

# Lab 05: UDP and TCP Basics

ในปฏิบัติการครั้งนี้ผู้เรียนจะได้ศึกษาพฤติกรรมการทำงานเบื้องต้นของ User Datagram Protocol (UDP) และ Transmission Control Protocol (TCP) ซึ่งทั้งสอง protocols ถูกจัดว่าทำงานอยู่ในชั้น Transport-Layer

## A. User Datagram Protocol (UDP)

จากที่ได้เรียนรู้ไปแล้วในรายวิชาทฤษฎีว่า UDP ถูกออกแบบมาให้มีความคล่องตัว มีการทำงานไม่ซับซ้อน การทดลองในส่วนนี้จึงสามารถทำเสร็จได้ภายในเวลาไม่นาน

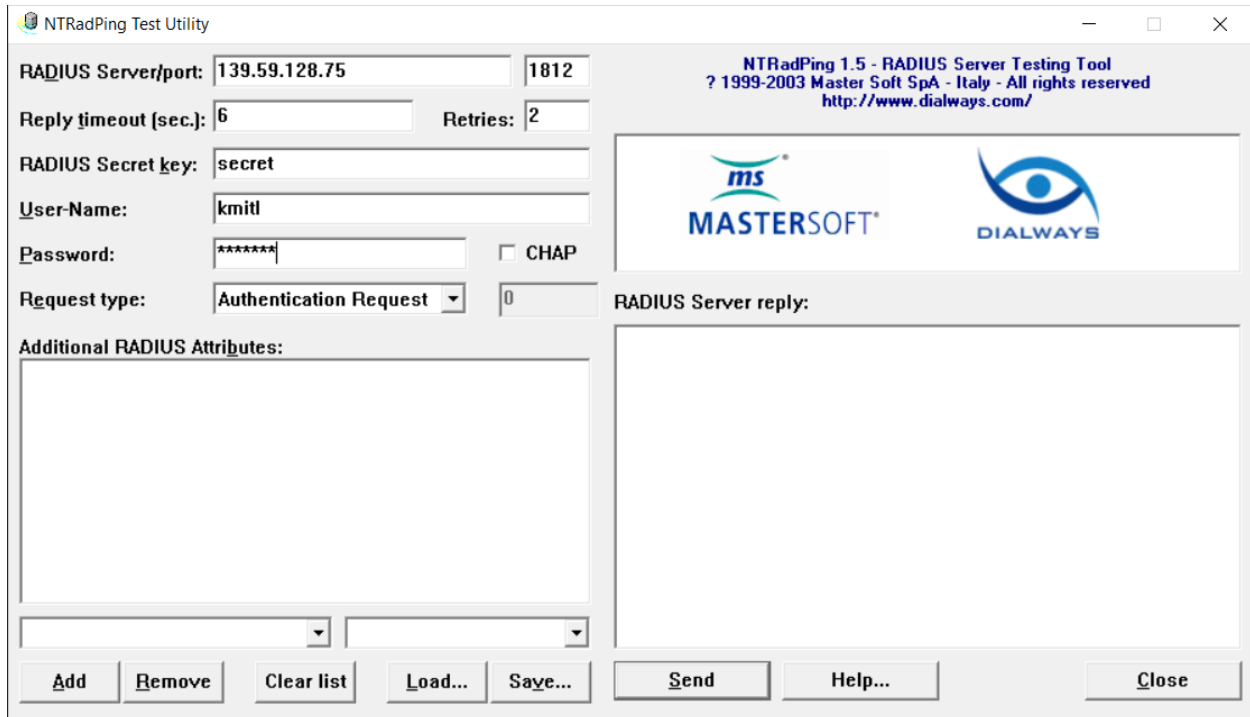
ลำดับในการทดลองนี้เริ่มจากการดักจับ packets ด้วย Wireshark และทำบางสิ่งที่ทำให้เครื่องของผู้เรียนส่งและได้รับ UDP packets จำนวนหนึ่ง ซึ่งก็มีโอกาสเป็นไปได้ว่าถึงแม้จะไม่ได้ทำอะไร (นอกเหนือจากการสั่ง Wireshark ให้ดักจับ) เครื่องของผู้เรียนก็จะยังมีการส่ง UDP packets ออกไปบ้างเป็นปกติอยู่แล้ว โดยเฉพาะในการทำงานของ DNS ซึ่งจะส่ง DNS query และรับ DNS response ซึ่งรับส่งโดยใช้ UDP ดังนั้นจึงเป็นไปได้สูงที่ผู้เรียนจะพบ UDP packets ในการดักจับ

อย่างไรก็ดี เพื่อให้สามารถระบุเจาะจง UDP segment ที่เราจะศึกษา ในปฏิบัติการนี้จะให้ผู้เรียนทดลองโดยการให้ protocol ในชั้น Application Layer ที่ชื่อ Remote Authentication Dial-In User Service (RADIUS) ซึ่งจะประกอบโดย RADIUS client และ RADIUS server โดยให้ทำตามขั้นตอนต่อไปนี้

1. เปิด web browser และเข้าไปที่ URL ต่อไปนี้ <https://idblender.com/tools/public-radius> ซึ่งเป็นเว็บไซต์ที่เปิดให้บริการ public RADIUS server เพื่อใช้สำหรับทดสอบ โดย RADIUS server ดังกล่าวทำงานที่หมายเลข IP address 139.59.128.75 และ port หมายเลข 1812
2. จากในหน้าจอให้เลื่อนลงมาที่ส่วน Created identities เพื่อตรวจสอบว่ามี User-Name และ Cleartext-Password ใดๆ กำหนดไว้แล้วหรือไม่ หากยังไม่มี ให้กรอกข้อมูลต่อไปนี้และกด Submit

User-Name	kmitl
Cleartext-Password	CEkmitl

3. ดาวน์โหลดซอฟต์แวร์ที่จะทำหน้าที่เป็น RADIUS client ซึ่งมีชื่อว่า NTRadPing จาก link ต่อไปนี้ [https://community.microfocus.com/cfs-file/\\_key/communityserver-wikis-components-files/00-00-00-01-70/ntradping.zip](https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-01-70/ntradping.zip)
4. ให้แตกไฟล์ ntradping.zip ออกมาจะพบไฟล์ชื่อ NTRadPing.exe ให้คลิกขวาที่ไฟล์ดังกล่าวและเลือก Run as administrator ซึ่งจะทำให้นหน้าต่างของ NTRadPing Test Utility ปรากฏขึ้นมาดังภาพ รูป 1



The screenshot shows the NTRadPing Test Utility window. It has a title bar 'NTRadPing Test Utility' and standard window controls. The interface is divided into several sections. On the left, there are input fields for 'RADIUS Server/port' (139.59.128.75, 1812), 'Reply timeout (sec.)' (6), 'Retries' (2), 'RADIUS Secret key' (secret), 'User-Name' (kmitl), 'Password' (masked with asterisks), and 'Request type' (Authentication Request). There is also a checkbox for 'CHAP'. Below these is a section for 'Additional RADIUS Attributes' with a large text area and two dropdown menus. On the right, there is a header for 'NTRadPing 1.5 - RADIUS Server Testing Tool' with copyright information and logos for 'MASTER SOFT' and 'DIALWAYS'. Below the logos is a section for 'RADIUS Server reply' with a large text area. At the bottom, there are buttons for 'Add', 'Remove', 'Clear list', 'Load...', 'Save...', 'Send', 'Help...', and 'Close'.

รูป 1 หน้าต่าง NTRadPing Test Utility

5. ในหน้าต่าง NTRadPing Test Utility ให้กรอกข้อมูลดังต่อไปนี้

RADIUS Server	139.59.128.75
RADIUS port	1812
Reply timeout (sec.)	6
Retries	2
RADIUS Secret key	secret
User-Name	kmitl
Password	CEkmitl
Request type	Authentication Request

6. เปิด Wireshark และเริ่มทำการ capture packet โดยใช้ Capture filter ต่อไปนี้

host 139.59.128.75 and udp port 1812

radtest -t pap kmitl CEkmitl '139.59.128.75:1812' 0 secret  
(macOS)

7. สลับกลับมาที่หน้าต่าง NTRadPing Test Utility และกดปุ่ม Send หากทำถูกต้องควรจะมีบรรทัด response: Access-Accept ปรากฏขึ้นใน RADIUS Server reply
8. ทดลองเปลี่ยนค่า Password เป็นค่าอื่นที่ไม่ตรงกับค่าที่ตั้งไว้ก่อนหน้านี้ จากนั้นให้กดปุ่ม Send เพื่อส่ง Access Request อีกครั้ง
9. ทดลองเปลี่ยนค่า Password กลับเป็นค่า CEkmitl อีกครั้ง จากนั้นกดปุ่ม Send เพื่อส่ง Access Request อีกครั้ง
10. สลับไปหน้า Wireshark และสั่งให้หยุด capture
11. ให้ save ไฟล์ไว้ด้วยชื่อ Lab05-A.pcapng

## Questions (A)

หลังจากทำตามขั้นตอนข้างต้นแล้ว ให้ใช้ไฟล์ packet capture ที่ save เอาไว้ในการตอบคำถามต่อไปนี้

- 1) จาก packets ที่ดักจับได้ จงค้นหาว่า UDP segment แรก มีหมายเลขลำดับ packet เป็นหมายเลขอะไร? และประเภทของ Application-Layer payload หรือ protocol ที่ถูกนำส่งด้วย UDP segment เป็น Application-Layer protocol ไດ?

1	0.000000	192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=175
2	0.241254	139.59.128.75	192.168.21.99	RADIUS	69	Access-Accept id=175
3	17.814614	192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=42

> Frame 1: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface en0, id 0

> Ethernet II, Src: Apple\_a8:6e:3b (74:a6:cd:a8:6e:3b), Dst: 02:4d:e3:f6:5e:45 (02:4d:e3:f6:5e:45)

> Internet Protocol Version 4, Src: 192.168.21.99, Dst: 139.59.128.75

> User Datagram Protocol, Src Port: 64918, Dst Port: 1812

Source Port: 64918

Destination Port: 1812

Length: 83

Checksum: 0xfed5 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

> [Timestamps]

UDP payload (75 bytes)

RADIUS Protocol

Code: Access-Request (1)

Packet identifier: 0xaf (175)

Length: 75

Authenticator: 69d2bcfbcc68baafd42ab62f9f5f6d0a

[The response to this request is in frame 2]

Attribute Value Pairs

> AVP: t=User-Name(1) l=7 val=kmitl

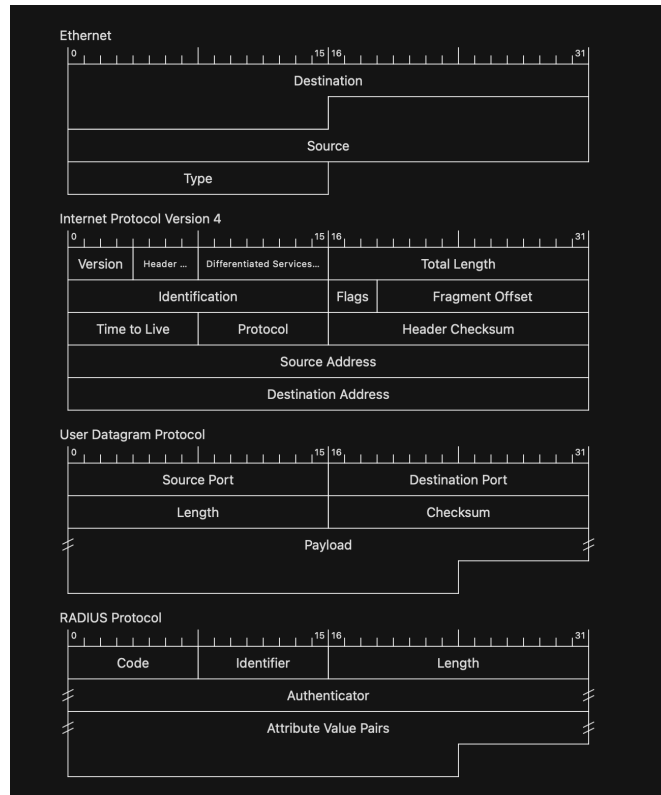
> AVP: t=User-Password(2) l=18 val=Encrypted

> AVP: t=NAS-IP-Address(4) l=6 val=127.0.0.1

> AVP: t=NAS-Port(5) l=6 val=0

> AVP: t=Message-Authenticator(80) l=18 val=ef1f85c219af8f2390fba6a8044f1491

- a.
  - b. No. 1
  - c. Radius
- 2) ที่ Menu bar เลือก Edit -> Preferences เพื่อให้ Preferences ปรากฏขึ้นมา ในหน้าต่างดังกล่าว ให้เลือก หัวข้อ Appearance -> Layout จะพบว่ามีการปรับ Layout หน้าจอ Wireshark โดยให้ปรับ Pane 3 ให้เป็น Packet Diagram และกดปุ่ม OK เพื่อปิดหน้าต่าง Preferences จากนั้นจึงมาพิจารณาข้อมูลใน Packet Detail Pane ของ packet ดังกล่าวและหาว่าใน UDP header มี field อยู่ทั้งหมดกี่ fields? และแต่ละ field มีชื่ออะไรบ้าง?



- a.
- b. Source Port , Destination Port , Length , Checksum , Payload
- 3) จากการศึกษารายละเอียดใน Packet Diagram ของ UDP แต่ละ field ใน UDP header มีความยาวเท่าไรในหน่วย bytes?
  - a. Source Port = 2 bytes , Destination Port = 2 bytes, Length = 2 bytes, Checksum = 2 bytes, Payload = 75 bytes
- 4) ค่าของ field ที่ชื่อว่า Length ใน UDP header เป็นความยาวของอะไร? ทดลองตรวจสอบค่าความยาวกับ UDP packet ที่ผู้เรียนดักจับมาได้ว่ามีค่าเท่ากับที่ตอบหรือไม่
  - a. ตรงกัน
- 5) ขนาดสูงสุดที่เป็นไปได้ของ UDP payload มีขนาดเป็นกี่ bytes? (คำใบ้: โปรดพิจารณาคำตอบของคำถามก่อนหน้า)
  - a. 75 bytes
- 6) ค่าต่ำสุดและค่าสูงสุดที่เป็นไปได้ของหมายเลข source port มีค่าเป็นเท่าใด?
  - a. หมายเลข source port ของ UDP (User Datagram Protocol) มีค่าตั้งแต่ 0 ถึง 65535 เนื่องจากหมายเลขพอร์ตเป็น unsigned 16-bit integer ในการส่งข้อมูลแบบ UDP พอร์ตที่มีค่าต่ำกว่า 1024 เป็น well-known ports พอร์ตที่มีค่าตั้งแต่ 1024 ถึง 49151 เป็น registered ports ซึ่งสามารถใช้โดยโปรแกรมแอปพลิเคชันทั่วไปได้ และพอร์ตที่มีค่าตั้งแต่ 49152 ถึง 65535 เป็น dynamic หรือ private ports ที่สามารถใช้สำหรับการสื่อสารภายในหรือการเชื่อมต่อชั่วคราวได้.

- 7) หมายเลข Protocol สำหรับ UDP คือหมายเลขใด? ให้ผู้เรียนตอบเป็นเลขฐาน 10 โดยในการหาคำตอบของคำถามนี้ ให้ผู้เรียนค้นหาและตรวจสอบค่าของ field ที่ชื่อว่า Protocol ใน header ของ Internet Protocol (IP) ของ packet

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.000000		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request
2	0.241254		139.59.128.75	192.168.21.99	RADIUS	69	Access-Accept
3	17.814614		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request
4	22.820003		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request
5	27.825447		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request
6	41.285457		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request
7	41.527459		139.59.128.75	192.168.21.99	RADIUS	69	Access-Accept

```

> Frame 1: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface en0, id 0
> Ethernet II, Src: Apple_a8:6e:3b (74:a6:cd:a8:6e:3b), Dst: 02:4d:e3:f6:5e:45 (02:4d:e3:f6:5e:45)
> Internet Protocol Version 4, Src: 192.168.21.99, Dst: 139.59.128.75
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 103
    Identification: 0xb414 (46100)
  > 0000 .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xe4df [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.21.99
    Destination Address: 139.59.128.75
  
```

- a.  
b. 17
- 8) ค้นหา UDP packets ใดคู่หนึ่ง ซึ่งประกอบด้วย UDP packet ที่ส่งออกจาก host ฝั่งเครื่องของผู้เรียนและ packet ที่ host ฝั่งเครื่องค้นหาตอบกลับมายังเครื่องผู้เรียน (ข้อสังเกต: ใน Packet List Pane ที่คอลัมน์ No. จะมีลูกศรแสดง UDP packets ที่เข้าคู่กันระหว่างส่งออกไปและตอบกลับ โดยหมายเลข IP ของผู้ส่งใน packet แรก จะเป็นหมายเลขเดียวกับ IP ของผู้รับใน packet ที่สอง) โปรดระบุว่า packet แรก มีหมายเลข packet เป็นหมายเลขใด? และ packet ที่สองมีหมายเลข packet เป็นหมายเลขใด? หมายเลข port ของ packets ทั้งสองมีความสัมพันธ์กันอย่างไร? จงอธิบาย

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.000000		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=175
2	0.241254		139.59.128.75	192.168.21.99	RADIUS	69	Access-Accept id=175

```

> Frame 1: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface en0, id 0
> Ethernet II, Src: Apple_a8:6e:3b (74:a6:cd:a8:6e:3b), Dst: 02:4d:e3:f6:5e:45 (02:4d:e3:f6:5e:45)
> Internet Protocol Version 4, Src: 192.168.21.99, Dst: 139.59.128.75
  > User Datagram Protocol, Src Port: 64918, Dst Port: 1812
    Source Port: 64918
    Destination Port: 1812
    Length: 83
    Checksum: 0xfed5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (75 bytes)
  > RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0xaf (175)
    Length: 75
    Authenticator: 69d2bcfbcc68baafd42ab62f9f5f6d0a
    [The response to this request is in frame 2]
  > Attribute Value Pairs
    > AVP: t=User-Name(1) l=7 val=kmitl
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=NAS-IP-Address(4) l=6 val=127.0.0.1
    > AVP: t=NAS-Port(5) l=6 val=0
    > AVP: t=Message-Authenticator(80) l=18 val=ef1f85c219af8f2390fba6a8044f1491
  
```

- a.  
b. Request No. 1 , Response No.2

01076117 Computer Networks in Practice  
Computer Engineering, KMITL

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.000000		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=175
2	0.241254		139.59.128.75	192.168.21.99	RADIUS	69	Access-Accept id=175

```

> Frame 2: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface en0, id 0
> Ethernet II, Src: 02:4d:e3:f6:5e:45 (02:4d:e3:f6:5e:45), Dst: Apple_a8:6e:3b (74:a6:cd:a8:6e:3b)
> Internet Protocol Version 4, Src: 139.59.128.75, Dst: 192.168.21.99
> User Datagram Protocol, Src Port: 1812, Dst Port: 64918
  Source Port: 1812
  Destination Port: 64918
  Length: 35
  Checksum: 0x9441 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  > [Timestamps]
  UDP payload (27 bytes)
  > RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0xaf (175)
    Length: 27
    Authenticator: a9af8158d52cb81c9b42cabfde5143d0
    [This is a response to a request in frame 1]
    [Time from request: 0.241254000 seconds]
  > Attribute Value Pairs
    > AVP: t=User-Name(1) l=7 val=kmitl
  
```

c.

d. Source Port กับ Destination Port บ่งบอกการติดต่อกันและกัน

- 9) จาก trace ไฟล์ พบว่ามีการส่ง Access-Request ออกไปทั้งหมดกี่ครั้ง? แต่แต่ละครั้งใช้ source port หมายเลขใดบ้าง? เครื่องคอมพิวเตอร์ของผู้เรียนซึ่งทำหน้าที่เป็น host ต้นทางใช้หลักการใดในการเลือกหมายเลข source port? จงอธิบาย

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.000000		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=175
2	0.241254		139.59.128.75	192.168.21.99	RADIUS	69	Access-Accept id=175
3	17.814614		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=42
4	22.820003		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=42, Duplicate Request
5	27.825447		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=42, Duplicate Request
6	41.285457		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=13
7	41.527459		139.59.128.75	192.168.21.99	RADIUS	69	Access-Accept id=13

a.

b. 5 Access-Request

c. No 1. Source Port: 1812

d. No 3-5. Source Port: 59498

e. No 6. Source Port: 64873

f. ระบบปฏิบัติการจะเลือก source port อย่างอัตโนมัติจากช่วงพอร์ตที่มีอยู่ โดยจะเลือกพอร์ตที่ไม่ถูกใช้งานอยู่ในขณะนั้น เพื่อลดโอกาสของการชนกันของหมายเลขพอร์ตและเพื่อให้การสื่อสารเป็นไปอย่างลื่นไหล.

g. ครั้งแรกจะใช้ well-known port ซึ่งเป็นพิเศษอย่างยิ่งเนื่องจาก 1812 มักจะเกี่ยวข้องกับ RADIUS protocol. ส่วนการเลือกพอร์ตต่อไปอาจบ่งชี้ว่ามีการใช้งานพอร์ตแบบ dynamic ซึ่งมักจะเกิดขึ้นเมื่อมีการสร้าง session ใหม่.

- 10) ในรอบที่ RADIUS client ส่ง Access Request ไปพร้อมกับ Password ที่ผิดนั้น พบว่าได้รับ packet ตอบกลับมา จาก RADIUS server หรือไม่? ผู้เรียนสามารถบอกได้ชัดเจนหรือไม่ว่าเกิดอะไรขึ้นบ้าง? Access Request ที่ส่งไป ถึง RADIUS server หรือไม่? RADIUS server ตอบกลับมาหรือไม่? หรือว่า packet ที่ RADIUS server ส่งกลับมา หายไประหว่างทาง?

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.000000		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=175
2	0.241254		139.59.128.75	192.168.21.99	RADIUS	69	Access-Accept id=175
3	17.814614		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=42
4	22.820003		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=42, Duplicate Request
5	27.825447		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=42, Duplicate Request
6	41.285457		192.168.21.99	139.59.128.75	RADIUS	117	Access-Request id=13
7	41.527459		139.59.128.75	192.168.21.99	RADIUS	69	Access-Accept id=13

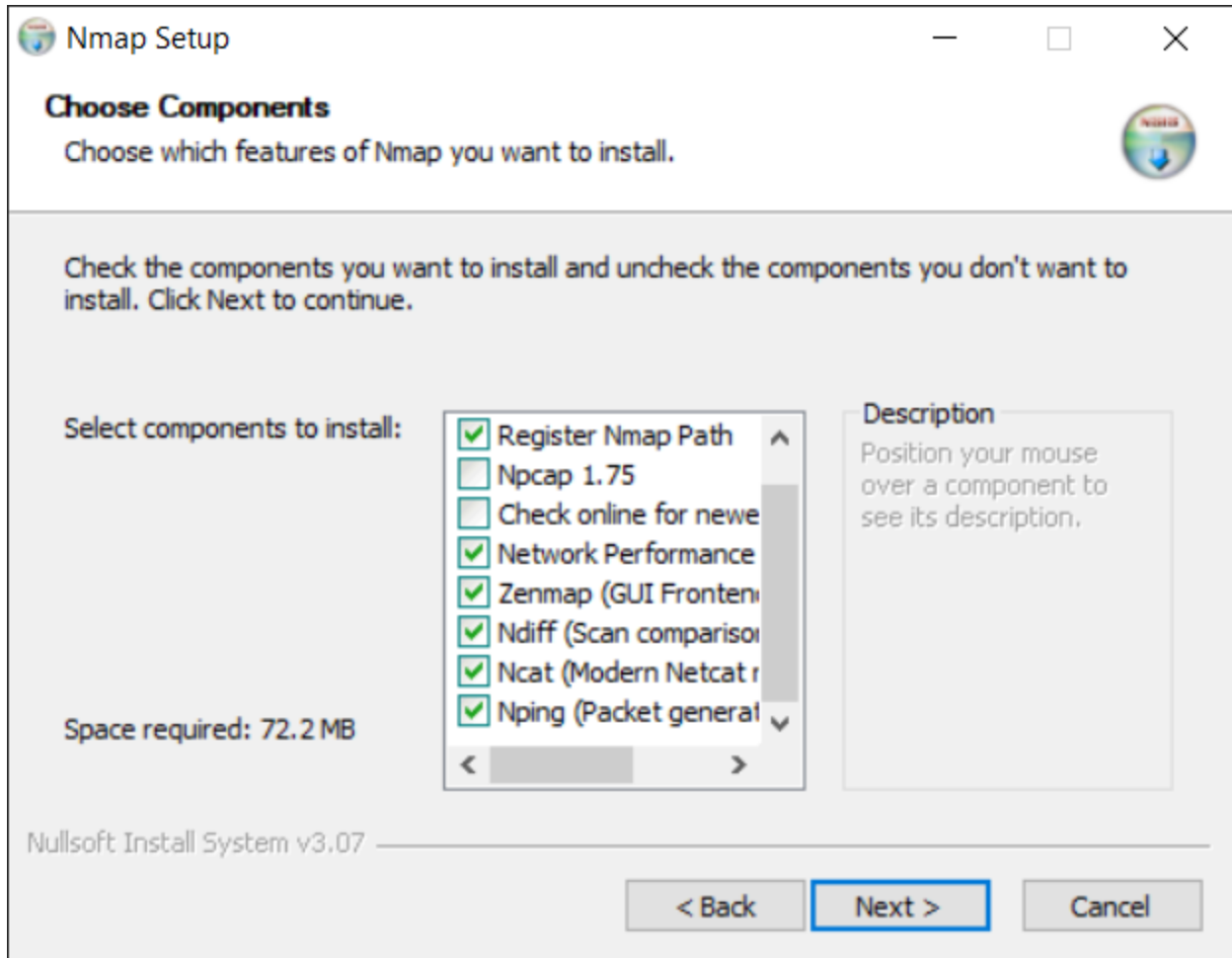
- a. ไม่ response กลับมา
- b. ไม่มีข้อมูลเพียงพอที่จะยืนยันว่า password ที่ส่งไปนั้นถูกต้องหรือไม่ หรือว่าการตอบกลับอย่างไรจาก server. จึงไม่สามารถสรุปได้ว่า password ที่ผิดนั้นได้รับการตอบกลับจาก server หรือไม่ และไม่สามารถระบุได้ว่าการสูญเสียแพ็คเก็ตเกิดในระหว่างทางหรือไม่.

## B. Transmission Control Protocol (TCP)

ในปฏิบัติการส่วนนี้เราจะสำรวจพฤติกรรมการทำงานของ TCP มากขึ้นในรายละเอียด เนื่องจาก TCP มีรายละเอียดหลายส่วน เราจะไม่สามารถศึกษาทุกแง่มุมของ TCP ได้ในปฏิบัติการเพียงครั้งเดียว ในครั้งนี้เราจะเน้นไปที่การศึกษาเรื่องการสร้างการเชื่อมต่อ (TCP connection setup) ซึ่งเราจะศึกษาโดยการวิเคราะห์จากบันทึกการจราจรการสร้างการเชื่อมต่อและในการร้องขอข้อมูลจากบริการ Quote of the Day (QOTD) เปรียบเทียบระหว่างกรณี TCP เทียบกับ UDP ซึ่งผู้เรียนสามารถศึกษาการทำงานของ protocol ดังกล่าวได้จากเอกสาร [RFC 865](#)

เพื่อความสะดวกในการทดลองตามปฏิบัติการในครั้งนี้ เพื่อให้ไม่จำเป็นต้องเขียนโปรแกรมเพื่อติดต่อสื่อสารกับฝั่ง server ผู้เรียนจะได้ใช้ command line utility ที่ชื่อว่า ncat ซึ่งพัฒนาขึ้นมาโดยเลียนแบบการทำงานของเครื่องมือดั้งเดิมที่ชื่อว่า netcat โดยสามารถติดตั้ง ncat พร้อมกับซอฟต์แวร์ที่ใช้ในการทำ port scan ที่ชื่อว่า Nmap ในการทดลองให้ทำตามขั้นตอนต่อไปนี้

1. เปิด web browser และเข้าไปที่ URL ต่อไปนี้ <https://nmap.org/download.html> เพื่อดาวน์โหลดไฟล์ติดตั้ง Nmap โดย ณ เวลาที่จัดทำเอกสารสำหรับปฏิบัติการนี้ ไฟล์ติดตั้ง Nmap เวอร์ชันล่าสุดคือไฟล์ชื่อ nmap-7.94-setup.exe
2. หลังจากดาวน์โหลดไฟล์ติดตั้งเรียบร้อยแล้ว ให้รันไฟล์ดังกล่าวเพื่อทำการติดตั้ง โดยให้ระบุตัวเลือกติดตั้ง components Ncat และ Nping รวมถึง component อื่นๆ ตามรูปที่ปรากฏต่อไปนี้



รูปที่ 2 การติดตั้ง component ของ Nmap

3. หลังจากติดตั้งเสร็จสิ้น ให้ทดสอบว่า ncat พร้อมใช้งานหรือไม่โดยเปิด command prompt และพิมพ์คำสั่งต่อไปนี้

```
ncat -help
```

หากติดตั้งสำเร็จพร้อมใช้งาน หน้าจอ command prompt จะแสดงคำอธิบายการใช้งาน ncat

4. เปิด Wireshark และเริ่มทำการ capture packet โดยใช้ Capture filter ต่อไปนี้

```
tcp port 17 or udp port 17
```

5. สลับกลับไปหน้าจอ command prompt และพิมพ์คำสั่งต่อไปนี้ เพื่อเป็นการร้องขอไปยัง QOTD server ที่ชื่อ `djxmx.net` ซึ่งให้บริการด้วย TCP ที่ port หมายเลข 17 โดยหลังจากพิมพ์คำสั่ง ให้กด Enter สองครั้งเพื่อให้กลับมาที่ prompt



```
ncat djxmx.net 17
```

6. ทำตามขั้นตอนในข้อที่แล้วอย่างน้อย 3 ครั้งเพื่อขอ quote ต่างๆ กัน
7. พิมพ์คำสั่งต่อไปนี้เพื่อเป็นการร้องขอไปยัง QOTD server ที่ชื่อ djxmx.net ซึ่งให้บริการด้วย UDP ที่ port หมายเลข 17 ซึ่งการใส่ -u เป็นการระบุว่าใช้ UDP โดยหลังจากพิมพ์คำสั่ง ให้กด Enter อย่างน้อย 2-3 ครั้ง โดยจะพบว่าหลังจากกด Enter แต่ละครั้ง จะปรากฏ quote ใหม่ขึ้นมาเรื่อยๆ หากต้องการหยุดและกลับมาที่ prompt ให้กด Ctrl + Z แล้วกด Enter (สำหรับกรณีของ macOS และ Linux ให้กด Ctrl + D แล้วกด Enter)

```
ncat -u djxmx.net 17
```

8. สลับไปหน้า Wireshark และสั่งให้หยุด capture
9. ให้ save ไฟล์ไว้ด้วยชื่อ Lab05-B.pcapng

## Questions (B)

- 11) จากการร้องขอ quote ผ่าน TCP โปรดระบุว่า quote แรกที่ได้มีข้อความว่าอะไร? จงค้นหาว่า packet ใดจากไฟล์ capture ที่เนื้อความ quote แรกปรากฏอยู่ในเนื้อหาของ packet โปรดระบุหมายเลข packet

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.000000		192.168.21.99	104.9.242.101	TCP	78	65008 → 17 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460
2	0.461915		104.9.242.101	192.168.21.99	TCP	66	17 → 65008 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3	0.462155		192.168.21.99	104.9.242.101	TCP	54	65008 → 17 [ACK] Seq=1 Ack=1 Win=262144 Len=0
4	0.830544		104.9.242.101	192.168.21.99	TCP	99	17 → 65008 [PSH, ACK] Seq=1 Ack=1 Win=263424 Len=45
5	0.830547		104.9.242.101	192.168.21.99	TCP	56	17 → 65008 [FIN, ACK] Seq=46 Ack=1 Win=263424 Len=0
6	0.830714		192.168.21.99	104.9.242.101	TCP	54	65008 → 17 [ACK] Seq=1 Ack=46 Win=262080 Len=0
7	0.830774		192.168.21.99	104.9.242.101	TCP	54	65008 → 17 [ACK] Seq=1 Ack=47 Win=262080 Len=0
8	2.130488		192.168.21.99	104.9.242.101	TCP	55	65008 → 17 [PSH, ACK] Seq=1 Ack=47 Win=262144 Len=1

> Frame 4: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface en0, id 0  
> Ethernet II, Src: 02:4d:e3:f6:5e:45 (02:4d:e3:f6:5e:45), Dst: Apple\_a8:6e:3b (74:a6:cd:a8:6e:3b)  
> Internet Protocol Version 4, Src: 104.9.242.101, Dst: 192.168.21.99  
> Transmission Control Protocol, Src Port: 17, Dst Port: 65008, Seq: 1, Ack: 1, Len: 45  
Data (45 bytes)  
Data: 2249742773206861726420746f2066696e6420676f6642068656c702e2e2e20d0a09202d204368657679d0d0  
[Length: 45]

- a.
- b. NO.4

```
~ (4.196s)
ncat djxmx.net 17
"It's hard to find good help..."
- Chevy
Ncat: Broken pipe.
```

- c.

```
"It's hard to find good help..."
- Chevy
```

- d.

- 12) จากหมายเลข packet ในข้อที่แล้ว ให้คลิกขวาที่ packet ดังกล่าวแล้วเลือก Follow -> TCP Stream ซึ่งจะมีผลให้ Wireshark สร้างและใช้ Display filter เพื่อแสดงเฉพาะ packets ของ TCP connection เดียวกัน จงตรวจสอบว่า Wireshark สร้าง Display filter อะไรให้? โปรดระบุ Display filter ดังกล่าวในคำตอบ



a.

- 13) หลังจากใช้ Follow -> TCP Stream เหลือ packets ที่แสดงผลใน Packet List Pane จำนวนกี่ packets? Packet ที่มีเนื้อความ quote ที่ server ส่งมาเป็น packet ลำดับที่เท่าไรจาก packets ทั้งหมดใน TCP connection นี้ (ไม่ใช่ packet No. แต่ให้นับว่าเป็นบรรทัดที่เท่าไร หลังจากจัดเรียงตามคอลัมน์เวลาแล้ว)

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.000000		192.168.21.99	184.9.242.101	TCP	78	65008 → 17 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2883767191 TSecr=0 SACK_PERM
2	0.461915		184.9.242.101	192.168.21.99	TCP	66	17 → 65008 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
3	0.462155		192.168.21.99	184.9.242.101	TCP	54	65008 → 17 [ACK] Seq=1 Ack=1 Win=262144 Len=0
4	0.830544		184.9.242.101	192.168.21.99	TCP	99	17 → 65008 [PSH, ACK] Seq=1 Ack=1 Win=263424 Len=45
5	0.830547		184.9.242.101	192.168.21.99	TCP	56	17 → 65008 [FIN, ACK] Seq=46 Ack=1 Win=263424 Len=0
6	0.830714		192.168.21.99	184.9.242.101	TCP	54	65008 → 17 [ACK] Seq=1 Ack=46 Win=262080 Len=0
7	0.830774		192.168.21.99	184.9.242.101	TCP	54	65008 → 17 [ACK] Seq=1 Ack=47 Win=262080 Len=0
8	2.130488		192.168.21.99	184.9.242.101	TCP	55	65008 → 17 [PSH, ACK] Seq=1 Ack=47 Win=262144 Len=1
9	2.611185		184.9.242.101	192.168.21.99	TCP	56	17 → 65008 [RST, ACK] Seq=47 Ack=2 Win=0 Len=0

a.

b. 9 packets

c. No. 4 บรรทัดที่ 4

- 14) ตอนเริ่มต้นของ TCP connection ในคอลัมน์ Info ของ 3 packets แรกมีข้อมูลอะไรปรากฏอยู่บ้าง นำข้อมูลเหล่านั้นมาเขียนในคำตอบ

```
Transmission Control Protocol, Src Port: 65008, Dst Port: 17, Seq: 0, Len: 0
  Source Port: 65008
  Destination Port: 17
  [Stream index: 0]
  > [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 1945428641
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1011 .... = Header Length: 44 bytes (11)
  > Flags: 0x0c2 (SYN, ECE, CWR)
  Window: 65535
  [Calculated window size: 65535]
  Checksum: 0x39af [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Ope
  > [Timestamps]
```

a.

```
Transmission Control Protocol, Src Port: 17, Dst Port: 65008, Seq: 0, Ack: 1, Len: 0
  Source Port: 17
  Destination Port: 65008
  [Stream index: 0]
  > [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 3116961891
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1945428642
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x052 (SYN, ACK, ECE)
  Window: 65535
  [Calculated window size: 65535]
  Checksum: 0x1f94 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Ope
  > [Timestamps]
  > [SEQ/ACK analysis]
```

b.

```
Transmission Control Protocol, Src Port: 65008, Dst Port: 17, Seq: 1, Ack: 1, Len: 0
  Source Port: 65008
  Destination Port: 17
  [Stream index: 0]
  > [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1945428642
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3116961892
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window: 4096
  [Calculated window size: 262144]
  [Window size scaling factor: 64]
  Checksum: 0x5093 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
```

C.

15) หากต้องการกรองให้ Packet List Pane แสดงผลเฉพาะ 3 packets แรกของ TCP connection จะต้องเขียน

Display filter ว่าอย่างไร

a. (tcp.stream eq 0) and (frame.number <= 3)

16) จากที่ผู้เรียนได้ทราบจากรายวิชาทฤษฎีแล้วว่าการส่งข้อมูลแบบเชื่อถือได้ (Reliable Data Transfer) มีการใช้ Timer เพื่อรอการตอบกลับเป็นระยะเวลาที่เหมาะสม ซึ่งระยะเวลาดังกล่าวมีความสัมพันธ์กับ RTT ระหว่างคู่สนทนา จงอธิบายว่า ผู้ client สามารถใช้ประโยชน์จากการรับส่ง packets ทั้ง 3 เพื่อหาค่า RTT ได้อย่างไร? ในทำนองเดียวกัน จงอธิบาย ผู้ server สามารถใช้ประโยชน์จากการรับส่ง packets ทั้ง 3 เพื่อหา RTT ได้อย่างไร?

a. ผู้ Client:

- การส่ง SYN (Time A): Client เริ่มนับเวลา (timer) เมื่อมันส่งแพ็คเก็ต SYN ไปยัง server เพื่อเริ่มการเชื่อมต่อ.
- การรับ SYN-ACK (Time B): Client หยุดนับเวลาเมื่อมันได้รับแพ็คเก็ต SYN-ACK กลับมาจาก server.
- คำนวณ RTT: RTT สามารถคำนวณได้โดยการหักเวลาที่ client ได้รับ SYN-ACK (Time B) ด้วยเวลาที่ client ส่ง SYN (Time A).

b. ผู้ Server:

- การรับ SYN (Time C): Server เริ่มนับเวลาเมื่อมันได้รับแพ็คเก็ต SYN จาก client.
- การส่ง SYN-ACK (Time D): Server ส่งแพ็คเก็ต SYN-ACK กลับไปยัง client และสามารถจดจำเวลาที่ส่งได้.
- การรับ ACK (Time E): เมื่อ server ได้รับแพ็คเก็ต ACK กลับมา, มันสามารถหยุดนับเวลาและใช้เวลาที่แพ็คเก็ต ACK ถูกส่งกลับมาเพื่อคำนวณ RTT โดยการหักเวลาที่ได้รับ ACK (Time E) ด้วยเวลาที่ส่ง SYN-ACK (Time D).

17) ค่าใน field ไตที่ Wireshark ได้คำนวณและแสดงผลค่า RTT ระหว่าง client และ server จงหาค่าดังกล่าวใน

Packet Details Pane จาก 3 packets แรก และระบุชื่อ field ดังกล่าวในคำตอบ

```
[Timestamps]
  [Time since first frame in this TCP stream: 0.461915000 seconds]
  [Time since previous frame in this TCP stream: 0.461915000 seconds]
[SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 1]
  [The RTT to ACK the segment was: 0.461915000 seconds]
  [iRTT: 0.462155000 seconds]
```

a.

```

✓ [Timestamps]
  [Time since first frame in this TCP stream: 0.462155000 seconds]
  [Time since previous frame in this TCP stream: 0.000240000 seconds]
✓ [SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 2]
  [The RTT to ACK the segment was: 0.000240000 seconds]
  [iRTT: 0.462155000 seconds]

```

b.

18) ให้ล้าง Display filter เพื่อให้กลับมาแสดงผลทุก packets ที่ดักจับได้อีกครั้ง และค้นหาวาในแต่ละอย่างที่ร้องขอ quote ผ่าน TCP เครื่องของผู้เรียนใช้ port หมายเลขอะไรบ้าง? โปรดระบุหมายเลขเหล่านั้นในคำตอบ

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.000000		192.168.21.99	184.9.242.101	TCP	78	65008 → 17 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2883767191 TSecr=0 SACK_PERM
2	0.463155		184.9.242.101	192.168.21.99	TCP	66	17 → 65008 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
3	0.462155		192.168.21.99	184.9.242.101	TCP	54	65008 → 17 [ACK] Seq=1 Ack=1 Win=262144 Len=0
4	0.830544		184.9.242.101	192.168.21.99	TCP	99	17 → 65008 [PSH, ACK] Seq=1 Ack=1 Win=263424 Len=45
5	0.830547		184.9.242.101	192.168.21.99	TCP	56	17 → 65008 [FIN, ACK] Seq=46 Ack=1 Win=263424 Len=0
6	0.830714		192.168.21.99	184.9.242.101	TCP	54	65008 → 17 [ACK] Seq=1 Ack=46 Win=262080 Len=0
7	0.830774		192.168.21.99	184.9.242.101	TCP	54	65008 → 17 [ACK] Seq=1 Ack=47 Win=262080 Len=0
8	2.130488		192.168.21.99	184.9.242.101	TCP	55	65008 → 17 [PSH, ACK] Seq=1 Ack=47 Win=262144 Len=1
9	2.611185		184.9.242.101	192.168.21.99	TCP	56	17 → 65008 [PSH, ACK] Seq=47 Ack=2 Win=0 Len=0
10	13.429134		192.168.21.99	184.230.16.86	TCP	78	65009 → 17 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=100212096 TSecr=0 SACK_PERM
11	13.703183		184.230.16.86	192.168.21.99	TCP	66	17 → 65009 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
12	13.703430		192.168.21.99	184.230.16.86	TCP	54	65009 → 17 [ACK] Seq=1 Ack=1 Win=262144 Len=0
13	13.977539		184.230.16.86	192.168.21.99	TCP	317	17 → 65009 [PSH, ACK] Seq=1 Ack=1 Win=263424 Len=263
14	13.977542		184.230.16.86	192.168.21.99	TCP	56	17 → 65009 [FIN, ACK] Seq=264 Ack=1 Win=263424 Len=0
15	13.977718		192.168.21.99	184.230.16.86	TCP	54	65009 → 17 [ACK] Seq=1 Ack=264 Win=261824 Len=0
16	13.977829		192.168.21.99	184.230.16.86	TCP	54	65009 → 17 [ACK] Seq=1 Ack=265 Win=261824 Len=0
17	16.593468		192.168.21.99	184.230.16.86	TCP	55	65009 → 17 [ACK] Seq=1 Ack=265 Win=262144 Len=1
18	16.594517		184.230.16.86	192.168.21.99	TCP	55	17 → 65009 [RST, ACK] Seq=265 Ack=2 Win=0 Len=0
19	21.128458		192.168.21.99	24.214.177.39	TCP	78	65010 → 17 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1374037334 TSecr=0 SACK_PERM
20	21.454227		24.214.177.39	192.168.21.99	TCP	66	17 → 65010 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
21	21.454461		192.168.21.99	24.214.177.39	TCP	54	65010 → 17 [ACK] Seq=1 Ack=1 Win=262144 Len=0
22	21.455150		24.214.177.39	192.168.21.99	TCP	55	TCP previous segment out of order! 17 → 65010 [FIN, ACK] Seq=300 Ack=1 Win=263424 Len=0
23	21.725203		24.214.177.39	192.168.21.99	TCP	362	[TCP Out-of-Order] 17 → 65010 [PSH, ACK] Seq=1 Ack=1 Win=263424 Len=308
24	21.725437		192.168.21.99	24.214.177.39	TCP	66	[TCP Dup ACK 21#1] 65010 → 17 [ACK] Seq=1 Ack=1 Win=262144 Len=0 SLE=309 SRE=310
25	21.725528		192.168.21.99	24.214.177.39	TCP	54	65010 → 17 [ACK] Seq=1 Ack=310 Win=261824 Len=0
26	22.734122		192.168.21.99	24.214.177.39	TCP	55	65010 → 17 [PSH, ACK] Seq=1 Ack=310 Win=262144 Len=1
27	23.305914		24.214.177.39	192.168.21.99	TCP	56	17 → 65010 [RST, ACK] Seq=310 Ack=2 Win=0 Len=0

a.

b. 65008

c. 65009

d. 65010

19) จากข้อ 18) เครื่องของผู้เรียนมีหลักการอย่างไรในการเลือกหมายเลข port ที่จะใช้งาน? จงอธิบาย

a. ระบบปฏิบัติการจะเลือก source port อย่างอัตโนมัติจากช่วงพอร์ตที่มีอยู่ โดยจะเลือกพอร์ตที่ไม่ถูกใช้งานอยู่ในขณะนั้น เพื่อลดโอกาสของการชนกันของหมายเลขพอร์ตและเพื่อให้การสื่อสารเป็นไปอย่างลื่นไหล.

20) ให้ล้าง Display filter เพื่อให้กลับมาแสดงผลทุก packets ที่ดักจับได้อีกครั้ง และเขียน Display filter ใหม่ให้แสดงผลเฉพาะ packet ที่มีการใช้งาน UDP และตรวจสอบว่ามี UDP จำนวนกี่ packets? เป็น packet ที่ client ส่งไปยัง server กี่ packets? และเป็น packets ที่ server ตอบกลับมาที่ client กี่ packet? จำนวน UDP segment ที่ส่งไปและได้รับตอบกลับมีจำนวนเท่ากันหรือไม่?

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
28	17.310347		192.168.21.99	24.214.177.39	UDP	43	60566 → 17 Len=1
29	17.803044		24.214.177.39	192.168.21.99	UDP	258	17 → 60566 Len=216
30	18.360263		192.168.21.99	24.214.177.39	UDP	43	60566 → 17 Len=1
31	18.642338		24.214.177.39	192.168.21.99	UDP	172	17 → 60566 Len=130
32	19.202462		192.168.21.99	24.214.177.39	UDP	43	60566 → 17 Len=1
33	19.496287		24.214.177.39	192.168.21.99	UDP	88	17 → 60566 Len=46

a.

b. 6 packets

c. Client sent 3 packets

d. Server sent 3 packets

e. เท่ากัน

- 21) ในบรรดา UDP segment ที่ server ตอบกลับมาหา client จงค้นหาว่ามี packets ที่เป็นการแลกเปลี่ยน control information โดยที่ไม่บรรจุเนื้อหา quote หรือไม่? ถ้าหากมี packets เหล่านั้นมี control information อะไร?
- a. ไม่มี

## Submission

จงตอบคำถามในส่วนที่ระบุหัวข้อ Question ตั้งแต่ (A) ไปจนถึง (B) ซึ่งมีคำถามรวมทั้งหมด 21 ข้อ โดยในคำตอบของแต่ละข้อด้วยให้อธิบายด้วยว่าหาคำตอบมาได้อย่างไร ตัวอย่างเช่น อธิบายว่าสามารถค้น packet ตามที่โจทย์ระบุได้ด้วยวิธีการใด หรือค่าที่นำมาตอบ นำมาจาก field ใดของ header ตาม protocol ใด

ในกรณีที่คัดลอกคำตอบของคนอื่นมา ให้ระบุชื่อของบุคคลที่เป็นต้นฉบับมาด้วย หากตรวจพบว่าการลอกมาแต่ไม่มีการระบุชื่อบุคคลที่เป็นต้นฉบับ ผู้สอนจะถือว่าทุจริตและอาจพิจารณาลงโทษให้ตกเกณฑ์รายวิชาในทันที

การส่งงาน ให้เขียนหรือพิมพ์หมายเลขข้อและคำตอบของข้อนั้นๆ และส่งเป็นไฟล์ PDF เท่านั้น กรุณาตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย section และ \_lab05 ตามตัวอย่างต่อไปนี้ 64019999\_sec20\_lab05.pdf