CS 224(M): Tutorial 3

DNS & SMTP

Name: Dhruv Ilesh Shah **Roll No.**: 150070016

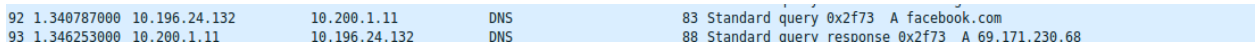
---

1. Find out the domain names and IP addresses of all the root name servers, using dig.

➢ Run the dig command to get the .com servers. Then dig the corresponding A record.

```
dhruv @ {~} says $ dig

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7699
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       516119  IN      NS      a.root-servers.net.
.                       516119  IN      NS      b.root-servers.net.
.                       516119  IN      NS      c.root-servers.net.
.                       516119  IN      NS      d.root-servers.net.
.                       516119  IN      NS      e.root-servers.net.
.                       516119  IN      NS      f.root-servers.net.
.                       516119  IN      NS      g.root-servers.net.
.                       516119  IN      NS      h.root-servers.net.
.                       516119  IN      NS      i.root-servers.net.
.                       516119  IN      NS      j.root-servers.net.
.                       516119  IN      NS      k.root-servers.net.
.                       516119  IN      NS      l.root-servers.net.
.                       516119  IN      NS      m.root-servers.net.

;; Query time: 2 msec
;; SERVER: 10.200.1.11#53(10.200.1.11)
;; WHEN: Fri Aug 12 10:30:16 IST 2016
;; MSG SIZE  rcvd: 228

dhruv @ {~} says $ dig a.root-servers.net.

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> a.root-servers.net.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25234
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;a.root-servers.net.            IN      A

;; ANSWER SECTION:
a.root-servers.net.     603883  IN      A       198.41.0.4

;; Query time: 5 msec
;; SERVER: 10.200.1.11#53(10.200.1.11)
;; WHEN: Fri Aug 12 10:31:04 IST 2016
;; MSG SIZE  rcvd: 52
```

2. Observe a DNS Query/Response when using the dig command.

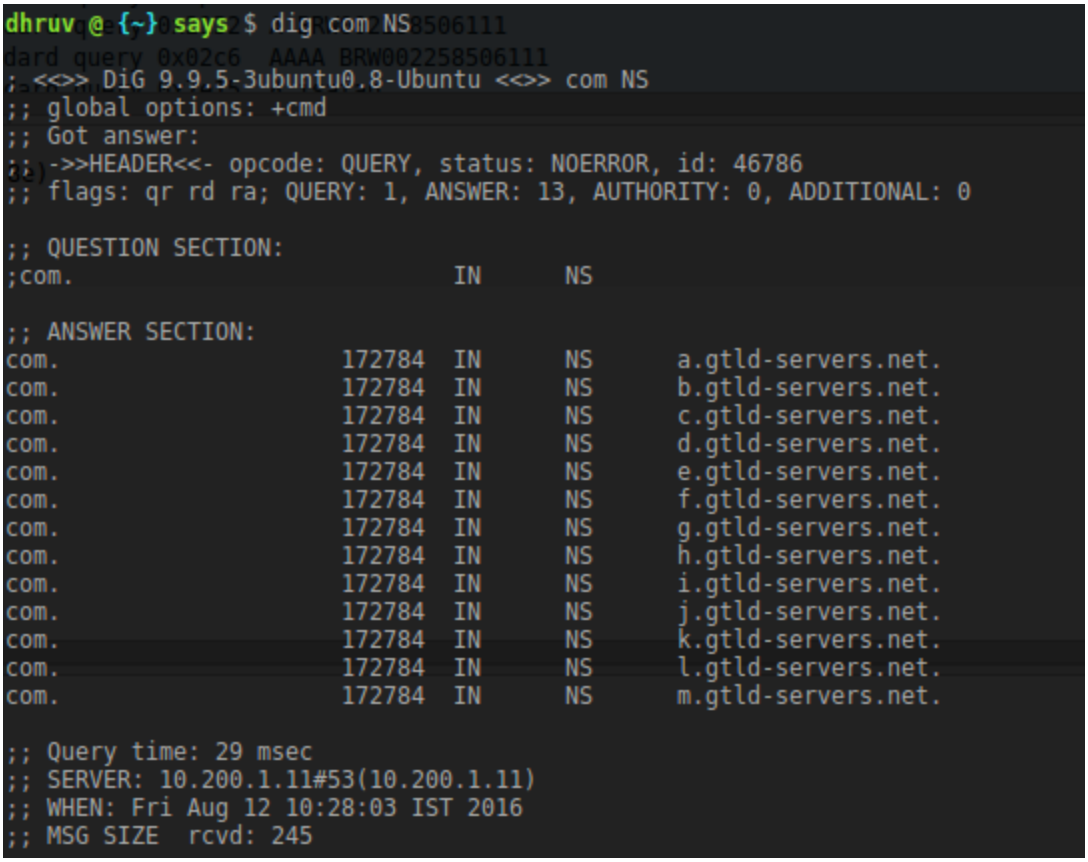


```
92 1.340787000  10.196.24.132   10.200.1.11     DNS   83 Standard query 0x2f73  A facebook.com
93 1.346253000  10.200.1.11     10.196.24.132   DNS   88 Standard query response 0x2f73  A 69.171.230.68
```

3. Observe DNS caching in a browsing session.

➢ When we fire a fresh query, the DNS query is captured in wireshark. But when a similar query is fired again (now, cached), it is not captured. This implies that the cached response stops the browser to fire the same query again.

4. Find out the domain names and IP addresses of some top level domain name servers using dig.



```
dhruv @ {~} says $ dig com NS

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46786
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;com.                           IN      NS

;; ANSWER SECTION:
com.                    172784  IN      NS      a.gtld-servers.net.
com.                    172784  IN      NS      b.gtld-servers.net.
com.                    172784  IN      NS      c.gtld-servers.net.
com.                    172784  IN      NS      d.gtld-servers.net.
com.                    172784  IN      NS      e.gtld-servers.net.
com.                    172784  IN      NS      f.gtld-servers.net.
com.                    172784  IN      NS      g.gtld-servers.net.
com.                    172784  IN      NS      h.gtld-servers.net.
com.                    172784  IN      NS      i.gtld-servers.net.
com.                    172784  IN      NS      j.gtld-servers.net.
com.                    172784  IN      NS      k.gtld-servers.net.
com.                    172784  IN      NS      l.gtld-servers.net.
com.                    172784  IN      NS      m.gtld-servers.net.

;; Query time: 29 msec
;; SERVER: 10.200.1.11#53(10.200.1.11)
;; WHEN: Fri Aug 12 10:28:03 IST 2016
;; MSG SIZE  rcvd: 245
```

```
dhruv @ {~} says $ dig j.gtld-servers.net.

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> j.gtld-servers.net.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10217
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;j.gtld-servers.net.            IN      A

;; ANSWER SECTION:
j.gtld-servers.net.     172796  IN      A       192.48.79.30

;; Query time: 6 msec
;; SERVER: 10.200.1.11#53(10.200.1.11)
;; WHEN: Fri Aug 12 10:41:22 IST 2016
;; MSG SIZE  rcvd: 52
```

5. **Find out the name server for the google.com domain using dig.**

```
dhruv @ {~} says $ dig google.com NS
; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> google.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15360
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      NS

;; ANSWER SECTION:
google.com.             163072  IN      NS      ns2.google.com.
google.com.             163072  IN      NS      ns1.google.com.
google.com.             163072  IN      NS      ns3.google.com.
google.com.             163072  IN      NS      ns4.google.com.

;; Query time: 3 msec
;; SERVER: 10.200.1.11#53(10.200.1.11)
;; WHEN: Fri Aug 12 10:43:54 IST 2016
;; MSG SIZE  rcvd: 100
```

6. Find out the mail server for the gmail.com domain using dig. Is it the same as the mail server for the google.com domain?

```
dhruv @ {~} says $ dig gmail.com MX

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> gmail.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61652
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;gmail.com.                     IN      MX

;; ANSWER SECTION:
gmail.com.              3137    IN      MX      30 alt3.gmail-smtp-in.l.google.com.
gmail.com.              3137    IN      MX      40 alt4.gmail-smtp-in.l.google.com.
gmail.com.              3137    IN      MX      5 gmail-smtp-in.l.google.com.
gmail.com.              3137    IN      MX      10 alt1.gmail-smtp-in.l.google.com.
gmail.com.              3137    IN      MX      20 alt2.gmail-smtp-in.l.google.com.

;; Query time: 2 msec
;; SERVER: 10.200.1.11#53(10.200.1.11)
;; WHEN: Fri Aug 12 10:45:42 IST 2016
;; MSG SIZE  rcvd: 150

dhruv @ {~} says $ dig google.com MX

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> google.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56384
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             433     IN      MX      20 alt1.aspmx.l.google.com.
google.com.             433     IN      MX      50 alt4.aspmx.l.google.com.
google.com.             433     IN      MX      30 alt2.aspmx.l.google.com.
google.com.             433     IN      MX      40 alt3.aspmx.l.google.com.
google.com.             433     IN      MX      10 aspmx.l.google.com.

;; Query time: 22 msec
;; SERVER: 10.200.1.11#53(10.200.1.11)
;; WHEN: Fri Aug 12 10:45:59 IST 2016
;; MSG SIZE  rcvd: 136
```

7. Observe the use of DNS for load balancing of web servers, using dig.

```
dhruv @ {~} says $ dig www.google.com

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49644
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.google.com.         292     IN      A       74.125.130.103
www.google.com.         292     IN      A       74.125.130.104
www.google.com.         292     IN      A       74.125.130.99
www.google.com.         292     IN      A       74.125.130.105
www.google.com.         292     IN      A       74.125.130.106
www.google.com.         292     IN      A       74.125.130.147

;; Query time: 81 msec
;; SERVER: 10.200.1.11#53(10.200.1.11)
;; WHEN: Fri Aug 12 10:49:30 IST 2016
;; MSG SIZE  rcvd: 128
```

```
dhruv @ {~} says $ dig www.google.com

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36379
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.google.com.         248     IN      A       74.125.130.147
www.google.com.         248     IN      A       74.125.130.105
www.google.com.         248     IN      A       74.125.130.106
www.google.com.         248     IN      A       74.125.130.104
www.google.com.         248     IN      A       74.125.130.99
www.google.com.         248     IN      A       74.125.130.103

;; Query time: 4 msec
;; SERVER: 10.200.1.11#53(10.200.1.11)
;; WHEN: Fri Aug 12 10:50:12 IST 2016
;; MSG SIZE  rcvd: 128
```

8. Demonstrate reverse DNS lookup using dig command.

```
dhruv @ {~} says $ dig -x 10.102.1.111


; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> -x 10.102.1.111
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57542
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;111.1.102.10.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
111.1.102.10.in-addr.arpa. 79092 IN     PTR     jeeadv.iitb.ac.in.
111.1.102.10.in-addr.arpa. 79092 IN     PTR     www.jeeadv.iitb.ac.in.
111.1.102.10.in-addr.arpa. 79092 IN     PTR     www2.iitb.ac.in.
111.1.102.10.in-addr.arpa. 79092 IN     PTR     www.climate.iitb.ac.in.
111.1.102.10.in-addr.arpa. 79092 IN     PTR     www.hss.iitb.ac.in.
111.1.102.10.in-addr.arpa. 79092 IN     PTR     www.phy.iitb.ac.in.
111.1.102.10.in-addr.arpa. 79092 IN     PTR     alumni.admin.iitb.ac.in.

;; Query time: 2 msec
;; SERVER: 10.200.1.11#53(10.200.1.11)
;; WHEN: Fri Aug 12 10:52:52 IST 2016
;; MSG SIZE  rcvd: 208
```

9. Which entity in the email system implements the vacation email service? Reason out.

➢ The receiver side email server implements the vacation email service. When the receiver side email server receives an email from the sender, a pre-configured automatic reply is sent.

➢ In particular, RFC 3834 is one such framework

10. What protocol does the user agent of web-mail use? Reason out.

➢ The user agent of the web-mail uses HTTP.

11. Looking at the headers of an email, find out the sequence of mail servers it went through, before reaching your mail server.

```
Return-Path: <eestudents-bounces@sandesh.ee.iitb.ac.in>
X-Original-To: dhruvshah@sandesh.ee.iitb.ac.in
Delivered-To: dhruvshah@sandesh.ee.iitb.ac.in
Received: from sandesh.ee.iitb.ac.in (localhost [127.0.0.1])
     by sandesh.ee.iitb.ac.in (Postfix) with ESMTP id 3BA9D2703DC;
     Mon, 8 Aug 2016 12:23:08 +0530 (IST)
Received: from sandesh.ee.iitb.ac.in (localhost [127.0.0.1])
     by sandesh.ee.iitb.ac.in (Postfix) with ESMTP id 39DA32703DA;
     Mon, 8 Aug 2016 12:23:07 +0530 (IST)
Received: from 10.107.1.1 (proxying for 10.107.63.143)
     by sandesh.ee.iitb.ac.in with HTTP;
     Mon, 8 Aug 2016 12:23:07 +0530 (IST)
```

12. Confirm that the email server mentioned in your email's header matches the MX record corresponding to the domain of your email address.

- As mentioned in the **Received** field of the header, the MX record for the email address must be 10.107.1.1

```
dhruv @ {~} says $ dig bhairav.ee.iitb.ac.in.

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> bhairav.ee.iitb.ac.in.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3240
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;bhairav.ee.iitb.ac.in.          IN      A

;; ANSWER SECTION:
bhairav.ee.iitb.ac.in.  81727   IN      A       10.107.1.1

;; Query time: 0 msec
;; SERVER: 10.200.1.11#53(10.200.1.11)
;; WHEN: Fri Aug 12 11:37:08 IST 2016
;; MSG SIZE  rcvd: 55
```

13. Look through the message headers of a series of messages in a single thread (or conversation), and figure out how the messages are classified as belonging to the same thread.

- Each fresh message has a **Message-ID** embedded in the header file. For every message in response to this message, the header file has a field **In-Reply-To** which can be used to group threads by conversation.

Date: Tue, 02 Aug 2016 18:10:55 +0000
References: <CAKMOprcMvJCFACFdouZV9Co==8pFngjYi9dn6920aKtCegCMhA@mail.gmail.com>
In-Reply-To: <CAKMOprcMvJCFACFdouZV9Co==8pFngjYi9dn6920aKtCegCMhA@mail.gmail.com>
User-Agent: NylasMailer/0.4
Message-Id: <q3md2sez1qztm5svay13r0sr-2147483647@mailer.nylas.com>
X-Inbox-Id: q3md2sez1qztm5svay13r0sr-2147483647
To: Sachin Zachariah <sachinenergyengg@gmail.com>
From: Dhruv Shah <dhruv.ilesh@gmail.com>
Subject: Re: Data for Analysing
Mime-Version: 1.0
Content-Type: multipart/alternative; boundary="4ef46778be0f462faa068181a64de82f"