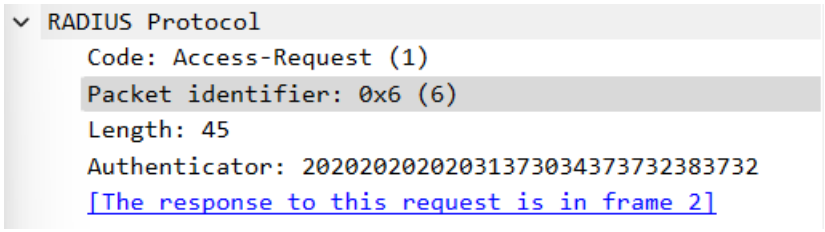
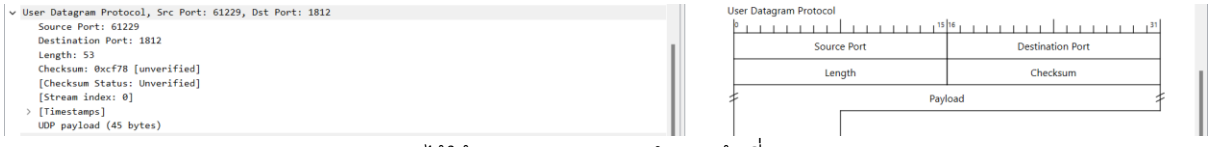
Question A :

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



Answer UDP segment แรกมีหมายเลขลำดับ packetเป็น 0x6 (สังเกตจาก field : Packet identifier จาก RADIUS Protocol) และประเภทของ Application-Layer payload (protocol) เป็น RADIUS protocol



(รูปไว้ใช้ประกอบการตอบคำถามข้อที่ 2-6)

2) ที่ Menu bar เลือก Edit -> Preferences เพื่อให้ Preferences ปรากฏขึ้นมา ในหน้าต่างดังกล่าว ให้เลือกหัวข้อ Appearance -> Layout จะพบว่ามีให้ปรับต่าง 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 มีชื่อว่าอะไรบ้าง?

Answer UDP header มีอยู่ทั้งหมด 5 fieldด้วยกัน โดยมีดังรายการด้านล่าง(สังเกตจาก UDP ใน packet detail pane)

1.Source Port
2.Destination Port
3.Length
4.Checksum
5.UDP payload (payload)

3) จากการศึกษาข้อมูลในแสดงใน Packet Diagram ของ UDP แต่ละ field ใน UDP header มีความยาวเท่าไรในหน่วย bytes?

Answer แต่ละfieldในUDP header มีความยาวเป็นดังนี้ (ข้อมูลจากการสังเกตจาก Packet Diagram)

1.Source Port มีความยาว 16บิต

2.Destination Port มีความยาวเป็น 16บิต

3.Length มีความยาวเป็น 16บิต

4.Checksum มีความยาวเป็น 16บิต

5.UDP payload (payload) มีความยาว 27-45ไบต์

4) ค่าของ field ที่ชื่อว่า Length ใน UDP header เป็นความยาวของอะไร? ทดลองตรวจสอบค่าความยาวกับ UDP packet ที่ผู้เรียนดักจับมาได้ว่ามีค่าเท่ากับที่ตอบหรือไม่

Answer field Length ใน UDP header คือความยาวของข้อมูลทุก field ใน UDP header เป็นหน่วย byte และที่ดักจับมาตรงกับคำตอบ เพราะ payload + 8 = Length (bytes)

5) ขนาดสูงสุดที่เป็นไปได้ของ UDP payload มีขนาดเป็นกี่ bytes? (คำใบ้: โปรดพิจารณาคำตอบของคำถามก่อนหน้า)

Answer มีขนาด = 2^{16} – 8(field อื่นนอกเหนือจาก payload) = 65,527 bytes เพราะว่า field Length มีขนาด 16บิต

6) ค่าต่ำสุดและค่าสูงสุดที่เป็นไปได้ของหมายเลข source port มีค่าเป็นเท่าใด?

Answer ค่าตั้งแต่ 0 ถึง 65,535 เพราะ field ของ source port มีขนาด 16บิต

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

```
Internet Protocol Version 4, Src: 172.20.10.2, 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: 73
    Identification: 0x946d (37997)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
```

Answer หมายเลข Protocol สำหรับ UDP คือหมายเลข 17(ฐาน10)

8) ค้นหาคู่ UDP packets คู่ใดคู่หนึ่ง ซึ่งประกอบด้วย UDP packet ที่ส่งออกจาก host ฝั่งเครื่องของผู้เรียนและ packet ที่ host ฝั่งเครื่องคู่สนทนาตอบกลับมายังเครื่องผู้เรียน (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

```
User Datagram Protocol, Src Port: 61229, Dst Port: 181
    Source Port: 61229
    Destination Port: 1812
```

(packet แรก)

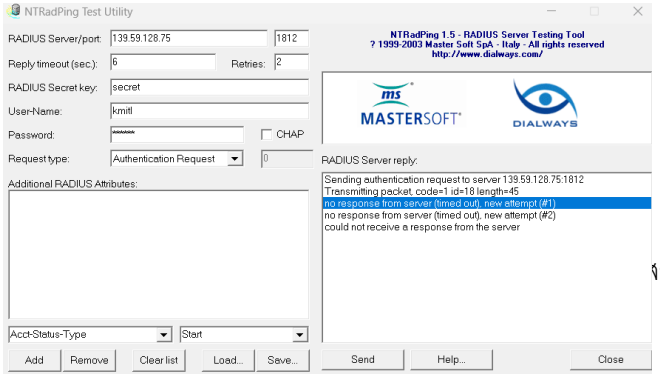
```
User Datagram Protocol, Src Port: 1812, Dst Port
    Source Port: 1812
    Destination Port: 61229
```

(packet ที่สอง)

Answer ทั้งpacket แรกและ packet ที่สองมีหมายเลขเป็น 0x6 โดย packet แรกมีหมายเลข Source port เป็น 61229(หมายเลข socket portของ Client) และหมายเลข Destination port เป็น 1812 (Server socket port)
ส่วน packet ที่สองมี Source port และ Destination port เป็น Destination port และ Source port ของ packet แรกตามลำดับ ซึ่งมีความสำคัญโดย packet แรกเป็นpacket ที่ client request ไปยัง server โดยอาศัย destination IP,destination Port ของ client และ packet ที่สองเป็นการ response กลับมาหา client ของ server (source port,destination port จึงสลับกัน) โดยการ request,response model implement ใน RADIUS protocol

9) จาก trace ไฟล์ พบว่ามีการส่ง Access-Request ออกไปทั้งหมดกี่ครั้ง? แต่ละครั้งใช้ source port หมายเลขใดบ้าง? เครื่องคอมพิวเตอร์ของผู้เรียนซึ่งทำหน้าที่เป็น host ต้นทางใช้หลักการใดในการเลือกหมายเลข source port? จงอธิบาย
Answer จาก trace file พบว่ามีการส่ง Access-Request ออกไปทั้งหมด 2ครั้ง โดยแต่ละครั้งใช้ source port หมายเลข 1812เช่นเดียวกัน โดย host ใช้หลักการสุ่มหมายเลข source port ในแต่ละการส่งไม่ให้เกิดการ conflict (ใช้หมายเลข port ซ้ำ)

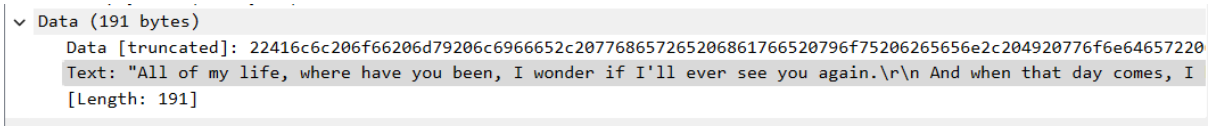
10) ในรอบที่ RADIUS client ส่ง Access Request ไปพร้อมกับ Password ที่ผิดนั้น พบว่าได้รับ packet ตอบกลับมาจาก RADIUS server หรือไม่? ผู้เรียนสามารถบอกได้ชัดเจนหรือไม่ว่าเกิดอะไรขึ้นบ้าง? Access Request ที่ส่งไปถึง RADIUS server หรือไม่? RADIUS server ตอบกลับมาหรือไม่? หรือว่า packet ที่ RADIUS server ส่งกลับมาหายไประหว่างทาง?



Answer packet ที่ทำการส่ง Access Request พร้อม Password ไปยัง RADIUS server พบว่าไม่มีการได้รับ packet ตอบกลับมาจากตัว server โดยการส่ง request ไปครั้งแรกแล้วเกิด timed out (ไม่มีการตอบกลับจาก server) จึงส่ง packet ไปอีกครั้งและพบว่า timed out อีกเช่นกัน Access Requst ส่งไปไม่ถึง RADIUS server และ RADIUS server ไม่มีการตอบกลับมายัง client

Question B:

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



Answer quote แรกมีข้อความว่า

“

"All of my life, where have you been, I wonder if I'll ever see you again.
And when that day comes, I know we could win, I wonder if I'll ever see you again..."
- Lenny Kravitz (Again)

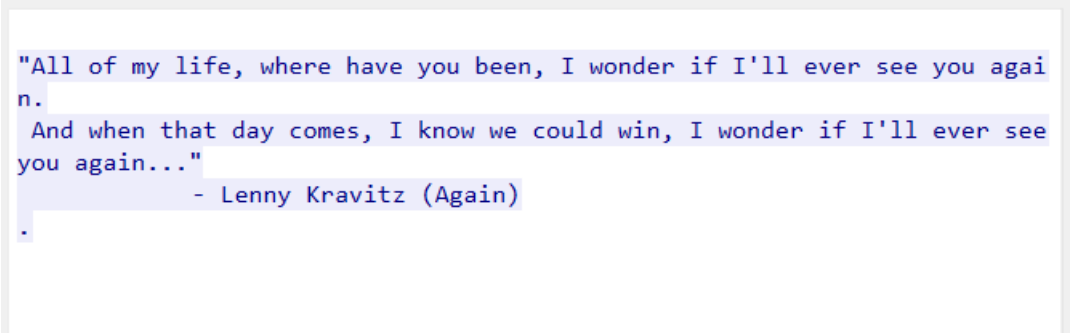
”

โดยปรากฏใน packet ลำดับที่5 ของ file trace

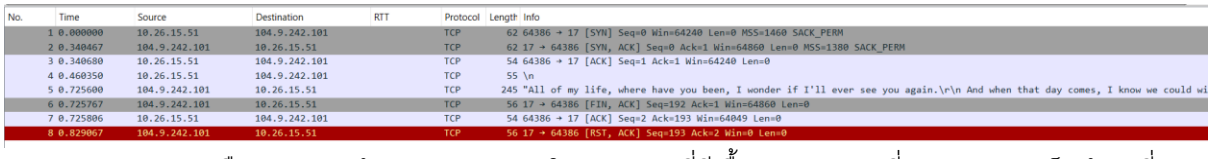
(โดยสังเกตจาก field data ใน TCP)

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

Answer Wireshark สร้าง Display filter ให้ดังนี้



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	Source	Destination	RTT	Protocol	Length	Info
1	0.000000	10.26.15.51	104.9.242.101		TCP	62	64386 → 17 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
2	0.340467	104.9.242.101	10.26.15.51		TCP	62	17 → 64386 [SYN, ACK] Seq=0 Ack=1 Win=64860 Len=0 MSS=1380 SACK_PERM
3	0.340680	10.26.15.51	104.9.242.101		TCP	54	64386 → 17 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.460350	10.26.15.51	104.9.242.101		TCP	55	\n
5	0.725600	104.9.242.101	10.26.15.51		TCP	245	"All of my life, where have you been, I wonder if I'll ever see you again.\r\n And when that day comes, I know we could wi
6	0.725767	104.9.242.101	10.26.15.51		TCP	56	17 → 64386 [FIN, ACK] Seq=192 Ack=1 Win=64860 Len=0
7	0.725806	10.26.15.51	104.9.242.101		TCP	54	64386 → 17 [ACK] Seq=2 Ack=193 Win=64049 Len=0
8	0.829067	104.9.242.101	10.26.15.51		TCP	56	17 → 64386 [RST, ACK] Seq=193 Ack=2 Win=0 Len=0

Answer เหลือ packets จำนวน 8 packets โดย packet ที่มีเนื้อความquote ที่ serverส่งมาเป็นลำดับที่ 5 จาก packets ทั้งหมดใน TCP connection นี้

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

Answer มีข้อมูลดังนี้

Sequence number
Window
Len
Maximum segment size (MSS)
SACK_PERM

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

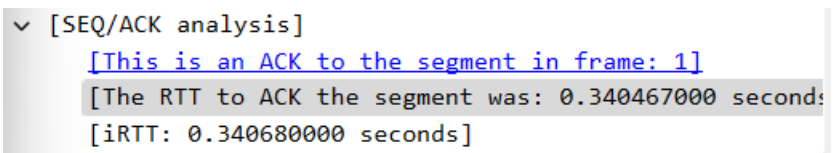
Answer

tcp.stream eq 0 and ((tcp.seq == 1 && tcp.ack == 1&&tcp.len==0 && !tcp.flags.fin == 1)||tcp.flags.syn==1)

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

Answer ฝั่ง client สามารถใช้ประโยชน์จากการดูเวลาที่ส่ง packet SYN จนกระทั่งได้รับ packet SYN/ACK กลับมา ส่วนฝั่ง server สามารถใช้ประโยชน์จากการส่ง packet SYN/ACK กลับไปหา client และรอรับ ACK ตอบกลับ

17) ค่าใน field ใดที่ Wireshark ได้คำนวณและแสดงผลค่า RTT ระหว่าง client และ server จงหาค่าดังกล่าวใน Packet Details Pane จาก 3 packets แรก และระบุชื่อ field ดังกล่าวในคำตอบ



Answer field SEQ/ACK analysis (จาก TCP)

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

Answer port หมายเลข 17 เพียงอย่างเดียว (สังเกตจาก source port, destination port ของแต่ละ packet ที่ทำการ capture ได้)

19) จากข้อ 18) เครื่องของผู้เรียนมีหลักการยังไงในการเลือกหมายเลข port ที่จะใช้งาน? จงอธิบาย

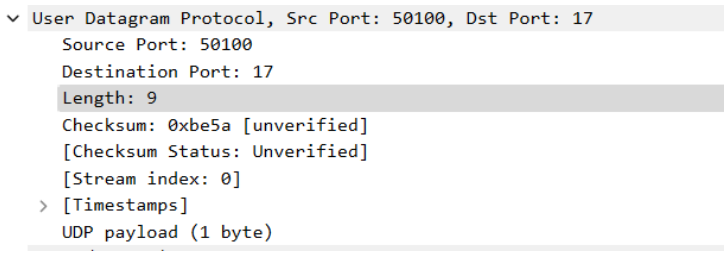
Answer โดยจากคำสั่ง ncat ที่ได้ทดลอง request รับ quote ผ่าน protocol ชนิด TCP,UDP ได้มีการระบุใช้งาน port 17 ใน command แต่portต้องไม่busy

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?

Answer packet ที่ client ทำการส่งไปมี 5 packets และ packetที่ได้รับการส่งกลับมาจากserverมี 5 packets เช่นเดียวกัน จำนวน segment ที่ทำการส่งไปและกลับมีจำนวนเท่ากันเพียงแต่ packet ที่ส่งจาก server จะมี payload ขนาดใหญ่กว่าเนื่องจากมีข้อมูล quote กลับมาด้วย

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

Answer มีโดย



Packet จะประกอบไปด้วย Port,Length,Checksum,payload

Reference :

ข้อที่ 9) หลักการที่ host ใช้เลือก source port : https://www.geeksforgeeks.org/difference-between-source-port-and-destination-port/

ข้อที่ 16) หลักการวัดค่า RTT จากการรับส่ง 3packets : https://blog.packet-foo.com/2014/07/determining-tcp-initial-round-trip-time/