

中国でGreatだよ

Matsuzaki 'maz' Yoshinobu

<maz@iij.ad.jp>

2013/08 @ APNIC36 network

何だかアクセスできないよ

Twitter

Facebook

YouTube



ERR_TIMED_OUT



ERR_NAME_RESOLUTION_FAILED



ERR_TIMED_OUT

APNICが用意したネットワークだよ

- AS#
 - 24555
- IPアドレス
 - 220.247.144.0/20 - transited by AS7497
 - 2001:df9::/32 - transited by AS4837
- キャッシュDNS
 - BIND9
 - 同じネットワーク内でIPv4/IPv6 dual stack だよ

Twitter

日本環境

```
$ dig twitter.com a +short
```

199.59.150.39

199.59.148.10

199.59.149.230

```
dig twitter.com aaaa +short
```

(回答無し)

中国環境

```
$ dig twitter.com a +short
```

46.82.174.68

```
$ dig twitter.com aaaa +short
```

2123::3e12



IPv4アドレスはDeutsche Telecom AG
IPv6アドレスは未割振り

Facebook

日本環境

```
$ dig www.facebook.com a +short
```

```
star.c10r.facebook.com.
```

```
173.252.73.52
```

```
$ dig www.facebook.com aaaa +short
```

```
star.c10r.facebook.com.
```

```
2a03:2880:2110:df07:face:b00c:0:1
```

中国環境

```
$ dig www.facebook.com a +short
```

```
(回答無し)
```

```
$ dig www.facebook.com aaaa +short
```

```
(回答無し)
```



どちらもServFailだった

YouTube

日本環境

```
$ dig www.youtube.com a +short
```

```
youtube-ui.l.google.com.
```

```
173.194.38.98
```

```
173.194.38.110
```

```
173.194.38.101
```

```
173.194.38.105
```

```
173.194.38.96
```

```
173.194.38.104
```

```
173.194.38.102
```

```
173.194.38.100
```

```
173.194.38.99
```

```
173.194.38.103
```

```
173.194.38.97
```

```
$ dig www.youtube.com aaaa +short
```

```
youtube-ui.l.google.com.
```

```
2404:6800:4008:c01::5d
```

中国環境

```
$ dig www.youtube.com a +short
```

```
159.106.121.75
```

```
$ dig www.youtube.com aaaa +short
```

```
youtube-ui.l.google.com.
```

```
2404:6800:4005:c00::5b
```



IPv4アドレスは米国DoD (米軍)
IPv6アドレスは正しそう

もっと良く見てみるよ

```
$ dig twitter.com @m.root-servers.net +norec
```

```
;<<>> DiG 9.8.3-P4 <<>> twitter.com @m.root-servers.net +norec  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24850  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
```

```
;; QUESTION SECTION:  
;twitter.com.          IN      A
```

```
;; ANSWER SECTION:  
twitter.com.          300    IN      A       78.16.49.15
```

```
;; Query time: 28 msec  
;; SERVER: 202.12.27.33#53(202.12.27.33)  
;; WHEN: Fri Aug 30 12:20:18 2013  
;; MSG SIZE rcvd: 45
```

回答が変わるよ

```
$ dig twitter.com @m.root-servers.net +norec
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com @m.root-servers.net +norec  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61158  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
```

```
;; QUESTION SECTION:  
;twitter.com.          IN      A
```

```
;; ANSWER SECTION:  
twitter.com.          39017  IN      A      243.185.187.30
```

```
;; Query time: 35 msec  
;; SERVER: 202.12.27.33#53(202.12.27.33)  
;; WHEN: Fri Aug 30 12:22:16 2013  
;; MSG SIZE rcvd: 45
```


たまには正しそうな回答もあるよ

```
$ dig twitter.com @m.root-servers.net +norec
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com @m.root-servers.net +norec
```

```
;; global options: +cmd
```

```
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13390
```

```
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 14
```

```
;; QUESTION SECTION:
```

```
;twitter.com.          IN      A
```

```
;; AUTHORITY SECTION:
```

```
com.          172800 IN      NS      c.gtld-servers.net.
```

```
com.          172800 IN      NS      a.gtld-servers.net.
```

```
com.          172800 IN      NS      l.gtld-servers.net.
```

```
com.          172800 IN      NS      i.gtld-servers.net.
```

```
: 以下略
```

EDNS0には対応していないよ

```
$ dig twitter.com a @m.root-servers.net +noredc +dnssec
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com a @m.root-servers.net +noredc +dnssec -4
```

```
;; global options: +cmd
```

```
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31728
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
```

```
;; QUESTION SECTION:
```

```
;twitter.com.          IN      A
```

```
;; ANSWER SECTION:
```

```
twitter.com.          17178  IN      A      8.7.198.45
```

```
;; Query time: 27 msec
```

```
;; SERVER: 202.12.27.33#53(202.12.27.33)
```

```
;; WHEN: Fri Aug 30 16:13:51 2013
```

```
;; MSG SIZE rcvd: 45
```

何を聞いてもA RRを答えるよ

```
$ dig twitter.com soa @m.root-servers.net +norec  
  
; <<>> DiG 9.8.3-P4 <<>> twitter.com soa @m.root-  
servers.net +norec  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:  
5992  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,  
ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;twitter.com.          IN      SOA  
  
;; ANSWER SECTION:  
twitter.com.          300    IN      A       203.98.7.65  
  
;; Query time: 28 msec  
;; SERVER: 202.12.27.33#53(202.12.27.33)  
;; WHEN: Fri Aug 30 12:23:56 2013  
;; MSG SIZE rcvd: 45
```

```
$ dig twitter.com aaaa @m.root-servers.net +norec  
+short  
203.98.7.65  
$ dig twitter.com mx @m.root-servers.net +norec +short  
78.16.49.15  
$ dig twitter.com md @m.root-servers.net +norec +short  
159.106.121.75  
$ dig twitter.com any @m.root-servers.net +norec +short  
159.106.121.75  
$ dig twitter.com txt @m.root-servers.net +norec +short  
46.82.174.68
```

誰に何を聞いてもA RRを答えるよ

```
$ dig twitter.com aaaa @www.iij.ad.jp +norec
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com aaaa @www.iij.ad.jp
+norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11286
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0
```

```
;; QUESTION SECTION:
```

```
;twitter.com.      IN      AAAA
```

```
;; ANSWER SECTION:
```

```
twitter.com.      4530 IN      A       203.98.7.65
```

```
;; Query time: 25 msec
```

```
;; SERVER: 202.232.2.164#53(202.232.2.164)
```

```
;; WHEN: Fri Aug 30 12:28:38 2013
```

```
$ dig twitter.com txt @d.dns.jp +norec +short
```

```
37.61.54.158
```

```
$ dig twitter.com soa @1.1.1.1 +norec +short
```

```
159.106.121.75
```

```
$ dig twitter.com mx @1.2.3.4 +norec +short
```

```
93.46.8.89
```

```
$ dig twitter.com aaaa @www.attn.jp +norec +short
```

```
93.46.8.89
```

ちなみに、指定された宛先ホストでパケットダンプしていると、問い合わせは届いている。

無応答でもDNS的にRefuse応答しても中国のクライアント側にはA RRがNOERRORで応答として届くよ

中国国内宛だと普通の挙動だよ

```
% dig twitter.com a @www.cnnic.cn +norec
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com a @www.cnnic.cn  
+norec  
;; global options: +cmd  
;; connection timed out; no servers could be reached
```

```
dig twitter.com a @a.cnnic.cn +norec
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com a @a.cnnic.cn +norec  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 57799  
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;twitter.com. IN A  
  
;; Query time: 30 msec  
;; SERVER: 203.119.25.5#53(203.119.25.5)  
;; WHEN: Fri Aug 30 12:36:23 2013  
;; MSG SIZE rcvd: 29
```

IPv6トランスポートだとちょっと違うよ

```
$ dig twitter.com aaaa @i.root-servers.net +norec
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com aaaa @i.root-servers.net
+norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62587
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 0

;; QUESTION SECTION:
;twitter.com.          IN      AAAA

;; ANSWER SECTION:
twitter.com.          25600  IN      AAAA  10::2222

;; AUTHORITY SECTION:
com.                  25600  IN      NS     twitter.com.

;; Query time: 29 msec
;; SERVER: 2001:7fe::53#53(2001:7fe::53)
;; WHEN: Fri Aug 30 12:58:39 2013
;; MSG SIZE rcvd: 71
```

AAAAにも答えられるけど、
すっげえAuthセクションが！！

```
$ dig twitter.com a @i.root-servers.net +norec
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com a @i.root-servers.net +norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3908
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;twitter.com.          IN      A

;; ANSWER SECTION:
twitter.com.          25600  IN      A      1.1.1.1

;; AUTHORITY SECTION:
com.                  25600  IN      NS     twitter.com.

;; Query time: 30 msec
;; SERVER: 2001:7fe::53#53(2001:7fe::53)
;; WHEN: Fri Aug 30 13:00:54 2013
;; MSG SIZE rcvd: 59
```

Aにも答えられるけど、
すっげえAuthセクションが！！

IPv6でもAとAAAA以外は駄目だね

```
$ dig twitter.com mx @i.root-servers.net +norec
;; Warning: Message parser reports malformed message
packet.
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com mx @i.root-
servers.net +norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:
41067
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 0
;; WARNING: Messages has 12 extra bytes at end
```

```
;; QUESTION SECTION:
;twitter.com.          IN      MX

;; Query time: 30 msec
;; SERVER: 2001:7fe::53#53(2001:7fe::53)
;; WHEN: Fri Aug 30 13:03:20 2013
;; MSG SIZE rcvd: 53
```

```
$ dig twitter.com any @i.root-servers.net +norec
;; Warning: Message parser reports malformed message packet.
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com any @i.root-servers.net
+norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17823
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 0
;; WARNING: Messages has 12 extra bytes at end
```

```
;; QUESTION SECTION:
;twitter.com.          IN      ANY
```

```
;; Query time: 30 msec
;; SERVER: 2001:7fe::53#53(2001:7fe::53)
;; WHEN: Fri Aug 30 13:03:31 2013
;; MSG SIZE rcvd: 53
```

誰に聞いても何か答えてくれるよ

```
$ dig twitter.com a @www.ij.ad.jp +norec

; <<>> DiG 9.8.3-P4 <<>> twitter.com a @2001:240:bb81::10:1
+norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7183
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;twitter.com.          IN      A

;; ANSWER SECTION:
twitter.com.          300    IN      A      255.255.255.255

;; Query time: 1182 msec
;; SERVER: 2001:240:bb81::10:1#53(2001:240:bb81::10:1)
;; WHEN: Fri Aug 30 13:09:59 2013
;; MSG SIZE rcvd: 45
```

```
% dig twitter.com txt @d.dns.jp +norec +short
;; Warning: Message parser reports malformed message packet.
% dig twitter.com soa @2001:: +norec +short
;; Got bad packet: bad label type
41 bytes
6d 8f 81 80 00 01 00 01 00 00 00 00 07 74 77 69      m.....twi
74 74 65 72 03 63 6f 6d 00 00 06 00 01 91 58 a9      tter.com.....X.
01 00 00 00 00 01 2c 00 00                          .....,..
% dig twitter.com mx @2001::1 +norec +short
;; Warning: Message parser reports malformed message packet.
% dig twitter.com aaaa @2002:: +norec +short
2123::3e12
% dig twitter.com a @www.attn.jp +norec +short
1.1.1.1
```

IPv6でも指定された宛先ホストに問い合わせは届いている。
無応答でもDNS的にRefuse応答しても中国のクライアント側には何らかNOERRORで応答として届くよ

IPv6でも中国国内はふつーだね

```
$ dig twitter.com a @www.cnnic.cn +norec
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com a @www.cnnic.cn  
+norec  
;; global options: +cmd  
;; connection timed out; no servers could be reached
```

```
$ dig twitter.com a @d.dns.cn +norec
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com a @d.dns.cn +norec  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 41022  
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 0,  
ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;twitter.com. IN A  
  
;; Query time: 72 msec  
;; SERVER: 2001:dc7:1000::1#53(2001:dc7:1000::1)  
;; WHEN: Fri Aug 30 13:08:10 2013  
;; MSG SIZE rcvd: 29
```

m.rootはIPv6だと正しそうだよ

```
dig twitter.com a @m.root-servers.net +norec
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter.com a @m.root-servers.net +norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27649
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 14

;; QUESTION SECTION:
;twitter.com.          IN      A

;; AUTHORITY SECTION:
com.                  172800 IN      NS      f.gtld-servers.net.
com.                  172800 IN      NS      d.gtld-servers.net.
: (中略)
;; Query time: 433 msec
;; SERVER: 2001:dc3::35#53(2001:dc3::35)
;; WHEN: Fri Aug 30 12:56:35 2013
;; MSG SIZE rcvd: 489
```

m.rootのhostname.bindみてみたよ

IPv6 -> M-CDG-2

```
% dig hostname.bind chaos txt @m.root-servers.net

;<<>> DiG 9.8.3-P4 <<>> hostname.bind chaos txt @m.root-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59791
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;hostname.bind.      CH  TXT

;; ANSWER SECTION:
hostname.bind.      0  CH  TXT  "M-CDG-2"

;; AUTHORITY SECTION:
hostname.bind.      0  CH  NS   hostname.bind.

;; Query time: 430 msec
;; SERVER: 2001:dc3::35#53(2001:dc3::35)
;; WHEN: Fri Aug 30 12:54:36 2013
;; MSG SIZE rcvd: 65
```

IPv4 -> M-NRT-DIXIE-3

```
dig hostname.bind chaos txt @m.root-servers.net -4

;<<>> DiG 9.8.3-P4 <<>> hostname.bind chaos txt @m.root-servers.net -4
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1353
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;hostname.bind.      CH  TXT

;; ANSWER SECTION:
hostname.bind.      0  CH  TXT  "M-NRT-DIXIE-3"

;; AUTHORITY SECTION:
hostname.bind.      0  CH  NS   hostname.bind.

;; Query time: 108 msec
;; SERVER: 202.12.27.33#53(202.12.27.33)
;; WHEN: Fri Aug 30 12:54:33 2013
;; MSG SIZE rcvd: 71
```

m.rootへの経路が違うんだね

IPv6 -> フランス

```
raceroute6 m.root-servers.net
traceroute6 to m.root-servers.net (2001:dc3::35) from
2001:df9:150:0:20c:29ff:fe00:309c, 64 hops max, 12 byte packets
 1 2001:df9:150::254 1.686 ms 1.429 ms 1.376 ms
 2 2400:dd00:9:1005::1 5.683 ms 13.791 ms 6.507 ms
 3 2400:dd00:0:2f::170 3.468 ms 4.967 ms 21.543 ms
 4 2400:dd00:0:23::205 203.997 ms 31.730 ms 26.125 ms
 5 2400:dd00:0:4::130 26.504 ms 26.307 ms 28.378 ms
 6 2400:dd00:0:2::194 26.583 ms 27.458 ms
   2400:dd00:0:3::194 27.192 ms
 7 2001:252:0:2::101 29.206 ms 33.123 ms 29.761 ms
 8 2001:252:0:100::2 27.281 ms 26.868 ms 26.805 ms
 9 orientplus-gw.mx1.lon.uk.geant.net 203.247 ms 209.589 ms
205.021 ms
10 ae0.mx1.par.fr.geant.net 206.534 ms 205.288 ms 205.491 ms
11 renater-lb1-gw.mx1.par.fr.geant.net 208.656 ms 207.238 ms
216.939 ms
12 te0-1-0-5-paris2-rtr-001.noc.renater.fr 213.523 ms 207.649 ms
210.258 ms
13 * * *
14 M.ROOT-SERVERS.NET 462.250 ms 430.529 ms 455.088 ms
```

IPv4 -> 東京

```
C:\>tracert -4 m.root-servers.net
```

m.root-servers.net [202.12.27.33] へのルートをトレースしています
経由するホップ数は最大 30 です:

```
 1  1 ms  <1 ms  4 ms 254.155.dhcp.conference.apricot.net [220.247.155
.254]
 2  *    *    *   要求がタイムアウトしました。
 3  *    *    *   要求がタイムアウトしました。
 4  24 ms 40 ms 25 ms 159.226.253.189
 5  26 ms 24 ms 24 ms 8.131 [159.226.253.61]
 6  193 ms 207 ms 238 ms 8.198 [159.226.253.54]
 7  *    *    *   要求がタイムアウトしました。
 8  *    *    *   要求がタイムアウトしました。
 9  122 ms 106 ms 104 ms tpr5-ge0-0-0-136.jp.apan.net [203.181.249.117]
10  100 ms 168 ms 100 ms vlan53-cisco2.notemachi.wide.ad.jp [203.178.133.
142]
11  165 ms 148 ms 133 ms ve-51.foundry6.otemachi.wide.ad.jp [203.178.141.
141]
12  137 ms 148 ms 138 ms ve-5.alala1.otemachi.wide.ad.jp [203.178.140.215
]
13  120 ms 106 ms 107 ms m-gw.nspixp2.wide.ad.jp [202.249.2.86]
14  106 ms 107 ms 106 ms M.ROOT-SERVERS.NET [202.12.27.33]
```

トレースを完了しました。

m.rootへのIPv4問い合わせ

16:30:24.406047 IP (tos 0x0, ttl 128, id 11425, offset 0, flags [none], proto UDP (17), length 57)
220.247.153.31.60938 > 202.12.27.33.53: 5+ A? twitter.com. (29)

28msec

16:30:24.434257 IP (tos 0x0, ttl 52, id 28944, offset 0, flags [none], proto UDP (17), length 73)
202.12.27.33.53 > 220.247.153.31.60938: 5 1/0/0 twitter.com. A 8.7.198.45 (45)

16:30:24.434552 IP (tos 0x10, ttl 213, id 19443, offset 0, flags [none], proto UDP (17), length 73)
202.12.27.33.53 > 220.247.153.31.60938: 5 1/0/0 twitter.com. A 78.16.49.15 (45)

100msec

16:30:24.514333 IP (tos 0x0, ttl 52, id 52732, offset 0, flags [none], proto UDP (17), length 517)
202.12.27.33.53 > 220.247.153.31.60938: 5- 0/13/14 (489)

例の応答が2個(28msec)到着後、本物っぽい応答が遅れて(100msec)到着

m.rootへのIPv6問い合わせ

16:21:49.753354 IP6 (hlim 64, next-header UDP (17) payload length: 37)
2001:df9:150:0:20c:29ff:fe00:309c.41081 > 2001:dc3::35.53: [udp sum ok] 27090 A? twitter.com.
(29)

450msec

16:21:50.205205 IP6 (hlim 36, next-header UDP (17) payload length: 497) 2001:dc3::35.53 >
2001:df9:150:0:20c:29ff:fe00:309c.41081: [udp sum ok] 27090- 0/13/14 (489)

2980msec

16:21:52.733836 IP6 (hlim 49, next-header UDP (17) payload length: 53) 2001:dc3::35.53 >
2001:df9:150:0:20c:29ff:fe00:309c.41081: [udp sum ok] 27090 1/0/0 twitter.com. A
255.255.255.255 (45)

本物の応答(450msec) vs 例の応答(2980msec)で、
本物の応答が勝っちゃった

Wikipediaは名前解決できたよ

```
$ dig en.wikipedia.org a
```

```
; <<> DiG 9.8.3-P4 <<> en.wikipedia.org a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14045
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;en.wikipedia.org.      IN      A

;; ANSWER SECTION:
en.wikipedia.org.      3118   IN      CNAME   wikipedia-lb.wikimedia.org.
wikipedia-lb.wikimedia.org. 119    IN      CNAME   wikipedia-lb.eqiad.wikimedia.org.
wikipedia-lb.eqiad.wikimedia.org. 3119   IN      A       208.80.154.225

;; AUTHORITY SECTION:
wikimedia.org.        68468  IN      NS       ns0.wikimedia.org.
wikimedia.org.        68468  IN      NS       ns1.wikimedia.org.
wikimedia.org.        68468  IN      NS       ns2.wikimedia.org.

;; ADDITIONAL SECTION:
ns1.wikimedia.org.    68468  IN      A        208.80.152.214
ns2.wikimedia.org.    68468  IN      A        91.198.174.239
ns0.wikimedia.org.    68468  IN      A        208.80.154.238

;; Query time: 3 msec
;; SERVER: 220.247.145.1#53(220.247.145.1)
;; WHEN: Fri Aug 30 15:03:16 2013
;; MSG SIZE rcvd: 222
```

```
dig en.wikipedia.org aaaa
```

```
; <<> DiG 9.8.3-P4 <<> en.wikipedia.org aaaa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42962
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;en.wikipedia.org.      IN      AAAA

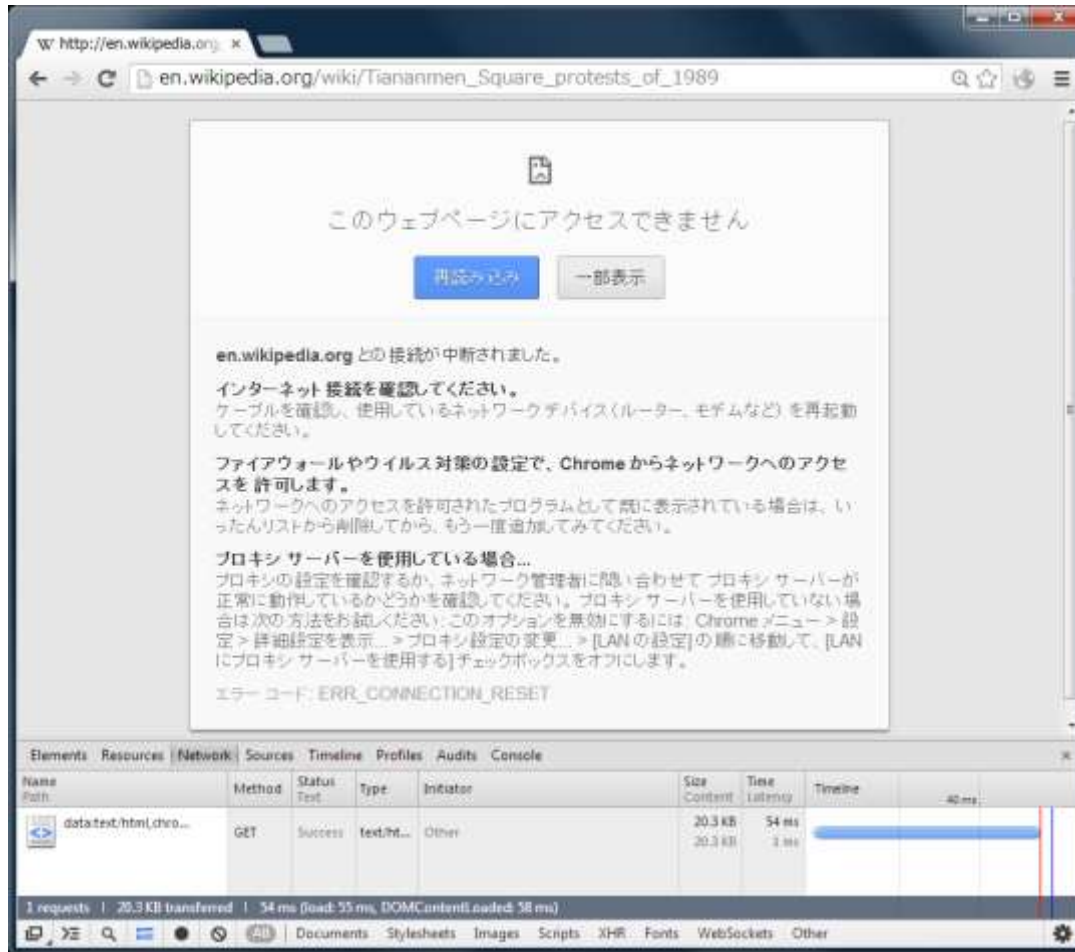
;; ANSWER SECTION:
en.wikipedia.org.      3116   IN      CNAME   wikipedia-lb.wikimedia.org.
wikipedia-lb.wikimedia.org. 117    IN      CNAME   wikipedia-lb.eqiad.wikimedia.org.
wikipedia-lb.eqiad.wikimedia.org. 3117   IN      AAAA    2620:0:861:ed1a::1

;; AUTHORITY SECTION:
wikimedia.org.        68466  IN      NS       ns2.wikimedia.org.
wikimedia.org.        68466  IN      NS       ns0.wikimedia.org.
wikimedia.org.        68466  IN      NS       ns1.wikimedia.org.

;; ADDITIONAL SECTION:
ns1.wikimedia.org.    68466  IN      A        208.80.152.214
ns2.wikimedia.org.    68466  IN      A        91.198.174.239
ns0.wikimedia.org.    68466  IN      A        208.80.154.238

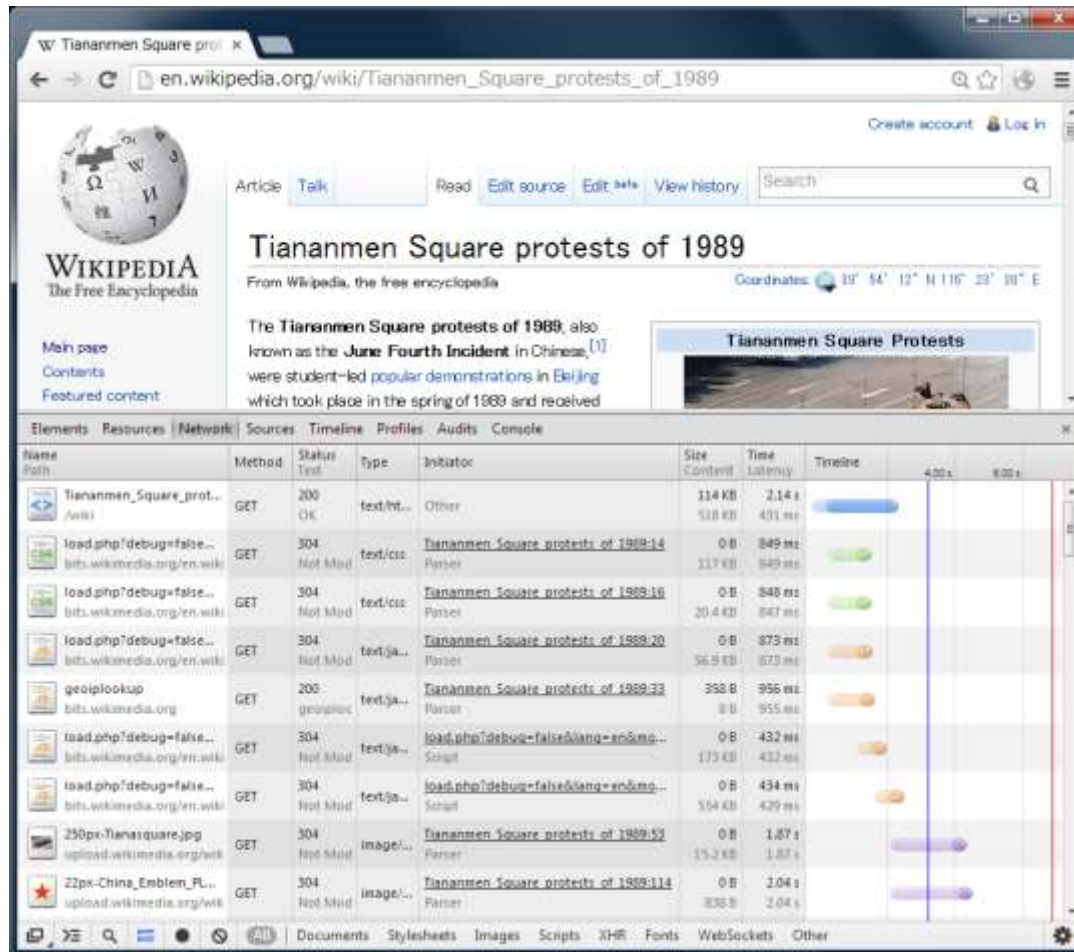
;; Query time: 6 msec
;; SERVER: 220.247.145.1#53(220.247.145.1)
;; WHEN: Fri Aug 30 15:03:18 2013
;; MSG SIZE rcvd: 234
```

IPv4で、とあるページを見てみたよ



どこからかRSTが飛んできたよ

IPv6だとアクセスできたよ！



The screenshot shows a web browser window displaying the Wikipedia article "Tiananmen Square protests of 1989". The browser's address bar shows the URL "en.wikipedia.org/wiki/Tiananmen_Square_protests_of_1989". The page content includes the Wikipedia logo, the article title, and a brief description: "The Tiananmen Square protests of 1989, also known as the June Fourth Incident in Chinese, were student-led popular demonstrations in Beijing which took place in the spring of 1989 and received".

The Chrome DevTools Network tab is open, showing a list of network requests. The table below represents the data from this tab:

Name	Method	Status	Type	Initiator	Size	Time	Latency	Timeline
Tiananmen_Square_prot... /wiki	GET	200 OK	text/html	Other	114 KB 510 KB	2,14 s 431 ms		
load.php?debug=false... bits.wikimedia.org/en/wiki	GET	304 Not Mod	text/css	Tiananmen_Square_protests_of_1989:14	0 B 117 KB	849 ms 849 ms		
load.php?debug=false... bits.wikimedia.org/en/wiki	GET	304 Not Mod	text/css	Tiananmen_Square_protests_of_1989:16	0 B 20.4 KB	848 ms 847 ms		
load.php?debug=false... bits.wikimedia.org/en/wiki	GET	304 Not Mod	text/javascript	Tiananmen_Square_protests_of_1989:20	0 B 56.9 KB	873 ms 873 ms		
geoiplookup bits.wikimedia.org	GET	200 geoprivacy	text/javascript	Tiananmen_Square_protests_of_1989:33	398 B 0 B	956 ms 955 ms		
load.php?debug=false... bits.wikimedia.org/en/wiki	GET	304 Not Mod	text/javascript	load.php?debug=false&lang=en&mo...	0 B 173 KB	432 ms 432 ms		
load.php?debug=false... bits.wikimedia.org/en/wiki	GET	304 Not Mod	text/javascript	load.php?debug=false&lang=en&mo...	0 B 534 KB	434 ms 429 ms		
250px-Tiananmen Square.jpg upload.wikimedia.org/wik	GET	304 Not Mod	image/jpeg	Tiananmen_Square_protests_of_1989:51	0 B 15.2 KB	1.87 s 1.87 s		
22px-China Emblem_FL... upload.wikimedia.org/wik	GET	304 Not Mod	image/png	Tiananmen_Square_protests_of_1989:114	0 B 830 B	2.04 s 2.04 s		

www.YouTube.comをhostsに書いたよ

18:36:35.491011 IP6 (flowlabel 0x92057, hlim 64, next-header TCP (6) payload length: 40) 2001:df9:150:0:20c:29ff:fe00:3092.54646 > 2404:6800:4008:c01::5d.80: Flags [S], cksum 0x8f8a (correct), seq 1995045044, win 65535, options [mss 1440,nop,wscale 6,sackOK,TS val 2429102 ecr 0], length 0

0x0000: 6009 2057 0028 0640 2001 0df9 0150 0000 `..W.(.@.....P..
0x0010: 020c 29ff fe00 3092 2404 6800 4008 0c01 ..)...O.\$..h.@...
0x0020: 0000 0000 0000 005d d576 0050 76e9 f8b4].v.Pv...
0x0030: 0000 0000 a002 ffff 8f8a 0000 0204 05a0
0x0040: 0103 0306 0402 080a 0025 10ae 0000 0000%.....

18:36:36.325399 IP6 (hlim 47, next-header TCP (6) payload length: 32) 2404:6800:4008:c01::5d.80 > 2001:df9:150:0:20c:29ff:fe00:3092.54646: Flags [S.], cksum 0x930a (correct), seq 1840108380, ack 1995045045, win 62304, options [mss 1416,nop,nop,sackOK,nop,wscale 6], length 0

0x0000: 6000 0000 0020 062f 2404 6800 4008 0c01 `...../\$..h.@...
0x0010: 0000 0000 0000 005d 2001 0df9 0150 0000]......P..
0x0020: 020c 29ff fe00 3092 0050 d576 6dad d35c ..)...O..P.vm..¥
0x0030: 76e9 f8b5 8012 f360 930a 0000 0204 0588 v.....`.....
0x0040: 0101 0402 0103 0306

SYN/ACKまで800msecも掛かかっているけど、ひとまず応答があったよ！

GET送ったらIPv6でもRSTが来たよ

```
18:36:36.326652 IP6 (flowlabel 0x92057, hlim 64, next-header TCP (6) payload len
gth: 331) 2001:df9:150:0:20c:29ff:fe00:3092.54646 > 2404:6800:4008:c01::5d.80: Flags [P.], cksum 0xf79f (correct), seq 1:312, ack 1, win 1039, length 311
0x0000: 6009 2057 014b 0640 2001 0df9 0150 0000  `..W.K.@.....P..
0x0010: 020c 29ff fe00 3092 2404 6800 4008 0c01  ..)...O.$..h.@...
0x0020: 0000 0000 0000 005d d576 0050 76e9 f8b5  .....].v.Pv...
0x0030: 6dad d35d 5018 040f f79f 0000 4745 5420  m..]P.....GET.
0x0040: 2f20 4854 5450 2f31 2e31 0d0a 486f 7374  /.HTTP/1.1..Host
0x0050: 3a20 7777 772e 796f 7574 7562 652e 636f  :.www.youtube.co
0x0060: 6d0d 0a55 7365 722d 4167 656e 743a 204d  m..User-Agent:.M
0x0070: 6f7a 696c 6c61 2f35 2e30 2028 5831 313b  ozilla/5.0.(X11;
      : (パケット省略)
18:36:36.359250 IP6 (hlim 55, next-header TCP (6) payload length: 20) 2404:6800:4008:c01::5d.80 > 2001:df9:150:0:20c:29ff:fe00:3092.54646: Flags [R.],
cksum 0x92fb (correct), seq 1, ack 312, win 13018, length 0
0x0000: 6000 0000 0014 0637 2404 6800 4008 0c01  `.....7$.h.@...
0x0010: 0000 0000 0000 005d 2001 0df9 0150 0000  .....].....P..
0x0020: 020c 29ff fe00 3092 0050 d576 6dad d35d  ..)...O..P.vm..]
0x0030: 76e9 f9ec 5014 32da 92fb 0000          v...P.2.....
18:36:36.659348 IP6 (hlim 47, next-header TCP (6) payload length: 20) 2404:6800:4008:c01::5d.80 > 2001:df9:150:0:20c:29ff:fe00:3092.54646: Flags [.),
cksum 0xc1fa (correct), seq 1, ack 312, win 991, length 0
0x0000: 6000 0000 0014 062f 2404 6800 4008 0c01  `...../$.h.@...
0x0010: 0000 0000 0000 005d 2001 0df9 0150 0000  .....].....P..
0x0020: 020c 29ff fe00 3092 0050 d576 6dad d35d  ..)...O..P.vm..]
0x0030: 76e9 f9ec 5010 03df c1fa 0000          v...P.....
```

2.6msec

322msec

RSTは2.6msecで受信したよ。その後のHopLimitの違うACKは332msec掛かってるけど
IPv6でも一部コンテンツフィルタに対応しているんだね

もうちょっとDNS関連だよ

- どんな方法で対象の問い合わせを見つけてるのかな？
- 何か抜け出す方法あるかな？

Case Sensitive?

dig **Twitter.com** a @m.root-servers.net

```
; <<>> DiG 9.8.3-P4 <<>> Twitter.com a @m.root-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44197
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;Twitter.com.          IN      A

;; ANSWER SECTION:
Twitter.com.        35782  IN      A      8.7.198.45

;; Query time: 32 msec
;; SERVER: 202.12.27.33#53(202.12.27.33)
;; WHEN: Fri Aug 30 15:32:46 2013
;; MSG SIZE rcvd: 45
```

0x20も対応してるよ

ホスト名を間違っても答えるよ！

```
$ dig maz.twitter.com aaaa @www.iij.ad.jp

; <<>> DiG 9.8.3-P4 <<>> maz.twitter.com aaaa
@www.iij.ad.jp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:
46972
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;maz.twitter.com.          IN      AAAA

;; ANSWER SECTION:
maz.twitter.com.          300    IN      AAAA    2620:f:8000::

;; Query time: 749 msec
;; SERVER:
2001:240:bb81::10:1#53(2001:240:bb81::10:1)
;; WHEN: Fri Aug 30 15:38:07 2013
;; MSG SIZE rcvd: 61
```

```
$ dig hoge.hoge.twitter.com aaaa @2002:: +short
2001::212
$ dig port53.twitter.com aaaa @2002:: +short
2123::3e12
$ dig ipv4.twitter.com a @2002:: +short
1.1.1.1
$ dig ipv4.twitter.com aaaa @2002:: +short
101::1234
$ dig ipv4.twitter.com aaaa @8.8.8.8 +short
243.185.187.39
$ dig ipv4.twitter.com a @8.8.8.8 +short
93.46.8.89
```

ドメイン名を間違っても答えるよ！

```
$ dig mazmazmaztwitter.com a @www.iij.ad.jp

; <<>> DiG 9.8.3-P4 <<>> mazmazmaztwitter.com a
@www.iij.ad.jp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43143
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;mazmazmaztwitter.com.      IN      A

;; ANSWER SECTION:
mazmazmaztwitter.com. 45548 IN      A      46.82.174.68

;; Query time: 32 msec
;; SERVER: 202.232.2.164#53(202.232.2.164)
;; WHEN: Fri Aug 30 15:45:27 2013
;; MSG SIZE rcvd: 54
```

```
$ dig wwwyoutube.com a @2001:: +short
255.255.255.255
$ dig hogehogeyoutube.com a @2001:: +short
255.255.255.255
$ dig hogehogefacebook.com a @2001:: +short
255.255.255.255
$ dig a---facebook.com a @2001:: +short
255.255.255.255
$ dig 1111facebook.com a @2001:: +short
255.255.255.255
```

全然違うドメインでも見過ごさないよ

```
$ dig twitter.com.example.jp a @www.ij.ad.jp

; <<>> DiG 9.8.3-P4 <<>> twitter.com.example.jp a
@www.ij.ad.jp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36486
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;twitter.com.example.jp.      IN      A

;; ANSWER SECTION:
twitter.com.example.jp. 300 IN A 255.255.255.255

;; Query time: 3287 msec
;; SERVER: 2001:240:bb81::10:1#53(2001:240:bb81::10:1)
;; WHEN: Fri Aug 30 15:54:23 2013
;; MSG SIZE rcvd: 56
```

```
$ dig twitter.comm a @2002:: +short
1.1.1.1
$ dig twitter.comm aaaa @2002:: +short
2001::212
$ dig aaa.youtube.company aaaa @2002:: +short
21:2::2
$ dig maz.facebook.com---pany aaaa @2001:: +short
2620:f:8000::ffff:ffff
$ dig a--youtube.com--b aaaa @2002:: +short
2001:da8:112::21ae
```


マッチする部分が無いと見過ごすよ

```
$ dig twitter-com a @i.root-servers.net +norec
```

```
; <<>> DiG 9.8.3-P4 <<>> twitter-com a @i.root-servers.net  
+norec
```

```
:: global options: +cmd
```

```
:: Got answer:
```

```
:: ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id:  
13326
```

```
:: flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 1,  
ADDITIONAL: 0
```

```
:: QUESTION SECTION:
```

```
;twitter-com. IN A
```

```
:: AUTHORITY SECTION:
```

```
. 86400 IN SOA a.root-servers.net.  
nstld.verisign-grs.com. 2013082901 1800 900 604800 86400
```

```
:: Query time: 470 msec
```

```
:: SERVER: 2001:7fe::53#53(2001:7fe::53)
```

```
:: WHEN: Fri Aug 30 15:50:33 2013
```

```
:: MSG SIZE rcvd: 104
```

```
$ dig youtube.com aaaa @2002:: +short
```

```
:
```

```
:: connection timed out; no servers could be reached
```

```
$ dig youtube.example.jp aaaa @8.8.8.8
```

```
:
```

```
:: ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id:  
44041
```

/対象ドメイン名/i

- パターンマッチだ！
 - Case Insensitive
 - 前後に何が付いても大丈夫
 - [.]はちゃんと[.]じゃないとダメ
- 対象ドメインを含むようなドメイン名を使うと、なぜか中国からのアクセスを禁止できるよ
 - `twitter.com.example.jp`
 - `youtube.com.example.jp`

DNS

- UDP/53はDNSの中でも最弱にspoof放題
- 奴がやられても、まだTCP/53があるじゃない
 - 乗っ取りにくい

TCP/53ばんざーい

```
$ dig youtube.com aaaa @8.8.8.8 +tc
```

```
; <<>> DiG 9.8.3-P4 <<>> youtube.com aaaa @8.8.8.8 +tc
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28380
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;youtube.com.          IN      AAAA

;; ANSWER SECTION:
youtube.com.          298    IN      AAAA    2404:6800:4005:c00::5d

;; Query time: 235 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Aug 30 16:33:23 2013
;; MSG SIZE rcvd: 57
```

RSTとかも来てなかったよ

まとめ

- 中国では国外へのUDP/53を見ている模様
 - TCP/53は今のところ監視対象外の模様
- パターンマッチで対象問い合わせを特定し、何等かIPアドレスを応答している
 - 応答するIPアドレスは傾向はあるものの適当
 - IPv4/IPv6で少し異なる挙動
- 本当の応答も返ってきているため、それを無視できるようにになれば、突破できるかも
 - RST
 - 偽のDNS応答