Al-Imam Mohammad Bin Saud Islamic University
College of Computer and Information Sciences,
Department of Computer Science
CS 330 computer networks
October 21, 2021

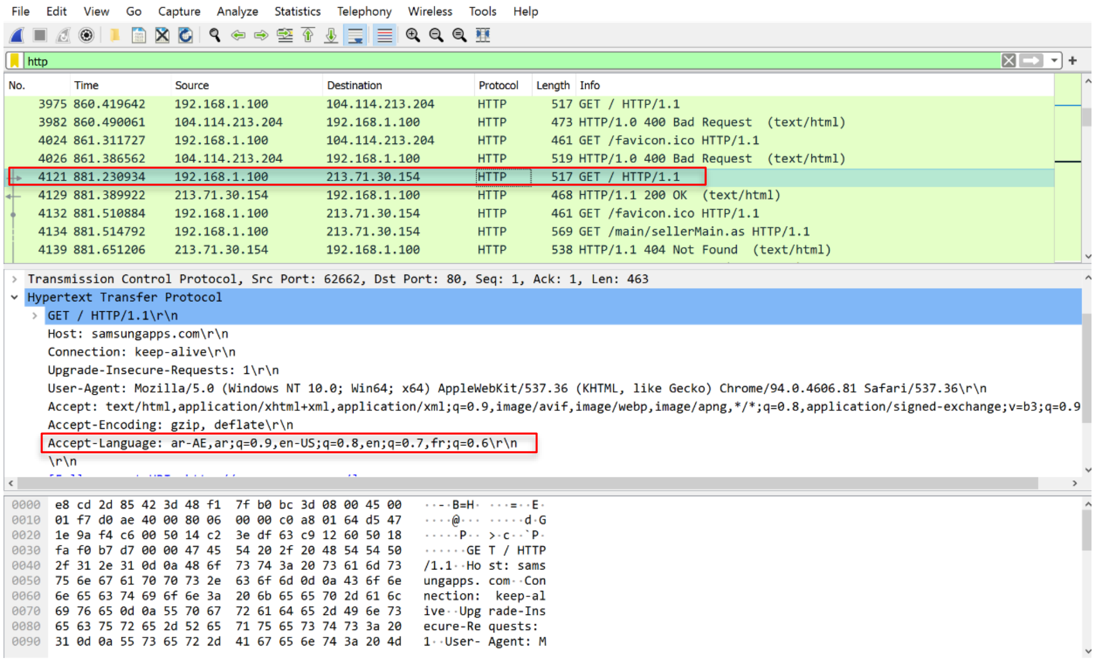
Lab Assignment

Wireshark Labs

Student's Name	Student's E-mail	Student's ID
Shoroog Saad Alarifi	sssalarifi@sm.imamu.edu.sa	440022128

Teacher: Basma Alsoli.

URL#1



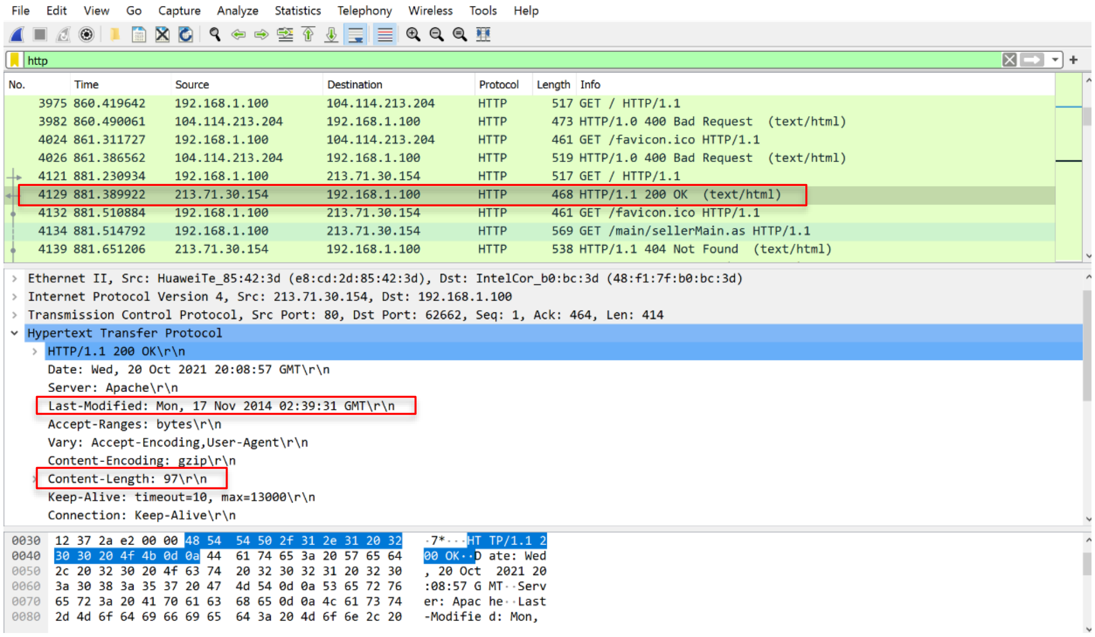
```
http
```

```
No.    Time         Source           Destination      Protocol  Length  Info
  3975 860.419642   192.168.1.100    104.114.213.204  HTTP       517 GET / HTTP/1.1
  3982 860.490061   104.114.213.204  192.168.1.100    HTTP       473 HTTP/1.0 400 Bad Request  (text/html)
  4024 861.311727   192.168.1.100    104.114.213.204  HTTP       461 GET /favicon.ico HTTP/1.1
  4026 861.386562   104.114.213.204  192.168.1.100    HTTP       519 HTTP/1.0 400 Bad Request  (text/html)
  4121 881.230934   192.168.1.100    213.71.30.154    HTTP       517 GET / HTTP/1.1
  4129 881.389922   213.71.30.154    192.168.1.100    HTTP       468 HTTP/1.1 200 OK  (text/html)
  4132 881.510884   192.168.1.100    213.71.30.154    HTTP       461 GET /favicon.ico HTTP/1.1
  4134 881.514792   192.168.1.100    213.71.30.154    HTTP       569 GET /main/sellerMain.as HTTP/1.1
  4139 881.651206   213.71.30.154    192.168.1.100    HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Transmission Control Protocol, Src Port: 62662, Dst Port: 80, Seq: 1, Ack: 1, Len: 463
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: samsungapps.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ar-AE,ar;q=0.9,en-US;q=0.8,en;q=0.7,fr;q=0.6\r\n
    \r\n
```

```
0000  e8 cd 2d 85 42 3d 48 f1  7f b0 bc 3d 08 00 45 00   ··-·B=H· ···=··E·
0010  01 f7 d0 ae 40 00 80 06  00 00 c0 a8 01 64 d5 47   ····@··· ·····d·G
0020  1e 9a f4 c6 00 50 14 c2  3e df 63 c9 12 60 50 18   ·····P·· >·c··`P·
0030  fa f0 b7 d7 00 00 47 45  54 20 2f 20 48 54 54 50   ······GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 73 61 6d 73   /1.1··Ho st: sams
0050  75 6e 67 61 70 70 73 2e  63 6f 6d 0d 0a 43 6f 6e   ungapps. com··Con
0060  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
0070  69 76 65 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   ive··Upg rade-Ins
0080  65 63 75 72 65 2d 52 65  71 75 65 73 74 73 3a 20   ecure-Re quests: 
0090  31 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   1··User- Agent: M
```

HTTP GET message [URL#1]



```
http
```

```
No.    Time         Source           Destination      Protocol  Length  Info
  3975 860.419642   192.168.1.100    104.114.213.204  HTTP       517 GET / HTTP/1.1
  3982 860.490061   104.114.213.204  192.168.1.100    HTTP       473 HTTP/1.0 400 Bad Request  (text/html)
  4024 861.311727   192.168.1.100    104.114.213.204  HTTP       461 GET /favicon.ico HTTP/1.1
  4026 861.386562   104.114.213.204  192.168.1.100    HTTP       519 HTTP/1.0 400 Bad Request  (text/html)
  4121 881.230934   192.168.1.100    213.71.30.154    HTTP       517 GET / HTTP/1.1
  4129 881.389922   213.71.30.154    192.168.1.100    HTTP       468 HTTP/1.1 200 OK  (text/html)
  4132 881.510884   192.168.1.100    213.71.30.154    HTTP       461 GET /favicon.ico HTTP/1.1
  4134 881.514792   192.168.1.100    213.71.30.154    HTTP       569 GET /main/sellerMain.as HTTP/1.1
  4139 881.651206   213.71.30.154    192.168.1.100    HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Ethernet II, Src: HuaweiTe_85:42:3d (e8:cd:2d:85:42:3d), Dst: IntelCor_b0:bc:3d (48:f1:7f:b0:bc:3d)
> Internet Protocol Version 4, Src: 213.71.30.154, Dst: 192.168.1.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 62662, Seq: 1, Ack: 464, Len: 414
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 20 Oct 2021 20:08:57 GMT\r\n
    Server: Apache\r\n
    Last-Modified: Mon, 17 Nov 2014 02:39:31 GMT\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding,User-Agent\r\n
    Content-Encoding: gzip\r\n
  > Content-Length: 97\r\n
    Keep-Alive: timeout=10, max=13000\r\n
    Connection: Keep-Alive\r\n
```

```
0030  12 37 2a e2 00 00 48 54  54 50 2f 31 2e 31 20 32   ·7*···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 57 65 64   00 OK··D ate: Wed
0050  2c 20 32 30 20 4f 63 74  20 32 30 32 31 20 32 30   , 20 Oct  2021 20
0060  3a 30 38 3a 35 37 20 47  4d 54 0d 0a 53 65 72 76   :08:57 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 0d 0a 4c 61 73 74   er: Apac he··Last
0080  2d 4d 6f 64 69 66 69 65  64 3a 20 4d 6f 6e 2c 20   -Modifie d: Mon, 
```

HTTP response message [URL#1]

a. What is the Internet address of the selected server? What is the Internet address of your computer that sent the HTTP GET message?

Internet address of Server : 213.71.30.154
Internet address of my computer :192.168.1.100

b. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?

Both server and my browser running HTTP 1.1

c. What languages (if any) does your browser indicate that it can accept to the server?

ar-AE and en-US (Arabic and English)

d. What is the status code returned from the server to your browser?

Status code :200 , status phrase : OK

e. When was the HTML file that you are retrieving last modified at the server?

Mon, 17 Nov 2014 02:39:31 GMT

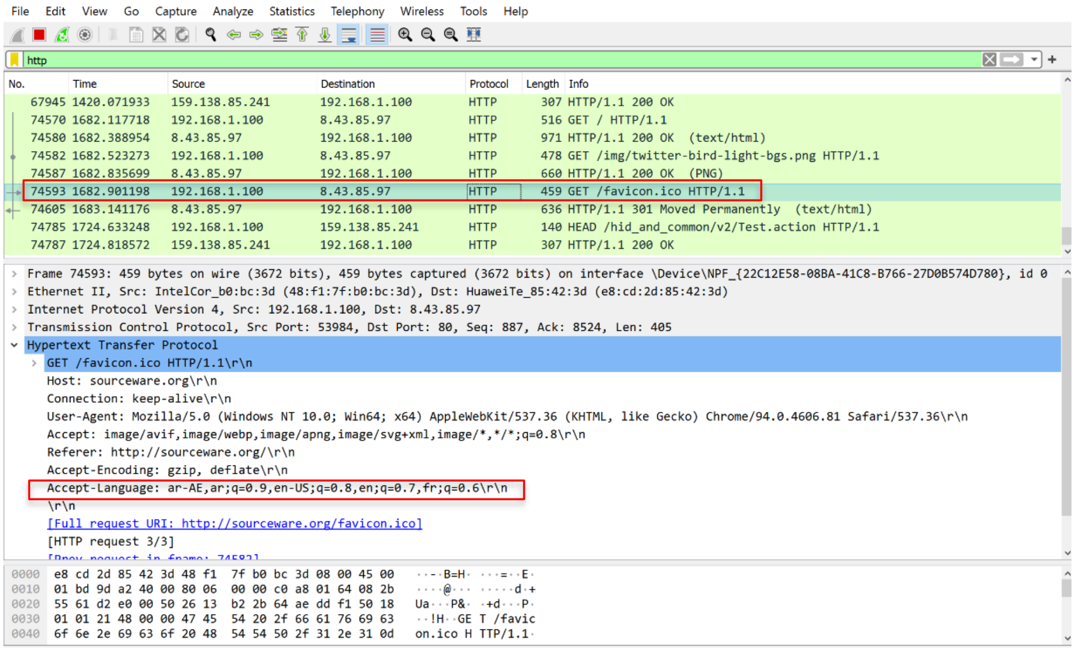
f. How many bytes of content are being returned to your browser?

97 bytes

g. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name them.

No. The raw data in the packet content window appears to match up exactly with what is shown in the packet-listing window

URL#2

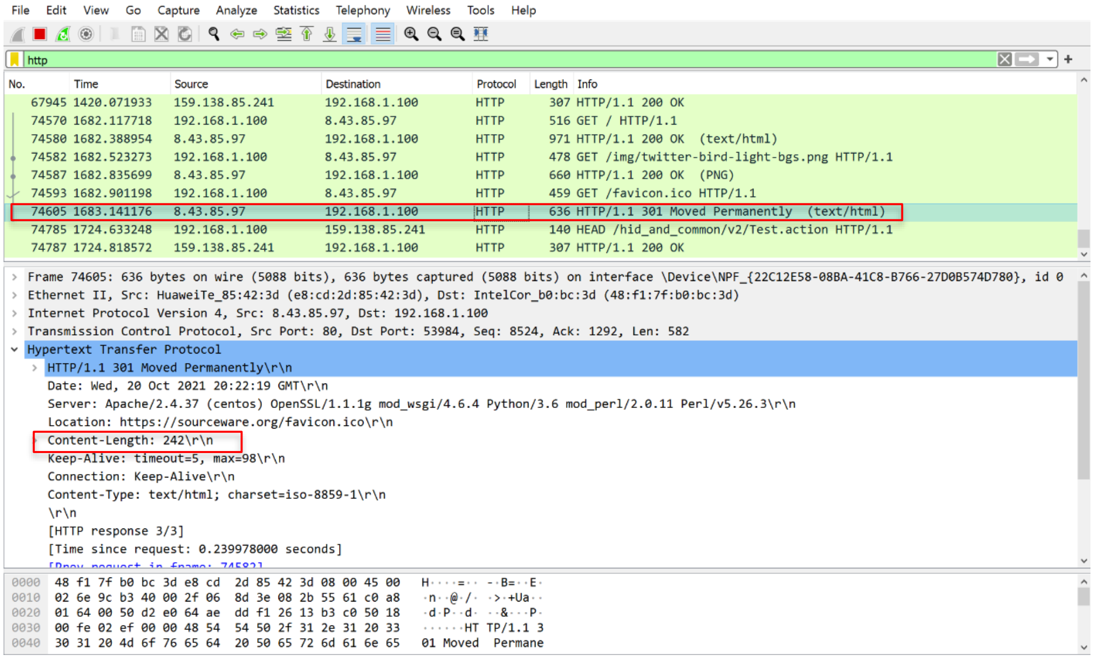


```
No.   Time         Source          Destination     Protocol Length Info
67945 1420.071933  159.138.85.241  192.168.1.100   HTTP     307 HTTP/1.1 200 OK
74570 1682.117718  192.168.1.100   8.43.85.97      HTTP     516 GET / HTTP/1.1
74580 1682.388954  8.43.85.97      192.168.1.100   HTTP     971 HTTP/1.1 200 OK  (text/html)
74582 1682.523273  192.168.1.100   8.43.85.97      HTTP     478 GET /img/twitter-bird-light-bgs.png HTTP/1.1
74587 1682.835699  8.43.85.97      192.168.1.100   HTTP     660 HTTP/1.1 200 OK  (PNG)
74593 1682.901198  192.168.1.100   8.43.85.97      HTTP     459 GET /favicon.ico HTTP/1.1
74605 1683.141176  8.43.85.97      192.168.1.100   HTTP     636 HTTP/1.1 301 Moved Permanently  (text/html)
74785 1724.633248  192.168.1.100   159.138.85.241  HTTP     140 HEAD /hid_and_common/v2/Test.action HTTP/1.1
74787 1724.818572  159.138.85.241  192.168.1.100   HTTP     307 HTTP/1.1 200 OK
```

```
> Frame 74593: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface \Device\NPF_{22C12E58-08BA-41C8-B766-27D0B574D780}, id 0
> Ethernet II, Src: IntelCor_b0:bc:3d (48:f1:7f:b0:bc:3d), Dst: HuaweiTe_85:42:3d (e8:cd:2d:85:42:3d)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 8.43.85.97
> Transmission Control Protocol, Src Port: 53984, Dst Port: 80, Seq: 887, Ack: 8524, Len: 405
v Hypertext Transfer Protocol
  > GET /favicon.ico HTTP/1.1\r\n
    Host: sourceware.org\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n
    Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://sourceware.org/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ar-AE,ar;q=0.9,en-US;q=0.8,en;q=0.7,fr;q=0.6\r\n
    \r\n
    [Full request URI: http://sourceware.org/favicon.ico]
    [HTTP request 3/3]
    [Prev request in frame: 74582]
```

```
0000  e8 cd 2d 85 42 3d 48 f1  7f b0 bc 3d 08 00 45 00   ··-·B=H· ··=··E·
0010  01 bd 9d a2 40 00 80 06  00 00 c0 a8 01 64 08 2b   ····@··· ·····d·+
0020  55 61 d2 e0 00 50 26 13  b2 2b 64 ae dd f1 50 18   Ua···P&· ·+d···P·
0030  01 01 21 48 00 00 47 45  54 20 2f 66 61 76 69 63   ··!H··GE T /favic
0040  6f 6e 2e 69 63 6f 20 48  54 54 50 2f 31 2e 31 0d   on.ico H TTP/1.1·
```

HTTP GET message [URL#2]



```
No.   Time         Source          Destination     Protocol Length Info
67945 1420.071933  159.138.85.241  192.168.1.100   HTTP     307 HTTP/1.1 200 OK
74570 1682.117718  192.168.1.100   8.43.85.97      HTTP     516 GET / HTTP/1.1
74580 1682.388954  8.43.85.97      192.168.1.100   HTTP     971 HTTP/1.1 200 OK  (text/html)
74582 1682.523273  192.168.1.100   8.43.85.97      HTTP     478 GET /img/twitter-bird-light-bgs.png HTTP/1.1
74587 1682.835699  8.43.85.97      192.168.1.100   HTTP     660 HTTP/1.1 200 OK  (PNG)
74593 1682.901198  192.168.1.100   8.43.85.97      HTTP     459 GET /favicon.ico HTTP/1.1
74605 1683.141176  8.43.85.97      192.168.1.100   HTTP     636 HTTP/1.1 301 Moved Permanently  (text/html)
74785 1724.633248  192.168.1.100   159.138.85.241  HTTP     140 HEAD /hid_and_common/v2/Test.action HTTP/1.1
74787 1724.818572  159.138.85.241  192.168.1.100   HTTP     307 HTTP/1.1 200 OK
```

```
> Frame 74605: 636 bytes on wire (5088 bits), 636 bytes captured (5088 bits) on interface \Device\NPF_{22C12E58-08BA-41C8-B766-27D0B574D780}, id 0
> Ethernet II, Src: HuaweiTe_85:42:3d (e8:cd:2d:85:42:3d), Dst: IntelCor_b0:bc:3d (48:f1:7f:b0:bc:3d)
> Internet Protocol Version 4, Src: 8.43.85.97, Dst: 192.168.1.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 53984, Seq: 8524, Ack: 1292, Len: 582
v Hypertext Transfer Protocol
  > HTTP/1.1 301 Moved Permanently\r\n
    Date: Wed, 20 Oct 2021 20:22:19 GMT\r\n
    Server: Apache/2.4.37 (centos) OpenSSL/1.1.1g mod_wsgi/4.6.4 Python/3.6 mod_perl/2.0.11 Perl/v5.26.3\r\n
    Location: https://sourceware.org/favicon.ico\r\n
  > Content-Length: 242\r\n
    Keep-Alive: timeout=5, max=98\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.239978000 seconds]
    [Prev request in frame: 74582]
```

```
0000  48 f1 7f b0 bc 3d e8 cd  2d 85 42 3d 08 00 45 00   H····=·· -·B=··E·
0010  02 6e 9c b3 40 00 2f 06  8d 3e 08 2b 55 61 c0 a8   ·n··@·/· ·>·+Ua··
0020  01 64 00 50 d2 e0 64 ae  dd f1 26 13 b3 c0 50 18   ·d·P··d· ··&···P·
0030  00 fe 02 ef 00 00 48 54  54 50 2f 31 2e 31 20 33   ······HT TP/1.1 3
0040  30 31 20 4d 6f 76 65 64  20 50 65 72 6d 61 6e 65   01 Moved  Permane
```

HTTP response message [URL#2]

a. What is the Internet address of the selected server? What is the Internet address of your computer that sent the HTTP GET message?

Internet address of Server : 8.43.85.97
Internet address of my computer : 192.168.1.100

b. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?

Both server and my browser running HTTP 1.1

c. What languages (if any) does your browser indicate that it can accept to the server?

ar-AE and en-US (Arabic and English)

d. What is the status code returned from the server to your browser?

Status code :301 , status phrase : Moved Permanently

e. When was the HTML file that you are retrieving last modified at the server?

I don't have last_modified in this response message.

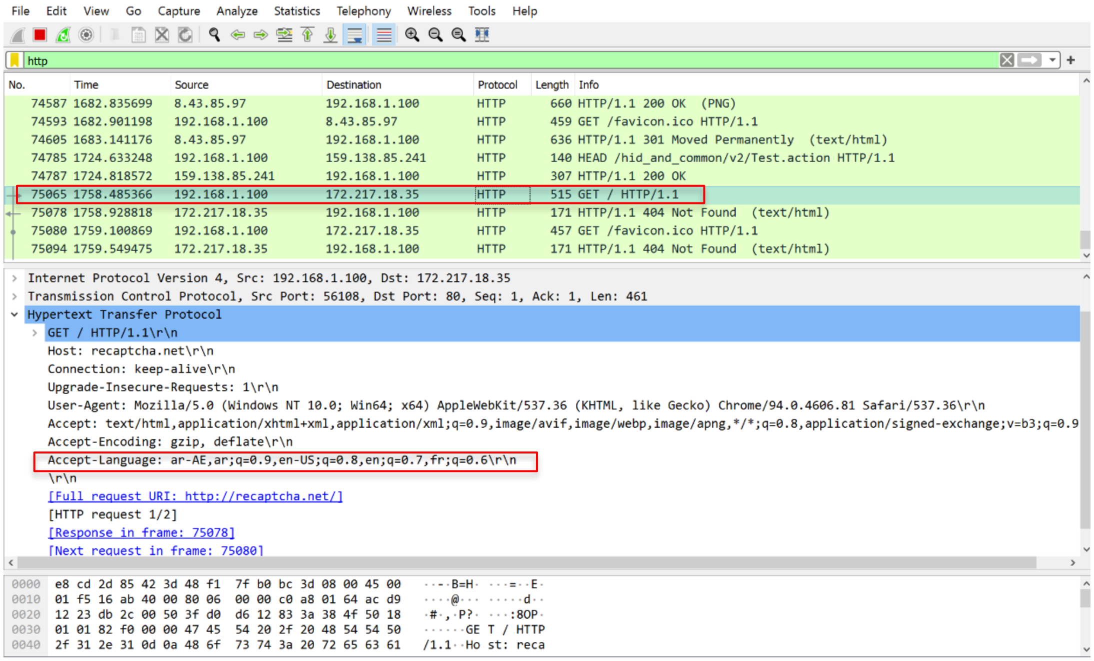
f. How many bytes of content are being returned to your browser?

242 bytes

g. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name them.

No. The raw data in the packet content window appears to match up exactly with what is shown in the packet-listing window

URL#3



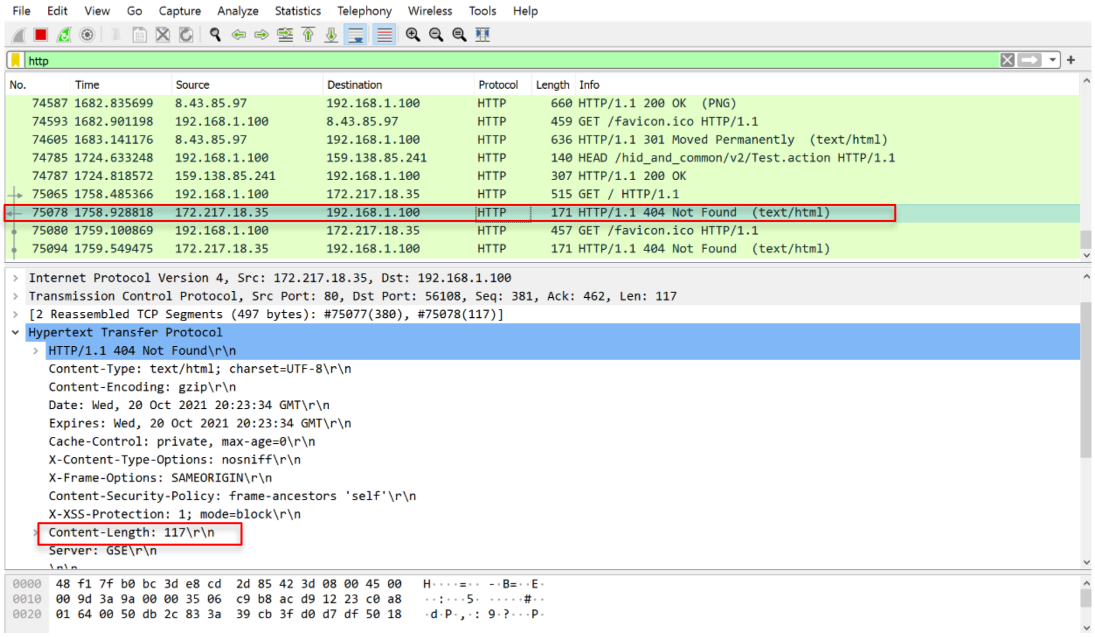
```
http
```

```
No.    Time         Source          Destination     Protocol  Length  Info
 74587 1682.835699  8.43.85.97      192.168.1.100   HTTP       660 HTTP/1.1 200 OK  (PNG)
 74593 1682.901198  192.168.1.100   8.43.85.97      HTTP       459 GET /favicon.ico HTTP/1.1
 74605 1683.141176  8.43.85.97      192.168.1.100   HTTP       636 HTTP/1.1 301 Moved Permanently  (text/html)
 74785 1724.633248  192.168.1.100   159.138.85.241  HTTP       140 HEAD /hid_and_common/v2/Test.action HTTP/1.1
 74787 1724.818572  159.138.85.241  192.168.1.100   HTTP       307 HTTP/1.1 200 OK
 75065 1758.485366  192.168.1.100   172.217.18.35   HTTP       515 GET / HTTP/1.1
 75078 1758.928818  172.217.18.35   192.168.1.100   HTTP       171 HTTP/1.1 404 Not Found  (text/html)
 75080 1759.100869  192.168.1.100   172.217.18.35   HTTP       457 GET /favicon.ico HTTP/1.1
 75094 1759.549475  172.217.18.35   192.168.1.100   HTTP       171 HTTP/1.1 404 Not Found  (text/html)
```

```
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 172.217.18.35
> Transmission Control Protocol, Src Port: 56108, Dst Port: 80, Seq: 1, Ack: 1, Len: 461
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: recaptcha.net\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ar-AE,ar;q=0.9,en-US;q=0.8,en;q=0.7,fr;q=0.6\r\n
    \r\n
    [Full request URI: http://recaptcha.net/]
    [HTTP request 1/2]
    [Response in frame: 75078]
    [Next request in frame: 75080]
```

```
0000  e8 cd 2d 85 42 3d 48 f1  7f b0 bc 3d 08 00 45 00   ··-·B=H· ···=··E·
0010  01 f5 16 ab 40 00 80 06  00 00 c0 a8 01 64 ac d9   ····@··· ·····d··
0020  12 23 db 2c 00 50 3f d0  d6 12 83 3a 38 4f 50 18   ·#·,·P?· ···:8OP·
0030  01 01 82 f0 00 00 47 45  54 20 2f 20 48 54 54 50   ······GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 72 65 63 61   /1.1··Ho st: reca
```

HTTP GET message [URL#3]



```
http
```

```
No.    Time         Source          Destination     Protocol  Length  Info
 74587 1682.835699  8.43.85.97      192.168.1.100   HTTP       660 HTTP/1.1 200 OK  (PNG)
 74593 1682.901198  192.168.1.100   8.43.85.97      HTTP       459 GET /favicon.ico HTTP/1.1
 74605 1683.141176  8.43.85.97      192.168.1.100   HTTP       636 HTTP/1.1 301 Moved Permanently  (text/html)
 74785 1724.633248  192.168.1.100   159.138.85.241  HTTP       140 HEAD /hid_and_common/v2/Test.action HTTP/1.1
 74787 1724.818572  159.138.85.241  192.168.1.100   HTTP       307 HTTP/1.1 200 OK
 75065 1758.485366  192.168.1.100   172.217.18.35   HTTP       515 GET / HTTP/1.1
 75078 1758.928818  172.217.18.35   192.168.1.100   HTTP       171 HTTP/1.1 404 Not Found  (text/html)
 75080 1759.100869  192.168.1.100   172.217.18.35   HTTP       457 GET /favicon.ico HTTP/1.1
 75094 1759.549475  172.217.18.35   192.168.1.100   HTTP       171 HTTP/1.1 404 Not Found  (text/html)
```

```
> Internet Protocol Version 4, Src: 172.217.18.35, Dst: 192.168.1.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 56108, Seq: 381, Ack: 462, Len: 117
> [2 Reassembled TCP Segments (497 bytes): #75077(380), #75078(117)]
v Hypertext Transfer Protocol
  > HTTP/1.1 404 Not Found\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Content-Encoding: gzip\r\n
    Date: Wed, 20 Oct 2021 20:23:34 GMT\r\n
    Expires: Wed, 20 Oct 2021 20:23:34 GMT\r\n
    Cache-Control: private, max-age=0\r\n
    X-Content-Type-Options: nosniff\r\n
    X-Frame-Options: SAMEORIGIN\r\n
    Content-Security-Policy: frame-ancestors 'self'\r\n
    X-XSS-Protection: 1; mode=block\r\n
  > Content-Length: 117\r\n
    Server: GSE\r\n
    \r\n
```

```
0000  48 f1 7f b0 bc 3d e8 cd  2d 85 42 3d 08 00 45 00   H····=·· -·B=··E·
0010  00 9d 3a 9a 00 00 35 06  c9 b8 ac d9 12 23 c0 a8   ··:···5· ·····#··
0020  01 64 00 50 db 2c 83 3a  39 cb 3f d0 d7 df 50 18   ·d·P·,·: 9·?···P·
```

HTTP response message [URL#3]

a. What is the Internet address of the selected server? What is the Internet address of your computer that sent the HTTP GET message?

Internet address of Server : 172.217.18.35
Internet address of my computer : 192.168.1.100

b. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?

Both server and my browser running HTTP 1.1

c. What languages (if any) does your browser indicate that it can accept to the server?

ar-AE and en-US (Arabic and English)

d. What is the status code returned from the server to your browser?

Status code : 404 , status phrase : Not Found

e. When was the HTML file that you are retrieving last modified at the server?

I don't have last_modified in this response message.

f. How many bytes of content are being returned to your browser?

117 bytes

g. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name them.

No. The raw data in the packet content window appears to match up exactly with what is shown in the packet-listing window