Lab Exercise 3: DNS & Socket Programming

By John Dao z5258962

Exercise 3: Digging into DNS (marked, include in the lab report)

Full output:

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> www.eecs.berkeley.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34491
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.eecs.berkeley.edu.         IN      A

;; ANSWER SECTION:
www.eecs.berkeley.edu.  53720   IN      CNAME   live-eecs.pantheonsite.io.
live-eecs.pantheonsite.io. 415  IN      CNAME   fe1.edge.pantheon.io.
fe1.edge.pantheon.io.   115     IN      A       23.185.0.1

;; AUTHORITY SECTION:
edge.pantheon.io.       115     IN      NS      ns-644.awsdns-16.net.
edge.pantheon.io.       115     IN      NS      ns-2013.awsdns-59.co.uk.
edge.pantheon.io.       115     IN      NS      ns-233.awsdns-29.com.
edge.pantheon.io.       115     IN      NS      ns-1213.awsdns-23.org.

;; ADDITIONAL SECTION:
ns-233.awsdns-29.com.   125522  IN      A       205.251.192.233
ns-233.awsdns-29.com.   55394   IN      AAAA    2600:9000:5300:e900::1
ns-644.awsdns-16.net.   37953   IN      A       205.251.194.132
ns-1213.awsdns-23.org.  125967  IN      A       205.251.196.189
ns-2013.awsdns-59.co.uk. 120910 IN      A       205.251.199.221
ns-2013.awsdns-59.co.uk. 120910 IN      AAAA    2600:9000:5307:dd00::1

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Oct 13 01:54:32 AEDT 2020
;; MSG SIZE  rcvd: 397

z5258962@vx4:.../z5258962/Desktop$
```

Q1. What is the IP address of www.eecs.berkeley.edu . What type of DNS query is sent to get this answer?

The ip address of the hostname is 23.185.0.1. It is of Type A

Q2. What is the canonical name for the eecs.berkeley web server (i.e. www.eecs.berkeley.edu)? Suggest a reason for having an alias for this server.

The canonical names are **live-eecs.pantheonsite.io** and **fel.edge.pantheon.io**.

A reason for having an alias for this server would be for ease of use as it is would not be very easy for a user to remember such a long canonical name

Question 3. What can you make of the rest of the response (i.e. the details available in the Authority and Additional sections)?

There are **4 name servers** within the authority section as displayed in the full output for the record edge.pantheon.io.

Within the additional section, there are IPs for the name servers listed above in the authority section.

Q4. What is the IP address of the local nameserver for your machine?

The IP address of the local nameserver for my machine is **129.94.242.2**

Question 5. What are the DNS nameservers for the "eecs.berkeley.edu." domain (note: the domain name is eecs.berkeley.edu and not www.eecs.berkeley.edu . This is an example of what is referred to as the apex/naked domain)? Find out their IP addresses? What type of DNS query is sent to obtain this information?

Full output

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29500
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;eecs.berkeley.edu.             IN      A

;; ANSWER SECTION:
eecs.berkeley.edu.      35918   IN      A       23.185.0.1

;; AUTHORITY SECTION:
eecs.berkeley.edu.      75972   IN      NS      adns1.berkeley.edu.
eecs.berkeley.edu.      75972   IN      NS      ns.CS.berkeley.edu.
eecs.berkeley.edu.      75972   IN      NS      adns2.berkeley.edu.
eecs.berkeley.edu.      75972   IN      NS      ns.eecs.berkeley.edu.
eecs.berkeley.edu.      75972   IN      NS      adns3.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     61170   IN      A       169.229.60.61
ns.eecs.berkeley.edu.   82212   IN      A       169.229.60.153
adns1.berkeley.edu.     2858    IN      A       128.32.136.3
adns1.berkeley.edu.     978     IN      AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     8104    IN      A       128.32.136.14
adns2.berkeley.edu.     2858    IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     978     IN      A       192.107.102.142
adns3.berkeley.edu.     2858    IN      AAAA    2607:f140:a000:d::abc

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Oct 13 02:05:42 AEDT 2020
;; MSG SIZE  rcvd: 323

z5258962@vx4:.../z5258962/Desktop$
```

The nameservers for "eecs.berkeley.edu are:

- adns1.berkeley.edu
    - IP (128.32.136.3)

        - IPV6 (2607:f140:ffff:fffe::3)
    - adns2.berkley.edu
        - IP (128.32.136.14)
        - IPV6 (2607:f140:ffff:fffe::e)
    - adns3.berkley.edu
        - IP (192.107.102.142)
        - IPV6 (2607:f140:a000:d::abc)
    - ns.CS.berkeley.edu
        - IP (169:229:60.61)
    - ns.eecs.berkley.edu
        - IP (169.229.60.153)

Q6. What is the DNS name associated with the IP address 111.68.101.54? What type of DNS query is sent to obtain this information?

Full output

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> -x 111.68.101.54
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40231
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;54.101.68.111.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
54.101.68.111.in-addr.arpa. 1070 IN     PTR     webserver.seecs.nust.edu.pk.

;; AUTHORITY SECTION:
101.68.111.in-addr.arpa. 37852  IN      NS      ns2.hec.gov.pk.
101.68.111.in-addr.arpa. 37852  IN      NS      ns1.hec.gov.pk.

;; ADDITIONAL SECTION:
ns1.hec.gov.pk.         1511    IN      A       103.4.93.5
ns2.hec.gov.pk.         1511    IN      A       103.4.93.6

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Oct 13 02:11:51 AEDT 2020
;; MSG SIZE  rcvd: 172

z5258962@vx4:.../z5258962/Desktop$
```

Webserver.seecs.nust.edu.pk

PTR query.

Q7. Run dig and query the CSE nameserver (129.94.242.33) for the mail servers for Yahoo! Mail (again the domain name is yahoo.com, not www.yahoo.com). Did you get an authoritative answer? Why? (HINT: Just because a response contains information in the authoritative part of the DNS response message does not mean it came from an authoritative name server. You should examine the flags in the response to determine the answer)

Full output

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; ANSWER SECTION:
yahoo.com.              313     IN      A       74.6.231.20
yahoo.com.              313     IN      A       74.6.231.21
yahoo.com.              313     IN      A       98.137.11.163
yahoo.com.              313     IN      A       98.137.11.164
yahoo.com.              313     IN      A       74.6.143.25
yahoo.com.              313     IN      A       74.6.143.26

;; AUTHORITY SECTION:
yahoo.com.              32919   IN      NS      ns5.yahoo.com.
yahoo.com.              32919   IN      NS      ns3.yahoo.com.
yahoo.com.              32919   IN      NS      ns1.yahoo.com.
yahoo.com.              32919   IN      NS      ns2.yahoo.com.
yahoo.com.              32919   IN      NS      ns4.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          27357   IN      A       68.180.131.16
ns1.yahoo.com.          42084   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          44784   IN      A       68.142.255.16
ns2.yahoo.com.          67834   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          281     IN      A       27.123.42.42
ns3.yahoo.com.          281     IN      AAAA    2406:8600:f03f:1f8::1003
ns4.yahoo.com.          39219   IN      A       98.138.11.157
ns5.yahoo.com.          6039    IN      A       202.165.97.53
ns5.yahoo.com.          6039    IN      AAAA    2406:2000:ff60::53

;; Query time: 0 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Tue Oct 13 02:14:37 AEDT 2020
;; MSG SIZE  rcvd: 416
```

No. There was no authoritative answer. This is due to there being no AA flags, indicating that the CSE server has no authority on the control of the Yahoo domain.

Q8. Repeat the above (i.e. Question 7) but use one of the nameservers obtained in Question 5. What is the result?

Full output

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @adns1.berkeley.edu yahoo.com MX
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 11280
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; Query time: 166 msec
;; SERVER: 128.32.136.3#53(128.32.136.3)
;; WHEN: Tue Oct 13 02:19:25 AEDT 2020
;; MSG SIZE  rcvd: 38

z5258962@vx4:.../z5258962/Desktop$
```

Query returned Refused status. There was no AA flag either.

Q9. Obtain the authoritative answer for the mail servers for Yahoo! mail. What type of DNS query is sent to obtain this information?

Full response

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @ns1.yahoo.com yahoo.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57604
;; flags: qr aa rd; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 10
;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1272
;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; ANSWER SECTION:
yahoo.com.              1800    IN      A       98.137.11.164
yahoo.com.              1800    IN      A       74.6.143.26
yahoo.com.              1800    IN      A       74.6.143.25
yahoo.com.              1800    IN      A       74.6.231.21
yahoo.com.              1800    IN      A       74.6.231.20
yahoo.com.              1800    IN      A       98.137.11.163

;; AUTHORITY SECTION:
yahoo.com.              172800  IN      NS      ns2.yahoo.com.
yahoo.com.              172800  IN      NS      ns1.yahoo.com.
yahoo.com.              172800  IN      NS      ns5.yahoo.com.
yahoo.com.              172800  IN      NS      ns4.yahoo.com.
yahoo.com.              172800  IN      NS      ns3.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          1209600 IN      A       68.180.131.16
ns2.yahoo.com.          1209600 IN      A       68.142.255.16
ns3.yahoo.com.          1800    IN      A       27.123.42.42
ns4.yahoo.com.          1209600 IN      A       98.138.11.157
ns5.yahoo.com.          86400   IN      A       202.165.97.53
ns1.yahoo.com.          86400   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          86400   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          1800    IN      AAAA    2406:8600:f03f:1f8::1003
ns5.yahoo.com.          86400   IN      AAAA    2406:2000:ff60::53

;; Query time: 145 msec
;; SERVER: 68.180.131.16#53(68.180.131.16)
;; WHEN: Tue Oct 13 02:21:53 AEDT 2020
;; MSG SIZE  rcvd: 416
```

The use of one of the nameservers (in this case ns1.yahoo.com) which is an authoritative name server will return an authoritative answer (AA)

Q10. In this exercise you simulate the iterative DNS query process to find the IP address of your machine (e.g. lyre00.cse.unsw.edu.au). If you are using VLAB Then find the IP address of one of the following: lyre00.cse.unsw.edu.au, lyre01.cse.unsw.edu.au, drum00.cse.unsw.edu.au or drum01.cse.unsw.edu.au. First, find the name server (query type NS) of the "." domain (root domain). Query this nameserver to find the authoritative name server for the "au." domain. Query this second server to find the authoritative nameserver for the "edu.au." domain. Now query this nameserver to find the authoritative nameserver for "unsw.edu.au". Next query the nameserver of unsw.edu.au to find the authoritative name server of cse.unsw.edu.au. Now query the nameserver of cse.unsw.edu.au to find the IP address of your host. How many DNS servers do you have to query to get the authoritative answer?

Full Path taken

Dig NS -> a.root-servers.net (198.41.0.4)
Dig @198.41.0.4 lyre00.cse.unsw.edu.au -> a.au (58.65.254.73)
Dig @58.65.254.73 lyre00.cse.unsw.edu.au -> q.au (65.22.196.1)
Dig @65.22.196.1 lyre00.cse.unsw.edu.au -> ns1.unsw.edu.au (129.94.0.192)
Dig @129.94.0.192 lyre00.cse.unsw.edu.au -> maestro.orchestra.cse.unsw.edu.au (129.94.242.33)
Dig @129.94.242.33 lyre00.cse.unsw.edu.au -> 129.94.210.20

A total of 5 requests were taken. A transcript of all commands (including wrong commands) taken can be found in the TAR.

Question 11. Can one physical machine have several names and/or IP addresses associated with it?

Yes. A machine can have several names and/or IP addresses associated with it.

Exercise 4: A Simple Web Server (Marked, submit your code)

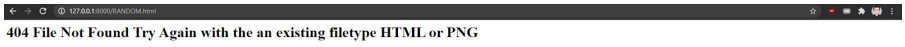
PYTHON START

```
λ python WebServer.py 8000
Webserver on 127.0.0.1:8000 is ready to recieve transmission
```

http://127.0.0.1:8000/myimage.png

http://127.0.0.1:8000/index.html (HTML INDEX WAS BLANK.)

http://127.0.0.1:8000/RANDOM.html



Screenshot of source code. Also included as jpg WITH PYTHON FILE

WebServer.py

D: > code > COMP3331 > lab3 > WebServer.py > ...

```python
# A simple Webserver by John Dao z5258962
from socket import *
import sys

if (len(sys.argv) > 2):
    raise ValueError ("Improper usage")

port = int(sys.argv[1])

serverSocket = socket(AF_INET, SOCK_STREAM)

# binds port onto local host and creates server socket
serverSocket.bind(('127.0.0.1', port))

# Enable server to listen for connection requests
serverSocket.listen(1)
print("Webserver on 127.0.0.1:" + str(port) + " is ready to recieve transmission\n")

while (1):
    # attempts to get data from client
    connectionSocket, addr = serverSocket.accept()
    message = connectionSocket.recv(1024)

    try:
        filename = message.decode().split(" ")[1][1:]
        with open(filename,'rb') as file:
            data = file.read()
            file.close()
        # file successfully recieved
        connectionSocket.send(("HTTP/1.1 200 OK \r\n").encode())

        # sending data after getting its type
        if 'png' in str(filename):
            connectionSocket.send(b'Content-Type: image/png \r\n\r\n')
        else:
            connectionSocket.send(b'Content-Type: image/png \r\n\r\n')
        connectionSocket.send(data)
        connectionSocket.close()

    except IOError:
        # Error wrong file/file not found
        connectionSocket.send(("HTTP/1.1 404 File Not Found \r\n").encode())
        connectionSocket.send("Content-Type: text/html \r\n\r\n".encode())
        connectionSocket.send("<html><h1>404 File Not Found Try Again with the an existing filetype HTML or PNG</h1></html>".encode())
        connectionSocket.close()

```