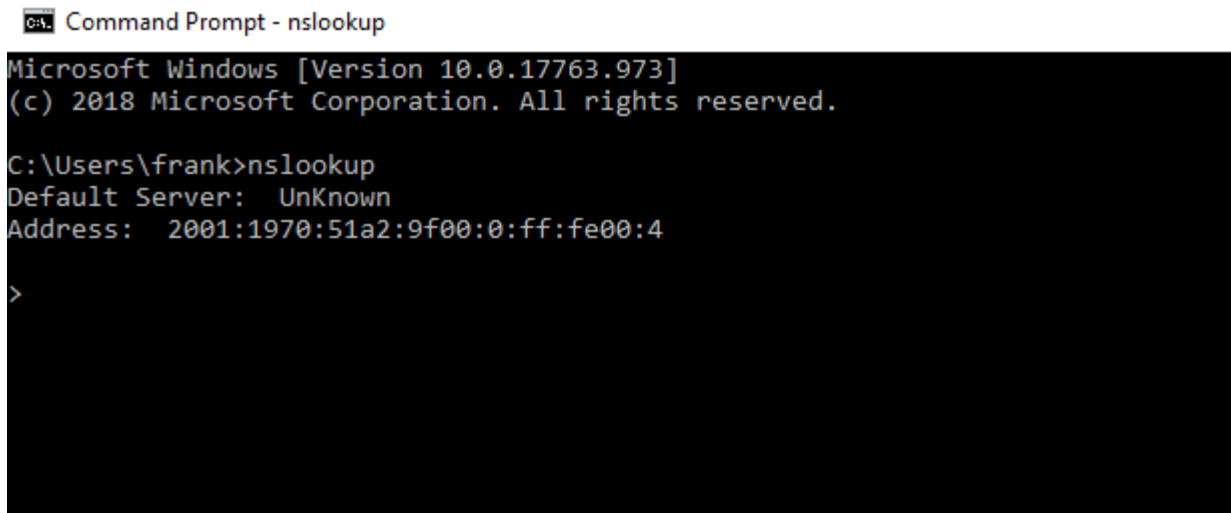


## Question 2: DNS Lab

**2-A:** What is your default server for nslookup and what is its IP address? To support your answer, also add the screen shot from your computer.



```
Command Prompt - nslookup

Microsoft Windows [Version 10.0.17763.973]
(c) 2018 Microsoft Corporation. All rights reserved.

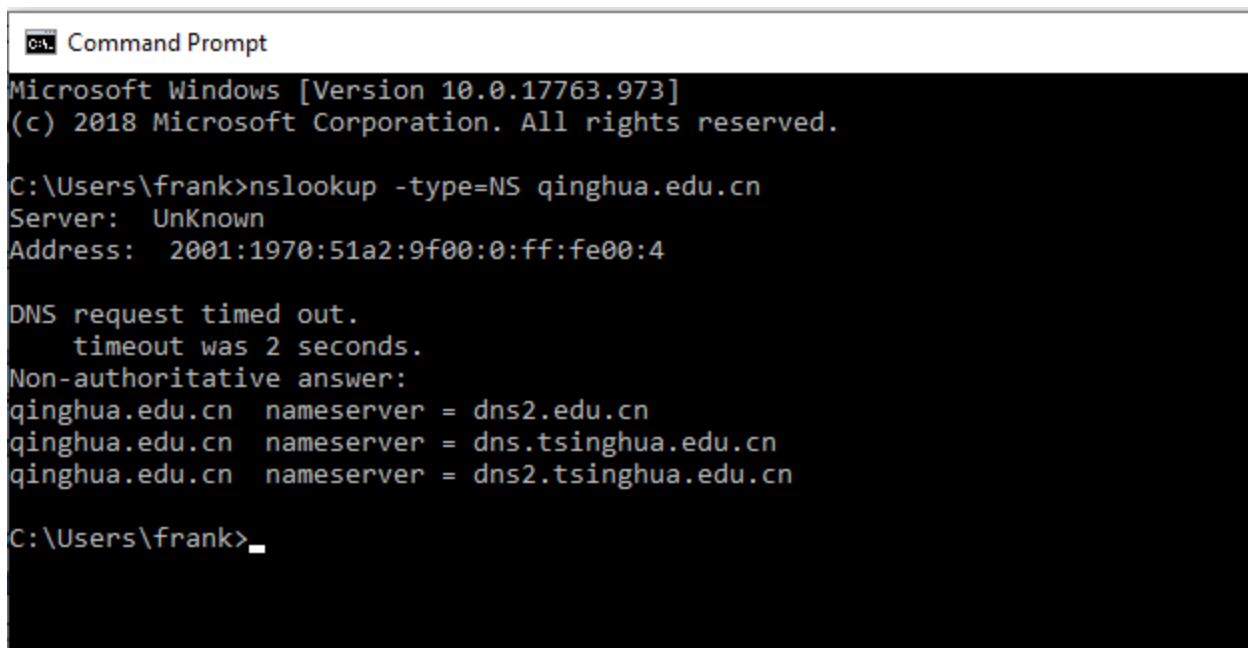
C:\Users\frank>nslookup
Default Server:  UnKnown
Address:  2001:1970:51a2:9f00:0:ff:fe00:4

>
```

As seen in the above screenshot, the default server for nslookup is: **2001:1970:51a2:9f00:0:ff:fe00:4**.  
Note: this is the ipv6 ip address

**2-B:** Add your answers to lab questions 1-3 in the submission document.

**2-B-1:** Run nslookup to obtain the IP address of a Web server in Asia. What is the ip address of that server?



```
Command Prompt

Microsoft Windows [Version 10.0.17763.973]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\frank>nslookup -type=NS qinghua.edu.cn
Server:  UnKnown
Address:  2001:1970:51a2:9f00:0:ff:fe00:4

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
qinghua.edu.cn  nameserver = dns2.edu.cn
qinghua.edu.cn  nameserver = dns.tsinghua.edu.cn
qinghua.edu.cn  nameserver = dns2.tsinghua.edu.cn

C:\Users\frank>
```

As seen above, the web server I queried was Qinghua university's server. The ipv6 address is:  
2001:1970:51a2:9f00:0:ff:fe00:4

## 2-B-2: Run nslookup to determine the authoritative DNS servers for a university in Europe.

```

C:\Users\frank>nslookup -type=NS london.ac.uk
Server: UnKnown
Address: 2001:1970:51a2:9f00:0:ff:fe00:4

Non-authoritative answer:
london.ac.uk nameserver = ns1.ulcc.ac.uk
london.ac.uk nameserver = ns0.ulcc.ac.uk

ns0.ulcc.ac.uk internet address = 193.63.88.11
ns1.ulcc.ac.uk internet address = 128.86.249.14

C:\Users\frank>

```

As seen above, the ipv6 address of the authoritative DNS server for the university college of london is:  
2001:1970:51a2:9f00:0:ff:fe00:4

**2-B-3: We want to represent the content of a DNS message in the form of a Python Dictionary where keys are the message field names and key-values are the field values. Provide the definition of this dictionary in the submission document.**

The screenshot displays a network capture of a DNS transaction. The packet list shows a query from 2001:1970:51a2:9f00:0:ff:fe00:4 to 2001:1970:51a2:9f00:0:ff:fe00:4. The details pane shows a Standard query response for 0x4570 A s2.google.com. The packet data shows the raw bytes of the DNS message.

No.	Time	Source	Destination	Protocol	Length	Info
168	6.890918	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	104	Standard query 0x4570 A s2.google.com
178	6.914925	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	149	Standard query response 0x4570 A s2.google.com
194	6.995196	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	97	Standard query 0x9121 AAAA fonts.gstatic.com
207	7.024976	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	161	Standard query response 0x9121 AAAA fonts.gstatic.com
244	7.553157	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	111	Standard query 0x384d AAAA webad.doubleclick.net
247	7.584042	192.168.0.235	8.8.8.8	DNS	91	Standard query 0x384d AAAA webad.doubleclick.net
248	7.589665	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	280	Standard query response 0x384d AAAA webad.doubleclick.net
306	7.684427	8.8.8.8	192.168.0.235	DNS	264	Standard query response 0x384d AAAA webad.doubleclick.net
345	7.890502	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	95	Standard query 0x5878 AAAA d.joi
346	7.914094	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	185	Standard query response 0x5878 AAAA d.joi
352	7.983816	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	103	Standard query 0xf936 AAAA adult
360	8.012623	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	187	Standard query response 0xf936 AAAA adult
380	8.873049	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	95	Standard query 0xc0f1 AAAA play
381	8.890025	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	123	Standard query response 0xc0f1 AAAA play
462	12.270660	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	95	Standard query 0x2ad7 AAAA ssl.g
478	12.297890	2001:1970:51a2:9f00:0:ff:fe00:4	2001:1970:51a2:9f00:0:ff:fe00:4	DNS	378	Standard query response 0x2ad7 AAAA ssl.g

Details of the selected packet (No. 178):

- User Datagram Protocol, Src Port: 53, Dst Port: 57041
- Domain Name System (response)
  - Transaction ID: 0x4570
  - Flags: 0x8100 Standard query response, No error
  - Questions: 1
  - Answer RRs: 2
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
  - Answers
    - [Request In: 168]
    - [Time: 0.024007000 seconds]

Packet Data (Hex):

```

0000  88 b1 11 80 67 45 02 00 00 00 00 04 86 dd 60 00  ....gE.....
0010  00 00 00 5f 11 40 20 01 19 70 51 a2 9f 00 00 00  ....@...pQ....
0020  00 ff fe 00 00 04 20 01 19 70 51 a2 9f 00 61 03  .......pQ....a

```

Taking the screenshot of a DNS response message above, we can define a python dictionary to capture this information as such:

```
DNS = {"Transaction ID:" : 0x72cf, "Flags:" : 0x0100 Standard query, "Questions:" : 1, "Answer RRs:" : 0,  
"Authority RRs:" : 0, "Additional RRs:" : 0, "Queries" : [Response In: 2565]}
```