14-740 Homework 1

Liangdong Xu

TOTAL POINTS

94 / 100

QUESTION 1

1 Question 1 4 / 5

- **0 pts** Correct
- **2 pts** Didn't answer whether the path changed in 3 runs.
- **4 pts** Did not report number of routers + change in path
- ✓ **- 1 pts** **Number of routers wrongly counted**
- **2 pts** Did not report number of routers
- **5 pts** Did not mark pages on grade scope. -5 overall penalty
- **1 pts** Did not answer if path changed in single run
- **2 pts** Didn't correctly answer whether the path changed in 3 runs.
- **1 pts** Did not include complete output in the report
- **0.5 pts** Counted end host (the last hop) as a router
- **0.5 pts** Didn't correctly answer whether the path changed in a single run.

There could be more than 30 routers, because the maximum number of hops in traceroute is 30 by default. Question asked to count the number of routers on the path, you could find a destination that is less than 30 hops away, or change the default max hops with the -m option. Also, please also count routers that timed out.

QUESTION 2

2 Question 2 2 / 2

- ✓ **- 0 pts** **Correct**
- **1 pts** Failed to show details and explanations.
- **0 pts** Missed the first ISP network CMU
- **0 pts** Missing ISPs in the answer

QUESTION 3

3 Question 3 2 / 2

- ✓ **- 0 pts** **Correct**

QUESTION 4

4 Question 4 2 / 2

- ✓ **- 0 pts** **Correct**
- **1 pts** Not enough details provided.
- **0.5 pts** Did not mention both use ICMP

QUESTION 5

5 Question 5 5 / 5

- ✓ **- 0 pts** **Correct**
- **5 pts** Screenshots/proof of work missing. Ping simulation not shown
- **1 pts** Didn't answer (implies didn't analyse) the question - do you get the same 5 intermediate machines as your previous traceroute tests?
- **4 pts** TTL Incorrect
- **4 pts** No TTL varied by using -t option to simulate traceroute
- **5 pts** Answer missing!
- **4 pts** Didn't explain -t(TTL), -c(count) options and how to use them (vary -t from 1 to 5). Screenshot/proof of work missing.

QUESTION 6

6 Question 6 2 / 2

- ✓ **- 0 pts** **Correct**

QUESTION 7

7 Question 7 1 / 1

- ✓ **- 0 pts** **Correct**
- **1 pts** Incorrect. @ is the correct command line option

QUESTION 8

8 Question 8 4 / 4

✓ **- 0 pts Correct**

- 3 pts Doesn't mention what -x does / wrong explanation

- 2 pts if you do not use the “-x” option, how would you achieve the same query? - question not answered/wrongly answered

- 1 pts missing example

- 1 pts missing/incorrect answer to question - why does this work?

- 1 pts incorrect/missing answer to question - will it work for all IP address - why/why-not?

- 1 pts Wrong explanation of -x option

- 0.5 pts Did not show the full dig command

- 0.5 pts Insufficient answer to question - why does this work?

QUESTION 9

9 Question 9 3 / 3

✓ **- 0 pts Correct**

- 0.5 pts Didn't made sure that "Additional Information" isn't displayed - use +noadditional

- 1 pts Output not shown

- 1.5 pts Incorrect/Incomplete /missing question: write several lines and comment on why each line was included and what it means

- 0.5 pts Missing explanation of .jp TLD and/or cmu.jp domain nameservers

- 0.5 pts Did now show/explain final CNAME record

- 1 pts Missing explanation of .jp TLD, cmu.jp domain nameservers and CNAME record

QUESTION 10

10 Question 10 6 / 6

✓ **- 0 pts Correct**

- 2 pts Wrongly answered: www-cmu-prod-vip.andrew.cmu.edu is our campus webserver (True). You can look up IP for www.cmu.edu, and then reverse lookup that IP address to verify this claim.

- 2 pts Wrongly answered: you@andrew.cmu.edu email gets sent to andrew-mx-0\[1-6].andrew.cmu.edu (True). Use command `dig andrew.cmu.edu mx`

- 2 pts Wrongly answered: Email to you@cmu.edu was handled by cmu-mx-0\[1-3].andrew.cmu.edu (False). Use command `dig cmu.edu mx`

- 3 pts Outputs not shown

- 0 pts For the third claim, email is actually handled by 0[1-4] servers

- 6 pts Not answered

- 1 pts Answer to the first claim is correct but proof is insufficient. You can look up IP for www.cmu.edu, and then reverse lookup that IP address to verify this claim.

- 1 pts This first claim is true. You can look up IP for www.cmu.edu, and then reverse lookup that IP address to verify this claim.

QUESTION 11

11 Question 11 3 / 3

✓ **- 0 pts Correct**

- 1 pts whois server names not listed, should be: whois.arin.net, whois.ripe.net, whois.apnic.net, whois.lacnic.net, whois.afrinic.net

- 1 pts Geographic location not mentioned.

- 1 pts whois server names incorrect, should be: whois.arin.net, whois.ripe.net, whois.apnic.net, whois.lacnic.net, whois.afrinic.net

- 0.5 pts whois server names not entirely correct, should be: whois.arin.net, whois.ripe.net, whois.apnic.net, whois.lacnic.net, whois.afrinic.net

QUESTION 12

12 Question 12 2 / 2

✓ **- 0 pts Correct**

- 1 pts command line option not mentioned or incorrect. correct answer = -h option

- 1 pts Use of the option not mentioned or incorrect. Main reason to use this option is registration information is not global. RIR databases contain regional registration information. Will need to specify the server for the regional internet registry in order to get the local registration of an organization

- 0 pts Use of the option is partially correct. Main reason to use this option is registration information is not global. RIR databases contain regional registration

information. Will need to specify the server for the regional internet registry in order to get the local registration of an organization

- **2 pts** No answer.
- **2 pts** Incorrect

QUESTION 13

13 Question 13 3 / 3

✓ **- 0 pts Correct**

- **3 pts** wrong/missing answer. Correct answer: 128.2.1.10
- **1 pts** Missing screenshot
- **3 pts** Unanswered

QUESTION 14

14 Question 14 2 / 2

✓ **- 0 pts Correct**

- **0.5 pts** Missing screenshot
- **2 pts** Unanswered
- **1 pts** Missing names of root name servers
- **1 pts** Missing IP addresses of root name servers
- **2 pts** Incorrect

QUESTION 15

15 Question 15 3 / 3

✓ **- 0 pts Correct**

- **3 pts** Did not use dig
- **1 pts** Missing screenshot
- **3 pts** Unanswered
- **3 pts** Did not answer public DNS service, and did not perform reverse lookup or examine trace
- **1 pts** Correct command, but did not answer (public) DNS service
- **2 pts** Did not answer public DNS service

QUESTION 16

16 Question 16 3 / 3

✓ **- 0 pts Correct**

- **3 pts** Incorrect answer. Correct answer: NSCACHE1.NET.CMU.EDU

QUESTION 17

17 Question 17 3 / 3

✓ **- 0 pts Correct**

- **2 pts** Missing proof / proof is insufficient
- **1 pts** wrong/missing explanation of why/why root servers do not support recursion.
- **3 pts** Missing answer
- **3 pts** Incorrect
- **1 pts** Proof is insufficient

QUESTION 18

18 Question 18 5 / 5

✓ **- 0 pts Correct**

- **2 pts** Missing or Incomplete: "Top level name servers for .beer domain"
- **1 pts** Missing/Incorrect : "Organization which owns the name servers", should be Registry Services, LLC. Command: `whois beer`
- **1 pts** Missing/Incorrect: "Technical point of contact", should be TLD Registry Services Technical. Command: `whois beer`
- **1 pts** Missing/Incorrect : "Command used / Output"
- **5 pts** Incorrect
- **5 pts** deducted 5/5 marks for submitting late to gradescope. Overall 10 points have been deducted for submitting late in Q18,19
- **1 pts** Did not use dig/whois to find technical point of contact and organization. Command: `whois beer`
- **5 pts** Did not answer

QUESTION 19

19 Question 19 4 / 5

- **0 pts** Correct
- **1 pts** Did not describe differences between INI and ECE, or description is incorrect and no proof was provided
- **0.5 pts** Missing screenshots (terminal dig command)
- **0.5 pts** Missing screenshots (browser/wireshark)
- **1 pts** IP addresses incorrect/missing, should be 128.2.42.52 and 128.2.131.95
- **1 pts** Did not explain results for INI, or incorrect explanation

✓ **- 1 pts Did not explain results for ECE, or incorrect explanation**

- 0.5 pts Explanation for INI is insufficient (e.g. did not explain HTTP 301 response)

- 0.5 pts Explanation for ECE is insufficient (e.g. did not explain HTTP 302 response)

- 5 pts Incorrect

- 5 pts Not answered

QUESTION 20

20 Question 20 4 / 4

✓ **- 0 pts Correct**

- 4 pts Incorrect

- 4 pts Did not answer

- 1 pts Did not use `whois` command

- 1 pts Did not show how the answer was found

QUESTION 21

21 Question 21 2.5 / 3

- 0 pts Correct

- 3 pts Incorrect

- 1 pts Missing proof/screenshot

- 3 pts Did not answer

✓ **- 0.5 pts Incomplete IP range**

QUESTION 22

22 Question 22 6.5 / 8

- 0 pts Correct

✓ **- 1 pts Part a incorrect :: Not adding `+norecurse`**

- 1 pts Part a incorrect

✓ **- 0.5 pts Part b :: did not add `+norecurse` for each `dig` command**

- 0.5 pts Part b :: did not include all screenshots/output/commands

- 3 pts Part b incorrect/missing

- 2 pts Part c incorrect/missing

- 2 pts Part d incorrect/missing

- 1 pts Did not add +norecurse

- 8 pts Did not answer

QUESTION 23

23 Question 23 8 / 8

✓ **- 0 pts Correct**

- 1.5 pts Part a :: Incorrect

- 1.5 pts Part b :: Incorrect

- 2 pts Part c :: Incorrect

- 1 pts Part c:: Partial Incorrect

- 3 pts Part d :: Incorrect

- 1 pts Part d :: Calculation Error/Missing

- 2 pts Part d :: Missing Math Formula

- 3 pts Missing calculation

- 0 pts Link wrong pages

QUESTION 24

24 Question 24 8 / 8

✓ **- 0 pts Correct**

- 1 pts Part a incorrect, should be d/s

- 0 pts Part a :: incorrect/missing unit

- 1 pts Part b incorrect, should be L/R

- 0 pts Part b :: incorrect/missing unit

- 2 pts Part c incorrect, should be: just leaving Host A

- 1 pts Part c partially incorrect, should be: just leaving Host A

- 2 pts Part d incorrect. If dprop > dtrans (i.e. if d/s > L / R) then the first bit is still in the link. Otherwise, the first bit
has already been received by Host B.

- 1 pts Part d partially incorrect. If dprop > dtrans (i.e. if d/s > L / R) then the first bit is still in the link. Otherwise, the first bit
has already been received by Host B.

- 2 pts Part e incorrect, should be 875km

- 0.5 pts Part e :: Simple math error, should be 875km

- 0.5 pts Part e :: Incorrect units used / Units not written

- 0 pts Failed to link correct pages

- 8 pts No answer.

QUESTION 25

25 Question 25 6 / 8

- 0 pts Correct

- 2 pts Part a, b, c, d, e :: μ calculation is incorrect,

should be 2568 requests/second

- **0.5 pts** Part a :: Incorrect □, should be 950 requests/second
- **0.5 pts** Part a :: Incorrect ρ, should be 0.37
- **0.5 pts** Part a :: Incorrect L, should be 0.587 requests
- **0.5 pts** Part a :: Incorrect Lq, should be 0.217 requests
- **1 pts** Part b :: Incorrect, should be 0.63
- **0.5 pts** Part b :: Minor math error, should be 0.63
- **1 pts** Part c :: Incorrect, should be 0.000351
- **0.5 pts** Part c :: Didn't consider the fact that more than 6 in the queue implies more than 7 in the system. Hence, it should be 1 - ∑(Pn) for n=0 to n=7. Should be 0.000351
- **0.5 pts** Part c :: Calculation error

✓ **- 1 pts Part d :: Incorrect, should be 0.229 ms**

- **0.5 pts** Part d :: Calculation error, should be 0.229 ms

✓ **- 1 pts Part e :: Incorrect, should be 0.618 ms**

- **0.5 pts** Part e :: Calculation error, should be 0.618 ms
- **0.5 pts** Missing or wrong unit. (1s = 1000ms)
- **0 pts** Link wrong pages
- **8 pts** Left Blank

14740 HW1

Liangdong Xu(liangdox@andrew.cmu.edu)

Oct, 2021

PART 1 ICMP TOOLS – TRACEROUTE AND PING

This is the result of the three tests. The tests are performed on baidu.com.

```
liangdox@linux-24:~$ traceroute baidu.com
traceroute to baidu.com (220.181.38.251), 30 hops max, 60 byte packets
 1  POD-D-CYH-VL141.GW.CMU.NET (128.2.13.130)  0.291 ms  0.300 ms  0.337 ms
 2  CORE0-POD-D-CYH.GW.CMU.NET (128.2.0.201)  0.268 ms  0.284 ms  0.312 ms
 3  POD-I-DCNS-CORE0.GW.CMU.NET (128.2.0.194)  34.760 ms  34.766 ms  34.772 ms
 4  * * *
 5  hundredge-0-0-0-28.59.core1.phil.net.internet2.edu (198.71.47.208)  11.303 ms  11.292 ms  11.301 ms
 6  163.253.1.136 (163.253.1.136)  15.052 ms  14.725 ms *
 7  163.253.1.8 (163.253.1.8)  14.708 ms 163.253.1.2 (163.253.1.2)  14.785 ms 163.253.1.8 (163.253.1.8)  14.702 ms
 8  lo-0.8.rtsw.ashb.net.internet2.edu (64.57.20.133)  19.850 ms  18.651 ms  18.727 ms
 9  218.30.54.56 (218.30.54.56)  14.409 ms  18.659 ms  18.606 ms
10  202.97.49.229 (202.97.49.229)  75.908 ms  75.910 ms  75.838 ms
11  202.97.92.17 (202.97.92.17)  239.008 ms  241.630 ms  237.469 ms
12  202.97.12.89 (202.97.12.89)  355.667 ms * *
13  202.97.48.217 (202.97.48.217)  336.656 ms *  336.630 ms
14  36.110.244.26 (36.110.244.26)  337.256 ms  337.361 ms  338.797 ms
15  * * *
16  * * 220.181.17.18 (220.181.17.18)  338.306 ms
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
liangdox@linux-24:~$ ping baidu.com -c 4
PING baidu.com (220.181.38.251) 56(84) bytes of data.
64 bytes from 220.181.38.251 (220.181.38.251): icmp_seq=1 ttl=40 time=353 ms
64 bytes from 220.181.38.251 (220.181.38.251): icmp_seq=2 ttl=40 time=353 ms
64 bytes from 220.181.38.251 (220.181.38.251): icmp_seq=3 ttl=40 time=353 ms

--- baidu.com ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 4291ms
rtt min/avg/max/mdev = 352.781/353.159/353.437/0.276 ms
liangdox@linux-24:~$ date
Sun 17 Oct 2021 12:11:10 AM EDT
liangdox@linux-24:~$
```

Fig. 1: First test

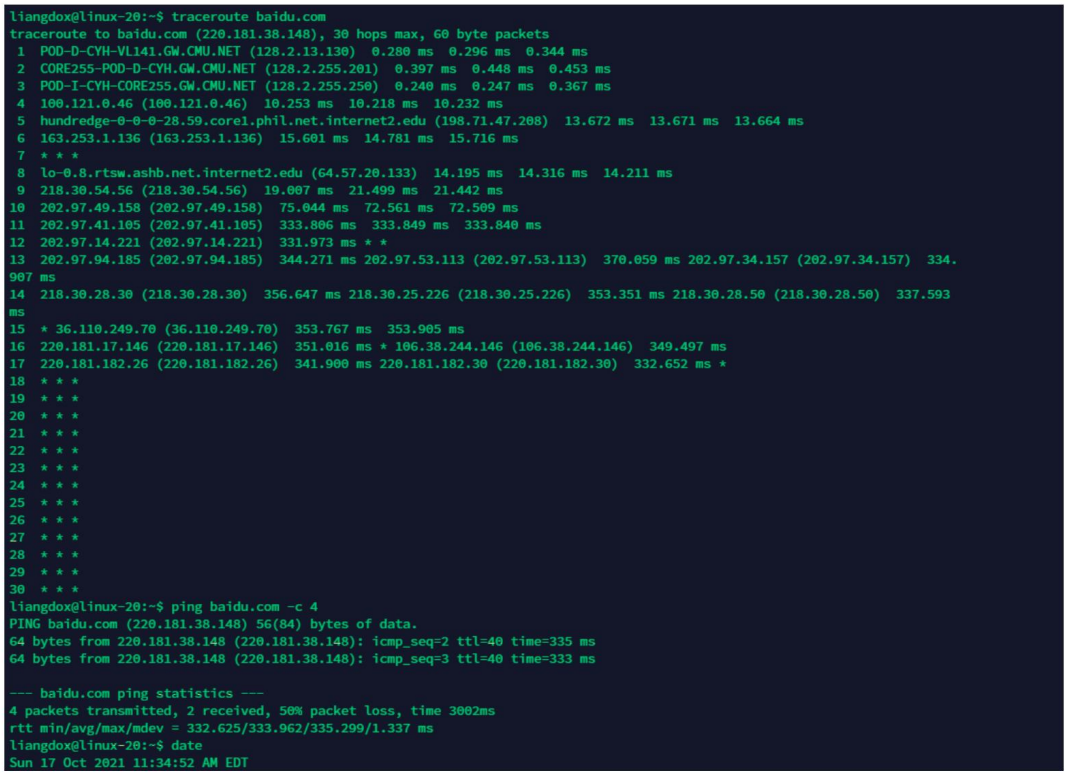

Fig. 2: Second test

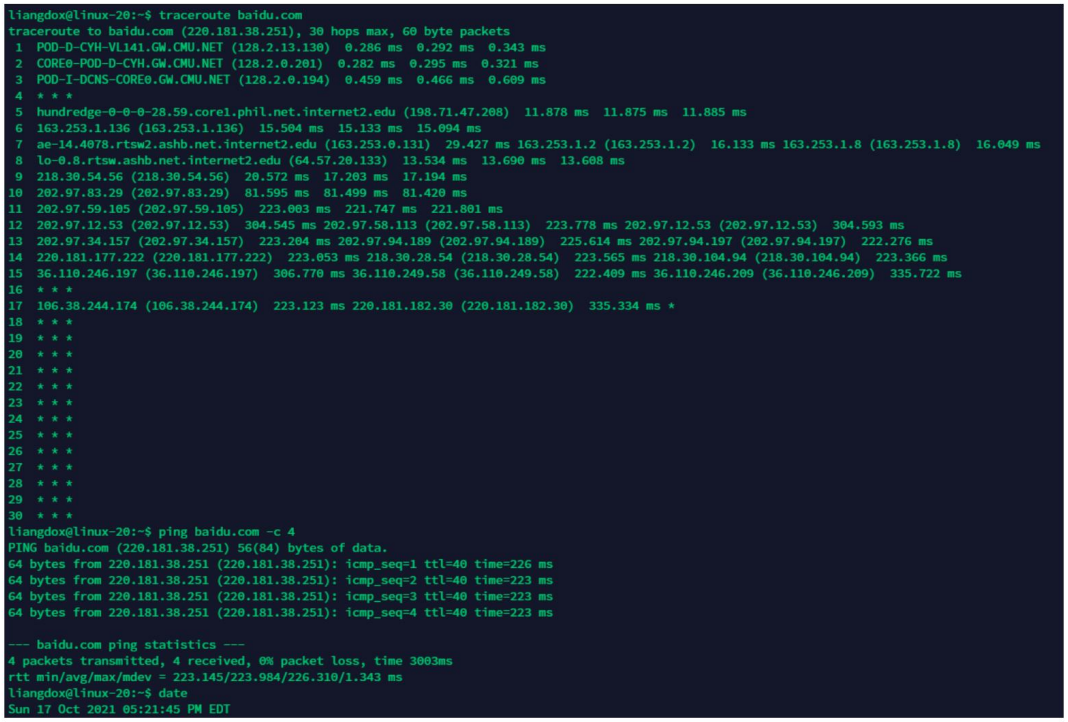

Fig. 3: Third test

question 1.1 Find the number of routers in the path at each of the 3 runs. Did the paths change between runs or even during a single run? (5 points)

Above is the output of the three test. The number of routers are (at least) 16, 17, 17 for the 3 runs. The paths did change between runs. Below is two traceroutes performed during a single run. As can be seen from Fig.4. The paths also changes during a single run

```
traceroute to baidu.com (220.181.38.148), 30 hops max, 60 byte packets
 1  POD-D-CYH-VL141.GW.CMU.NET (128.2.13.130)  0.280 ms  0.296 ms  0.344 ms
 2  CORE255-POD-D-CYH.GW.CMU.NET (128.2.255.201)  0.397 ms  0.448 ms  0.453 ms
 3  POD-I-CYH-CORE255.GW.CMU.NET (128.2.255.250)  0.240 ms  0.247 ms  0.367 ms
 4  100.121.0.46 (100.121.0.46)  10.253 ms  10.218 ms  10.232 ms
 5  hundredge-0-0-0-28.59.core1.phil.net.internet2.edu (198.71.47.208)  13.672 ms  13.671 ms  13.664 ms
 6  163.253.1.136 (163.253.1.136)  15.601 ms  14.781 ms  15.716 ms
 7  * * *
 8  lo-0.8.rtsw.ashb.net.internet2.edu (64.57.20.133)  14.195 ms  14.316 ms  14.211 ms
 9  218.30.54.56 (218.30.54.56)  19.007 ms  21.499 ms  21.442 ms
10  202.97.49.158 (202.97.49.158)  75.044 ms  72.561 ms  72.509 ms
11  202.97.41.105 (202.97.41.105)  333.806 ms  333.849 ms  333.840 ms
12  202.97.14.221 (202.97.14.221)  331.973 ms * *
13  202.97.94.185 (202.97.94.185)  344.271 ms 202.97.53.113 (202.97.53.113)  370.059 ms 202.97.34.157 (202.97.34.157)  334.
907 ms
14  218.30.28.30 (218.30.28.30)  356.647 ms 218.30.25.226 (218.30.25.226)  353.351 ms 218.30.28.50 (218.30.28.50)  337.593
ms
15  * 36.110.249.70 (36.110.249.70)  353.767 ms  353.905 ms
16  220.181.17.146 (220.181.17.146)  351.016 ms * 106.38.244.146 (106.38.244.146)  349.497 ms
17  220.181.182.26 (220.181.182.26)  341.900 ms 220.181.182.30 (220.181.182.30)  332.652 ms *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
liangdox@linux-20:~$ ping baidu.com -c 4
PING baidu.com (220.181.38.148) 56(84) bytes of data.
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=2 ttl=40 time=335 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=3 ttl=40 time=333 ms

--- baidu.com ping statistics ---
4 packets transmitted, 2 received, 50% packet loss, time 3002ms
rtt min/avg/max/mdev = 332.625/333.962/335.299/1.337 ms
liangdox@linux-20:~$ date
Sun 17 Oct 2021 11:34:52 AM EDT
liangdox@linux-20:~$ traceroute baidu.com
traceroute to baidu.com (220.181.38.148), 30 hops max, 60 byte packets
 1  POD-D-CYH-VL141.GW.CMU.NET (128.2.13.130)  0.389 ms  0.375 ms  0.365 ms
 2  CORE255-POD-D-CYH.GW.CMU.NET (128.2.255.201)  0.456 ms  0.562 ms  0.548 ms
 3  POD-I-CYH-CORE255.GW.CMU.NET (128.2.255.250)  0.296 ms  0.286 ms  0.376 ms
 4  100.121.0.46 (100.121.0.46)  10.259 ms  11.280 ms  10.237 ms
 5  hundredge-0-0-0-28.59.core1.phil.net.internet2.edu (198.71.47.208)  13.412 ms  13.402 ms  13.391 ms
 6  163.253.1.136 (163.253.1.136)  15.492 ms  17.010 ms  17.115 ms
 7  163.253.1.2 (163.253.1.2)  15.605 ms * *
 8  lo-0.8.rtsw.ashb.net.internet2.edu (64.57.20.133)  17.390 ms  17.380 ms  17.243 ms
 9  218.30.54.56 (218.30.54.56)  16.725 ms  18.038 ms  18.136 ms
10  202.97.49.158 (202.97.49.158)  70.596 ms  70.586 ms  70.574 ms
11  202.97.41.105 (202.97.41.105)  331.250 ms *  331.208 ms
12  202.97.12.53 (202.97.12.53)  349.720 ms * 202.97.28.125 (202.97.28.125)  351.117 ms
13  202.97.94.185 (202.97.94.185)  348.656 ms 202.97.34.157 (202.97.34.157)  333.873 ms 202.97.34.89 (202.97.34.89)  339.635 ms
14  218.30.104.94 (218.30.104.94)  361.855 ms 218.30.28.30 (218.30.28.30)  357.334 ms 218.30.28.50 (218.30.28.50)  347.075 ms
15  36.110.249.70 (36.110.249.70)  364.114 ms *  351.381 ms
16  * * *
17  106.38.244.150 (106.38.244.150)  357.711 ms 220.181.182.178 (220.181.182.178)  357.793 ms 106.38.244.130 (106.38.244.130)  337.118 ms
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Fig. 4: Second test

1 Question 1 4 / 5

- **0 pts** Correct
- **2 pts** Didn't answer whether the path changed in 3 runs.
- **4 pts** Did not report number of routers + change in path

✓ **- 1 pts** **Number of routers wrongly counted**

- **2 pts** Did not report number of routers
- **5 pts** Did not mark pages on grade scope. -5 overall penalty
- **1 pts** Did not answer if path changed in single run
- **2 pts** Didn't correctly answer whether the path changed in 3 runs.
- **1 pts** Did not include complete output in the report
- **0.5 pts** Counted end host (the last hop) as a router
- **0.5 pts** Didn't correctly answer whether the path changed in a single run.

There could be more than 30 routers, because the maximum number of hops in traceroute is 30 by default. Question asked to count the number of routers on the path, you could find a destination that is less than 30 hops away, or change the default max hops with the -m option. Also, please also count routers that timed out.

question 1.2 Try to identify the number of ISP networks that the traceroute packets pass through from source to destination. Routers with similar names and/or similar IP addresses could be considered as part of the same ISP. (2 points))

Take the path in Fig. 2 as an example.

```
traceroute baidu.com
traceroute to baidu.com (220.181.38.148), 30 hops max, 60 byte packets
 1  POD-D-CYH-VL141.GW.CMU.NET (128.2.13.130)  0.280 ms  0.296 ms  0.344 ms %CMU
 2  CORE255-POD-D-CYH.GW.CMU.NET (128.2.255.201)  0.397 ms  0.448 ms  0.453 ms %CMU
 3  POD-I-CYH-CORE255.GW.CMU.NET (128.2.255.250)  0.240 ms  0.247 ms  0.367 ms %CMU
 4  100.121.0.46 (100.121.0.46)  10.253 ms  10.218 ms  10.232 ms % Reserved IP address
     Shared address space communications between a service provider and its subscribers
 5  hundredge-0-0-0-28.59.core1.phil.net.internet2.edu (198.71.47.208)  13.672 ms  13.671 ms
      13.664 ms %Internet2
 6  163.253.1.136 (163.253.1.136)  15.601 ms  14.781 ms  15.716 ms %Internet2
 7  * * *
 8  lo-0.8.rtsw.ashb.net.internet2.edu (64.57.20.133)  14.195 ms  14.316 ms  14.211 ms %
     Internet2
 9  218.30.54.56 (218.30.54.56)  19.007 ms  21.499 ms  21.442 ms % ChinaNet POP
10  202.97.49.158 (202.97.49.158)  75.044 ms  72.561 ms  72.509 ms % China Telecom
11  202.97.41.105 (202.97.41.105)  333.806 ms  333.849 ms  333.840 ms % China Telecom
12  202.97.14.221 (202.97.14.221)  331.973 ms * * % China Telecom
13  202.97.94.185 (202.97.94.185)  344.271 ms 202.97.53.113 (202.97.53.113)  370.059 ms
    202.97.34.157 (202.97.34.157)  334.907 ms % China Telecom
14  218.30.28.30 (218.30.28.30)  356.647 ms 218.30.25.226 (218.30.25.226)  353.351 ms
    218.30.28.50 (218.30.28.50)  337.593 ms % China Telecom
15  * 36.110.249.70 (36.110.249.70)  353.767 ms  353.905 ms % China Telecom
16  220.181.17.146 (220.181.17.146)  351.016 ms * 106.38.244.146 (106.38.244.146)  349.497
    ms % China Telecom
17  220.181.182.26 (220.181.182.26)  341.900 ms 220.181.182.30 (220.181.182.30)  332.652 ms
    * % China Telecom
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

The first 3 router belongs to CMU ISP. The 4th address is a reserved ip address for sharing communications between a service provider and its subscriber. The 5th, 6th, and 8th router belongs to Internet2. 9th router is a ChinaNet POP router. 10th to 17th router are from China Telecom.

The packet first pass through CMU's network. Then it passed ISP internet2's network. Then it goes to a ChinaNet POP router. It then got transmitted in submarine cable and reached Chinese backbone network. It then goes through ISP China Telecom's network.

2 Question 2 **2 / 2**

✓ **- 0 pts** **Correct**

- 1 pts Failed to show details and explanations.

- 0 pts Missed the first ISP network CMU

- 0 pts Missing ISPs in the answer

question 1.3 Approximately how long did it take to run the entire traceroute command? Why so much longer than the round-trip-time indicated by ping? (2 points)

It takes about 20 seconds to run the entire traceroute command. This is because traceroute send 3 packets that will reach router n for every router n. It does this by sending multiple packets with different TTL. So traceroute is equivalent to running about 90 ping commands. That is why it takes much longer than ping.

question 1.4 What is the relationship between ping and traceroute?

They are both used to test the network connectivity. And they both rely on ICMP response to shoe time and their mechanism is similar.

Differences: Ping is a command common on all platforms. Traceroute is a program implemented by OS and is different on different platforms.

question 1.5 Simulate the first 5 steps of a traceroute query from unix.andrew.cmu.edu to your chosen domain, but only using ping (show your work). You won't have timing information, but do you get the same 5 intermediate machines as your previous traceroute tests? Just to be extra clear, for this question I'm asking you to use ping (perhaps with some command line options) such that the packets getting sent are substantially similar to those that traceroute would have sent. (5 points)

According to traceroute's algorithm, the command I used is

```
ping baidu.com -c 3 -t 1
ping baidu.com -c 3 -t 2
ping baidu.com -c 3 -t 3
ping baidu.com -c 3 -t 4
ping baidu.com -c 3 -t 5
```

in which -c 3 meanins sending 3 packets each time and -t appoints a increasing TTL. The results are shown down below in Fig.5. Fig.6 is a traceroute ran at the same time. As can be seen from the screenshots. They yield the same result for the first 5 hops.

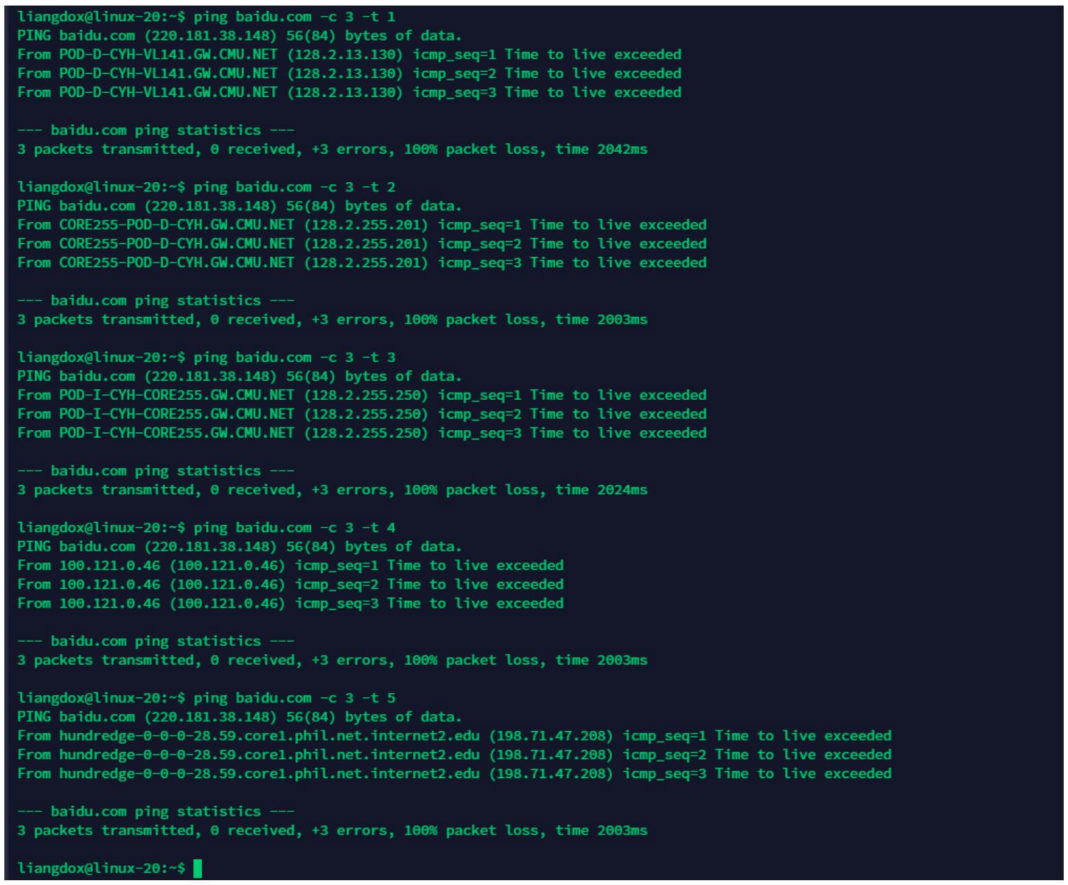

Fig. 5: Using ping to simulate traceroute

3 Question 3 **2 / 2**

✓ **- 0 pts** **Correct**

question 1.3 Approximately how long did it take to run the entire traceroute command? Why so much longer than the round-trip-time indicated by ping? (2 points)

It takes about 20 seconds to run the entire traceroute command. This is because traceroute send 3 packets that will reach router n for every router n. It does this by sending multiple packets with different TTL. So traceroute is equivalent to running about 90 ping commands. That is why it takes much longer than ping.

question 1.4 What is the relationship between ping and traceroute?

They are both used to test the network connectivity. And they both rely on ICMP response to shoe time and their mechanism is similar.

Differences: Ping is a command common on all platforms. Traceroute is a program implemented by OS and is different on different platforms.

question 1.5 Simulate the first 5 steps of a traceroute query from unix.andrew.cmu.edu to your chosen domain, but only using ping (show your work). You won't have timing information, but do you get the same 5 intermediate machines as your previous traceroute tests? Just to be extra clear, for this question I'm asking you to use ping (perhaps with some command line options) such that the packets getting sent are substantially similar to those that traceroute would have sent. (5 points)

According to traceroute's algorithm, the command I used is

```
ping baidu.com -c 3 -t 1
ping baidu.com -c 3 -t 2
ping baidu.com -c 3 -t 3
ping baidu.com -c 3 -t 4
ping baidu.com -c 3 -t 5
```

in which -c 3 meanins sending 3 packets each time and -t appoints a increasing TTL. The results are shown down below in Fig.5. Fig.6 is a traceroute ran at the same time. As can be seen from the screenshots. They yield the same result for the first 5 hops.

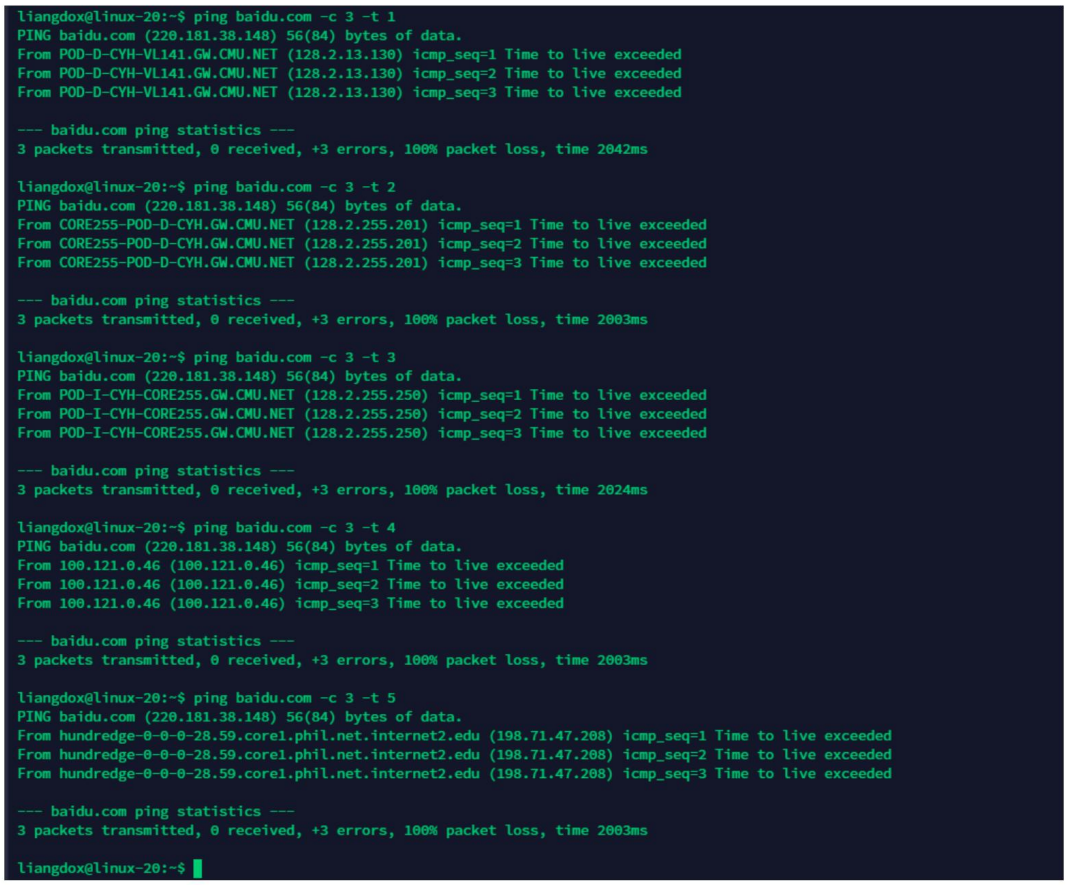

Fig. 5: Using ping to simulate traceroute

4 Question 4 2 / 2

✓ - **0 pts** **Correct**

- **1 pts** Not enough details provided.
- **0.5 pts** Did not mention both use ICMP

question 1.3 Approximately how long did it take to run the entire traceroute command? Why so much longer than the round-trip-time indicated by ping? (2 points)

It takes about 20 seconds to run the entire traceroute command. This is because traceroute send 3 packets that will reach router n for every router n. It does this by sending multiple packets with different TTL. So traceroute is equivalent to running about 90 ping commands. That is why it takes much longer than ping.

question 1.4 What is the relationship between ping and traceroute?

They are both used to test the network connectivity. And they both rely on ICMP response to shoe time and their mechanism is similar.

Differences: Ping is a command common on all platforms. Traceroute is a program implemented by OS and is different on different platforms.

question 1.5 Simulate the first 5 steps of a traceroute query from unix.andrew.cmu.edu to your chosen domain, but only using ping (show your work). You won't have timing information, but do you get the same 5 intermediate machines as your previous traceroute tests? Just to be extra clear, for this question I'm asking you to use ping (perhaps with some command line options) such that the packets getting sent are substantially similar to those that traceroute would have sent. (5 points)

According to traceroute's algorithm, the command I used is

```
ping baidu.com -c 3 -t 1
ping baidu.com -c 3 -t 2
ping baidu.com -c 3 -t 3
ping baidu.com -c 3 -t 4
ping baidu.com -c 3 -t 5
```

in which -c 3 meanins sending 3 packets each time and -t appoints a increasing TTL. The results are shown down below in Fig.5. Fig.6 is a traceroute ran at the same time. As can be seen from the screenshots. They yield the same result for the first 5 hops.

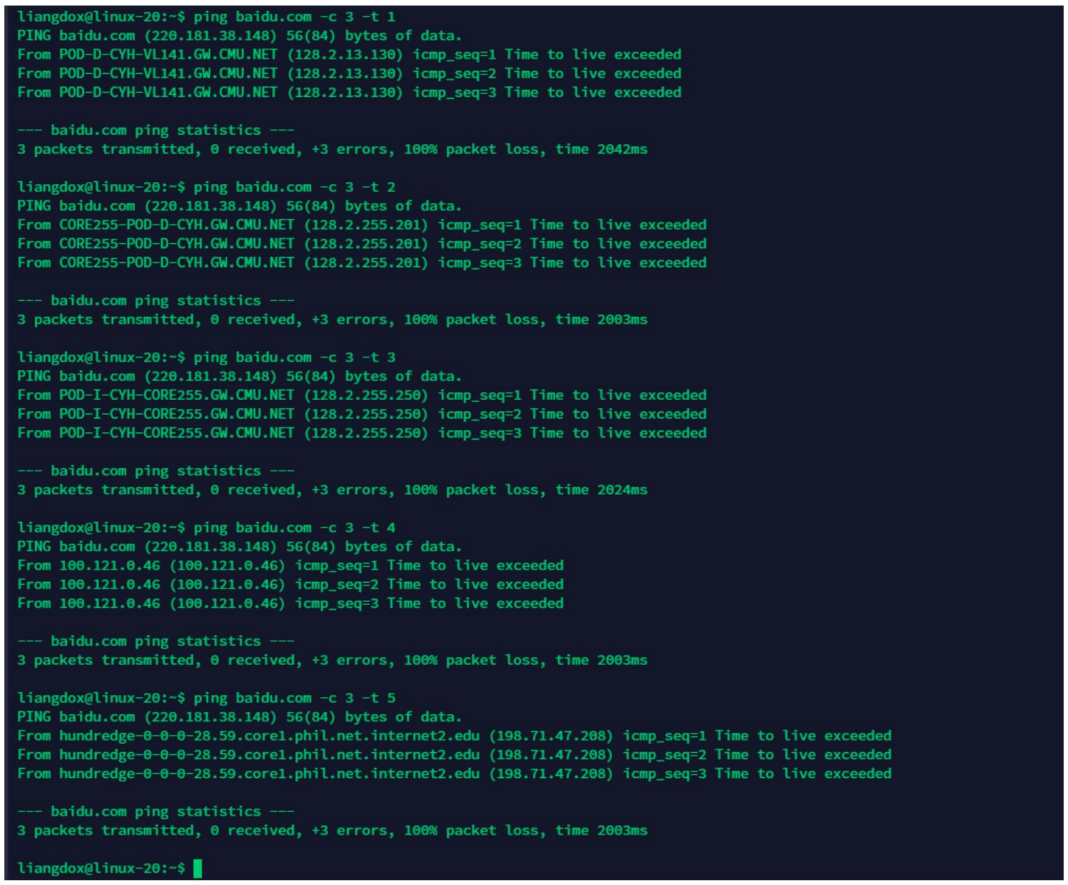

Fig. 5: Using ping to simulate traceroute

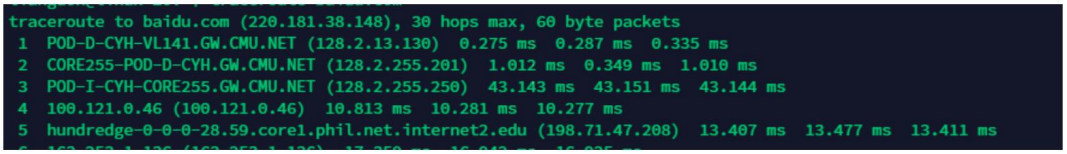

Fig. 6: traceroute's first 5 hops

.

5 Question 5 5 / 5

✓ **- 0 pts** **Correct**

- 5 pts Screenshots/proof of work missing. Ping simulation not shown

- 1 pts Didn't answer (implies didn't analyse) the question - do you get the same 5 intermediate machines as your previous traceroute tests?

- 4 pts TTL Incorrect

- 4 pts No TTL varied by using -t option to simulate traceroute

- 5 pts Answer missing!

- 4 pts Didn't explain -t(TTL), -c(count) options and how to use them (vary -t from 1 to 5). Screenshot/proof of work missing.

PART 2 DIG

question 2.1 A DNS response message comprises four different sections: question, answer, authority and additional. Explain briefly the information each of the sections contains. (2 point)

- question: Contains questions for Name Servers(NS)
- answer: Contains Resource Records(RR) that responds to the questions
- authority: Contains RRs that point toward authority NSs
- additional: Contains RRS that have additional information

question 2.2 What is the command-line option in dig to directly specify the name server to query? (1 point)

The command-line option is @. Using @ before a specific NS to query that NS.

```
dig @NS domain
```

For example, we can run

```
dig @ns7.baidu.com baidu.com
```

The output is shown below.

```
liangdox@linux-20:~$ dig @ns7.baidu.com baidu.com

; <<>> DiG 9.16.1-Ubuntu <<>> @ns7.baidu.com baidu.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27789
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 6
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
baidu.com.              600     IN      A       220.181.38.148
baidu.com.              600     IN      A       220.181.38.251

;; AUTHORITY SECTION:
baidu.com.              86400   IN      NS      ns4.baidu.com.
baidu.com.              86400   IN      NS      ns7.baidu.com.
baidu.com.              86400   IN      NS      ns3.baidu.com.
baidu.com.              86400   IN      NS      ns2.baidu.com.
baidu.com.              86400   IN      NS      dns.baidu.com.

;; ADDITIONAL SECTION:
dns.baidu.com.          600     IN      A       110.242.68.134
ns2.baidu.com.          86400   IN      A       220.181.33.31
ns3.baidu.com.          86400   IN      A       112.80.248.64
ns4.baidu.com.          86400   IN      A       14.215.178.80
ns7.baidu.com.          86400   IN      A       180.76.76.92

;; Query time: 76 msec
;; SERVER: 180.76.76.92#53(180.76.76.92)
;; WHEN: Sun Oct 17 17:20:53 EDT 2021
;; MSG SIZE  rcvd: 240
```

Fig. 7: dig @ns7.baidu.com baidu.com output

6 Question 6 2 / 2

✓ - 0 pts Correct

PART 2 DIG

question 2.1 A DNS response message comprises four different sections: question, answer, authority and additional. Explain briefly the information each of the sections contains. (2 point)

- question: Contains questions for Name Servers(NS)
- answer: Contains Resource Records(RR) that responds to the questions
- authority: Contains RRs that point toward authority NSs
- additional: Contains RRS that have additional information

question 2.2 What is the command-line option in dig to directly specify the name server to query? (1 point)

The command-line option is @. Using @ before a specific NS to query that NS.

```
dig @NS domain
```

For example, we can run

```
dig @ns7.baidu.com baidu.com
```

The output is shown below.

```
liangdox@linux-20:~$ dig @ns7.baidu.com baidu.com

; <<>> DiG 9.16.1-Ubuntu <<>> @ns7.baidu.com baidu.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27789
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 6
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
baidu.com.              600     IN      A       220.181.38.148
baidu.com.              600     IN      A       220.181.38.251

;; AUTHORITY SECTION:
baidu.com.              86400   IN      NS      ns4.baidu.com.
baidu.com.              86400   IN      NS      ns7.baidu.com.
baidu.com.              86400   IN      NS      ns3.baidu.com.
baidu.com.              86400   IN      NS      ns2.baidu.com.
baidu.com.              86400   IN      NS      dns.baidu.com.

;; ADDITIONAL SECTION:
dns.baidu.com.          600     IN      A       110.242.68.134
ns2.baidu.com.          86400   IN      A       220.181.33.31
ns3.baidu.com.          86400   IN      A       112.80.248.64
ns4.baidu.com.          86400   IN      A       14.215.178.80
ns7.baidu.com.          86400   IN      A       180.76.76.92

;; Query time: 76 msec
;; SERVER: 180.76.76.92#53(180.76.76.92)
;; WHEN: Sun Oct 17 17:20:53 EDT 2021
;; MSG SIZE  rcvd: 240
```

Fig. 7: dig @ns7.baidu.com baidu.com output

7 Question 7 **1 / 1**

✓ **- 0 pts** **Correct**

- 1 pts Incorrect. @ is the correct command line option

question 2.3 What does the "-x" command-line option in dig do? If you do not use the "-x" option, how would you achieve the same query? Use an example to illustrate. Why does this work? Will it work for EVERY IP address? Why or why not? (4 points)

The "-x" command-line option in dig performs simplified reverse lookups for mapping addresses to names.

According to the manual, the -x command lookup for a name like 94.2.0.192.in-addr.arpa and sets the query type and class to PTR and IN respectively. We can do it without using -x too. We just need to reverse the address and append ".in-addr.arpa". This will be the name we use. Then we also need to set the query type to PTR and set class to IN. So the command we use is

```
dig PTR <reversed ip>.in-addr.arpa
```

notice the class is not set using -c because -c's default class is IN.

For example, if we want to look up 8.8.8.6 with -x option.

```
dig 8.8.8.6 -x
```

We can also use

```
dig PTR 6.8.8.8.in-addr.arpa
```

```
liangdox@linux-20:~$ dig PTR 6.8.8.8.in-addr.arpa

; <<>> DiG 9.16.1-Ubuntu <<>> PTR 6.8.8.8.in-addr.arpa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 58656
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
8.8.8.in-addr.arpa.     60      IN      SOA     ns1.google.com. dns-admin.google.com. 403574256 900 900 1800 60

;; Query time: 28 msec
;; SERVER: 128.2.1.10#53(128.2.1.10)
;; WHEN: Sun Oct 17 17:50:08 EDT 2021
;; MSG SIZE  rcvd: 109

liangdox@linux-20:~$ dig -x 8.8.8.6

; <<>> DiG 9.16.1-Ubuntu <<>> -x 8.8.8.6
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 28326
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
8.8.8.in-addr.arpa.     58      IN      SOA     ns1.google.com. dns-admin.google.com. 403574256 900 900 1800 60

;; Query time: 0 msec
;; SERVER: 128.2.1.10#53(128.2.1.10)
;; WHEN: Sun Oct 17 17:50:10 EDT 2021
;; MSG SIZE  rcvd: 109

liangdox@linux-20:~$
```

Fig. 8: two outputs

This works because PTR records that supports reverse DNS lookup is maintained. In this example, <reversed ip>.in-addr.arpa contains the matching PTR record. So reverse DNS lookup can work.

However, this will not work for all IP address. Because having a matching PTR record is a recommendation instead of an strict requirement. Not all IP addresses have a reverse entry.

8 Question 8 4 / 4

✓ **- 0 pts** **Correct**

- 3 pts Doesn't mention what -x does / wrong explanation

- 2 pts if you do not use the “-x” option, how would you achieve the same query? - question not answered/wrongly answered

- 1 pts missing example

- 1 pts missing/incorrect answer to question - why does this work?

- 1 pts incorrect/missing answer to question - will it work for all IP address - why/why-not?

- 1 pts Wrong explanation of -x option

- 0.5 pts Did not show the full dig command

- 0.5 pts Insufficient answer to question - why does this work?

question 2.4 Use the +trace option to query the CNAME record for www.cmuj.jp. Also, make sure "Additional Information" isn't displayed. Copy the output into your report. Then, write several sentences interpreting the various parts of the output, commenting on why each line was included and what it means. (3 points)

The command used is

```
dig  www.cmuj.jp +trace +noadditional
```

The result is

```
; <<>> DiG 9.16.1-Ubuntu <<>> www.cmuj.jp +trace +noadditional
;; global options: +cmd
.                       141666  IN      NS      a.root-servers.net.
.                       141666  IN      NS      h.root-servers.net.
.                       141666  IN      NS      e.root-servers.net.
.                       141666  IN      NS      f.root-servers.net.
.                       141666  IN      NS      g.root-servers.net.
.                       141666  IN      NS      c.root-servers.net.
.                       141666  IN      NS      d.root-servers.net.
.                       141666  IN      NS      b.root-servers.net.
.                       141666  IN      NS      m.root-servers.net.
.                       141666  IN      NS      i.root-servers.net.
.                       141666  IN      NS      k.root-servers.net.
.                       141666  IN      NS      l.root-servers.net.
.                       141666  IN      NS      j.root-servers.net.
.                       245114  IN      RRSIG   NS 8 0 518400 20211027170000 20211014160000
    14748 . OSt9ghiFOwIoNx0lVOsN6VW5V7UuEyLxgzIBknWcubtwgFSe6+J4xMWX V2BfDz/
    HFLcb0HVJv8n8VR9KbmwyYwyJo3Lk7dRGzhGODXbG1JDiARpo
    cPVKSna4vXj5EKocvqbSajOCZfqRhFNwA4TnPWrU0u1Vl37h0a2p0lnv
    RJeKR6wbNrwWGczPuwB6vKFfjvkKKqQY+s8qBzbboTu+jsgZ9yREybyH Xh1sp/0DCNnn81b+y+7qk/
    dJPZCzldn5ngWQA2wjVX0MSZWhe6uMZ0ih lZoxm3jH4Rf3H+
    ULu075fLSmiLTtXgSMMnZiO5ksRMDnafIwXockRdxp uPkcEw==
;; Received 1097 bytes from 128.2.1.10#53(128.2.1.10) in 0 ms

jp.                     172800  IN      NS      d.dns.jp.
jp.                     172800  IN      NS      f.dns.jp.
jp.                     172800  IN      NS      h.dns.jp.
jp.                     172800  IN      NS      e.dns.jp.
jp.                     172800  IN      NS      c.dns.jp.
jp.                     172800  IN      NS      a.dns.jp.
jp.                     172800  IN      NS      b.dns.jp.
jp.                     172800  IN      NS      g.dns.jp.
jp.                     86400   IN      DS      46369 8 2 39
    F054DCB3EC1E93D8AE6D8F1AAAD91794055EA36895045FAF6F65F0 2FEBC579
jp.                     86400   IN      RRSIG   DS 8 1 86400 20211030170000 20211017160000
    14748 . WxW7UTT7oKal0JET9xlhUoT2vmfOjM0poafaywWVL7mPjYi25rYhAGVu
    Rkg9JT998awCZm80T8TA7BrtkmmQJ76jTB/RYVHlQ99CFZ8nEH5QswIu obXtIvas0TA2wB/3
    PWO40LfjOb3QPsLAafgFdxENwpqoQ5/wMSeXTsPO R91G/9Zw9El/ARwO3bhQJoNNnIb+22
    gpJOZkA2v5cdWmN9Fv8jtmRgzB EEoc08Ht/ZYFn/Gfp6oCiwjtgPjslpiUcQHKA1AaBEMa+Go4M5RfDEgK
    Sc7uodl49MfLKFyQFwjmNQraK12iI9sgvFol7y3XYh46RuwjA+BMF70z wUscAQ==
;; Received 863 bytes from 192.36.148.17#53(i.root-servers.net) in 32 ms

cmuj.jp.                86400   IN      NS      mwns1.customer.ne.jp.
cmuj.jp.                86400   IN      NS      mwns2.customer.ne.jp.
IK6DN8V5HA34KDOCOKIIQ65KR905DGBR.jp. 900 IN NSEC3 1 1 8 2F502B2552
    IKMA0N1QI2LN69OB2GNUP3CMSV7GSVSR NS SOA RRSIG DNSKEY NSEC3PARAM
IK6DN8V5HA34KDOCOKIIQ65KR905DGBR.jp. 900 IN RRSIG NSEC3 8 2 900 20211115174508
    20211016174508 49539 jp. fV5S7u/WRDdH8q+u4mJx2tV94EDUuEb0+uYGMqoS/T6Wis4zwQ0rTZVS
    q57jDffJb/3F/x+h3ijDUIDvSAydfiuJDQIVCb3WYLpSih4BmxxQy/hz
    uqHYQ48ERvIyMtSAOg6fm1hsR02HBc09U0O9otTOjHvi4ZbhvVPUfzqn at4=
3OOIQ3F0F9LFGQ9VJJVPJMNBSV8QIVC1.jp. 900 IN NSEC3 1 1 8 2F502B2552 3
    P3VAMRHB3783N8UK3KFU44UBB7EER5H NS DS RRSIG
3OOIQ3F0F9LFGQ9VJJVPJMNBSV8QIVC1.jp. 900 IN RRSIG NSEC3 8 2 900 20211115174508
    20211016174508 49539 jp. PC3GgxQHl697BwtHar8fLl1PyWXMcQGQokEIATwW0xk+M6aWwnS/+rpe +
    L4c12NE5J/Na14hSTLUHzUN9wOQmWz7GFOemNLtUvG1irSiAf9OdczY RrJNvU09c8dRaksxRrHaChfoL/
    yQvp5G1+a59nFaI64r28LB3MC143gG VgU=
;; Received 613 bytes from 210.138.175.244#53(d.dns.jp) in 20 ms

www.cmuj.jp.            3600    IN      CNAME   cmuj.jp.
cmuj.jp.                3600    IN      A       60.43.157.130
cmuj.jp.                3600    IN      NS      mwns1.customer.ne.jp.
cmuj.jp.                3600    IN      NS      mwns2.customer.ne.jp.
;; Received 150 bytes from 202.17.152.183#53(mwns2.customer.ne.jp) in 152 ms
```

The first two line shows the version of the DiG, the command and and the global options that are set.

What is displayed after that shows the root server information received from 128.2.1.10, which is the DNS server CMU's unix machine is using. This part of the output is shown below.

The last line show where the RRs are from, the size of data we received, and the time it took.

All lines before that are RRs the we received from it.

```
.                       141666  IN      NS      a.root-servers.net.
.                       141666  IN      NS      h.root-servers.net.
.                       141666  IN      NS      e.root-servers.net.
.                       141666  IN      NS      f.root-servers.net.
.                       141666  IN      NS      g.root-servers.net.
.                       141666  IN      NS      c.root-servers.net.
.                       141666  IN      NS      d.root-servers.net.
.                       141666  IN      NS      b.root-servers.net.
.                       141666  IN      NS      m.root-servers.net.
.                       141666  IN      NS      i.root-servers.net.
.                       141666  IN      NS      k.root-servers.net.
.                       141666  IN      NS      l.root-servers.net.
.                       141666  IN      NS      j.root-servers.net.
.                       245114  IN      RRSIG   NS 8 0 518400 20211027170000 20211014160000
    14748 . OSt9ghiFOwIoNx0lVOsN6VW5V7UuEyLxgzIBknWcubtwgFSe6+J4xMWX V2BfDz/
    HFLcb0HVJv8n8VR9KbmwyYwyJo3Lk7dRGzhGODXbG1JDiARpo
    cPVKSna4vXj5EKocvqbSajOCZfqRhFNwA4TnPWrU0u1Vl37h0a2p0lnv
    RJeKR6wbNrwWGczPuwB6vKFfjvkKKqQY+s8qBzbboTu+jsgZ9yREybyH Xh1sp/0DCNnn81b+y+7qk/
    dJPZCzldn5ngWQA2wjVX0MSZWhe6uMZ0ih lZoxm3jH4Rf3H+
    ULu075fLSmiLTtXgSMMnZiO5ksRMDnafIwXockRdxp uPkcEw==
;; Received 1097 bytes from 128.2.1.10#53(128.2.1.10) in 0 ms
```

The question is then sent to i.root-servers.net. i.root-servers.net replied with a list of TLD NSs for .jp. as shown below.

The last line show where the RRs are from, the size of data we received, and the time it took.

All lines before that are RRs the we received from it.

```
jp.                     172800  IN      NS      d.dns.jp.
jp.                     172800  IN      NS      f.dns.jp.
jp.                     172800  IN      NS      h.dns.jp.
jp.                     172800  IN      NS      e.dns.jp.
jp.                     172800  IN      NS      c.dns.jp.
jp.                     172800  IN      NS      a.dns.jp.
jp.                     172800  IN      NS      b.dns.jp.
jp.                     172800  IN      NS      g.dns.jp.
jp.                     86400   IN      DS      46369 8 2 39
    F054DCB3EC1E93D8AE6D8F1AAAD91794055EA36895045FAF6F65F0 2FEBC579
jp.                     86400   IN      RRSIG   DS 8 1 86400 20211030170000 20211017160000
    14748 . WxW7UTT7oKal0JET9xlhUoT2vmfOjM0poafaywWVL7mPjYi25rYhAGVu
    Rkg9JT998awCZm80T8TA7BrtkmmQJ76jTB/RYVHlQ99CFZ8nEH5QswIu obXtIvas0TA2wB/3
    PWO40LfjOb3QPsLAafgFdxENwpqoQ5/wMSeXTsPO R91G/9Zw9El/ARwO3bhQJoNNnIb+22
    gpJOZkA2v5cdWmN9Fv8jtmRgzB EEoc08Ht/ZYFn/Gfp6oCiwjtgPjslpiUcQHKA1AaBEMa+Go4M5RfDEgK
    Sc7uodl49MfLKFyQFwjmNQraK12iI9sgvFol7y3XYh46RuwjA+BMF70z wUscAQ==
;; Received 863 bytes from 192.36.148.17#53(i.root-servers.net) in 32 ms
```

The question is then sent to TLD NS d.dns.jp. It replies with a list of authoritative NS as shown below.

The last line show where the RRs are from, the size of data we received, and the time it took.

All lines before that are RRs the we received from it.

```
cmuj.jp.                86400   IN      NS      mwns1.customer.ne.jp.
cmuj.jp.                86400   IN      NS      mwns2.customer.ne.jp.
IK6DN8V5HA34KDOCOKIIQ65KR905DGBR.jp. 900 IN NSEC3 1 1 8 2F502B2552
    IKMA0N1QI2LN69OB2GNUP3CMSV7GSVSR NS SOA RRSIG DNSKEY NSEC3PARAM
IK6DN8V5HA34KDOCOKIIQ65KR905DGBR.jp. 900 IN RRSIG NSEC3 8 2 900 20211115174508
    20211016174508 49539 jp. fV5S7u/WRDdH8q+u4mJx2tV94EDUuEb0+uYGMqoS/T6Wis4zwQ0rTZVS
    q57jDffJb/3F/x+h3ijDUIDvSAydfiuJDQIVCb3WYLpSih4BmxxQy/hz
    uqHYQ48ERvIyMtSAOg6fm1hsR02HBc09U0O9otTOjHvi4ZbhvVPUfzqn at4=
3OOIQ3F0F9LFGQ9VJJVPJMNBSV8QIVC1.jp. 900 IN NSEC3 1 1 8 2F502B2552 3
    P3VAMRHB3783N8UK3KFU44UBB7EER5H NS DS RRSIG
3OOIQ3F0F9LFGQ9VJJVPJMNBSV8QIVC1.jp. 900 IN RRSIG NSEC3 8 2 900 20211115174508
    20211016174508 49539 jp. PC3GgxQHl697BwtHar8fLl1PyWXMcQGQokEIATwW0xk+M6aWwnS/+rpe +
    L4c12NE5J/Na14hSTLUHzUN9wOQmWz7GFOemNLtUvG1irSiAf9OdczY RrJNvU09c8dRaksxRrHaChfoL/
    yQvp5G1+a59nFaI64r28LB3MC143gG VgU=
;; Received 613 bytes from 210.138.175.244#53(d.dns.jp) in 20 ms
```

Lastly the question is then sent to authoritative NS mwns2.customer.ne.jp. And we receive a list of RRs containing answer as well as addtional information as shown below

The last line show where the RRs are from, the size of data we received, and the time it took.
All lines before that is a list of RRs containing answer as well as addtional information.

```
1  www.cmuj.jp.            3600    IN      CNAME   cmuj.jp.
2  cmuj.jp.                3600    IN      A       60.43.157.130
3  cmuj.jp.                3600    IN      NS      mwns1.customer.ne.jp.
4  cmuj.jp.                3600    IN      NS      mwns2.customer.ne.jp.
5  ;; Received 150 bytes from 202.17.152.183#53(mwns2.customer.ne.jp) in 152 ms
```

9 Question 9 3 / 3

✓ **- 0 pts Correct**

- 0.5 pts Didn't made sure that "Additional Information" isn't displayed - use +noadditional

- 1 pts Output not shown

- 1.5 pts Incorrect/Incomplete /missing question: write several lines and comment on why each line was included and what it means

- 0.5 pts Missing explanation of .jp TLD and/or cmu.jp domain nameservers

- 0.5 pts Did now show/explain final CNAME record

- 1 pts Missing explanation of .jp TLD, cmu.jp domain nameservers and CNAME record

question 2.5 In lecture 6, I made the following claims. Use dig to verify each one. Make sure to show the command(s) you used and the output produced for each. Then, write a description or annotate the output to show how you know the answer supports or refutes each claim. (6 points)

2.5-a www-cmu-prod-vip.andrew.cmu.edu is our campus webserver

First, I ran

```
dig www.cmu.edu
```

The output is shown below

```
;; ANSWER SECTION:
www.cmu.edu.            21      IN      CNAME   WWW.R53.cmu.edu.
WWW.R53.cmu.edu.        21      IN      A       128.2.42.52
```

Fig. 9: output

It seems that www.cmu.edu have a CNAME record of www.r53.cmu.edu. And the ip address for WWW.R53.cmu.edu is 128.2.42.52. Then I ran

```
dig 128.2.42.52 -x
```

The PTR record show that the host name of 128.2.42.52 is www-cmu-prod-vip.andrew.cmu.edu

```
liangdox@linux-20:~$ dig -x 128.2.42.52

; <<>> DiG 9.16.1-Ubuntu <<>> -x 128.2.42.52
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45078
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
52.42.2.128.in-addr.arpa. 7705  IN      PTR     WWW-CMU-PROD-VIP.ANDREW.CMU.EDU.

;; AUTHORITY SECTION:
42.2.128.in-addr.arpa.  48037   IN      NS      NSAUTH2.NET.CMU.EDU.
42.2.128.in-addr.arpa.  48037   IN      NS      NSAUTH1.NET.CMU.EDU.

;; ADDITIONAL SECTION:
NSAUTH1.NET.CMU.EDU.    52294   IN      A       128.2.1.8
NSAUTH2.NET.CMU.EDU.    57865   IN      A       128.237.148.168

;; Query time: 0 msec
;; SERVER: 128.2.1.10#53(128.2.1.10)
;; WHEN: Sun Oct 17 21:42:43 EDT 2021
;; MSG SIZE  rcvd: 178
```

Fig. 10: output

I also tried

```
telnet www.cmu.edu 80
```

```
liangdox@linux-20:~$ telnet www.cmu.edu 80
Trying 128.2.42.52...
Connected to WWW.R53.cmu.edu.
Escape character is '^]'.
```

Fig. 11: output

And the output(Fig.11) showed that I am connected to www.r53.cmu.edu.

2.5-b you@andrew.cmu.edu email gets sent to andrew-mx-0[1-6].andrew.cmu.edu

In order to get the mail exchanger record. I used

```
dig andrew.cmu.edu MX
```

The ouput is shown below.

As can be seen from the answer section the you@andrew.cmu.edu email is handled by andrew-mx-0[1-6].andrew.cmu.edu.

```
liangdox@linux-20:~$ dig andrew.cmu.edu MX

; <<>> DiG 9.16.1-Ubuntu <<>> andrew.cmu.edu MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3272
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 2, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;andrew.cmu.edu.                        IN      MX

;; ANSWER SECTION:
andrew.cmu.edu.         4218    IN      MX      10 ANDREW-MX-06.andrew.cmu.edu.
andrew.cmu.edu.         4218    IN      MX      10 ANDREW-MX-01.andrew.cmu.edu.
andrew.cmu.edu.         4218    IN      MX      10 ANDREW-MX-02.andrew.cmu.edu.
andrew.cmu.edu.         4218    IN      MX      10 ANDREW-MX-03.andrew.cmu.edu.
andrew.cmu.edu.         4218    IN      MX      10 ANDREW-MX-04.andrew.cmu.edu.
andrew.cmu.edu.         4218    IN      MX      10 ANDREW-MX-05.andrew.cmu.edu.

;; AUTHORITY SECTION:
andrew.cmu.edu.         47263   IN      NS      NSAUTH2.NET.cmu.edu.
andrew.cmu.edu.         47263   IN      NS      NSAUTH1.NET.cmu.edu.

;; ADDITIONAL SECTION:
ANDREW-MX-04.andrew.cmu.edu. 4208 IN    A       128.2.157.7
ANDREW-MX-05.andrew.cmu.edu. 4211 IN    A       128.2.157.8
ANDREW-MX-06.andrew.cmu.edu. 4211 IN    A       128.2.157.74
ANDREW-MX-01.andrew.cmu.edu. 4208 IN    A       128.2.158.83
ANDREW-MX-02.andrew.cmu.edu. 4211 IN    A       128.2.158.85
ANDREW-MX-03.andrew.cmu.edu. 4211 IN    A       128.2.158.87
NSAUTH2.NET.cmu.edu.    57241   IN      A       128.237.148.168
NSAUTH1.NET.cmu.edu.    51670   IN      A       128.2.1.8

;; Query time: 4 msec
;; SERVER: 128.2.1.10#53(128.2.1.10)
;; WHEN: Sun Oct 17 21:53:07 EDT 2021
;; MSG SIZE  rcvd: 393
```

Fig. 12: output

2.5-c Email to you@cmu.edu was handled by cmu-mx-0[1-3].andrew.cmu.edu

Similar to 2.5-b, run

```
dig cmu.edu MX
```

The ouput is shown below.
As can be seen from the answer section the you@cmu.edu email is handled by cmu-mx-0[1-4].andrew.cmu.edu

```
liangdox@linux-20:~$ dig cmu.edu MX

; <<>> DiG 9.16.1-Ubuntu <<>> cmu.edu MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49540
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 3, ADDITIONAL: 8

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

;; ANSWER SECTION:
cmu.edu.                1356    IN      MX      10 CMU-MX-02.ANDREW.cmu.edu.
cmu.edu.                1356    IN      MX      10 CMU-MX-03.ANDREW.cmu.edu.
cmu.edu.                1356    IN      MX      10 CMU-MX-04.ANDREW.cmu.edu.
cmu.edu.                1356    IN      MX      10 CMU-MX-01.ANDREW.cmu.edu.

;; AUTHORITY SECTION:
cmu.edu.                1356    IN      NS      NY-SERVER-03.NET.cmu.edu.
cmu.edu.                1356    IN      NS      NSAUTH1.NET.cmu.edu.
cmu.edu.                1356    IN      NS      NSAUTH2.NET.cmu.edu.

;; ADDITIONAL SECTION:
CMU-MX-04.ANDREW.cmu.edu. 532   IN      A       128.2.157.83
CMU-MX-01.ANDREW.cmu.edu. 7     IN      A       128.2.158.90
CMU-MX-02.ANDREW.cmu.edu. 5     IN      A       128.2.158.91
CMU-MX-03.ANDREW.cmu.edu. 588   IN      A       128.2.157.82
NSAUTH2.NET.cmu.edu.    54374   IN      A       128.237.148.168
NSAUTH1.NET.cmu.edu.    48803   IN      A       128.2.1.8
NY-SERVER-03.NET.cmu.edu. 122   IN      A       38.96.147.4

;; Query time: 4 msec
;; SERVER: 128.2.1.10#53(128.2.1.10)
;; WHEN: Sun Oct 17 22:40:54 EDT 2021
;; MSG SIZE  rcvd: 334
```

Fig. 13: output

10 Question 10 6 / 6

✓ **- 0 pts** **Correct**

- 2 pts Wrongly answered: www-cmu-prod-vip.andrew.cmu.edu is our campus webserver (True). You can look up IP for www.cmu.edu, and then reverse lookup that IP address to verify this claim.

- 2 pts Wrongly answered: you@andrew.cmu.edu email gets sent to andrew-mx-0\[1-6].andrew.cmu.edu (True). Use command `dig andrew.cmu.edu mx`

- 2 pts Wrongly answered: Email to you@cmu.edu was handled by cmu-mx-0\[1-3].andrew.cmu.edu (False). Use command `dig cmu.edu mx`

- 3 pts Outputs not shown

- 0 pts For the third claim, email is actually handled by 0[1-4] servers

- 6 pts Not answered

- 1 pts Answer to the first claim is correct but proof is insufficient. You can look up IP for www.cmu.edu, and then reverse lookup that IP address to verify this claim.

- 1 pts This first claim is true. You can look up IP for www.cmu.edu, and then reverse lookup that IP address to verify this claim.

PART 3 WHOIS

question 3.1 List the 5 Regional Internet Registries (RIRs) along with the general geographic locations they are associated with. Also, list their whois server names. (3 points)

According to Wikipedia[2], the 5 existing Regional Internet registry are

- The African Network Information Center (AFRINIC) serves Africa. whois server name is whois.afrinic.net
- The American Registry for Internet Numbers (ARIN) serves Antarctica, Canada, parts of the Caribbean, and the United States. whois server name is whois.arin.net
- The Asia-Pacific Network Information Centre (APNIC) serves East Asia, Oceania, South Asia, and Southeast Asia. whois server name is whois.apnic.net
- The Latin America and Caribbean Network Information Centre (LACNIC) serves most of the Caribbean and all of Latin America. whois server name is whois.lacnic.net
- The Réseaux IP Européens Network Coordination Centre (RIPE NCC) serves Europe, Central Asia, Russia, and West Asia. whois server name is whois.ripe.net

11 Question 11 3 / 3

✓ **- 0 pts** **Correct**

- 1 pts whois server names not listed, should be: whois.arin.net, whois.ripe.net, whois.apnic.net, whois.lacnic.net, whois.afrinic.net

- 1 pts Geographic location not mentioned.

- 1 pts whois server names incorrect, should be: whois.arin.net, whois.ripe.net, whois.apnic.net, whois.lacnic.net, whois.afrinic.net

- 0.5 pts whois server names not entirely correct, should be: whois.arin.net, whois.ripe.net, whois.apnic.net, whois.lacnic.net, whois.afrinic.net

question 3.2 What is the command-line option in whois to directly specify the server to query? Why do you need to use this option? (2 points)

To specify the server to query, the code to use is -h.

Because if we don't specify the server to query, by default, the whois information will typically come from a database which only contain information of Registry Service Provider. And we can not see the full record such as company name, contact, etc. For example,

```
whois youtube.com
```

yields

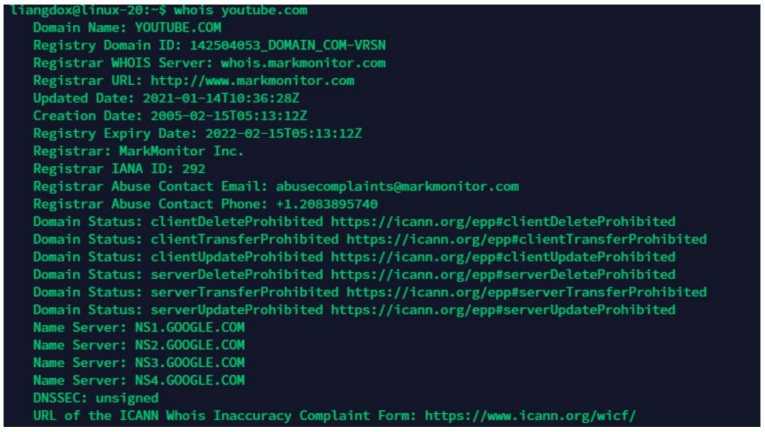

Fig. 14: output

By checking https://www.markmonitor.com/. I found this is a Registry Service Provider. So we need to run

```
whois youtube.com -h whois.markmonitor.com
```

Now we can see the actual company(Google LLC)'s name and contact information.

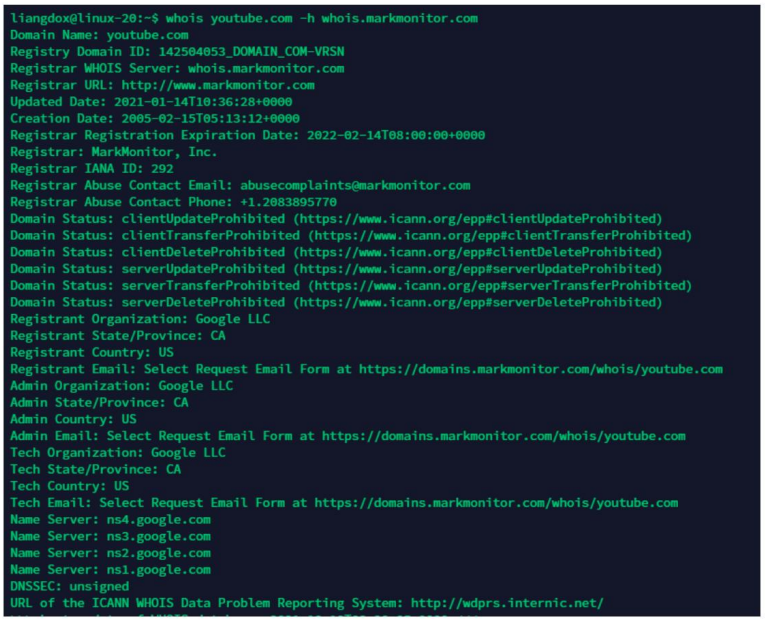

Fig. 15: output

12 Question 12 2 / 2

✓ **- 0 pts** **Correct**

- 1 pts command line option not mentioned or incorrect. correct answer = -h option

- 1 pts Use of the option not mentioned or incorrect. Main reason to use this option is registration information is not global. RIR databases contain regional registration information. Will need to specify the server for the regional internet registry in order to get the local registration of an organization

- 0 pts Use of the option is partially correct. Main reason to use this option is registration information is not global. RIR databases contain regional registration information. Will need to specify the server for the regional internet registry in order to get the local registration of an organization

- 2 pts No answer.

- 2 pts Incorrect

PART 4 PUTTING IT ALL TOGETHER

question 4.1 What is the IP address of the default local DNS server for CMU (from viewpoint of unix.andrew.cmu.edu)? (3 points)

We can use

```
dig
```

and find the server information in the output or just use

```
dig | grep SERVER
```

for simplification

The output is shown below. The default local DNS server is 128.2.1.10.

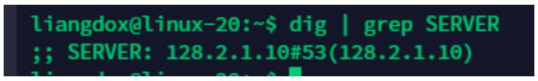

Fig. 16: output

The backup DNS server can be shown using

```
cat /etc/resolv.conf
```

The default local DNS server is 128.2.1.10. and the backup DNS is 128.2.1.11

13 Question 13 3 / 3

✓ **- 0 pts** **Correct**

- 3 pts wrong/missing answer. Correct answer: 128.2.1.10

- 1 pts Missing screenshot

- 3 pts Unanswered

question 4.2 Find the names and IP addresses of all root name servers. (2 points)

By running

```
dig
```

the output is a list of root name servers names and ip address

```
; <<>> DiG 9.16.1-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8509
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       479803  IN      NS      a.root-servers.net.
.                       479803  IN      NS      f.root-servers.net.
.                       479803  IN      NS      c.root-servers.net.
.                       479803  IN      NS      e.root-servers.net.
.                       479803  IN      NS      d.root-servers.net.
.                       479803  IN      NS      m.root-servers.net.
.                       479803  IN      NS      g.root-servers.net.
.                       479803  IN      NS      k.root-servers.net.
.                       479803  IN      NS      h.root-servers.net.
.                       479803  IN      NS      b.root-servers.net.
.                       479803  IN      NS      l.root-servers.net.
.                       479803  IN      NS      i.root-servers.net.
.                       479803  IN      NS      j.root-servers.net.

;; ADDITIONAL SECTION:
m.root-servers.net.     151228  IN      A       202.12.27.33
m.root-servers.net.     151228  IN      AAAA    2001:dc3::35
b.root-servers.net.     151228  IN      A       199.9.14.201
b.root-servers.net.     151228  IN      AAAA    2001:500:200::b
c.root-servers.net.     151228  IN      A       192.33.4.12
c.root-servers.net.     151228  IN      AAAA    2001:500:2::c
d.root-servers.net.     151228  IN      A       199.7.91.13
d.root-servers.net.     151228  IN      AAAA    2001:500:2d::d
e.root-servers.net.     151228  IN      A       192.203.230.10
e.root-servers.net.     151228  IN      AAAA    2001:500:a8::e
f.root-servers.net.     151228  IN      A       192.5.5.241
f.root-servers.net.     151228  IN      AAAA    2001:500:2f::f
g.root-servers.net.     151228  IN      A       192.112.36.4
g.root-servers.net.     151228  IN      AAAA    2001:500:12::d0d
h.root-servers.net.     151228  IN      A       198.97.190.53
h.root-servers.net.     151228  IN      AAAA    2001:500:1::53
a.root-servers.net.     151228  IN      A       198.41.0.4
a.root-servers.net.     151228  IN      AAAA    2001:503:ba3e::2:30
i.root-servers.net.     151228  IN      A       192.36.148.17
i.root-servers.net.     151228  IN      AAAA    2001:7fe::53
j.root-servers.net.     151228  IN      A       192.58.128.30
j.root-servers.net.     151228  IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     151228  IN      A       193.0.14.129
k.root-servers.net.     151228  IN      AAAA    2001:7fd::1
l.root-servers.net.     151228  IN      A       199.7.83.42
l.root-servers.net.     151228  IN      AAAA    2001:500:9f::42

;; Query time: 0 msec
;; SERVER: 128.2.1.10#53(128.2.1.10)
;; WHEN: Tue Oct 19 21:47:46 EDT 2021
;; MSG SIZE  rcvd: 811
```

so the names and IP addresses of all root name servers is shown in the table below

name	ipv4 address	ipv6 address
a.root-servers.net	198.41.0.4	2001:503:ba3e::2:30
b.root-servers.net	199.9.14.201	2001:500:200::b
c.root-servers.net	192.33.4.12	2001:500:2::c
d.root-servers.net	199.7.91.13	2001:500:2d::d
e.root-servers.net	192.203.230.10	2001:500:a8::e
f.root-servers.net	192.5.5.241	2001:500:2f::f
g.root-servers.net	192.112.36.4	2001:500:12::d0d
h.root-servers.net	198.97.190.53	2001:500:1::53
i.root-servers.net	192.36.148.17	2001:7fe::53
j.root-servers.net	192.58.128.30	2001:503:c27::2:30
k.root-servers.net	193.0.14.129	2001:7fd::1
l.root-servers.net	199.7.83.42	2001:500:9f::42
m.root-servers.net	202.12.27.33	2001:dc3::35

Fig. 17: names and IP addresses of all root name servers

14 Question 14 2 / 2

✓ - **0 pts** **Correct**

- **0.5 pts** Missing screenshot
- **2 pts** Unanswered
- **1 pts** Missing names of root name servers
- **1 pts** Missing IP addresses of root name servers
- **2 pts** Incorrect

question 4.3 Using dig, make an educated guess as to what service Google is running on server(s) with IP address of 8.8.4.4. (3 points)

Google is running a DNS service on 8.8.4.4.
Firstly, I ran

```
dig -x 8.8.4.4
```

The ouput is

```
; <<>> DiG 9.16.1-Ubuntu <<>> -x 8.8.4.4
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54359
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

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

;; ANSWER SECTION:
4.4.8.8.in-addr.arpa.   73336   IN      PTR     dns.google.

;; AUTHORITY SECTION:
4.8.8.in-addr.arpa.     3488    IN      NS      ns1.google.com.
4.8.8.in-addr.arpa.     3488    IN      NS      ns2.google.com.
4.8.8.in-addr.arpa.     3488    IN      NS      ns4.google.com.
4.8.8.in-addr.arpa.     3488    IN      NS      ns3.google.com.

;; ADDITIONAL SECTION:
ns3.google.com.         135060  IN      A       216.239.36.10
ns3.google.com.         96473   IN      AAAA    2001:4860:4802:36::a
ns1.google.com.         135060  IN      A       216.239.32.10
ns1.google.com.         137702  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         135060  IN      A       216.239.34.10
ns2.google.com.         137702  IN      AAAA    2001:4860:4802:34::a
ns4.google.com.         135060  IN      A       216.239.38.10
ns4.google.com.         137702  IN      AAAA    2001:4860:4802:38::a

;; Query time: 0 msec
;; SERVER: 128.2.1.10#53(128.2.1.10)
;; WHEN: Tue Oct 19 22:04:33 EDT 2021
;; MSG SIZE  rcvd: 331
```

It shows that the name is dns.google
I try to use it as NS server by running

```
dig @8.8.4.4 cmu.edu
```

and I can receive a proper respond

```
; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.4.4 cmu.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6576
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cmu.edu.                       IN      A

;; ANSWER SECTION:
cmu.edu.                21592   IN      A       128.2.42.10

;; Query time: 36 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Tue Oct 19 22:02:18 EDT 2021
;; MSG SIZE  rcvd: 52
```

So I believe Google is running a DNS service on 8.8.4.4.

15 Question 15 3 / 3

✓ **- 0 pts** **Correct**

- 3 pts Did not use dig

- 1 pts Missing screenshot

- 3 pts Unanswered

- 3 pts Did not answer public DNS service, and did not perform reverse lookup or examine trace

- 1 pts Correct command, but did not answer (public) DNS service

- 2 pts Did not answer public DNS service

question 4.4 What is the hostname of the default (local) nameserver? (3 points)

By running

```
dig -x 128.2.1.10
```

I fount that the hostname of the default NS is NSCACHE1.NET.CMU.EDU.
I also ran

```
dig NSCACHE1.NET.CMU.EDU
```

and check the A record to double-check.

```
liangdox@linux-20:~$ dig -x 128.2.1.10

; <<>> DiG 9.16.1-Ubuntu <<>> -x 128.2.1.10
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21740
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
10.1.2.128.in-addr.arpa. 20597  IN      PTR     NSCACHE1.NET.CMU.EDU.

;; AUTHORITY SECTION:
1.2.128.in-addr.arpa.   42194   IN      NS      NSAUTH1.NET.CMU.EDU.
1.2.128.in-addr.arpa.   42194   IN      NS      NSAUTH2.NET.CMU.EDU.

;; ADDITIONAL SECTION:
NSAUTH1.NET.CMU.EDU.    45819   IN      A       128.2.1.8
NSAUTH2.NET.CMU.EDU.    51390   IN      A       128.237.148.168

;; Query time: 0 msec
;; SERVER: 128.2.1.10#53(128.2.1.10)
;; WHEN: Sun Oct 17 23:30:38 EDT 2021
;; MSG SIZE  rcvd: 162

liangdox@linux-20:~$ NSCACHE1.NET.CMU.EDU
NSCACHE1.NET.CMU.EDU: command not found
liangdox@linux-20:~$ dig NSCACHE1.NET.CMU.EDU

; <<>> DiG 9.16.1-Ubuntu <<>> NSCACHE1.NET.CMU.EDU
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8044
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;NSCACHE1.NET.CMU.EDU.          IN      A

;; ANSWER SECTION:
NSCACHE1.NET.CMU.EDU.   29866   IN      A       128.2.1.10

;; AUTHORITY SECTION:
NET.CMU.EDU.            41355   IN      NS      NSAUTH1.NET.CMU.EDU.
NET.CMU.EDU.            41355   IN      NS      NSAUTH2.NET.CMU.EDU.

;; ADDITIONAL SECTION:
NSAUTH2.NET.CMU.EDU.    51352   IN      A       128.237.148.168
NSAUTH1.NET.CMU.EDU.    45781   IN      A       128.2.1.8

;; Query time: 0 msec
;; SERVER: 128.2.1.10#53(128.2.1.10)
;; WHEN: Sun Oct 17 23:31:16 EDT 2021
;; MSG SIZE  rcvd: 141
```

Fig. 18: output

16 Question 16 3 / 3

✓ **- 0 pts** **Correct**

- 3 pts Incorrect answer. Correct answer: NSCACHE1.NET.CMU.EDU

question 4.5 I mentioned in class that the root name servers do not support recursive requests. Prove it. Explain why or why not. (3 points)

I use dig on google.com and specified a root NS(198.41.0.4) to query by running this command:

```
dig @198.41.0.4 google.com
```

The output is as shown below, the root NS did not return any answer. It only return some TLD NS address. If it support recursive requests, it would have forwarded the query to tld server by itself and return the answer.
The reason why root NS do not support recursive requests is that the load can be distributed in this way. If root NS have to handle all request using recursive querying. The root NS will be under an extremely heavy load.

```
liangdox@linux-20:~$ dig @198.41.0.4 google.com

; <<>> DiG 9.16.1-Ubuntu <<>> @198.41.0.4 google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3097
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available

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

;; AUTHORITY SECTION:
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.

;; ADDITIONAL SECTION:
e.gtld-servers.net.     172800  IN      A       192.12.94.30
e.gtld-servers.net.     172800  IN      AAAA    2001:502:1ca1::30
b.gtld-servers.net.     172800  IN      A       192.33.14.30
b.gtld-servers.net.     172800  IN      AAAA    2001:503:231d::2:30
j.gtld-servers.net.     172800  IN      A       192.48.79.30
j.gtld-servers.net.     172800  IN      AAAA    2001:502:7094::30
m.gtld-servers.net.     172800  IN      A       192.55.83.30
m.gtld-servers.net.     172800  IN      AAAA    2001:501:b1f9::30
i.gtld-servers.net.     172800  IN      A       192.43.172.30
i.gtld-servers.net.     172800  IN      AAAA    2001:503:39c1::30
f.gtld-servers.net.     172800  IN      A       192.35.51.30
f.gtld-servers.net.     172800  IN      AAAA    2001:503:d414::30
a.gtld-servers.net.     172800  IN      A       192.5.6.30
a.gtld-servers.net.     172800  IN      AAAA    2001:503:a83e::2:30
g.gtld-servers.net.     172800  IN      A       192.42.93.30
g.gtld-servers.net.     172800  IN      AAAA    2001:503:eea3::30
h.gtld-servers.net.     172800  IN      A       192.54.112.30
h.gtld-servers.net.     172800  IN      AAAA    2001:502:8cc::30
l.gtld-servers.net.     172800  IN      A       192.41.162.30
l.gtld-servers.net.     172800  IN      AAAA    2001:500:d937::30
k.gtld-servers.net.     172800  IN      A       192.52.178.30
k.gtld-servers.net.     172800  IN      AAAA    2001:503:d2d::30
c.gtld-servers.net.     172800  IN      A       192.26.92.30
c.gtld-servers.net.     172800  IN      AAAA    2001:503:83eb::30
d.gtld-servers.net.     172800  IN      A       192.31.80.30
d.gtld-servers.net.     172800  IN      AAAA    2001:500:856e::30

;; Query time: 24 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Sun Oct 17 23:40:46 EDT 2021
;; MSG SIZE  rcvd: 835

liangdox@linux-20:~$
```

Fig. 19: output

17 Question 17 3 / 3

✓ **- 0 pts** **Correct**

- 2 pts Missing proof / proof is insufficient

- 1 pts wrong/missing explanation of why/why root servers do not support recursion.

- 3 pts Missing answer

- 3 pts Incorrect

- 1 pts Proof is insufficient

question 4.6 Find the top-level name servers for the .beer domain. Which organization owns these name servers? What is the technical point-of-contact? (If you use multiple steps to find the answers, show each step in your report). (5 points)

The easiest way to get the TLD NS for .beer is running whois on the Top Level Domain

```
whois beer
```

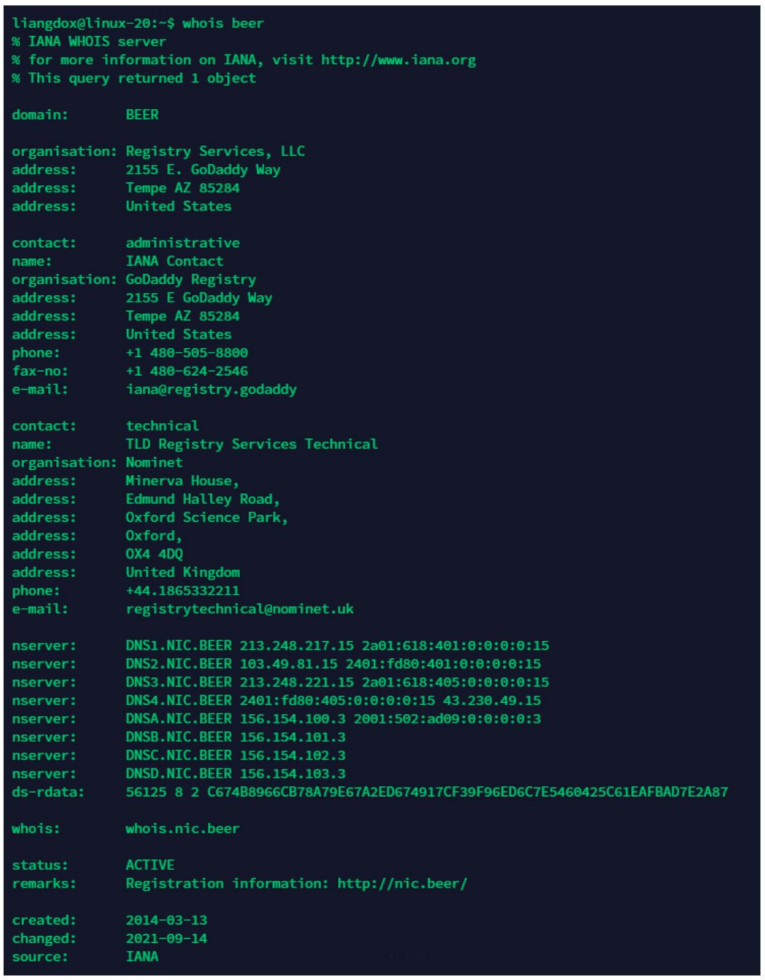

Fig. 20: output

we can get the top-level name servers are dns[1-4].nic.beer and dns[a-d].nic.beer.

```
nserver:      DNS1.NIC.BEER 213.248.217.15 2a01:618:401:0:0:0:0:15
nserver:      DNS2.NIC.BEER 103.49.81.15 2401:fd80:401:0:0:0:0:15
nserver:      DNS3.NIC.BEER 213.248.221.15 2a01:618:405:0:0:0:0:15
nserver:      DNS4.NIC.BEER 2401:fd80:405:0:0:0:0:15 43.230.49.15
nserver:      DNSA.NIC.BEER 156.154.100.3 2001:502:ad09:0:0:0:0:3
nserver:      DNSB.NIC.BEER 156.154.101.3
nserver:      DNSC.NIC.BEER 156.154.102.3
nserver:      DNSD.NIC.BEER 156.154.103.3
```

The organization that owns these NS is GoDaddy Registry.
The technical point-of-contact is

```
name:         TLD Registry Services Technical
organisation: Nominet
address:      Minerva House,
address:      Edmund Halley Road,
address:      Oxford Science Park,
address:      Oxford,
address:      OX4 4DQ
address:      United Kingdom
phone:        +44.1865332211
e-mail:       registrytechnical@nominet.uk
```

18 Question 18 5 / 5

✓ **- 0 pts Correct**

- 2 pts Missing or Incomplete: "Top level name servers for .beer domain"

- 1 pts Missing/Incorrect : "Organization which owns the name servers", should be Registry Services, LLC. Command: `whois beer`

- 1 pts Missing/Incorrect: "Technical point of contact", should be TLD Registry Services Technical. Command: `whois beer`

- 1 pts Missing/Incorrect : "Command used / Output"

- 5 pts Incorrect

- 5 pts deducted 5/5 marks for submitting late to gradescope. Overall 10 points have been deducted for submitting late in Q18,19

- 1 pts Did not use dig/whois to find technical point of contact and organization. Command: `whois beer`

- 5 pts Did not answer

question 4.7 Use dig to find the IP address for www.ini.cmu.edu and www.ece.cmu.edu. Then, use the IP addresses in your browser to load the web pages (i.e. just type those IP addresses in your browser's address bar. Do you get what you'd expect to get? Explain what you see. Your explanation should, for instance, illustrate any differences between INI and ECE, and use your knowledge of the HTTP protocol. (5 points)

Run

```
dig www.ini.cmu.edu
dig www.ece.cmu.edu
```

yields

```
liangdox@linux-20:~$ dig  www.ini.cmu.edu

; <<>> DiG 9.16.1-Ubuntu <<>> www.ini.cmu.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27836
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 6

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

;; ANSWER SECTION:
www.ini.cmu.edu.        389     IN      CNAME   WWW.R53.cmu.edu.
WWW.R53.cmu.edu.        36      IN      A       128.2.42.52

;; AUTHORITY SECTION:
R53.cmu.edu.            151     IN      NS      ns-579.awsdns-08.net.
R53.cmu.edu.            151     IN      NS      ns-1554.awsdns-02.co.uk.
R53.cmu.edu.            151     IN      NS      ns-1178.awsdns-19.org.
R53.cmu.edu.            151     IN      NS      ns-352.awsdns-44.com.

;; ADDITIONAL SECTION:
ns-1178.awsdns-19.org.  126241  IN      A       205.251.196.154
ns-1554.awsdns-02.co.uk. 126180 IN      A       205.251.198.18
ns-352.awsdns-44.com.   126048  IN      A       205.251.193.96
ns-352.awsdns-44.com.   91440   IN      AAAA    2600:9000:5301:6000::1
ns-579.awsdns-08.net.   126241  IN      A       205.251.194.67

;; Query time: 0 msec
;; SERVER: 128.2.1.10#53(128.2.1.10)
;; WHEN: Mon Oct 18 00:06:13 EDT 2021
;; MSG SIZE  rcvd: 314

liangdox@linux-20:~$ dig www.ece.cmu.edu

; <<>> DiG 9.16.1-Ubuntu <<>> www.ece.cmu.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1806
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4

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

;; ANSWER SECTION:
www.ece.cmu.edu.        62078   IN      A       128.2.131.95

;; AUTHORITY SECTION:
ece.cmu.edu.            39243   IN      NS      FS1.ece.cmu.edu.
ece.cmu.edu.            39243   IN      NS      FS0.ece.cmu.edu.
ece.cmu.edu.            39243   IN      NS      FS3.ece.cmu.edu.

;; ADDITIONAL SECTION:
FS1.ece.cmu.edu.        7281    IN      A       128.2.129.22
FS0.ece.cmu.edu.        7378    IN      A       128.2.129.20
FS3.ece.cmu.edu.        7281    IN      A       128.2.129.21

;; Query time: 0 msec
;; SERVER: 128.2.1.10#53(128.2.1.10)
;; WHEN: Mon Oct 18 00:06:29 EDT 2021
;; MSG SIZE  rcvd: 162
```

Fig. 21: output

One interesting finding is that www.ini.cmu.edu has an ip address of 128.2.42.52. Which is the same with cmu.edu But opening 128.2.42.52 and 128.2.131.95 yields unexpected results.

Opening 128.2.42.52 ends up in https://www.cmu.edu/.

Opening 128.2.131.95 result in a "Your connection is not private" page. If I click open anyway, I end up at a weird login page

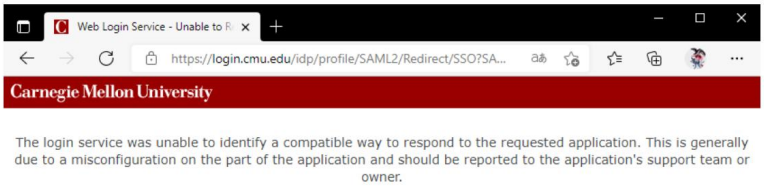

Fig. 22: result of opening 128.2.131.95

4.7-a www.ini.cmu.edu

For www.ini.cmu.edu, I think the reason why opening 128.2.42.52 does not open www.ini.cmu.edu is that 128.2.42.52 is not the ip-address of this page. Instead 128.2.42.52 is the CDN server for cmu.edu webpages. When accessing www.ini.cmu.edu, the client will establish TLS connection and then send the requested page using SNI. The CDN server will direct the client to the best server to get this webpage.
I opened www.ini.cmu.edu and used Wireshark to capture the packets. As can be seen from the Wireshark result,

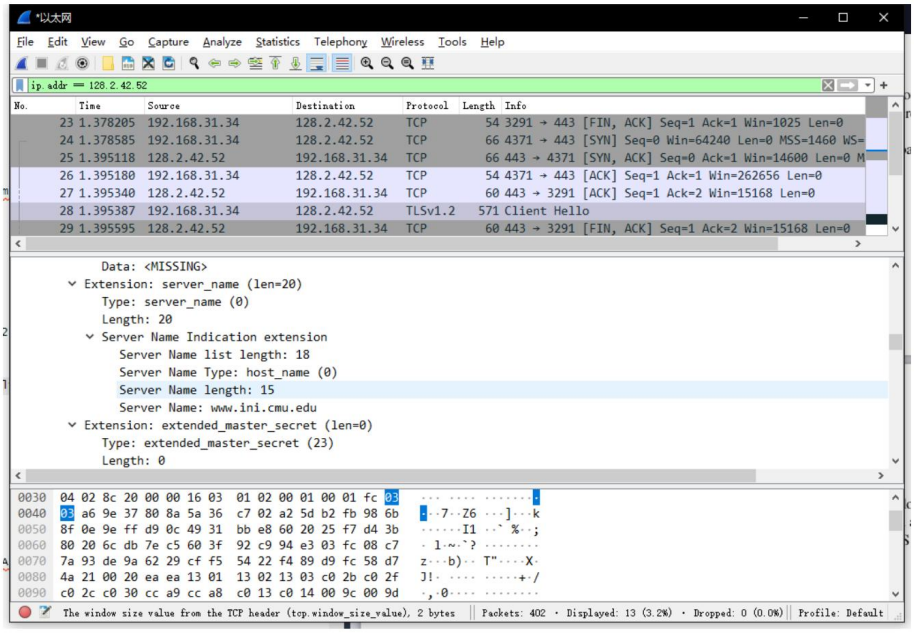

Fig. 23: output

In the Client Hello message, The client sent a TLS packet to 128.2.42.52 with the actual server name they request(www.ini.cmu.edu) in SNI extension. So 128.2.42.52 can inform the client where to get the webpage.

4.7-b www.ece.cmu.edu

As for www.ece.cmu.edu, I don't know why it end up in a weird login page. But I think the reason why opening the ip cannot open the webpage is due to the same reason. 128.2.131.95 is the ip address of an CDN server and to access the actual page. The client will need to establish TLS connection and announce the page they want to access via SNI extension in Client Hello message.

19 Question 19 4 / 5

- **0 pts** Correct
- **1 pts** Did not describe differences between INI and ECE, or description is incorrect and no proof was provided
- **0.5 pts** Missing screenshots (terminal dig command)
- **0.5 pts** Missing screenshots (browser/wireshark)
- **1 pts** IP addresses incorrect/missing, should be 128.2.42.52 and 128.2.131.95
- **1 pts** Did not explain results for INI, or incorrect explanation

✓ **- 1 pts Did not explain results for ECE, or incorrect explanation**

- **0.5 pts** Explanation for INI is insufficient (e.g. did not explain HTTP 301 response)
- **0.5 pts** Explanation for ECE is insufficient (e.g. did not explain HTTP 302 response)
- **5 pts** Incorrect
- **5 pts** Not answered

question 4.8 Find out details about Autonomous System Number 8. Include the OrgName, OrgID, ASName and the ASHandle in your answer. (4 points)

I ran

```
whois AS8
```

The output is

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#


ASNumber:       8
ASName:         RICE-AS
ASHandle:       AS8
RegDate:        1984-03-26
Updated:        1997-11-10
Ref:            https://rdap.arin.net/registry/autnum/8


OrgName:        Rice University
OrgId:          RICEUN
Address:        Networking MS 119
Address:        6100 Main Street
City:           Houston
StateProv:      TX
PostalCode:     77005
Country:        US
RegDate:        1983-12-02
Updated:        2020-09-09
Ref:            https://rdap.arin.net/registry/entity/RICEUN


OrgTechHandle: HOCKE30-ARIN
OrgTechName:   Hockett, Matt
OrgTechPhone:  +1-713-348-2280
OrgTechEmail:  mlh9@rice.edu
OrgTechRef:    https://rdap.arin.net/registry/entity/HOCKE30-ARIN

OrgAbuseHandle: RUH-ORG-ARIN
OrgAbuseName:   Rice University Networking
OrgAbusePhone:  +1-713-348-5244
OrgAbuseEmail:  ipadmin@rice.edu
OrgAbuseRef:    https://rdap.arin.net/registry/entity/RUH-ORG-ARIN

OrgTechHandle: RUH-ORG-ARIN
OrgTechName:   Rice University Networking
OrgTechPhone:  +1-713-348-5244
OrgTechEmail:  ipadmin@rice.edu
OrgTechRef:    https://rdap.arin.net/registry/entity/RUH-ORG-ARIN

RTechHandle: RUH-ORG-ARIN
RTechName:   Rice University Networking
RTechPhone:  +1-713-348-5244
RTechEmail:  ipadmin@rice.edu
RTechRef:    https://rdap.arin.net/registry/entity/RUH-ORG-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#
```

The details are shown above, specificly,

- OrgName: Rice University
- OrgID: RICEUN
- ASName: RICE-AS
- ASHandle: AS8

20 Question 20 **4 / 4**

✓ **- 0 pts** **Correct**

- 4 pts Incorrect

- 4 pts Did not answer

- 1 pts Did not use `whois` command

- 1 pts Did not show how the answer was found

question 4.9 Find the IP address range assigned to CMU. (3 points)

I discovered the answer for this when doing q 4.6. I ran

```
whois 128.2.42.10
```

and the output is

```
liangdox@linux-15:~$ whois 128.2.42.10

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#


NetRange:       128.2.0.0 - 128.2.255.255
CIDR:           128.2.0.0/16
NetName:        CMU-NET
NetHandle:      NET-128-2-0-0-1
Parent:         NET128 (NET-128-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS9
Organization:   Carnegie Mellon University (CARNEG-Z)
RegDate:        1984-04-17
Updated:        2012-04-02
Ref:            https://rdap.arin.net/registry/ip/128.2.0.0


OrgName:        Carnegie Mellon University
OrgId:          CARNEG-Z
Address:        Cyert Hall 215
Address:        5000 Forbes Avenue
City:           Pittsburgh
StateProv:      PA
PostalCode:     15213
Country:        US
RegDate:        2009-12-01
Updated:        2020-03-27
Ref:            https://rdap.arin.net/registry/entity/CARNEG-Z
```

Fig. 24: output

It seems that the ip range is 128.2.0.0-128.2.255.255 . The Origin AS is AS9, but I did not know how to get ip-range of a whole ASN.

21 Question 21 2.5 / 3

- **0 pts** Correct
- **3 pts** Incorrect
- **1 pts** Missing proof/screenshot
- **3 pts** Did not answer

✓ **- 0.5 pts** **Incomplete IP range**

question 4.10 Find the IP address of linux.ece.cmu.edu

4.10-a Ask the C root server for the address of linux without recursion. (1 points)

I ran

```
dig @c.root-servers.net linux.ece.cmu.edu
```

The output is

```
; <<>> DiG 9.16.1-Ubuntu <<>> @c.root-servers.net linux.ece.cmu.edu
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4925
;; 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
; COOKIE: 4ec01ebdbe07441820699d69616e44f79cf934010b41c611 (good)
;; QUESTION SECTION:
;linux.ece.cmu.edu.             IN      A

;; AUTHORITY SECTION:
edu.                    172800  IN      NS      b.edu-servers.net.
edu.                    172800  IN      NS      d.edu-servers.net.
edu.                    172800  IN      NS      h.edu-servers.net.
edu.                    172800  IN      NS      a.edu-servers.net.
edu.                    172800  IN      NS      i.edu-servers.net.
edu.                    172800  IN      NS      c.edu-servers.net.
edu.                    172800  IN      NS      l.edu-servers.net.
edu.                    172800  IN      NS      k.edu-servers.net.
edu.                    172800  IN      NS      g.edu-servers.net.
edu.                    172800  IN      NS      m.edu-servers.net.
edu.                    172800  IN      NS      f.edu-servers.net.
edu.                    172800  IN      NS      j.edu-servers.net.
edu.                    172800  IN      NS      e.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: 12 msec
;; SERVER: 192.33.4.12#53(192.33.4.12)
;; WHEN: Tue Oct 19 00:09:27 EDT 2021
;; MSG SIZE  rcvd: 869
```

4.10-b Go through the hierarchy from the root without recursion and following the referrals manually until you have found the address of linux.ece.cmu.edu. Show all your work. (3 points)

I first ran

```
dig @c.root-servers.net linux.ece.cmu.edu
```

The output is

```
; <<>> DiG 9.16.1-Ubuntu <<>> @c.root-servers.net linux.ece.cmu.edu
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4925
;; 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
; COOKIE: 4ec01ebdbe07441820699d69616e44f79cf934010b41c611 (good)
;; QUESTION SECTION:
;linux.ece.cmu.edu.             IN      A

;; AUTHORITY SECTION:
edu.                    172800  IN      NS      b.edu-servers.net.
edu.                    172800  IN      NS      d.edu-servers.net.
edu.                    172800  IN      NS      h.edu-servers.net.
edu.                    172800  IN      NS      a.edu-servers.net.
edu.                    172800  IN      NS      i.edu-servers.net.
edu.                    172800  IN      NS      c.edu-servers.net.
edu.                    172800  IN      NS      l.edu-servers.net.
edu.                    172800  IN      NS      k.edu-servers.net.
edu.                    172800  IN      NS      g.edu-servers.net.
edu.                    172800  IN      NS      m.edu-servers.net.
edu.                    172800  IN      NS      f.edu-servers.net.
edu.                    172800  IN      NS      j.edu-servers.net.
edu.                    172800  IN      NS      e.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: 12 msec
;; SERVER: 192.33.4.12#53(192.33.4.12)
;; WHEN: Tue Oct 19 00:09:27 EDT 2021
;; MSG SIZE  rcvd: 869
```

Then I ran

```
dig @a.edu-servers.net linux.ece.cmu.edu
```

The output is

```
; <<>> DiG 9.16.1-Ubuntu <<>> @a.edu-servers.net linux.ece.cmu.edu
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63628
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;linux.ece.cmu.edu.             IN      A

;; AUTHORITY SECTION:
cmu.edu.                172800  IN      NS      ny-server-03.net.cmu.edu.
cmu.edu.                172800  IN      NS      nsauth1.net.cmu.edu.
cmu.edu.                172800  IN      NS      nsauth2.net.cmu.edu.

;; ADDITIONAL SECTION:
ny-server-03.net.cmu.edu. 172800 IN     A       38.96.147.4
nsauth1.net.cmu.edu.    172800  IN      A       128.2.1.8
nsauth2.net.cmu.edu.    172800  IN      A       128.237.148.168

;; Query time: 68 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Tue Oct 19 00:11:58 EDT 2021
;; MSG SIZE  rcvd: 169
```

Next, I ran

```
dig @nsauth1.net.cmu.edu linux.ece.cmu.edu
```

The output is

```
; <<>> DiG 9.16.1-Ubuntu <<>> @nsauth1.net.cmu.edu linux.ece.cmu.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12444
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;linux.ece.cmu.edu.             IN      A

;; AUTHORITY SECTION:
ece.cmu.edu.            86400   IN      NS      FS3.ece.cmu.edu.
ece.cmu.edu.            86400   IN      NS      FS0.ece.cmu.edu.
ece.cmu.edu.            86400   IN      NS      FS1.ece.cmu.edu.

;; ADDITIONAL SECTION:
FS0.ece.cmu.edu.        86400   IN      A       128.2.129.20
FS1.ece.cmu.edu.        86400   IN      A       128.2.129.22
FS3.ece.cmu.edu.        86400   IN      A       128.2.129.21

;; Query time: 0 msec
;; SERVER: 128.2.1.8#53(128.2.1.8)
;; WHEN: Tue Oct 19 00:13:06 EDT 2021
;; MSG SIZE  rcvd: 148
```

Lastly, I ran

```
dig @FS3.ece.cmu.edu linux.ece.cmu.edu
```

The output is

```
; <<>> DiG 9.16.1-Ubuntu <<>> @FS3.ece.cmu.edu linux.ece.cmu.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12994
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
```

```
; COOKIE: 7955458d3fd72c107a9c9a69616e4601ba567f96fe4321e5 (good)
;; QUESTION SECTION:
;linux.ece.cmu.edu.             IN      A

;; ANSWER SECTION:
LINUX.ece.cmu.edu.      86400   IN      CNAME   ECE-LINUX.ECE.CMU.EDU.
ECE-LINUX.ece.cmu.edu.  86400   IN      A       128.2.131.23

;; AUTHORITY SECTION:
ECE.CMU.EDU.            86400   IN      NS      FS1.ECE.CMU.EDU.
ECE.CMU.EDU.            86400   IN      NS      FS3.ECE.CMU.EDU.
ECE.CMU.EDU.            86400   IN      NS      FS0.ECE.CMU.EDU.

;; ADDITIONAL SECTION:
FS0.ece.cmu.edu.        86400   IN      A       128.2.129.20
FS1.ece.cmu.edu.        86400   IN      A       128.2.129.22
FS3.ece.cmu.edu.        86400   IN      A       128.2.129.21

;; Query time: 0 msec
;; SERVER: 128.2.129.21#53(128.2.129.21)
;; WHEN: Tue Oct 19 00:13:53 EDT 2021
;; MSG SIZE  rcvd: 255
```

And in the answer section we can see that the ip address of linux.ece.cmu.edu is 128.2.131.23.

4.10-c What is the address? (2 points)

The ip address of linux.ece.cmu.edu is 128.2.131.23.

4.10-d How many iterations did it take? (2 points)

It took 4 iterations. First on root NS. Second on TLD NS. The third is on CMU's NS and the last is on ECE department's NS.

22 Question 22 6.5 / 8

- **0 pts** Correct

✓ - **1 pts** **Part a incorrect :: Not adding `+norecurse`**

- **1 pts** Part a incorrect

✓ - **0.5 pts** **Part b :: did not add `+norecurse` for each `dig` command**

- **0.5 pts** Part b :: did not include all screenshots/output/commands
- **3 pts** Part b incorrect/missing
- **2 pts** Part c incorrect/missing
- **2 pts** Part d incorrect/missing
- **1 pts** Did not add +norecurse
- **8 pts** Did not answer

PART 5 OTHER QUESTIONS

question 5.1 Refer to Lecture 01 (Networking Introduction), slide 30 for this problem. Suppose users share a 1Mbps link. Also suppose each user requires 100Kbps when transmitting, but each user transmits only 10 percent of the time. (8 points)

5.1-a When circuit switching is used, how many users can be supported? Let'scall this number $n_{circuit}$.

$n_{circuit} = 1Mbps/100Kbps = 10$

5.1-b For a packet switching network, what is the probability that a given user is transmitting?

the probability that a given user is transmitting is 0.1

5.1-c uppose there are 40 users. Find the probability that at any given time, exactly n users are transmitting simultaneously.

The formula should be

$$\begin{pmatrix} M \\ n \end{pmatrix} p^n (1-p)^{M-n}$$

where

$$M = 40, p = 0.1,$$

So the the probability that at any given time, exactly n users are transmitting simultaneously is

$$\begin{pmatrix} 40 \\ n \end{pmatrix} 0.1^n 0.9^{40-n}$$

5.1-d Again, suppose there are 40 users. Find the probability that there are ($n_{circuit} + 1$) or more users transmitting simultaneously.

The formula is

$$\sum_{n=n_{circuit}+1}^{M} \begin{pmatrix} M \\ n \end{pmatrix} p^n (1-p)^{M-n}$$

where

$$M = 40, p = 0.1, n_{circuit} = 1$$

$$\sum_{n=n_{circuit}+1}^{M} \begin{pmatrix} M \\ n \end{pmatrix} p^n (1-p)^{M-n} = \sum_{n=11}^{40} \begin{pmatrix} 40 \\ n \end{pmatrix} 0.1^n 0.9^{40-n}$$

In order to calculate this, I simply ran a piece of python code

```
from scipy.special import comb
a = 0
for i in range(11,41):
    a=a+(0.1)**i*(0.9)**(40-i)*comb(40,i)
print(a)
```

The result is 0.00147

23 Question 23 8 / 8

✓ **- 0 pts** **Correct**

- 1.5 pts Part a :: Incorrect

- 1.5 pts Part b :: Incorrect

- 2 pts Part c :: Incorrect

- 1 pts Part c:: Partial Incorrect

- 3 pts Part d :: Incorrect

- 1 pts Part d :: Calculation Error/Missing

- 2 pts Part d :: Missing Math Formula

- 3 pts Missing calculation

- 0 pts Link wrong pages

question 5.2 Let's explore propagation delay and transmission delay. Suppose there are two hosts, A and B, connected by a single link with bandwidth R bps. The physical link's length is d meters. Propagation speed in the link is s m/s. At time $t = 0$, Host A begins to send a packet of L bits to Host B. (8 points).

5.2-a Express the propagation delay, d_{prop}, in terms of d and s.

$$d_{prop} = d/s$$

5.2-b Determine the transmission time of the packet, d_{trans}, in terms of L and R.

$$d_{trans} = L/R$$

5.2-c At time $t = d_{trans}$, where is the last bit of the packet?

The last bit of the packet just left the sender

5.2-d At time $t = d_{trans}$, where is the first bit of the packet?

The first bit has travelled $d_{trans} * s$ distance or have already arrived at the receiver.

5.2-e Suppose $s = 2.8 \times 10^8$ m/s, $L = 150$ bits and $R = 48$ kbps. Find the distance d such that d_{prop} is equal to d_{trans}.

$$d_{prop} = d_{trans}$$

is equivalent to

$$d/s = L/R$$

$$d/(2.8 \times 10^8) = 150/(48 \times 10^3)$$

$d = 8.75 \times 10^5$ meters

24 Question 24 8 / 8

✓ **- 0 pts Correct**

- 1 pts Part a incorrect, should be d/s

- 0 pts Part a :: incorrect/missing unit

- 1 pts Part b incorrect, should be L/R

- 0 pts Part b :: incorrect/missing unit

- 2 pts Part c incorrect, should be: just leaving Host A

- 1 pts Part c partially incorrect, should be: just leaving Host A

- 2 pts Part d incorrect. If dprop > dtrans (i.e. if d/s > L / R) then the first bit is still in the link. Otherwise, the first bit
has already been received by Host B.

- 1 pts Part d partially incorrect. If dprop > dtrans (i.e. if d/s > L / R) then the first bit is still in the link. Otherwise, the first bit
has already been received by Host B.

- 2 pts Part e incorrect, should be 875km

- 0.5 pts Part e :: Simple math error, should be 875km

- 0.5 pts Part e :: Incorrect units used / Units not written

- 0 pts Failed to link correct pages

- 8 pts No answer.

question 5.3 A webserver receives an average of 950 HTTP requests per second. 740 of them are simple GET requests for static pages, each of which takes, on average, 100 µS to reply to. 124 of them are GET requests for dynamic pages. Because responding to these requests requires at least one database lookup, they take 1 mS to process. The remaining are PUT requests that require database writes – they take 2 mS to process. Model the webserver as an M/M/1 system. (8 points)

5.3-a Find $\lambda, \mu, \rho, L, L_q$

$$\lambda = 950$$

Average time each request take is

$$t_{process} = (100 * 740 * 10^{-6} + 124 * 10^{-3} + 86 * 2 * 10^{-3})/950 = \frac{37}{95000}\ seconds$$

$$\mu = 1/(37/95000) = \frac{95000}{37} \approx 2567.568$$

$$\rho = \frac{\lambda}{\mu} = 0.37$$

$$L = \frac{\rho}{1-\rho} \approx 0.5873$$

$$L_q = \frac{\rho^2}{1-\rho} \approx 0.2173$$

5.3-b What percentage of the time is the webserver idle?

probability that there n jobs in the system is

$$P_n = \rho^n[1-\rho]$$

$$P_0 = 1 - \rho = 0.63$$

So 63% of time is the webserver idle.

5.3-c How often are there more than 6 requests in the webserver's queue?

probability that there n jobs in the system is

$$P_n = \rho^n[1-\rho]$$

$$\sum_{n=0}^{7} P_n \approx 0.999649$$

probability that there more than 6 requests in the webserver's queue(more than 7 requests in the webserver's system)

$$1 - \sum_{n=0}^{7} P_n \approx 0.000351$$

probability that there more than 6 requests in the webserver's queue is 0.000351

5.3-d What is the average waiting time for a request?

the average waiting time for a request is

$$W = \frac{1}{\mu - \lambda} = \frac{37}{59850} \approx 0.000618\ seconds$$

5.3-e What is the average total time for a request?

the average total time for a request is

$$W + t_{process} = \frac{37}{59850} + \frac{37}{95000} \approx 0.001008\ seconds$$

PART 6 REFERENCE

[1] https://en.wikipedia.org/wiki/Domain_Name_System
[2] https://en.wikipedia.org/wiki/Regional_Internet_registry

25 Question 25 6 / 8

- **0 pts** Correct
- **2 pts** Part a, b, c, d, e :: μ calculation is incorrect, should be 2568 requests/second
- **0.5 pts** Part a :: Incorrect □, should be 950 requests/second
- **0.5 pts** Part a :: Incorrect ρ, should be 0.37
- **0.5 pts** Part a :: Incorrect L, should be 0.587 requests
- **0.5 pts** Part a :: Incorrect Lq, should be 0.217 requests
- **1 pts** Part b :: Incorrect, should be 0.63
- **0.5 pts** Part b :: Minor math error, should be 0.63
- **1 pts** Part c :: Incorrect, should be 0.000351
- **0.5 pts** Part c :: Didn't consider the fact that more than 6 in the queue implies more than 7 in the system. Hence, it should be 1 - ∑(Pn) for n=0 to n=7. Should be 0.000351
- **0.5 pts** Part c :: Calculation error

✓ **- 1 pts Part d :: Incorrect, should be 0.229 ms**

- **0.5 pts** Part d :: Calculation error, should be 0.229 ms

✓ **- 1 pts Part e :: Incorrect, should be 0.618 ms**

- **0.5 pts** Part e :: Calculation error, should be 0.618 ms
- **0.5 pts** Missing or wrong unit. (1s = 1000ms)
- **0 pts** Link wrong pages
- **8 pts** Left Blank