计算机学院_计算机网络_课程实验报告

实验题目： DNS		学号：202200130048
日期：3.19	班级： 6	姓名： 陈静雯
Email：1205037094@qq.com		

实验方法介绍：

通过 nslookup 和 wireshark 跟踪分析 dns 的过程和作用

实验过程描述：

1.nslookup

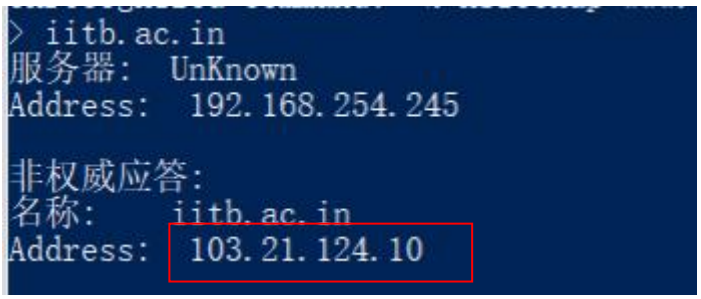
2.The DNS cache on your computer

3. Tracing DNS with Wireshark

结论分析：

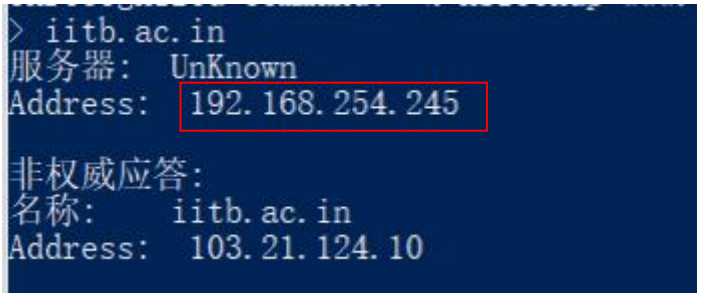
1.Run nslookup to obtain the IP address of the web server for the Indian Institute of Technology in Bombay, India: www.iitb.ac.in. What is the IP address of www.iitb.ac.in

103.21.124.10



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

192.168.254.245



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

non-authoritative server,非权威应答

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 为 dns3.iitb.ac.in，ip 地址为 103.21.127.129

```
> set ty=NS
> iitb.ac.in
服务器:  UnKnown
Address:  192.168.254.245

非权威应答:
iitb.ac.in      nameserver = dns3.iitb.ac.in
iitb.ac.in      nameserver = dns2.iitb.ac.in
iitb.ac.in      nameserver = dns1.iitb.ac.in

dns1.iitb.ac.in internet address = 103.21.125.129
dns2.iitb.ac.in internet address = 103.21.126.129
dns3.iitb.ac.in internet address = 103.21.127.129
>
```

5. 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?

packet number：882，sent over TCP

881	122.935329	172.25.199.141	192.168.254.245	TCP	56	36772 → 53 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2 [TCP segment of a reassembled PDU]
882	122.935366	172.25.199.141	192.168.254.245	DNS	89	Standard query 0xc99b AAAA gaia.cs.umass.edu

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?

packet number：895，通过 TCP 接收

894	122.939316	172.25.199.141	192.168.254.245	TCP	54	36773 → 53 [ACK] Seq=39 Ack=157 Win=64085 Len=0
895	122.942467	192.168.254.245	172.25.199.141	DNS	91	Standard query response 0xc99b AAAA gaia.cs.umass.edu

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

Dst：53，src：36772

```
Transmission Control Protocol, Src Port: 36772, Dst Port: 53, Seq: 3, Ack: 1, Len: 35
    Source Port: 36772
    Destination Port: 53
```

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

发送到 192.168.254.245

```
[Header checksum status: Unverified]
Source Address: 172.25.199.141
Destination Address: 192.168.254.245
```

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

1 个 question，0 个 answer

```
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  gaia.cs.umass.edu: type A, class IN
      Name: gaia.cs.umass.edu
      [Name Length: 17]
      [Label Count: 4]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
```

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?

1 个 question, 1 个 answer

```
Questions: 1
Answer RRs: 1
Authority RRs: 3
Additional RRs: 3
Queries
  gaia.cs.umass.edu: type A, class IN
      Name: gaia.cs.umass.edu
      [Name Length: 17]
      [Label Count: 4]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
Answers
  gaia.cs.umass.edu: type A, class IN, addr 128.119.245.12
Authoritative nameservers
  umass.edu: type NS, class IN, ns ns2.umass.edu
  umass.edu: type NS, class IN, ns ns3.umass.edu
  umass.edu: type NS, class IN, ns ns1.umass.edu
```

11. 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/?

437

437	82.326438	172.25.199.141	128.119.245.12	HTTP	545	GET /kurose_ross/ HTTP/1.1

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?

354

What is the packet number in the trace of the received DNS response?

362

349	82.054114	172.25.199.141	192.168.254.245	DNS	89	Standard query 0x958d AAAA gaia.cs.umass.edu
352	82.054349	172.25.199.141	192.168.254.245	DNS	89	Standard query 0x0065 HTTPS gaia.cs.umass.edu
354	82.054498	172.25.199.141	192.168.254.245	DNS	89	Standard query 0xf0ca A gaia.cs.umass.edu
361	82.057368	192.168.254.245	172.25.199.141	DNS	144	Standard query response 0x958d AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
362	82.057369	192.168.254.245	172.25.199.141	DNS	209	Standard query response 0xf0ca A gaia.cs.umass.edu A 128.119.245.12 NS ns1.umass.edu NS ns2.umass.edu NS
369	82.062036	192.168.254.245	172.25.199.141	DNS	91	Standard query response 0x0065 HTTPS gaia.cs.umass.edu
379	82.070803	172.25.199.141	192.168.254.245	DNS	89	Standard query 0xd577 AAAA gaia.cs.umass.edu
383	82.071964	172.25.199.141	192.168.254.245	DNS	89	Standard query 0xe5b1 A gaia.cs.umass.edu
388	82.074142	192.168.254.245	172.25.199.141	DNS	902	Standard query response 0xe5b1 A gaia.cs.umass.edu A 128.119.245.12 NS f.edu-servers.net NS i.edu-server
392	82.077009	192.168.254.245	172.25.199.141	DNS	91	Standard query response 0xd577 AAAA gaia.cs.umass.edu

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?

483

481	83.054857	172.25.199.141	128.119.245.12	HTTP	465	GET /kurose_ross/custom.css HTTP/1.1
482	83.054962	172.25.199.141	128.119.245.12	HTTP	449	GET /kurose_ross/script.js HTTP/1.1
483	83.055160	172.25.199.141	128.119.245.12	HTTP	529	GET /kurose_ross/header_graphic_book_8E_3.jpg HTTP/1.1

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.

497，响应速度变快了

495	83.063196	172.25.199.141	192.168.254.245	TCP	54	36735 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
496	83.063310	172.25.199.141	192.168.254.245	TCP	56	36735 → 53 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2 [TCP segment of a reassembled PDU]
497	83.063349	172.25.199.141	192.168.254.245	DNS	98	Standard query 0xf67d A stackpath.bootstrapcdn.com
498	83.063412	192.168.254.245	172.25.199.141	TCP	62	53 → 36736 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM
499	83.063413	192.168.254.245	172.25.199.141	TCP	62	53 → 36737 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM
500	83.063465	172.25.199.141	192.168.254.245	TCP	54	36736 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
501	83.063495	172.25.199.141	192.168.254.245	TCP	54	36737 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
502	83.063525	172.25.199.141	192.168.254.245	TCP	56	36736 → 53 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2 [TCP segment of a reassembled PDU]
503	83.063568	172.25.199.141	192.168.254.245	DNS	98	Standard query 0x15b6 HTTPS stackpath.bootstrapcdn.com
504	83.063620	172.25.199.141	192.168.254.245	TCP	56	36737 → 53 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2 [TCP segment of a reassembled PDU]
505	83.063647	172.25.199.141	192.168.254.245	DNS	87	Standard query 0x07cd AAAA code.jquery.com

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

Dst port query：53

src port response：53

64	24.813506	172.25.140.166	192.168.254.245	DNS	76	Standard query 0x0002 A www.cs.umass.edu
65	24.814640	192.168.254.245	172.25.140.166	DNS	194	Standard query response 0x0002 A www.cs.umass.edu A 128.119.240.84 NS ns3.umass.edu NS ns1.umass.edu NS ns2.umass.edu A 128.119…

```
User Datagram Protocol, Src Port: 64085, Dst Port: 53
    Source Port: 64085
    Destination Port: 53
```

```
User Datagram Protocol, Src Port: 53, Dst Port: 64085
    Source Port: 53
    Destination Port: 64085
```

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

192.168.254.245，yes

```
Source Address: 172.25.140.166
Destination Address: 192.168.254.245
```

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

Type:A，no answer

```
[Label Count: 4]
Type: A (1) (Host Address)
Class: IN (0x0001)
```

```
> Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
```

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

1 question, 1 answer

```
  Questions: 1
  Answer RRs: 1
  Authority RRs: 3
  Additional RRs: 3
v Queries
  v www.cs.umass.edu: type A, class IN
      Name: www.cs.umass.edu
      [Name Length: 16]
      [Label Count: 4]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
v Answers
  > www.cs.umass.edu: type A, class IN, addr 128.119.240.84
> Authoritative nameservers
```

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

192.168.254.245, yes

```
104 33.730893   172.25.140.166   192.168.254.245   DNS   69 Standard query 0x0002 NS umass.edu
105 34.029325   192.168.254.245  172.25.140.166    DNS   171 Standard query response 0x0002 NS umass.edu NS ns3.umass.edu NS ns2.umass.edu NS ns1.umass.edu A 128.119.10.27 A 128.11
```

```
[Header checksum status: Unverified]
Source Address: 172.25.140.166
Destination Address: 192.168.254.245
```

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

1 question, no answer

```
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
v Queries
  v umass.edu: type NS, class IN
      Name: umass.edu
      [Name Length: 9]
      [Label Count: 2]
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
```

18. 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?

3 answer，权威服务器的 name，3 additional record，权威服务器的 ip 地址

```
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 3
Queries
  umass.edu: type NS, class IN
    Name: umass.edu
    [Name Length: 9]
    [Label Count: 2]
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
Answers
  umass.edu: type NS, class IN, ns ns3.umass.edu
  umass.edu: type NS, class IN, ns ns2.umass.edu
  umass.edu: type NS, class IN, ns ns1.umass.edu
Additional records
  ns1.umass.edu: type A, class IN, addr 128.119.10.27
  ns2.umass.edu: type A, class IN, addr 128.119.10.28
  ns3.umass.edu: type A, class IN, addr 69.16.40.18
[Request In: 104]
```

结论：

1. type=A 为非权威应答，NS 为权威应答
2. Dns cache 可以加快访问速度
3. Wireshark 跟踪捕获 dns 信息后可以查看发送接收的 ip 地址，question 和 answer 的具体内容