

Inclass เรื่อง Getting start to Wireshark

กลุ่ม 1 รหัสนักศึกษา 65050368 ชื่อ สกุล ฌนภัทร์ เกิดเปี่ยม

ทำร่วมกับเพื่อน หรือ ไม่ ทำร่วมกัน ถ้าทำให้ระบุนักศึกษา และ รายชื่อเพื่อน

รหัสนักศึกษา 65050242 ชื่อ สกุล ฌนภัทร์ วรกิตติวงศ์

## 1. TCP

1.1 Yes or No Yes

1.2 โปรโตคอลนี้อยู่ใน TCP/IP stack layer Transport Layer

1.3 มี packet ของ Protocol อื่นขึ้นมาหรือไม่ ถ้ามี เป็น Protocol อะไรบ้าง มี 2 Protocol คือ TLSv1.2 และ HTTP

| *Ethernet  |            |               |               |          |        |   |
|--|------------|---------------|---------------|----------|--------|---|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help |            |               |               |          |        |   |
| tcp  |            |               |               |          |        |   |
| No.  | Time       | Source        | Destination   | Protocol | Length | Info  |
| 44524  | 488.246563 | 52.231.20.35  | 10.45.7.37    | TLSv1.2  | 85     | Application Data  |
| 44525  | 488.293231 | 10.45.7.37    | 52.231.20.35  | TCP      | 54     | 52015 → 8883 [ACK] Seq=218 Ack=218 Win=1029 Len=0                           |
| 44962  | 513.797414 | 10.45.7.37    | 103.21.25.201 | TCP      | 66     | 56568 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM            |
| 44963  | 513.799105 | 103.21.25.201 | 10.45.7.37    | TCP      | 66     | 80 → 56568 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128 |
| 44964  | 513.799189 | 10.45.7.37    | 103.21.25.201 | TCP      | 54     | 56568 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0                               |
| 44965  | 513.799373 | 10.45.7.37    | 103.21.25.201 | HTTP     | 165    | GET /connecttest.txt HTTP/1.1   |
| 44966  | 513.805399 | 103.21.25.201 | 10.45.7.37    | TCP      | 60     | 80 → 56568 [ACK] Seq=1 Ack=112 Win=64256 Len=0                              |
| 44967  | 513.805399 | 103.21.25.201 | 10.45.7.37    | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)  |
| 44968  | 513.805399 | 103.21.25.201 | 10.45.7.37    | TCP      | 60     | 80 → 56568 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0                       |
| 44969  | 513.805464 | 10.45.7.37    | 103.21.25.201 | TCP      | 54     | 56568 → 80 [ACK] Seq=112 Ack=189 Win=262400 Len=0                           |
| 44970  | 513.805568 | 10.45.7.37    | 103.21.25.201 | TCP      | 54     | 56568 → 80 [FIN, ACK] Seq=112 Ack=189 Win=262400 Len=0                      |
| 44973  | 514.117280 | 10.45.7.37    | 103.21.25.201 | TCP      | 54     | [TCP Retransmission] 56568 → 80 [FIN, ACK] Seq=112 Ack=189 Win=262400 Len=0 |
| 44974  | 514.119480 | 103.21.25.201 | 10.45.7.37    | TCP      | 60     | 80 → 56568 [ACK] Seq=189 Ack=113 Win=64256 Len=0                            |
| 46104  | 543.836350 | 10.45.7.37    | 103.21.25.187 | TCP      | 66     | 56569 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM            |
| 46105  | 543.838737 | 103.21.25.187 | 10.45.7.37    | TCP      | 66     | 80 → 56569 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128 |
| 46106  | 543.838821 | 10.45.7.37    | 103.21.25.187 | TCP      | 54     | 56569 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0                               |
| 46107  | 543.839026 | 10.45.7.37    | 103.21.25.187 | HTTP     | 165    | GET /connecttest.txt HTTP/1.1   |
| 46108  | 543.842937 | 103.21.25.187 | 10.45.7.37    | TCP      | 60     | 80 → 56569 [ACK] Seq=1 Ack=112 Win=64256 Len=0                              |
| 46109  | 543.843327 | 103.21.25.187 | 10.45.7.37    | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)  |
| 46110  | 543.843327 | 103.21.25.187 | 10.45.7.37    | TCP      | 60     | 80 → 56569 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0                       |
| 46111  | 543.843384 | 10.45.7.37    | 103.21.25.187 | TCP      | 54     | 56569 → 80 [ACK] Seq=112 Ack=189 Win=262400 Len=0                           |
| 46112  | 543.843524 | 10.45.7.37    | 103.21.25.187 | TCP      | 54     | 56569 → 80 [FIN, ACK] Seq=112 Ack=189 Win=262400 Len=0                      |
| 46114  | 543.845597 | 103.21.25.187 | 10.45.7.37    | TCP      | 60     | 80 → 56569 [ACK] Seq=189 Ack=113 Win=64256 Len=0                            |
| 46405  | 551.051884 | 104.196.0.153 | 10.45.7.37    | TCP      | 60     | 443 → 50898 [RST, ACK] Seq=2 Ack=1 Win=249 Len=0                            |

## 2. QUIC

### 2.1 Yes or No Yes

### 2.2 โปรโตคอลนี้อยู่ใน TCP/IP stack layer Transport Layer

### 2.3 มี packet ของ Protocol อื่นขึ้นมาหรือไม่ ถ้ามี เป็น Protocol อะไรบ้าง ไม่มี Protocol อื่น

Wireshark interface showing a capture on the 'quic' filter. The packet list displays various QUIC packets between source 10.45.7.37 and destination 142.251.175.84.

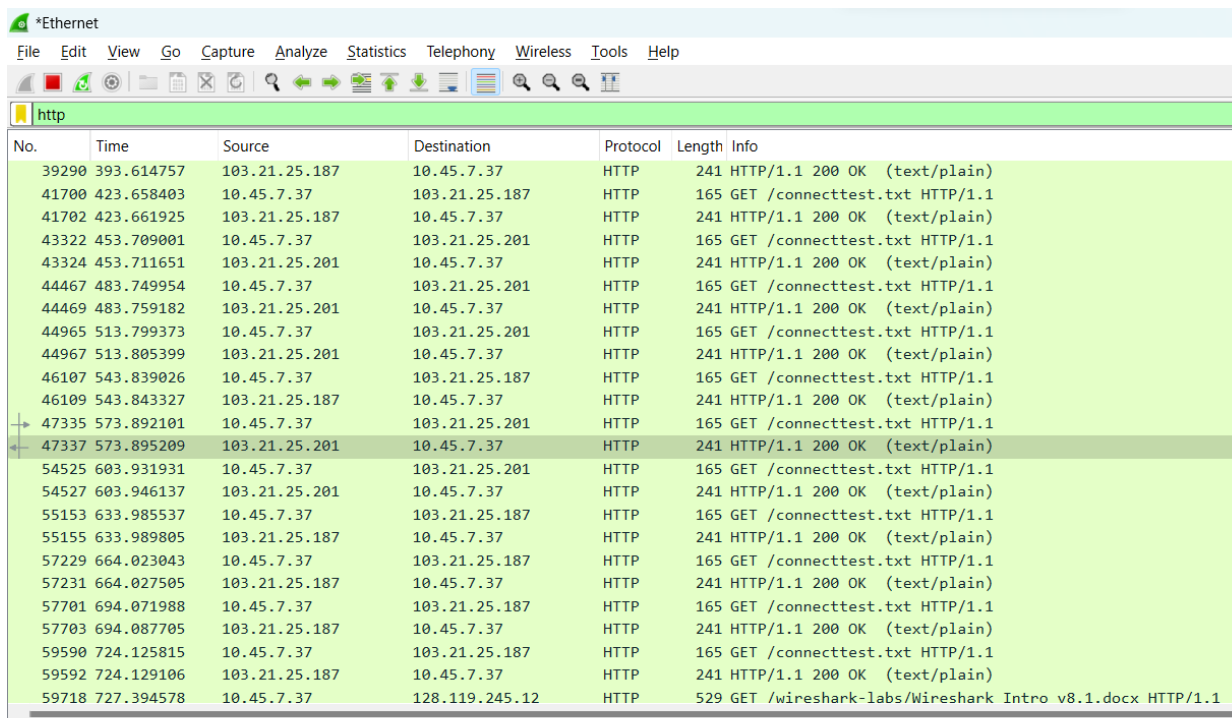
| No.   | Time       | Source         | Destination    | Protocol | Length | Info  |
|-------|------------|----------------|----------------|----------|--------|---|
| 47747 | 579.005395 | 10.45.7.37     | 142.251.175.84 | QUIC     | 1292   | Initial, DCID=fa29f820d76d0c08, PKN: 1, CRYPTO  |
| 47748 | 579.005470 | 10.45.7.37     | 142.251.175.84 | QUIC     | 1292   | Initial, DCID=fa29f820d76d0c08, PKN: 2, PADDING, CRYPTO                                     |
| 47749 | 579.006318 | 10.45.7.37     | 142.251.223.68 | QUIC     | 1292   | Initial, DCID=3b5c3302e7d3793c, PKN: 1, CRYPTO  |
| 47750 | 579.006350 | 10.45.7.37     | 142.251.223.68 | QUIC     | 1292   | Initial, DCID=3b5c3302e7d3793c, PKN: 2, PING, CRYPTO, PADDING, PING, PADDING, PING, PADDING |
| 47757 | 579.038550 | 142.251.175.84 | 10.45.7.37     | QUIC     | 1292   | Initial, SCID=fa29f820d76d0c08, PKN: 1, ACK, PADDING  |
| 47758 | 579.038550 | 142.251.175.84 | 10.45.7.37     | QUIC     | 1292   | Initial, SCID=fa29f820d76d0c08, PKN: 2, CRYPTO, PADDING                                     |
| 47759 | 579.038821 | 142.251.175.84 | 10.45.7.37     | QUIC     | 1292   | Initial, SCID=fa29f820d76d0c08, PKN: 3, CRYPTO, PADDING                                     |
| 47760 | 579.038821 | 142.251.175.84 | 10.45.7.37     | QUIC     | 1292   | Handshake, SCID=fa29f820d76d0c08  |
| 47761 | 579.039229 | 10.45.7.37     | 142.251.175.84 | QUIC     | 1292   | Initial, DCID=fa29f820d76d0c08, PKN: 3, ACK, PADDING  |
| 47762 | 579.039236 | 142.251.175.84 | 10.45.7.37     | QUIC     | 1292   | Handshake, SCID=fa29f820d76d0c08  |
| 47763 | 579.039293 | 10.45.7.37     | 142.251.175.84 | QUIC     | 81     | Handshake, DCID=fa29f820d76d0c08  |
| 47764 | 579.039445 | 142.251.175.84 | 10.45.7.37     | QUIC     | 1292   | Handshake, SCID=fa29f820d76d0c08  |
| 47765 | 579.042520 | 142.251.223.68 | 10.45.7.37     | QUIC     | 1292   | Initial, SCID=f55c3302e7d3793c, PKN: 1, ACK, PADDING  |
| 47766 | 579.043002 | 10.45.7.37     | 142.251.175.84 | QUIC     | 82     | Handshake, DCID=fa29f820d76d0c08  |
| 47767 | 579.043346 | 142.251.223.68 | 10.45.7.37     | QUIC     | 1292   | Initial, SCID=f55c3302e7d3793c, PKN: 2, CRYPTO, PADDING                                     |
| 47768 | 579.043346 | 142.251.223.68 | 10.45.7.37     | QUIC     | 1292   | Initial, SCID=f55c3302e7d3793c, PKN: 3, CRYPTO, PADDING                                     |
| 47769 | 579.043725 | 10.45.7.37     | 142.251.223.68 | QUIC     | 1292   | Initial, DCID=f55c3302e7d3793c, PKN: 3, ACK, PADDING  |
| 47770 | 579.051333 | 142.251.223.68 | 10.45.7.37     | QUIC     | 1292   | Handshake, SCID=f55c3302e7d3793c  |
| 47771 | 579.051586 | 142.251.223.68 | 10.45.7.37     | QUIC     | 1292   | Handshake, SCID=f55c3302e7d3793c  |
| 47772 | 579.051698 | 10.45.7.37     | 142.251.223.68 | QUIC     | 81     | Handshake, DCID=f55c3302e7d3793c  |
| 47773 | 579.051818 | 142.251.223.68 | 10.45.7.37     | QUIC     | 1292   | Handshake, SCID=f55c3302e7d3793c  |
| 47774 | 579.062519 | 10.45.7.37     | 142.251.223.68 | QUIC     | 82     | Handshake, DCID=f55c3302e7d3793c  |
| 47777 | 579.070517 | 142.251.175.84 | 10.45.7.37     | QUIC     | 867    | Protected Payload (KP0)   |
| 47778 | 579.072454 | 10.45.7.37     | 142.251.175.84 | QUIC     | 82     | Handshake, DCID=fa29f820d76d0c08  |

## 3. HTTP

3.1 Yes or No Yes

3.2 โปรโตคอลนี้อยู่ใน TCP/IP stack layer Application Layer

3.3 มี packet ของ Protocol อื่นขึ้นมาหรือไม่ ถ้ามี เป็น Protocol อะไรบ้าง ไม่มี Protocol อื่น



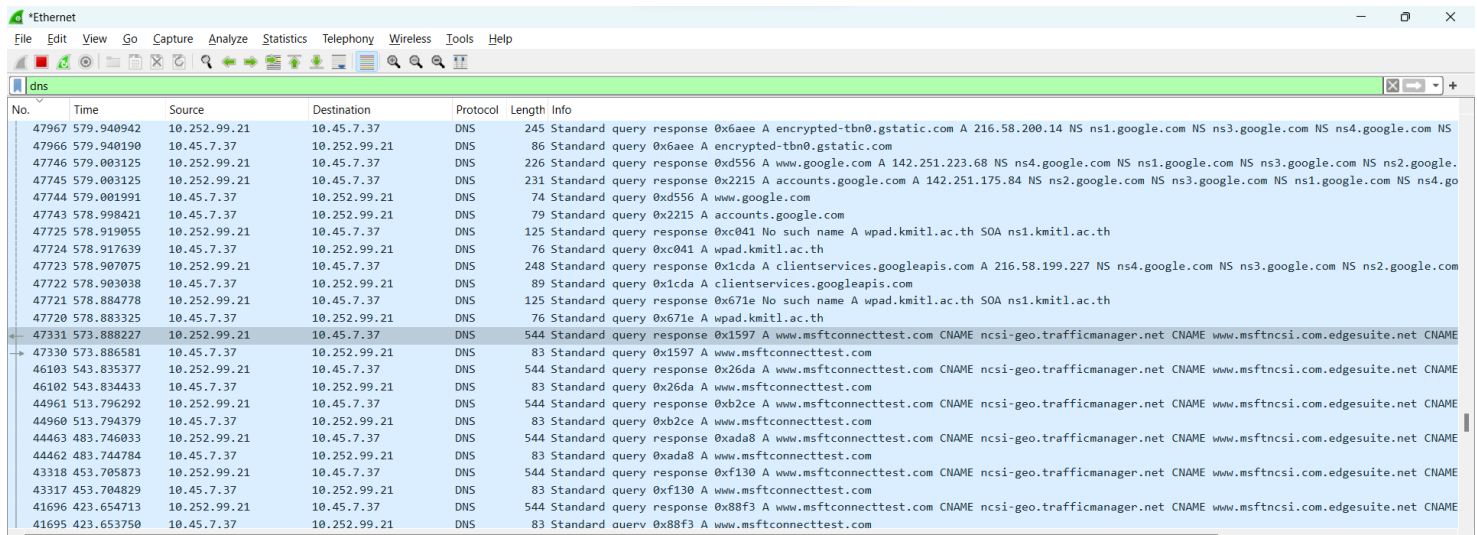
| No.   | Time       | Source        | Destination    | Protocol | Length | Info   |
|-------|------------|---------------|----------------|----------|--------|--|
| 39290 | 393.614757 | 103.21.25.187 | 10.45.7.37     | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)                           |
| 41700 | 423.658403 | 10.45.7.37    | 103.21.25.187  | HTTP     | 165    | GET /connecttest.txt HTTP/1.1                          |
| 41702 | 423.661925 | 103.21.25.187 | 10.45.7.37     | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)                           |
| 43322 | 453.709001 | 10.45.7.37    | 103.21.25.201  | HTTP     | 165    | GET /connecttest.txt HTTP/1.1                          |
| 43324 | 453.711651 | 103.21.25.201 | 10.45.7.37     | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)                           |
| 44467 | 483.749954 | 10.45.7.37    | 103.21.25.201  | HTTP     | 165    | GET /connecttest.txt HTTP/1.1                          |
| 44469 | 483.759182 | 103.21.25.201 | 10.45.7.37     | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)                           |
| 44965 | 513.799373 | 10.45.7.37    | 103.21.25.201  | HTTP     | 165    | GET /connecttest.txt HTTP/1.1                          |
| 44967 | 513.805399 | 103.21.25.201 | 10.45.7.37     | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)                           |
| 46107 | 543.839026 | 10.45.7.37    | 103.21.25.187  | HTTP     | 165    | GET /connecttest.txt HTTP/1.1                          |
| 46109 | 543.843327 | 103.21.25.187 | 10.45.7.37     | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)                           |
| 47335 | 573.892101 | 10.45.7.37    | 103.21.25.201  | HTTP     | 165    | GET /connecttest.txt HTTP/1.1                          |
| 47337 | 573.895209 | 103.21.25.201 | 10.45.7.37     | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)                           |
| 54525 | 603.931931 | 10.45.7.37    | 103.21.25.201  | HTTP     | 165    | GET /connecttest.txt HTTP/1.1                          |
| 54527 | 603.946137 | 103.21.25.201 | 10.45.7.37     | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)                           |
| 55153 | 633.985537 | 10.45.7.37    | 103.21.25.187  | HTTP     | 165    | GET /connecttest.txt HTTP/1.1                          |
| 55155 | 633.989805 | 103.21.25.187 | 10.45.7.37     | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)                           |
| 57229 | 664.023043 | 10.45.7.37    | 103.21.25.187  | HTTP     | 165    | GET /connecttest.txt HTTP/1.1                          |
| 57231 | 664.027505 | 103.21.25.187 | 10.45.7.37     | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)                           |
| 57701 | 694.071988 | 10.45.7.37    | 103.21.25.187  | HTTP     | 165    | GET /connecttest.txt HTTP/1.1                          |
| 57703 | 694.087705 | 103.21.25.187 | 10.45.7.37     | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)                           |
| 59590 | 724.125815 | 10.45.7.37    | 103.21.25.187  | HTTP     | 165    | GET /connecttest.txt HTTP/1.1                          |
| 59592 | 724.129106 | 103.21.25.187 | 10.45.7.37     | HTTP     | 241    | HTTP/1.1 200 OK (text/plain)                           |
| 59718 | 727.394578 | 10.45.7.37    | 128.119.245.12 | HTTP     | 529    | GET /wireshark-labs/Wireshark Intro v8.1.docx HTTP/1.1 |

## 4. DNS

4.1 Yes or No Yes

4.2 โปรโตคอลนี้อยู่ใน TCP/IP stack layer Application Layer

4.3 มี packet ของ Protocol อื่นขึ้นมาหรือไม่ ถ้ามี เป็น Protocol อะไรบ้าง ไม่มี Protocol อื่น



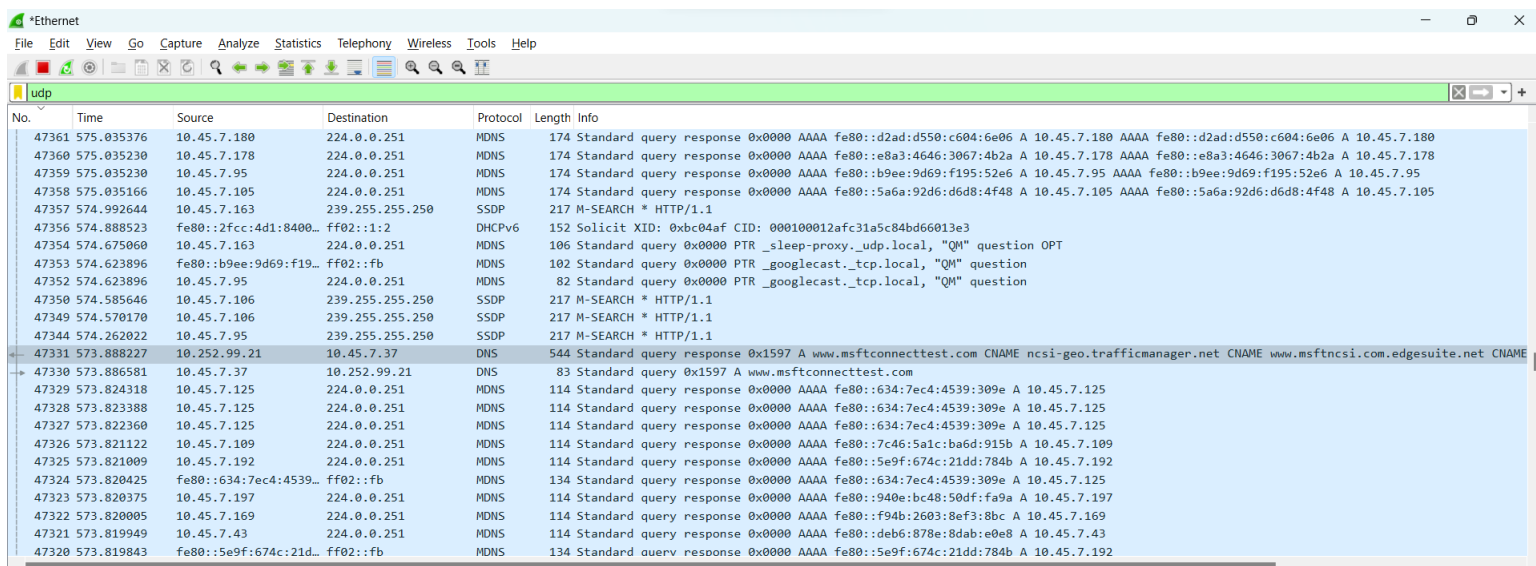
| No.   | Time       | Source       | Destination  | Protocol | Length | Info  |
|-------|------------|--------------|--------------|----------|--------|---|
| 47967 | 579.940942 | 10.252.99.21 | 10.45.7.37   | DNS      | 245    | Standard query response 0x6aee A encrypted-tbn0.gstatic.com A 216.58.200.14 NS ns1.google.com NS ns3.google.com NS ns4.google.com NS  |
| 47966 | 579.940190 | 10.45.7.37   | 10.252.99.21 | DNS      | 86     | Standard query 0x6aee A encrypted-tbn0.gstatic.com  |
| 47746 | 579.003125 | 10.252.99.21 | 10.45.7.37   | DNS      | 226    | Standard query response 0xd556 A www.google.com A 142.251.223.68 NS ns4.google.com NS ns1.google.com NS ns3.google.com NS ns2.google. |
| 47745 | 579.003125 | 10.252.99.21 | 10.45.7.37   | DNS      | 231    | Standard query response 0x2215 A accounts.google.com A 142.251.175.84 NS ns2.google.com NS ns3.google.com NS ns1.google.com NS ns4.go |
| 47744 | 579.001991 | 10.45.7.37   | 10.252.99.21 | DNS      | 74     | Standard query 0xd556 A www.google.com  |
| 47743 | 578.998421 | 10.45.7.37   | 10.252.99.21 | DNS      | 79     | Standard query 0x2215 A accounts.google.com   |
| 47725 | 578.919055 | 10.252.99.21 | 10.45.7.37   | DNS      | 125    | Standard query response 0xc041 No such name A wpad.kmitl.ac.th SOA ns1.kmitl.ac.th  |
| 47724 | 578.917639 | 10.45.7.37   | 10.252.99.21 | DNS      | 76     | Standard query 0xc041 A wpad.kmitl.ac.th  |
| 47723 | 578.907075 | 10.252.99.21 | 10.45.7.37   | DNS      | 248    | Standard query response 0x1cda A clientservices.googleapis.com A 216.58.199.227 NS ns4.google.com NS ns3.google.com NS ns2.google.com |
| 47722 | 578.903038 | 10.45.7.37   | 10.252.99.21 | DNS      | 89     | Standard query 0x1cda A clientservices.googleapis.com   |
| 47721 | 578.884778 | 10.252.99.21 | 10.45.7.37   | DNS      | 125    | Standard query response 0x671e No such name A wpad.kmitl.ac.th SOA ns1.kmitl.ac.th  |
| 47720 | 578.883325 | 10.45.7.37   | 10.252.99.21 | DNS      | 76     | Standard query 0x671e A wpad.kmitl.ac.th  |
| 47331 | 573.888227 | 10.252.99.21 | 10.45.7.37   | DNS      | 544    | Standard query response 0x1597 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME |
| 47330 | 573.886581 | 10.45.7.37   | 10.252.99.21 | DNS      | 83     | Standard query 0x1597 A www.msftconnecttest.com   |
| 46103 | 543.835377 | 10.252.99.21 | 10.45.7.37   | DNS      | 544    | Standard query response 0x26da A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME |
| 46102 | 543.834433 | 10.45.7.37   | 10.252.99.21 | DNS      | 83     | Standard query 0x26da A www.msftconnecttest.com   |
| 44961 | 513.796292 | 10.252.99.21 | 10.45.7.37   | DNS      | 544    | Standard query response 0xb2ce A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME |
| 44960 | 513.794379 | 10.45.7.37   | 10.252.99.21 | DNS      | 83     | Standard query 0xb2ce A www.msftconnecttest.com   |
| 44463 | 483.746033 | 10.252.99.21 | 10.45.7.37   | DNS      | 544    | Standard query response 0xada8 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME |
| 44462 | 483.744784 | 10.45.7.37   | 10.252.99.21 | DNS      | 83     | Standard query 0xada8 A www.msftconnecttest.com   |
| 43318 | 453.705873 | 10.252.99.21 | 10.45.7.37   | DNS      | 544    | Standard query response 0xf130 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME |
| 43317 | 453.704829 | 10.45.7.37   | 10.252.99.21 | DNS      | 83     | Standard query 0xf130 A www.msftconnecttest.com   |
| 41696 | 423.654713 | 10.252.99.21 | 10.45.7.37   | DNS      | 544    | Standard query response 0x88f3 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME |
| 41695 | 423.653750 | 10.45.7.37   | 10.252.99.21 | DNS      | 83     | Standard query 0x88f3 A www.msftconnecttest.com   |

## 5. UDP

## 5.1 Yes or No Yes

## 5.2 โปรโตคอลนี้อยู่ใน TCP/IP stack layer Transport Layer

## 5.3 มี packet ของ Protocol อื่นขึ้นมาหรือไม่ ถ้ามี เป็น Protocol อะไรบ้าง มี 4 Protocol คือ MDNS, SSDP, DHCPv6 และ DNS



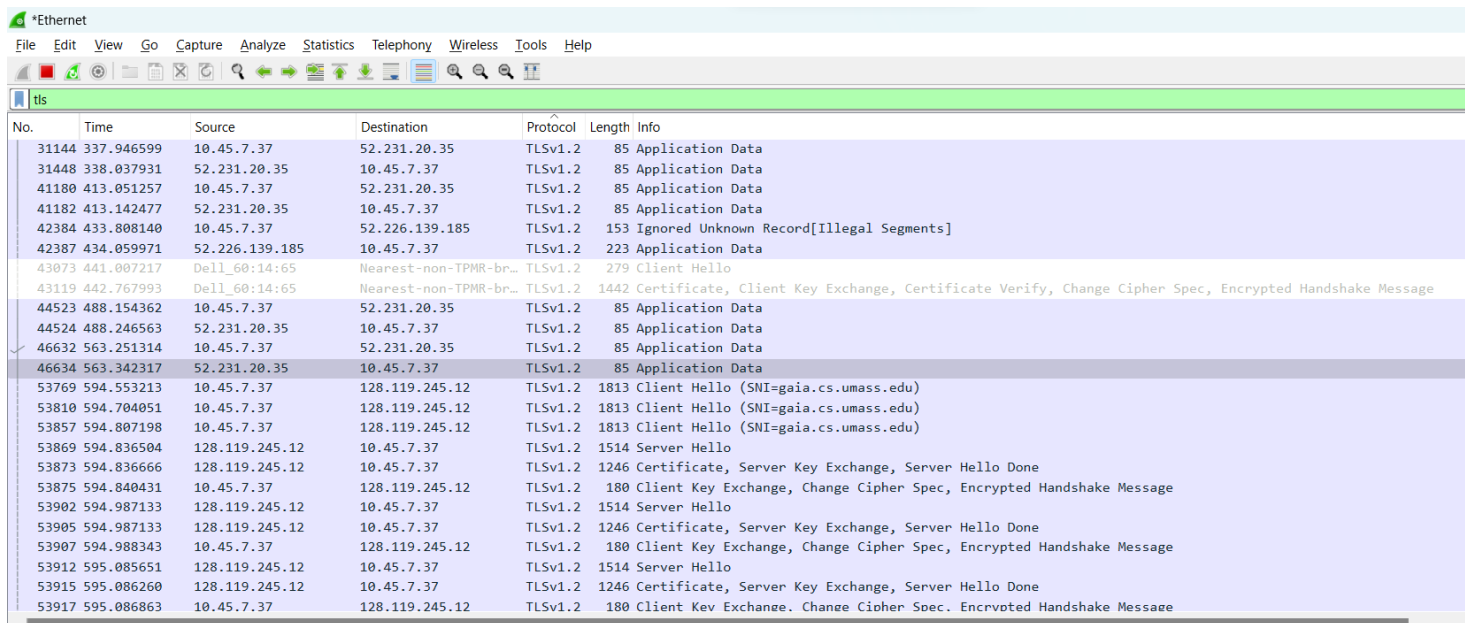
| No.   | Time       | Source                 | Destination     | Protocol | Length | Info  |
|-------|------------|------------------------|-----------------|----------|--------|---|
| 47361 | 575.035376 | 10.45.7.180            | 224.0.0.251     | MDNS     | 174    | Standard query response 0x0000 AAAA fe80::d2ad:d550:c604:6e06 A 10.45.7.180 AAAA fe80::d2ad:d550:c604:6e06 A 10.45.7.180              |
| 47360 | 575.035230 | 10.45.7.178            | 224.0.0.251     | MDNS     | 174    | Standard query response 0x0000 AAAA fe80::e8a3:4646:3067:4b2a A 10.45.7.178 AAAA fe80::e8a3:4646:3067:4b2a A 10.45.7.178              |
| 47359 | 575.035230 | 10.45.7.95             | 224.0.0.251     | MDNS     | 174    | Standard query response 0x0000 AAAA fe80::b9ee:9d69:f195:52e6 A 10.45.7.95 AAAA fe80::b9ee:9d69:f195:52e6 A 10.45.7.95                |
| 47358 | 575.035166 | 10.45.7.105            | 224.0.0.251     | MDNS     | 174    | Standard query response 0x0000 AAAA fe80::5a6a:92d6:d6d8:4f48 A 10.45.7.105 AAAA fe80::5a6a:92d6:d6d8:4f48 A 10.45.7.105              |
| 47357 | 574.992644 | 10.45.7.163            | 239.255.255.250 | SSDP     | 217    | M-SEARCH * HTTP/1.1   |
| 47356 | 574.888523 | fe80::2fcc:4d1:8400... | ff02::1:2       | DHCPv6   | 152    | Solicit XID: 0xbc04af CID: 000100012afc31a5c84bd66013e3   |
| 47354 | 574.675060 | 10.45.7.163            | 224.0.0.251     | MDNS     | 106    | Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT  |
| 47353 | 574.623896 | fe80::b9ee:9d69:f19... | ff02::fb        | MDNS     | 102    | Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question   |
| 47352 | 574.623896 | 10.45.7.95             | 224.0.0.251     | MDNS     | 82     | Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question   |
| 47350 | 574.585646 | 10.45.7.106            | 239.255.255.250 | SSDP     | 217    | M-SEARCH * HTTP/1.1   |
| 47349 | 574.570170 | 10.45.7.106            | 239.255.255.250 | SSDP     | 217    | M-SEARCH * HTTP/1.1   |
| 47344 | 574.262022 | 10.45.7.95             | 239.255.255.250 | SSDP     | 217    | M-SEARCH * HTTP/1.1   |
| 47331 | 573.888227 | 10.252.99.21           | 10.45.7.37      | DNS      | 544    | Standard query response 0x1597 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME |
| 47330 | 573.886581 | 10.45.7.37             | 10.252.99.21    | DNS      | 83     | Standard query 0x1597 A www.msftconnecttest.com   |
| 47329 | 573.824318 | 10.45.7.125            | 224.0.0.251     | MDNS     | 114    | Standard query response 0x0000 AAAA fe80::634:7ec4:4539:309e A 10.45.7.125  |
| 47328 | 573.823388 | 10.45.7.125            | 224.0.0.251     | MDNS     | 114    | Standard query response 0x0000 AAAA fe80::634:7ec4:4539:309e A 10.45.7.125  |
| 47327 | 573.822360 | 10.45.7.125            | 224.0.0.251     | MDNS     | 114    | Standard query response 0x0000 AAAA fe80::634:7ec4:4539:309e A 10.45.7.125  |
| 47326 | 573.821122 | 10.45.7.109            | 224.0.0.251     | MDNS     | 114    | Standard query response 0x0000 AAAA fe80::7c46:5a1c:ba6d:915b A 10.45.7.109   |
| 47325 | 573.821009 | 10.45.7.192            | 224.0.0.251     | MDNS     | 114    | Standard query response 0x0000 AAAA fe80::5e9f:674c:21dd:784b A 10.45.7.192   |
| 47324 | 573.820425 | fe80::634:7ec4:4539... | ff02::fb        | MDNS     | 134    | Standard query response 0x0000 AAAA fe80::634:7ec4:4539:309e A 10.45.7.125  |
| 47323 | 573.820375 | 10.45.7.197            | 224.0.0.251     | MDNS     | 114    | Standard query response 0x0000 AAAA fe80::940e:bc48:50df:fa9a A 10.45.7.197   |
| 47322 | 573.820005 | 10.45.7.169            | 224.0.0.251     | MDNS     | 114    | Standard query response 0x0000 AAAA fe80::f94b:2603:8ef3:8bc A 10.45.7.169  |
| 47321 | 573.819949 | 10.45.7.43             | 224.0.0.251     | MDNS     | 114    | Standard query response 0x0000 AAAA fe80::deb6:878e:8dab:e0e8 A 10.45.7.43  |
| 47320 | 573.819843 | fe80::5e9f:674c:21d... | ff02::fb        | MDNS     | 134    | Standard query response 0x0000 AAAA fe80::5e9f:674c:21dd:784b A 10.45.7.192   |

## 6. TLSv1.2

6.1 Yes or No Yes

6.2 โปรโตคอลนี้อยู่ใน TCP/IP stack layer Transport Layer

6.3 มี packet ของ Protocol อื่นขึ้นมาหรือไม่ ถ้ามี เป็น Protocol อะไรบ้าง มี 1 Protocol คือ TLSv1.3



| No.   | Time       | Source         | Destination            | Protocol | Length | Info  |
|-------|------------|----------------|------------------------|----------|--------|---|
| 31144 | 337.946599 | 10.45.7.37     | 52.231.20.35           | TLSv1.2  | 85     | Application Data  |
| 31448 | 338.037931 | 52.231.20.35   | 10.45.7.37             | TLSv1.2  | 85     | Application Data  |
| 41180 | 413.051257 | 10.45.7.37     | 52.231.20.35           | TLSv1.2  | 85     | Application Data  |
| 41182 | 413.142477 | 52.231.20.35   | 10.45.7.37             | TLSv1.2  | 85     | Application Data  |
| 42384 | 433.808140 | 10.45.7.37     | 52.226.139.185         | TLSv1.2  | 153    | Ignored Unknown Record[Illegal Segments]  |
| 42387 | 434.059971 | 52.226.139.185 | 10.45.7.37             | TLSv1.2  | 223    | Application Data  |
| 43073 | 441.007217 | Dell_60:14:65  | Nearest-non-TPMR-br... | TLSv1.2  | 279    | Client Hello  |
| 43119 | 442.767993 | Dell_60:14:65  | Nearest-non-TPMR-br... | TLSv1.2  | 1442   | Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message |
| 44523 | 488.154362 | 10.45.7.37     | 52.231.20.35           | TLSv1.2  | 85     | Application Data  |
| 44524 | 488.246563 | 52.231.20.35   | 10.45.7.37             | TLSv1.2  | 85     | Application Data  |
| 46632 | 563.251314 | 10.45.7.37     | 52.231.20.35           | TLSv1.2  | 85     | Application Data  |
| 46634 | 563.342317 | 52.231.20.35   | 10.45.7.37             | TLSv1.2  | 85     | Application Data  |
| 53769 | 594.553213 | 10.45.7.37     | 128.119.245.12         | TLSv1.2  | 1813   | Client Hello (SNI=gaia.cs.umass.edu)  |
| 53810 | 594.704051 | 10.45.7.37     | 128.119.245.12         | TLSv1.2  | 1813   | Client Hello (SNI=gaia.cs.umass.edu)  |
| 53857 | 594.807198 | 10.45.7.37     | 128.119.245.12         | TLSv1.2  | 1813   | Client Hello (SNI=gaia.cs.umass.edu)  |
| 53869 | 594.836504 | 128.119.245.12 | 10.45.7.37             | TLSv1.2  | 1514   | Server Hello  |
| 53873 | 594.836666 | 128.119.245.12 | 10.45.7.37             | TLSv1.2  | 1246   | Certificate, Server Key Exchange, Server Hello Done   |
| 53875 | 594.840431 | 10.45.7.37     | 128.119.245.12         | TLSv1.2  | 180    | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message                                  |
| 53902 | 594.987133 | 128.119.245.12 | 10.45.7.37             | TLSv1.2  | 1514   | Server Hello  |
| 53905 | 594.987133 | 128.119.245.12 | 10.45.7.37             | TLSv1.2  | 1246   | Certificate, Server Key Exchange, Server Hello Done   |
| 53907 | 594.988343 | 10.45.7.37     | 128.119.245.12         | TLSv1.2  | 180    | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message                                  |
| 53912 | 595.085651 | 128.119.245.12 | 10.45.7.37             | TLSv1.2  | 1514   | Server Hello  |
| 53915 | 595.086260 | 128.119.245.12 | 10.45.7.37             | TLSv1.2  | 1246   | Certificate, Server Key Exchange, Server Hello Done   |
| 53917 | 595.086863 | 10.45.7.37     | 128.119.245.12         | TLSv1.2  | 180    | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message                                  |