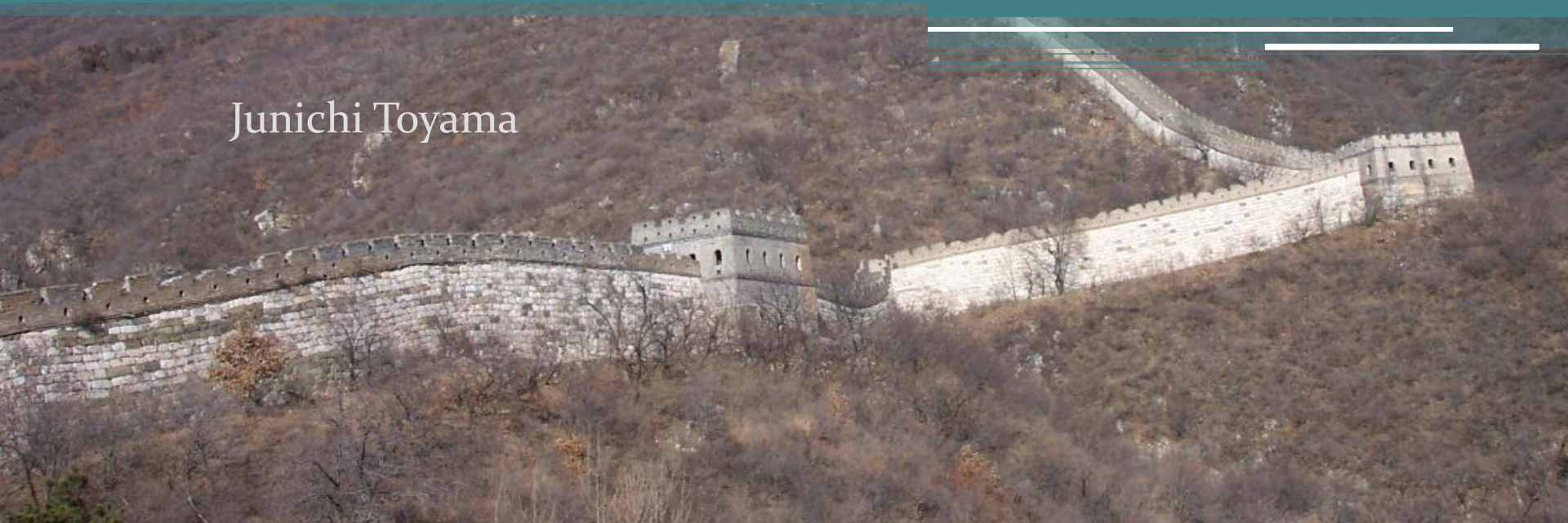
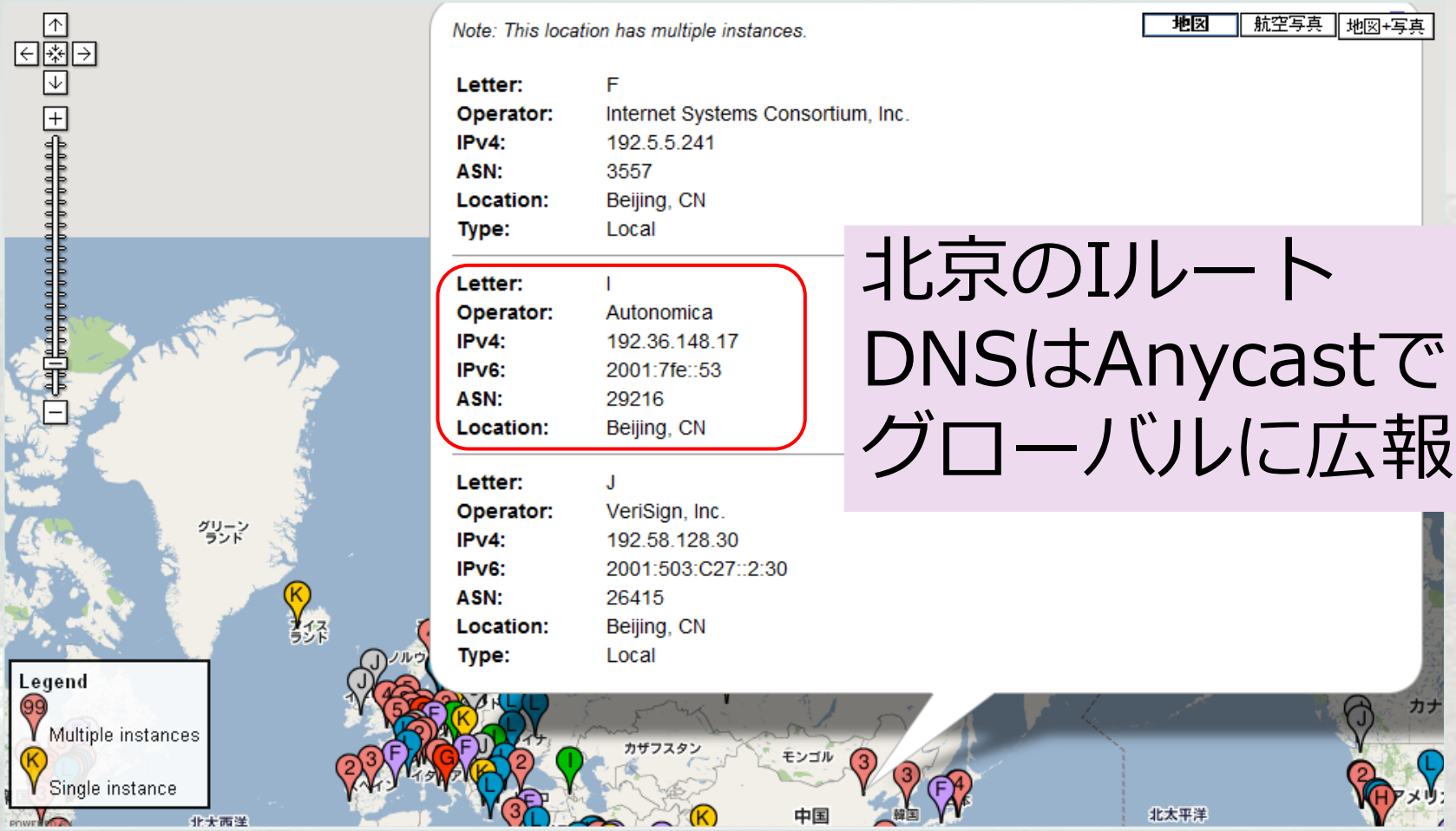
特定の条件下で発生する通信エラーに関する考察
～中国編～



Junichi Toyama

中国・北京のルートDNSサーバ

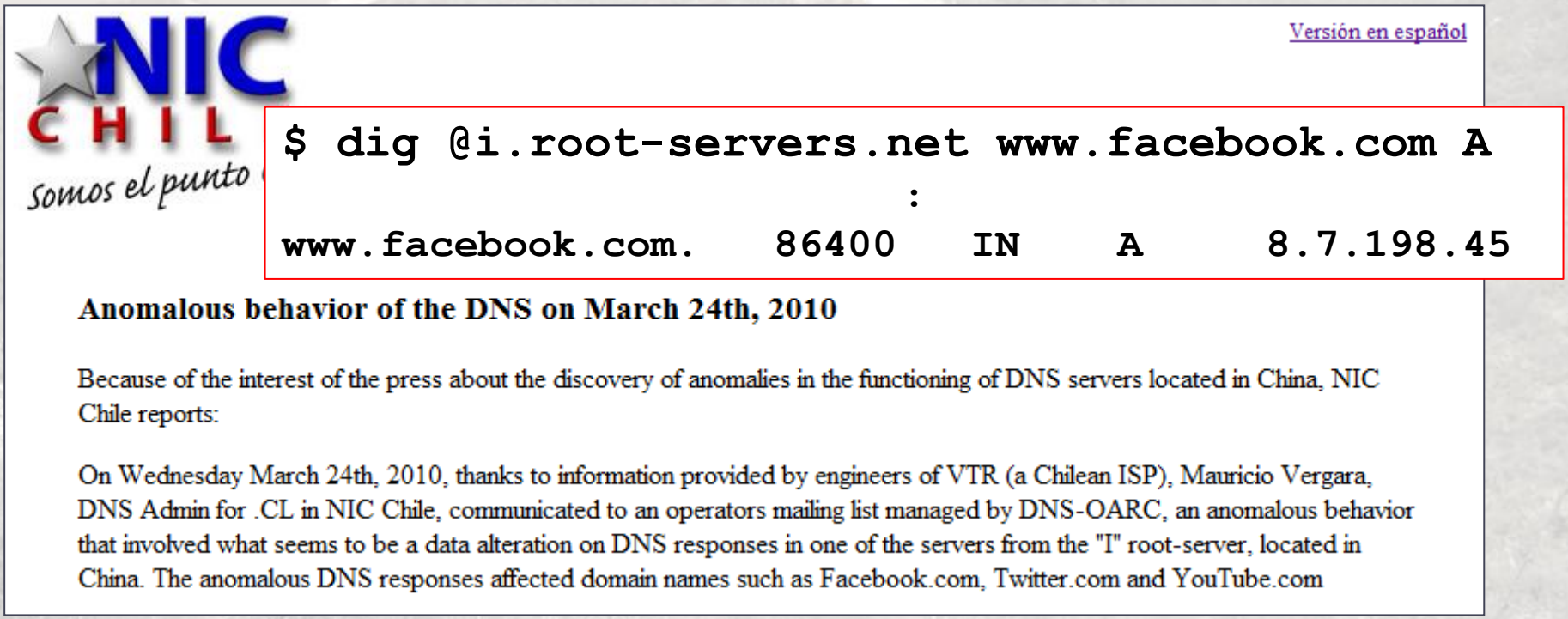


北京のIルートDNSはAnycastでグローバルに広報

出典: http://www.root-servers.org/

2010年3月24日、
中国の"I"ルートサーバが異常動作

FacebookやTwitterなどのドメイン名の問い合わせに対し
異常な応答。チリなどからアクセス不能に。



NIC CHILE
somos el punto

Versión en español

```
$ dig @i.root-servers.net www.facebook.com A
                    :
www.facebook.com.    86400    IN    A      8.7.198.45
```

Anomalous behavior of the DNS on March 24th, 2010

Because of the interest of the press about the discovery of anomalies in the functioning of DNS servers located in China, NIC Chile reports:

On Wednesday March 24th, 2010, thanks to information provided by engineers of VTR (a Chilean ISP), Mauricio Vergara, DNS Admin for .CL in NIC Chile, communicated to an operators mailing list managed by DNS-OARC, an anomalous behavior that involved what seems to be a data alteration on DNS responses in one of the servers from the "I" root-server, located in China. The anomalous DNS responses affected domain names such as Facebook.com, Twitter.com and YouTube.com

出典: http://www.nic.cl/anuncios/2010-03-29-eng.html

I-Root DNS管理者曰く

「Netnod/Autonomicaは、
提供しているルートDNSデータが、
IANAが公開しているデータのまま
であることを100%明言する。」

出典：DNS-OARCのdns-operationsメーリングリストの投稿より要約
https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005349.html

Subject: 中国でのDNS書き換え (facebook, youtube & twitter)

「問題はI-rootに限らない。中国にあるDNSサーバの応答は全部、書き換えられてるようだ。」

出典：DNS-OARCのdns-operationsメーリングリストの投稿より要約
https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005349

緊急対応として経路広報が停止され、解決

…しかし、根本原因は残ったまま

レッツトライ!

.cnのネームサーバのうちの1ノード

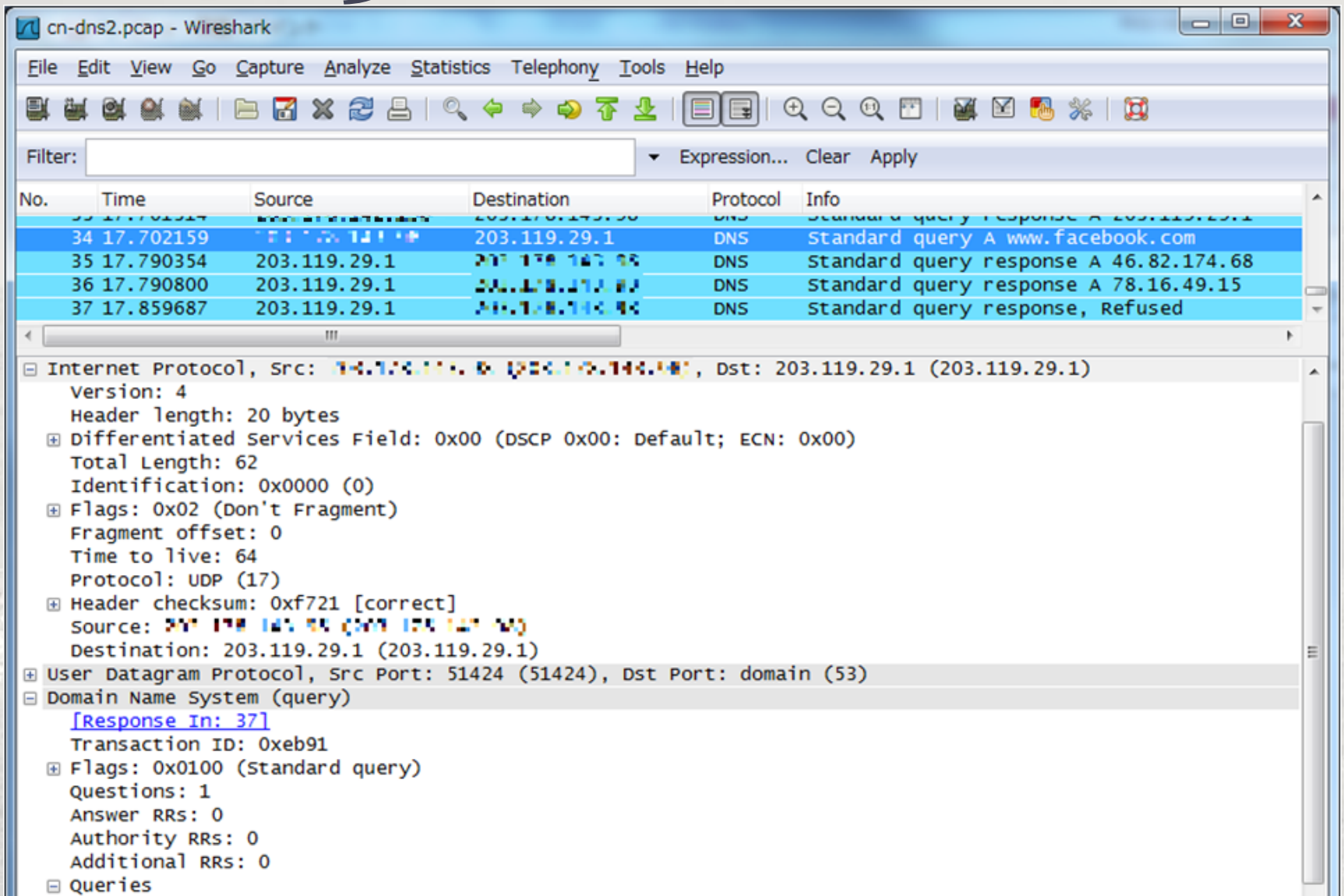
$ dig a www.facebook.com @e.dns.cn

通常のccTLDの権威DNSは、再帰問い合わせに応答しないはずだが…

```
$ dig a www.facebook.com @e.dns.cn

; <<>> DiG 9.2.4 <<>> a www.facebook.com @e.
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43473
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       7405    IN      A       203.98.7.65

;; Query time: 94 msec
;; SERVER: 203.119.29.1#53(203.119.29.1)
;; WHEN: Wed Jan 19 21:24:56 2011
;; MSG SIZE  rcvd: 66
```

www.facebook.com. 7405 IN A 203.98.7.65

1クエリに3個も応答が…



パケットの流れを整理

	Response Time	Transaction ID	TTL	Questions	Answer RRs	Authority RRs	Additional RRs	Answers
クエリ	0ms	0xeb91	64	1	0	0	0	-
応答#1	88.2ms	0xeb91	50	1	1	0	0	A 46.82.174.68
応答#2	88.6ms	0xeb91	78	1	1	0	0	A 78.16.49.15
応答#3	157.5ms	0xeb91	45	1	0	0	0	Refused

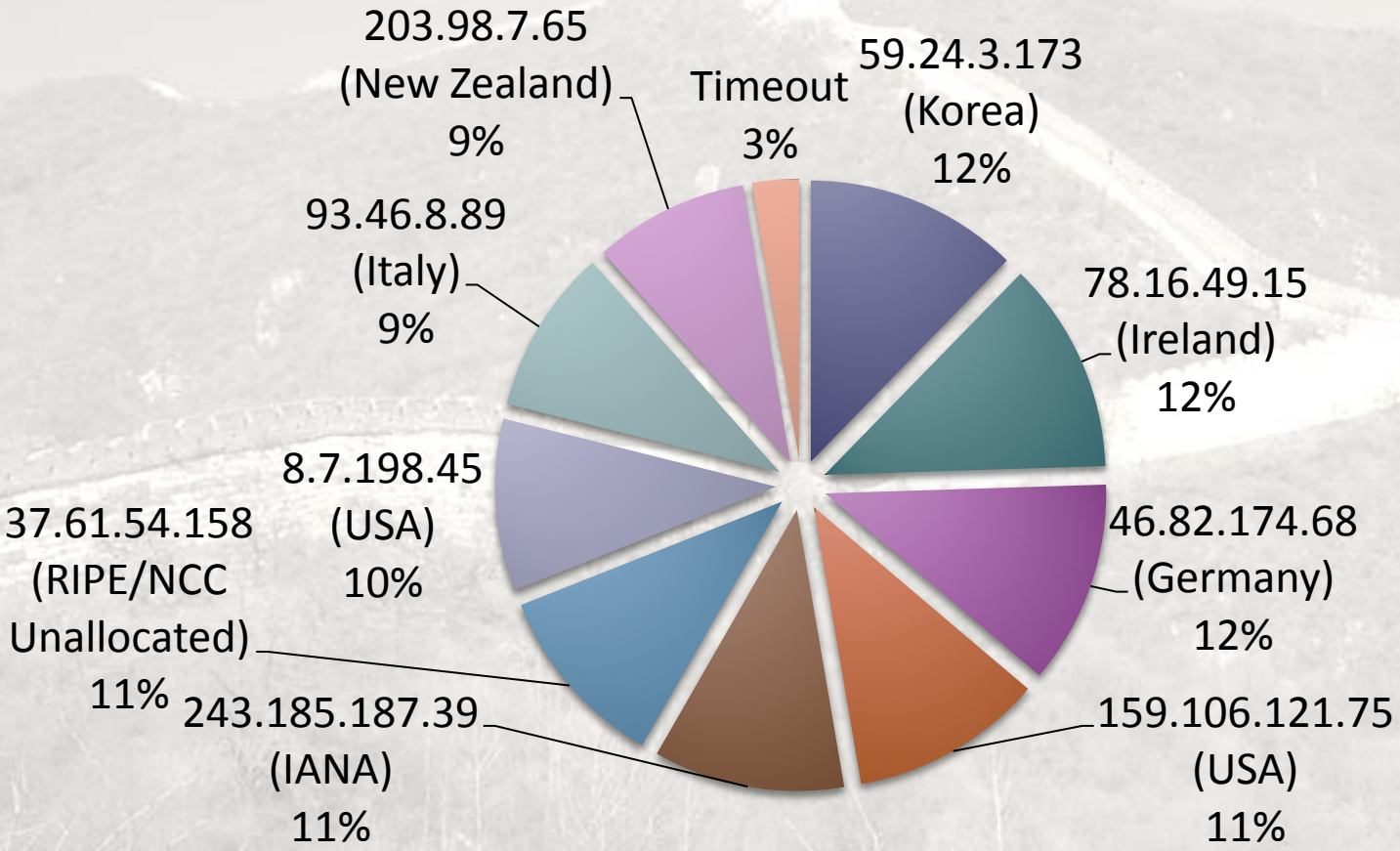
全て同一のTransaction ID,異なるTTL

本物の応答より先に偽物の応答を受信

クエリの応答内容

www.facebook.comに対して1000回クエリを実施

- 応答中のIPアドレスはFacebookとは無関係
  - 9個のIPアドレス群からほぼランダムに選択される

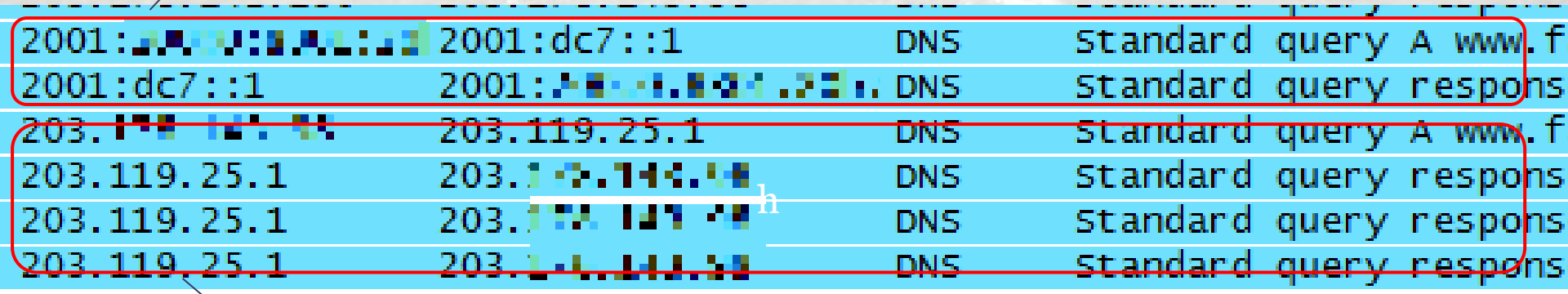


Great FirewallのIPv6対応状況

- a.dns.cnはIPv4/IPv6デュアルスタック

```
$ dig a www.facebook.com -6(-4) @a.dns.cn
```

IPv6でのクエリには1パケットだけが返っている



IPv4でのクエリには合計3パケットが返っている

→現時点ではIPv6には未対応の模様

まとめ

- 通信障害が発生する一部事例を紹介
  - i-rootDNSサーバのインシデント
  - Great firewallの概要
  - DNSポイズニング
- 不自然な通信エラーが発生した場合、Great Firewallが原因の可能性がある

便利なサイト

- Chinese Firewall Test - ViewDNS.info
  - http://viewdns.info/chinesefirewall/
  - 中国国内5箇所からドメイン名の名前解決を実施、DNSポイゾニングが行われているか判別
- Website Test behind the Great Firewall of China
  - http://www.websitepulse.com/help/testtools.china-test.html
  - 中国国内(北京、上海、広州、香港)と中国国外から同じWebページを表示し、サーバの応答を比較

参考文献

- Accidentally Importing Censorship The I-root instance in China
  - http://www.nanog.org/meetings/nanog49/presentations/Tuesday/Madory-I-root-lightning-talk.pdf
- Accidentally Importing Censorship
  - http://www.renesys.com/blog/2010/06/two-strikes-i-root.shtml
- The Great DNS Wall of China
  - http://cs.nyu.edu/~pcw216/work/nds/final.pdf
- Ignoring the Great Firewall of China
  - http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf
- Wikipediaの関連エントリ
  - http://ja.wikipedia.org/wiki/金楯
  - http://ja.wikipedia.org/wiki/中国のネット検閲
  - http://zh.wikipedia.org/zh/%E9%98%B2%E7%81%AB%E9%95%BF%E5%9F%8E
  - http://en.wikipedia.org/wiki/Golden_Shield_Project
  - http://en.wikipedia.org/wiki/Internet_censorship_in_the_People's_Republic_of_China