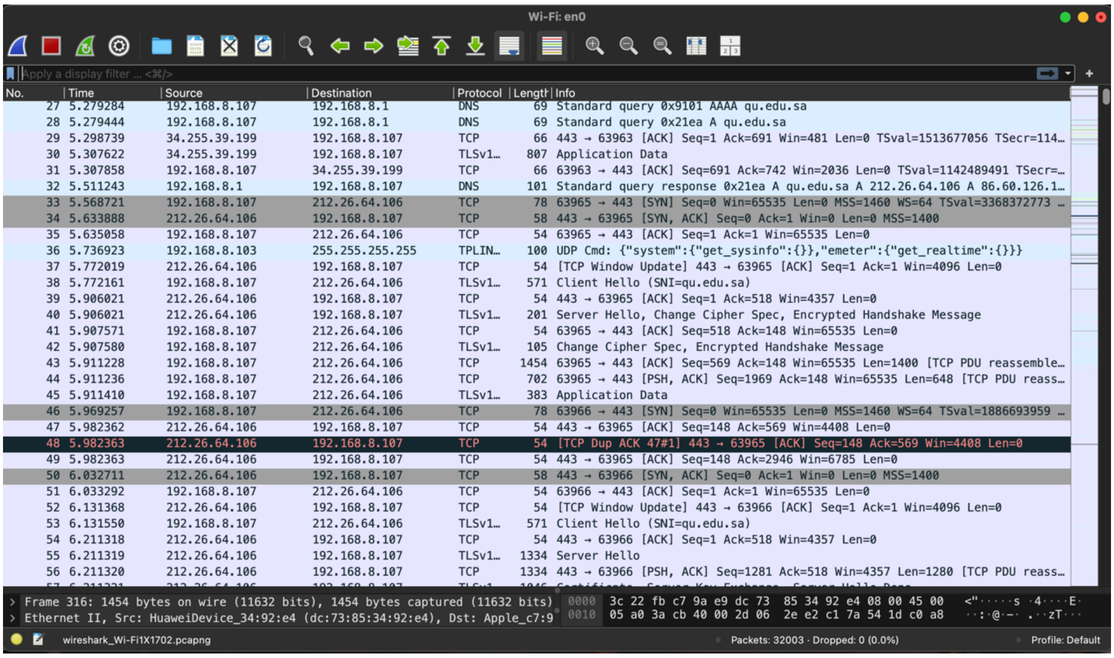
LabWeek2

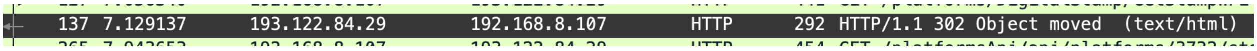
Part 1: Capturing HTTP Traffic.

Start Wireshark and capture packets.

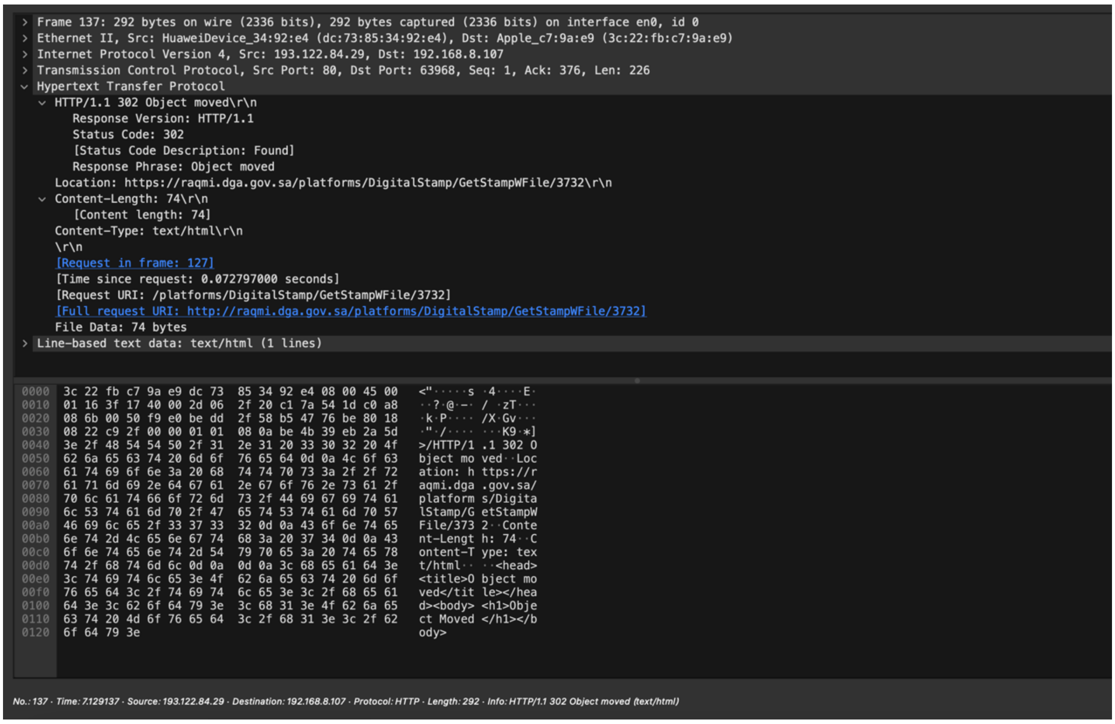


```
Wi-Fi: en0
Apply a display filter ... <⌘/>
No.  Time      Source          Destination      Protocol Length Info
 27 5.279284  192.168.8.107   192.168.8.1      DNS        69 Standard query 0x9101 AAAA qu.edu.sa
 28 5.279444  192.168.8.107   192.168.8.1      DNS        69 Standard query 0x21ea A qu.edu.sa
 29 5.298739  34.255.39.199   192.168.8.107    TCP        66 443 → 63963 [ACK] Seq=1 Ack=691 Win=481 Len=0 TSval=1513677056 TSecr=114…
 30 5.307622  34.255.39.199   192.168.8.107    TLSv1…    807 Application Data
 31 5.307858  192.168.8.107   34.255.39.199    TCP        66 63963 → 443 [ACK] Seq=691 Ack=742 Win=2036 Len=0 TSval=1142489491 TSecr=…
 32 5.511243  192.168.8.1     192.168.8.107    DNS       101 Standard query response 0x21ea A qu.edu.sa A 212.26.64.106 A 86.60.126.1…
 33 5.568721  192.168.8.107   212.26.64.106    TCP        78 63965 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3368372773 …
 34 5.633888  212.26.64.106   192.168.8.107    TCP        58 443 → 63965 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1400
 35 5.635058  192.168.8.107   212.26.64.106    TCP        54 63965 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
 36 5.736923  192.168.8.103   255.255.255.255  TPLIN…    100 UDP Cmd: {"system":{"get_sysinfo":{}},"emeter":{"get_realtime":{}}}
 37 5.772019  212.26.64.106   192.168.8.107    TCP        54 [TCP Window Update] 443 → 63965 [ACK] Seq=1 Ack=1 Win=4096 Len=0
 38 5.772161  192.168.8.107   212.26.64.106    TLSv1…    571 Client Hello (SNI=qu.edu.sa)
 39 5.906021  212.26.64.106   192.168.8.107    TCP        54 443 → 63965 [ACK] Seq=1 Ack=518 Win=4357 Len=0
 40 5.906021  212.26.64.106   192.168.8.107    TLSv1…    201 Server Hello, Change Cipher Spec, Encrypted Handshake Message
 41 5.907571  192.168.8.107   212.26.64.106    TCP        54 63965 → 443 [ACK] Seq=518 Ack=148 Win=65535 Len=0
 42 5.907580  192.168.8.107   212.26.64.106    TLSv1…    105 Change Cipher Spec, Encrypted Handshake Message
 43 5.911228  192.168.8.107   212.26.64.106    TCP      1454 63965 → 443 [ACK] Seq=569 Ack=148 Win=65535 Len=1400 [TCP PDU reassemble…
 44 5.911236  192.168.8.107   212.26.64.106    TCP       702 63965 → 443 [PSH, ACK] Seq=1969 Ack=148 Win=65535 Len=648 [TCP PDU reass…
 45 5.911410  192.168.8.107   212.26.64.106    TLSv1…    383 Application Data
 46 5.969257  192.168.8.107   212.26.64.106    TCP        78 63966 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1886693959 …
 47 5.982362  212.26.64.106   192.168.8.107    TCP        54 443 → 63965 [ACK] Seq=148 Ack=569 Win=4408 Len=0
 48 5.982363  212.26.64.106   192.168.8.107    TCP        54 [TCP Dup ACK 47#1] 443 → 63965 [ACK] Seq=148 Ack=569 Win=4408 Len=0
 49 5.982363  212.26.64.106   192.168.8.107    TCP        54 443 → 63965 [ACK] Seq=148 Ack=2946 Win=6785 Len=0
 50 6.032711  212.26.64.106   192.168.8.107    TCP        58 443 → 63966 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1400
 51 6.033292  192.168.8.107   212.26.64.106    TCP        54 63966 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
 52 6.131368  212.26.64.106   192.168.8.107    TCP        54 [TCP Window Update] 443 → 63966 [ACK] Seq=1 Ack=1 Win=4096 Len=0
 53 6.131550  192.168.8.107   212.26.64.106    TLSv1…    571 Client Hello (SNI=qu.edu.sa)
 54 6.211318  212.26.64.106   192.168.8.107    TCP        54 443 → 63966 [ACK] Seq=1 Ack=518 Win=4357 Len=0
 55 6.211319  212.26.64.106   192.168.8.107    TLSv1…   1334 Server Hello
 56 6.211320  212.26.64.106   192.168.8.107    TCP      1334 443 → 63966 [PSH, ACK] Seq=1281 Ack=518 Win=4357 Len=1280 [TCP PDU reass…

> Frame 316: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)   0000  3c 22 fb c7 9a e9 dc 73  85 34 92 e4 08 00 45 00   <"·····s ·4····E·
> Ethernet II, Src: HuaweiDevice_34:92:e4 (dc:73:85:34:92:e4), Dst: Apple_c7:9   0010  05 a0 3a cb 40 00 2d 06  2e e2 c1 7a 54 1d c0 a8   ··:·@·-· .··zT···

wireshark_Wi-Fi1X1702.pcapng          Packets: 32003 · Dropped: 0 (0.0%)          Profile: Default
```

Filter HTTP packets and analyze them.

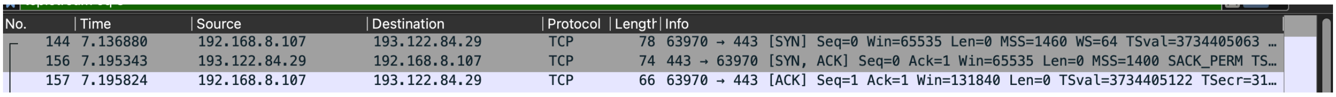


```
137  7.129137   193.122.84.29   192.168.8.107   HTTP   292 HTTP/1.1 302 Object moved  (text/html)
```



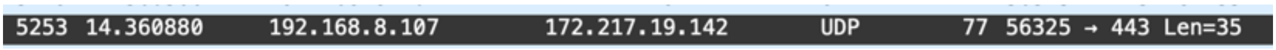
```
> Frame 137: 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits) on interface en0, id 0
> Ethernet II, Src: HuaweiDevice_34:92:e4 (dc:73:85:34:92:e4), Dst: Apple_c7:9a:e9 (3c:22:fb:c7:9a:e9)
> Internet Protocol Version 4, Src: 193.122.84.29, Dst: 192.168.8.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 63968, Seq: 1, Ack: 376, Len: 226
v Hypertext Transfer Protocol
  v HTTP/1.1 302 Object moved\r\n
      Response Version: HTTP/1.1
      Status Code: 302
      [Status Code Description: Found]
      Response Phrase: Object moved
    Location: https://raqmi.dga.gov.sa/platforms/DigitalStamp/GetStampWFile/3732\r\n
  v Content-Length: 74\r\n
      [Content length: 74]
    Content-Type: text/html\r\n
    \r\n
    [Request in frame: 127]
    [Time since request: 0.072797000 seconds]
    [Request URI: /platforms/DigitalStamp/GetStampWFile/3732]
    [Full request URI: http://raqmi.dga.gov.sa/platforms/DigitalStamp/GetStampWFile/3732]
    File Data: 74 bytes
> Line-based text data: text/html (1 lines)

0000  3c 22 fb c7 9a e9 dc 73  85 34 92 e4 08 00 45 00   <"·····s ·4····E·
0010  01 16 3f 17 40 00 2d 06  2f 20 c1 7a 54 1d c0 a8   ··?·@·-· / ·zT···
0020  08 6b 00 50 f9 e0 be dd  2f 58 b5 47 76 be 80 18   ·k·P···· /X·Gv···
0030  08 22 c9 2f 00 00 01 01  08 0a be 4b 39 eb 2a 5d   ·"·/···· ···K9·*]
0040  3e 2f 48 54 54 50 2f 31  2e 31 20 33 30 32 20 4f   >/HTTP/1 .1 302 O
0050  62 6a 65 63 74 20 6d 6f  76 65 64 0d 0a 4c 6f 63   bject mo ved··Loc
0060  61 74 69 6f 6e 3a 20 68  74 74 70 73 3a 2f 2f 72   ation: h ttps://r
0070  61 71 6d 69 2e 64 67 61  2e 67 6f 76 2e 73 61 2f   aqmi.dga .gov.sa/
0080  70 6c 61 74 66 6f 72 6d  73 2f 44 69 67 69 74 61   platform s/Digita
0090  6c 53 74 61 6d 70 2f 47  65 74 53 74 61 6d 70 57   lStamp/G etStampW
00a0  46 69 6c 65 2f 33 37 33  32 0d 0a 43 6f 6e 74 65   File/373 2··Conte
00b0  6e 74 2d 4c 65 6e 67 74  68 3a 20 37 34 0d 0a 43   nt-Lengt h: 74··C
00c0  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 74 65 78   ontent-T ype: tex
00d0  74 2f 68 74 6d 6c 0d 0a  0d 0a 3c 68 65 61 64 3e   t/html·· ··<head>
00e0  3c 74 69 74 6c 65 3e 4f  62 6a 65 63 74 20 6d 6f   <title>O bject mo
00f0  76 65 64 3c 2f 74 69 74  6c 65 3e 3c 2f 68 65 61   ved</tit le></hea
0100  64 3e 3c 62 6f 64 79 3e  3c 68 31 3e 4f 62 6a 65   d><body> <h1>Obje
0110  63 74 20 4d 6f 76 65 64  3c 2f 68 31 3e 3c 2f 62   ct Moved </h1></b
0120  6f 64 79 3e                                        ody>

No.: 137 · Time: 7.129137 · Source: 193.122.84.29 · Destination: 192.168.8.107 · Protocol: HTTP · Length: 292 · Info: HTTP/1.1 302 Object moved (text/html)
```

Part 2: Analyzing TCP/IP Traffic.

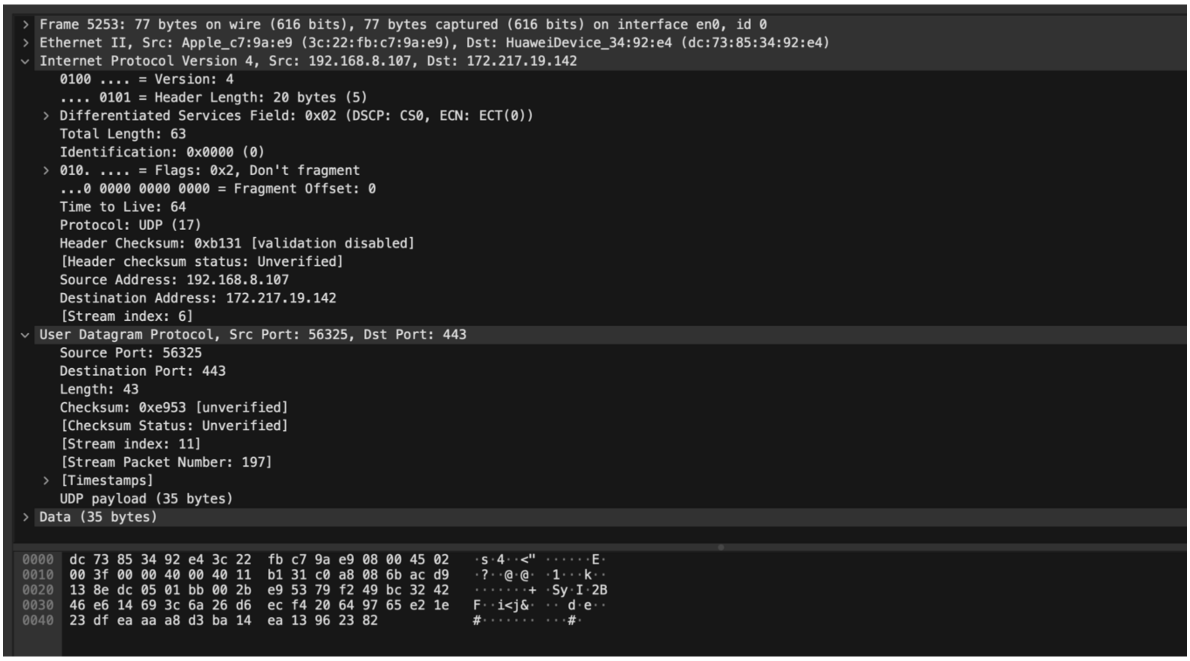


```
No.       |Time      |Source          |Destination     |Protocol |Length|Info
  144 7.136880  192.168.8.107   193.122.84.29   TCP        78 63970 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3734405063 …
  156 7.195343  193.122.84.29   192.168.8.107   TCP        74 443 → 63970 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM TS…
  157 7.195824  192.168.8.107   193.122.84.29   TCP        66 63970 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=3734405122 TSecr=31…
```

Part 3: Capturing and Analyzing UDP Traffic.



```
5253 14.360880    192.168.8.107     172.217.19.142    UDP      77 56325 → 443 Len=35
```



```
> Frame 5253: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface en0, id 0
> Ethernet II, Src: Apple_c7:9a:e9 (3c:22:fb:c7:9a:e9), Dst: HuaweiDevice_34:92:e4 (dc:73:85:34:92:e4)
v Internet Protocol Version 4, Src: 192.168.8.107, Dst: 172.217.19.142
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0))
    Total Length: 63
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xb131 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.8.107
    Destination Address: 172.217.19.142
    [Stream index: 6]
v User Datagram Protocol, Src Port: 56325, Dst Port: 443
    Source Port: 56325
    Destination Port: 443
    Length: 43
    Checksum: 0xe953 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 11]
    [Stream Packet Number: 197]
  > [Timestamps]
    UDP payload (35 bytes)
> Data (35 bytes)

0000  dc 73 85 34 92 e4 3c 22  fb c7 9a e9 08 00 45 02   ·s·4··<" ······E·
0010  00 3f 00 00 40 00 40 11  b1 31 c0 a8 08 6b ac d9   ·?··@·@· ·1···k··
0020  13 8e dc 05 01 bb 00 2b  e9 53 79 f2 49 bc 32 42   ·······+ ·Sy·I·2B
0030  46 e6 14 69 3c 6a 26 d6  ec f4 20 64 97 65 e2 1e   F··i<j&· ·· d·e··
0040  23 df ea aa a8 d3 ba 14  ea 13 96 23 82            #······· ···#·
```