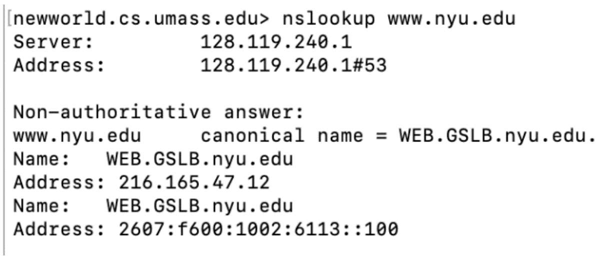
HW2 DNS

Basic knowledge: nslookup

Let’s start our investigation of the DNS by examining the nslookup command, which will invoke the underlying DNS services to implement its functionality. The nslookup command is available in most Microsoft, Apple IOS, and Linux operating systems. To run nslookup you just type the nslookup command on the command line in a DOS window, Mac IOS terminal window, or Linux shell.

In its most basic operation, nslookup allows the host running nslookup to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain (TLD) DNS server, an authoritative DNS server, or an intermediate DNS server (see the textbook for definitions of these terms). For example, nslookup can be used to retrieve a “Type=A” DNS record that maps a hostname (e.g., www.nyu.edu) to its IP address. To accomplish this task, nslookup sends a DNS query to the specified DNS server (or the default local DNS server for the host on which nslookup is run, if no specific DNS server is specified), receives a DNS response from that DNS server, and displays the result.

Let’s take nslookup out for a spin! We’ll first run nslookup on the Linux command line on the newworld.cs.umass.edu host located in the CS Department at the University of Massachusetts (UMass) campus, where the local name server is named primo.cs.umass.edu (which has an IP address 128.119.240.1). Let’s try nslookup in its simplest form:



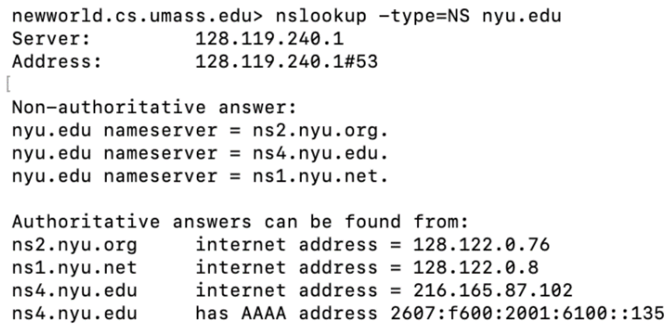
```
[newworld.cs.umass.edu> nslookup www.nyu.edu
Server:         128.119.240.1
Address:        128.119.240.1#53

Non-authoritative answer:
www.nyu.edu     canonical name = WEB.GSLB.nyu.edu.
Name:   WEB.GSLB.nyu.edu
Address: 216.165.47.12
Name:   WEB.GSLB.nyu.edu
Address: 2607:f600:1002:6113::100
```

Figure 1: the basic nslookup command

In this example the nslookup command is given one argument, a hostname (www.nyu.edu). In words, this command is saying “please send me the IP address for the host www.nyu.edu.” As shown in the screenshot, the response from this command provides two pieces of information: (1) the name and IP address of the DNS server that provides the answer – in this case the local DNS server at UMass; and (2) the answer itself, which is the canonical host name and IP address of www.nyu.edu. You may have noticed that there are two name/address pairs provided for www.nyu.edu. The first (216.165.47.12) is an IPv4 address in the familiar-looking dotted decimal notation; the second (2607:f600:1002:6113::100) is a longer and more complicated looking IPv6 address. We'll learn about IPv4 and IPv6 and their two different addressing schemes later in Chapter 4. For now, let's just focus on our more comfortable (and common) IPv4 world[1].

Although the response came from the local DNS server (with IP address 128.119.240.1) at UMass, it is quite possible that this local DNS server iteratively contacted several other DNS servers to get the answer, as described in Section 2.4 of the textbook.

In addition to using nslookup to query for a DNS "Type=A" record, we can also use nslookup to nslookup to query for a "TYPE=NS" record, which returns the hostname (and its IP address) of an authoritative DNS server that knows how to obtain the IP addresses for hosts in the authoritative server's domain.

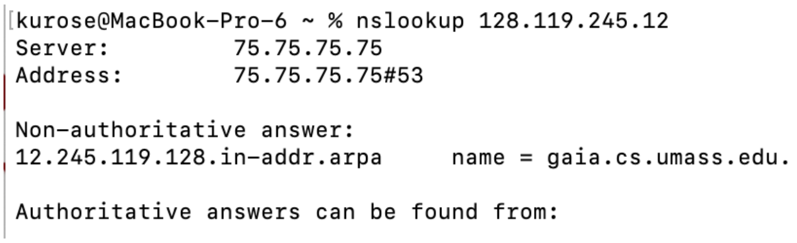


```
newworld.cs.umass.edu> nslookup -type=NS nyu.edu
Server:         128.119.240.1
Address:        128.119.240.1#53

Non-authoritative answer:
nyu.edu nameserver = ns2.nyu.org.
nyu.edu nameserver = ns4.nyu.edu.
nyu.edu nameserver = ns1.nyu.net.

Authoritative answers can be found from:
ns2.nyu.org     internet address = 128.122.0.76
ns1.nyu.net     internet address = 128.122.0.8
ns4.nyu.edu     internet address = 216.165.87.102
ns4.nyu.edu     has AAAA address 2607:f600:2001:6100::135
```

Figure 2: using nslookup to find the authoritative name servers for the nyu.edu domain

In the example in Figure 2, we've invoked nslookup with the option "-type=NS" and the domain "nyu.edu". This causes nslookup to send a query for a type-NS record to the default local DNS server. In words, the query is saying, "please send me the host names of the authoritative DNS for nyu.edu". (When the –type option is not used, *nslookup* uses the default, which is to query for type A records.) The answer, displayed in the above screenshot, first indicates the DNS server that is providing the answer (which is the default local UMass DNS server with address 128.119.240.1) along with three NYU DNS name servers. Each of these servers is indeed an authoritative DNS server for the hosts on the NYU campus. However, nslookup also indicates that the answer is “non-authoritative,” meaning that this answer came from the cache of some server rather than from an authoritative NYU DNS server. Finally, the answer also includes the IP addresses of the authoritative DNS servers at NYU. (Even though the type-NS query generated by nslookup did not explicitly ask for the IP addresses, the local DNS server returned these “for free” and *nslookup* displays the result.)

Lastly, we sometimes might be interested in discovering the name of the host associated with a given IP address, i.e., the reverse of the lookup shown in Figure 1 (where the host’s name was known/specified and the host’s IP address was returned). nslookup can also be used to perform this so-called “reverse DNS lookup.” In Figure 3, for example, we specify an IP address as the nslookup argument (128.119.245.12 in this example) and nslookup returns the host name with that address (gaia.cs.umass.edu in this example)



```
[kurose@MacBook-Pro-6 ~ % nslookup 128.119.245.12
Server:         75.75.75.75
Address:        75.75.75.75#53

Non-authoritative answer:
12.245.119.128.in-addr.arpa     name = gaia.cs.umass.edu.

Authoritative answers can be found from:
```

Figure 3: using nslookup to perform a “reverse DNS lookup”

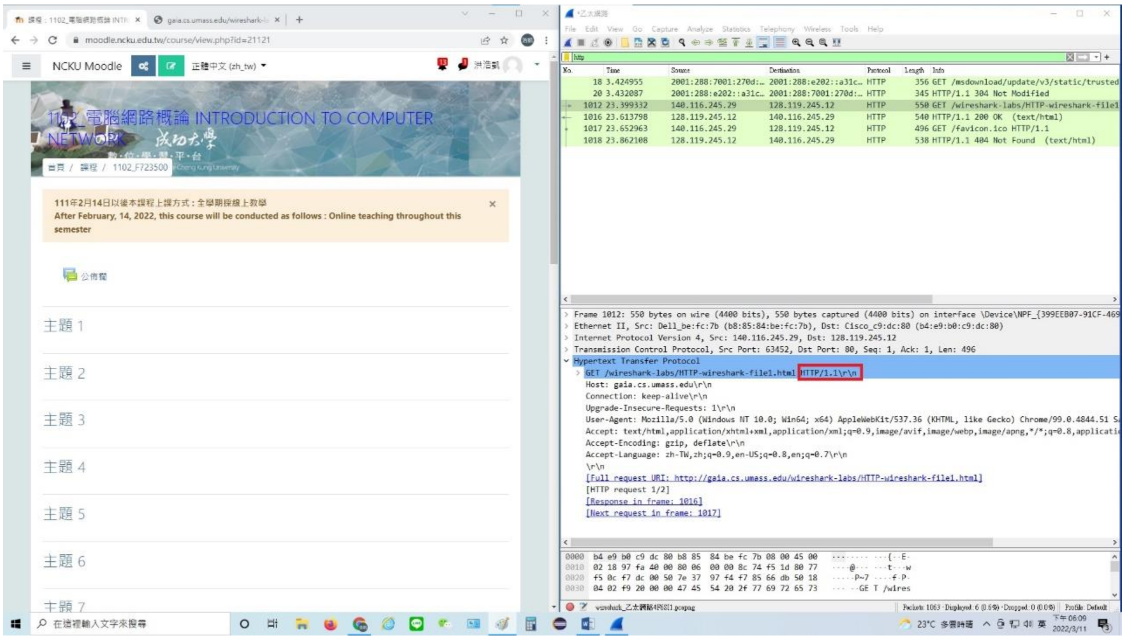
HW rules:

(Please take a screenshot to show your moodle and wireshark then highlight the answer or you will get no score.)

***Discussion is encouraged, but DO NOT share your homework to your classmate. If plagiarism is found, both students will get 0 score in this assignment.**

Example Question: Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running? Example

ANS:



```
No.   Time       Source               Destination          Protocol Length Info
   18 3.424955   2001:288:7001:270d:… 2001:288:e202::a31c… HTTP     356 GET /msdownload/update/v3/static/trusted
   20 3.432087   2001:288:e202::a31c… 2001:288:7001:270d:… HTTP     345 HTTP/1.1 304 Not Modified
 1012 23.399332  140.116.245.29       128.119.245.12       HTTP     550 GET /wireshark-labs/HTTP-wireshark-file1
 1016 23.613798  128.119.245.12       140.116.245.29       HTTP     540 HTTP/1.1 200 OK  (text/html)
 1017 23.652963  140.116.245.29       128.119.245.12       HTTP     496 GET /favicon.ico HTTP/1.1
 1018 23.862108  128.119.245.12       140.116.245.29       HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 1012: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{399EEB07-91CF-469
> Ethernet II, Src: Dell_be:fc:7b (b8:85:84:be:fc:7b), Dst: Cisco_c9:dc:80 (b4:e9:b0:c9:dc:80)
> Internet Protocol Version 4, Src: 140.116.245.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 63452, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 S
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicati
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 1016]
    [Next request in frame: 1017]
```

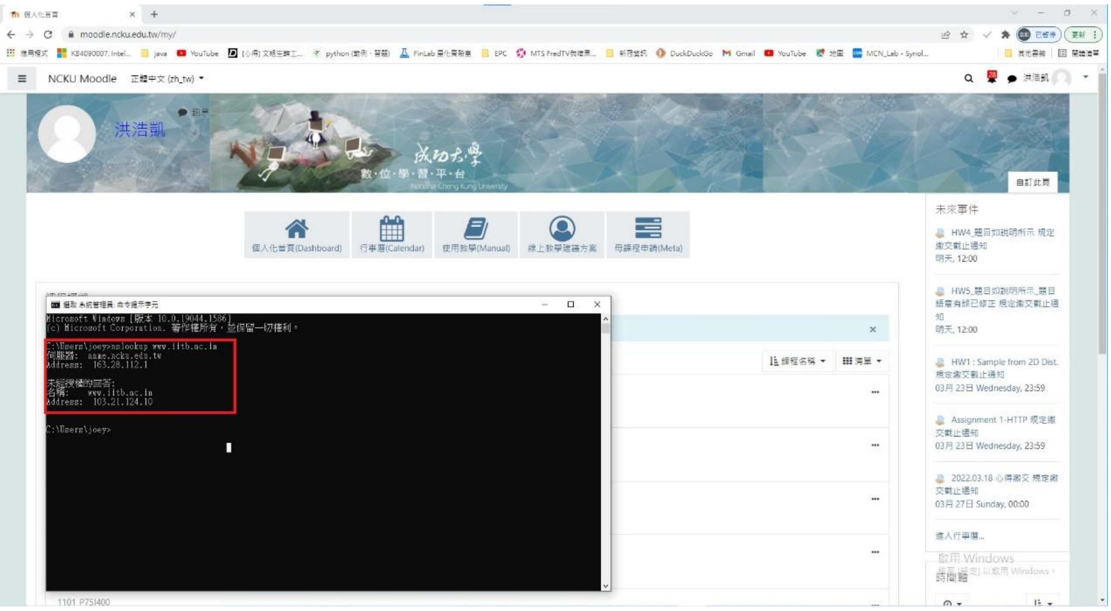
```
0000  b4 e9 b0 c9 dc 80 b8 85  84 be fc 7b 08 00 45 00   ········ ···{··E·
0010  02 18 97 fa 40 00 80 06  00 00 8c 74 f5 1d 80 77   ····@··· ···t···w
0020  f5 0c f7 dc 00 50 7e 37  97 f4 f7 85 66 db 50 18   ·····P~7 ····f·P·
0030  04 02 f9 20 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
```

NCKU Moodle
1102 電腦網路概論 INTRODUCTION TO COMPUTER NETWORK
111年2月14日以後本課程上課方式：全學期授線上教學
After February, 14, 2022, this course will be conducted as follows : Online teaching throughout this semester
主題 1
主題 2
主題 3
主題 4
主題 5
主題 6
主題 7
Packets: 1063 · Displayed: 6 (0.6%) · Dropped: 0 (0.0%)
Profile: Default
2022/3/11

Part I. nslookup operations (40%)

Descriptions:

Now that we’ve provided an overview of nslookup, it’s time for you to test drive it yourself. Do the following (You may find out the answer of question 1-1, 1-2 in selected region).



```
Microsoft Windows [版本 10.0.19044.1586]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users\joey>nslookup www.iitb.ac.in
伺服器:  name.ncku.edu.tw
Address:  163.28.112.1

未經授權的回答:
名稱:    www.iitb.ac.in
Address:  103.21.124.10

C:\Users\joey>
```

Question 1-1: Run nslookup to obtain the IP address of the web server for the Indian Institute of Technology in Bombay, India: www.iitb.ac.in. What is the IP address of www.iitb.ac.in. (15%)

Question 1-2: What is the IP address of the DNS server that provided the answer to your nslookup command in question 1 above? (15%)

Question 1-3: Did the answer to your nslookup command in question 1 above come from an authoritative or non-authoritative server?
(Hint: You can use nslookup -type=NS to check and answer authoritative or non-authoritative server 10%)

Part II. Tracing DNS with Wireshark (60%)

Now that we are familiar with nslookup and clearing the DNS resolver cache, we're ready to get down to some serious business. Let's first capture the DNS messages that are generated by ordinary Web-surfing activity.

You can also explicitly clear the records in your DNS cache. There's no harm in doing so – it will just mean that your computer will need to invoke the distributed DNS service next time it needs to use the DNS name resolution service, since it will find no records in the cache.
On a Mac computer, you can enter the following command into a terminal window to clear your DNS resolver cache:

```
sudo killall -HUP mDNSResponder
```

On Windows computer you can enter the following command at the command prompt:

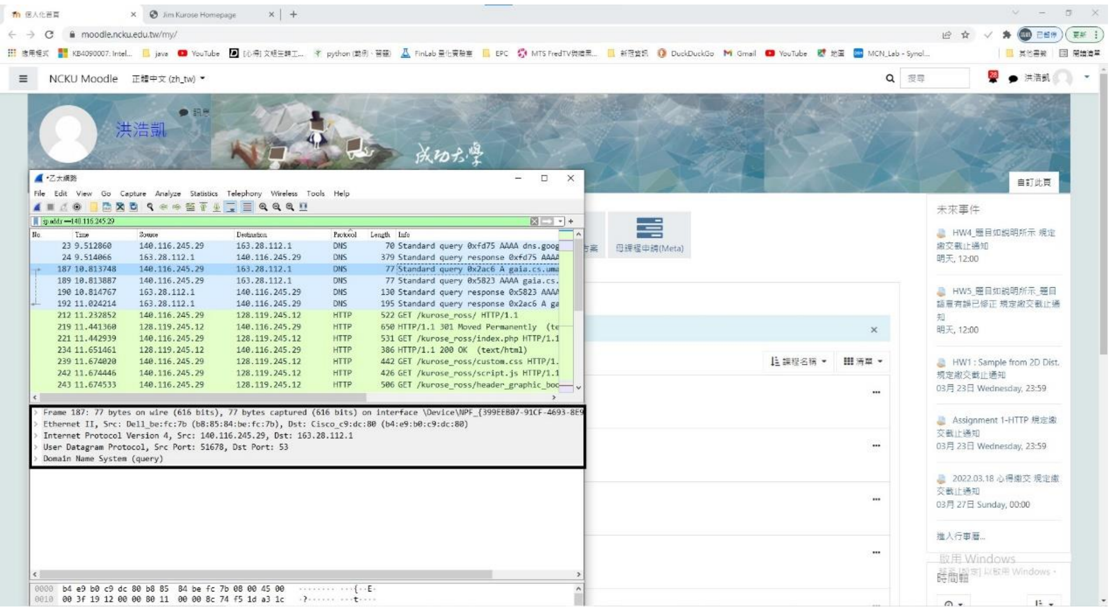
```
ipconfig /flushdns
```

and on a Linux computer, enter:

```
sudo systemd-resolve --flush-caches
```

- Clear the DNS cache in your host, as described above.
- Open your Web browser and clear your browser cache.
- Open Wireshark and enter ip.addr == <your_IP_address> into the display filter, where <your_IP_address> is the IPv4 address of your computer . With this filter, Wireshark will only display packets that either originate from, or are destined to, your host.
- Start packet capture in Wireshark.
- With your browser, visit the Web page: http://gaia.cs.umass.edu/kurose_ross/
- Stop packet capture.

Question 2-1: Locate the first DNS query message resolving the name gaia.cs.umass.edu. Is this query message sent over UDP or TCP? (The answer may found in marked region 10%)



ip.addr==140.116.245.29

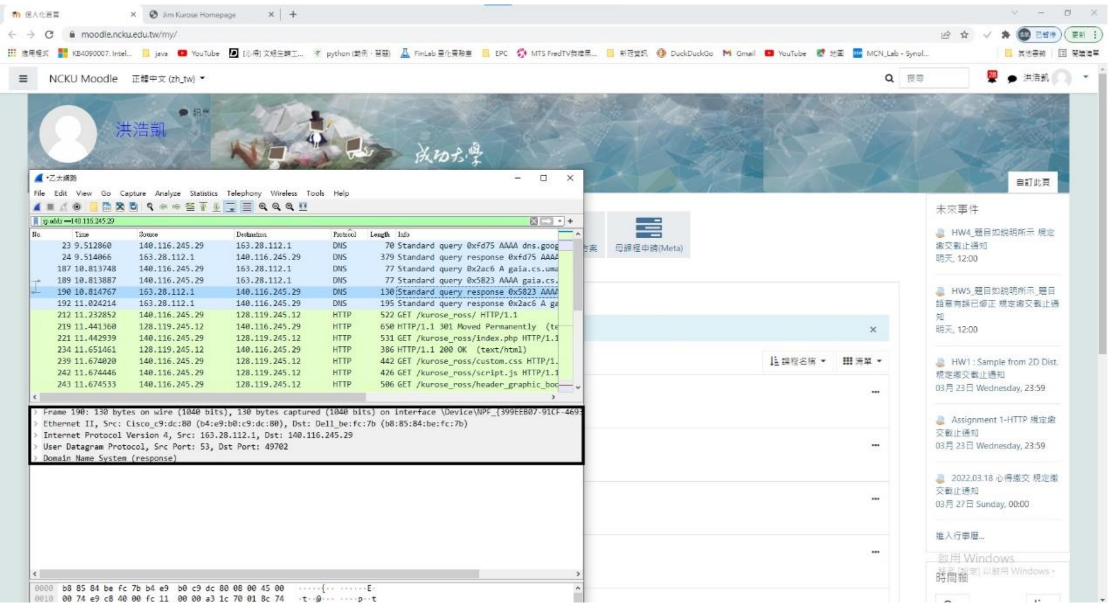
```
No.  Time       Source          Destination     Protocol Length Info
  23 9.512860   140.116.245.29  163.28.112.1    DNS         70 Standard query 0xfd75 AAAA dns.goog
  24 9.514066   163.28.112.1    140.116.245.29  DNS        379 Standard query response 0xfd75 AAAA
 187 10.813748  140.116.245.29  163.28.112.1    DNS         77 Standard query 0x2ac6 A gaia.cs.uma
 189 10.813887  140.116.245.29  163.28.112.1    DNS         77 Standard query 0x5823 AAAA gaia.cs.
 190 10.814767  163.28.112.1    140.116.245.29  DNS        130 Standard query response 0x5823 AAAA
 192 11.024214  163.28.112.1    140.116.245.29  DNS        195 Standard query response 0x2ac6 A ga
 212 11.232852  140.116.245.29  128.119.245.12  HTTP       522 GET /kurose_ross/ HTTP/1.1
 219 11.441360  128.119.245.12  140.116.245.29  HTTP       650 HTTP/1.1 301 Moved Permanently  (te
 221 11.442939  140.116.245.29  128.119.245.12  HTTP       531 GET /kurose_ross/index.php HTTP/1.1
 234 11.651461  128.119.245.12  140.116.245.29  HTTP       386 HTTP/1.1 200 OK  (text/html)
 239 11.674020  140.116.245.29  128.119.245.12  HTTP       442 GET /kurose_ross/custom.css HTTP/1.
 242 11.674446  140.116.245.29  128.119.245.12  HTTP       426 GET /kurose_ross/script.js HTTP/1.1
 243 11.674533  140.116.245.29  128.119.245.12  HTTP       506 GET /kurose_ross/header_graphic_boo
```

```
> Frame 187: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{399EEB07-91CF-4693-8E9
> Ethernet II, Src: Dell_be:fc:7b (b8:85:84:be:fc:7b), Dst: Cisco_c9:dc:80 (b4:e9:b0:c9:dc:80)
> Internet Protocol Version 4, Src: 140.116.245.29, Dst: 163.28.112.1
> User Datagram Protocol, Src Port: 51678, Dst Port: 53
> Domain Name System (query)
```

```
0000  b4 e9 b0 c9 dc 80 b8 85  84 be fc 7b 08 00 45 00
0010  00 3f 19 12 00 00 80 11  00 00 8c 74 f5 1d a3 1c
```

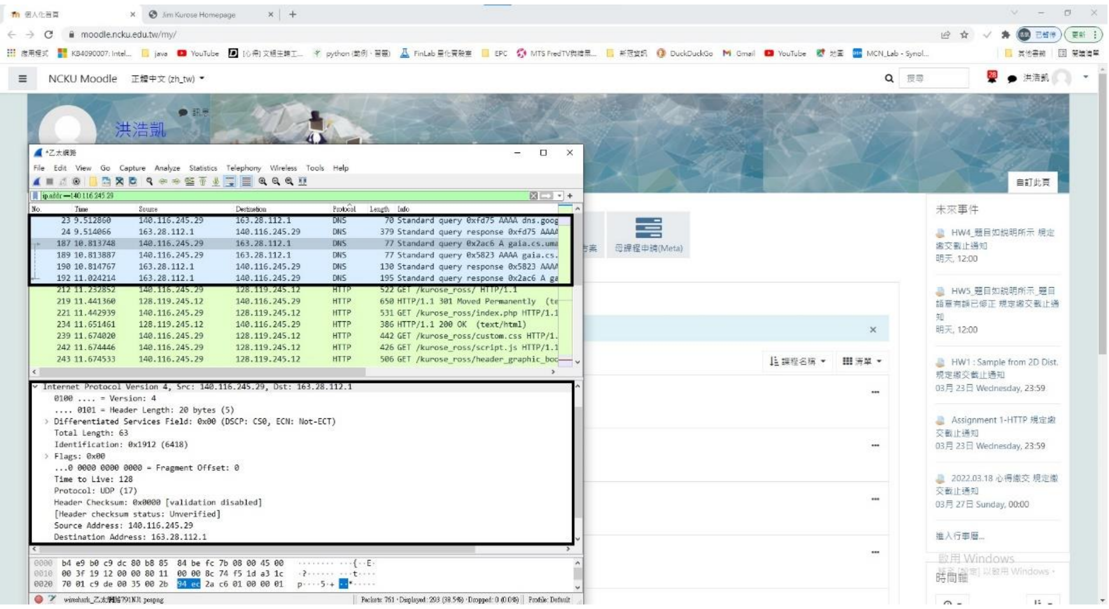
*乙太網路
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
NCKU Moodle
洪浩凱
未來事件

Question 2-2: What is the destination port for the DNS query message? What is the source port of the DNS response message? (The answer may found in marked region 10%)



```
ip.addr==140.116.245.29

No.   Time        Source           Destination      Protocol Length Info
   23 9.512860    140.116.245.29   163.28.112.1     DNS        70 Standard query 0xfd75 AAAA dns.goog
   24 9.514066    163.28.112.1     140.116.245.29   DNS       379 Standard query response 0xfd75 AAAA
  187 10.813748   140.116.245.29   163.28.112.1     DNS        77 Standard query 0x2ac6 A gaia.cs.uma
  189 10.813887   140.116.245.29   163.28.112.1     DNS        77 Standard query 0x5823 AAAA gaia.cs.
  190 10.814767   163.28.112.1     140.116.245.29   DNS       130 Standard query response 0x5823 AAAA
  192 11.024214   163.28.112.1     140.116.245.29   DNS       195 Standard query response 0x2ac6 A ga
  212 11.232852   140.116.245.29   128.119.245.12   HTTP      522 GET /kurose_ross/ HTTP/1.1
  219 11.441360   128.119.245.12   140.116.245.29   HTTP      650 HTTP/1.1 301 Moved Permanently  (te
  221 11.442939   140.116.245.29   128.119.245.12   HTTP      531 GET /kurose_ross/index.php HTTP/1.1
  234 11.651461   128.119.245.12   140.116.245.29   HTTP      386 HTTP/1.1 200 OK  (text/html)
  239 11.674020   140.116.245.29   128.119.245.12   HTTP      442 GET /kurose_ross/custom.css HTTP/1.
  242 11.674446   140.116.245.29   128.119.245.12   HTTP      426 GET /kurose_ross/script.js HTTP/1.1
  243 11.674533   140.116.245.29   128.119.245.12   HTTP      506 GET /kurose_ross/header_graphic_boo

> Frame 190: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface \Device\NPF_{399EEB07-91CF-469
> Ethernet II, Src: Cisco_c9:dc:80 (b4:e9:b0:c9:dc:80), Dst: Dell_be:fc:7b (b8:85:84:be:fc:7b)
> Internet Protocol Version 4, Src: 163.28.112.1, Dst: 140.116.245.29
> User Datagram Protocol, Src Port: 53, Dst Port: 49702
> Domain Name System (response)

0000  b8 85 84 be fc 7b b4 e9  b0 c9 dc 80 08 00 45 00   .....{.. ......E.
0010  00 74 e9 c8 40 00 fc 11  00 00 a3 1c 70 01 8c 74   .t..@... ....p..t
```

Question 2-3: To what IP address is the DNS query message sent? (The answer may found in marked region 10%)

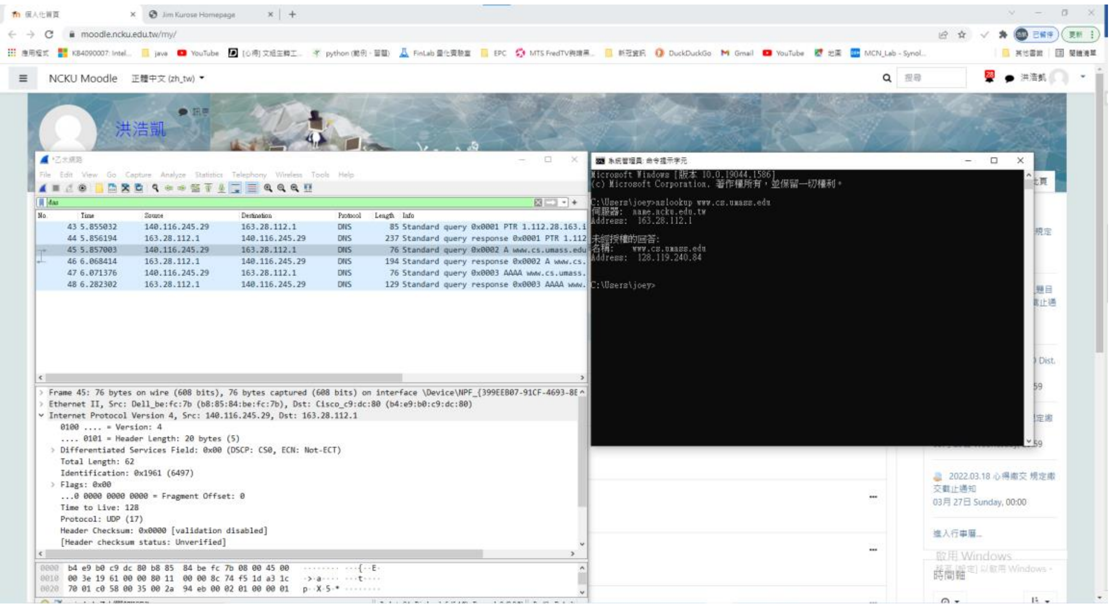


```
ip.addr==140.116.245.29

No.   Time        Source           Destination      Protocol Length Info
   23 9.512860    140.116.245.29   163.28.112.1     DNS        70 Standard query 0xfd75 AAAA dns.goog
   24 9.514066    163.28.112.1     140.116.245.29   DNS       379 Standard query response 0xfd75 AAAA
  187 10.813748   140.116.245.29   163.28.112.1     DNS        77 Standard query 0x2ac6 A gaia.cs.uma
  189 10.813887   140.116.245.29   163.28.112.1     DNS        77 Standard query 0x5823 AAAA gaia.cs.
  190 10.814767   163.28.112.1     140.116.245.29   DNS       130 Standard query response 0x5823 AAAA
  192 11.024214   163.28.112.1     140.116.245.29   DNS       195 Standard query response 0x2ac6 A ga
  212 11.232852   140.116.245.29   128.119.245.12   HTTP      522 GET /kurose_ross/ HTTP/1.1
  219 11.441360   128.119.245.12   140.116.245.29   HTTP      650 HTTP/1.1 301 Moved Permanently  (te
  221 11.442939   140.116.245.29   128.119.245.12   HTTP      531 GET /kurose_ross/index.php HTTP/1.1
  234 11.651461   128.119.245.12   140.116.245.29   HTTP      386 HTTP/1.1 200 OK  (text/html)
  239 11.674020   140.116.245.29   128.119.245.12   HTTP      442 GET /kurose_ross/custom.css HTTP/1.
  242 11.674446   140.116.245.29   128.119.245.12   HTTP      426 GET /kurose_ross/script.js HTTP/1.1
  243 11.674533   140.116.245.29   128.119.245.12   HTTP      506 GET /kurose_ross/header_graphic_boo

v Internet Protocol Version 4, Src: 140.116.245.29, Dst: 163.28.112.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 63
    Identification: 0x1912 (6418)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 140.116.245.29
    Destination Address: 163.28.112.1

0000  b4 e9 b0 c9 dc 80 b8 85  84 be fc 7b 08 00 45 00   ........ ...{..E.
0010  00 3f 19 12 00 00 80 11  00 00 8c 74 f5 1d a3 1c   .?...... ...t....
0020  70 01 c9 de 00 35 00 2b  94 ec 2a c6 01 00 00 01   p....5.+ ..*.....

wireshark_乙太網路791KJ1.pcapng     Packets: 761 · Displayed: 203 (38.5%) · Dropped: 0 (0.0%)     Profile: Default
```

Now let's play with nslookup.

- Start packet capture.
- Do an nslookup on www.cs.umass.edu
- Stop packet capture.

You should get a trace that looks something like the following in your Wireshark window.



```
dns
No.  Time       Source          Destination     Protocol Length Info
  43 5.855032   140.116.245.29  163.28.112.1    DNS       85 Standard query 0x0001 PTR 1.112.28.163.i
  44 5.856194   163.28.112.1    140.116.245.29  DNS      237 Standard query response 0x0001 PTR 1.112
  45 5.857003   140.116.245.29  163.28.112.1    DNS       76 Standard query 0x0002 A www.cs.umass.edu
  46 6.068414   163.28.112.1    140.116.245.29  DNS      194 Standard query response 0x0002 A www.cs.
  47 6.071376   140.116.245.29  163.28.112.1    DNS       76 Standard query 0x0003 AAAA www.cs.umass.
  48 6.282302   163.28.112.1    140.116.245.29  DNS      129 Standard query response 0x0003 AAAA www.
```

```
> Frame 45: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{399EEB07-91CF-4693-8E
> Ethernet II, Src: Dell_be:fc:7b (b8:85:84:be:fc:7b), Dst: Cisco_c9:dc:80 (b4:e9:b0:c9:dc:80)
v Internet Protocol Version 4, Src: 140.116.245.29, Dst: 163.28.112.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 62
    Identification: 0x1961 (6497)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  b4 e9 b0 c9 dc 80 b8 85  84 be fc 7b 08 00 45 00   ········ ···{··E·
0010  00 3e 19 61 00 00 80 11  00 00 8c 74 f5 1d a3 1c   ·>·a···· ···t····
0020  70 01 c0 58 00 35 00 2a  94 eb 00 02 01 00 00 01   p··X·5·* ········
```

```
Microsoft Windows [版本 10.0.19044.1586]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users\joey>nslookup www.cs.umass.edu
伺服器:  name.ncku.edu.tw
Address:  163.28.112.1

未經授權的回答:
名稱:    www.cs.umass.edu
Address:  128.119.240.84


C:\Users\joey>
```

NCKU Moodle
洪浩凱
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
系統管理員: 命令提示字元

Question 2-4: What is the destination port for the DNS query message? What is the source port of the DNS response message? (15%)

Question 2-5: To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? (You need to show the screenshot and answer Yes or No. 15%)