

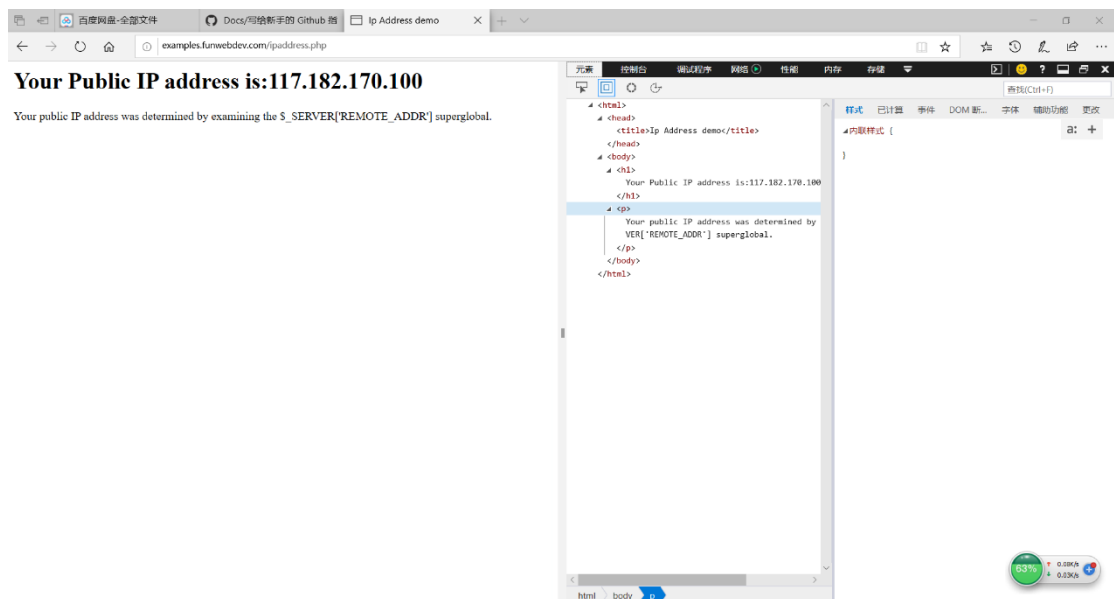
Lab0

1.我的 IP 地址

无线局域网适配器 WLAN:

```
连接特定的 DNS 后缀 . . . . . : bbrouter
IPv6 地址 . . . . . : 2409:8a5c:1018:9b10:f9f1:125f:acc3:695d
临时 IPv6 地址. . . . . : 2409:8a5c:1018:9b10:ad1a:ef7a:3c0c:234d
本地链接 IPv6 地址. . . . . : fe80::f9f1:125f:acc3:695d%3
IPv4 地址 . . . . . : 192.168.1.6
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : fe80::1%3
                  192.168.1.1
```

2.分析一个网页的组成部分（Microsoft Edge）



3. 1) baidu.com 的 A 地址记录

```
PS C:\Users\86159> nslookup baidu.com
服务器:  YHTC_GW.bbrouter
Address:  192.168.1.1

非权威应答:
名称:     baidu.com.bbrouter
Address:  218.204.57.254
```

2) baidu.com 的域名服务器

```
PS C:\Users\86159> nslookup -qt=ns baidu.com
服务器:  YHTC_GW.bbrouter
Address:  192.168.1.1

非权威应答:
baidu.com      nameserver = ns4.baidu.com
baidu.com      nameserver = ns7.baidu.com
baidu.com      nameserver = ns2.baidu.com
baidu.com      nameserver = ns3.baidu.com
baidu.com      nameserver = dns.baidu.com
```

3) 使用授权服务器查询 baidu.com 的 IP 地址

```
PS C:\Users\86159> nslookup baidu.com ns4.baidu.com
服务器:  UnKnown
Address:  14.215.178.80

名称:     baidu.com
Addresses: 39.156.69.79
          220.181.38.148
```

```
PS C:\Users\86159> nslookup baidu.com ns7.baidu.com
服务器:  UnKnown
Address:  180.76.76.92
```

```
DNS request timed out.
    timeout was 2 seconds.
名称:     baidu.com
Addresses: 220.181.38.148
          39.156.69.79
```

```
PS C:\Users\86159> nslookup baidu.com ns3.baidu.com
服务器:  UnKnown
Address:  112.80.248.64
```

```
名称:     baidu.com
Addresses: 39.156.69.79
          220.181.38.148
```

```
PS C:\Users\86159> nslookup baidu.com dns.baidu.com
服务器:  UnKnown
Address:  202.108.22.220
```

```
名称:     baidu.com
Addresses: 39.156.69.79
          220.181.38.148
```

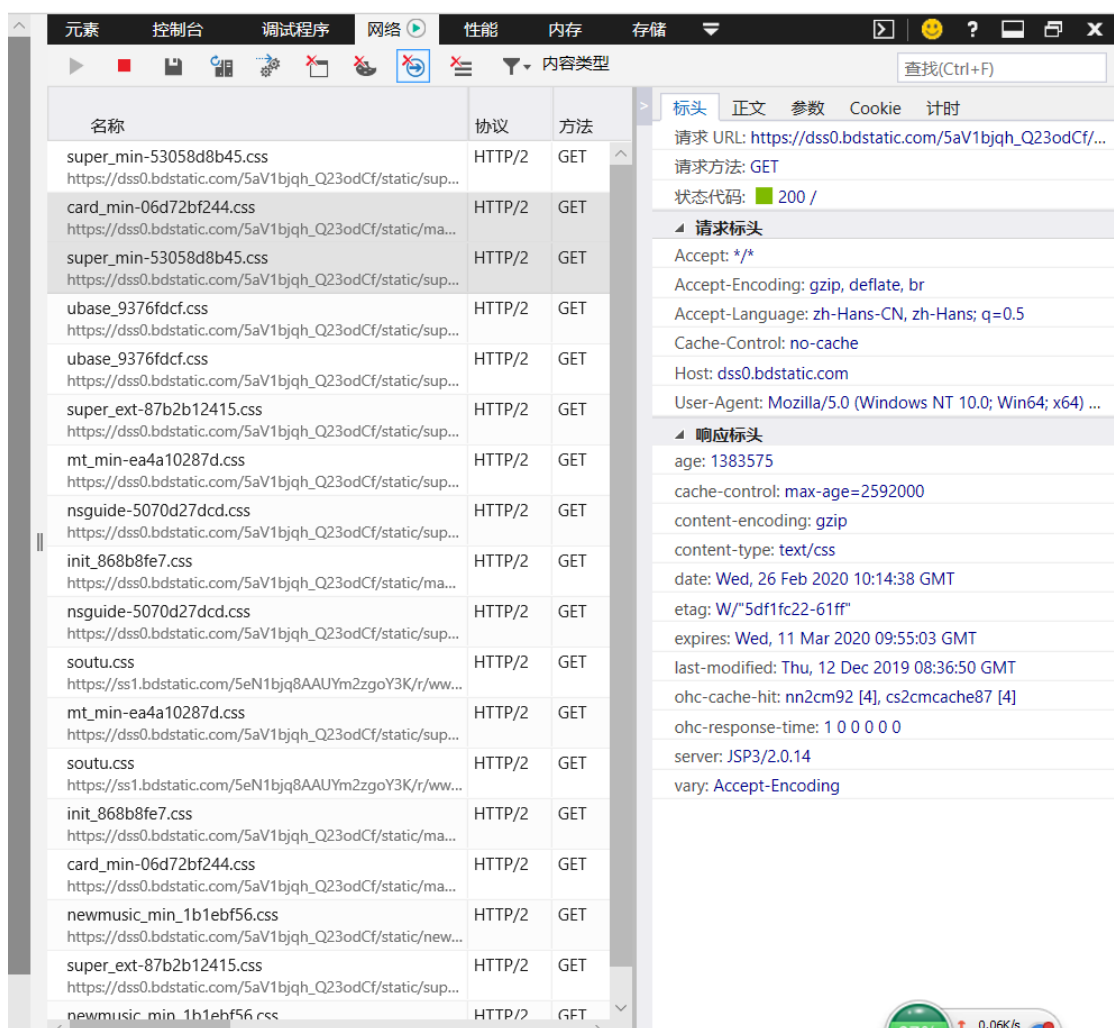
4) 查询 114.114.114.114 匹配的主机名

```
PS C:\Users\86159> nslookup 114.114.114.114
服务器:  nsc0.gxnnptt.net.cn
Address:  202.103.224.68

名称:     public1.114dns.com
Address:  114.114.114.114

PS C:\Users\86159>
```

4.观察 HTTP 的标头



The screenshot shows the Network tab in a web browser's developer tools. The left pane lists several CSS files being loaded via HTTP GET requests. The right pane shows the 'Headers' tab for the selected request, displaying request and response headers.

名称	协议	方法
super_min-53058d8b45.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/sup...	HTTP/2	GET
card_min-06d72bf244.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/ma...	HTTP/2	GET
super_min-53058d8b45.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/sup...	HTTP/2	GET
ubase_9376fddf.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/sup...	HTTP/2	GET
ubase_9376fddf.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/sup...	HTTP/2	GET
super_ext-87b2b12415.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/sup...	HTTP/2	GET
mt_min-ea4a10287d.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/sup...	HTTP/2	GET
nsguide-5070d27dcd.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/sup...	HTTP/2	GET
init_868b8fe7.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/ma...	HTTP/2	GET
nsguide-5070d27dcd.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/sup...	HTTP/2	GET
soutu.css https://ss1.bdstatic.com/5eN1bjq8AAUym2zgoY3K/r/ww...	HTTP/2	GET
mt_min-ea4a10287d.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/sup...	HTTP/2	GET
soutu.css https://ss1.bdstatic.com/5eN1bjq8AAUym2zgoY3K/r/ww...	HTTP/2	GET
init_868b8fe7.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/ma...	HTTP/2	GET
card_min-06d72bf244.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/ma...	HTTP/2	GET
newmusic_min_1b1ebf56.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/new...	HTTP/2	GET
super_ext-87b2b12415.css https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/static/sup...	HTTP/2	GET
newmusic_min_1h1ebf56.css	HTTP/2	GET

请求标头

- 请求 URL: https://dss0.bdstatic.com/5aV1bjqh_Q23odCf/...
- 请求方法: GET
- 状态代码: 200 /

响应标头

- age: 1383575
- cache-control: max-age=2592000
- content-encoding: gzip
- content-type: text/css
- date: Wed, 26 Feb 2020 10:14:38 GMT
- etag: W/"5df1fc22-61ff"
- expires: Wed, 11 Mar 2020 09:55:03 GMT
- last-modified: Thu, 12 Dec 2019 08:36:50 GMT
- ohc-cache-hit: nn2cm92 [4], cs2cmcache87 [4]
- ohc-response-time: 1 0 0 0 0
- server: JSP3/2.0.14
- vary: Accept-Encoding

5.追踪数据包

1) 跟踪一个从我的计算机发往 *microsoft.com* 的数据包

(抱歉, 多次尝试但是还是存在超时现象, 以下是超时最少的情况)

```
PS C:\Users\86159> tracert microsoft.com

通过最多 30 个跃点跟踪
到 microsoft.com [40.76.4.15] 的路由:

  1  1116 ms      1 ms      1 ms  YHTC_GW.bbrouter [192.168.1.1]
  2      3 ms      3 ms     10 ms  10.88.0.1
  3     14 ms      9 ms      7 ms  221.180.70.121
  4     11 ms      9 ms      7 ms  218.204.2.57
  5      8 ms      7 ms      7 ms  218.204.2.10
  6      9 ms      7 ms      8 ms  221.183.19.89
  7     17 ms     20 ms     17 ms  221.183.11.33
  8     24 ms     18 ms     17 ms  221.176.24.158
  9     50 ms      *        53 ms  221.176.24.58
 10     75 ms      *        58 ms  221.183.30.146
 11     56 ms     62 ms     57 ms  223.118.2.202
 12     87 ms     83 ms     89 ms  223.119.0.174
 13    144 ms    212 ms    321 ms  ae26-0.icr01.hkg31.ntwk.msn.net [104.44.237.197]
 14    513 ms    609 ms    406 ms  be-120-0.ibr02.hkg31.ntwk.msn.net [104.44.11.141]
 15    324 ms    404 ms      *    be-10-0.ibr02.tyo79.ntwk.msn.net [104.44.17.192]
 16    363 ms      *      *    be-6-0.ibr02.tyo30.ntwk.msn.net [104.44.17.183]
 17    391 ms      *    324 ms  be-9-0.ibr02.lax30.ntwk.msn.net [104.44.18.43]
 18    350 ms    303 ms    302 ms  be-8-0.ibr02.sn1.ntwk.msn.net [104.44.17.74]
 19    368 ms    303 ms      *    be-3-0.ibr02.atl30.ntwk.msn.net [104.44.19.114]
 20    333 ms    404 ms    405 ms  be-6-0.ibr02.bn6.ntwk.msn.net [104.44.17.232]
 21    341 ms    303 ms    301 ms  be-2-0.ibr04.bl20.ntwk.msn.net [104.44.19.153]
 22      *      381 ms    303 ms  ae160-0.icr01.bl20.ntwk.msn.net [104.44.22.210]
 23      *      *      *    请求超时。
 24      *      *      *    请求超时。
 25      *      *      *    请求超时。
 26      *      *      *    请求超时。
 27      *      *      *    请求超时。
 28      *      *      *    请求超时。
 29      *      *      *    请求超时。
 30      *      *      *    请求超时。

跟踪完成。
```

2) 利用 whois 查询 tencent.com 的相关信息

Whois Identity for everyone

tencentL.com WHOIS

DOMAINS WEBSITE CLOUD HOSTING SERVERS EMAIL SECURITY WHOIS SUPPORT LOGIN

tencent.com Updated 17 hours ago

Domain Information

Domain:	tencent.com
Registrar:	MarkMonitor Inc.
Registered On:	1998-01-14 屏蔽右键 Ctrl + Alt + A
Expires On:	2021-01-12 屏蔽右键 Ctrl + Alt + O
Updated On:	2019-01-12 屏蔽右键 Ctrl + Alt + S
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.qq.com ns2.qq.com ns3.qq.com ns4.qq.com

Registrant Contact

100% 100% 100% 100%

Registrant Contact

Organization:	Tencent Technology (shenzhen) Co.Ltd.
State:	Guang Dong
Country:	CN
Email:	Select Request Email Form at https://domains.markmonitor.com/whois/tencent.com

Administrative Contact

Organization:	Tencent Technology (shenzhen) Co.Ltd.
State:	Guang Dong
Country:	CN
Email:	Select Request Email Form at https://domains.markmonitor.com/whois/tencent.com

Technical Contact

Organization:	Tencent Technology (shenzhen) Co.Ltd.
State:	Guang Dong
Country:	CN
Email:	Select Request Email Form at https://domains.markmonitor.com/whois/tencent.com

.space Sale
\$24.88 \$0.88
BUY NOW
*Offer ends 29th February 2020

.me On Sale!
\$7.88 \$18.88
VIEW MORE

WORDPRESS Introducing

WORDPRESS HOSTING Introducing
\$3.58 /mo
VIEW MORE

Raw Whois Data

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#clientUpdateProhib>)
Domain Status: clientTransferProhibited (<https://www.icann.org/epp#clientTransferPr>)
Domain Status: clientDeleteProhibited (<https://www.icann.org/epp#clientDeleteProhib>)
Domain Status: serverUpdateProhibited (<https://www.icann.org/epp#serverUpdateProhib>)
Domain Status: serverTransferProhibited (<https://www.icann.org/epp#serverTransferPr>)
Domain Status: serverDeleteProhibited (<https://www.icann.org/epp#serverDeleteProhib>)
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>
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/ten>
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/tenc>
Name Server: ns3.qq.com
Name Server: ns4.qq.com
Name Server: ns1.qq.com
Name Server: ns2.qq.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>
>>> Last update of WHOIS database: 2020-02-26T05:04:52-0800 <<<

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

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, 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