Thanakorn Seemek
603110310092

TCP/IP

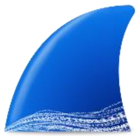
-การวิเคราะห์ข้อมูลเครือข่ายด้วย wireshark

Wireshark is Data Detection program IP in loop network

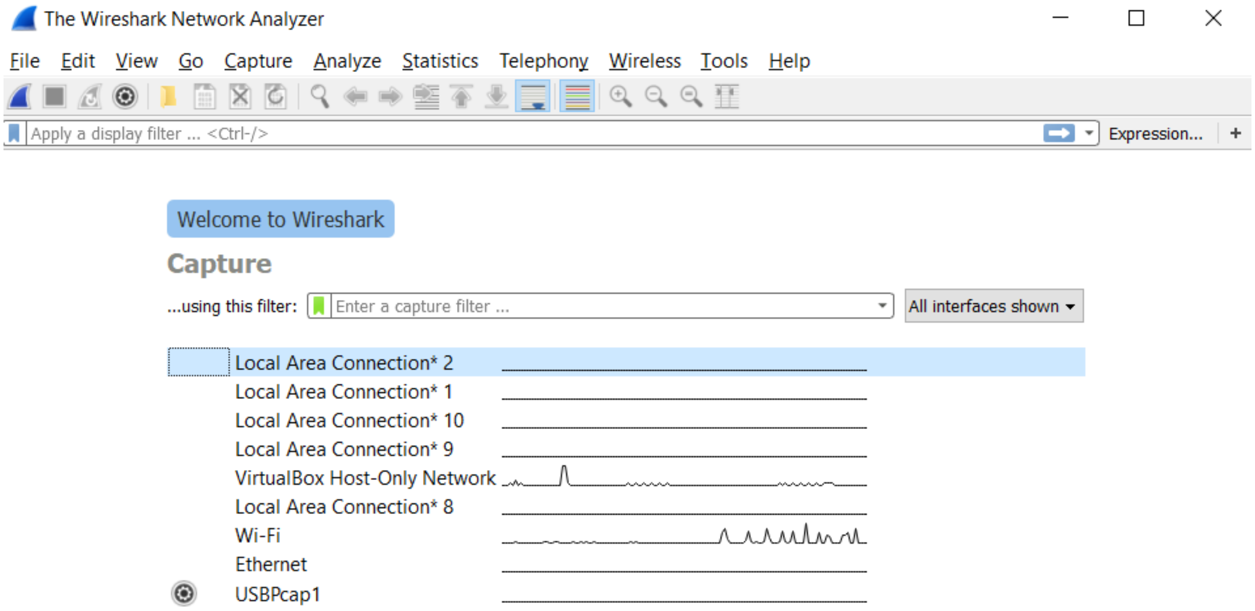
Wireshark -Can detect only //http

-No can detect only //https because of the code IP

-Program wireshark



-The look of the program Wireshark



Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

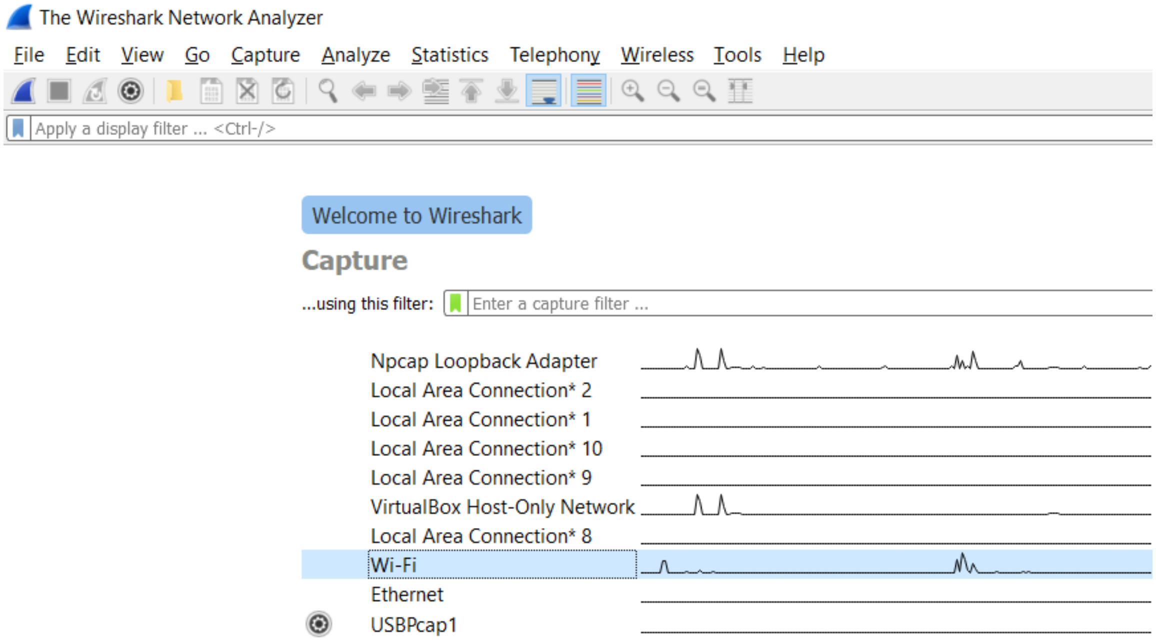
Capture

...using this filter: Enter a capture filter ...

Local Area Connection* 2
Local Area Connection* 1
Local Area Connection* 10
Local Area Connection* 9
VirtualBox Host-Only Network
Local Area Connection* 8
Wi-Fi
Ethernet
USBPcap1

1) Select the information you want to detect.

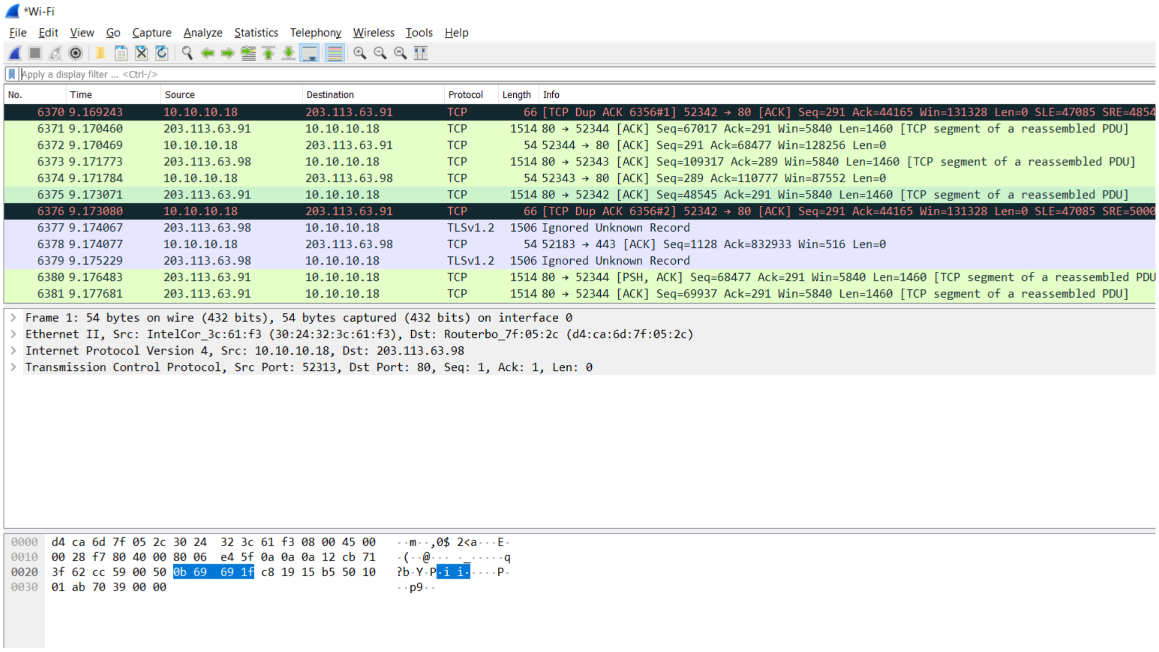
-I will choose to detect Wi-Fi


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …

Npcap Loopback Adapter
Local Area Connection* 2
Local Area Connection* 1
Local Area Connection* 10
Local Area Connection* 9
VirtualBox Host-Only Network
Local Area Connection* 8
Wi-Fi
Ethernet
USBPcap1

2) Double click the Wi-Fi

-Detection of the data package.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

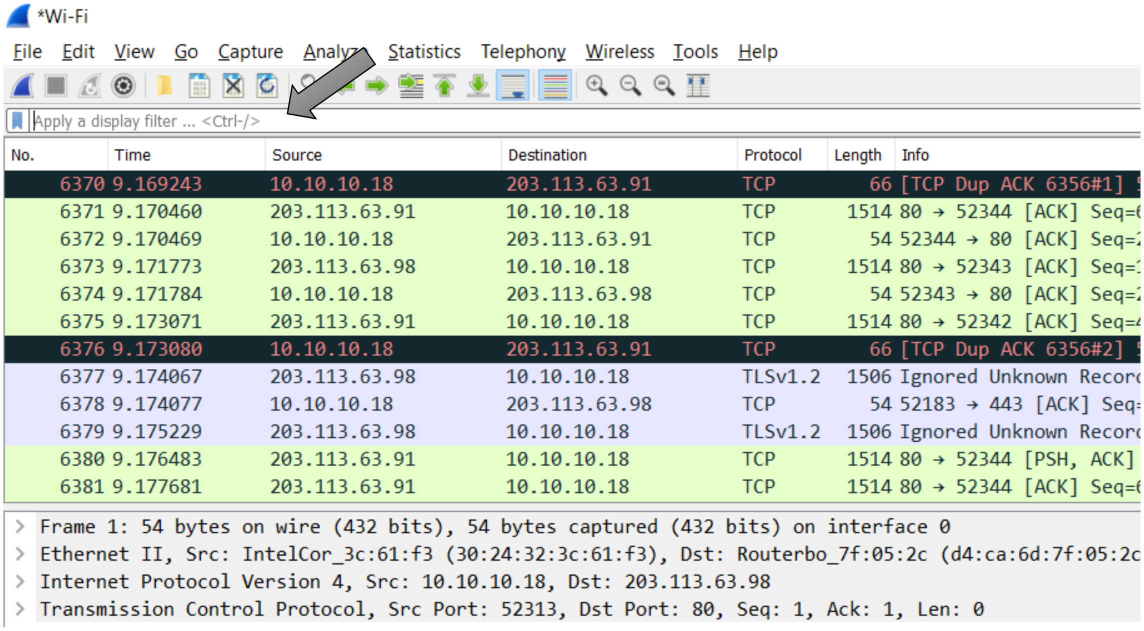
```
No.    Time      Source         Destination    Protocol Length Info
  6370 9.169243  10.10.10.18    203.113.63.91  TCP        66 [TCP Dup ACK 6356#1] 52342 → 80 [ACK] Seq=291 Ack=44165 Win=131328 Len=0 SLE=47085 SRE=4854
  6371 9.170460  203.113.63.91  10.10.10.18    TCP      1514 80 → 52344 [ACK] Seq=67017 Ack=291 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
  6372 9.170469  10.10.10.18    203.113.63.91  TCP        54 52344 → 80 [ACK] Seq=291 Ack=68477 Win=128256 Len=0
  6373 9.171773  203.113.63.98  10.10.10.18    TCP      1514 80 → 52343 [ACK] Seq=109317 Ack=289 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
  6374 9.171784  10.10.10.18    203.113.63.98  TCP        54 52343 → 80 [ACK] Seq=289 Ack=110777 Win=87552 Len=0
  6375 9.173071  203.113.63.91  10.10.10.18    TCP      1514 80 → 52342 [ACK] Seq=48545 Ack=291 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
  6376 9.173080  10.10.10.18    203.113.63.91  TCP        66 [TCP Dup ACK 6356#2] 52342 → 80 [ACK] Seq=291 Ack=44165 Win=131328 Len=0 SLE=47085 SRE=5000
  6377 9.174067  203.113.63.98  10.10.10.18    TLSv1.2  1506 Ignored Unknown Record
  6378 9.174077  10.10.10.18    203.113.63.98  TCP        54 52183 → 443 [ACK] Seq=1128 Ack=832933 Win=516 Len=0
  6379 9.175229  203.113.63.98  10.10.10.18    TLSv1.2  1506 Ignored Unknown Record
  6380 9.176483  203.113.63.91  10.10.10.18    TCP      1514 80 → 52344 [PSH, ACK] Seq=68477 Ack=291 Win=5840 Len=1460 [TCP segment of a reassembled PDU
  6381 9.177681  203.113.63.91  10.10.10.18    TCP      1514 80 → 52344 [ACK] Seq=69937 Ack=291 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
```

```
> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: IntelCor_3c:61:f3 (30:24:32:3c:61:f3), Dst: Routerbo_7f:05:2c (d4:ca:6d:7f:05:2c)
> Internet Protocol Version 4, Src: 10.10.10.18, Dst: 203.113.63.98
> Transmission Control Protocol, Src Port: 52313, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

```
0000  d4 ca 6d 7f 05 2c 30 24  32 3c 61 f3 08 00 45 00   ··m··,0$ 2<a···E·
0010  00 28 f7 80 40 00 80 06  e4 5f 0a 0a 0a 12 cb 71   ·(··@··· ·_·····q
0020  3f 62 cc 59 00 50 0b 69  69 1f c8 19 15 b5 50 10   ?b·Y·P·i i·····P·
0030  01 ab 70 39 00 00                                  ··p9··
```

-stop for see the information you want to see.

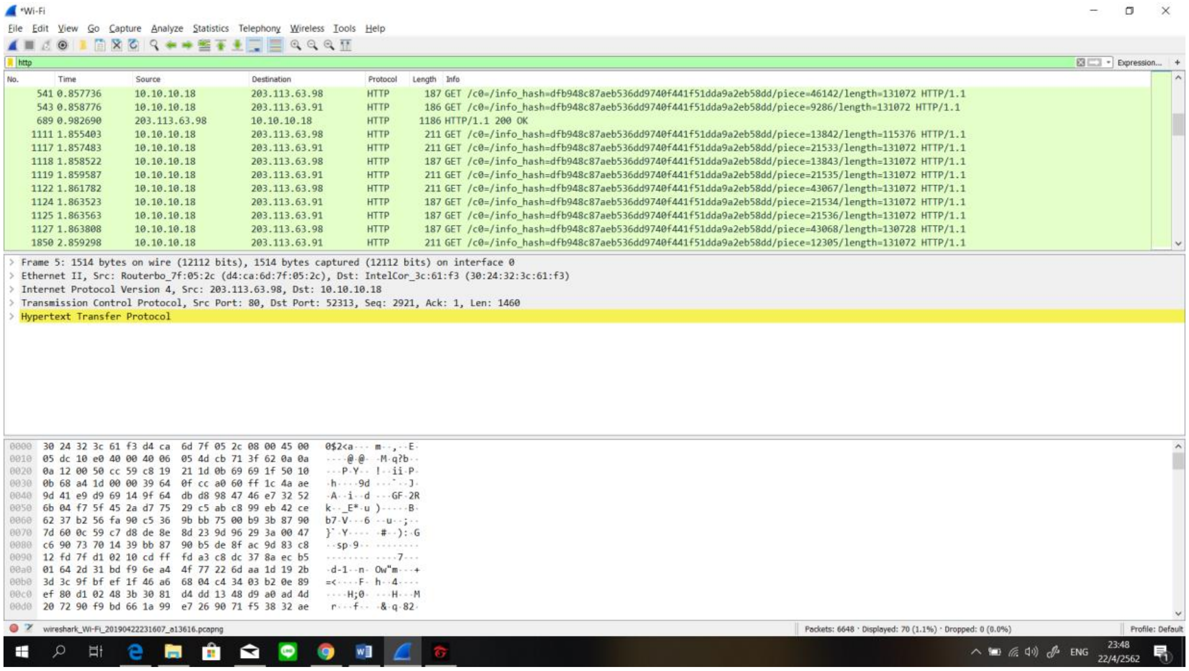
3) Finding the information you need
-Apply a display filter……<Ctr-/>


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.    Time      Source         Destination    Protocol Length Info
  6370 9.169243  10.10.10.18    203.113.63.91  TCP        66 [TCP Dup ACK 6356#1]
  6371 9.170460  203.113.63.91  10.10.10.18    TCP      1514 80 → 52344 [ACK] Seq=
  6372 9.170469  10.10.10.18    203.113.63.91  TCP        54 52344 → 80 [ACK] Seq=
  6373 9.171773  203.113.63.98  10.10.10.18    TCP      1514 80 → 52343 [ACK] Seq=
  6374 9.171784  10.10.10.18    203.113.63.98  TCP        54 52343 → 80 [ACK] Seq=
  6375 9.173071  203.113.63.91  10.10.10.18    TCP      1514 80 → 52342 [ACK] Seq=
  6376 9.173080  10.10.10.18    203.113.63.91  TCP        66 [TCP Dup ACK 6356#2]
  6377 9.174067  203.113.63.98  10.10.10.18    TLSv1.2  1506 Ignored Unknown Recor
  6378 9.174077  10.10.10.18    203.113.63.98  TCP        54 52183 → 443 [ACK] Seq=
  6379 9.175229  203.113.63.98  10.10.10.18    TLSv1.2  1506 Ignored Unknown Recor
  6380 9.176483  203.113.63.91  10.10.10.18    TCP      1514 80 → 52344 [PSH, ACK]
  6381 9.177681  203.113.63.91  10.10.10.18    TCP      1514 80 → 52344 [ACK] Seq=

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: IntelCor_3c:61:f3 (30:24:32:3c:61:f3), Dst: Routerbo_7f:05:2c (d4:ca:6d:7f:05:2c
> Internet Protocol Version 4, Src: 10.10.10.18, Dst: 203.113.63.98
> Transmission Control Protocol, Src Port: 52313, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

4) Search for //http data


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

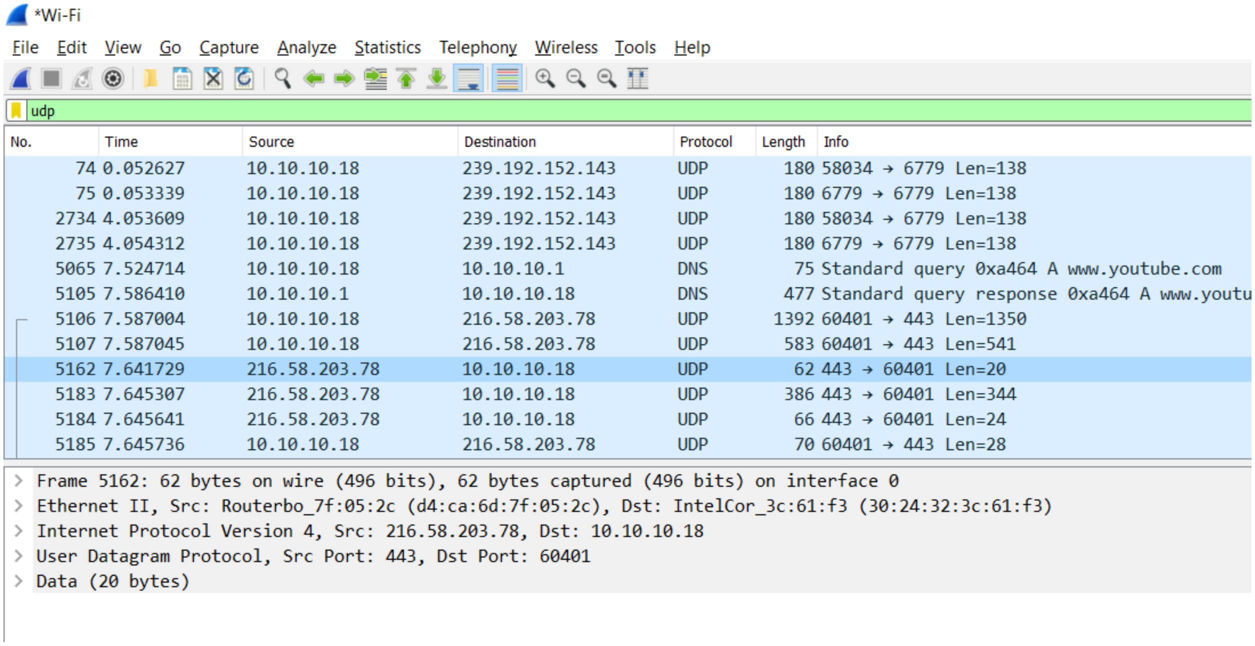
```
No.    Time      Source         Destination    Protocol Length Info
   541 0.857736  10.10.10.18    203.113.63.98  HTTP      187 GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=46142/length=131072 HTTP/1.1
   543 0.858776  10.10.10.18    203.113.63.91  HTTP      186 GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=9286/length=131072 HTTP/1.1
   689 0.982690  203.113.63.98  10.10.10.18    HTTP     1186 HTTP/1.1 200 OK
  1111 1.855403  10.10.10.18    203.113.63.98  HTTP      211 GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=13842/length=115376 HTTP/1.1
  1117 1.857483  10.10.10.18    203.113.63.91  HTTP      211 GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=21533/length=131072 HTTP/1.1
  1118 1.858522  10.10.10.18    203.113.63.98  HTTP      187 GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=13843/length=131072 HTTP/1.1
  1119 1.859587  10.10.10.18    203.113.63.91  HTTP      211 GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=21535/length=131072 HTTP/1.1
  1122 1.861782  10.10.10.18    203.113.63.98  HTTP      211 GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=43067/length=131072 HTTP/1.1
  1124 1.863523  10.10.10.18    203.113.63.91  HTTP      187 GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=21534/length=131072 HTTP/1.1
  1125 1.863563  10.10.10.18    203.113.63.91  HTTP      187 GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=21536/length=131072 HTTP/1.1
  1127 1.863808  10.10.10.18    203.113.63.98  HTTP      187 GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=43068/length=130728 HTTP/1.1
  1850 2.859298  10.10.10.18    203.113.63.91  HTTP      211 GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=12305/length=131072 HTTP/1.1

> Frame 5: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Routerbo_7f:05:2c (d4:ca:6d:7f:05:2c), Dst: IntelCor_3c:61:f3 (30:24:32:3c:61:f3)
> Internet Protocol Version 4, Src: 203.113.63.98, Dst: 10.10.10.18
> Transmission Control Protocol, Src Port: 80, Dst Port: 52313, Seq: 2921, Ack: 1, Len: 1460
> Hypertext Transfer Protocol

0000  30 24 32 3c 61 f3 d4 ca  6d 7f 05 2c 08 00 45 00   0$2<a··· m··,··E·
0010  05 dc 10 e0 40 00 40 06  05 4d cb 71 3f 62 0a 0a   ····@·@· ·M·q?b··
0020  0a 12 00 50 cc 59 c8 19  21 1d 0b 69 69 1f 50 10   ···P·Y·· !··ii·P·
0030  0b 68 a4 1d 00 00 39 64  0f cc a0 60 ff 1c 4a ae   ·h····9d ···`··J·
0040  9d 41 e9 d9 69 14 9f 64  db d8 98 47 46 e7 32 52   ·A··i··d ···GF·2R
0050  6b 04 f7 5f 45 2a d7 75  29 c5 ab c8 99 eb 42 ce   k··_E*·u )·····B·
0060  62 37 b2 56 fa 90 c5 36  9b bb 75 00 b9 3b 87 90   b7·V···6 ··u··;··
0070  7d 60 0c 59 c7 d8 de 8e  8d 23 9d 96 29 3a 00 47   }`·Y···· ·#··):·G
0080  c6 90 73 70 14 39 bb 87  90 b5 de 8f ac 9d 83 c8   ··sp·9·· ········
0090  12 fd 7f d1 02 10 cd ff  fd a3 c8 dc 37 8a ec b5   ········ ····7···
00a0  01 64 2d 31 bd f9 6e a4  4f 77 22 6d aa 1d 19 2b   ·d-1··n· Ow"m···+
00b0  3d 3c 9f bf ef 1f 46 a6  68 04 c4 34 03 b2 0e 89   =<····F· h··4····
00c0  ef 80 d1 02 48 3b 30 81  d4 dd 13 48 d9 a0 ad 4d   ····H;0· ···H···M
00d0  20 72 90 f9 bd 66 1a 99  e7 26 90 71 f5 38 32 ae    r···f·· ·&·q·82·

wireshark_Wi-Fi_20190422231607_a13616.pcapng    Packets: 6648 · Displayed: 70 (1.1%) · Dropped: 0 (0.0%)    Profile: Default
```

5) Search for //UDP data

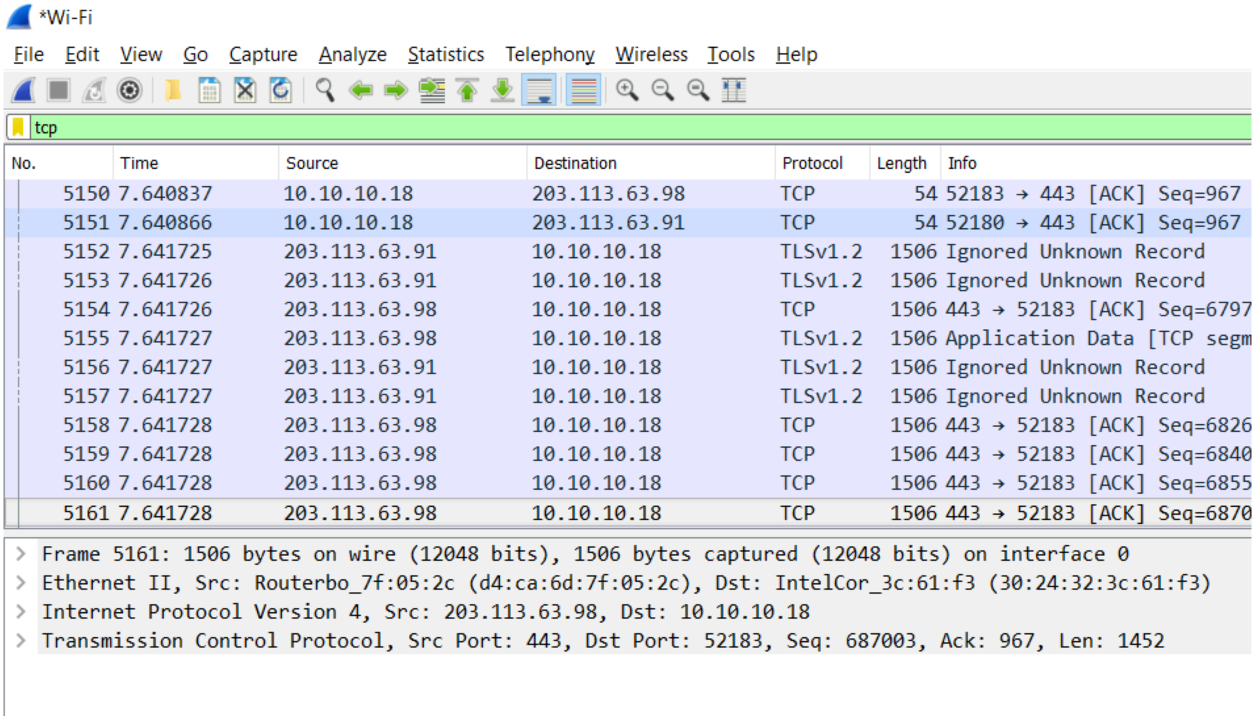

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
74	0.052627	10.10.10.18	239.192.152.143	UDP	180	58034 → 6779 Len=138
75	0.053339	10.10.10.18	239.192.152.143	UDP	180	6779 → 6779 Len=138
2734	4.053609	10.10.10.18	239.192.152.143	UDP	180	58034 → 6779 Len=138
2735	4.054312	10.10.10.18	239.192.152.143	UDP	180	6779 → 6779 Len=138
5065	7.524714	10.10.10.18	10.10.10.1	DNS	75	Standard query 0xa464 A www.youtube.com
5105	7.586410	10.10.10.1	10.10.10.18	DNS	477	Standard query response 0xa464 A www.youtu
5106	7.587004	10.10.10.18	216.58.203.78	UDP	1392	60401 → 443 Len=1350
5107	7.587045	10.10.10.18	216.58.203.78	UDP	583	60401 → 443 Len=541
5162	7.641729	216.58.203.78	10.10.10.18	UDP	62	443 → 60401 Len=20
5183	7.645307	216.58.203.78	10.10.10.18	UDP	386	443 → 60401 Len=344
5184	7.645641	216.58.203.78	10.10.10.18	UDP	66	443 → 60401 Len=24
5185	7.645736	10.10.10.18	216.58.203.78	UDP	70	60401 → 443 Len=28

```
> Frame 5162: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
> Ethernet II, Src: Routerbo_7f:05:2c (d4:ca:6d:7f:05:2c), Dst: IntelCor_3c:61:f3 (30:24:32:3c:61:f3)
> Internet Protocol Version 4, Src: 216.58.203.78, Dst: 10.10.10.18
> User Datagram Protocol, Src Port: 443, Dst Port: 60401
> Data (20 bytes)
```

6) Search for //TCP data

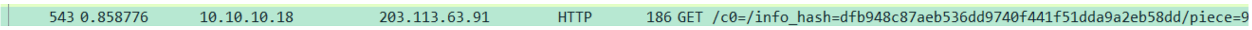

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
5150	7.640837	10.10.10.18	203.113.63.98	TCP	54	52183 → 443 [ACK] Seq=967
5151	7.640866	10.10.10.18	203.113.63.91	TCP	54	52180 → 443 [ACK] Seq=967
5152	7.641725	203.113.63.91	10.10.10.18	TLSv1.2	1506	Ignored Unknown Record
5153	7.641726	203.113.63.91	10.10.10.18	TLSv1.2	1506	Ignored Unknown Record
5154	7.641726	203.113.63.98	10.10.10.18	TCP	1506	443 → 52183 [ACK] Seq=6797
5155	7.641727	203.113.63.98	10.10.10.18	TLSv1.2	1506	Application Data [TCP segm
5156	7.641727	203.113.63.91	10.10.10.18	TLSv1.2	1506	Ignored Unknown Record
5157	7.641727	203.113.63.91	10.10.10.18	TLSv1.2	1506	Ignored Unknown Record
5158	7.641728	203.113.63.98	10.10.10.18	TCP	1506	443 → 52183 [ACK] Seq=6826
5159	7.641728	203.113.63.98	10.10.10.18	TCP	1506	443 → 52183 [ACK] Seq=6840
5160	7.641728	203.113.63.98	10.10.10.18	TCP	1506	443 → 52183 [ACK] Seq=6855
5161	7.641728	203.113.63.98	10.10.10.18	TCP	1506	443 → 52183 [ACK] Seq=6870

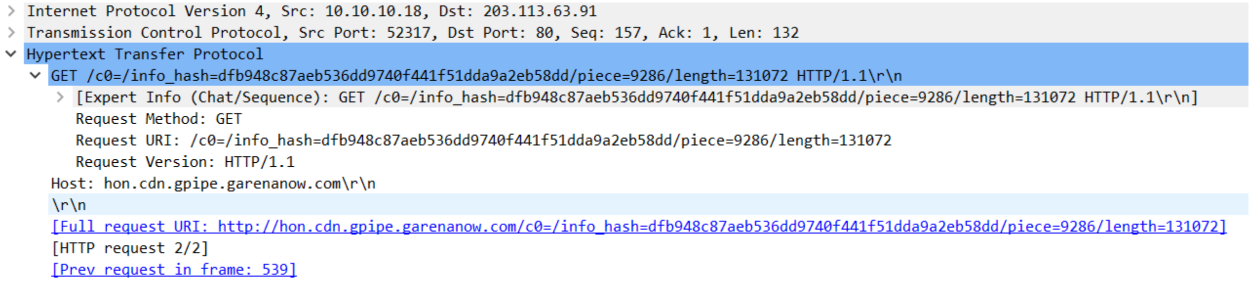
```
> Frame 5161: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface 0
> Ethernet II, Src: Routerbo_7f:05:2c (d4:ca:6d:7f:05:2c), Dst: IntelCor_3c:61:f3 (30:24:32:3c:61:f3)
> Internet Protocol Version 4, Src: 203.113.63.98, Dst: 10.10.10.18
> Transmission Control Protocol, Src Port: 443, Dst Port: 52183, Seq: 687003, Ack: 967, Len: 1452
```

7) The procedure of the HTTP protocol to show which packet is a request for a webpage and which packets are a response.



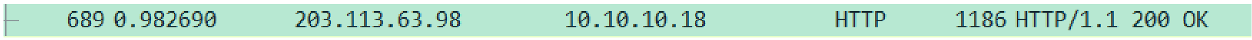
```
543 0.858776   10.10.10.18   203.113.63.91   HTTP   186 GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=9
```

-client send Request go to server past header request line a website



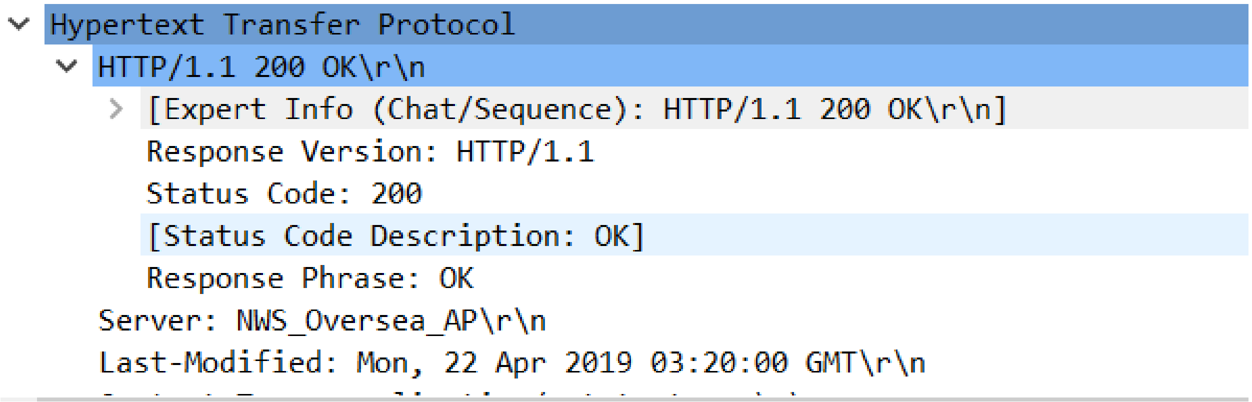
```
> Internet Protocol Version 4, Src: 10.10.10.18, Dst: 203.113.63.91
> Transmission Control Protocol, Src Port: 52317, Dst Port: 80, Seq: 157, Ack: 1, Len: 132
v Hypertext Transfer Protocol
  v GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=9286/length=131072 HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=9286/length=131072 HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=9286/length=131072
      Request Version: HTTP/1.1
    Host: hon.cdn.gpipe.garenanow.com\r\n
    \r\n
    [Full request URI: http://hon.cdn.gpipe.garenanow.com/c0=/info_hash=dfb948c87aeb536dd9740f441f51dda9a2eb58dd/piece=9286/length=131072]
    [HTTP request 2/2]
    [Prev request in frame: 539]
```

-Responses server



```
689 0.982690   203.113.63.98   10.10.10.18   HTTP   1186 HTTP/1.1 200 OK
```

-Server responses past header (Status line = Status-code 200 “OK”) means that the request is successful.



```
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Server: NWS_Oversea_AP\r\n
    Last-Modified: Mon, 22 Apr 2019 03:20:00 GMT\r\n
```

8) UDP (User Datagram Protocol) works on layer4 as a connection, sending less data, no connection.

9) TCP or Transmission Control Protocol. It is a protocol used in the Internet protocol set, which is the form of a protocol group commonly used as a standard in the Internet.

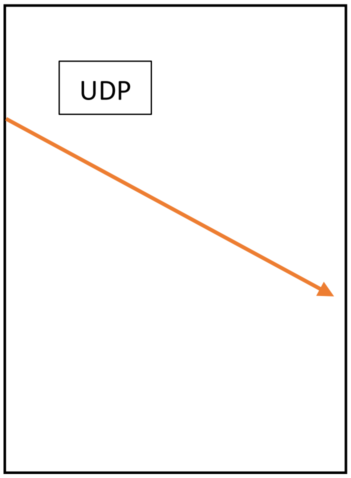
-TCP : transmission Control Protocol (Transport layer)

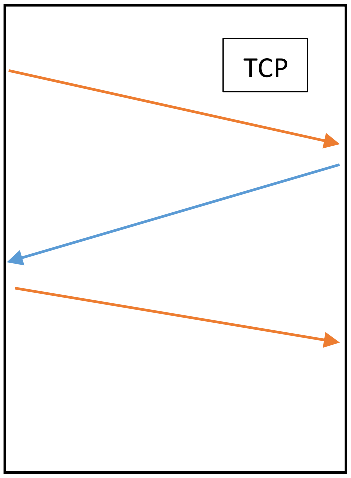
- IP : Internet Protocol (Network layer)

TCP / IP The function of TCP is to create precision based on the sequence and check for errors. To send information Connect with IP Network

Thanakorn Seemek
603110310092

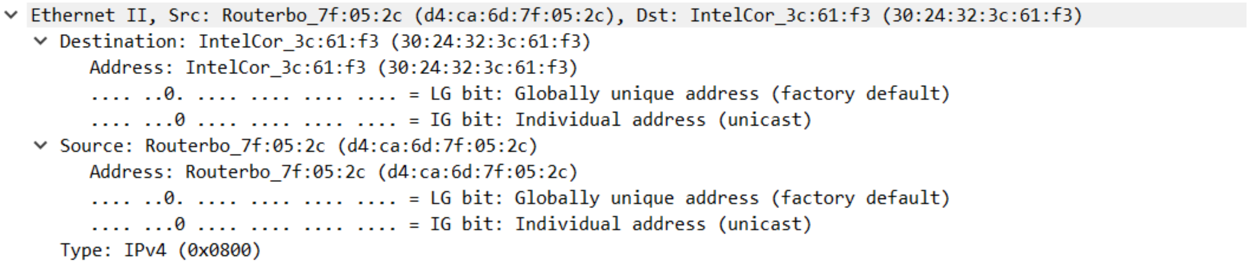
10) UDP is data transmission without confirmation of data transmission. Is that the sender cannot know whether the information has reached the recipient yet.





11)MSNMS protocols for program MSN Messagers Is to see the messages that are exported.

12) Ethenet protocols for program Check IP



```
Ethernet II, Src: Routerbo_7f:05:2c (d4:ca:6d:7f:05:2c), Dst: IntelCor_3c:61:f3 (30:24:32:3c:61:f3)
  Destination: IntelCor_3c:61:f3 (30:24:32:3c:61:f3)
    Address: IntelCor_3c:61:f3 (30:24:32:3c:61:f3)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Routerbo_7f:05:2c (d4:ca:6d:7f:05:2c)
    Address: Routerbo_7f:05:2c (d4:ca:6d:7f:05:2c)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```