Ouestions A

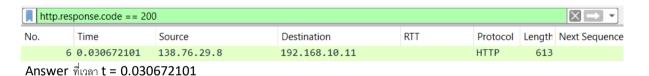
1) เครื่อง client ที่ส่ง HTTP GET request ในไฟล์ nat-inside-wireshark-trace1-1.pcapng ใช้หมายเลข IP address หมายเลขใด? TCP segment ที่นำส่ง HTTP GET request ระบุหมายเลข source port เป็น เลขอะไร? HTTP GET request ถูกส่งไปยังหมายเลข destination IP หมายเลขใด? TCP segment ที่ น้ำส่ง HTTP GET request ระบหมายเลข destination port เป็นเลขอะไร?

∨ Transmission Control Protocol, Src Port: 53924, Dst Por Source Address: 192.168.10.11 Source Port: 53924 Destination Address: 138.76.29.8 Destination Port: 80

> (11 TCP segment port) (ฐป ip segment address)

Answer ใน HTTP GET request ใช้หมายเลข IP เป็น 192.168.10.11 โดย TCP segment ที่นำส่ง HTTP GET request ใช้หมายเลข source port เป็นหมายเลข 53924 และ HTTP GET request ถูกส่งไปยังหมายเลข destination IP เป็น 138.76.29.8 โดย TCP segment ที่น้ำส่ง HTTP GET request ระบุหมายเลข destination port เป็นหมายเลข 80

2) เมื่อเวลาเท่าไร (สำหรับคำถามเวลานับจากนี้ โปรดระบุเวลานับจากเริ่มต้นไฟล์ trace ไม่ใช่เวลา wall-clock) ที่ HTTP 200 OK message จาก web server ถูกส่งต่อจาก NAT router ไปยังเครื่อง client ซึ่งอยู่ในฝั่ง LAN



3) หมายเลข source IP และ destination IP และหมายเลข TCP source port และ destination port ของ IP datagram ที่นาส่ง HTTP 200 OK message มีค่าเป็นเท่าใดบ้าง?

∨ Transmission Control Protocol, Src Port: 80, Dst Port: 5: Source Address: 138.76.29.8

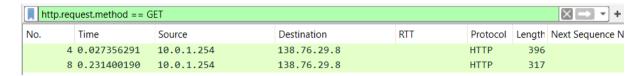
Source Port: 80

Destination Address: 192.168.10.11 Destination Port: 53924

(1월 ip segment address) (11 TCP segment port)

Answer HTTP 200 OK message ใช้หมายเลข source IP เป็น 138.76.29.8 โดย TCP segment ที่นำส่ง HTTP 200 OK message ใช้หมายเลข source port เป็นหมายเลข 80 และ HTTP 200 OK message ถูกส่งไป ยังหมายเลข destination IP เป็น 192.168.10.11 โดย TCP segment ที่นำส่ง HTTP 200 OK message ระบุ หมายเลข destination port เป็นหมายเลข 53924

4) เมื่อเวลาเท่าไร ที่ HTTP GET message ปรากฏขึ้นในไฟล์ nat-outside-wireshark-trace1-1.pcapng?



Answer เมื่อเวลา t = 0.027356291

5) หมายเลข source IP และ destination IP และหมายเลข TCP source port และ destination port ของ IP datagram ที่นาส่ง HTTP GET มีค่าเป็นเท่าใดบ้าง? (โปรดระบุค่าตามที่บันทึกได้ในไฟล์ nat-outside-wireshark-trace1-1.pcapng)

Source Address: 10.0.1.254 Source Port: 53924
Destination Address: 138.76.29.8 Destination Port: 80

(ฐปภาพ ip segment address)

(ฐปภาพ TCP segment port)

Answer ใน HTTP GET request ใช้หมายเลข IP เป็น 10.0.1.254 โดย TCP segment ที่นำส่ง HTTP GET request ใช้หมายเลข source port เป็นหมายเลข 53924 และ HTTP GET request ถูกส่งไปยังหมายเลข destination IP เป็น 138.76.29.8 โดย TCP segment ที่นำส่ง HTTP GET request ระบุหมายเลข destination port เป็นหมายเลข 80

- 6) จากข้อ 5) ค่าของ field ทั้ง 4 มี field ใดบ้างที่แตกต่างจากข้อ 1) ?

 Answer มีเพียง field Destination Address ใน ip segment เท่านั้น
- 7) จากการตรวจสอบ HTTP GET message เทียบระหว่างไฟล์ทั้งสอง มี field ใดใน HTTP header ที่ เปลี่ยนแปลงหรือไม่? ถ้าหากมีพบว่าเป็น field ใดบ้าง?

```
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
   [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
        [GET / HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
     Request Method: GET
     Request URI: /
     Request Version: HTTP/1.1
   Host: 138.76.29.8\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
   Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
```

(nat-outside-wireshark)

```
Hypertext Transfer Protocol
 ✓ GET / HTTP/1.1\r\n
   V [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
        [GET / HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /
     Request Version: HTTP/1.1
   Host: 138.76.29.8\r\n
   User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
   Accept-Language: en-US,en;q=0.5\r\n
   Accept-Encoding: gzip, deflate\r\n
   Connection: keep-alive\r\n
   Upgrade-Insecure-Requests: 1\r\n
```

(nat-inside-wireshark)

Answer จะเห็นว่าใน HTTP headerระหว่างไฟล์ทั้งสอง ทุกๆ fieldมีค่าเหมือนกันทุกประการไม่มีการ เปลี่ยนแปลง

8) ใน IP datagram ที่นำส่ง HTTP GET จาก datagram ที่ดักจับได้ในฝั่ง LAN (ฝั่งด้านใน) กับ datagram ที่ถูก ส่งต่อออกมายังฝั่งที่ใกล้กับการเชื่อมต่อ Internet (ฝั่งด้านนอก) ของ NAT router มีค่าของ field ใดที่ เปลี่ยนแปลงไปบ้างจากรายชื่อ field ใน IP header ต่อไปนี้: Version, Header Length, Flags, Checksum, Time to Live? หากมีการเปลี่ยนแปลงค่า โปรดระบุค่าเดิมและค่าใหม่

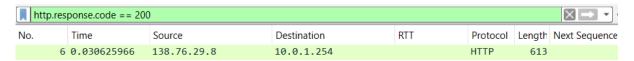
```
∨ Internet Protocol Version 4, Src: 192.168.10.11, Dst: 13
                                                                      ∨ Internet Protocol Version 4, Src: 10.0.1.254, Dst: 138.7
     0100 .... = Version: 4
                                                                           0100 .... = Version: 4
       .. 0101 = Header Length: 20 bytes (5)
                                                                              .. 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: )
                                                                         > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: I
     Total Length: 382
                                                                           Total Length: 382
     Identification: 0x6296 (25238)
                                                                           Identification: 0x6296 (25238)
   v 010. .... = Flags: 0x2, Don't fragment
                                                                         ∨ 010. .... = Flags: 0x2, Don't fragment
                                                                              0... = Reserved bit: Not set
       0... = Reserved bit: Not set
                                                                              .1.. .... = Don't fragment: Set
       .1.. .... = Don't fragment: Set
                                                                              ..0. .... = More fragments: Not set
       ..0. .... = More fragments: Not set
                                                                             ..0 0000 0000 0000 = Fragment Offset: 0
     ...0 0000 0000 0000 = Fragment Offset: 0
                                                                           Time to Live: 63
     Time to Live: 64
                                                                           Protocol: TCP (6)
     Protocol: TCP (6)
                                                                           Header Checksum: 0x2492 [validation disabled]
    Header Checksum: 0x64dc [validation disabled]
                                                                           [Header checksum status: Unverified]
     [Header checksum status: Unverified]
                                                                           Source Address: 10 0 1 254
     Source Address: 192,168,10,11
                                                                           Destination Address: 138.76.29.8
     Destination Address: 138.76.29.8
          (รปภาพ ip datagram ของ inside)
                                                                               (รปภาพ ip datagram ของ outsude)
```

Answer จะเห็นว่าการนำส่ง HTTP GET จากฝั่ง LAN ต่อออกมายังฝั่งการเชื่อมต่อ internet ของ NAT router มี ค่า 2 fields ด้วยกันที่ต่างกัน คือ Header Checksum กับ Time to Live (โดยจะบอกค่าก่อนผ่าน NAT router และ หลังจากผ่าน NAT router แล้วตามลำดับ)

Header Checksum เดิม : 0x64dc เป็น 0x2492

Time to Live เดิม : 64 เป็น 63

9) เมื่อเวลาเท่าไร ที่ HTTP 200 OK message ปรากฏขึ้นในไฟล์ nat-outside-wireshark-trace1-1.pcapng?



Answer ที่เวลา t = 0.030625966

10) หมายเลข source IP และ destination IP และหมายเลข TCP source port และ destination port ของ IP datagram ที่นำส่ง HTTP reply (~200 OK") มีค่าเป็น

Source Address: 138.76.29.8 Source

Destination Address: 10.0.1.254

Source Port: 80

Destination Port: 53924

เท่าใดบ้าง? (โปรดระบุค่าตามที่บันทึกได้ในไฟล์ nat-

outside-wireshark-trace1-1.pcapng)

(ฐปภาพ ip segment address)

(ฐปภาพ TCP segment port)

Answer HTTP 200 OK message ใช้หมายเลข source IP เป็น 138.76.29.8 โดย TCP segment ที่นำส่ง HTTP 200 OK message ใช้หมายเลข source port เป็นหมายเลข 80 และ HTTP 200 OK message ถูกส่งไป ยังหมายเลข destination IP เป็น 10.0.1.254 โดย TCP segment ที่นำส่ง HTTP 200 OK message ระบุ หมายเลข destination port เป็นหมายเลข 53924

- 11) หมายเลข source IP และ destination IP และหมายเลข TCP source port และ destination port ของ IP datagram ที่นำส่ง HTTP reply (~200 OK") ซึ่งถูกส่งจาก router ไปยัง host ปลายทางที่อยู่ด้านขวาตาม รูป 1 มีค่าเป็นเท่าใดบ้าง? (โปรดระบุค่าตามที่บันทึกได้ในไฟล์ nat-inside-wireshark-trace1-1.pcapng)
 Answer คำตอบเหมือนข้อ 3ทุกประการ
- 12) หากมีให้เพียงไฟล์ trace จานวนสองไฟล์ซึ่งดักจับ packets จากสองฝั่งของ NAT device ผู้เรียนสามารถระบุได้ หรือไม่ว่าฝั่งใดเป็นฝั่งเริ่มต้นส่งข้อมูลก่อนที่จะเกิดการ NAT ขึ้น? สามารถสังเกตได้จากอะไร? จงอธิบาย Answer สามารถระบุได้โดย
 - 1.เนื่องจากการส่งข้อมูลที่ผ่านการทำ NAT นั้นจำเป็นต้องเริ่มจากตัว host ก่อนดังนั้นจึงสามารถคาดการณ์ได้ว่าผึ่งที่ใช้ Source ip address เป็น private ip address จะเป็นฝ่ายเริ่มส่งข้อมูลก่อน
 - 2.เนื่องจากข้อมูลต้องส่งจาก inside ก่อนออกไป outside ดังนั้นใน ip datagram สามารถสังเกตจาก field ttl ได้โดยถ้า ttl มากกว่า จะเป็นฝ่ายเริ่มส่งข้อมูลก่อน
 - 3.สามารถสังเกตได้จากเวลาเมื่อทำการเริ่ม capture หากทั้งสองไฟล์เริ่ม capture พร้อมกันฝั่งที่เวลาน้อยกว่าในการส่ง request จะเป็นฝ่ายเริ่มส่งข้อมูลก่อน