DNS Wireshark Lab

nslookup

1. 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

- The IP address of www.iitb.ac.in is `103.21.124.133`.

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

- IP address of the DNS server is `10.0.2.1`

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

- The answer came from a `non-authoritative server`

4. Use the nslookup command to determine the name of the authoritative name server for the iit.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?

- Name of authoritative ser is `dns1.iitb.ac.in`
- To fine the IP address `dns1.iitb.ac.in`, the following command can be used.
- ```
  nslookup dns1.iitb.ac.in
  ```
- The IP address is `103.21.125.129`

Tracing DNS with Wireshark

> Reference files for this part
>
> - DNS_Wireshark_Lab/wireshark_files/Tracing_DNS_with_wireshark.pcapng
> - DNS_Wireshark_Lab/wireshark_files/DNS_nslookup_2.pcapng
> - DNS_Wireshark_Lab/wireshark_pdfs/DNS_nslookup-query.pdf
> - DNS_Wireshark_Lab/wireshark_pdfs/DNS_nslookup-response.pdf
> - DNS_Wireshark_Lab/wireshark_pdfs/DNS_nslookup-query_2.pdf
> - DNS_Wireshark_Lab/wireshark_pdfs/DNS_nslookup-response_2.pdf

5. Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number1 in the trace for the DNS query message? Is this query message sent over UDP or TCP?

- The packet number is `1`
- The query message is sent over `UDP`
  ```

6. 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?

- The packet number is `3`
- The query message is sent over `UDP`

7. What is the destination port for the DNS query message? What is the source port of the DNS response message?

- The destination port for the DNS query message is `53`
- The source port of the the DNS response message is `53`.

8. To what IP address is the DNS query message sent?

- The DNS query message is sent to the IP 12.0.2.1

9. Examine the DNS query message. How many "questions" does this DNS message contain? How many "answers" answers does it contain?

- Number of questions is `1`
- Number of answers is `0`

10. 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?

- Number of questions is `1`
- Number of answers is `1`

> Reference files for question 11
>
> - DNS_Wireshark_Lab/wireshark_files/Tracing_DNS_with_wireshark.pcapng
> - DNS_Wireshark_Lab/wireshark_pdfs/DNS_nslookup-get_8.pdf
> - DNS_Wireshark_Lab/wireshark_pdfs/DNS_nslookup-get_93.pdf

11. The web page for the base file http://gaia.cs.umass.edu/kurose_ross/ references the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg , which, like the base webpage, is on gaia.cs.umass.edu. What is the packet number in the trace for the initial HTTP GET request for the base file http://gaia.cs.umass.edu/kurose_ross/? What is the packet number in the trace of the DNS query made to resolve gaia.cs.umass.edu so that this initial HTTP request can be sent to the gaia.cs.umass.edu IP address? What is the packet number in the trace of the received DNS response? What is the packet number in the trace for the HTTP GET request for the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg? What is the packet number in the DNS query made to resolve gaia.cs.umass.edu so that this second HTTP request can be sent to the gaia.cs.umass.edu IP address? Discuss how DNS caching affects the answer to this last question.

- The packet number in the trace for the initial HTTP GET request for the base file http://gaia.cs.umass.edu/kurose_ross/ is `8`
- The packet number in the trace of the DNS query made to resolve gaia.cs.umass.edu so that this initial HTTP request can be sent to the gaia.cs.umass.edu IP address is `1`

- the packet number in the trace of the received DNS response is `3`
- The packet number in the trace for the HTTP GET request for the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg is `93`
- `There is no` packet number in the DNS query made to resolve gaia.cs.umass.edu so that this second HTTP request can be sent to the gaia.cs.umass.edu IP address.
- `DNS cache` saves the initial resolution of gaia.cs.umass.edu in the client. As a result, the client will not bother sending a DNS request, since it already has the IP address in its DNS cache. It will make an HTTP GET request directly to http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg

> Reference file for the questions below
>
> - DNS_Wireshark_Lab/wireshark_files/DNS_nslookup_2.pcapng

12. What is the destination port for the DNS query message? What is the source port of the DNS response message?

- The destination port for the DNS query message is `53`
- The source port of the DNS response message `53`

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

- The DNS query message is sent to `10.0.2.1`
- Yes

14. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

- It is a `type A`
- Yes, one question.

15. Examine the DNS response message to the query message. How many "questions" does this DNS response message contain? How many "answers"?

- There is one question
- There is one answer

> Reference files for questions below
>
> - DNS_Wireshark_Lab/wireshark_files/Tracing_DNS_type-NS.pcapng
> - DNS_Wireshark_Lab/wireshark_pdfs/nslookup_NS.pdf
> - DNS_Wireshark_Lab/wireshark_pdfs/nslookup_NS-query.pdf
> - DNS_Wireshark_Lab/wireshark_pdfs/nslookup_NS-reponse.pdf

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

- The IP address is `10.0.2.1`

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

- There is one question
- There are no answers

18. Examine the DNS response message (in particular the DNS response message that has type “NS”). 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 (if additional information is returned)?

- There are three answers
- There information contained in the answers are
    - umass.edu: type NS, class IN, ns ns1.umass.edu
    - umass.edu: type NS, class IN, ns ns2.umass.edu
    - umass.edu: type NS, class IN, ns ns3.umass.edu
- Each answer has `Namse: umass`, `Type: NS(2) (Authoritative Name Server)`, `Class: IN (0x0001)`, `Time to live: 3169 (52 minutes, 49 seconds)`, `Data length: 6` and `Name Server: ns(k).umass.edu`, where k =1,2,3.
- There are three additionl resource records returned.
- The additional information contains the IP addresses of the servers in the three answers above along with the name of the servers.
- For example, the additional information contains: `Name:ns2.umass.edu Address: 128.119.10.28` `Name: ns1.umass.edu Address: 128.119.10.27` `Name: ns3.umass.edu Address: 69.16.40.18`