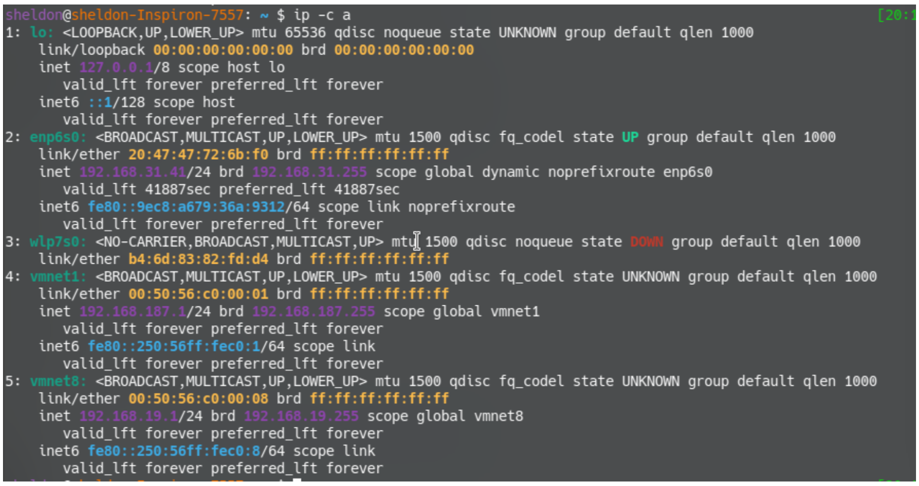
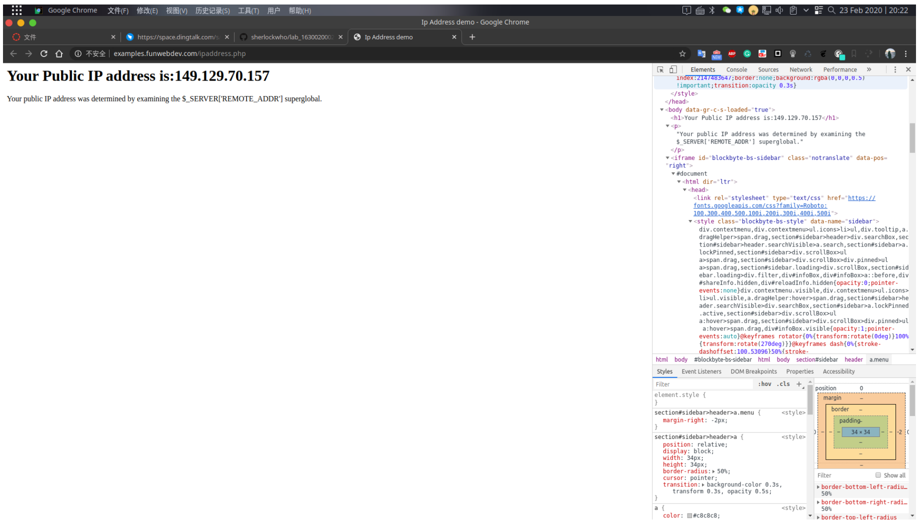
16300200027_lab0

IP地址



```
sheldon@sheldon-Inspiron-7557: ~ $ ip -c a                                                                    [20:1
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp6s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 20:47:47:72:6b:f0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.31.41/24 brd 192.168.31.255 scope global dynamic noprefixroute enp6s0
       valid_lft 41887sec preferred_lft 41887sec
    inet6 fe80::9ec8:a679:36a:9312/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: wlp7s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether b4:6d:83:82:fd:d4 brd ff:ff:ff:ff:ff:ff
4: vmnet1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:50:56:c0:00:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.187.1/24 brd 192.168.187.255 scope global vmnet1
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fec0:1/64 scope link
       valid_lft forever preferred_lft forever
5: vmnet8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:50:56:c0:00:08 brd ff:ff:ff:ff:ff:ff
    inet 192.168.19.1/24 brd 192.168.19.255 scope global vmnet8
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fec0:8/64 scope link
       valid_lft forever preferred_lft forever
```

分析网页组成部分



Your Public IP address is:149.129.70.157

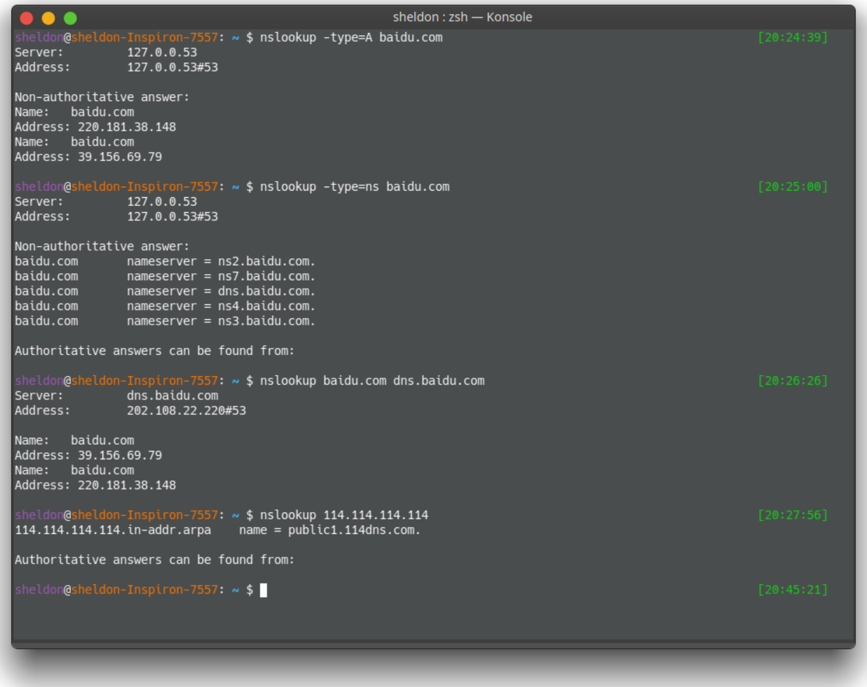
Your public IP address was determined by examining the $_SERVER['REMOTE_ADDR'] superglobal.

```
      index:2147483647;border:none;background:rgba(0,0,0,0.5)
      !important;transition:opacity 0.3s}
    </style>
  </head>
▼<body data-gr-c-s-loaded="true">
    <h1>Your Public IP address is:149.129.70.157</h1>
  ▼<p>
      "Your public IP address was determined by examining the
      $_SERVER['REMOTE_ADDR'] superglobal."
    </p>
  ▼<iframe id="blockbyte-bs-sidebar" class="notranslate" data-pos=
  "right">
    ▼#document
      ▼<html dir="ltr">
        ▼<head>
            <link rel="stylesheet" type="text/css" href="https://
            fonts.googleapis.com/css?family=Roboto:
            100,300,400,500,100i,200i,300i,400i,500i">
          ▼<style class="blockbyte-bs-style" data-name="sidebar">
              div.contextmenu,div.contextmenu>ul.icons>li>ul,div.tooltip,a.
              dragHelper>span.drag,section#sidebar>header>div.searchBox,sec
              tion#sidebar>header.searchVisible>a.search,section#sidebar>a.
              lockPinned,section#sidebar>div.scrollBox>ul
              a>span.drag,section#sidebar>div.scrollBox>div.pinned>ul
              a>span.drag,section#sidebar.loading>div.scrollBox,section#sid
              ebar.loading>div.filter,div#infoBox,div#infoBox>a::before,div
              #shareInfo.hidden,div#reloadInfo.hidden{opacity:0;pointer-
              events:none}div.contextmenu.visible,div.contextmenu>ul.icons>
              li>ul.visible,a.dragHelper:hover>span.drag,section#sidebar>he
              ader.searchVisible>div.searchBox,section#sidebar>a.lockPinned
              .active,section#sidebar>div.scrollBox>ul
              a:hover>span.drag,section#sidebar>div.scrollBox>div.pinned>ul
               a:hover>span.drag,div#infoBox.visible{opacity:1;pointer-
              events:auto}@keyframes rotator{0%{transform:rotate(0deg)}100%
              {transform:rotate(270deg)}}@keyframes dash{0%{stroke-
              dashoffset:100.53096}50%{stroke-

html  body  #blockbyte-bs-sidebar  html  body  section#sidebar  header  a.menu
```

```
element.style {
}
section#sidebar>header>a.menu {                    <style>
  margin-right: -2px;
}
section#sidebar>header>a {                         <style>
  position: relative;
  display: block;
  width: 34px;
  height: 34px;
  border-radius: ▸ 50%;
  cursor: pointer;
  transition: ▸ background-color 0.3s,
     transform 0.3s, opacity 0.5s;
}
a {                                                <style>
  color: ■#c8c8c8;
```

```
position        0
▸ border-bottom-left-radiu…
  50%
▸ border-bottom-right-radi…
  50%
▸ border-top-left-radius
```

域名服务器



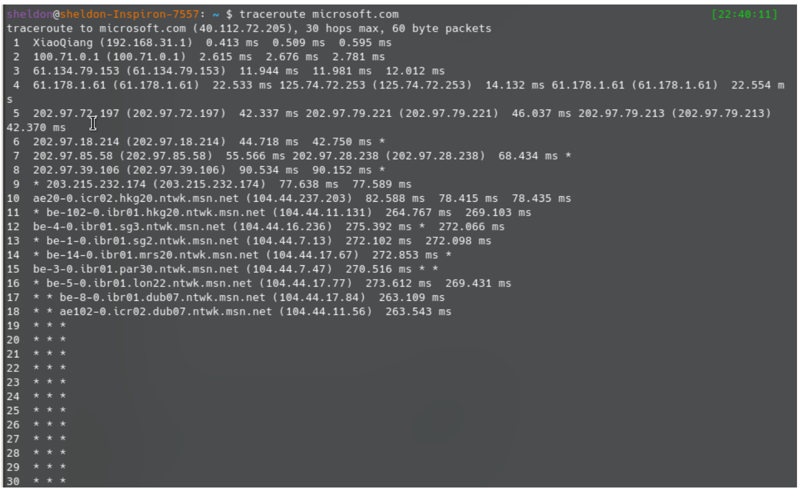
```
sheldon@sheldon-Inspiron-7557: ~ $ nslookup -type=A baidu.com                                     [20:24:39]
Server:         127.0.0.53
Address:        127.0.0.53#53

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

sheldon@sheldon-Inspiron-7557: ~ $ nslookup -type=ns baidu.com                                    [20:25:00]
Server:         127.0.0.53
Address:        127.0.0.53#53

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

Authoritative answers can be found from:

sheldon@sheldon-Inspiron-7557: ~ $ nslookup baidu.com dns.baidu.com                               [20:26:26]
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

sheldon@sheldon-Inspiron-7557: ~ $ nslookup 114.114.114.114                                       [20:27:56]
114.114.114.114.in-addr.arpa    name = public1.114dns.com.

Authoritative answers can be found from:

sheldon@sheldon-Inspiron-7557: ~ $                                                                [20:45:21]
```

观察http标头

User-Agent: `Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.116 Safari/537.36`

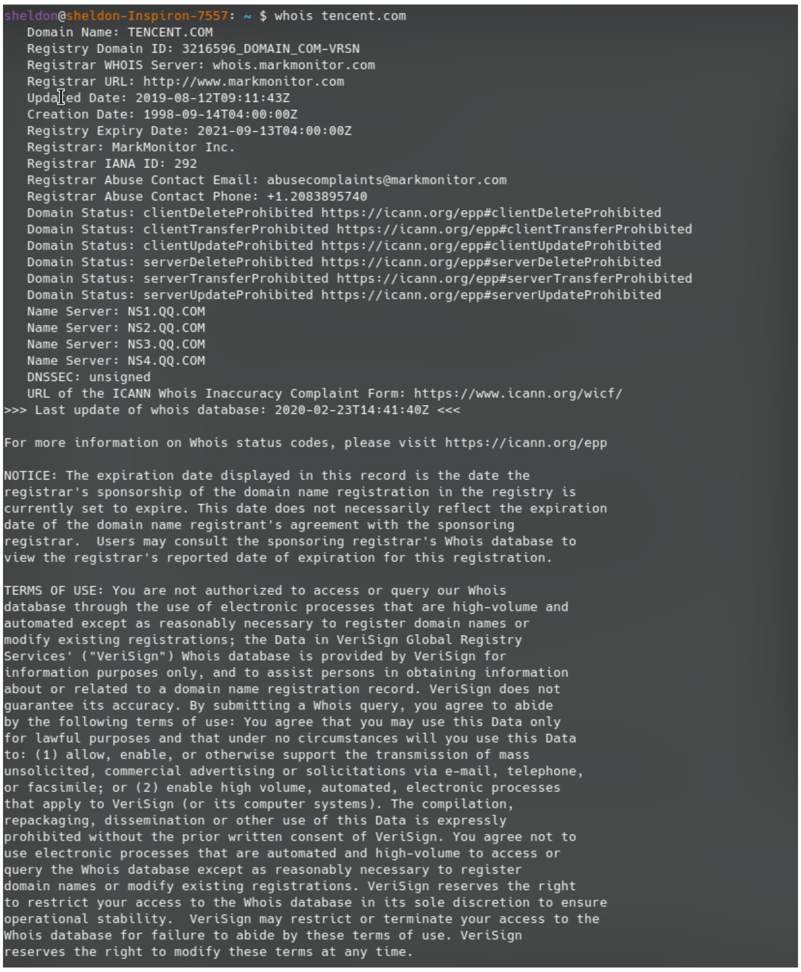
追踪数据包

1. 追踪microsoft.com

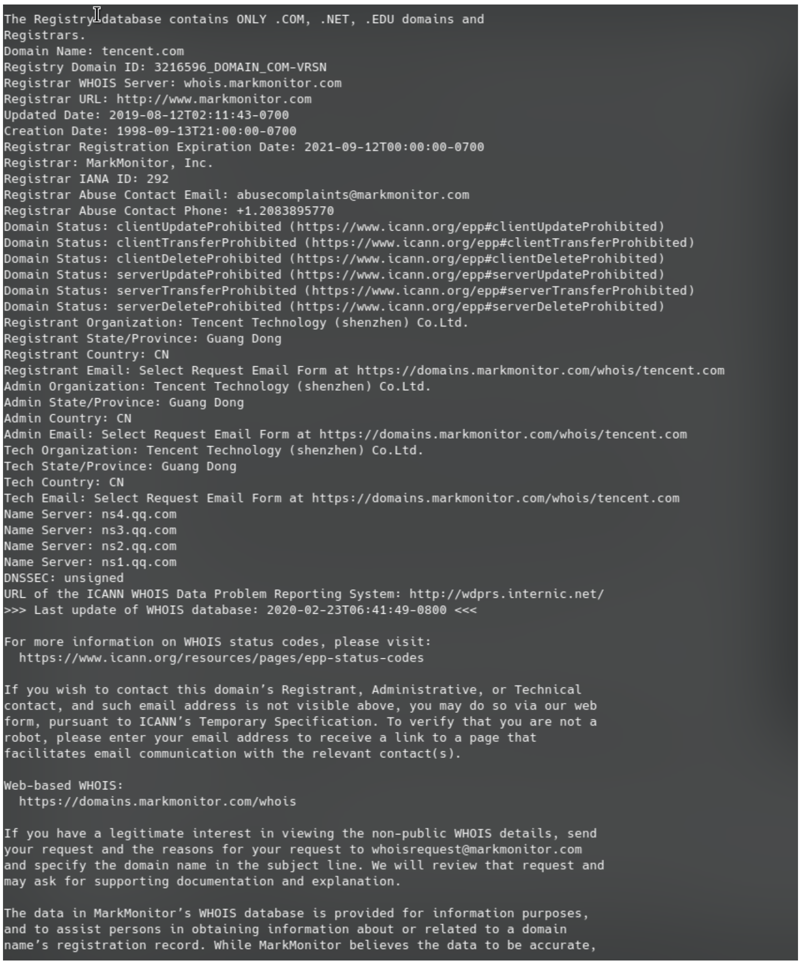


```
sheldon@sheldon-Inspiron-7557: ~ $ traceroute microsoft.com                                                        [22:40:11]
traceroute to microsoft.com (40.112.72.205), 30 hops max, 60 byte packets
 1  XiaoQiang (192.168.31.1)  0.413 ms  0.509 ms  0.595 ms
 2  100.71.0.1 (100.71.0.1)  2.615 ms  2.676 ms  2.781 ms
 3  61.134.79.153 (61.134.79.153)  11.944 ms  11.981 ms  12.012 ms
 4  61.178.1.61 (61.178.1.61)  22.533 ms 125.74.72.253 (125.74.72.253)  14.132 ms 61.178.1.61 (61.178.1.61)  22.554 m
s
 5  202.97.72.197 (202.97.72.197)  42.337 ms 202.97.79.221 (202.97.79.221)  46.037 ms 202.97.79.213 (202.97.79.213)
42.370 ms
 6  202.97.18.214 (202.97.18.214)  44.718 ms  42.750 ms *
 7  202.97.85.58 (202.97.85.58)  55.566 ms 202.97.28.238 (202.97.28.238)  68.434 ms *
 8  202.97.39.106 (202.97.39.106)  90.534 ms  90.152 ms *
 9  * 203.215.232.174 (203.215.232.174)  77.638 ms  77.589 ms
10  ae20-0.icr02.hkg20.ntwk.msn.net (104.44.237.203)  82.588 ms  78.415 ms  78.435 ms
11  * be-102-0.ibr01.hkg20.ntwk.msn.net (104.44.11.131)  264.767 ms  269.103 ms
12  be-4-0.ibr01.sg3.ntwk.msn.net (104.44.16.236)  275.392 ms *  272.066 ms
13  * be-1-0.ibr01.sg2.ntwk.msn.net (104.44.7.13)  272.102 ms  272.098 ms
14  * be-14-0.ibr01.mrs20.ntwk.msn.net (104.44.17.67)  272.853 ms *
15  be-3-0.ibr01.par30.ntwk.msn.net (104.44.7.47)  270.516 ms * *
16  * be-5-0.ibr01.lon22.ntwk.msn.net (104.44.17.77)  273.612 ms  269.431 ms
17  * * be-8-0.ibr01.dub07.ntwk.msn.net (104.44.17.84)  263.109 ms
18  * * ae102-0.icr02.dub07.ntwk.msn.net (104.44.11.56)  263.543 ms
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

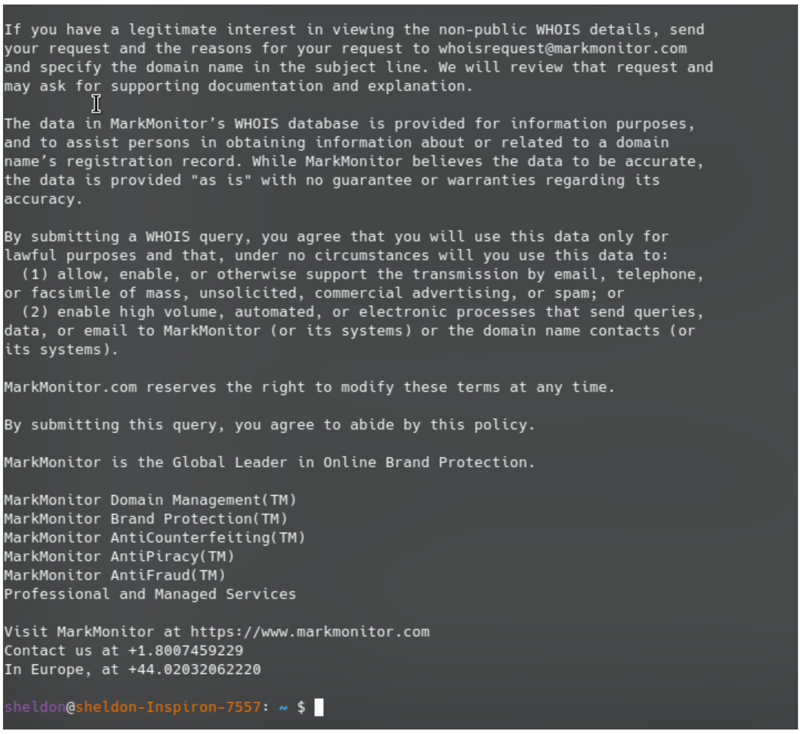
2. whois tencent.com



```
sheldon@sheldon-Inspiron-7557: ~ $ whois tencent.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: 2020-02-23T14:41:40Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.
```



```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
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: ns4.qq.com
Name Server: ns3.qq.com
Name Server: ns2.qq.com
Name Server: ns1.qq.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-02-23T06:41:49-0800 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain’s Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN’s Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor’s WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name’s registration record. While MarkMonitor believes the data to be accurate,
```



```
If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor’s WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name’s registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
  (1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
  (2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).

MarkMonitor.com reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor is the Global Leader in Online Brand Protection.

MarkMonitor Domain Management(TM)
MarkMonitor Brand Protection(TM)
MarkMonitor AntiCounterfeiting(TM)
MarkMonitor AntiPiracy(TM)
MarkMonitor AntiFraud(TM)
Professional and Managed Services

Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220

sheldon@sheldon-Inspiron-7557: ~ $
```