School of Computer Science and Cybersecurity

CUC

Lab Report #

|  |  |
| --- | --- |
| Lab Name | Wireshark Lab7:DNS |
| Course Name | Computer Networks |

|  |  |  |  |
| --- | --- | --- | --- |
| Name | 赵婧宇 | Student ID | 201711123028 |

|  |  |
| --- | --- |
| Partners |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Date | 2019.06.13 | Lab Location | #48 |

|  |
| --- |
| Notes： |

**Section I Introduction**

Prepares the reader to understand the whole experiment.

|  |  |
| --- | --- |
| **Must Have:**  1. Clearly stated purpose of the experiment  2. Important background and/or theory | **May include:**  1. Description of specialized equipment  2. Justification of experiment's importance |

The Domain Name System (DNS) translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we’ll take a closer look at the client side of DNS. Recall that the client’s role in the DNS is relatively simple – a client sends a query to its local DNS server, and receives a response back. As shown in the textbook, much can go on “under the covers,” invisible to the DNS clients, as the hierarchical DNS servers communicate with each other to either recursively or iteratively resolve the client’s DNS query. From the DNS client’s standpoint, however, the protocol is quite simple – a query is formulated to the local DNS server and a response is received from that server.

Before beginning this lab, you’ll probably want to review DNS by reading Section 7.1 of the text. In particular, you may want to review the material on local DNS servers, DNS caching, DNS records and messages, and the TYPE field in the DNS record.

**Section II Methods & Materials**

Can be lists or even "refer to lab manual" where appropriate.

**Section III Procedure & Results**

Describes ACTUAL process, especially changes from planned method.

|  |
| --- |
| * **number** and **title** tables and graphs correctly and clearly * draw attention to key points in tables or graphs with a sentence * provide sample calculation only * state key result in sentence form |

**1. nslookup**

In this lab, we’ll make extensive use of the nslookup tool, which is available in most Linux/Unix and Microsoft platforms today. To run nslookup in Linux/Unix, you just type the nslookup command on the command line. To run it in Windows, open the Command Prompt and run nslookup on the command line.

In it is most basic operation, nslookup tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server (see the textbook for definitions of these terms). To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

The above screenshot shows the results of three independent nslookup commands (displayed in the Windows Command Prompt). In this example, the client host is located on the campus of Communication University of China in Beijing, where the default local DNS server is ns2.cuc.edu.cn. When running nslookup, if no DNS server is specified, then nslookup sends the query to the default DNS server, which in this case is ns2.cuc.edu.cn. Consider the first command:

nslookup [www.mit.edu](http://www.mit.edu)

In words, this command is saying “please send me the IP address for the host www.mit.edu”. As shown in the screenshot, the response from this command provides two pieces of information: (1) the name and IP address of the DNS server that provides the answer; and (2) the answer itself, which is the host name and IP address of www.mit.edu. Although the response came from the local DNS server at Communication University of China, it is quite possible that this local DNS server iteratively contacted several other DNS servers to get the answer, as described in Section 7.1 of the textbook.

Now consider the second command:

nslookup –type=NS mit.edu

In this example, we have provided the option “-type=NS” and the domain “mit.edu”. This causes nslookup to send a query for a type-NS record to the default local DNS server. In words, the query is saying, “please send me the host names of the authoritative DNS for mit.edu”. (When the –type option is not used, nslookup uses the default, which is to query for type A records.) The answer, displayed in the above screenshot, first indicates the DNS server that is providing the answer (which is the default local DNS server) along with three MIT nameservers. Each of these servers is indeed an authoritative DNS server for the hosts on the MIT campus. However, nslookup also indicates that the answer is “non-authoritative,” meaning that this answer came from the cache of some server rather than from an authoritative MIT DNS server. Finally, the answer also includes the IP addresses of the authoritative DNS servers at MIT. (Even though the type-NS query generated by nslookup did not explicitly ask for the IP addresses, the local DNS server returned these “for free” and nslookup displays the result.) Now finally consider the third command:

nslookup www.pku.edu.cn bitsy.mit.edu

In this example, we indicate that we want to the query sent to the DNS server bitsy.mit.edu rather than to the default DNS server (ns2.cuc.edu.cn). Thus, the query and reply transaction takes place directly between our querying host and bitsy.mit.edu. In this example, the DNS server bitsy.mit.edu provides the IP address of the host www.pku.edu.cn, which is a web server at the Peking University in Beijing,China.

Now that we have gone through a few illustrative examples, you are perhaps wondering about the general syntax of nslookup commands. The syntax is:

nslookup –option1 –option2 host-to-find dns-server

In general, nslookup can be run with zero, one, two or more options. And as we have seen in the above examples, the dns-server is optional as well; if it is not supplied, the query is sent to the default local DNS server.

**2. ipconfig**

ipconfig (for Windows) and ifconfig (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues. Here we’ll only describe ipconfig, although the Linux/Unix ifconfig is very similar. ipconfig can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on. For example, if you all this information about your host simply by entering ipconfig \all

**3. Tracing DNS with Wireshark**

Now that we are familiar with nslookup and ipconfig, we’re ready to get down to some serious business. Let’s first capture the DNS packets that are generated by ordinary Web-surfing activity.

• Use ipconfig to empty the DNS cache in your host.

• Open your browser and empty your browser cache. (With Internet Explorer, go to Tools menu and select Internet Options; then in the General tab select Delete Files.)

• Open Wireshark and enter “ip.addr == your\_IP\_address” into the filter, where you obtain your\_IP\_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.

• Start packet capture in Wireshark.

• With your browser, visit the Web page: http://www.ietf.org

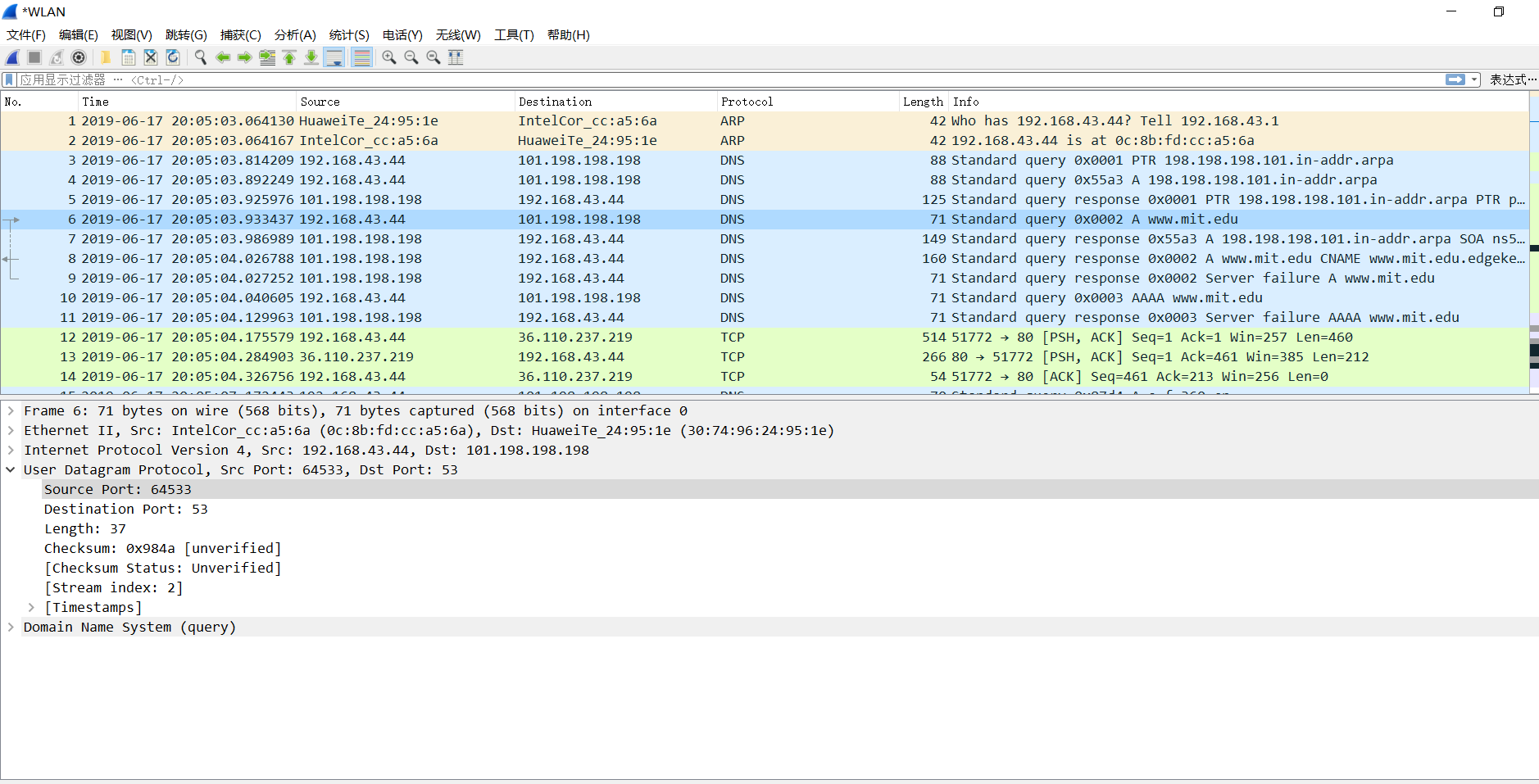
• Stop packet capture.

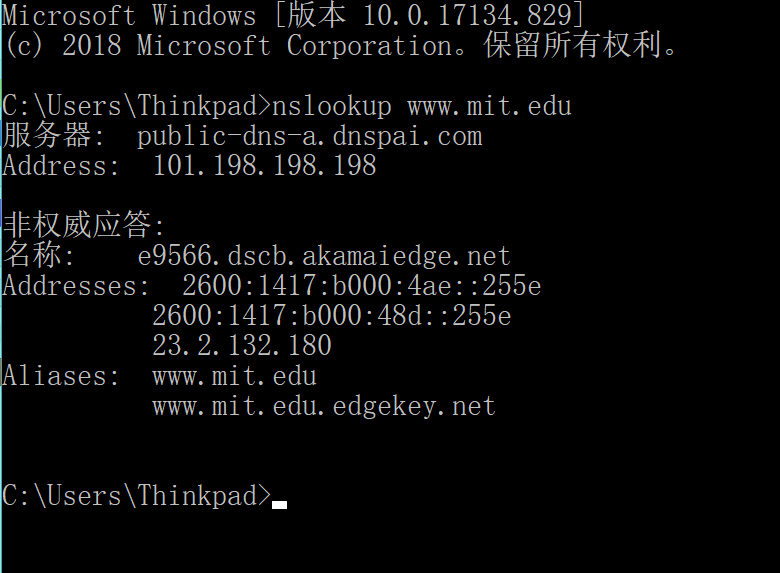
Let’s play with nslookup.

• Start packet capture.

• Do an nslookup on www.mit.edu

• Stop packet capture.



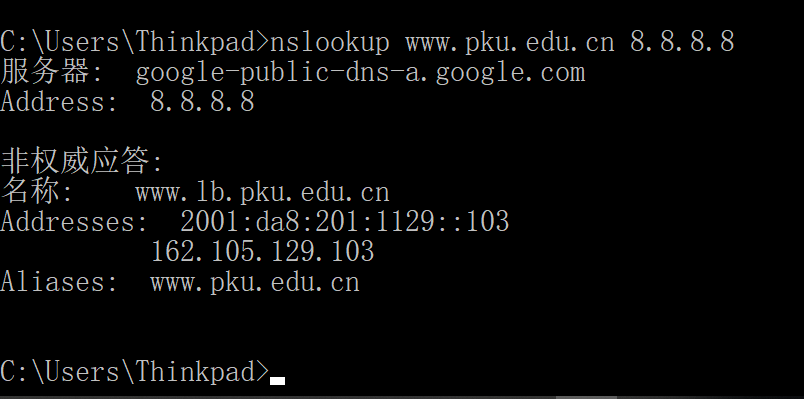


Now repeat the previous experiment, but instead issue the command:

nslookup –type=NS mit.edu

Now repeat the previous experiment, but instead issue the command:

nslookup www.pku.edu.cn 8.8.8.8



**Section IV Discussion**

Answer the questions in the section [what to hand in] of the lab guide, includes two aspects:

|  |
| --- |
| 1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?   C:\Users\Thinkpad\AppData\Local\Temp\WeChat Files\7d35484d8ba9f8b4072a517ab01d26b.png   1. Run nslookup to determine the authoritative DNS servers for a university in Europe.   C:\Users\Thinkpad\AppData\Local\Temp\WeChat Files\9bfd251a22c9484ea5b43a18f973429.png   1. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for netease mail. What is its IP address?   C:\Users\Thinkpad\AppData\Local\Temp\WeChat Files\d8323f1f18514107fd90ed665d35d4d.png   1. Locate the DNS query and response messages. Are then sent over UDP or TCP?   Answer: UDP   1. What is the destination port for the DNS query message? What is the source port of DNS response message?   C:\Users\Thinkpad\AppData\Local\Temp\WeChat Files\c8be81aa65efec1a3f1ee1374cbe057.png     1. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?   Answer:Destination 与用本地DNS服务器的IP地址相同。  C:\Users\Thinkpad\AppData\Local\Temp\WeChat Files\e2842f0609fec2b41fbc2013510a074.png  C:\Users\Thinkpad\AppData\Local\Temp\WeChat Files\399309cabd710b7e085e6c84b6a4f7d.png   1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?   C:\Users\Thinkpad\AppData\Local\Temp\1560389262(1).png  Answer: Type is A, No answers.   1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?   Answers: There are three answers, including NAME, TYPE, CLASS, TIME , DATA, ADDRESS.   1. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?   Answer: No, it doesn’t   1. This web page contains images. Before retrieving each image, does your host issue new DNS queries?   Answer: No.   1. What is the destination port for the DNS query message? What is the source port of DNS response message?      1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?   Answer: Yes.   1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?      1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?      1. Provide a screenshot.   *WLAN   1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?      1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?     Answer: The type is NS, no answers   1. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?   Answer: It doesn’t provide IP address   1. Provide a screenshot.   *WLAN   1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?     Answer: 8.8.8.8; 不是，与指定的服务器IP地址一致   1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?      1. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?     Answer: Two answers, it contains Name, Type, Class, Time to live, Data length and CNAME |
| 1. Provide a screenshot.   lab7-4.pcapng |
|  |
|  |

**Section V Conclusion**

States what is known as a result of the experiment.

|  |  |
| --- | --- |
| **Must do:**  1. State what's known  2. Justify that statement | **May do:**  1. State significance of findings  2. Suggest further research |

When input nslookup www.pku.edu.cn bitsy.mit.edu, request was failed,

Then change to nslookup [www.pku.edu.cn](http://www.pku.edu.cn) 8.8.8.8