**Lab 5: DNS [45 points]**

Due: 4/30/2022

**Objectives:** Gain a hands-on understanding of how to work with the DNS protocol by:

1. Creating programs that investigate DNS servers
2. Investigating the *dig* tool with Wireshark

For this lab you’ll be writing programs in Python using the *dns* package with the *resolver* class and *query* function to do DNS lookups. To use this package you’ll need to have the *dnspython* package installed in your environment then you should be able to use:

import dns

from dns import resolver

# DNS Programs

1. Write a Python program (with comments) to determine the IP address of a user-provided domain name. [5 points]  
     
   Sample Output:  
   What FQDN should I look up? cs.millersville.edu  
   IP of cs.millersville.edu is 166.66.86.12
2. Write a Python program (with comments) to determine the MX record and preference number for a user-provided domain name. Keep in mind, it’s possible to have multiple MX records for a single domain so your solution will need to loop through the results. [10 points]  
     
   Sample Output:  
   What domain should I check the MX record for? millersville.edu  
   The MX for millersville.edu is: millersville-edu.mail.protection.outlook.com. The preference number # is 0
3. What does the preference number from question #2 indicate in an MX record? [2 points]

**Indicates in what order the records should be used. The lower the number, the higher the priority.**

1. Write a Python program (with comments) to determine the A, AAAA (if available), MX, NS, SOA, and TXT records for a user-provided domain name. The *dns* package will raise an exception for A and AAAA queries with no response. [10 points]  
     
   Sample Output:  
   What domain should I query? millersville.edu  
   millersville.edu. A 166.66.85.3  
   millersville.edu. MX millersville-edu.mail.protection.outlook.com.  
   millersville.edu. NS ns3-01.azure-dns.org.  
   millersville.edu. NS ns4-01.azure-dns.info.  
   millersville.edu. NS ns1-01.azure-dns.com.  
   millersville.edu. NS ns2-01.azure-dns.net.  
   millersville.edu. SOA ns1-01.azure-dns.com. azuredns-hostmaster.microsoft.com.  
   millersville.edu. TXT "status-page-domain-verification=rj8n788r8q95"  
   millersville.edu. TXT "facebook-domain-verification=1g50tszgoounf52grdxei6eknidjqd"  
   millersville.edu. TXT "docusign=c2556d31-53e6-4b14-b3d0-946397116f6a"  
   millersville.edu. TXT "docusign=3491eacb-a18d-4921-ba79-7c90bbf8768d"  
   millersville.edu. TXT "amazonses:vhqQjHyx3OVf20qXgm4HjtUgdnQ6viV7brKsoHyvlSg="  
   millersville.edu. TXT "adobe-idp-site-verification=3498a319-f150-403a-a553-461dd389805a"  
   millersville.edu. TXT "00y2dMYhvUKLzMNFeFzjnaHYAmKTrDJace0l/4YhkvA5nv6ypEFhCYYMnxDFj6iByfBRK3cq7ZU5bIixPKFLhA=="  
   millersville.edu. TXT "v=spf1 include:verifymyfafsa.com include:stspg-customer.com include:servers.mcsv.net include:spf.protection.outlook.com include:a.\_spf.brightspace.com include:spf.constantcontact.com ip4:192.254.121.248 ip4:199.231.134.73" "/32 ip4:209.143.65.64/26 ip4:13.89.184.95 ip4:176.31.145.254 ip4:199.244.78.23 ip4:199.244.78.224 ip4:205.235.80.96/27 ip4:148.51.134.96/27 ip4:148.51.134.128/26 ip4:205.235.89.0/27 ip4:205.235.89.96/27 ip4:205.235.89.128/26 ip4:166.66.86.75 ~all"
2. What does the SOA record type represent? [2 points]  
   **Stores information/metadata about the domain such as the email address of the administrator and when the domain was last updated.**
3. Many large domains have TXT records with verification strings in them (you can see these in the sample output from question #5 above for facebook, docusign, etc. What is the purpose of these verification TXT entries? [2 points]

**TXT provides a way to connect text with a domain. Typically used for spam prevention and similar cases**

# Investigating the *dig* tool with Wireshark

For the following questions you’ll be using Wireshark and the *dig* tool to issue DNS requests and observe the responses. *Dig* is a Linux command-line utility so you can use it from a Linux command-line or the MacOS Terminal.  
  
Recall from class that the **root** DNS servers are named from a-m. I will be using the IP address for a.root-servers.net in my example so choose **any other** root server to use.

1. Look up the IP address of one of the root servers other than a.root-servers.net using the *dig* tool. The syntax is: *dig <hostname>* What server did you choose and what is the IP address? [1 point]

**h.root-servers.net**

**198.97.190.53**

1. In the second column of the output you should see the number 172800. What does this number represent and what does it mean? [2 points]

**TTL: How long to cache a query answer before requesting a new one**

1. *Dig* can query a specific nameserver using the syntax: *dig @<IP address> <hostname>*.  
   Example: **dig @198.41.0.4** [**www.millersville.edu**](http://www.millersville.edu/)  
     
   Run the dig command above for [www.millersville.edu](http://www.millersville.edu/) specifying the IP address of the root server you looked up after the @ sign. Provide a screenshot of your output. [1 point]

; <<>> DiG 9.16.20 <<>> @198.97.190.53 www.millersville.edu

; (1 server found)

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60273

;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

;; QUESTION SECTION:

;www.millersville.edu. IN A

;; AUTHORITY SECTION:

edu. 172800 IN NS a.edu-servers.net.

edu. 172800 IN NS b.edu-servers.net.

edu. 172800 IN NS c.edu-servers.net.

edu. 172800 IN NS d.edu-servers.net.

edu. 172800 IN NS e.edu-servers.net.

edu. 172800 IN NS f.edu-servers.net.

edu. 172800 IN NS g.edu-servers.net.

edu. 172800 IN NS h.edu-servers.net.

edu. 172800 IN NS i.edu-servers.net.

edu. 172800 IN NS j.edu-servers.net.

edu. 172800 IN NS k.edu-servers.net.

edu. 172800 IN NS l.edu-servers.net.

edu. 172800 IN NS m.edu-servers.net.

;; ADDITIONAL SECTION:

a.edu-servers.net. 172800 IN A 192.5.6.30

b.edu-servers.net. 172800 IN A 192.33.14.30

c.edu-servers.net. 172800 IN A 192.26.92.30

d.edu-servers.net. 172800 IN A 192.31.80.30

e.edu-servers.net. 172800 IN A 192.12.94.30

f.edu-servers.net. 172800 IN A 192.35.51.30

g.edu-servers.net. 172800 IN A 192.42.93.30

h.edu-servers.net. 172800 IN A 192.54.112.30

i.edu-servers.net. 172800 IN A 192.43.172.30

j.edu-servers.net. 172800 IN A 192.48.79.30

k.edu-servers.net. 172800 IN A 192.52.178.30

l.edu-servers.net. 172800 IN A 192.41.162.30

m.edu-servers.net. 172800 IN A 192.55.83.30

a.edu-servers.net. 172800 IN AAAA 2001:503:a83e::2:30

b.edu-servers.net. 172800 IN AAAA 2001:503:231d::2:30

c.edu-servers.net. 172800 IN AAAA 2001:503:83eb::30

d.edu-servers.net. 172800 IN AAAA 2001:500:856e::30

e.edu-servers.net. 172800 IN AAAA 2001:502:1ca1::30

f.edu-servers.net. 172800 IN AAAA 2001:503:d414::30

g.edu-servers.net. 172800 IN AAAA 2001:503:eea3::30

h.edu-servers.net. 172800 IN AAAA 2001:502:8cc::30

i.edu-servers.net. 172800 IN AAAA 2001:503:39c1::30

j.edu-servers.net. 172800 IN AAAA 2001:502:7094::30

k.edu-servers.net. 172800 IN AAAA 2001:503:d2d::30

l.edu-servers.net. 172800 IN AAAA 2001:500:d937::30

m.edu-servers.net. 172800 IN AAAA 2001:501:b1f9::30

;; Query time: 13 msec

;; SERVER: 198.97.190.53#53(198.97.190.53)

;; WHEN: Tue Mar 29 21:12:34 EDT 2022

;; MSG SIZE rcvd: 844

1. Run the same dig command from question #7 for google.com and bbc.co.uk. Provide screenshots of your output. [2 points]

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17806

;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 65494

;; QUESTION SECTION:

;bbc.co.uk. IN A

;; ANSWER SECTION:

bbc.co.uk. 300 IN A 151.101.0.81

bbc.co.uk. 300 IN A 151.101.64.81

bbc.co.uk. 300 IN A 151.101.128.81

bbc.co.uk. 300 IN A 151.101.192.81

; <<>> DiG 9.16.20 <<>> google.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41297

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

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 65494

;; QUESTION SECTION:

;google.com. IN A

;; ANSWER SECTION:

google.com. 221 IN A 142.250.176.206

;; Query time: 3 msec

;; SERVER: 127.0.0.53#53(127.0.0.53)

;; WHEN: Tue Mar 29 21:15:46 EDT 2022

;; MSG SIZE rcvd: 55

;; Query time: 13 msec

;; SERVER: 127.0.0.53#53(127.0.0.53)

;; WHEN: Tue Mar 29 21:14:54 EDT 2022

;; MSG SIZE rcvd: 102

1. Look through the output from your commands in questions #9 and #10. Describe at least 2 additional pieces of useful information (other than the one from #8). There are more than 2 useful pieces of information. [2 points]

**Query Time: Time for DNS query to return**

**Port used for DNS request**

1. Open Wireshark and start a capture. Repeat your dig command from question #9 above. Stop the capture. You can filter only DNS traffic by inputting “dns” into the filter bar at the top and hitting Enter. Take a screenshot of your Wireshark window with the “dns” filter applied. [1 point]
2. Select the DNS response in Wireshark. Explore the details of the response by clicking the dropdown arrow next to “Domain Name System” in the packet details window. Provide a screenshot of the of your response with the details section expanded. [2 points]
3. Looking at the details in the expanded DNS section find and describe 3 important pieces of information (there are more than 3). [3 points]