Question A

1) จาก ICMP echo request ที่ส่งจากเครื่องของผู้เรียนไปยัง gaia.cs.umass.edu แต่ละ echo request ถูกแบ่งออกเป็น IPv4 datagrams กี่ datagrams? แต่ละ datagram มีขนาดเท่าใดบ้าง?

ip.id == 0x81e9

No.	Time	Source	Destination	RTT	Protocol	Length	Next Sequence
1	0.000000	172.20.10.2	172.20.10.1		IPv4	1514	
2	0.000000	172.20.10.2	172.20.10.1		IPv4	1514	
3	0.000000	172.20.10.2	172.20.10.1		ICMP	1074	

Answer แบ่งออกเป็น 3 datagrams โดยแต่ละ datagram จะมีขนาด 1514,1514,1074 bytes ตามลำดับ (สังเกตจาก field identification ใน ip protocol)

2) จาก ICMP echo reply ที่ส่งจาก gaia.cs.umass.edu มายังเครื่องผู้เรียน แต่ละ echo reply ถูกแบ่งออกเป็น IPv4 datagrams กี่ datagrams? แต่ละ datagram มีขนาดเท่าใดบ้าง?

ip.id == 0xc74b

No.	Time	Source	Destination	RTT	Protocol	Length	Next Sequence Num
10	9.821162	172.20.10.1	172.20.10.2		IPv4	1514	
11	9.821162	172.20.10.1	172.20.10.2		IPv4	1514	
12	9.821162	172.20.10.1	172.20.10.2	17.313	ICMP	1074	

Answer แบ่งออกเป็น 3 datagrams โดยแต่ละ datagram จะมีขนาด 1514,1514,1074 bytes ตามลำดับ (สังเกตจาก field identification ใน ip protocol)

3) พิจารณาขนาดของแต่ละ IPv4 fragment จากข้อ 1) และ 2) หลังจากผ่านการ fragmentation แล้ว แต่ละคู่ echo request / echo reply ถูกแบ่งเป็น IPv4 datagrams โดยฝั่งผู้ส่งและผู้รับมีแนวทางการกำหนดขนาดของแต่ละ IPv4 fragment เหมือนหรือต่างกันอย่างไร? จงอธิบาย

Answer มีแนวทางการกำหนดขนาดของแต่ละ IPv4 fragment เหมือนกันโดยขนาดของ datagram จะไม่มากกว่า 1514 bytes ทั้ง echo request / echo reply

4) ข้อมูลใดใน IPv4 header ที่สามารถใช้บ่งบอกว่า datagram นี้ผ่านการ fragmentation มาแล้ว?

Answer จะมี fragment offset,flags,id โดยหาก flags ของ more fragments ถูก set หมายความว่าผ่านการ fragmentation มาแล้วยังไม่ใช่ packet สุดท้าย ส่วนถ้า offset มีค่ามากที่สุด more fragments มีค่าเป็น 0 หมายความว่าเป็น packet สุดท้ายของ packet ที่มาจาก id เดียวกัน

5) ข้อมูลใดใน IPv4 header ที่สามารถใช้บ่งบอกว่า packet นั้นเป็น fragment แรกหรือเป็น fragment สุดท้าย?

ip.flags.mf == 1 and ip.frag_offset == 0

No.	Time	Source	Destination	RTT	Protocol	Length	Next Sequence
1	0.000000	172.20.10.2	172.20.10.1		IPv4	1514	
4	4.819946	172.20.10.2	172.20.10.1		IPv4	1514	
7	9.803849	172.20.10.2	172.20.10.1		IPv4	1514	
10	9.821162	172.20.10.1	172.20.10.2		IPv4	1514	
13	10.822807	172.20.10.2	172.20.10.1		IPv4	1514	
16	10.839180	172.20.10.1	172.20.10.2		IPv4	1514	

(first fragment packet)

ip.flags.mf == 0

No.	Time	Source	Destination	RTT	Protocol	Length	Next Sequence Nu
3	0.000000	172.20.10.2	172.20.10.1		ICMP	1074	
6	4.819946	172.20.10.2	172.20.10.1		ICMP	1074	
9	9.803849	172.20.10.2	172.20.10.1		ICMP	1074	
12	9.821162	172.20.10.1	172.20.10.2	17.313	ICMP	1074	
15	10.822807	172.20.10.2	172.20.10.1		ICMP	1074	
18	10.839180	172.20.10.1	172.20.10.2	16.373	ICMP	1074	

(last fragment packet)

Answer fragment packet แรกสามารถบอกได้จาก more fragment flag มีค่าเป็น 1 และ fragment offset มีค่าเป็น 0 ส่วน fragment packet สุดท้ายเป็น packet ที่มี more fragment flag มีค่าเป็น 0 และ fragment offset มีค่ามากที่สุด

6) พิจารณา IPv4 datagram ที่เป็น fragment ลำดับที่ 2 จากการทำ fragmentation ข้อมูลใดใน IPv4 header ที่สามารถใช้บ่งบอกว่า datagram นี้ไม่ใช่ fragment แรก และไม่ใช่ fragment สุดท้าย?

ip.flags.mf == 1 and ip.frag_offset != 0

No.	Time	Source	Destination	RTT	Protocol	Length	Next Sequence Nu
2	0.000000	172.20.10.2	172.20.10.1		IPv4	1514	
5	4.819946	172.20.10.2	172.20.10.1		IPv4	1514	
8	9.803849	172.20.10.2	172.20.10.1		IPv4	1514	
11	9.821162	172.20.10.1	172.20.10.2		IPv4	1514	
14	10.822807	172.20.10.2	172.20.10.1		IPv4	1514	
17	10.839180	172.20.10.1	172.20.10.2		IPv4	1514	

(second fragment packet)

Answer โดย packet ที่ไม่ใช่ทั้ง fragment แรก และไม่ใช่ fragment สุดท้ายสามารถระบุได้จากการที่มี more fragment flag ค่าเป็น 1 และ fragment offset ไม่ใช่ 0 (ในการทดลองนี้มีจำนวน 3 fragments วิธีนี้จึงเป็นการระบุ fragment ที่สองได้แต่หากมากกว่า 3 fragments วิธีนี้ไม่สามารถระบุ fragmentลำกับที่2ได้)

7) หลังจาก fragmentation หากเปรียบเทียบระหว่าง fragment แรก และ fragment ที่สอง ค่าของ field ใดที่เปลี่ยนแปลงไป?

```
✓ 001. .... = Flags: 0x1, More fragments
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
  ...0 0000 1011 1001 = Fragment Offset: 1480
```

Answer ค่า field fragment offset โดย fragment แรกมีค่าเป็น 0 ส่วน fragment ที่สองมีค่าเป็น 1480

8) พิจารณา IPv4 datagram ที่เป็น fragment ลำดับที่ 3 จากการทำ fragmentation ข้อมูลใดใน IPv4 header ที่สามารถใช้บ่งบอกว่า datagram นี้เป็น fragment สุดท้าย?

```
✓ 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
```

Answer more flagments flag ใน flags มีการ set ค่าเป็น 0

Question B

9) ตรวจสอบ DHCP Discover message ว่าถูกส่งออกไปโดยใช้ Transport Layer Protocol เป็น UDP หรือ TCP?

```
> Frame 1: 358 bytes on wire (2864 bits), 358 bytes captur
> Ethernet II, Src: ChongqingFug_85:1c:00 (a8:93:4a:85:1c:
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.
> User Datagram Protocol, Src Port: 68, Dst Port: 67
✓ Dynamic Host Configuration Protocol (Request)
```

Answer DHCP Discover message ถูกส่งออกไปโดยใช้ Transport Layer Protocol เป็น UDP

10) ตรวจสอบ IP datagram ซึ่งบรรจุ Discover message ว่าใช้หมายเลข source IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

Answer Discover message ใช้หมายเลข source IP address เป็น 0.0.0.0 ซึ่งเป็นหมายเลข default ใช้สำหรับบ่งบอก address ที่ยังไม่ทราบหรือยังไม่ถูก assign (สำหรับ DHCP client จะเริ่มต้นด้วย ip address นี้ก่อนที่จะได้ ip address ที่ถูกต้อง)

11) ตรวจสอบ IP datagram ซึ่งบรรจุ Discover message ว่าใช้หมายเลข destination IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

Answer Discover message ใช้หมายเลข destination IP address เป็น 255.255.255.255 เป็นหมายเลข boardcast address (ใช้ตะโกนบอกทุกๆ device ใน subnetนั้นๆ)

12) ค่าของ transaction ID ที่อยู่ใน DHCP Discover message มีค่าเป็นเท่าใด?

```
✓ Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xaee0df1d
```

Answer มีค่าเป็น 0xaee0df1d (จาก DHCP field Transaction ID)

13) ตรวจสอบ Option ใน DHCP Discover message มีข้อมูลใดอื่นอีกบ้างนอกจากหมายเลข IP address ที่ client เสนอหรือว่าร้องขอจาก DHCP server? จงระบุข้อมูลมาอย่างน้อย 5 อย่าง

```
> Option: (53) DHCP Message Type (Discover)
> Option: (61) Client identifier
> Option: (50) Requested IP Address (172.20.10.2)
> Option: (12) Host Name
> Option: (60) Vendor class identifier
> Option: (55) Parameter Request List
> Option: (255) End
```

Answer 1. DHCP Message Type
2. Client identifier
3. Host Name
4. Vendor class identifier
5.Parameter Request List
6. End

14) ผู้เรียนทราบได้อย่างไรว่า DHCP Offer message นี้ถูกส่งมาเพื่อตอบ DHCP Discover message ที่ผู้เรียนได้ศึกษาไปในข้อ 9) ถึงข้อ 13) ที่ผ่านมา

ip.dst == 172.20.10.2 and dhcp.id == 0xaee0df1d

No.	Time	Source	Destination	RTT	Protocol	Length	Next Sequence Nu
2	0.008346	172.20.10.1	172.20.10.2		DHCP	342	
4	0.029613	172.20.10.1	172.20.10.2		DHCP	342	

Answer เพราะ DHCP Offer message นั้นมี transaction id เหมือนกับ DHCP Discover message

15) ตรวจสอบ IP datagram ซึ่งบรรจุ Offer message ว่าใช้หมายเลข source IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

Answer IP datagram ที่บรรจุ Offer message ใช้หมายเลข source IP address เป็น 172.20.10.1 เป็นหมายเลข default gateway ที่ใช้ในการ route ไปยังภายนอกของ LAN

16) ตรวจสอบ IP datagram ซึ่งบรรจุ Offer message ว่าใช้หมายเลข destination IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย (คำใบ้: ตรวจสอบไฟล์ trace อย่างละเอียด คำตอบของคำถามนี้อาจจะแตกต่างจากภาพในเอกสารประกอบการเรียน)

Answer IP datagram ที่บรรจุ Offer message ใช้หมายเลข destination IP address เป็น 172.20.10.2 ซึ่งเป็น local private networks และจะถูกกำหนดให้ใช้ใน network

17) ตรวจสอบ Option ใน DHCP Offer message มีข้อมูลใดอื่นอีกบ้างนอกจากหมายเลข IP address ที่ DHCP server ส่งให้กับ DHCP client? จงระบุข้อมูลมาอย่างน้อย 5 อย่าง

```
> Option: (53) DHCP Message Type (ACK)
> Option: (54) DHCP Server Identifier (172.20.10.1)
> Option: (51) IP Address Lease Time
> Option: (1) Subnet Mask (255.255.255.240)
> Option: (3) Router
> Option: (6) Domain Name Server
> Option: (255) End
```

Answer 1. DHCP Message Type
2. IP Address Lease Time
3. Subnet Mask
4. Router
5. Domain Name Server
6. End

18) ตรวจสอบ IP datagram ซึ่งบรรจุ DHCP Request message ว่าใช้หมายเลข source port หมายเลขใด? และใช้ destination port หมายเลขใด?

```
Source Port: 67
Destination Port: 68
```

Answer source port เป็นหมายเลข 67 และหมายเลข destination port เป็นหมายเลข 68

19) ตรวจสอบ IP datagram ซึ่งบรรจุ Request message ว่าใช้หมายเลข source IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

Answer Request message ใช้หมายเลข source IP address เป็น 0.0.0.0 ซึ่งเป็นหมายเลข default ใช้สำหรับบ่งบอก address ที่ยังไม่ทราบหรือยังไม่ถูก assign (สำหรับ DHCP client จะเริ่มต้นด้วย ip address นี้ก่อนที่จะได้ ip address ที่ถูกต้อง)

20) ตรวจสอบ IP datagram ซึ่งบรรจุ Request message ว่าใช้หมายเลข destination IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

Answer Request message ใช้หมายเลข destination IP address เป็น 255.255.255.255 เป็นหมายเลข boardcast address (ใช้ตะโกนบอกทุกๆ device ใน subnetนั้นๆ)

21) ค่าของ transaction ID ที่อยู่ใน DHCP Request message มีค่าเป็นเท่าใด? ค่าดังกล่าวมีค่าตรงกับ transaction ID ใน Discover message และ Offer message ก่อนหน้านี้หรือไม่?

```
Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xaee0df1d
```

Answer มีค่าเป็น 0xaee0df1d (จาก DHCP field Transaction ID) โดยมีค่าตรงกะนใน Discover message และ Offer message

22) ตรวจสอบค่า Options ใน DHCP Discover message โดยให้ตรวจสอบ Parameter Request List ซึ่ง DHCP RFC ระบุเอาไว้ว่า

"The client can inform the server which configuration parameters the client is interested in by including the 'parameter request list' option. The data portion of this option explicitly lists the options requested by tag number."

ผู้เรียนสังเกตเห็นความแตกต่างใดบ้างระหว่าง Parameter Request List ที่พบใน Request message และ Discover message ก่อนหน้านี้

สำหรับคำถามส่วนสุดท้าย ให้ค้นหา DHCP ACK message จากไฟล์ trace และตอบคำถามต่อไปนี้

```
Option: (55) Parameter Request List
    Length: 14
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (31) Perform Router Discover
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (43) Vendor-Specific Information
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
    Parameter Request List Item: (119) Domain Search
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (252) Private/Proxy autodiscovery
```

(DHCP DISCOVER)

```
Option: (55) Parameter Request List
    Length: 14
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (31) Perform Router Discover
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (43) Vendor-Specific Information
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
    Parameter Request List Item: (119) Domain Search
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (252) Private/Proxy autodiscovery
```

(DHCP REQUEST)

Answer ไม่พบความแตกต่างเหมือนกันทุกประการ

23) ตรวจสอบ IP datagram ซึ่งบรรจุ ACK message ว่าใช้หมายเลข source IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

Answer IP datagram ที่บรรจุ ACK message ใช้หมายเลข source IP address เป็น 172.20.10.1 เป็นหมายเลข default gateway ที่ใช้ในการ route ไปยังภายนอกของ LAN

24) ตรวจสอบ IP datagram ซึ่งบรรจุ ACK message ว่าใช้หมายเลข destination IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

Answer IP datagram ที่บรรจุ ACK message ใช้หมายเลข destination IP address เป็น 172.20.10.2 ซึ่งเป็น local private networks และจะถูกกำหนดให้ใช้ใน network

25) ใน DHCP ACK message มี field ชื่ออะไร (ตามที่ปรากฏใน Wireshark) ที่เก็บค่าหมายเลข IP address ที่ DHCP server แจกจ่ายให้กับ client?

```
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xaee0df1d
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 172.20.10.2
```

Answer มี field Your (client) IP address ใน(DHCP protocol)

26) DHCP server อนุญาตให้ client ใช้งานหมายเลข IP เป็นระยะเวลานานเท่าใด? (คำใบ้: โปรดสังเกต lease time)

```
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (172.20.10.1)
  v Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: 1 day (86400)
```

Answer จาก DHCP Offer (ใน field option ใน DHCP protocol)

27) ใน DHCP ACK message ที่ DHCP server ส่งกลับมาให้กับ DHCP client ระบุหมายเลข IP ของ first-hop router (หรือที่เรียกว่า default gateway) เป็นหมายเลขอะไร?

```
  ⌄ Option: (3) Router
      Length: 4
      Router: 172.20.10.1
```

Answer หมายเลข 172.20.10.1 (ได้จาก DHCP ACK message ใน field option)