HW5 DHCP

HW rules:

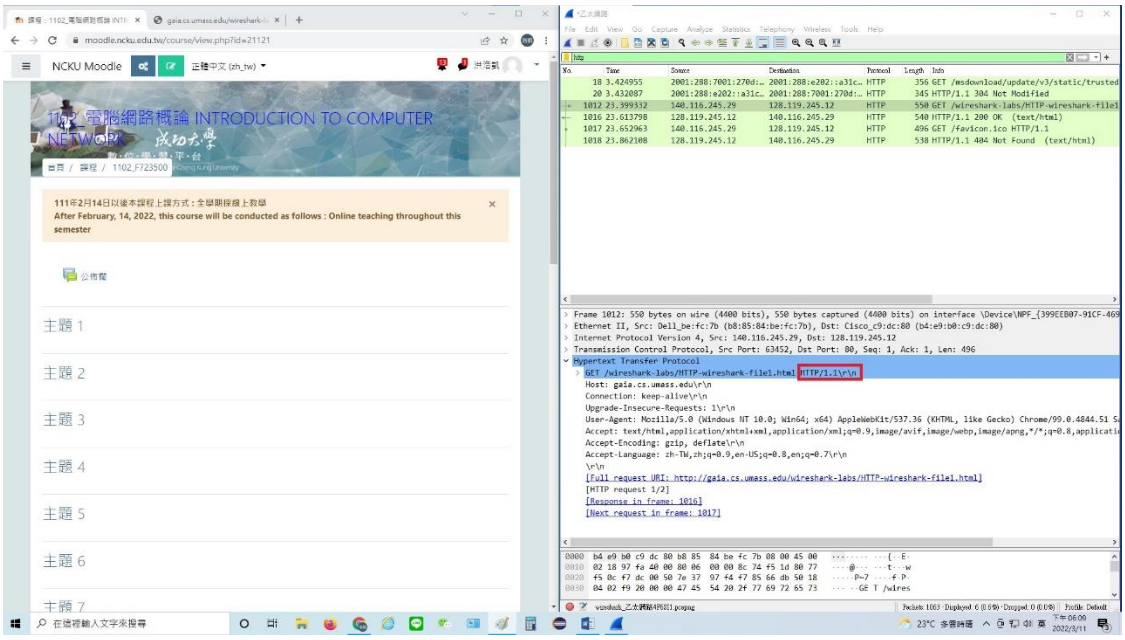
(Please take a screenshot to show your moodle and wireshark then highlight the answer or you will get no score.)

Note: Handing late will lead to a perceptibly lower 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:



課程：1102_電腦網路概論 INTR
gaia.cs.umass.edu/wireshark-l
moodle.ncku.edu.tw/course/view.php?id=21121
NCKU Moodle
正體中文 (zh_tw)
洪浩凱
1102_電腦網路概論 INTRODUCTION TO COMPUTER NETWORK
成功大學
數·位·學·習·平·台
首頁 / 課程 / 1102_F723500
公佈欄
主題 1
主題 2
主題 3
主題 4
主題 5
主題 6
主題 7
在這裡輸入文字來搜尋
*乙太網路
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

111年2月14日以後本課程上課方式：全學期採線上教學
After February, 14, 2022, this course will be conducted as follows : Online teaching throughout this semester

```
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
```

wireshark_乙太網路4F6SI1.pcapng
Packets: 1063 · Displayed: 6 (0.6%) · Dropped: 0 (0.0%)
Profile: Default
23°C 多雲時晴
下午 06:09
2022/3/11

HW5 DHCP:

Description:

Gathering a Packet Trace

The first two steps in the DHCP protocol in Figure 4.24 (using the Discover and Offer messages) are optional (in the sense that they need not always be used when, for example, a new IP address is needed, or an existing DHCP address is to be renewed); the Request and ACK messages are not. In order to collect a trace that will contain all four DHCP message types, we'll need to take a few command line actions on a Mac, Linux or PC.

On a Mac:

1. In a terminal window/shell enter the following command:
   ```
   % sudo ipconfig set en0 none
   ```
   Where en0 (in this example) is the interface on which you want to capture packets using Wireshark. You can easily find the list of interface names in Wireshark by choosing Capture->options. This command will de-configure network interface en0.
2. Start up Wireshark, capturing packets on the interface you de-configured in Step 1.
3. In the terminal window/shell enter the following command:
   ```
   % sudo ipconfig set en0 dhcp
   ```
   This will cause the DHCP protocol to request and receive an IP address and other information from the DHCP server.
4. After waiting for a few seconds, stop Wireshark capture.

On a Linux machine:

1. In a terminal window/shell, enter the following commands:
   ```
   sudo ip addr flush en0
   sudo dhclient -r
   ```
   where en0 (in this example) is the interface on which you want to capture packets using Wireshark. You can easily find the list of interface names in Wireshark by choosing Capture -> Options. This command will remove the existing IP address of the interface, and release any existing DHCP address leases.
2. Start up Wireshark, capturing packets in the interface you de-configured in Step 1.

3. In the terminal window/shell, enter the following command:

   sudo dhclient en0

   where, as with above, en0 is the interface on which you are currently capturing packets. This will cause the DHCP protocol to request and receive an IP address and other information from the DHCP server.
4. After waiting for a few seconds, stop Wireshark capture.

On a PC:

1. In a command-line window enter the following command:

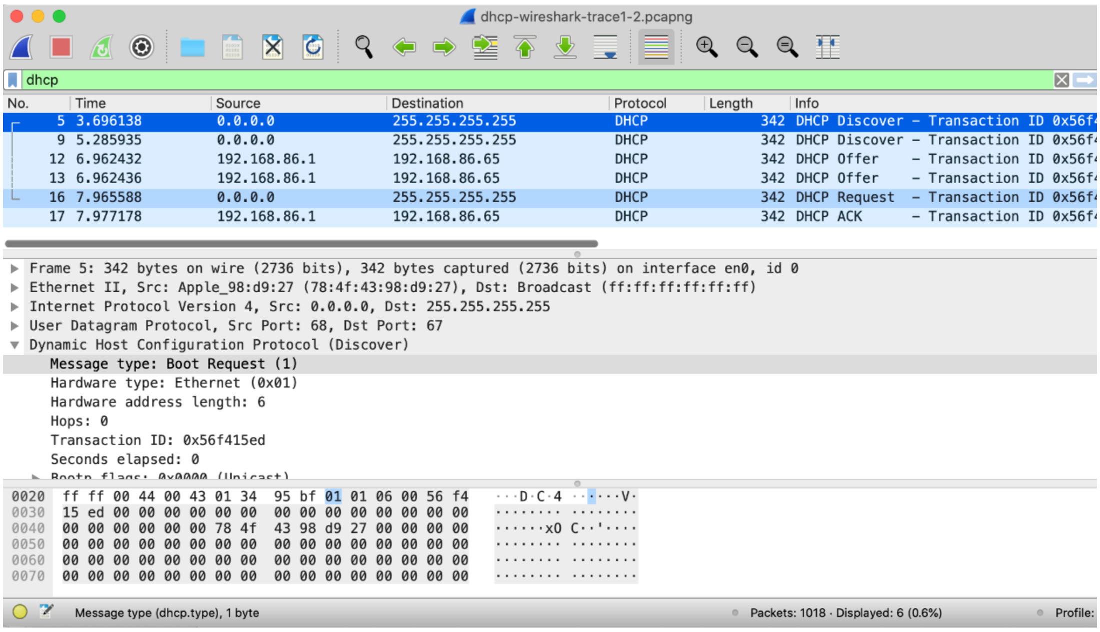
   > ipconfig /release

   This command will cause your PC to give up its IP address.
2. Start up Wireshark.
3. In the command-line window enter the following command:

   > ipconfig /renew

   This will cause the DHCP protocol to request and receive an IP address and other information from a DHCP server.
4. After waiting for a few seconds, stop Wireshark capture.

After stopping Wireshark capture in step 4, you should take a peek in your Wireshark window to make sure you've actually captured the packets that we're looking for. If you enter "dhcp" into the display filter field (as shown in the light green field in the top left of Figure 1), your screen (on a Mac) should look similar to Figure 1.



dhcp

```
No.   Time       Source          Destination       Protocol  Length  Info
   5  3.696138   0.0.0.0         255.255.255.255   DHCP         342  DHCP Discover - Transaction ID 0x56f4
   9  5.285935   0.0.0.0         255.255.255.255   DHCP         342  DHCP Discover - Transaction ID 0x56f4
  12  6.962432   192.168.86.1    192.168.86.65     DHCP         342  DHCP Offer    - Transaction ID 0x56f4
  13  6.962436   192.168.86.1    192.168.86.65     DHCP         342  DHCP Offer    - Transaction ID 0x56f4
  16  7.965588   0.0.0.0         255.255.255.255   DHCP         342  DHCP Request  - Transaction ID 0x56f4
  17  7.977178   192.168.86.1    192.168.86.65     DHCP         342  DHCP ACK      - Transaction ID 0x56f4
```

```
▶ Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▶ User Datagram Protocol, Src Port: 68, Dst Port: 67
▼ Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x56f415ed
    Seconds elapsed: 0
  ▶ Bootp flags: 0x0000 (Unicast)
```

```
0020  ff ff 00 44 00 43 01 34  95 bf 01 01 06 00 56 f4   ···D·C·4 ······V·
0030  15 ed 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 78 4f  43 98 d9 27 00 00 00 00   ······xO C··'····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Message type (dhcp.type), 1 byte

Packets: 1018 · Displayed: 6 (0.6%)

Profile:

Figure 1: Wireshark display, showing the capture of DHCP Discover, Offer, Request and ACK messages

DHCP Questions:

Let’s start by looking at the DHCP Discover message. Locate the IP datagram containing the first Discover message in your trace.

Question 1: Is this DHCP Discover message sent out using UDP or TCP as the underlying transport protocol? **(10%)**

Question 2: What is the source IP address used in the IP datagram containing the Discover message? **(10%)**

Question 3: What is the destination IP address used in the datagram containing the Discover message? **(10%)**

Now let’s look at the DHCP Offer message. Locate the IP datagram containing the DHCP Offer message in your trace that was sent by a DHCP server in the response to the DHCP Discover message that you studied in questions 1-3 above.

Question 4: How do you know that this Offer message is being sent in response to the DHCP Discover message you studied in questions 1-3 above? **(20%)**

It would appear that once the DHCP Offer message is received, that the client may have all of the information it needs to proceed. However, the client may have received OFFERs from multiple DHCP servers and so a second phase is needed, with two more mandatory messages – the client-to-server DHCP Request message, and the server-to-client DHCP ACK message is needed. But at least the client knows there is at least one DHCP server out there! Let’s take a look at the DHCP Request message, remembering that although we’ve already seen a Discover message in our trace, that is not always the case when a DHCP request message is sent.

Locate the IP datagram containing the first DHCP Request message in your trace, and answer the following questions.

Question 5: What is the UDP source port number in the IP datagram containing the first DHCP Request message in your trace? What is the UDP destination port number being used? **(20%)**

Question 6: What is the value in the transaction ID field of this DHCP Request message? Does it match the transaction IDs of the earlier Discover and Offer messages? **(10%)**

Locate the IP datagram containing the first DHCP ACK message in your trace, and answer the following questions.

Question 7: What is the name of the field in the DHCP ACK message (as indicated in the Wireshark window) that contains the assigned client IP address? **(10%)**

Question 8: For how long a time (the so-called “lease time”) has the DHCP server assigned this IP address to the client? **(10%)**