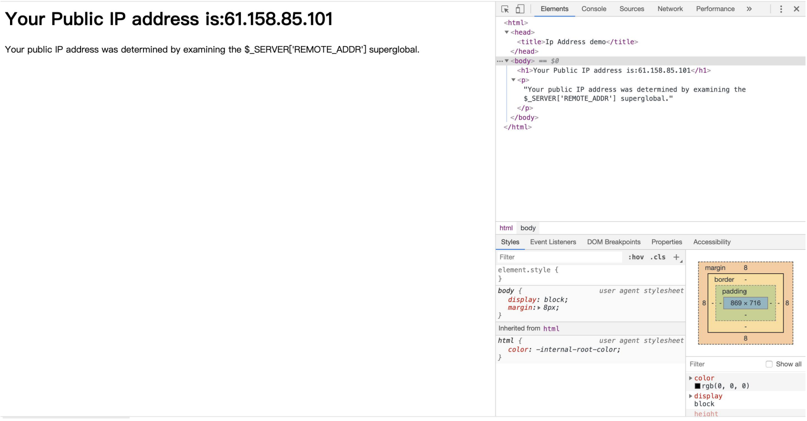
Lab0

你的 IP 地址

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether f8:ff:c2:28:04:f1
        inet6 fe80::1036:bb5f:34da:dc53%en0 prefixlen 64 secured scopeid 0x6
        inet 192.168.5.103 netmask 0xffffff00 broadcast 192.168.5.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

分析一个网页的组成部分



Your Public IP address is:61.158.85.101

Your public IP address was determined by examining the $_SERVER['REMOTE_ADDR'] superglobal.

```
<html>
▼<head>
   <title>Ip Address demo</title>
 </head>
…▼<body> == $0
   <h1>Your Public IP address is:61.158.85.101</h1>
  ▼<p>
     "Your public IP address was determined by examining the
     $_SERVER['REMOTE_ADDR'] superglobal."
   </p>
 </body>
</html>
```

```
element.style {
}
body {                          user agent stylesheet
   display: block;
   margin:▸ 8px;
}
Inherited from html
html {                          user agent stylesheet
   color: -internal-root-color;
}
```

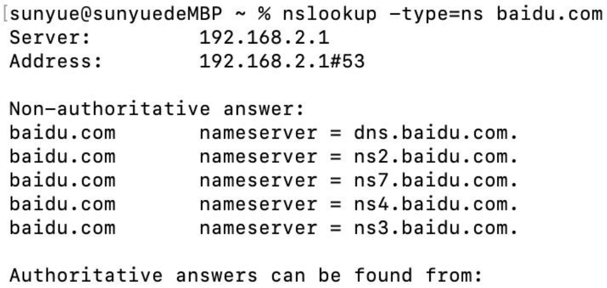
```
▸ color
  ■rgb(0, 0, 0)
▸ display
  block
  height
```

域名服务器

1.查询 baidu.com 的 A 地址记录截图;

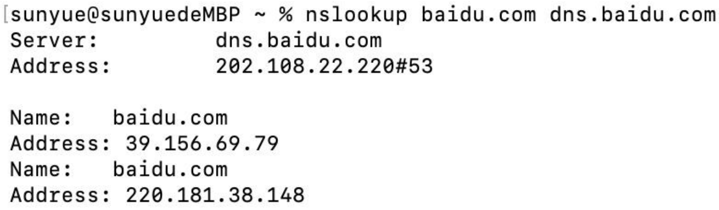
```
[sunyue@bogon learngit % nslookup baidu.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   baidu.com
Address: 220.181.38.148
Name:   baidu.com
Address: 39.156.69.79

[sunyue@bogon learngit % nslookup -type=ns baidu.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
baidu.com       nameserver = ns4.baidu.com.
baidu.com       nameserver = ns2.baidu.com.
baidu.com       nameserver = dns.baidu.com.
baidu.com       nameserver = ns7.baidu.com.
baidu.com       nameserver = ns3.baidu.com.

Authoritative answers can be found from:

[sunyue@bogon learngit % nslookup baidu.com ns4.baidu.com
Server:         ns4.baidu.com
Address:        14.215.178.80#53

Name:   baidu.com
Address: 220.181.38.148
Name:   baidu.com
Address: 39.156.69.79

[sunyue@bogon learngit % nslookup 114.114.114.114
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
114.114.114.114.in-addr.arpa    name = public1.114dns.com.

Authoritative answers can be found from:
```

2.查询 baidu.com 的 域名服务器截图；



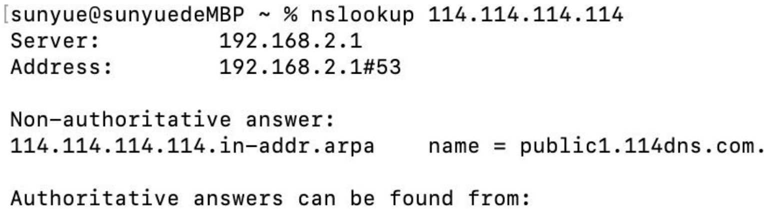
```
sunyue@sunyuedeMBP ~ % nslookup -type=ns baidu.com
Server:         192.168.2.1
Address:        192.168.2.1#53

Non-authoritative answer:
baidu.com       nameserver = dns.baidu.com.
baidu.com       nameserver = ns2.baidu.com.
baidu.com       nameserver = ns7.baidu.com.
baidu.com       nameserver = ns4.baidu.com.
baidu.com       nameserver = ns3.baidu.com.

Authoritative answers can be found from:
```

3.使用授权服务器查询 baidu.com 的 IP 地址的截图；



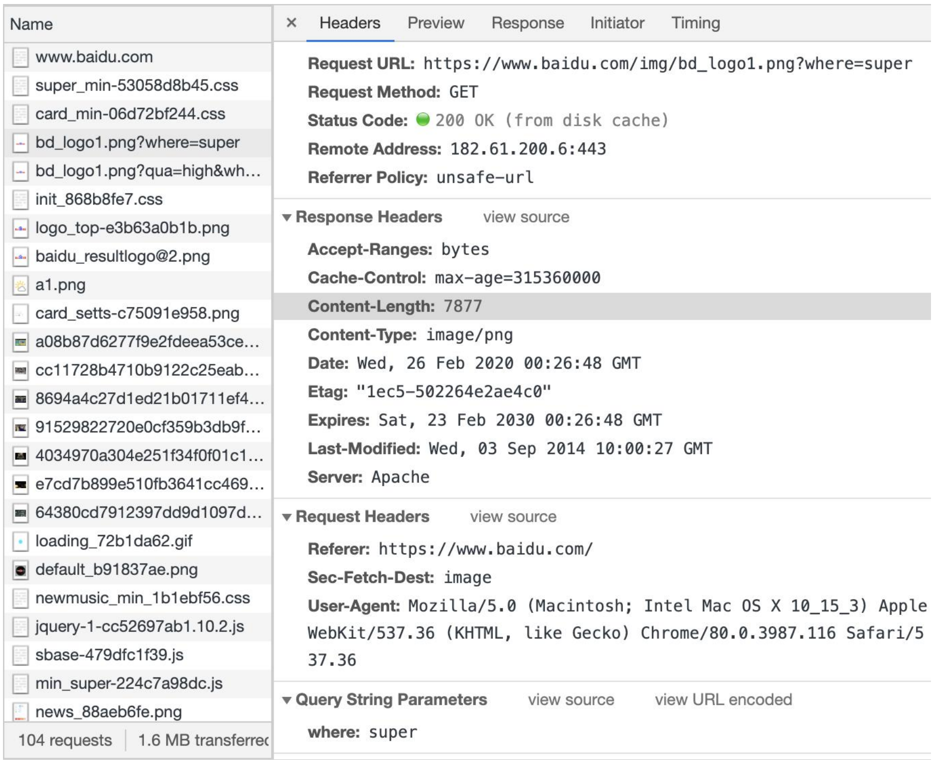
```
sunyue@sunyuedeMBP ~ % nslookup baidu.com dns.baidu.com
Server:         dns.baidu.com
Address:        202.108.22.220#53

Name:   baidu.com
Address: 39.156.69.79
Name:   baidu.com
Address: 220.181.38.148
```

3.查询 114.114.114.114 匹配的主机名的截图。



```
sunyue@sunyuedeMBP ~ % nslookup 114.114.114.114
Server:         192.168.2.1
Address:        192.168.2.1#53

Non-authoritative answer:
114.114.114.114.in-addr.arpa    name = public1.114dns.com.

Authoritative answers can be found from:
```

观察 HTTP 标头 (HTTP headers)



www.baidu.com
super_min-53058d8b45.css
card_min-06d72bf244.css
bd_logo1.png?where=super
bd_logo1.png?qua=high&wh…
init_868b8fe7.css
logo_top-e3b63a0b1b.png
baidu_resultlogo@2.png
a1.png
card_setts-c75091e958.png
a08b87d6277f9e2fdeea53ce…
cc11728b4710b9122c25eab…
8694a4c27d1ed21b01711ef4…
91529822720e0cf359b3db9f…
4034970a304e251f34f0f01c1…
e7cd7b899e510fb3641cc469…
64380cd7912397dd9d1097d…
loading_72b1da62.gif
default_b91837ae.png
newmusic_min_1b1ebf56.css
jquery-1-cc52697ab1.10.2.js
sbase-479dfc1f39.js
min_super-224c7a98dc.js
news_88aeb6fe.png

104 requests | 1.6 MB transferrec

Request URL: https://www.baidu.com/img/bd_logo1.png?where=super
Request Method: GET
Status Code: ● 200 OK (from disk cache)
Remote Address: 182.61.200.6:443
Referrer Policy: unsafe-url

▾ **Response Headers** view source

Accept-Ranges: bytes
Cache-Control: max-age=315360000
Content-Length: 7877
Content-Type: image/png
Date: Wed, 26 Feb 2020 00:26:48 GMT
Etag: "1ec5-502264e2ae4c0"
Expires: Sat, 23 Feb 2030 00:26:48 GMT
Last-Modified: Wed, 03 Sep 2014 10:00:27 GMT
Server: Apache

▾ **Request Headers** view source

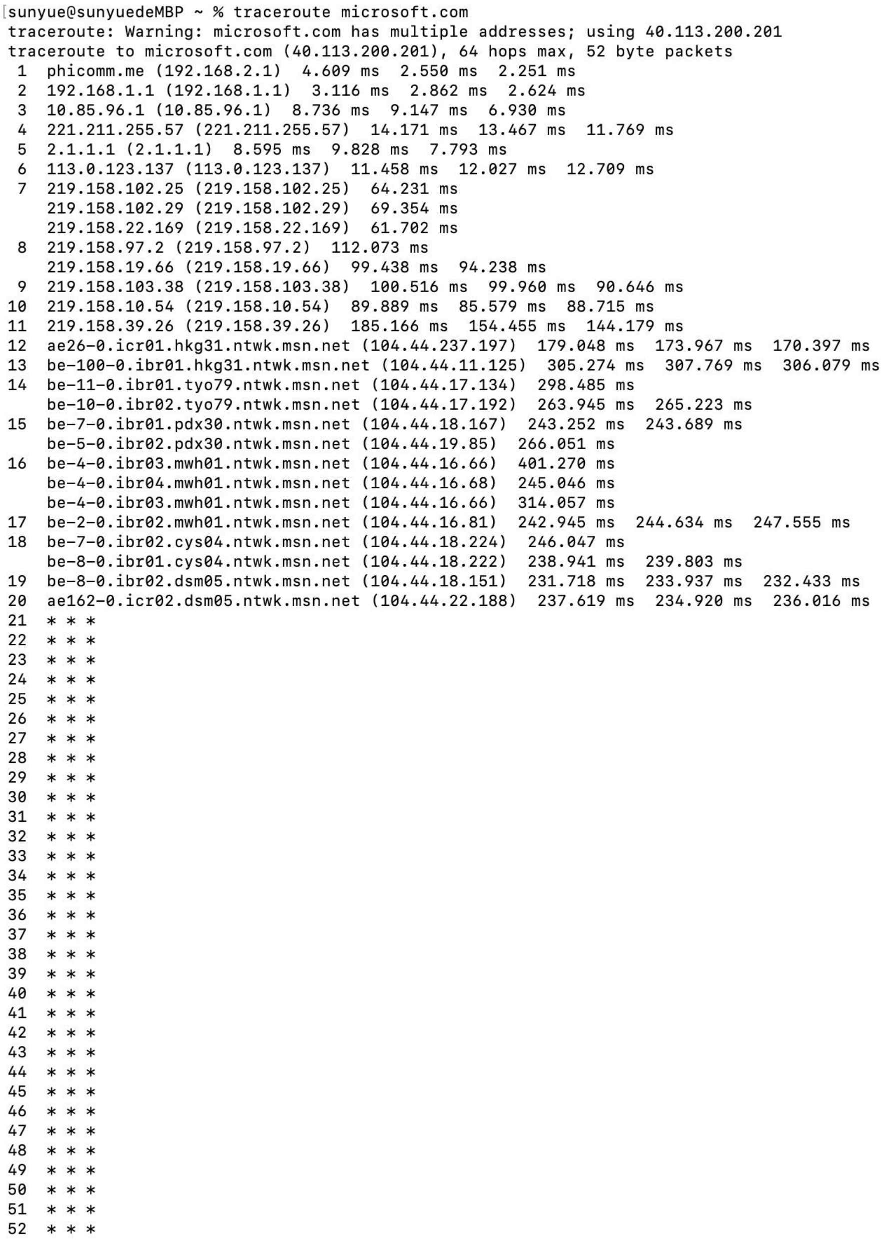
Referer: https://www.baidu.com/
Sec-Fetch-Dest: image
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.116 Safari/537.36

▾ **Query String Parameters** view source view URL encoded

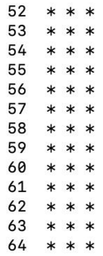
where: super

追踪数据包 (Tracing a packet)

1.跟踪一个从你的计算机发往 microsoft.com 的数据包，并截图。

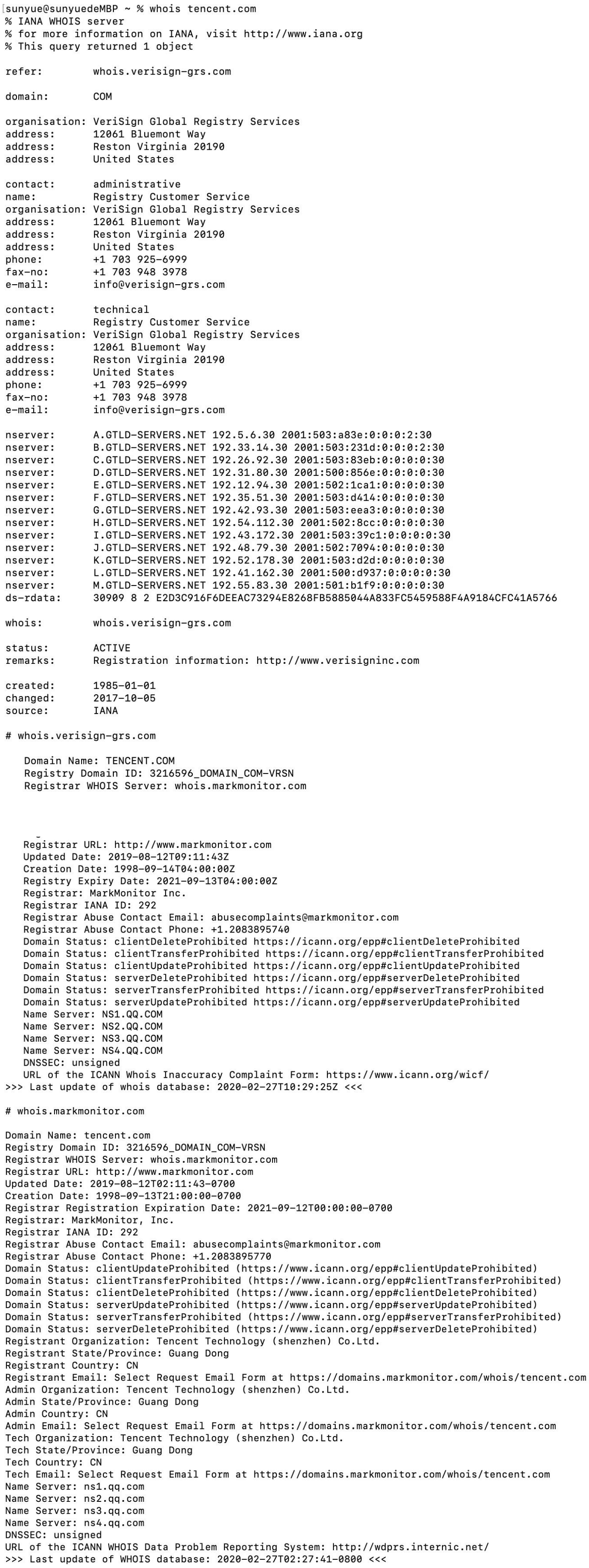


```
[sunyue@sunyuedeMBP ~ % traceroute microsoft.com
 traceroute: Warning: microsoft.com has multiple addresses; using 40.113.200.201
 traceroute to microsoft.com (40.113.200.201), 64 hops max, 52 byte packets
  1  phicomm.me (192.168.2.1)  4.609 ms  2.550 ms  2.251 ms
  2  192.168.1.1 (192.168.1.1)  3.116 ms  2.862 ms  2.624 ms
  3  10.85.96.1 (10.85.96.1)  8.736 ms  9.147 ms  6.930 ms
  4  221.211.255.57 (221.211.255.57)  14.171 ms  13.467 ms  11.769 ms
  5  2.1.1.1 (2.1.1.1)  8.595 ms  9.828 ms  7.793 ms
  6  113.0.123.137 (113.0.123.137)  11.458 ms  12.027 ms  12.709 ms
  7  219.158.102.25 (219.158.102.25)  64.231 ms
     219.158.102.29 (219.158.102.29)  69.354 ms
     219.158.22.169 (219.158.22.169)  61.702 ms
  8  219.158.97.2 (219.158.97.2)  112.073 ms
     219.158.19.66 (219.158.19.66)  99.438 ms  94.238 ms
  9  219.158.103.38 (219.158.103.38)  100.516 ms  99.960 ms  90.646 ms
 10  219.158.10.54 (219.158.10.54)  89.889 ms  85.579 ms  88.715 ms
 11  219.158.39.26 (219.158.39.26)  185.166 ms  154.455 ms  144.179 ms
 12  ae26-0.icr01.hkg31.ntwk.msn.net (104.44.237.197)  179.048 ms  173.967 ms  170.397 ms
 13  be-100-0.ibr01.hkg31.ntwk.msn.net (104.44.11.125)  305.274 ms  307.769 ms  306.079 ms
 14  be-11-0.ibr01.tyo79.ntwk.msn.net (104.44.17.134)  298.485 ms
     be-10-0.ibr02.tyo79.ntwk.msn.net (104.44.17.192)  263.945 ms  265.223 ms
 15  be-7-0.ibr01.pdx30.ntwk.msn.net (104.44.18.167)  243.252 ms  243.689 ms
     be-5-0.ibr02.pdx30.ntwk.msn.net (104.44.19.85)  266.051 ms
 16  be-4-0.ibr03.mwh01.ntwk.msn.net (104.44.16.66)  401.270 ms
     be-4-0.ibr04.mwh01.ntwk.msn.net (104.44.16.68)  245.046 ms
     be-4-0.ibr03.mwh01.ntwk.msn.net (104.44.16.66)  314.057 ms
 17  be-2-0.ibr02.mwh01.ntwk.msn.net (104.44.16.81)  242.945 ms  244.634 ms  247.555 ms
 18  be-7-0.ibr02.cys04.ntwk.msn.net (104.44.18.224)  246.047 ms
     be-8-0.ibr01.cys04.ntwk.msn.net (104.44.18.222)  238.941 ms  239.803 ms
 19  be-8-0.ibr02.dsm05.ntwk.msn.net (104.44.18.151)  231.718 ms  233.937 ms  232.433 ms
 20  ae162-0.icr02.dsm05.ntwk.msn.net (104.44.22.188)  237.619 ms  234.920 ms  236.016 ms
 21  * * *
 22  * * *
 23  * * *
 24  * * *
 25  * * *
 26  * * *
 27  * * *
 28  * * *
 29  * * *
 30  * * *
 31  * * *
 32  * * *
 33  * * *
 34  * * *
 35  * * *
 36  * * *
 37  * * *
 38  * * *
 39  * * *
 40  * * *
 41  * * *
 42  * * *
 43  * * *
 44  * * *
 45  * * *
 46  * * *
 47  * * *
 48  * * *
 49  * * *
 50  * * *
 51  * * *
 52  * * *
```



```
 52  * * *
 53  * * *
 54  * * *
 55  * * *
 56  * * *
 57  * * *
 58  * * *
 59  * * *
 60  * * *
 61  * * *
 62  * * *
 63  * * *
 64  * * *
```

2.利用 whois 查询 tencent.com 的相关信息，并截图 (网页或命令行都需要所有相关



```
[sunyue@sunyuedeMBP ~ % whois tencent.com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.verisign-grs.com

domain:       COM

organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States

contact:      administrative
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

contact:      technical
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

nserver:      A.GTLD-SERVERS.NET 192.5.6.30 2001:503:a83e:0:0:0:2:30
nserver:      B.GTLD-SERVERS.NET 192.33.14.30 2001:503:231d:0:0:0:2:30
nserver:      C.GTLD-SERVERS.NET 192.26.92.30 2001:503:83eb:0:0:0:0:30
nserver:      D.GTLD-SERVERS.NET 192.31.80.30 2001:500:856e:0:0:0:0:30
nserver:      E.GTLD-SERVERS.NET 192.12.94.30 2001:502:1ca1:0:0:0:0:30
nserver:      F.GTLD-SERVERS.NET 192.35.51.30 2001:503:d414:0:0:0:0:30
nserver:      G.GTLD-SERVERS.NET 192.42.93.30 2001:503:eea3:0:0:0:0:30
nserver:      H.GTLD-SERVERS.NET 192.54.112.30 2001:502:8cc:0:0:0:0:30
nserver:      I.GTLD-SERVERS.NET 192.43.172.30 2001:503:39c1:0:0:0:0:30
nserver:      J.GTLD-SERVERS.NET 192.48.79.30 2001:502:7094:0:0:0:0:30
nserver:      K.GTLD-SERVERS.NET 192.52.178.30 2001:503:d2d:0:0:0:0:30
nserver:      L.GTLD-SERVERS.NET 192.41.162.30 2001:500:d937:0:0:0:0:30
nserver:      M.GTLD-SERVERS.NET 192.55.83.30 2001:501:b1f9:0:0:0:0:30
ds-rdata:     30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CFC41A5766

whois:        whois.verisign-grs.com

status:       ACTIVE
remarks:      Registration information: http://www.verisigninc.com

created:      1985-01-01
changed:      2017-10-05
source:       IANA

# whois.verisign-grs.com

   Domain Name: TENCENT.COM
   Registry Domain ID: 3216596_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com



   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-08-12T09:11:43Z
   Creation Date: 1998-09-14T04:00:00Z
   Registry Expiry Date: 2021-09-13T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.QQ.COM
   Name Server: NS2.QQ.COM
   Name Server: NS3.QQ.COM
   Name Server: NS4.QQ.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-02-27T10:29:25Z <<<

# whois.markmonitor.com

Domain Name: tencent.com
Registry Domain ID: 3216596_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-08-12T02:11:43-0700
Creation Date: 1998-09-13T21:00:00-0700
Registrar Registration Expiration Date: 2021-09-12T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Tencent Technology (shenzhen) Co.Ltd.
Registrant State/Province: Guang Dong
Registrant Country: CN
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/tencent.com
Admin Organization: Tencent Technology (shenzhen) Co.Ltd.
Admin State/Province: Guang Dong
Admin Country: CN
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/tencent.com
Tech Organization: Tencent Technology (shenzhen) Co.Ltd.
Tech State/Province: Guang Dong
Tech Country: CN
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/tencent.com
Name Server: ns1.qq.com
Name Server: ns2.qq.com
Name Server: ns3.qq.com
Name Server: ns4.qq.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-02-27T02:27:41-0800 <<<
```