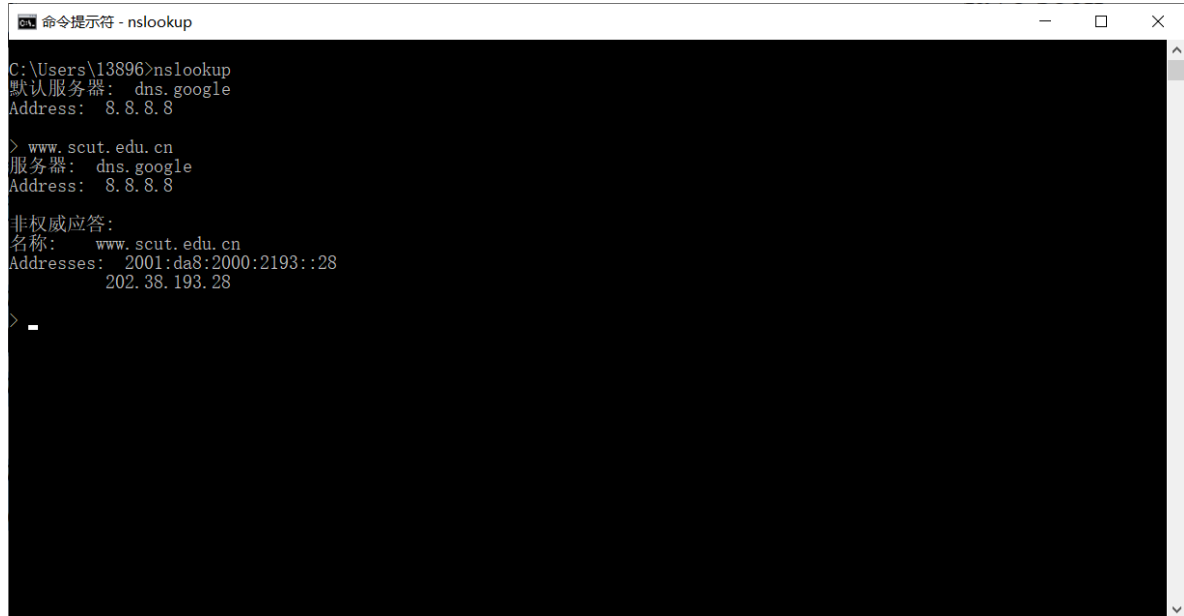


1. nslookup

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

Answer: My school's web server's IP address is 202.38.193.28



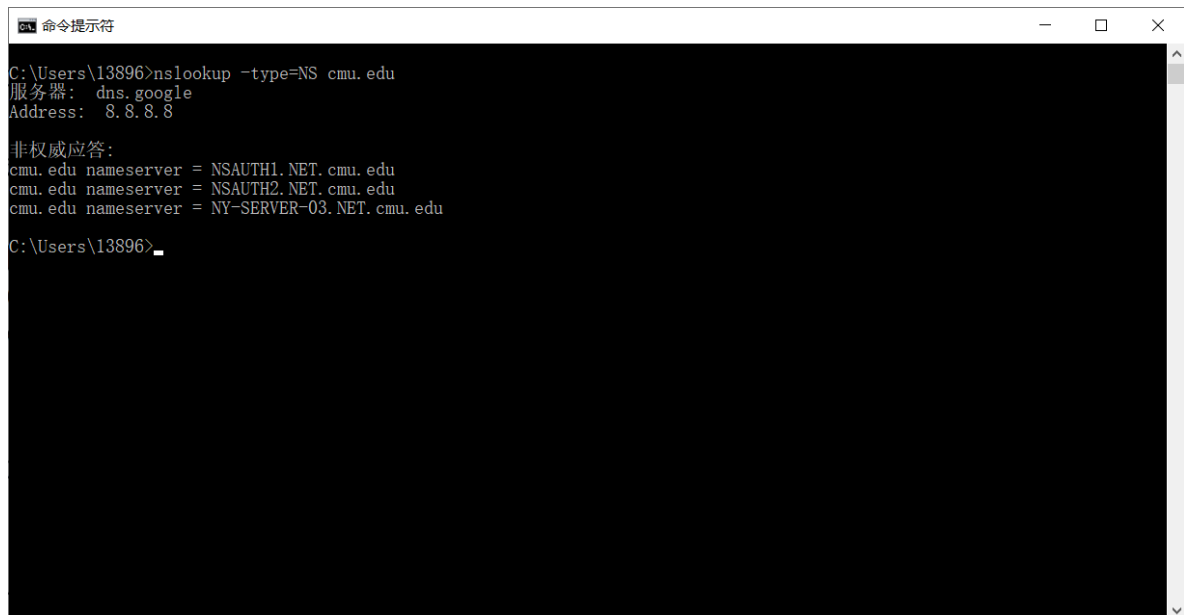
```
命令提示符 - nslookup
C:\Users\13896>nslookup
默认服务器: dns.google
Address: 8.8.8.8

> www.scut.edu.cn
服务器: dns.google
Address: 8.8.8.8

非权威应答:
名称: www.scut.edu.cn
Addresses: 2001:da8:2000:2193::28
202.38.193.28

> _
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe.



```
命令提示符
C:\Users\13896>nslookup -type=NS cmu.edu
服务器: dns.google
Address: 8.8.8.8

非权威应答:
cmu.edu nameserver = NSAUTH1.NET.cmu.edu
cmu.edu nameserver = NSAUTH2.NET.cmu.edu
cmu.edu nameserver = NY-SERVER-03.NET.cmu.edu

C:\Users\13896>_
```

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

```
命令提示符
nslookup [-opt ...] host server # 仅查找使用 "server" 的 "host"

C:\Users\13896>nslookup NSAUTH1.NET.cmu.edu mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
服务器:  UnKnown
Address:  209.73.190.11

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 请求 UnKnown 超时

C:\Users\13896>
```

2. ipconfig

- `ipconfig /all`

```
1920 x 1080
C:\Users\13896>ipconfig /all

Windows IP 配置

   主机名 . . . . . : LAPTOP-6MP5H902
   主 DNS 后缀 . . . . . : 
   节点类型 . . . . . : 混合
   IP 路由已启用 . . . . . : 否
   WINS 代理已启用 . . . . . : 否

以太网适配器 以太网 3:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . : 
   描述 . . . . . : TAP-Windows Adapter V9
   物理地址 . . . . . : 00-FF-84-04-04-79
   DHCP 已启用 . . . . . : 否
   自动配置已启用 . . . . . : 是

以太网适配器 VirtualBox Host-Only Network:

   连接特定的 DNS 后缀 . . . . . : 
   描述 . . . . . : VirtualBox Host-Only Ethernet Adapter
   物理地址 . . . . . : 0A-00-27-00-00-09
   DHCP 已启用 . . . . . : 否
   自动配置已启用 . . . . . : 是
   本地链接 IPv6 地址 . . . . . : fe80::1d1a:891a:7a8a:elf5N9(首选)
   IPv4 地址 . . . . . : 192.168.56.1(首选)
   子网掩码 . . . . . : 255.255.255.0
   默认网关 . . . . . : 168427550
   DHCPv6 IAID . . . . . : 
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-20-FF-09-38-54-E1-AD-54-B0-06
   DNS 服务器 . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
   TCP/IP 上的 NetBIOS . . . . . : 已启用

无线局域网适配器 WLAN:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . : scut.edu.cn
   描述 . . . . . : Intel(R) Dual Band Wireless-AC 3165
   物理地址 . . . . . : 88-B1-11-E6-B6-6C
   DHCP 已启用 . . . . . : 是
   自动配置已启用 . . . . . : 是

无线局域网适配器 本地连接* 1:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . : 
   描述 . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   物理地址 . . . . . : 8A-B1-11-E6-B6-6C
   DHCP 已启用 . . . . . : 是
   自动配置已启用 . . . . . : 是

无线局域网适配器 本地连接* 2:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . : 
   描述 . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   物理地址 . . . . . : 88-B1-11-E6-B6-6D
   DHCP 已启用 . . . . . : 是
   自动配置已启用 . . . . . : 是

以太网适配器 以太网:

   连接特定的 DNS 后缀 . . . . . : 
   描述 . . . . . : Realtek PCIe GbE Family Controller
   物理地址 . . . . . : 54-E1-AD-54-B0-06
   DHCP 已启用 . . . . . : 是
   自动配置已启用 . . . . . : 是
   IPv4 地址 . . . . . : 222.16.62.151(首选)
   子网掩码 . . . . . : 255.255.255.0
   默认网关 . . . . . : 222.16.62.254
   DNS 服务器 . . . . . : 8.8.8.8
   TCP/IP 上的 NetBIOS . . . . . : 已启用

C:\Users\13896>
```

3. Tracing DNS with Wireshark

4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Answer: Both UDP

The image shows a Wireshark packet capture of DNS traffic. The packet list pane displays several DNS queries and responses. A red arrow points to the 'User Datagram Protocol' entry in the packet details pane, which shows 'Src Port: 62333, Dst Port: 53'. The packet bytes pane shows the raw data of the DNS query and response.

No.	Time	Source	Destination	Protocol	Length	Info
92	18:48:15.864352	222.16.62.151	8.8.8.8	DNS	72	Standard query 0xd68b A www.ietf.org
93	18:48:15.864368	222.16.62.151	8.8.8.8	DNS	72	Standard query 0xd68b A www.ietf.org
94	18:48:15.866453	8.8.8.8	222.16.62.151	DNS	165	Standard query response 0xd68b A www.ietf.org CNAME www.ietf.org
125	18:48:17.050550	222.16.62.151	8.8.8.8	DNS	89	Standard query 0xc352 A nav.smartscreen.microsoft.com
126	18:48:17.050565	222.16.62.151	8.8.8.8	DNS	89	Standard query 0xc352 A nav.smartscreen.microsoft.com
128	18:48:17.076241	222.16.62.151	8.8.8.8	DNS	89	Standard query 0xc352 A nav.smartscreen.microsoft.com
129	18:48:17.076256	222.16.62.151	8.8.8.8	DNS	89	Standard query 0xc352 A nav.smartscreen.microsoft.com
130	18:48:17.078552	8.8.8.8	222.16.62.151	DNS	210	Standard query response 0xc352 A nav.smartscreen.microsoft.com
493	18:48:18.414745	222.16.62.151	8.8.8.8	DNS	78	Standard query 0x16e6 A analytics.ietf.org
494	18:48:18.414768	222.16.62.151	8.8.8.8	DNS	78	Standard query 0x16e6 A analytics.ietf.org
495	18:48:18.417872	8.8.8.8	222.16.62.151	DNS	108	Standard query response 0x16e6 A analytics.ietf.org CNAME ietf.org

Internet Protocol Version 4, Src: 222.16.62.151, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 62333, Dst Port: 53
Source Port: 62333

Internet Protocol Version 4, Src: 8.8.8.8, Dst: 222.16.62.151
User Datagram Protocol, Src Port: 53, Dst Port: 62333
Source Port: 53

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

Answer: As can see in the picture above, both port are 53

6. 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: They are the same.

The image shows a Wireshark packet capture of DNS traffic. The packet list pane displays several DNS queries and responses. A red arrow points to the 'Destination' column, which shows '8.8.8.8' for the first two packets.

No.	Time	Source	Destination	Protocol	Length	Info
92	18:48:15.864352	222.16.62.151	8.8.8.8	DNS	72	Standard query 0xd68b A www.ietf.org
93	18:48:15.864368	222.16.62.151	8.8.8.8	DNS	72	Standard query 0xd68b A www.ietf.org

服务器: dns.google
Address: 8.8.8.8

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

Answer: Type is A, means query for IP address, it doesn't contain any answers.

```
Domain Name System (query)
  Transaction ID: 0xd68b
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  < Queries
    > www.ietf.org: type A, class IN
    [Response In: 94]
```

8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

```
Domain Name System (response)
  Transaction ID: 0xd68b
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 4
  Authority RRs: 0
  Additional RRs: 0
  < Queries
    > www.ietf.org: type A, class IN
  < Answers
    > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.110.6
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 172.67.33.249
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.111.6
  [Request In: 92]
  [Time: 0.002101000 seconds]
```

9. 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: Yes, there is.

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

Answer: No, it already have local DNS cache.

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

ip.addr == 222.16.62.151 and dns

No.	Time	Source	Destination	Protocol	Length	Info
1301	19:18:29.385367	222.16.62.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
1302	19:18:29.385394	222.16.62.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
1303	19:18:29.386894	8.8.8.8	222.16.62.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa
1304	19:18:29.388336	222.16.62.151	8.8.8.8	DNS	71	Standard query 0x0002 A www.mit.edu
1305	19:18:29.388344	222.16.62.151	8.8.8.8	DNS	71	Standard query 0x0002 A www.mit.edu
1309	19:18:29.559325	8.8.8.8	222.16.62.151	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net
1310	19:18:29.563832	222.16.62.151	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
1311	19:18:29.563860	222.16.62.151	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
1314	19:18:29.640674	8.8.8.8	222.16.62.151	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net

Protocol: UDP (17)
Header checksum: 0xb897 [validation disabled]
[Header checksum status: Unverified]
Source: 222.16.62.151
Destination: 8.8.8.8

User Datagram Protocol, Src Port: 53288, Dst Port: 53

Domain Name System (query)
Transaction ID: 0x0002
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

Queries
> www.mit.edu: type A, class IN

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

Answer: Yes, it is.

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

Answer: there are three DNS queries, type of which are PTR, A, AAAA. doesn't contain any answers.

14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

1304	19:18:29.388330	222.16.62.151	8.8.8.8	DNS	71	Standard query 0x0002 A www.mit.edu
1305	19:18:29.388344	222.16.62.151	8.8.8.8	DNS	71	Standard query 0x0002 A www.mit.edu
1309	19:18:29.559325	8.8.8.8	222.16.62.151	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net
1310	19:18:29.563832	222.16.62.151	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
1311	19:18:29.563860	222.16.62.151	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
1314	19:18:29.640674	8.8.8.8	222.16.62.151	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net

Destination: 222.16.62.151
> User Datagram Protocol, Src Port: 53, Dst Port: 53288

Domain Name System (response)
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0

Answers
> www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
> www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
> e9566.dscb.akamaiedge.net: type A, class IN, addr 104.122.4.43

[request ID: 1304]
[Time: 0.170995000 seconds]

15. Provide a screenshot. **Answer: as above.**

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

Answer: YES

ip.addr == 222.16.62.151 and dns

No.	Time	Source	Destination	Protocol	Length	Info
476	19:24:21.814577	222.16.62.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
477	19:24:21.814614	222.16.62.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
478	19:24:21.816775	8.8.8.8	222.16.62.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.
479	19:24:21.818785	222.16.62.151	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
480	19:24:21.818812	222.16.62.151	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
485	19:24:22.026776	8.8.8.8	222.16.62.151	DNS	234	Standard query response 0x0002 NS mit.edu NS use5.a

> Frame 476: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{F4F6F9D4-FAEC-4D22-ACE7-746265CB46}

> Ethernet II, Src: LCFChFe_54:b0:06 (54:e1:ad:54:b0:06), Dst: Hangzhou_49:1d:00 (0c:da:41:49:1d:00)

> Internet Protocol Version 4, Src: 222.16.62.151, Dst: 8.8.8.8

> User Datagram Protocol, Src Port: 50714, Dst Port: 53

Source Port: 50714

Destination Port: 53

Length: 46

Checksum: 0xf35c [unverified]

[Checksum Status: Unverified]

[Stream index: 38]

> [Timestamps]

> Domain Name System (query)

Transaction ID: 0x0001

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

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

Answer: type is NS, no answers.

No.	Time	Source	Destination	Protocol	Length	Info
479	19:24:21.818785	222.16.62.151	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
480	19:24:21.818812	222.16.62.151	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
485	19:24:22.026776	8.8.8.8	222.16.62.151	DNS	234	Standard query response 0x0002 NS mit.edu NS use5.akam.net NS u

> Frame 479: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{F4F6F9D4-FAEC-4D22-ACE7-746265CB46A}, id 0

> Ethernet II, Src: LCFChFe_54:b0:06 (54:e1:ad:54:b0:06), Dst: Hangzhou_49:1d:00 (0c:da:41:49:1d:00)

> Internet Protocol Version 4, Src: 222.16.62.151, Dst: 8.8.8.8

> User Datagram Protocol, Src Port: 50715, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x0002

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

> mit.edu type NS, class IN

[Response time: 482]

18. 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 nameservers?

Answer: the type=NS

•**name** is domain

•**value** is hostname of authoritative name server for this domain

479	19:24:21.818785	222.16.62.151	8.8.8.8	DNS	67 Standard query response 0x0002 NS mit.edu
480	19:24:21.818812	222.16.62.151	8.8.8.8	DNS	67 Standard query response 0x0002 NS mit.edu
485	19:24:22.026776	8.8.8.8	222.16.62.151	DNS	234 Standard query response 0x0002 NS mit.edu NS use5.akam.net

> Frame 485: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{F4F6F9D4-FAEC-4D22-ACE7-746265CB46EA},
 > Ethernet II, Src: Hangzhou_49:1d:00 (0c:da:41:49:1d:00), Dst: LCFCHeFe_54:b0:06 (54:e1:ad:54:b0:06)
 > Internet Protocol Version 4, Src: 8.8.8.8, Dst: 222.16.62.151
 > User Datagram Protocol, Src Port: 53, Dst Port: 50715
 > Domain Name System (response)
 Transaction ID: 0x0002
 Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 8
 Authority RRs: 0
 Additional RRs: 0
 Queries:
 Answers:
 > mit.edu: type NS, class IN, ns use5.akam.net
 > mit.edu: type NS, class IN, ns use2.akam.net
 > mit.edu: type NS, class IN, ns ns1-37.akam.net
 > mit.edu: type NS, class IN, ns asia2.akam.net
 > mit.edu: type NS, class IN, ns asia1.akam.net
 > mit.edu: type NS, class IN, ns usw2.akam.net
 > mit.edu: type NS, class IN, ns ns1-173.akam.net
 > mit.edu: type NS, class IN, ns eur5.akam.net
 [Request In: 479]
 [Time: 0.207991000 seconds]

19. Provide a screenshot. **Answer: As above.**

20. 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?

ip.addr == 222.16.62.151 and dns						
No.	Time	Source	Destination	Protocol	Length	
76	19:36:17.215324	222.16.62.151	8.8.8.8	DNS	7	
77	19:36:17.215341	222.16.62.151	8.8.8.8	DNS	7	
79	19:36:17.240361	222.16.62.151	8.8.8.8	DNS	7	
80	19:36:17.240373	222.16.62.151	8.8.8.8	DNS	7	
82	19:36:17.318691	8.8.8.8	222.16.62.151	DNS	8	
83	19:36:17.321692	222.16.62.151	18.0.72.3	DNS	8	
84	19:36:17.321709	222.16.62.151	18.0.72.3	DNS	8	
199	19:36:19.323338	222.16.62.151	18.0.72.3	DNS	7	
200	19:36:19.323352	222.16.62.151	18.0.72.3	DNS	7	
244	19:36:21.324308	222.16.62.151	18.0.72.3	DNS	7	
245	19:36:21.324336	222.16.62.151	18.0.72.3	DNS	7	

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

22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

23. Provide a screenshot.

***the last 4 questions got a time out**