of the web server for the Indian Institute of Technology in Bombay, India: www.iitb.ac.in. What is the IP address of [www.iitb.ac.in](http://www.iitb.ac.in)?

A: The IP address of the web server for the IIT is 103.21.124.10

文本

描述已自动生成

Q2: What is the IP address of the DNS server that provided the answer to your nslookup command in question 1 above?

A: The IP address of the DNS server is 75.75.75.75 provided by Comcast.

文本

描述已自动生成

Q3: Did the answer to your nslookup command in question 1 above come from an authoritative or non-authoritative server?

A: It is from an non-anthoritative server.

文本

描述已自动生成

Q4: Use the nslookup command to determine the name of the authoritative name server for the iitb.ac.in domain. What is that name? (If there are more than one authoritative servers, what is the name of the first authoritative server returned by nslookup)? If you had to find the IP address of that authoritative name server, how would you do so?

A: The name is “dns3.iitb.ac.in”. I can use command “nslookup dns3.iitb.ac.in” to find the IP address of the authoritative name server.

文本

描述已自动生成

文本

描述已自动生成

Q5: Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number in the trace for the DNS query message? Is this query message sent over UDP or TCP?

A: The package number is 70. This query message sent over UDP.

图形用户界面, 应用程序

描述已自动生成

图形用户界面, 应用程序, Word

描述已自动生成

Q6: Now locate the corresponding DNS response to the initial DNS query. What is the packet number in the trace for the DNS response message? Is this response message received via UDP or TCP?

A: The package number in the trace for the DNS response message is 89. This response message received via UDP.

图形用户界面, 应用程序, Word

描述已自动生成

文本

描述已自动生成

Q7: What is the destination port for the DNS query message? What is the source port of the DNS response message?

A: The destination port for the DNS query message is 53. The source port of the DNS response message is 53.

图形用户界面, 应用程序, Word

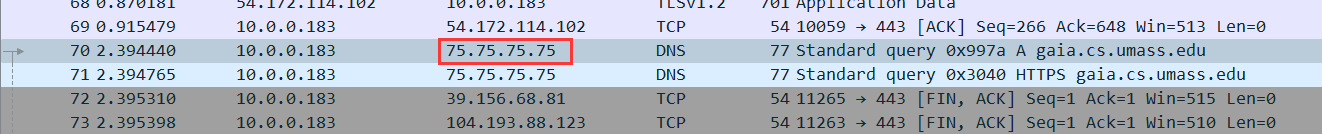
描述已自动生成

图形用户界面, 应用程序, 表格

描述已自动生成

Q8: To what IP address is the DNS query message sent?

A: 75.75.75.75



Q9: Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

A: This DNS message contains 1 question and it contains 0 answer.

图形用户界面, 文本, 应用程序

描述已自动生成

Q10: Examine the DNS response message to the initial query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

A: This DNS message contains 1 question and contains 1 answer.

图形用户界面, 应用程序, Word

描述已自动生成

Q11: This web page contains images. Before retrieving each image, does your host issue new DNS queries?

A: No, my host did not issue new DNS queries according to WireShark (ignore HTTPS DNS query). When the web page was loaded at the first time, all the DNS records of images were cached in local. Thus, my host used cached DNS before retrieving each images.

图片包含 日历

描述已自动生成

Q12: What is the destination port for the DNS query message? What is the source port of the DNS response message?

A: The destination port for the DNS query message is 53. The source port of the DNS response message is 53.

图形用户界面, 应用程序, 表格

描述已自动生成

图形用户界面, 应用程序

描述已自动生成

Q13: To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

A: The DNS query message sent to 75.75.75.75. This IP address is my default local DNS server.

表格

中度可信度描述已自动生成

Q14: Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers” ?

A: The type is A. No, it does not contain any answer.

图形用户界面, 应用程序

描述已自动生成

Q15: Examine the DNS response message to the query message. How many “questions” does this DNS response message contain? How many “answers”?

A: This DNS response message contains 1 question. It contains 1 answer.

图形用户界面, 应用程序, Word

描述已自动生成

Q16: To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

A: The IP address is 75.75.75.75. It is the IP address of my default local DNS server.

图片包含 图形用户界面

描述已自动生成

Q17: Examine the DNS query message. How many questions does the query have? Does the query message contain any “answers”?

A: The query has 1 question. The query message does not contain any answer.

图形用户界面, 应用程序, Word

描述已自动生成

Q18: Examine the DNS response message. How many answers does the response have? What information is contained in the answers? How many additional resource records are returned? What additional information is included in these additional resource records?

A: The response has 3 answers. The answers contain “umass.edu: type NS, class IN, ns ns3.umass.edu”, “umass.edu: type NS, class IN, ns ns1.umass.edu” and “umass.edu: type NS, class IN, ns ns2.umass.edu”.

3 additional resource records are returned. The additional information is “ns1.umass.edu: type A, class IN, addr 128.119.10.27”,” ns2.umass.edu: type A, class IN, addr 128.119.10.28” and “ns3.umass.edu: type A, class IN, addr 69.16.40.18”.

图形用户界面, 应用程序

描述已自动生成

文本

描述已自动生成

图形用户界面, 文本, 应用程序

描述已自动生成

文本

描述已自动生成

Q19: What are the IP addresses returned by DNS when the host requests a DNS lookup for www.youtube.com? If there is more than one DNS query, list all the unique IPs in the DNS responses.

A: The IP addresses returned by DNS are 74.125.226.224-74.125.226.233 and 74.125.226.238.

图形用户界面, 应用程序, 表格

描述已自动生成

Q20: What are the IP addresses returned by DNS when the host requests a DNS lookup for any hostname containing googlevideo.com? If there is more than 1 DNS query, list all the unique IPs in the DNS responses.

A: The IP address returned by DNS is 128.205.159.13.

图形用户界面, 应用程序

描述已自动生成

Q21: What are the IP addresses returned by DNS when the source requests a DNS lookup for s.youtube.com? If there is more than 1 DNS query, list all the unique IPs in the DNS responses.

A: The IP addresses returned by DNS are 74.125.226.224-74.125.226.233 and 74.125.226.238.

图形用户界面, 应用程序, 日历

描述已自动生成

Q22: Are the IPs in questions (19), (20), and (21) the same or different? How do you explain this?

A: The DNS responses of [www.youtube.com](http://www.youtube.com) and s.youtube.com are the same. But the DNS response of IP addresses returned by DNS when the host requests a DNS lookup for any hostname containing googlevideo.com are different from them.

Q23: Identify the GET request containing “videoplayback”. To which IP is this request sent to?

A: This request sent to 128.205.159.13.

表格

描述已自动生成

Q24: Check the authoritative nameservers in all the DNS response packets corresponding to DNS queries for any hostname containing youtube.com or googlevideo.com. What do you observe about the order of the nameservers listed in each response? Is it the same or different? Justify your answer.

A: The authoritative nameservers are the same (ns1.google.com to ns4.google.com). But the order of those nameservers listed in each response is different. To explain the order of those nameservers, it is because different websites need to use different servers, so load balancing can be achieved.

图形用户界面, 应用程序, 表格, Excel

描述已自动生成

[www.youtube.com](http://www.youtube.com)

图形用户界面, 应用程序, Word

描述已自动生成

s.youtube.com

图形用户界面, 应用程序

描述已自动生成

.googlevideo.com