qname色々

Matsuzaki ‘maz’ Yoshinobu

<maz@iij.da.jp>

障害切り分けに便利なqname

- ネームサーバの識別
- 問い合わせ元情報
- DNSSECの検証テスト

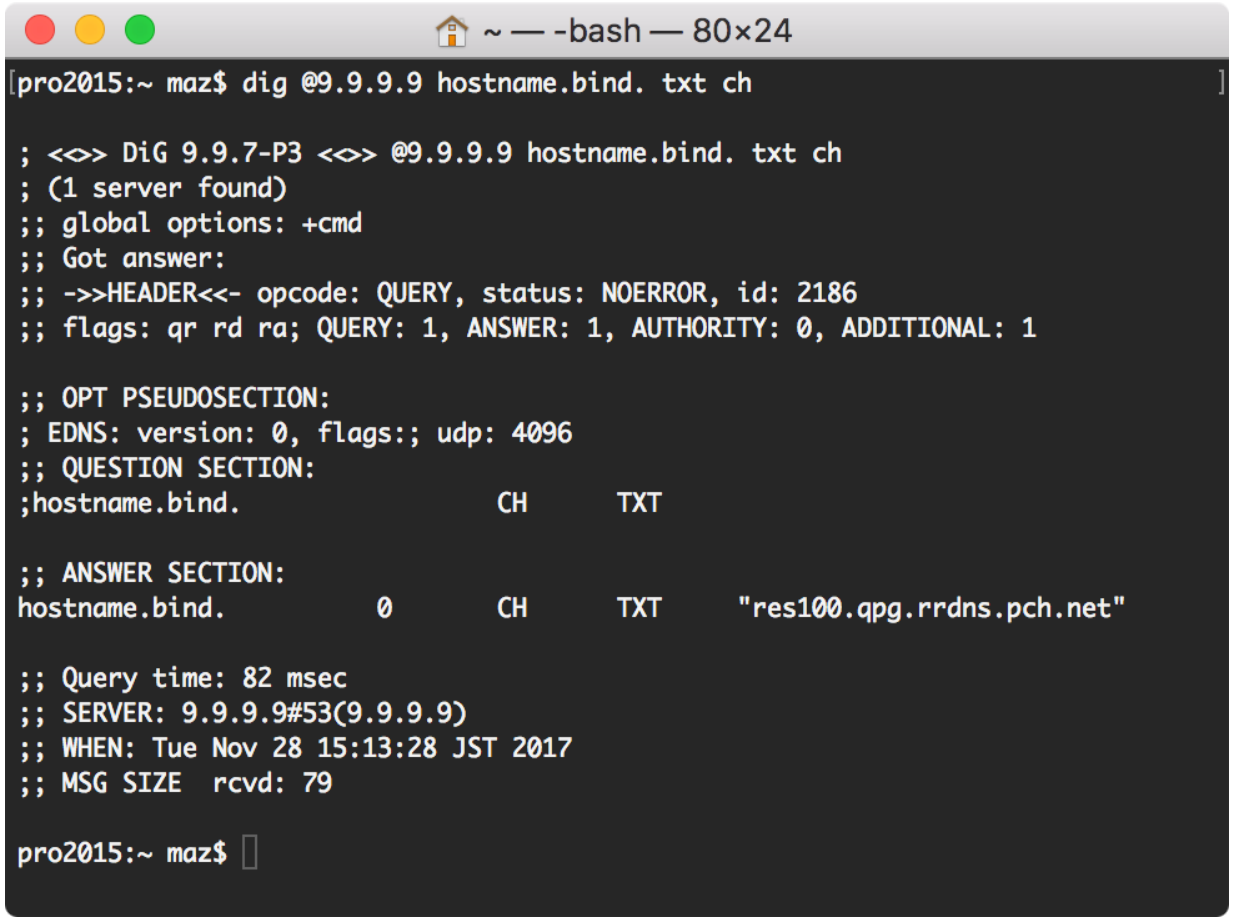
- これらは概ね各組織の勝手実装であったり、ネームサーバ設定に依存しているので、挙動や応答が変わることがあります

ISC BIND由来

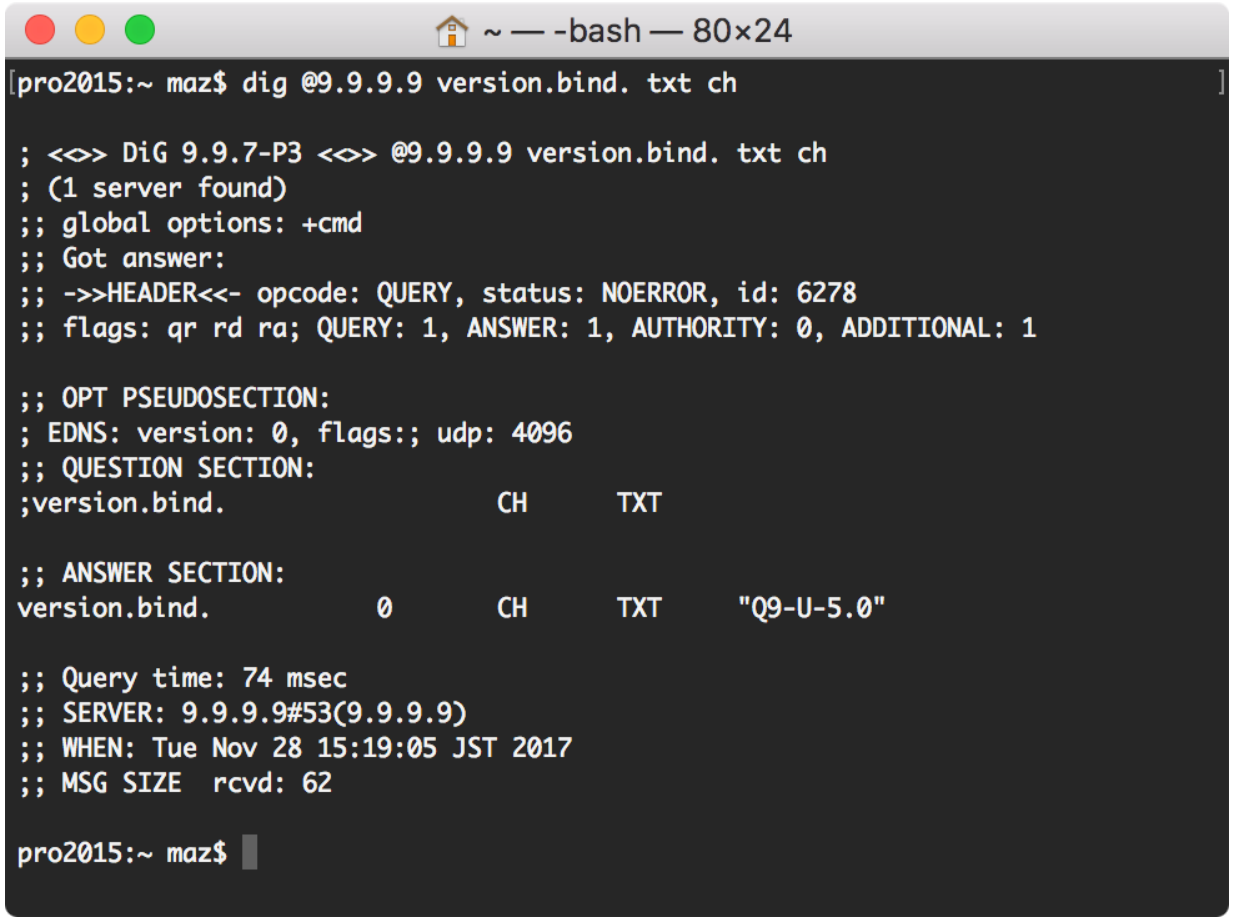
- hostname.bind. CH TXT
  - ホスト名っぽいものを答える
- version.bind. CH TXT
  - 実装のバージョンっぽいものを答える

- 最近は隠すのが流行って来たね
- hostnameはanycastなノードの判定に便利

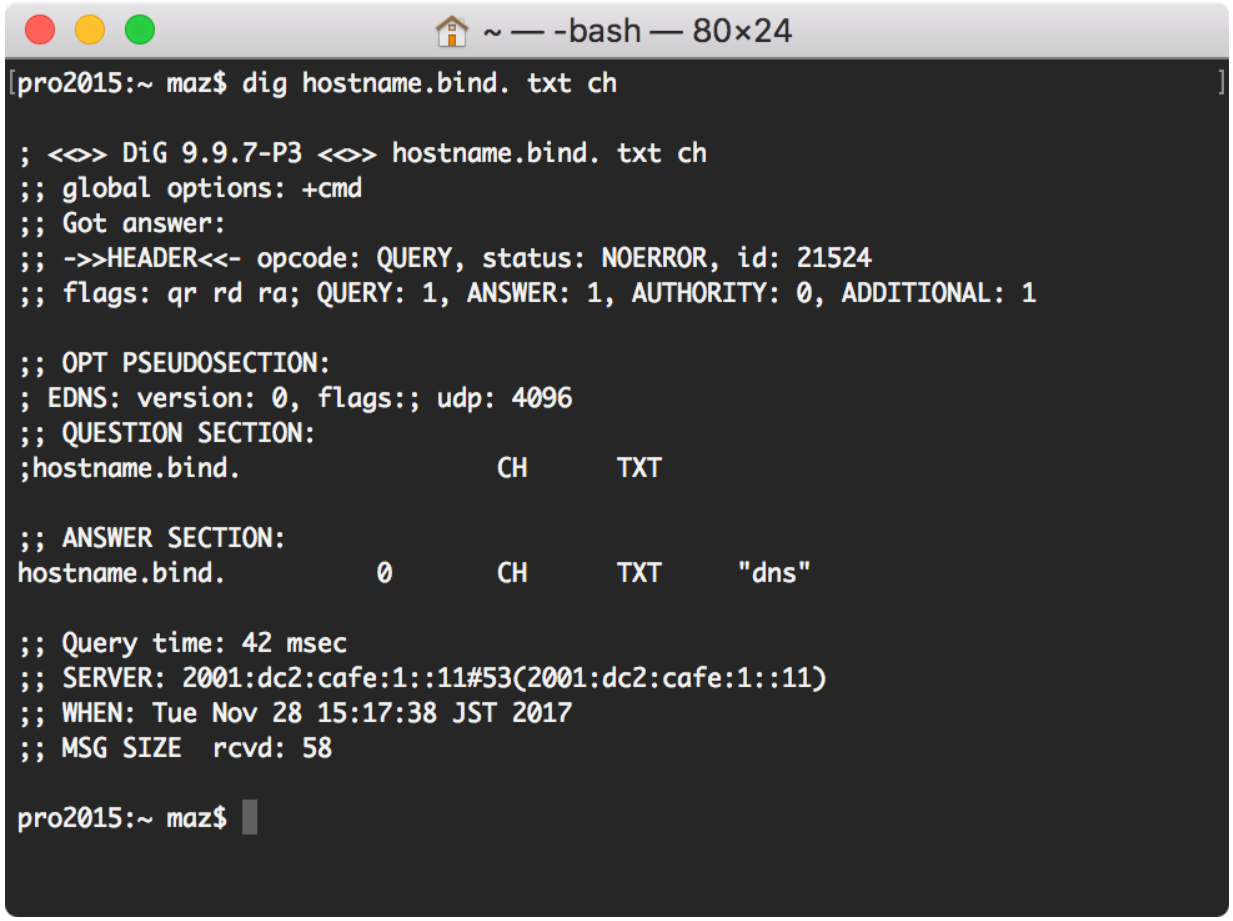
例えば噂の9.9.9.9


~ — -bash — 80×24
pro2015:~ maz$ dig @9.9.9.9 hostname.bind. txt ch
; <<>> DiG 9.9.7-P3 <<>> @9.9.9.9 hostname.bind. txt ch
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2186
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;hostname.bind. CH TXT
;; ANSWER SECTION:
hostname.bind. 0 CH TXT "res100.qpg.rrdns.pch.net"
;; Query time: 82 msec
;; SERVER: 9.9.9.9#53(9.9.9.9)
;; WHEN: Tue Nov 28 15:13:28 JST 2017
;; MSG SIZE rcvd: 79
pro2015:~ maz$

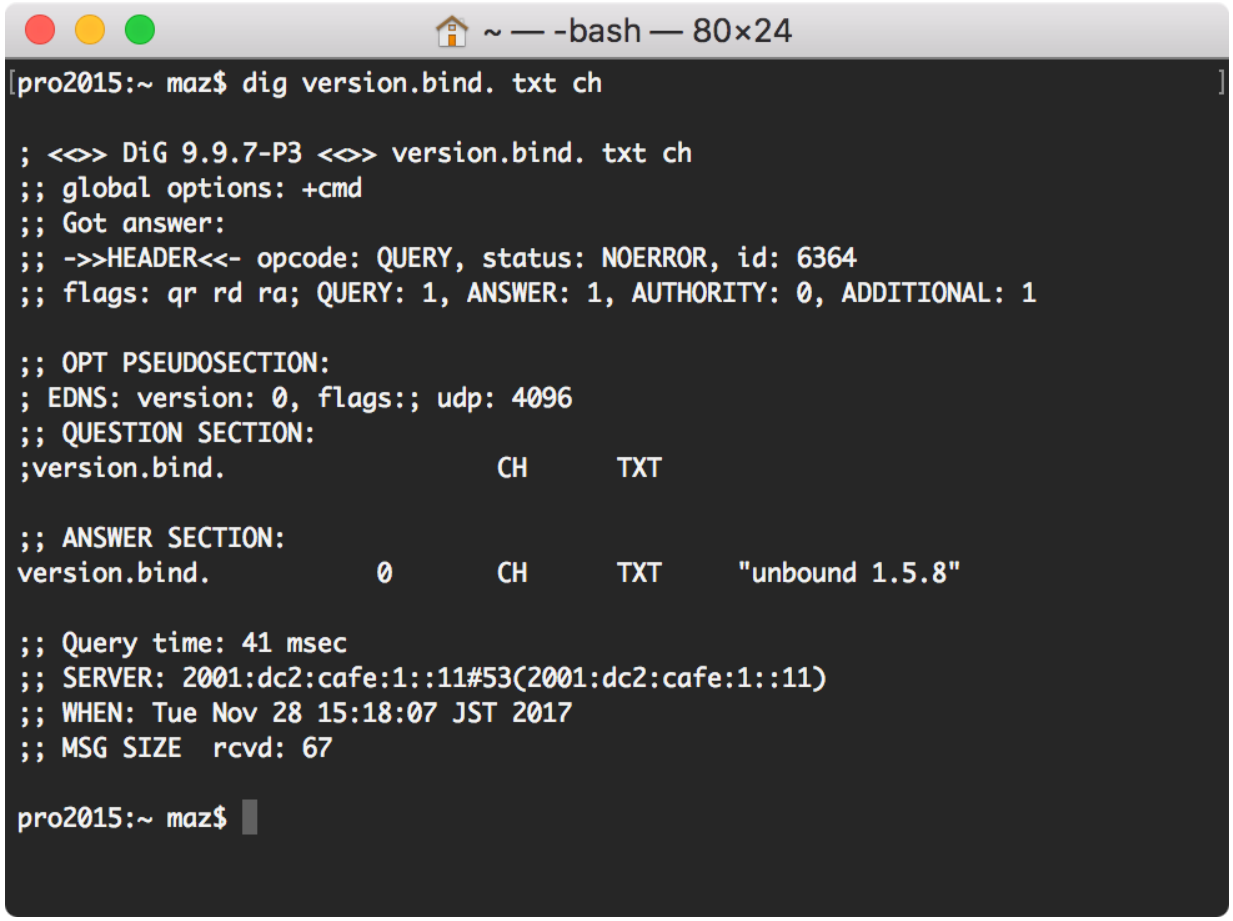
例えば噂の9.9.9.9


~ — -bash — 80×24
pro2015:~ maz$ dig @9.9.9.9 version.bind. txt ch
; <<>> DiG 9.9.7-P3 <<>> @9.9.9.9 version.bind. txt ch
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6278
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;version.bind. CH TXT
;; ANSWER SECTION:
version.bind. 0 CH TXT "Q9-U-5.0"
;; Query time: 74 msec
;; SERVER: 9.9.9.9#53(9.9.9.9)
;; WHEN: Tue Nov 28 15:19:05 JST 2017
;; MSG SIZE rcvd: 62
pro2015:~ maz$

例えばここの参照用サーバ



例えばここの参照用サーバ

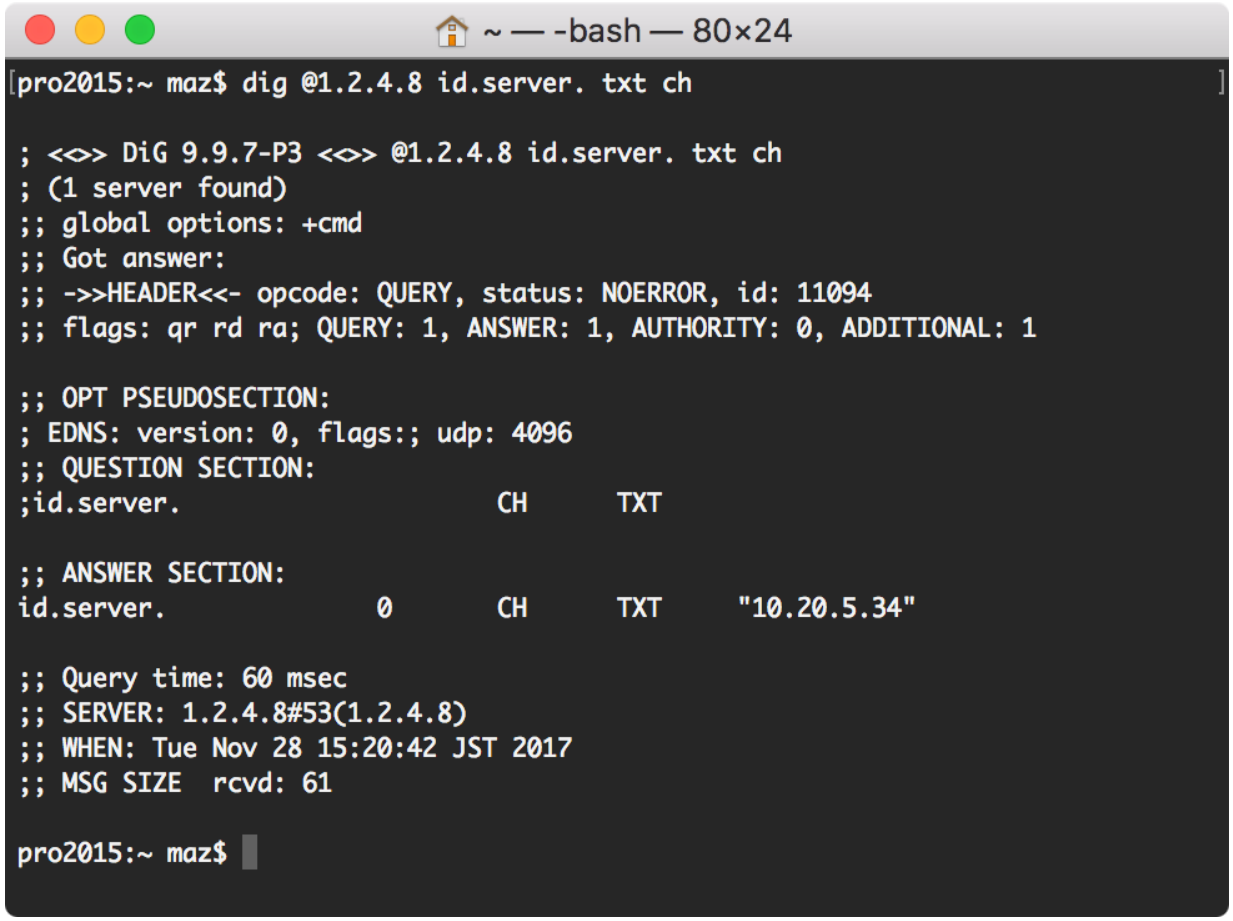


RFC4892的qname

- id.server. CH TXT
  - ネームサーバを特定するための文字列を答える

例えば1.2.4.8

10.20.5.0/24だと外側？10.20.8.0/24だと内側？



l.root-servers.netでの取り組み

- identity.l.root-servers.org. IN txt
- identity.l.root-servers.org. IN A
- おまけ
  - RFC5001的NSID

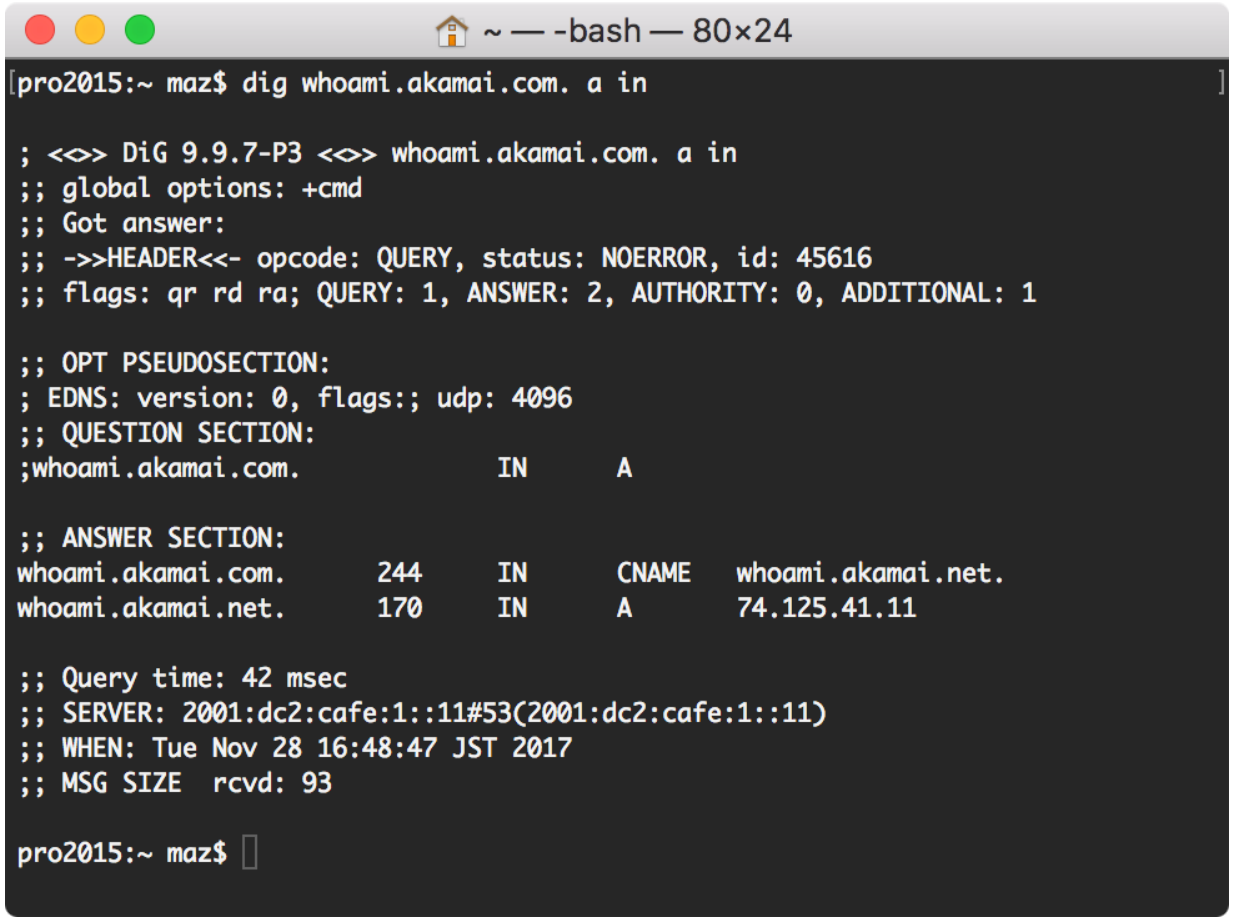
~ — -bash — 80×24

```
pro2015:~ maz$ dig  +nsid  @l.root-servers.net

; <<>> DiG 9.9.7-P3 <<>> +nsid @l.root-servers.net
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22392
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; NSID: 6c 61 78 35 36 2e 6c 2e 72 6f 6f 74 2d 73 65 72 76 65 72 73 2e 6f 72 67
 (l) (a) (x) (5) (6) (.) (l) (.) (r) (o) (o) (t) (-) (s) (e) (r) (v) (e) (r) (s)
 (.) (o) (r) (g)
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
```

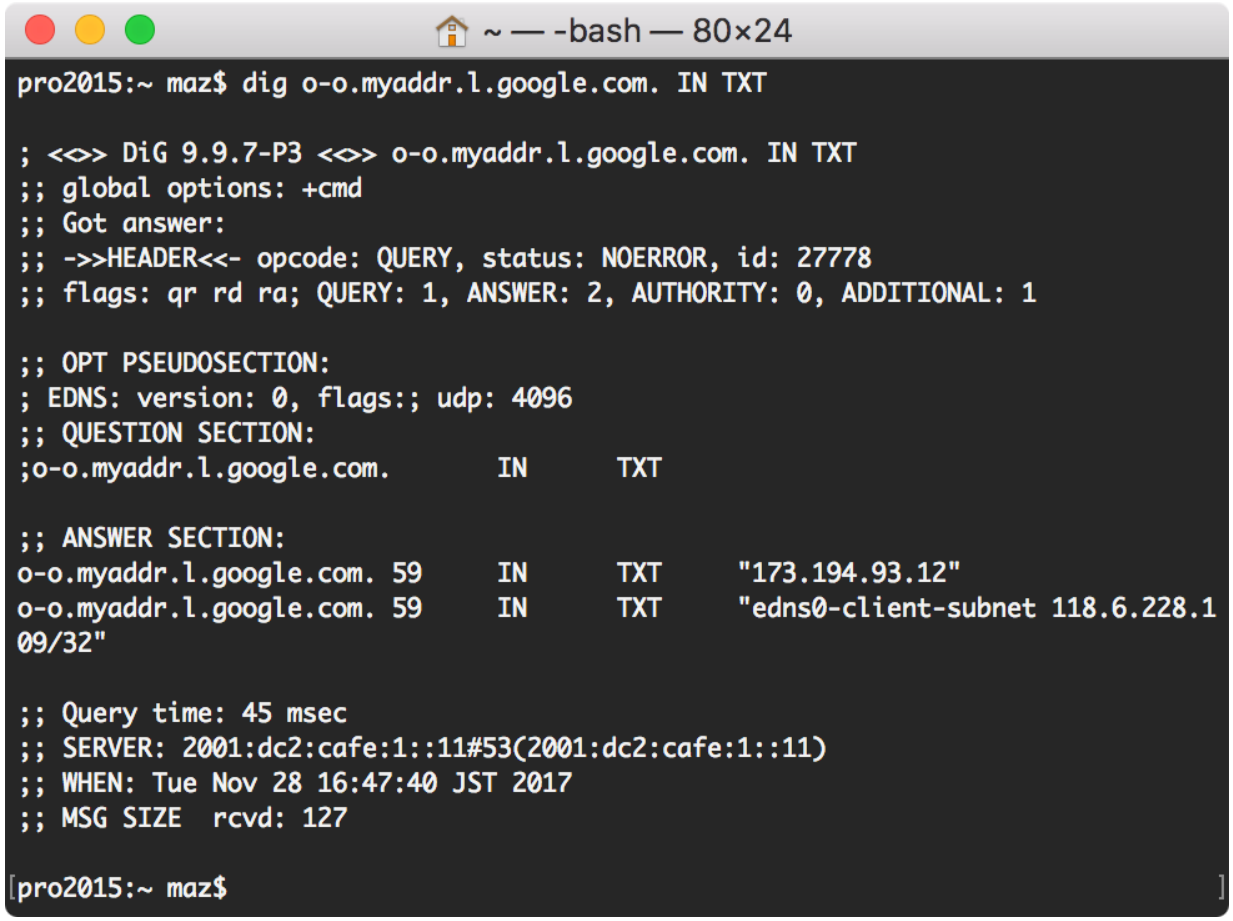
問い合わせ元情報

- 権威サーバで見えた情報
  - 参照しているフルリゾルバのIPアドレス
  - あればedns0-client-subnetの情報
- whoami.akamai.com. IN A
  - IPv4のみ
- o-o.myaddr.l.google.com. IN TXT
  - IPv4/IPv6, ecs対応
- maxmind.test-ipv6.com. IN TXT
  - さらに追加の情報を表示

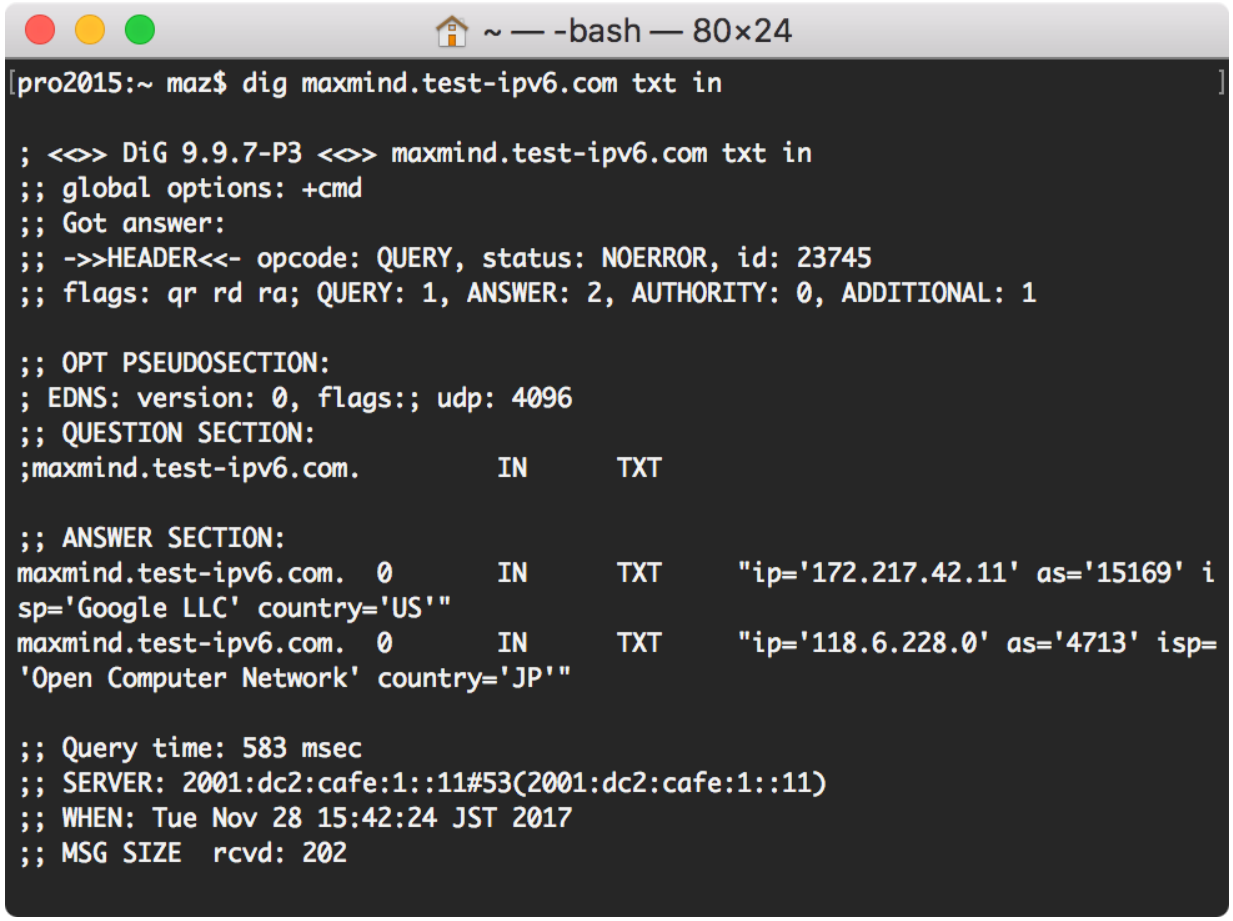
例えばここの参照用サーバ



例えばここの参照用サーバ

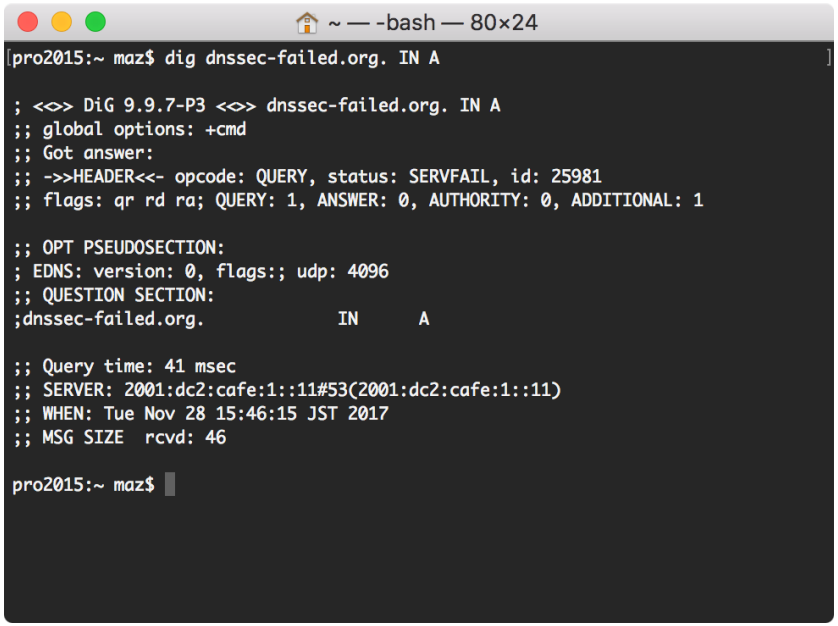


例えばここの参照用サーバ



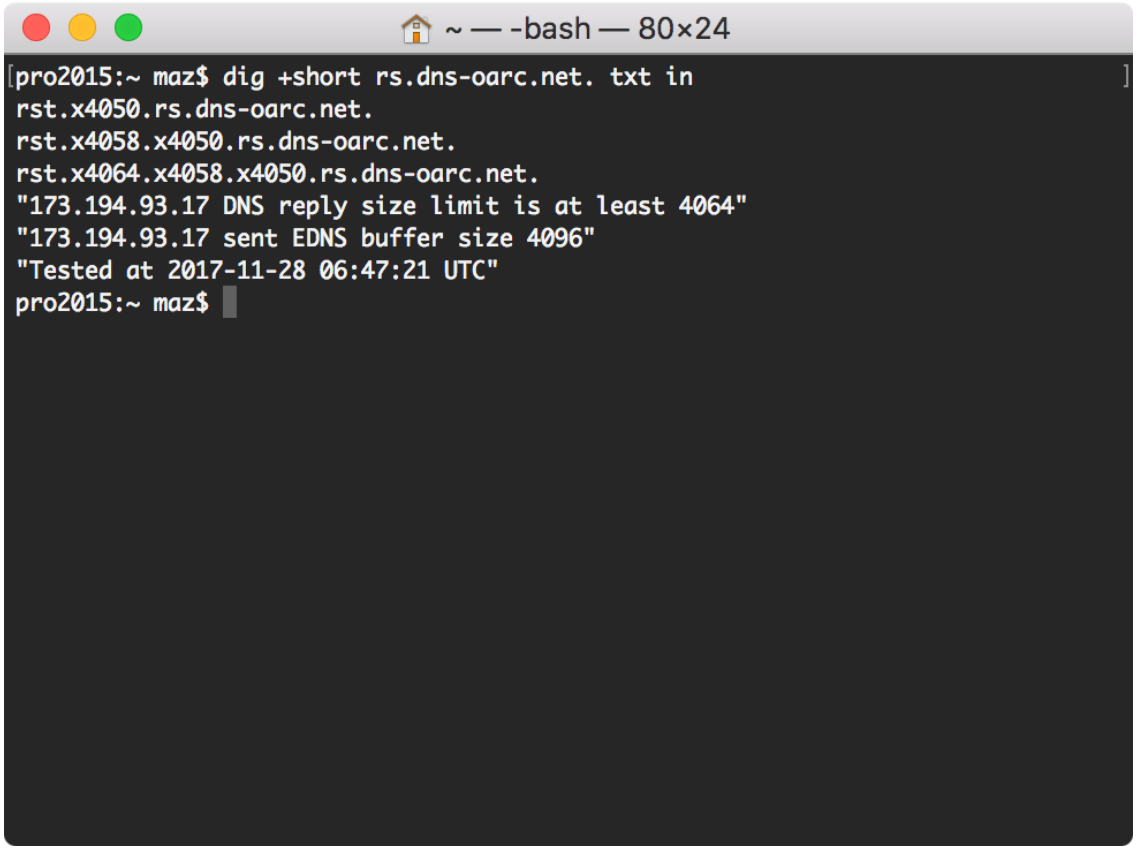
DNSSEC検証の確認

- dnssec-failed.org. IN A
  - DNSSEC検証が失敗するはず
  - SERVFAILが得られないと、そもそもDNSSEC検証していないか、何か設定間違い



受け入れ可能な応答サイズ確認

- rs.dns-oarc.net. IN TXT

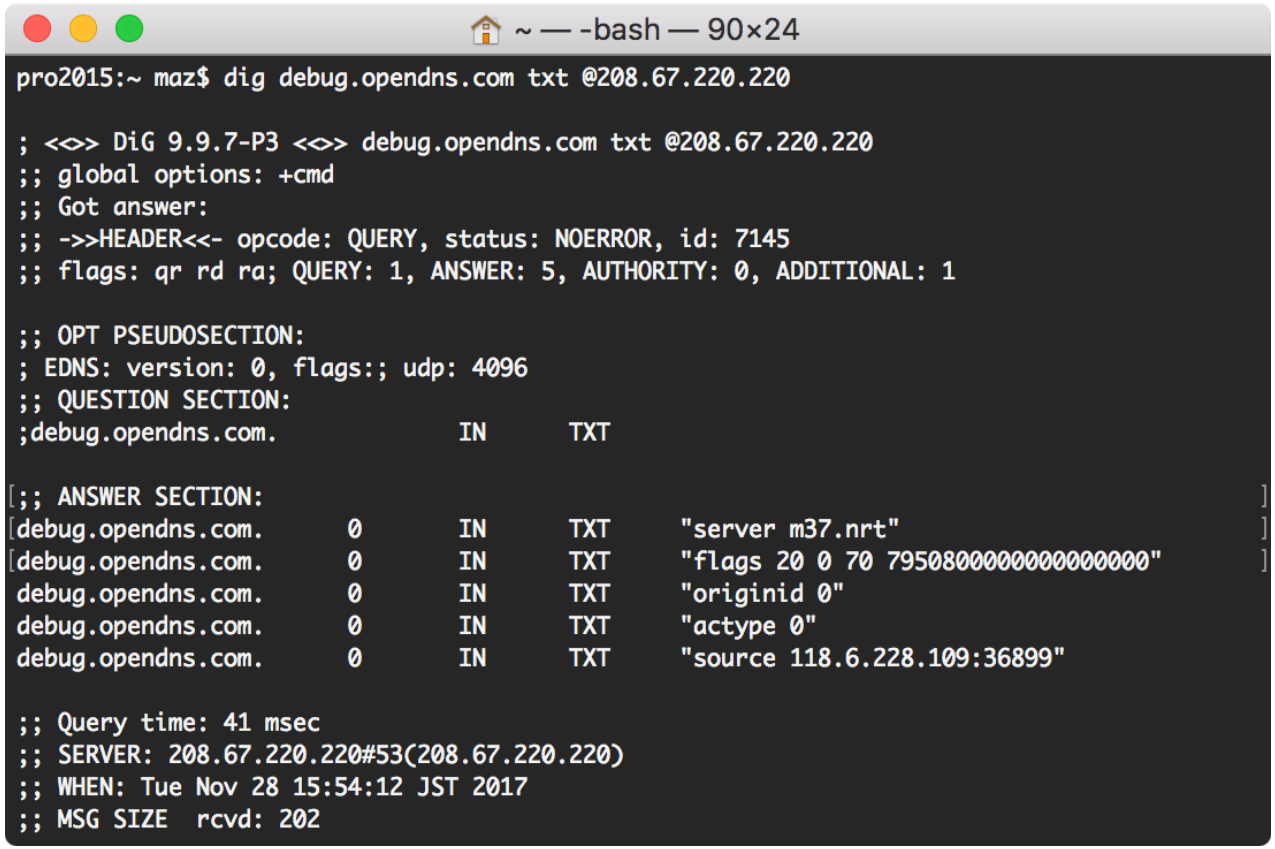


Google Public DNS用

- locations.publicdns.goog. IN TXT
  - Google Public DNSのネームサーバ群で利用しているIPアドレスブロック
- test.dns.google.com. IN TXT
  - Google Public DNSのみが応答するレコードで、“Thanks for using Google Public DNS.” が期待される

OpenDNS用

- debug.opendns.com. IN TXT



まとめ

- 便利なqname色々あります
- 障害切り分け時に便利
- これらは概ね各組織の勝手実装であったり、ネームサーバ設定に依存しているので、挙動や応答が変わることがあります