

```
C:\Users\acer>nslookup www.baidu.com
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
名称:     www.a.shifen.com
Addresses: 182.61.200.6
          182.61.200.7
Aliases:  www.baidu.com
```

1.

2.

```
C:\Users\acer>nslookup -type=NS tu-dresden.de
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
tu-dresden.de    nameserver = adns1.zih.tu-dresden.de
tu-dresden.de    nameserver = dns-3.dfn.de
tu-dresden.de    nameserver = dns-1.dfn.de
tu-dresden.de    nameserver = adns2.zih.tu-dresden.de
```

3.

```
C:\Users\acer>nslookup -type=MX www.yahoo.com
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
www.yahoo.com    canonical name = atsv2-fp-shed.wgl.b.yahoo.com
wgl.b.yahoo.com
    primary name server = yf1.yahoo.com
    responsible mail addr = hostmaster.yahoo-inc.com
    serial    = 1569653955
    refresh   = 30 (30 secs)
    retry     = 30 (30 secs)
    expire    = 86400 (1 day)
    default TTL = 300 (5 mins)
```

4. Through UDP

5. Query destination: 53

Response source: 53

▼ User Datagram Protocol, Src Port: 51392, Dst Port: 53  
Source Port: 51392  
Destination Port: 53

6. Destination IP address: 202.38.64.17

My local DNS server's IP address: 202.38.64.17

```
无线局域网适配器 WLAN:  
连接特定的 DNS 后缀 . . . . . : ustc.edu.cn  
描述 . . . . . : Qualcomm Atheros QCA61x4A Wireless Network Adapter  
物理地址. . . . . : 3C-A0-67-F6-4C-B9  
DHCP 已启用 . . . . . : 是  
自动配置已启用. . . . . : 是  
IPv6 地址 . . . . . : 2001:da8:d800:196:d102:200a:83bb:7ff4(首选)  
临时 IPv6 地址. . . . . : 2001:da8:d800:196:18de:a0fd:668d:50d3(首选)  
本地链接 IPv6 地址. . . . . : fe80::d102:200a:83bb:7ff4%17(首选)  
IPv4 地址 . . . . . : 210.45.119.62(首选)  
子网掩码 . . . . . : 255.255.254.0  
获得租约的时间 . . . . . : 2019年9月28日 18:32:00  
租约过期的时间 . . . . . : 2019年9月28日 22:02:03  
默认网关 . . . . . : 210.45.118.1  
DHCP 服务器 . . . . . : 202.38.64.17  
DHCPv6 IAID . . . . . : 104636519  
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-20-70-85-0A-FC-45-96-A1-1C-98  
DNS 服务器 . . . . . : 202.38.64.56  
                      : 202.38.64.17  
TCP/IP 上的 NetBIOS . . . . . : 已启用
```

7. “Type” is Host Address and contains no “answers”

▼ Domain Name System (query)  
Transaction ID: 0xfd10  
‣ Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
▼ Queries  
‣ www.ietf.org: type A, class IN  
Name: www.ietf.org  
[Name Length: 12]  
[Label Count: 3]  
Type: A (Host Address) (1)  
Class: IN (0x0001)

8. Three answers.

```

▼ Answers
  ▼ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    Name: www.ietf.org
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 300
    Data length: 33
    CNAME: www.ietf.org.cdn.cloudflare.net
  ▼ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300
    Data length: 4
    Address: 104.20.1.85
  ▼ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300
    Data length: 4
    Address: 104.20.0.85

```

## 9. 104.20.1.85

104.20.1.85	TCP	66 50230 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
104.20.1.85	TCP	66 50231 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
182.254.42.87	TCP	66 50232 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
104.20.1.85	TCP	66 50233 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

10. My host didn't issue new DNS query.

11. Query destination port and response source port are both 53.

12. 202.38.64.56 and it's my default DNS server.

13. "Type" is Host Address and contains no "answers".

14. Standard query response, no such name.

```

▼ Domain Name System (response)
  Transaction ID: 0xae2
  > Flags: 0x8583 Standard query response, No such name
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 0

```

No.	Time	Source	Destination	Protocol	Length	Info
140	2.748476	58.251.112.232	210.45.119.62	TCP	60	443 → 51757 [ACK] Seq=1 Ack=263 Win=15544 Len=0
141	2.748477	58.251.112.232	210.45.119.62	HTTP	122	HTTP/1.1 200 OK Continuation
142	2.748578	210.45.119.62	111.206.57.226	TCP	54	59564 → 80 [ACK] Seq=3737 Ack=1369 Win=252 Len=0
143	2.748932	210.45.119.62	58.251.112.232	TCP	54	51757 → 443 [FIN, ACK] Seq=263 Ack=69 Win=64172 Len=0
144	2.749983	210.45.119.62	182.254.42.87	UDP	724	52941 → 8080 Len=682
145	2.769334	182.254.42.87	210.45.119.62	TCP	60	80 → 51756 [ACK] Seq=1 Ack=500 Win=15360 Len=0
146	2.771786	182.254.42.87	210.45.119.62	HTTP	896	HTTP/1.1 200 OK
148	2.773364	210.45.119.62	182.254.42.87	TCP	66	51759 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
149	2.773840	210.45.119.62	182.254.42.87	TCP	54	51756 → 80 [FIN, ACK] Seq=500 Ack=843 Win=64694 Len=0
150	2.773923	202.38.64.17	210.45.119.62	DNS	128	Standard query response 0xaae2 No such name A www.mit.edu.ustc.edu.cn SOA ns.ustc.edu.cn
151	2.801411	182.254.42.87	210.45.119.62	UDP	644	8080 → 52941 Len=602
152	2.802463	58.251.112.242	210.45.119.62	TCP	60	8080 → 51758 [ACK] Seq=1 Ack=495 Win=17408 Len=0
153	2.808798	58.251.112.242	210.45.119.62	HTTP	303	HTTP/1.1 200 OK (text/html)
154	2.809227	210.45.119.62	58.251.112.242	TCP	54	51758 → 8080 [FIN, ACK] Seq=495 Ack=250 Win=65280 Len=0
155	2.817967	210.45.119.62	58.251.112.242	TCP	66	51760 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
157	2.948208	58.251.112.232	210.45.119.62	TCP	60	443 → 51757 [FIN, ACK] Seq=69 Ack=264 Win=15544 Len=0

Frame 150: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface 0  
 Ethernet II, Src: Hangzhou\_91:72:e2 (Scid:78:91:72:e2), Dst: Liteontef\_6:4c:b9 (Scid:06:7f:64:c9)  
 Destination: Liteontef\_6:4c:b9 (Scid:06:7f:64:c9)  
 Source: Hangzhou\_91:72:e2 (Scid:78:91:72:e2)  
 Type: IPv4 (0x0800)  
 Internet Protocol Version 4, Src: 202.38.64.17, Dst: 210.45.119.62  
 User Datagram Protocol, Src Port: 53, Dst Port: 57631  
 Domain Name System (response)  
 Transaction ID: 0xaae2  
 Flags: 0x8583 Standard query response, No such name  
 Questions: 1  
 Answer RRs: 0  
 Authority RRs: 1  
 Additional RRs: 0  
 Queries  
 www.mit.edu.ustc.edu.cn: type A, class IN  
 Name: www.mit.edu.ustc.edu.cn  
 [Name length: 23]  
 [Label count: 6]

15.

16. 202.38.64.56, and it's my DNS server.

17. "Type" is IP, and contains no "answers".

18. Answers below

#### Answers

- > mit.edu: type NS, class IN, ns use5.akam.net
- > mit.edu: type NS, class IN, ns ns1-173.akam.net
- > mit.edu: type NS, class IN, ns usw2.akam.net
- > mit.edu: type NS, class IN, ns asia2.akam.net
- > mit.edu: type NS, class IN, ns eur5.akam.net
- > mit.edu: type NS, class IN, ns use2.akam.net
- > mit.edu: type NS, class IN, ns asia1.akam.net
- > mit.edu: type NS, class IN, ns ns1-37.akam.net

IP addresses are not provided.

No.	Time	Source	Destination	Protocol	Length	Info
121	2.540872	182.254.41.37	210.45.119.62	OIDQ	689	OIDQ Protocol
144	3.044209	210.45.119.62	182.254.41.37	OIDQ	89	OIDQ Protocol
145	3.080735	210.45.119.62	202.38.64.56	DNS	67	Standard query 0xf594 A mit.edu
146	3.084055	182.254.41.37	210.45.119.62	OIDQ	689	OIDQ Protocol
148	3.090270	210.45.119.62	182.254.41.37	OIDQ	81	OIDQ Protocol
150	3.128647	182.254.41.37	210.45.119.62	OIDQ	89	OIDQ Protocol
151	3.134442	202.38.64.56	210.45.119.62	DNS	83	Standard query response 0xf594 A mit.edu A 23.42.66.203
155	3.178685	202.38.64.56	210.45.119.62	DNS	234	Standard query response 0x0004 NS mit.edu NS use5.akam.net NS ns1-173.akam.net NS usw2.akam.net NS asia2...
160	3.234596	210.45.119.62	111.206.57.226	TCP	306	59564 → 80 [PSH, ACK] Seq=1773 Ack=940 Win=255 Len=332
164	3.266008	111.206.57.226	210.45.119.62	TCP	106	80 → 59564 [PSH, ACK] Seq=949 Ack=2105 Win=1938 Len=52
165	3.306985	210.45.119.62	111.206.57.226	TCP	54	59564 → 80 [ACK] Seq=2105 Ack=1001 Win=255 Len=0
170	3.425888	210.45.119.62	182.254.41.37	UDP	89	4000 → 8000 Len=47
174	3.471660	182.254.41.37	210.45.119.62	OIDQ	121	OIDQ Protocol
175	3.507114	182.254.41.37	210.45.119.62	UDP	97	8000 → 4000 Len=55
179	3.591474	210.45.119.62	182.254.41.37	OIDQ	89	OIDQ Protocol
181	3.631787	182.254.41.37	210.45.119.62	OIDQ	689	OIDQ Protocol

Queries  
 mit.edu: type NS, class IN  
 Name: mit.edu  
 [Name Length: 7]  
 [Label Count: 2]  
 Type: NS (authoritative Name Server) (2)  
 Class: IN (0x0001)  
 Answers  
 mit.edu: type NS, class IN, ns use5.akam.net  
 Name: mit.edu  
 Type: NS (authoritative Name Server) (2)  
 Class: IN (0x0001)  
 Time to live: 600  
 Data length: 15  
 Name Server: use5.akam.net  
 mit.edu: type NS, class IN, ns ns1-173.akam.net  
 mit.edu: type NS, class IN, ns usw2.akam.net  
 mit.edu: type NS, class IN, ns asia2.akam.net  
 mit.edu: type NS, class IN, ns eur5.akam.net

19.



20. 202.38.64.1, it's not my DNS server but the ns.ustc.edu.cn.

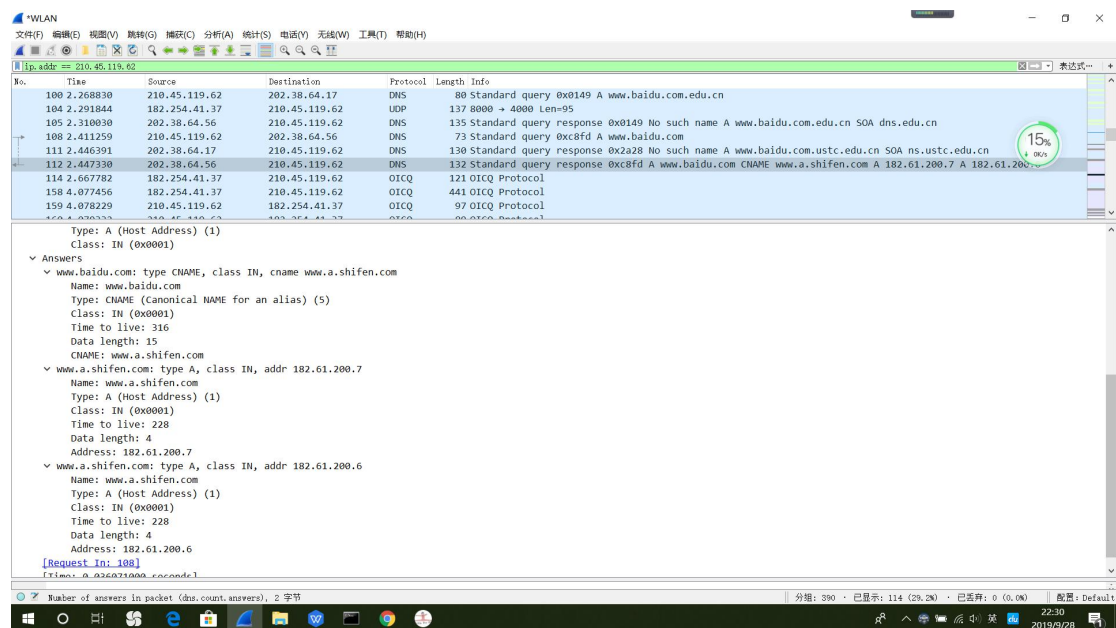
21. “Type” is IP, “answers”

```

  Answers
    www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
      Name: www.baidu.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 316
      Data length: 15
      CNAME: www.a.shifen.com
    www.a.shifen.com: type A, class IN, addr 182.61.200.7
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 228
      Data length: 4
      Address: 182.61.200.7
    www.a.shifen.com: type A, class IN, addr 182.61.200.6
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 228
      Data length: 4
      Address: 182.61.200.6

```

22.



23.