আন্তর্জাতিক ইসলামী বিশ্ববিদ্যালয় চট্টগ্রাম

الجامعة الإسلامية العالمية شيتاغونغ

International Islamic University Chittagong

Department of Computer Science & Engineering

Lab Report 01

Course Code : **CSE-3633**

Course Title : **Computer Network**

Submitted To:

Abdul Kayum

Adjunct Faculty, Department of CSE,

International Islamic University Chittagong.

Submitted By:

Name : **Shahariar Nafiz**

ID : **C221361**

Section : **7DM**

Semester : **7th**

Date of Submission: 06-03-2025

Title: Introduction to Wireshark.

Objective:

The objective of this lab is to familiarize students with the Wireshark network protocol analyzer. Students will learn how to capture and analyze network packets, observe the interaction between different protocols, and understand the structure of HTTP messages. By the end of this lab, students should be able to:

Install and run Wireshark.

Capture network traffic.

Filter and analyze specific protocols (e.g., HTTP).

Interpret packet details and understand the encapsulation process.

Tools and Requirements:

Wireshark: A free and open-source packet analyzer.

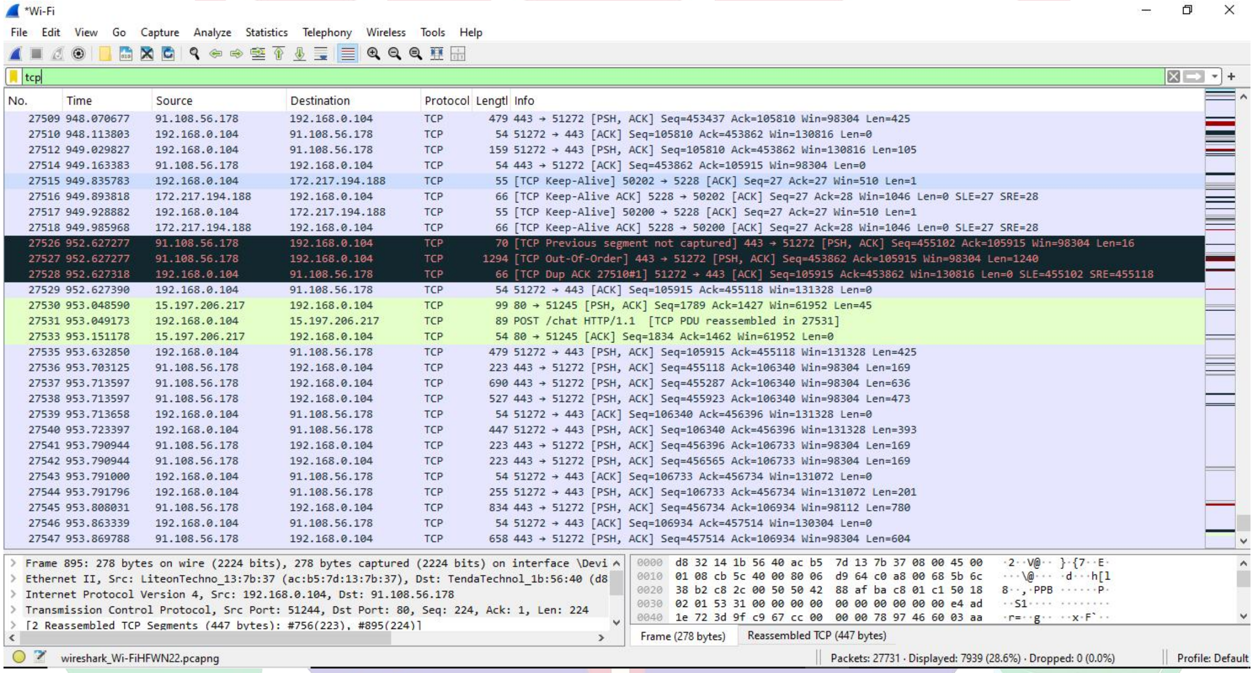
Computer: A computer running Windows, Mac, or Linux/Unix.

Internet Connection: To generate network traffic and capture packets.

Web Browser: To generate HTTP traffic.

Procedure:

1. Which of the following protocols are shown as appearing (i.e., are listed in the Wireshark “protocol” column) in your trace file: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?



tcp

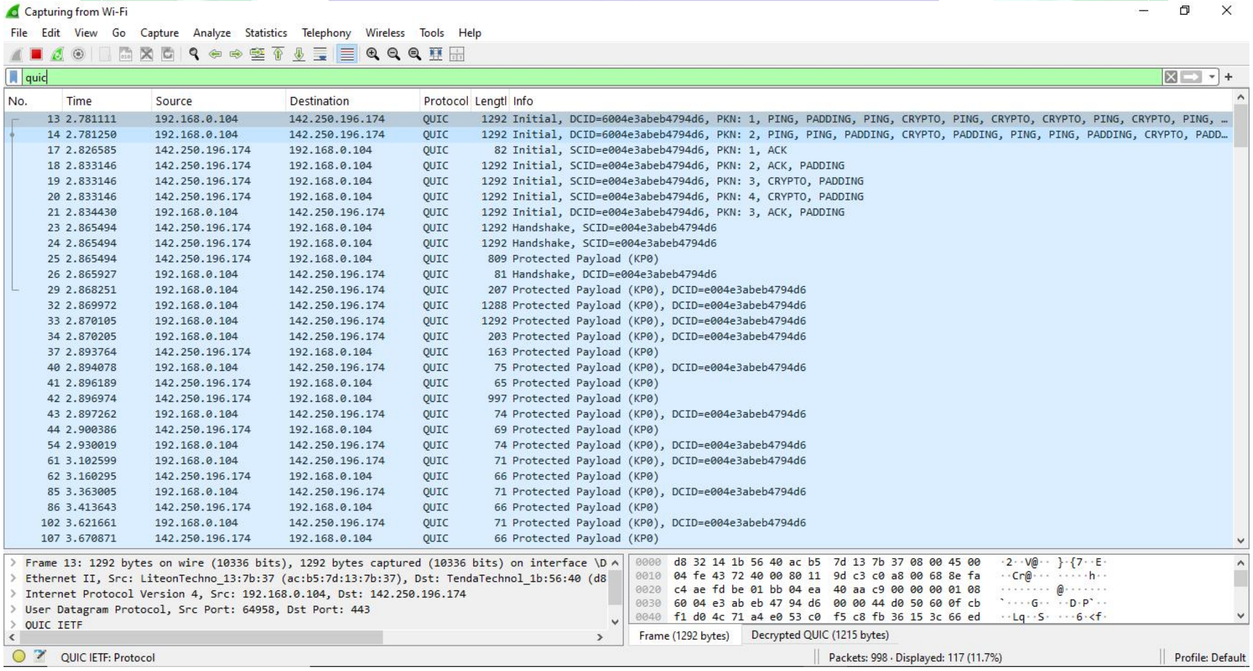
```
No.   Time       Source          Destination     Protocol Lengtl Info
27509 948.070677 91.108.56.178   192.168.0.104   TCP       479 443 → 51272 [PSH, ACK] Seq=453437 Ack=105810 Win=98304 Len=425
27510 948.113803 192.168.0.104   91.108.56.178   TCP        54 51272 → 443 [ACK] Seq=105810 Ack=453862 Win=130816 Len=0
27512 949.029827 192.168.0.104   91.108.56.178   TCP       159 51272 → 443 [PSH, ACK] Seq=105810 Ack=453862 Win=130816 Len=105
27514 949.163383 91.108.56.178   192.168.0.104   TCP        54 443 → 51272 [ACK] Seq=453862 Ack=105915 Win=98304 Len=0
27515 949.835783 192.168.0.104   172.217.194.188 TCP        55 [TCP Keep-Alive] 50202 → 5228 [ACK] Seq=27 Ack=27 Win=510 Len=1
27516 949.893818 172.217.194.188 192.168.0.104   TCP        66 [TCP Keep-Alive ACK] 5228 → 50202 [ACK] Seq=27 Ack=28 Win=1046 Len=0 SLE=27 SRE=28
27517 949.928882 192.168.0.104   172.217.194.188 TCP        55 [TCP Keep-Alive] 50200 → 5228 [ACK] Seq=27 Ack=27 Win=510 Len=1
27518 949.985968 172.217.194.188 192.168.0.104   TCP        66 [TCP Keep-Alive ACK] 5228 → 50200 [ACK] Seq=27 Ack=28 Win=1046 Len=0 SLE=27 SRE=28
27526 952.627277 91.108.56.178   192.168.0.104   TCP        70 [TCP Previous segment not captured] 443 → 51272 [PSH, ACK] Seq=455102 Ack=105915 Win=98304 Len=16
27527 952.627277 91.108.56.178   192.168.0.104   TCP      1294 [TCP Out-Of-Order] 443 → 51272 [PSH, ACK] Seq=453862 Ack=105915 Win=98304 Len=1240
27528 952.627318 192.168.0.104   91.108.56.178   TCP        66 [TCP Dup ACK 27510#1] 51272 → 443 [ACK] Seq=105915 Ack=453862 Win=130816 Len=0 SLE=455102 SRE=455118
27529 952.627390 192.168.0.104   91.108.56.178   TCP        54 51272 → 443 [ACK] Seq=105915 Ack=455118 Win=131328 Len=0
27530 953.048590 15.197.206.217  192.168.0.104   TCP        99 80 → 51245 [PSH, ACK] Seq=1789 Ack=1427 Win=61952 Len=45
27531 953.049173 192.168.0.104   15.197.206.217  TCP        89 POST /chat HTTP/1.1  [TCP PDU reassembled in 27531]
27533 953.151178 15.197.206.217  192.168.0.104   TCP        54 80 → 51245 [ACK] Seq=1834 Ack=1462 Win=61952 Len=0
27535 953.632850 192.168.0.104   91.108.56.178   TCP       479 51272 → 443 [PSH, ACK] Seq=105915 Ack=455118 Win=131328 Len=425
27536 953.703125 91.108.56.178   192.168.0.104   TCP       223 443 → 51272 [PSH, ACK] Seq=455118 Ack=106340 Win=98304 Len=169
27537 953.713597 91.108.56.178   192.168.0.104   TCP       690 443 → 51272 [PSH, ACK] Seq=455287 Ack=106340 Win=98304 Len=636
27538 953.713597 91.108.56.178   192.168.0.104   TCP       527 443 → 51272 [PSH, ACK] Seq=455923 Ack=106340 Win=98304 Len=473
27539 953.713658 192.168.0.104   91.108.56.178   TCP        54 51272 → 443 [ACK] Seq=106340 Ack=456396 Win=131328 Len=0
27540 953.723397 192.168.0.104   91.108.56.178   TCP       447 51272 → 443 [PSH, ACK] Seq=106340 Ack=456396 Win=131328 Len=393
27541 953.790944 91.108.56.178   192.168.0.104   TCP       223 443 → 51272 [PSH, ACK] Seq=456396 Ack=106733 Win=98304 Len=169
27542 953.790944 91.108.56.178   192.168.0.104   TCP       223 443 → 51272 [PSH, ACK] Seq=456565 Ack=106733 Win=98304 Len=169
27543 953.791000 192.168.0.104   91.108.56.178   TCP        54 51272 → 443 [ACK] Seq=106733 Ack=456734 Win=131072 Len=0
27544 953.791796 192.168.0.104   91.108.56.178   TCP       255 51272 → 443 [PSH, ACK] Seq=106733 Ack=456734 Win=131072 Len=201
27545 953.808031 91.108.56.178   192.168.0.104   TCP       834 443 → 51272 [PSH, ACK] Seq=456734 Ack=106934 Win=98112 Len=780
27546 953.863339 192.168.0.104   91.108.56.178   TCP        54 51272 → 443 [ACK] Seq=106934 Ack=457514 Win=130304 Len=0
27547 953.869788 91.108.56.178   192.168.0.104   TCP       658 443 → 51272 [PSH, ACK] Seq=457514 Ack=106934 Win=98304 Len=604
```

```
> Frame 895: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface \Devi
> Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: TendaTechnol_1b:56:40 (d8
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 91.108.56.178
> Transmission Control Protocol, Src Port: 51244, Dst Port: 80, Seq: 224, Ack: 1, Len: 224
> [2 Reassembled TCP Segments (447 bytes): #756(223), #895(224)]
```

```
0000  d8 32 14 1b 56 40 ac b5  7d 13 7b 37 08 00 45 00   ·2··V@·· }·{7··E·
0010  01 08 cb 5c 40 00 80 06  d9 64 c0 a8 00 68 5b 6c   ···\@··· ·d···h[l
0020  38 b2 c8 2c 00 50 50 42  88 af ba c8 01 c1 50 18   8··,·PPB ······P·
0030  02 01 53 31 00 00 00 00  00 00 00 00 00 00 e4 ad   ··S1···· ········
0040  1e 72 3d 9f c9 67 cc 00  00 00 78 97 46 60 03 aa   ·r=··g·· ··x·F`··
```

Frame (278 bytes) | Reassembled TCP (447 bytes)

wireshark_Wi-FiHFWN22.pcapng | Packets: 27731 · Displayed: 7939 (28.6%) · Dropped: 0 (0.0%) | Profile: Default



quic

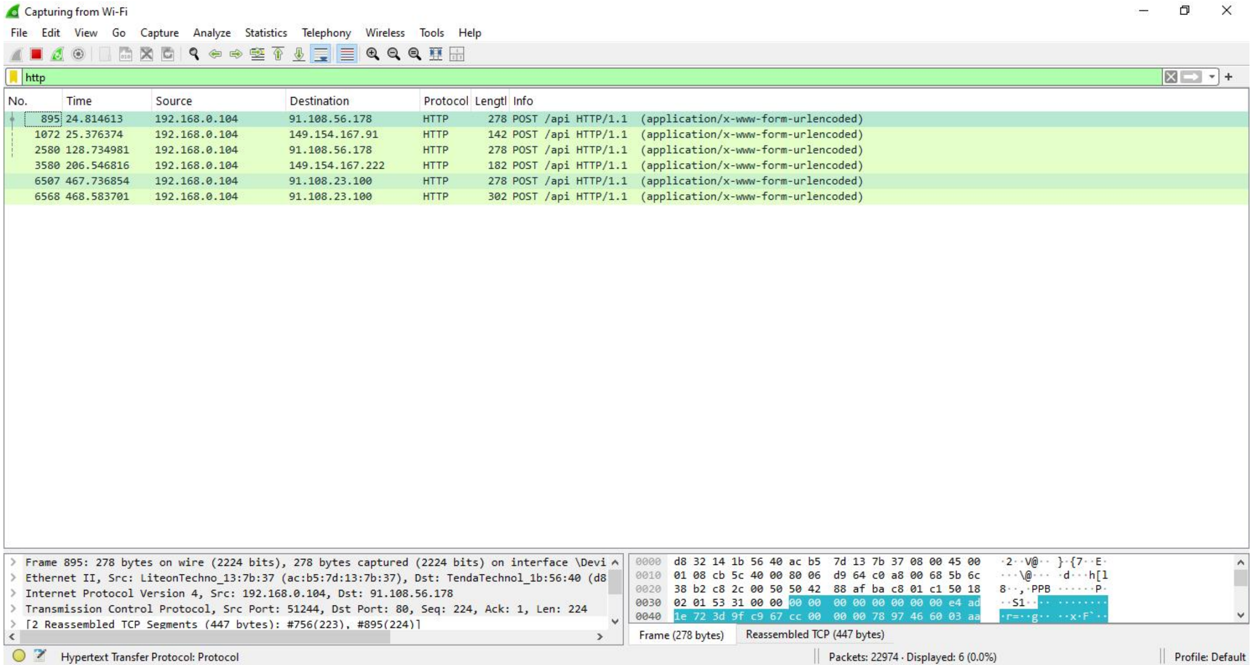
```
No.  Time     Source          Destination     Protocol Lengtl Info
 13 2.781111 192.168.0.104   142.250.196.174 QUIC     1292 Initial, DCID=6004e3abeb4794d6, PKN: 1, PING, PADDING, PING, CRYPTO, PING, CRYPTO, CRYPTO, PING, CRYPTO, PING, …
 14 2.781250 192.168.0.104   142.250.196.174 QUIC     1292 Initial, DCID=6004e3abeb4794d6, PKN: 2, PING, PING, PADDING, CRYPTO, PADDING, PING, PING, PADDING, CRYPTO, PADD…
 17 2.826585 142.250.196.174 192.168.0.104   QUIC       82 Initial, SCID=e004e3abeb4794d6, PKN: 1, ACK
 18 2.833146 142.250.196.174 192.168.0.104   QUIC     1292 Initial, SCID=e004e3abeb4794d6, PKN: 2, ACK, PADDING
 19 2.833146 142.250.196.174 192.168.0.104   QUIC     1292 Initial, SCID=e004e3abeb4794d6, PKN: 3, CRYPTO, PADDING
 20 2.833146 142.250.196.174 192.168.0.104   QUIC     1292 Initial, SCID=e004e3abeb4794d6, PKN: 4, CRYPTO, PADDING
 21 2.834430 192.168.0.104   142.250.196.174 QUIC     1292 Initial, DCID=e004e3abeb4794d6, PKN: 3, ACK, PADDING
 23 2.865494 142.250.196.174 192.168.0.104   QUIC     1292 Handshake, SCID=e004e3abeb4794d6
 24 2.865494 142.250.196.174 192.168.0.104   QUIC     1292 Handshake, SCID=e004e3abeb4794d6
 25 2.865494 142.250.196.174 192.168.0.104   QUIC      809 Protected Payload (KP0)
 26 2.865927 192.168.0.104   142.250.196.174 QUIC       81 Handshake, DCID=e004e3abeb4794d6
 29 2.868251 192.168.0.104   142.250.196.174 QUIC      207 Protected Payload (KP0), DCID=e004e3abeb4794d6
 32 2.869972 192.168.0.104   142.250.196.174 QUIC     1288 Protected Payload (KP0), DCID=e004e3abeb4794d6
 33 2.870105 192.168.0.104   142.250.196.174 QUIC     1292 Protected Payload (KP0), DCID=e004e3abeb4794d6
 34 2.870205 192.168.0.104   142.250.196.174 QUIC      203 Protected Payload (KP0), DCID=e004e3abeb4794d6
 37 2.893764 142.250.196.174 192.168.0.104   QUIC      163 Protected Payload (KP0)
 40 2.894078 192.168.0.104   142.250.196.174 QUIC       75 Protected Payload (KP0), DCID=e004e3abeb4794d6
 41 2.896189 142.250.196.174 192.168.0.104   QUIC       65 Protected Payload (KP0)
 42 2.896974 142.250.196.174 192.168.0.104   QUIC      997 Protected Payload (KP0)
 43 2.897262 192.168.0.104   142.250.196.174 QUIC       74 Protected Payload (KP0), DCID=e004e3abeb4794d6
 44 2.900386 142.250.196.174 192.168.0.104   QUIC       69 Protected Payload (KP0)
 54 2.930019 192.168.0.104   142.250.196.174 QUIC       74 Protected Payload (KP0), DCID=e004e3abeb4794d6
 61 3.102599 192.168.0.104   142.250.196.174 QUIC       71 Protected Payload (KP0), DCID=e004e3abeb4794d6
 62 3.160295 142.250.196.174 192.168.0.104   QUIC       66 Protected Payload (KP0)
 85 3.363005 192.168.0.104   142.250.196.174 QUIC       71 Protected Payload (KP0), DCID=e004e3abeb4794d6
 86 3.413643 142.250.196.174 192.168.0.104   QUIC       66 Protected Payload (KP0)
102 3.621661 192.168.0.104   142.250.196.174 QUIC       71 Protected Payload (KP0), DCID=e004e3abeb4794d6
107 3.670871 142.250.196.174 192.168.0.104   QUIC       66 Protected Payload (KP0)
```

```
> Frame 13: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \D
> Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: TendaTechnol_1b:56:40 (d8
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 142.250.196.174
> User Datagram Protocol, Src Port: 64958, Dst Port: 443
> QUIC IETF
```

```
0000  d8 32 14 1b 56 40 ac b5  7d 13 7b 37 08 00 45 00   ·2··V@·· }·{7··E·
0010  04 fe 43 72 40 00 80 11  9d c3 c0 a8 00 68 8e fa   ··Cr@··· ·····h··
0020  c4 ae fd be 01 bb 04 ea  40 aa c9 00 00 00 01 08   ········ @·······
0030  60 04 e3 ab eb 47 94 d6  00 00 44 d0 50 60 0f cb   `····G·· ··D·P`··
0040  f1 d0 4c 71 a4 e0 53 c0  f5 c8 fb 36 15 3c 66 ed   ··Lq··S· ···6·<f·
```

Frame (1292 bytes) | Decrypted QUIC (1215 bytes)

QUIC IETF: Protocol | Packets: 998 · Displayed: 117 (11.7%) | Profile: Default


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

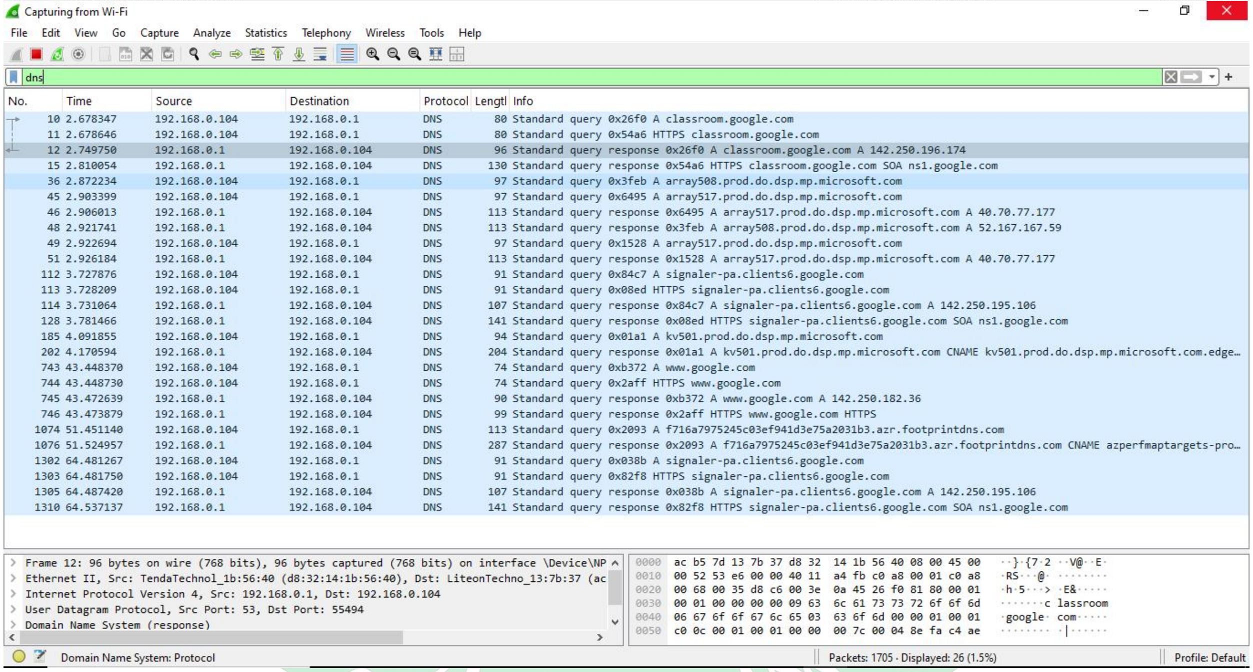
```
http
```

```
No.   Time        Source         Destination      Protocol Lengtl Info
  895 24.814613   192.168.0.104  91.108.56.178    HTTP      278 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
 1072 25.376374   192.168.0.104  149.154.167.91   HTTP      142 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
 2580 128.734981  192.168.0.104  91.108.56.178    HTTP      278 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
 3580 206.546816  192.168.0.104  149.154.167.222  HTTP      182 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
 6507 467.736854  192.168.0.104  91.108.23.100    HTTP      278 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
 6568 468.583701  192.168.0.104  91.108.23.100    HTTP      302 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
```

```
> Frame 895: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface \Devi
> Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: TendaTechnol_1b:56:40 (d8
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 91.108.56.178
> Transmission Control Protocol, Src Port: 51244, Dst Port: 80, Seq: 224, Ack: 1, Len: 224
> [2 Reassembled TCP Segments (447 bytes): #756(223), #895(224)]
```

```
0000  d8 32 14 1b 56 40 ac b5  7d 13 7b 37 08 00 45 00   ·2··V@·· }·{7··E·
0010  01 08 cb 5c 40 00 80 06  d9 64 c0 a8 00 68 5b 6c   ···\@··· ·d···h[l
0020  38 b2 c8 2c 00 50 50 42  88 af ba c8 01 c1 50 18   8··,·PPB ······P·
0030  02 01 53 31 00 00 00 00  00 00 00 00 00 00 e4 ad   ··S1···· ········
0040  1e 72 3d 9f c9 67 cc 00  00 00 78 97 46 60 03 aa   ·r=··g·· ··x·F`··
```

Hypertext Transfer Protocol: Protocol | Packets: 22974 · Displayed: 6 (0.0%) | Profile: Default


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

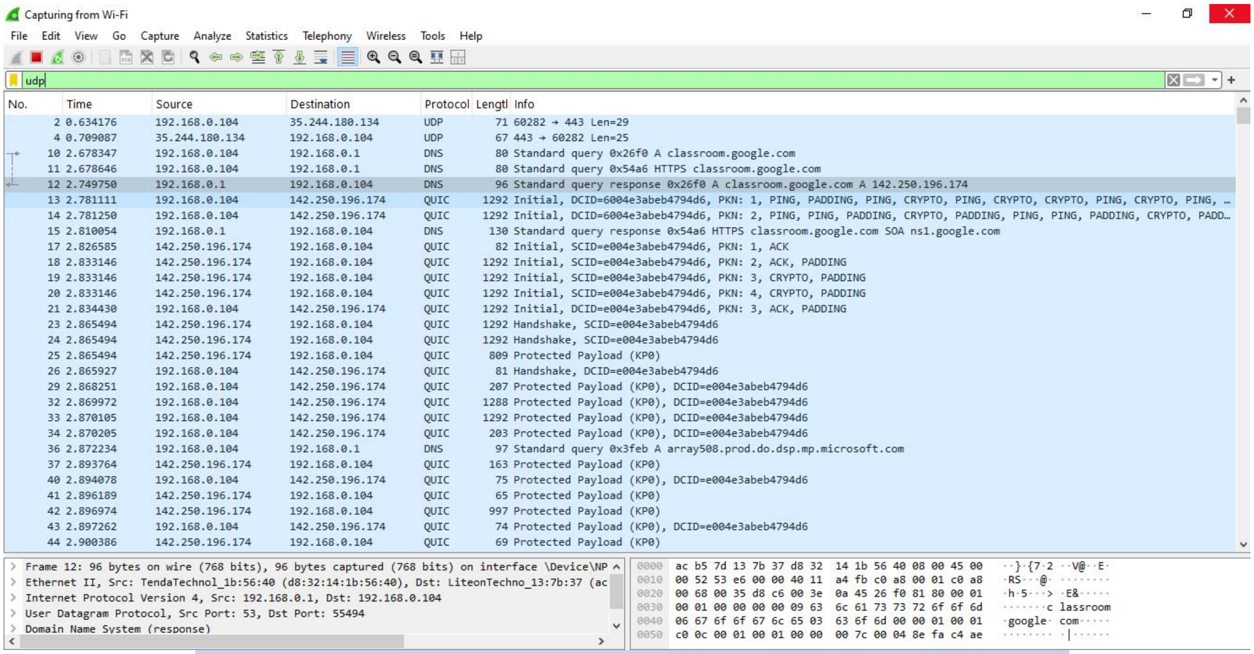
```
dns
```

```
No.   Time        Source         Destination    Protocol Lengtl Info
   10 2.678347    192.168.0.104  192.168.0.1    DNS        80 Standard query 0x26f0 A classroom.google.com
   11 2.678646    192.168.0.104  192.168.0.1    DNS        80 Standard query 0x54a6 HTTPS classroom.google.com
   12 2.749750    192.168.0.1    192.168.0.104  DNS        96 Standard query response 0x26f0 A classroom.google.com A 142.250.196.174
   15 2.810054    192.168.0.1    192.168.0.104  DNS       130 Standard query response 0x54a6 HTTPS classroom.google.com SOA ns1.google.com
   36 2.872234    192.168.0.104  192.168.0.1    DNS        97 Standard query 0x3feb A array508.prod.do.dsp.mp.microsoft.com
   45 2.903399    192.168.0.104  192.168.0.1    DNS        97 Standard query 0x6495 A array517.prod.do.dsp.mp.microsoft.com
   46 2.906013    192.168.0.1    192.168.0.104  DNS       113 Standard query response 0x6495 A array517.prod.do.dsp.mp.microsoft.com A 40.70.77.177
   48 2.921741    192.168.0.1    192.168.0.104  DNS       113 Standard query response 0x3feb A array508.prod.do.dsp.mp.microsoft.com A 52.167.167.59
   49 2.922694    192.168.0.104  192.168.0.1    DNS        97 Standard query 0x1528 A array517.prod.do.dsp.mp.microsoft.com
   51 2.926184    192.168.0.1    192.168.0.104  DNS       113 Standard query response 0x1528 A array517.prod.do.dsp.mp.microsoft.com A 40.70.77.177
  112 3.727876    192.168.0.104  192.168.0.1    DNS        91 Standard query 0x84c7 A signaler-pa.clients6.google.com
  113 3.728209    192.168.0.104  192.168.0.1    DNS        91 Standard query 0x08ed HTTPS signaler-pa.clients6.google.com
  114 3.731064    192.168.0.1    192.168.0.104  DNS       107 Standard query response 0x84c7 A signaler-pa.clients6.google.com A 142.250.195.106
  128 3.781466    192.168.0.1    192.168.0.104  DNS       141 Standard query response 0x08ed HTTPS signaler-pa.clients6.google.com SOA ns1.google.com
  185 4.091855    192.168.0.104  192.168.0.1    DNS        94 Standard query 0x01a1 A kv501.prod.do.dsp.mp.microsoft.com
  202 4.170594    192.168.0.1    192.168.0.104  DNS       204 Standard query response 0x01a1 A kv501.prod.do.dsp.mp.microsoft.com CNAME kv501.prod.do.dsp.mp.microsoft.com.edge…
  743 43.448370   192.168.0.104  192.168.0.1    DNS        74 Standard query 0xb372 A www.google.com
  744 43.448730   192.168.0.104  192.168.0.1    DNS        74 Standard query 0x2aff HTTPS www.google.com
  745 43.472639   192.168.0.1    192.168.0.104  DNS        90 Standard query response 0xb372 A www.google.com A 142.250.182.36
  746 43.473879   192.168.0.1    192.168.0.104  DNS        99 Standard query response 0x2aff HTTPS www.google.com HTTPS
 1074 51.451140   192.168.0.104  192.168.0.1    DNS       113 Standard query 0x2093 A f716a7975245c03ef941d3e75a2031b3.azr.footprintdns.com
 1076 51.524957   192.168.0.1    192.168.0.104  DNS       287 Standard query response 0x2093 A f716a7975245c03ef941d3e75a2031b3.azr.footprintdns.com CNAME azperfmaptargets-pro…
 1302 64.481267   192.168.0.104  192.168.0.1    DNS        91 Standard query 0x038b A signaler-pa.clients6.google.com
 1303 64.481750   192.168.0.104  192.168.0.1    DNS        91 Standard query 0x82f8 HTTPS signaler-pa.clients6.google.com
 1305 64.487420   192.168.0.1    192.168.0.104  DNS       107 Standard query response 0x038b A signaler-pa.clients6.google.com A 142.250.195.106
 1310 64.537137   192.168.0.1    192.168.0.104  DNS       141 Standard query response 0x82f8 HTTPS signaler-pa.clients6.google.com SOA ns1.google.com
```

```
> Frame 12: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface \Device\NP
> Ethernet II, Src: TendaTechnol_1b:56:40 (d8:32:14:1b:56:40), Dst: LiteonTechno_13:7b:37 (ac
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104
> User Datagram Protocol, Src Port: 53, Dst Port: 55494
> Domain Name System (response)
```

```
0000  ac b5 7d 13 7b 37 d8 32  14 1b 56 40 08 00 45 00   ··}·{7·2 ··V@··E·
0010  00 52 53 e6 00 00 40 11  a4 fb c0 a8 00 01 c0 a8   ·RS···@· ········
0020  00 68 00 35 d8 c6 00 3e  0a 45 26 f0 81 80 00 01   ·h·5···> ·E&·····
0030  00 01 00 00 00 00 09 63  6c 61 73 73 72 6f 6f 6d   ·······c lassroom
0040  06 67 6f 6f 67 6c 65 03  63 6f 6d 00 00 01 00 01   ·google· com·····
0050  c0 0c 00 01 00 01 00 00  00 7c 00 04 8e fa c4 ae   ········ ·|······
```

Domain Name System: Protocol | Packets: 1705 · Displayed: 26 (1.5%) | Profile: Default

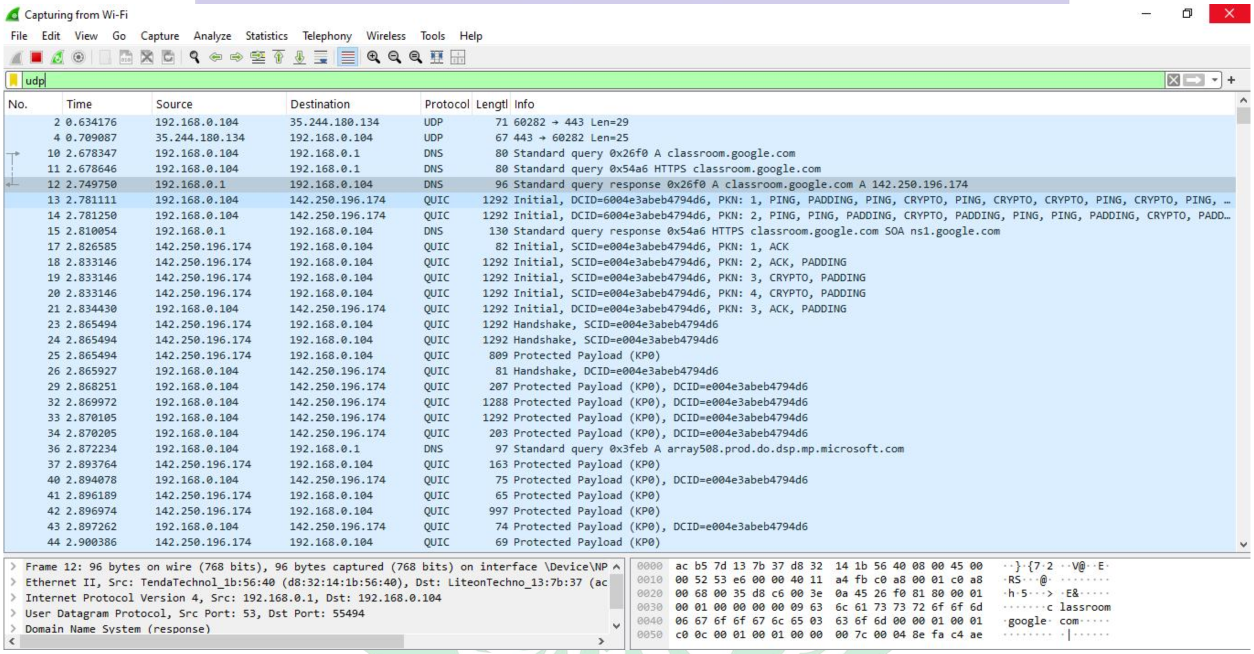

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

```
No.  Time      Source          Destination     Protocol Lengtl Info
   2 0.634176  192.168.0.104   35.244.180.134  UDP        71 60282 → 443 Len=29
   4 0.709087  35.244.180.134  192.168.0.104   UDP        67 443 → 60282 Len=25
  10 2.678347  192.168.0.104   192.168.0.1     DNS        80 Standard query 0x26f0 A classroom.google.com
  11 2.678646  192.168.0.104   192.168.0.1     DNS        80 Standard query 0x54a6 HTTPS classroom.google.com
  12 2.749750  192.168.0.1     192.168.0.104   DNS        96 Standard query response 0x26f0 A classroom.google.com A 142.250.196.174
  13 2.781111  192.168.0.104   142.250.196.174 QUIC     1292 Initial, DCID=6004e3abeb4794d6, PKN: 1, PING, PADDING, PING, CRYPTO, PING, CRYPTO, CRYPTO, PING, CRYPTO, PING, …
  14 2.781250  192.168.0.104   142.250.196.174 QUIC     1292 Initial, DCID=6004e3abeb4794d6, PKN: 2, PING, PING, PADDING, CRYPTO, PADDING, PING, PING, PADDING, CRYPTO, PADD…
  15 2.810054  192.168.0.1     192.168.0.104   DNS       130 Standard query response 0x54a6 HTTPS classroom.google.com SOA ns1.google.com
  17 2.826585  142.250.196.174 192.168.0.104   QUIC       82 Initial, SCID=e004e3abeb4794d6, PKN: 1, ACK
  18 2.833146  142.250.196.174 192.168.0.104   QUIC     1292 Initial, SCID=e004e3abeb4794d6, PKN: 2, ACK, PADDING
  19 2.833146  142.250.196.174 192.168.0.104   QUIC     1292 Initial, SCID=e004e3abeb4794d6, PKN: 3, CRYPTO, PADDING
  20 2.833146  142.250.196.174 192.168.0.104   QUIC     1292 Initial, SCID=e004e3abeb4794d6, PKN: 4, CRYPTO, PADDING
  21 2.834430  192.168.0.104   142.250.196.174 QUIC     1292 Initial, DCID=e004e3abeb4794d6, PKN: 3, ACK, PADDING
  23 2.865494  142.250.196.174 192.168.0.104   QUIC     1292 Handshake, SCID=e004e3abeb4794d6
  24 2.865494  142.250.196.174 192.168.0.104   QUIC     1292 Handshake, SCID=e004e3abeb4794d6
  25 2.865494  142.250.196.174 192.168.0.104   QUIC      809 Protected Payload (KP0)
  26 2.865927  192.168.0.104   142.250.196.174 QUIC       81 Handshake, DCID=e004e3abeb4794d6
  29 2.868251  192.168.0.104   142.250.196.174 QUIC      207 Protected Payload (KP0), DCID=e004e3abeb4794d6
  32 2.869972  192.168.0.104   142.250.196.174 QUIC     1288 Protected Payload (KP0), DCID=e004e3abeb4794d6
  33 2.870105  192.168.0.104   142.250.196.174 QUIC     1292 Protected Payload (KP0), DCID=e004e3abeb4794d6
  34 2.870205  192.168.0.104   142.250.196.174 QUIC      203 Protected Payload (KP0), DCID=e004e3abeb4794d6
  36 2.872234  192.168.0.104   192.168.0.1     DNS        97 Standard query 0x3feb A array508.prod.do.dsp.mp.microsoft.com
  37 2.893764  142.250.196.174 192.168.0.104   QUIC      163 Protected Payload (KP0)
  40 2.894078  192.168.0.104   142.250.196.174 QUIC       75 Protected Payload (KP0), DCID=e004e3abeb4794d6
  41 2.896189  142.250.196.174 192.168.0.104   QUIC       65 Protected Payload (KP0)
  42 2.896974  142.250.196.174 192.168.0.104   QUIC      997 Protected Payload (KP0)
  43 2.897262  192.168.0.104   142.250.196.174 QUIC       74 Protected Payload (KP0), DCID=e004e3abeb4794d6
  44 2.900386  142.250.196.174 192.168.0.104   QUIC       69 Protected Payload (KP0)
```

```
> Frame 12: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface \Device\NP
> Ethernet II, Src: TendaTechnol_1b:56:40 (d8:32:14:1b:56:40), Dst: LiteonTechno_13:7b:37 (ac
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104
> User Datagram Protocol, Src Port: 53, Dst Port: 55494
> Domain Name System (response)
```

```
0000  ac b5 7d 13 7b 37 d8 32  14 1b 56 40 08 00 45 00   ··}·{7·2 ··V@··E·
0010  00 52 53 e6 00 00 40 11  a4 fb c0 a8 00 01 c0 a8   ·RS···@· ········
0020  00 68 00 35 d8 c6 00 3e  0a 45 26 f0 81 80 00 01   ·h·5···> ·E&·····
0030  00 01 00 00 00 00 09 63  6c 61 73 73 72 6f 6f 6d   ·······c lassroom
0040  06 67 6f 6f 67 6c 65 03  63 6f 6d 00 00 01 00 01   ·google· com·····
0050  c0 0c 00 01 00 01 00 00  00 7c 00 04 8e fa c4 ae   ········ ·|······
```


Capturing from Wi-Fi

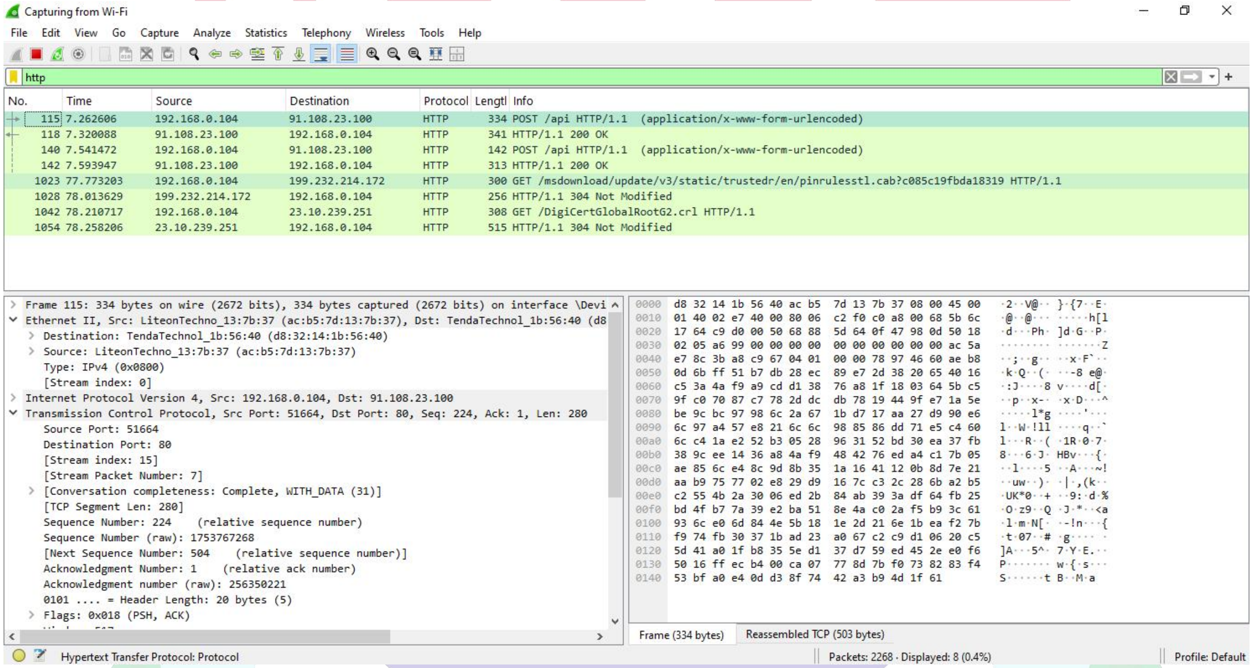
udp

```
No.  Time      Source          Destination     Protocol Lengtl Info
   2 0.634176  192.168.0.104   35.244.180.134  UDP        71 60282 → 443 Len=29
   4 0.709087  35.244.180.134  192.168.0.104   UDP        67 443 → 60282 Len=25
  10 2.678347  192.168.0.104   192.168.0.1     DNS        80 Standard query 0x26f0 A classroom.google.com
  11 2.678646  192.168.0.104   192.168.0.1     DNS        80 Standard query 0x54a6 HTTPS classroom.google.com
  12 2.749750  192.168.0.1     192.168.0.104   DNS        96 Standard query response 0x26f0 A classroom.google.com A 142.250.196.174
  13 2.781111  192.168.0.104   142.250.196.174 QUIC     1292 Initial, DCID=6004e3abeb4794d6, PKN: 1, PING, PADDING, PING, CRYPTO, PING, CRYPTO, CRYPTO, PING, CRYPTO, PING, …
  14 2.781250  192.168.0.104   142.250.196.174 QUIC     1292 Initial, DCID=6004e3abeb4794d6, PKN: 2, PING, PING, PADDING, CRYPTO, PADDING, PING, PING, PADDING, CRYPTO, PADD…
  15 2.810054  192.168.0.1     192.168.0.104   DNS       130 Standard query response 0x54a6 HTTPS classroom.google.com SOA ns1.google.com
  17 2.826585  142.250.196.174 192.168.0.104   QUIC       82 Initial, SCID=e004e3abeb4794d6, PKN: 1, ACK
  18 2.833146  142.250.196.174 192.168.0.104   QUIC     1292 Initial, SCID=e004e3abeb4794d6, PKN: 2, ACK, PADDING
  19 2.833146  142.250.196.174 192.168.0.104   QUIC     1292 Initial, SCID=e004e3abeb4794d6, PKN: 3, CRYPTO, PADDING
  20 2.833146  142.250.196.174 192.168.0.104   QUIC     1292 Initial, SCID=e004e3abeb4794d6, PKN: 4, CRYPTO, PADDING
  21 2.834430  192.168.0.104   142.250.196.174 QUIC     1292 Initial, DCID=e004e3abeb4794d6, PKN: 3, ACK, PADDING
  23 2.865494  142.250.196.174 192.168.0.104   QUIC     1292 Handshake, SCID=e004e3abeb4794d6
  24 2.865494  142.250.196.174 192.168.0.104   QUIC     1292 Handshake, SCID=e004e3abeb4794d6
  25 2.865494  142.250.196.174 192.168.0.104   QUIC      809 Protected Payload (KP0)
  26 2.865927  192.168.0.104   142.250.196.174 QUIC       81 Handshake, DCID=e004e3abeb4794d6
  29 2.868251  192.168.0.104   142.250.196.174 QUIC      207 Protected Payload (KP0), DCID=e004e3abeb4794d6
  32 2.869972  192.168.0.104   142.250.196.174 QUIC     1288 Protected Payload (KP0), DCID=e004e3abeb4794d6
  33 2.870105  192.168.0.104   142.250.196.174 QUIC     1292 Protected Payload (KP0), DCID=e004e3abeb4794d6
  34 2.870205  192.168.0.104   142.250.196.174 QUIC      203 Protected Payload (KP0), DCID=e004e3abeb4794d6
  36 2.872234  192.168.0.104   192.168.0.1     DNS        97 Standard query 0x3feb A array508.prod.do.dsp.mp.microsoft.com
  37 2.893764  142.250.196.174 192.168.0.104   QUIC      163 Protected Payload (KP0)
  40 2.894078  192.168.0.104   142.250.196.174 QUIC       75 Protected Payload (KP0), DCID=e004e3abeb4794d6
  41 2.896189  142.250.196.174 192.168.0.104   QUIC       65 Protected Payload (KP0)
  42 2.896974  142.250.196.174 192.168.0.104   QUIC      997 Protected Payload (KP0)
  43 2.897262  192.168.0.104   142.250.196.174 QUIC       74 Protected Payload (KP0), DCID=e004e3abeb4794d6
  44 2.900386  142.250.196.174 192.168.0.104   QUIC       69 Protected Payload (KP0)
```

```
> Frame 12: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface \Device\NP
> Ethernet II, Src: TendaTechnol_1b:56:40 (d8:32:14:1b:56:40), Dst: LiteonTechno_13:7b:37 (ac
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104
> User Datagram Protocol, Src Port: 53, Dst Port: 55494
> Domain Name System (response)
```

```
0000  ac b5 7d 13 7b 37 d8 32  14 1b 56 40 08 00 45 00   ··}·{7·2 ··V@··E·
0010  00 52 53 e6 00 00 40 11  a4 fb c0 a8 00 01 c0 a8   ·RS···@· ········
0020  00 68 00 35 d8 c6 00 3e  0a 45 26 f0 81 80 00 01   ·h·5···> ·E&·····
0030  00 01 00 00 00 00 09 63  6c 61 73 73 72 6f 6f 6d   ·······c lassroom
0040  06 67 6f 6f 67 6c 65 03  63 6f 6d 00 00 01 00 01   ·google· com·····
0050  c0 0c 00 01 00 01 00 00  00 7c 00 04 8e fa c4 ae   ········ ·|······
```

2. How long did it take from when the HTTP GET message was sent until the HTTPOK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began.(If you want to display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)



http

```
No.   Time       Source           Destination      Protocol Lengtl Info
  115 7.262606   192.168.0.104    91.108.23.100    HTTP     334 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
  118 7.320088   91.108.23.100    192.168.0.104    HTTP     341 HTTP/1.1 200 OK
  140 7.541472   192.168.0.104    91.108.23.100    HTTP     142 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
  142 7.593947   91.108.23.100    192.168.0.104    HTTP     313 HTTP/1.1 200 OK
 1023 77.773203  192.168.0.104    199.232.214.172  HTTP     300 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?c085c19fbda18319 HTTP/1.1
 1028 78.013629  199.232.214.172  192.168.0.104    HTTP     256 HTTP/1.1 304 Not Modified
 1042 78.210717  192.168.0.104    23.10.239.251    HTTP     308 GET /DigiCertGlobalRootG2.crl HTTP/1.1
 1054 78.258206  23.10.239.251    192.168.0.104    HTTP     515 HTTP/1.1 304 Not Modified
```

```
> Frame 115: 334 bytes on wire (2672 bits), 334 bytes captured (2672 bits) on interface \Devi
v Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: TendaTechnol_1b:56:40 (d8
  > Destination: TendaTechnol_1b:56:40 (d8:32:14:1b:56:40)
  > Source: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 91.108.23.100
v Transmission Control Protocol, Src Port: 51664, Dst Port: 80, Seq: 224, Ack: 1, Len: 280
    Source Port: 51664
    Destination Port: 80
    [Stream index: 15]
    [Stream Packet Number: 7]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 280]
    Sequence Number: 224    (relative sequence number)
    Sequence Number (raw): 1753767268
    [Next Sequence Number: 504    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 256350221
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
```

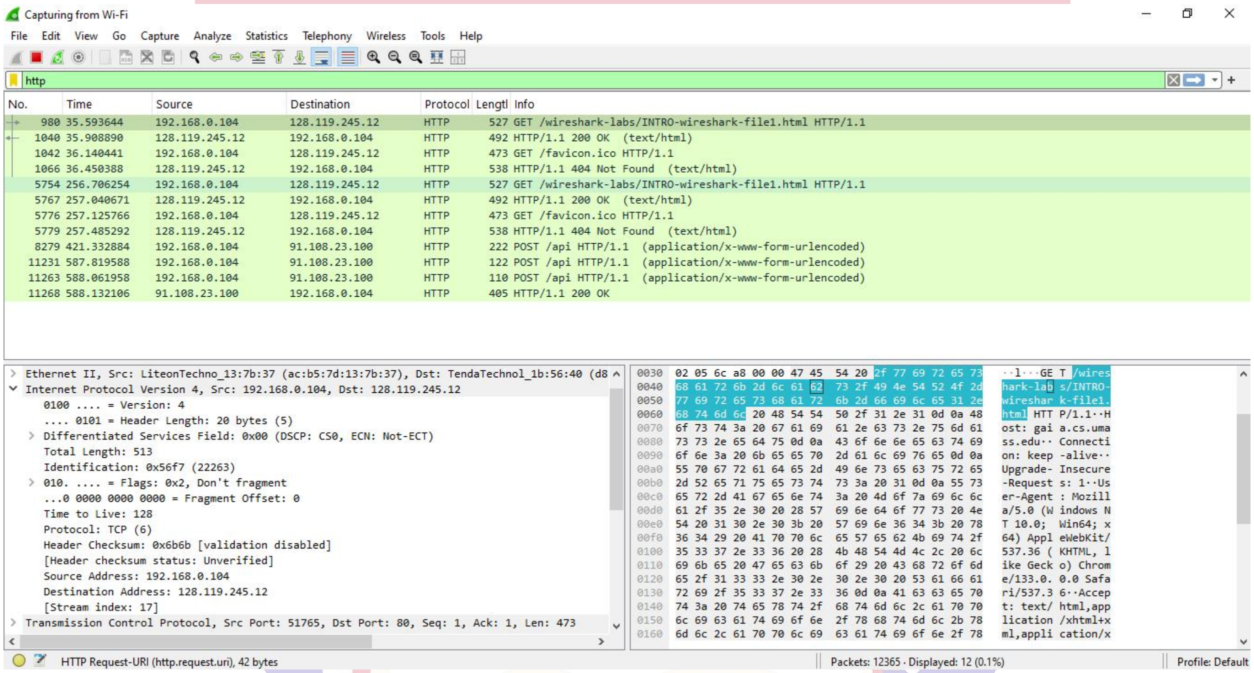
```
0000  d8 32 14 1b 56 40 ac b5  7d 13 7b 37 08 00 45 00   ·2··V@·· }·{7··E·
0010  01 40 02 e7 40 00 80 06  c2 f0 c0 a8 00 68 5b 6c   ·@··@··· ·····h[l
0020  17 64 c9 d0 00 50 68 88  5d 64 0f 47 98 0d 50 18   ·d···Ph· ]d·G··P·
0030  02 05 a6 99 00 00 00 00  00 00 00 00 00 00 ac 5a   ········ ·······Z
0040  e7 8c 3b a8 c9 67 04 01  00 00 78 97 46 60 ae b8   ··;··g·· ··x·F`··
0050  0d 6b ff 51 b7 db 28 ec  89 e7 2d 38 20 65 40 16   ·k·Q··(· ··-8 e@·
0060  c5 3a 4a f9 a9 cd d1 38  76 a8 1f 18 03 64 5b c5   ·:J····8 v····d[·
0070  9f c0 70 87 c7 78 2d dc  db 78 19 44 9f e7 1a 5e   ··p··x-· ·x·D···^
0080  be 9c bc 97 98 6c 2a 67  1b d7 17 aa 27 d9 90 e6   ·····l*g ····'···
0090  6c 97 a4 57 e8 21 6c 6c  98 85 86 dd 71 e5 c4 60   l··W·!ll ····q··`
00a0  6c c4 1a e2 52 b3 05 28  96 31 52 bd 30 ea 37 fb   l···R··( ·1R·0·7·
00b0  38 9c ee 14 36 a8 4a f9  48 42 76 ed a4 c1 7b 05   8···6·J· HBv···{·
00c0  ae 85 6c e4 8c 9d 8b 35  1a 16 41 12 0b 8d 7e 21   ··l····5 ··A···~!
00d0  aa b9 75 77 02 e8 29 d9  16 7c c3 2c 28 6b a2 b5   ··uw··)· ·|·,(k··
00e0  c2 55 4b 2a 30 06 ed 2b  84 ab 39 3a df 64 fb 25   ·UK*0··+ ··9:·d·%
00f0  bd 4f b7 7a 39 e2 ba 51  8e 4a c0 2a f5 b9 3c 61   ·O·z9··Q ·J·*··<a
0100  93 6c e0 6d 84 4e 5b 18  1e 2d 21 6e 1b ea f2 7b   ·l·m·N[· ·-!n···{
0110  f9 74 fb 30 37 1b ad 23  a0 67 c2 c9 d1 06 20 c5   ·t·07··# ·g···· ·
0120  5d 41 a0 1f b8 35 5e d1  37 d7 59 ed 45 2e e0 f6   ]A···5^· 7·Y·E.··
0130  50 16 ff ec b4 00 ca 07  77 8d 7b f0 73 82 83 f4   P······· w·{·s···
0140  53 bf a0 e4 0d d3 8f 74  42 a3 b9 4d 1f 61         S······t B··M·a
```

Hypertext Transfer Protocol: Protocol

Packets: 2268 · Displayed: 8 (0.4%)

Profile: Default

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer or (if you are using the trace file) the computer that sent the HTTP GET message?


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

http

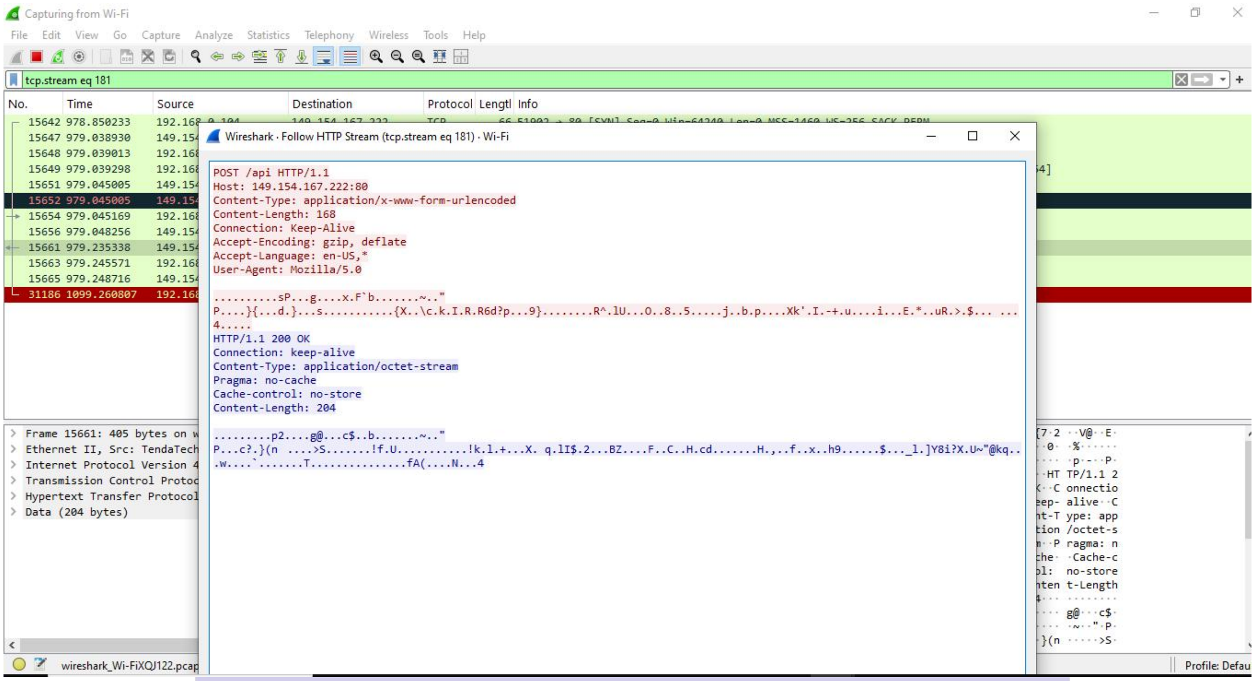
```
No.    Time         Source           Destination      Protocol Lengtl Info
  980 35.593644    192.168.0.104    128.119.245.12    HTTP      527 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 1040 35.908890    128.119.245.12   192.168.0.104     HTTP      492 HTTP/1.1 200 OK  (text/html)
 1042 36.140441    192.168.0.104    128.119.245.12    HTTP      473 GET /favicon.ico HTTP/1.1
 1066 36.450388    128.119.245.12   192.168.0.104     HTTP      538 HTTP/1.1 404 Not Found  (text/html)
 5754 256.706254   192.168.0.104    128.119.245.12    HTTP      527 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 5767 257.040671   128.119.245.12   192.168.0.104     HTTP      492 HTTP/1.1 200 OK  (text/html)
 5776 257.125766   192.168.0.104    128.119.245.12    HTTP      473 GET /favicon.ico HTTP/1.1
 5779 257.485292   128.119.245.12   192.168.0.104     HTTP      538 HTTP/1.1 404 Not Found  (text/html)
 8279 421.332884   192.168.0.104    91.108.23.100     HTTP      222 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
11231 587.819588   192.168.0.104    91.108.23.100     HTTP      122 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
11263 588.061958   192.168.0.104    91.108.23.100     HTTP      110 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
11268 588.132106   91.108.23.100    192.168.0.104     HTTP      405 HTTP/1.1 200 OK
```

```
> Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: TendaTechnol_1b:56:40 (d8
v Internet Protocol Version 4, Src: 192.168.0.104, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 513
    Identification: 0x56f7 (22263)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x6b6b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.104
    Destination Address: 128.119.245.12
    [Stream index: 17]
> Transmission Control Protocol, Src Port: 51765, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
```

```
0030  02 05 6c a8 00 00 47 45  54 20 2f 77 69 72 65 73   ··l···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63 74 69   ss.edu·· Connecti
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 55 73   -Request s: 1··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
00d0  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows N
00e0  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b 20 78   T 10.0;  Win64; x
00f0  36 34 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   64) Appl eWebKit/
0100  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
0110  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
0120  65 2f 31 33 33 2e 30 2e  30 2e 30 20 53 61 66 61   e/133.0. 0.0 Safa
0130  72 69 2f 35 33 37 2e 33  36 0d 0a 41 63 63 65 70   ri/537.3 6··Accep
0140  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t: text/ html,app
0150  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
0160  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
```

HTTP Request-URI (http.request.uri), 42 bytes | Packets: 12365 · Displayed: 12 (0.1%) | Profile: Default

4. Expand the information on the HTTP message in the Wireshark "Details of selected packet" window (see Figure 3 above) so you can see the fields in the HTTP GET request message. What type of Web browser issued the HTTP request? The answer is shown at the right end of the information following the "User-Agent:" field in the expanded HTTP message display. [This field value in the HTTP message is how a web server learns what type of browser you are using.] Firefox, Safari, Microsoft Internet Edge, Other



Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.stream eq 181

No.   Time          Source
15642 978.850233    192.168.0.104     149.154.167.222   TCP   66 51902 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
15647 979.038930    149.154
15648 979.039013    192.168
15649 979.039298    192.168                                                                                   4]
15651 979.045005    149.154
15652 979.045005    149.154
15654 979.045169    192.168
15656 979.048256    149.154
15661 979.235338    149.154
15663 979.245571    192.168
15665 979.248716    149.154
31186 1099.260807   192.168

> Frame 15661: 405 bytes on w
> Ethernet II, Src: TendaTech
> Internet Protocol Version 4
> Transmission Control Protoc
> Hypertext Transfer Protocol
> Data (204 bytes)

wireshark_Wi-FiXQJ122.pcap                                                     Profile: Defau
```

Wireshark · Follow HTTP Stream (tcp.stream eq 181) · Wi-Fi

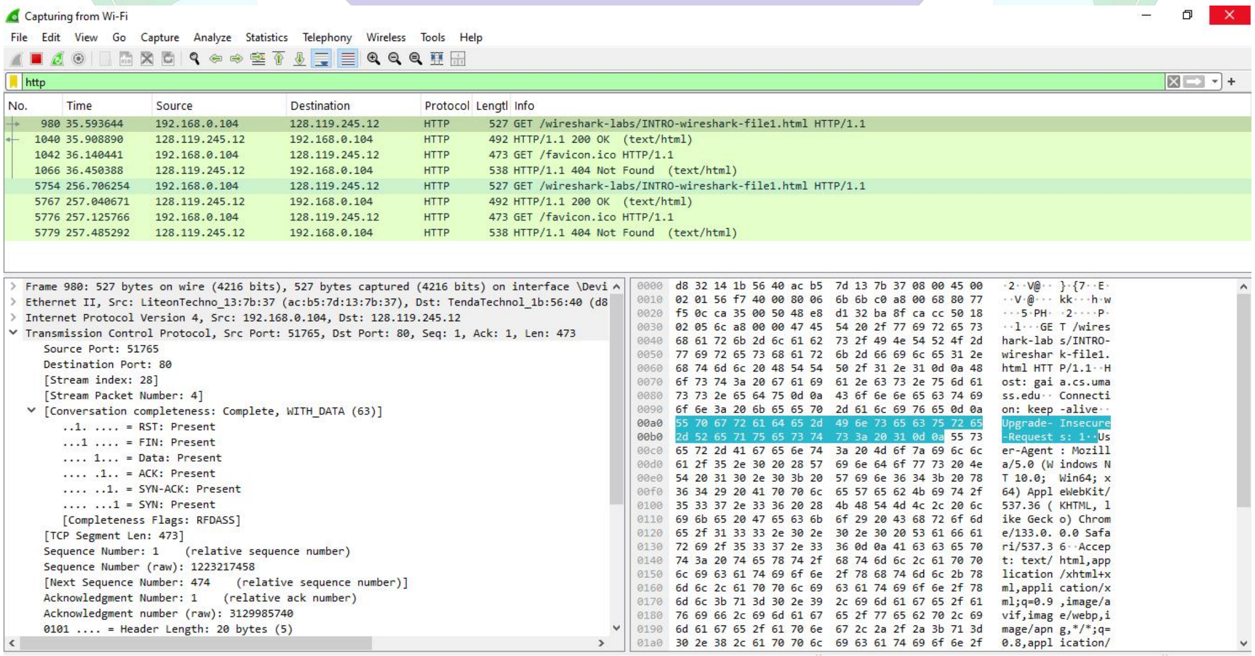
```
POST /api HTTP/1.1
Host: 149.154.167.222:80
Content-Type: application/x-www-form-urlencoded
Content-Length: 168
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept-Language: en-US,*
User-Agent: Mozilla/5.0

..........sP...g....x.F`b.......~.."
P....}{...d.}...s...........{X..\c.k.I.R.R6d?p...9}........R^.lU...O..8..5.....j..b.p....Xk'.I.-+.u....i...E.*..uR.>.$... ...
4.....
HTTP/1.1 200 OK
Connection: keep-alive
Content-Type: application/octet-stream
Pragma: no-cache
Cache-control: no-store
Content-Length: 204

.........p2....g@...c$..b.......~.."
P...c?.}(n  ....>S.......!f.U...........!k.l.+...X. q.lI$.2...BZ....F..C..H.cd.......H.,..f..x..h9......$..._l.]Y8i?X.U~"@kq..
.w....`.......T...............fA(....N...4
```

```
{7·2  ··V@··E·
 ·0·  ·%·····
····  ·p·-··P·
··HT TP/1.1 2
K··C onnectio
eep- alive··C
nt-T ype: app
tion /octet-s
n··P ragma: n
che·  ·Cache-c
ol:  no-store
nten t-Length
4···  ·······
····  g@···c$·
····  ·~··"·P·
·}(n  ·····>S·
```

5. Expand the information on the Transmission Control Protocol for this packet in the Wireshark "Details of selected packet" window (see Figure 3 in the lab writeup) so you can see the fields in the TCP segment carrying the HTTP message. What is the destination port number (the number following "Dest Port:" for the TCP segment containing the HTTP request) to which this HTTP request is being sent?



Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

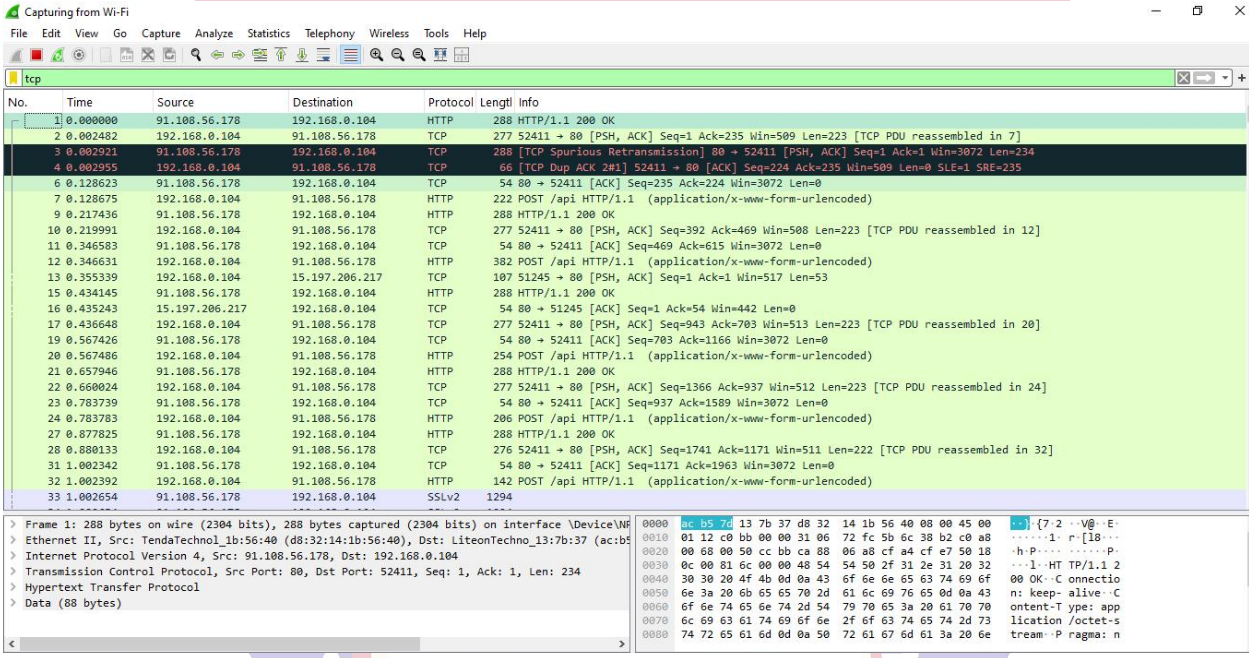
```
http

No.   Time         Source          Destination     Protocol Lengtl Info
  980 35.593644    192.168.0.104   128.119.245.12  HTTP     527 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 1040 35.908890    128.119.245.12  192.168.0.104   HTTP     492 HTTP/1.1 200 OK  (text/html)
 1042 36.140441    192.168.0.104   128.119.245.12  HTTP     473 GET /favicon.ico HTTP/1.1
 1066 36.450388    128.119.245.12  192.168.0.104   HTTP     538 HTTP/1.1 404 Not Found  (text/html)
 5754 256.706254   192.168.0.104   128.119.245.12  HTTP     527 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 5767 257.040671   128.119.245.12  192.168.0.104   HTTP     492 HTTP/1.1 200 OK  (text/html)
 5776 257.125766   192.168.0.104   128.119.245.12  HTTP     473 GET /favicon.ico HTTP/1.1
 5779 257.485292   128.119.245.12  192.168.0.104   HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 980: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Devi
> Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: TendaTechnol_1b:56:40 (d8
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 51765, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
     Source Port: 51765
     Destination Port: 80
     [Stream index: 28]
     [Stream Packet Number: 4]
   v [Conversation completeness: Complete, WITH_DATA (63)]
        ..1. .... = RST: Present
        ...1 .... = FIN: Present
        .... 1... = Data: Present
        .... .1.. = ACK: Present
        .... ..1. = SYN-ACK: Present
        .... ...1 = SYN: Present
        [Completeness Flags: RFDASS]
     [TCP Segment Len: 473]
     Sequence Number: 1    (relative sequence number)
     Sequence Number (raw): 1223217458
     [Next Sequence Number: 474    (relative sequence number)]
     Acknowledgment Number: 1    (relative ack number)
     Acknowledgment number (raw): 3129985740
     0101 .... = Header Length: 20 bytes (5)
```

```
0000  d8 32 14 1b 56 40 ac b5  7d 13 7b 37 08 00 45 00   ·2··V@·· }·{7··E·
0010  02 01 56 f7 40 00 80 06  6b 6b c0 a8 00 68 80 77   ··V·@··· kk···h·w
0020  f5 0c ca 35 00 50 48 e8  d1 32 ba 8f ca cc 50 18   ···5·PH· ·2····P·
0030  02 05 6c a8 00 00 47 45  54 20 2f 77 69 72 65 73   ··l···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63 74 69   ss.edu·· Connecti
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 55 73   -Request s: 1··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
00d0  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows N
00e0  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b 20 78   T 10.0;  Win64; x
00f0  36 34 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   64) Appl eWebKit/
0100  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
0110  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
0120  65 2f 31 33 33 2e 30 2e  30 2e 30 20 53 61 66 61   e/133.0. 0.0 Safa
0130  72 69 2f 35 33 37 2e 33  36 0d 0a 41 63 63 65 70   ri/537.3 6··Accep
0140  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t: text/ html,app
0150  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
0160  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
0170  6d 6c 3b 71 3d 30 2e 39  2c 69 6d 61 67 65 2f 61   ml;q=0.9 ,image/a
0180  76 69 66 2c 69 6d 61 67  65 2f 77 65 62 70 2c 69   vif,imag e/webp,i
0190  6d 61 67 65 2f 61 70 6e  67 2c 2a 2f 2a 3b 71 3d   mage/apn g,*/*;q=
01a0  30 2e 38 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   0.8,appl ication/
```

6. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.


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

```
tcp

No.   Time      Source          Destination     Protocol Lengtl Info
    1 0.000000  91.108.56.178   192.168.0.104   HTTP     288 HTTP/1.1 200 OK
    2 0.002482  192.168.0.104   91.108.56.178   TCP      277 52411 → 80 [PSH, ACK] Seq=1 Ack=235 Win=509 Len=223 [TCP PDU reassembled in 7]
    3 0.002921  91.108.56.178   192.168.0.104   TCP      288 [TCP Spurious Retransmission] 80 → 52411 [PSH, ACK] Seq=1 Ack=1 Win=3072 Len=234
    4 0.002955  192.168.0.104   91.108.56.178   TCP       66 [TCP Dup ACK 2#1] 52411 → 80 [ACK] Seq=224 Ack=235 Win=509 Len=0 SLE=1 SRE=235
    6 0.128623  91.108.56.178   192.168.0.104   TCP       54 80 → 52411 [ACK] Seq=235 Ack=224 Win=3072 Len=0
    7 0.128675  192.168.0.104   91.108.56.178   HTTP     222 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
    9 0.217436  91.108.56.178   192.168.0.104   HTTP     288 HTTP/1.1 200 OK
   10 0.219991  192.168.0.104   91.108.56.178   TCP      277 52411 → 80 [PSH, ACK] Seq=392 Ack=469 Win=508 Len=223 [TCP PDU reassembled in 12]
   11 0.346583  91.108.56.178   192.168.0.104   TCP       54 80 → 52411 [ACK] Seq=469 Ack=615 Win=3072 Len=0
   12 0.346631  192.168.0.104   91.108.56.178   HTTP     382 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
   13 0.355339  192.168.0.104   15.197.206.217  TCP      107 51245 → 80 [PSH, ACK] Seq=1 Ack=1 Win=517 Len=53
   15 0.434145  91.108.56.178   192.168.0.104   HTTP     288 HTTP/1.1 200 OK
   16 0.435243  15.197.206.217  192.168.0.104   TCP       54 80 → 51245 [ACK] Seq=1 Ack=54 Win=442 Len=0
   17 0.436648  192.168.0.104   91.108.56.178   TCP      277 52411 → 80 [PSH, ACK] Seq=943 Ack=703 Win=513 Len=223 [TCP PDU reassembled in 20]
   19 0.567426  91.108.56.178   192.168.0.104   TCP       54 80 → 52411 [ACK] Seq=703 Ack=1166 Win=3072 Len=0
   20 0.567486  192.168.0.104   91.108.56.178   HTTP     254 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
   21 0.657946  91.108.56.178   192.168.0.104   HTTP     288 HTTP/1.1 200 OK
   22 0.660024  192.168.0.104   91.108.56.178   TCP      277 52411 → 80 [PSH, ACK] Seq=1366 Ack=937 Win=512 Len=223 [TCP PDU reassembled in 24]
   23 0.783739  91.108.56.178   192.168.0.104   TCP       54 80 → 52411 [ACK] Seq=937 Ack=1589 Win=3072 Len=0
   24 0.783783  192.168.0.104   91.108.56.178   HTTP     206 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
   27 0.877825  91.108.56.178   192.168.0.104   HTTP     288 HTTP/1.1 200 OK
   28 0.880133  192.168.0.104   91.108.56.178   TCP      276 52411 → 80 [PSH, ACK] Seq=1741 Ack=1171 Win=511 Len=222 [TCP PDU reassembled in 32]
   31 1.002342  91.108.56.178   192.168.0.104   TCP       54 80 → 52411 [ACK] Seq=1171 Ack=1963 Win=3072 Len=0
   32 1.002392  192.168.0.104   91.108.56.178   HTTP     142 POST /api HTTP/1.1  (application/x-www-form-urlencoded)
   33 1.002654  91.108.56.178   192.168.0.104   SSLv2   1294
```

```
> Frame 1: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface \Device\NF
> Ethernet II, Src: TendaTechnol_1b:56:40 (d8:32:14:1b:56:40), Dst: LiteonTechno_13:7b:37 (ac:b5
> Internet Protocol Version 4, Src: 91.108.56.178, Dst: 192.168.0.104
> Transmission Control Protocol, Src Port: 80, Dst Port: 52411, Seq: 1, Ack: 1, Len: 234
> Hypertext Transfer Protocol
> Data (88 bytes)
```

```
0000  ac b5 7d 13 7b 37 d8 32  14 1b 56 40 08 00 45 00   ··}·{7·2 ··V@··E·
0010  01 12 c0 bb 00 00 31 06  72 fc 5b 6c 38 b2 c0 a8   ······1· r·[l8···
0020  00 68 00 50 cc bb ca 88  06 a8 cf a4 cf e7 50 18   ·h·P···· ······P·
0030  0c 00 81 6c 00 00 48 54  54 50 2f 31 2e 31 20 32   ···l··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 6e 65 63 74 69 6f   00 OK··C onnectio
0050  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 43   n: keep- alive··C
0060  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 61 70 70   ontent-T ype: app
0070  6c 69 63 61 74 69 6f 6e  2f 6f 63 74 65 74 2d 73   lication /octet-s
0080  74 72 65 61 6d 0d 0a 50  72 61 67 6d 61 3a 20 6e   tream··P ragma: n
```

Thank You