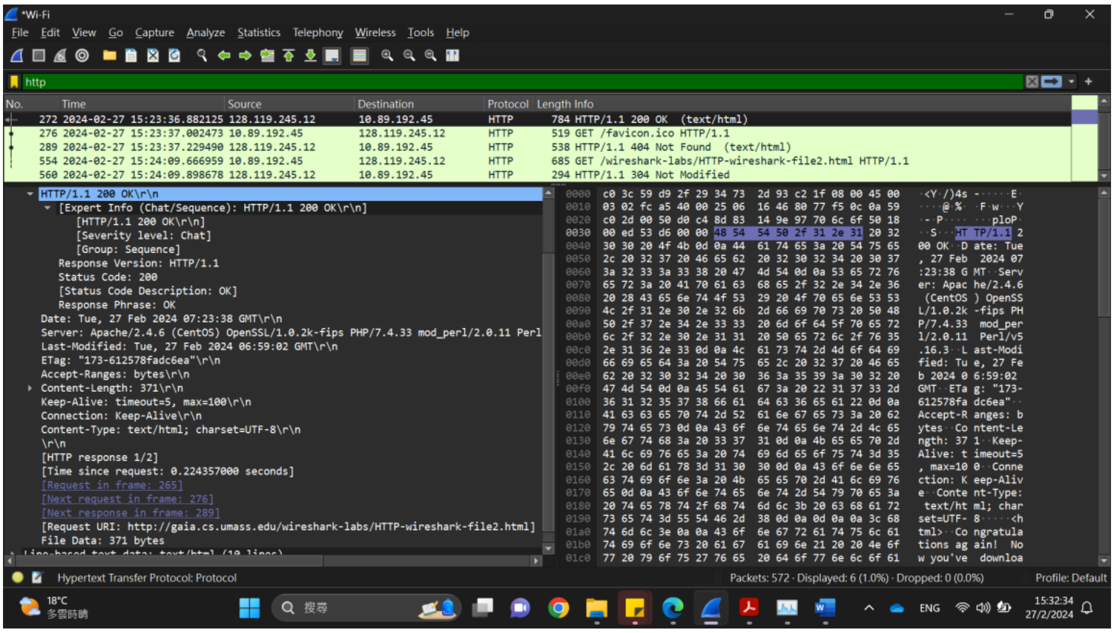
Name: CHAN, Chun Hin
Student ID: 20853893
Email: chchanec@connect.ust.hk

Wireshark Lab: HTTP

Part 2:

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?



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

http

```
No.  Time                        Source          Destination     Protocol Length Info
 272 2024-02-27 15:23:36.882125 128.119.245.12  10.89.192.45    HTTP     784 HTTP/1.1 200 OK  (text/html)
 276 2024-02-27 15:23:37.002473 10.89.192.45    128.119.245.12  HTTP     519 GET /favicon.ico HTTP/1.1
 289 2024-02-27 15:23:37.229490 128.119.245.12  10.89.192.45    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
 554 2024-02-27 15:24:09.666959 10.89.192.45    128.119.245.12  HTTP     685 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 560 2024-02-27 15:24:09.898678 128.119.245.12  10.89.192.45    HTTP     294 HTTP/1.1 304 Not Modified
```

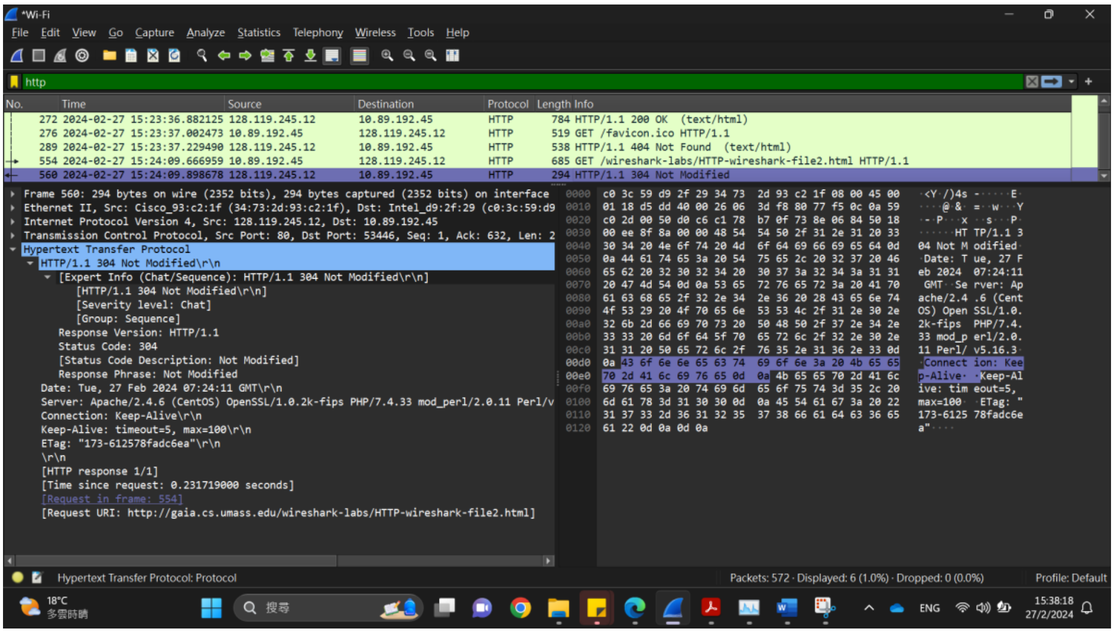
```
HTTP/1.1 200 OK\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
Date: Tue, 27 Feb 2024 07:23:38 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl
Last-Modified: Tue, 27 Feb 2024 06:59:02 GMT\r\n
ETag: "173-612578fadc6ea"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 371\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.224357000 seconds]
[Request in frame: 265]
[Next request in frame: 276]
[Next response in frame: 289]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
Line-based text data: text/html (10 lines)
```

```
0000  c0 3c 59 d9 2f 29 34 73  2d 93 c2 1f 08 00 45 00   ·<Y·/)4s -·····E·
0010  03 02 fc a5 40 00 25 06  16 46 80 77 f5 0c 0a 59   ····@·%· ·F·w···Y
0020  c0 2d 00 50 d0 c4 8d 83  14 9e 97 70 6c 6f 50 18   ·-·P···· ···ploP·
0030  00 ed 53 d6 00 00 48 54  54 50 2f 31 2e 31 20 32   ··S···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 75 65   00 OK··D ate: Tue
0050  2c 20 32 37 20 46 65 62  20 32 30 32 34 20 30 37   , 27 Feb  2024 07
0060  3a 32 33 3a 33 38 20 47  4d 54 0d 0a 53 65 72 76   :23:38 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64 5f 70 65 72   P/7.4.33  mod_per
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 35   l/2.0.11  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 54 75  65 2c 20 32 37 20 46 65   fied: Tu e, 27 Fe
00e0  62 20 32 30 32 34 20 30  36 3a 35 39 3a 30 32 20   b 2024 0 6:59:02
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 31 37 33 2d   GMT··ETa g: "173-
0100  36 31 32 35 37 38 66 61  64 63 36 65 61 22 0d 0a   612578fa dc6ea"··
0110  41 63 63 65 70 74 2d 52  61 6e 67 65 73 3a 20 62   Accept-R anges: b
0120  79 74 65 73 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   ytes··Co ntent-Le
0130  6e 67 74 68 3a 20 33 37  31 0d 0a 4b 65 65 70 2d   ngth: 37 1··Keep-
0140  41 6c 69 76 65 3a 20 74  69 6d 65 6f 75 74 3d 35   Alive: t imeout=5
0150  2c 20 6d 61 78 3d 31 30  30 0d 0a 43 6f 6e 6e 65   , max=10 0··Conne
0160  63 74 69 6f 6e 3a 20 4b  65 65 70 2d 41 6c 69 76   ction: K eep-Aliv
0170  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   e··Conte nt-Type:
0180  20 74 65 78 74 2f 68 74  6d 6c 3b 20 63 68 61 72    text/ht ml; char
0190  73 65 74 3d 55 54 46 2d  38 0d 0a 0d 0a 0a 3c 68   set=UTF- 8·····<h
01a0  74 6d 6c 3e 0a 0a 43 6f  6e 67 72 61 74 75 6c 61   tml>··Co ngratula
01b0  74 69 6f 6e 73 20 61 67  61 69 6e 21 20 20 4e 6f   tions ag ain!  No
01c0  77 20 79 6f 75 27 76 65  20 64 6f 77 6e 6c 6f 61   w you've  downloa
```

Hypertext Transfer Protocol: Protocol   Packets: 572 · Displayed: 6 (1.0%) · Dropped: 0 (0.0%)   Profile: Default

Yes, the server explicitly return the contents of the file. It is because the status code I received is 200, and its corresponding status code description and phrase returned is “OK”. Also, I received a content length of 371 and a file data of 371 bytes, which implies the server is explicitly returning the contents of the html file.

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.


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

```
No.  Time                       Source          Destination     Protocol Length Info
 272 2024-02-27 15:23:36.882125 128.119.245.12  10.89.192.45    HTTP     784 HTTP/1.1 200 OK  (text/html)
 276 2024-02-27 15:23:37.002473 10.89.192.45    128.119.245.12  HTTP     519 GET /favicon.ico HTTP/1.1
 289 2024-02-27 15:23:37.229490 128.119.245.12  10.89.192.45    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
 554 2024-02-27 15:24:09.666959 10.89.192.45    128.119.245.12  HTTP     685 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 560 2024-02-27 15:24:09.898678 128.119.245.12  10.89.192.45    HTTP     294 HTTP/1.1 304 Not Modified
```

```
> Frame 560: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface
> Ethernet II, Src: Cisco_93:c2:1f (34:73:2d:93:c2:1f), Dst: Intel_d9:2f:29 (c0:3c:59:d9
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.89.192.45
> Transmission Control Protocol, Src Port: 80, Dst Port: 53446, Seq: 1, Ack: 632, Len: 2
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        [HTTP/1.1 304 Not Modified\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Tue, 27 Feb 2024 07:24:11 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-612578fadc6ea"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.231719000 seconds]
    [Request in frame: 554]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

```
0000  c0 3c 59 d9 2f 29 34 73  2d 93 c2 1f 08 00 45 00   ·<Y·/)4s -·····E·
0010  01 18 d5 dd 40 00 26 06  3d f8 80 77 f5 0c 0a 59   ····@·&· =··w···Y
0020  c0 2d 00 50 d0 c6 c1 78  b7 0f 73 8e 06 84 50 18   ·-·P···x ··s···P·
0030  00 ee 8f 8a 00 00 48 54  54 50 2f 31 2e 31 20 33   ······HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified·
0050  0a 44 61 74 65 3a 20 54  75 65 2c 20 32 37 20 46   ·Date: T ue, 27 F
0060  65 62 20 32 30 32 34 20  30 37 3a 32 34 3a 31 31   eb 2024  07:24:11
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0080  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
00b0  33 33 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   33 mod_p erl/2.0.
00c0  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
00d0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 4b 65 65   ·Connect ion: Kee
00e0  70 2d 41 6c 69 76 65 0d  0a 4b 65 65 70 2d 41 6c   p-Alive· ·Keep-Al
00f0  69 76 65 3a 20 74 69 6d  65 6f 75 74 3d 35 2c 20   ive: tim eout=5,
0100  6d 61 78 3d 31 30 30 0d  0a 45 54 61 67 3a 20 22   max=100· ·ETag: "
0110  31 37 33 2d 36 31 32 35  37 38 66 61 64 63 36 65   173-6125 78fadc6e
0120  61 22 0d 0a 0d 0a                                  a"····
```

Hypertext Transfer Protocol: Protocol

Packets: 572 · Displayed: 6 (1.0%) · Dropped: 0 (0.0%)

Profile: Default

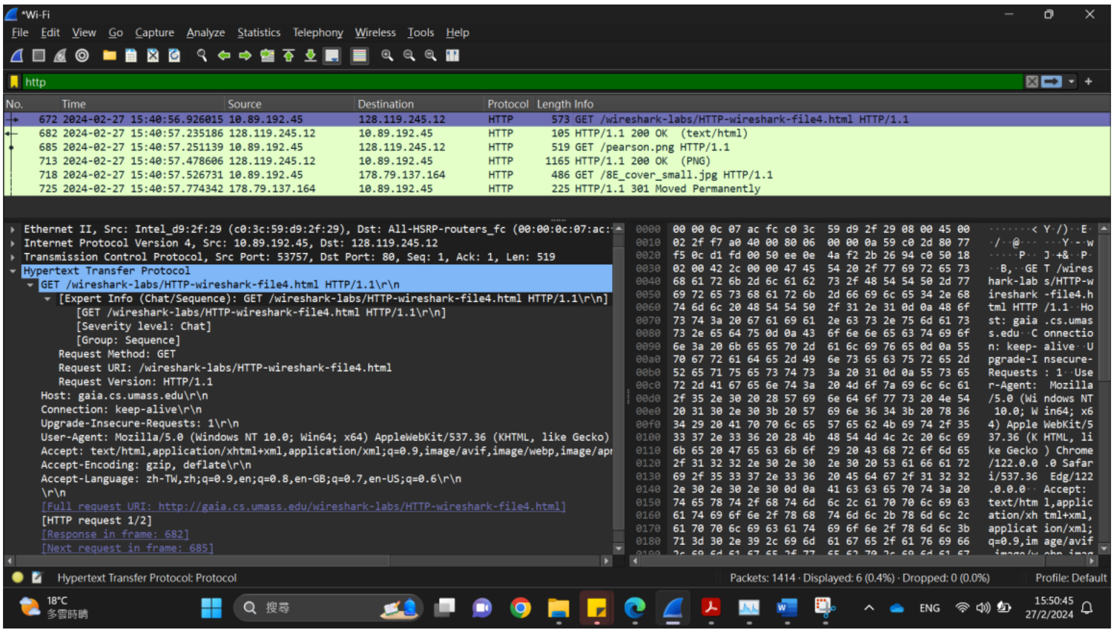
The HTTP status code returned from the server in response to the second HTTP GET is 304.

The phrase returned from the server in response to the second HTTP GET is “Not Modified”.

The server did not explicitly return the contents of the file, because based on the returned status code 304 and the corresponding phrase “Not Modified”, if the server knows that this website has not been modified, it will just returned the cached version of the same website to us instead.

Part 4:

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?


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

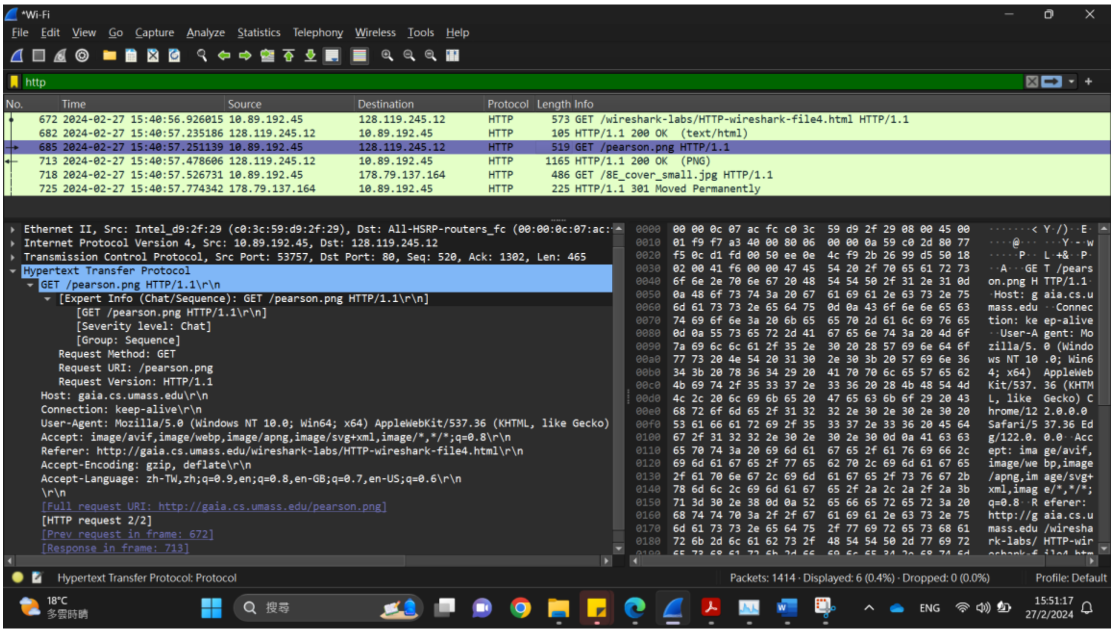
```
No.  Time                       Source          Destination     Protocol Length Info
672 2024-02-27 15:40:56.926015 10.89.192.45    128.119.245.12  HTTP      573 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
682 2024-02-27 15:40:57.235186 128.119.245.12  10.89.192.45    HTTP      105 HTTP/1.1 200 OK  (text/html)
685 2024-02-27 15:40:57.251139 10.89.192.45    128.119.245.12  HTTP      519 GET /pearson.png HTTP/1.1
713 2024-02-27 15:40:57.478606 128.119.245.12  10.89.192.45    HTTP     1165 HTTP/1.1 200 OK  (PNG)
718 2024-02-27 15:40:57.526731 10.89.192.45    178.79.137.164  HTTP      486 GET /8E_cover_small.jpg HTTP/1.1
725 2024-02-27 15:40:57.774342 178.79.137.164  10.89.192.45    HTTP      225 HTTP/1.1 301 Moved Permanently
```

```
Ethernet II, Src: Intel_d9:2f:29 (c0:3c:59:d9:2f:29), Dst: All-HSRP-routers_fc (00:00:0c:07:ac:
Internet Protocol Version 4, Src: 10.89.192.45, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53757, Dst Port: 80, Seq: 1, Ack: 1, Len: 519
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
      [GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file4.html
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\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)
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apr
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-TW,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
  [HTTP request 1/2]
  [Response in frame: 682]
  [Next request in frame: 685]
```

```
0000  00 00 0c 07 ac fc c0 3c  59 d9 2f 29 08 00 45 00   ·······< Y·/)··E·
0010  02 2f f7 a0 40 00 80 06  00 00 0a 59 c0 2d 80 77   ·/··@··· ···Y·-·w
0020  f5 0c d1 fd 00 50 ee 0e  4a f2 2b 26 94 c0 50 18   ·····P·· J·+&··P·
0030  02 00 42 2c 00 00 47 45  54 20 2f 77 69 72 65 73   ··B,··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 34 2e 68   ireshark -file4.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0120  2f 31 32 32 2e 30 2e 30  2e 30 20 53 61 66 61 72   /122.0.0 .0 Safar
0130  69 2f 35 33 37 2e 33 36  20 45 64 67 2f 31 32 32   i/537.36  Edg/122
0140  2e 30 2e 30 2e 30 0d 0a  41 63 63 65 70 74 3a 20   .0.0.0·· Accept: 
0150  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm l,applic
0160  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
0170  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
0180  71 3d 30 2e 39 2c 69 6d  61 67 65 2f 61 76 69 66   q=0.9,im age/avif
```

Hypertext Transfer Protocol: Protocol
Packets: 1414 · Displayed: 6 (0.4%) · Dropped: 0 (0.0%)
Profile: Default

18°C
多雲時晴
搜尋
ENG
15:50:45
27/2/2024

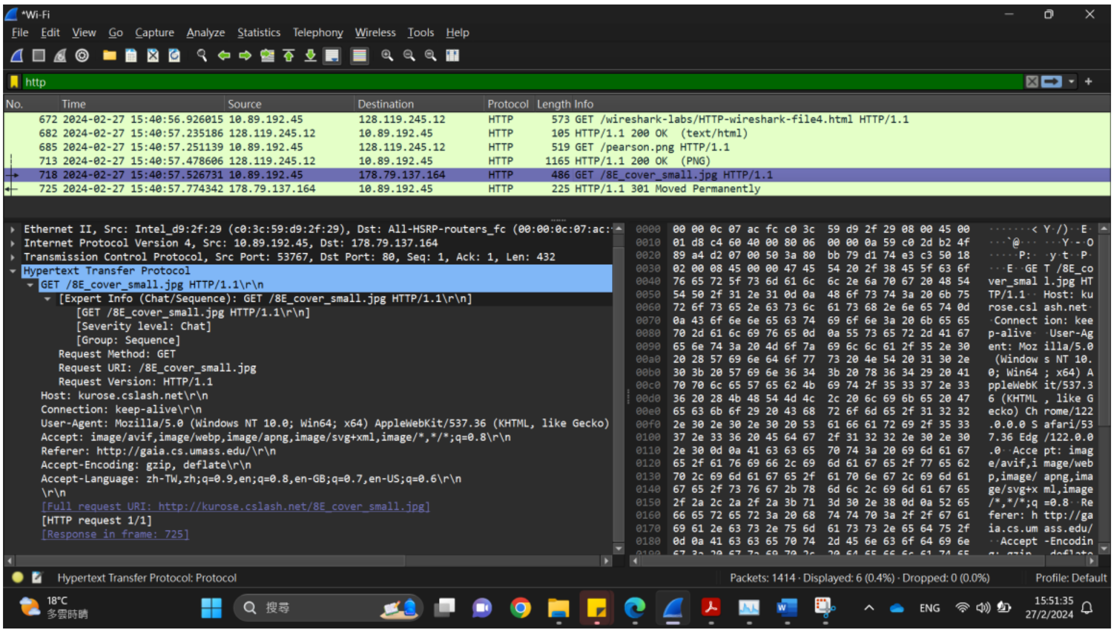

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time                       Source          Destination     Protocol Length Info
672 2024-02-27 15:40:56.926015 10.89.192.45    128.119.245.12  HTTP      573 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
682 2024-02-27 15:40:57.235186 128.119.245.12  10.89.192.45    HTTP      105 HTTP/1.1 200 OK  (text/html)
685 2024-02-27 15:40:57.251139 10.89.192.45    128.119.245.12  HTTP      519 GET /pearson.png HTTP/1.1
713 2024-02-27 15:40:57.478606 128.119.245.12  10.89.192.45    HTTP     1165 HTTP/1.1 200 OK  (PNG)
718 2024-02-27 15:40:57.526731 10.89.192.45    178.79.137.164  HTTP      486 GET /8E_cover_small.jpg HTTP/1.1
725 2024-02-27 15:40:57.774342 178.79.137.164  10.89.192.45    HTTP      225 HTTP/1.1 301 Moved Permanently
```

```
Ethernet II, Src: Intel_d9:2f:29 (c0:3c:59:d9:2f:29), Dst: All-HSRP-routers_fc (00:00:0c:07:ac:
Internet Protocol Version 4, Src: 10.89.192.45, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53757, Dst Port: 80, Seq: 520, Ack: 1302, Len: 465
Hypertext Transfer Protocol
  GET /pearson.png HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /pearson.png HTTP/1.1\r\n]
      [GET /pearson.png HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /pearson.png
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
  Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-TW,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/pearson.png]
  [HTTP request 2/2]
  [Prev request in frame: 672]
  [Response in frame: 713]
```

```
0000  00 00 0c 07 ac fc c0 3c  59 d9 2f 29 08 00 45 00   ·······< Y·/)··E·
0010  01 f9 f7 a3 40 00 80 06  00 00 0a 59 c0 2d 80 77   ····@··· ···Y·-·w
0020  f5 0c d1 fd 00 50 ee 0e  4c f9 2b 26 99 d5 50 18   ·····P·· L·+&··P·
0030  02 00 41 f6 00 00 47 45  54 20 2f 70 65 61 72 73   ··A···GE T /pears
0040  6f 6e 2e 70 6e 67 20 48  54 54 50 2f 31 2e 31 0d   on.png H TTP/1.1·
0050  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   ·Host: g aia.cs.u
0060  6d 61 73 73 2e 65 64 75  0d 0a 43 6f 6e 6e 65 63   mass.edu ··Connec
0070  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0080  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
0090  7a 69 6c 6c 61 2f 35 2e  30 20 28 57 69 6e 64 6f   zilla/5. 0 (Windo
00a0  77 73 20 4e 54 20 31 30  2e 30 3b 20 57 69 6e 36   ws NT 10 .0; Win6
00b0  34 3b 20 78 36 34 29 20  41 70 70 6c 65 57 65 62   4; x64)  AppleWeb
00c0  4b 69 74 2f 35 33 37 2e  33 36 20 28 4b 48 54 4d   Kit/537. 36 (KHTM
00d0  4c 2c 20 6c 69 6b 65 20  47 65 63 6b 6f 29 20 43   L, like  Gecko) C
00e0  68 72 6f 6d 65 2f 31 32  32 2e 30 2e 30 2e 30 20   hrome/12 2.0.0.0 
00f0  53 61 66 61 72 69 2f 35  33 37 2e 33 36 20 45 64   Safari/5 37.36 Ed
0100  67 2f 31 32 32 2e 30 2e  30 2e 30 0d 0a 41 63 63   g/122.0. 0.0··Acc
0110  65 70 74 3a 20 69 6d 61  67 65 2f 61 76 69 66 2c   ept: ima ge/avif,
0120  69 6d 61 67 65 2f 77 65  62 70 2c 69 6d 61 67 65   image/we bp,image
0130  2f 61 70 6e 67 2c 69 6d  61 67 65 2f 73 76 67 2b   /apng,im age/svg+
0140  78 6d 6c 2c 69 6d 61 67  65 2f 2a 2c 2a 2f 2a 3b   xml,imag e/*,*/*;
0150  71 3d 30 2e 38 0d 0a 52  65 66 65 72 65 72 3a 20   q=0.8··R eferer: 
0160  68 74 74 70 3a 2f 2f 67  61 69 61 2e 63 73 2e 75   http://g aia.cs.u
0170  6d 61 73 73 2e 65 64 75  2f 77 69 72 65 73 68 61   mass.edu /wiresha
0180  72 6b 2d 6c 61 62 73 2f  48 54 54 50 2d 77 69 72   rk-labs/ HTTP-wir
```

Hypertext Transfer Protocol: Protocol
Packets: 1414 · Displayed: 6 (0.4%) · Dropped: 0 (0.0%)
Profile: Default


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

```
No.  Time                        Source          Destination     Protocol Length Info
 672 2024-02-27 15:40:56.926015 10.89.192.45    128.119.245.12  HTTP      573 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 682 2024-02-27 15:40:57.235186 128.119.245.12  10.89.192.45    HTTP      105 HTTP/1.1 200 OK  (text/html)
 685 2024-02-27 15:40:57.251139 10.89.192.45    128.119.245.12  HTTP      519 GET /pearson.png HTTP/1.1
 713 2024-02-27 15:40:57.478606 128.119.245.12  10.89.192.45    HTTP     1165 HTTP/1.1 200 OK  (PNG)
 718 2024-02-27 15:40:57.526731 10.89.192.45    178.79.137.164  HTTP      486 GET /8E_cover_small.jpg HTTP/1.1
 725 2024-02-27 15:40:57.774342 178.79.137.164  10.89.192.45    HTTP      225 HTTP/1.1 301 Moved Permanently
```

```
> Ethernet II, Src: Intel_d9:2f:29 (c0:3c:59:d9:2f:29), Dst: All-HSRP-routers_fc (00:00:0c:07:ac:
> Internet Protocol Version 4, Src: 10.89.192.45, Dst: 178.79.137.164
> Transmission Control Protocol, Src Port: 53767, Dst Port: 80, Seq: 1, Ack: 1, Len: 432
v Hypertext Transfer Protocol
  v GET /8E_cover_small.jpg HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /8E_cover_small.jpg HTTP/1.1\r\n]
        [GET /8E_cover_small.jpg HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /8E_cover_small.jpg
      Request Version: HTTP/1.1
    Host: kurose.cslash.net\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-TW,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
    \r\n
    [Full request URI: http://kurose.cslash.net/8E_cover_small.jpg]
    [HTTP request 1/1]
    [Response in frame: 725]
```

```
0000  00 00 0c 07 ac fc c0 3c  59 d9 2f 29 08 00 45 00   ·······< Y·/)··E·
0010  01 d8 c4 60 40 00 80 06  00 00 0a 59 c0 2d b2 4f   ···`@··· ···Y·-·O
0020  89 a4 d2 07 00 50 3a 80  bb 79 d1 74 e3 c3 50 18   ·····P:· ·y·t··P·
0030  02 00 08 45 00 00 47 45  54 20 2f 38 45 5f 63 6f   ···E··GE T /8E_co
0040  76 65 72 5f 73 6d 61 6c  6c 2e 6a 70 67 20 48 54   ver_smal l.jpg HT
0050  54 50 2f 31 2e 31 0d 0a  48 6f 73 74 3a 20 6b 75   TP/1.1·· Host: ku
0060  72 6f 73 65 2e 63 73 6c  61 73 68 2e 6e 65 74 0d   rose.csl ash.net·
0070  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 6b 65 65   ·Connect ion: kee
0080  70 2d 61 6c 69 76 65 0d  0a 55 73 65 72 2d 41 67   p-alive· ·User-Ag
0090  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00a0  20 28 57 69 6e 64 6f 77  73 20 4e 54 20 31 30 2e    (Window s NT 10.
00b0  30 3b 20 57 69 6e 36 34  3b 20 78 36 34 29 20 41   0; Win64 ; x64) A
00c0  70 70 6c 65 57 65 62 4b  69 74 2f 35 33 37 2e 33   ppleWebK it/537.3
00d0  36 20 28 4b 48 54 4d 4c  2c 20 6c 69 6b 65 20 47   6 (KHTML , like G
00e0  65 63 6b 6f 29 20 43 68  72 6f 6d 65 2f 31 32 32   ecko) Ch rome/122
00f0  2e 30 2e 30 2e 30 20 53  61 66 61 72 69 2f 35 33   .0.0.0 S afari/53
0100  37 2e 33 36 20 45 64 67  2f 31 32 32 2e 30 2e 30   7.36 Edg /122.0.0
0110  2e 30 0d 0a 41 63 63 65  70 74 3a 20 69 6d 61 67   .0··Acce pt: imag
0120  65 2f 61 76 69 66 2c 69  6d 61 67 65 2f 77 65 62   e/avif,i mage/web
0130  70 2c 69 6d 61 67 65 2f  61 70 6e 67 2c 69 6d 61   p,image/ apng,ima
0140  67 65 2f 73 76 67 2b 78  6d 6c 2c 69 6d 61 67 65   ge/svg+x ml,image
0150  2f 2a 2c 2a 2f 2a 3b 71  3d 30 2e 38 0d 0a 52 65   /*,*/*;q =0.8··Re
0160  66 65 72 65 72 3a 20 68  74 74 70 3a 2f 2f 67 61   ferer: h ttp://ga
0170  69 61 2e 63 73 2e 75 6d  61 73 73 2e 65 64 75 2f   ia.cs.um ass.edu/
0180  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -Encodin
```

```
Hypertext Transfer Protocol: Protocol        Packets: 1414 · Displayed: 6 (0.4%) · Dropped: 0 (0.0%)        Profile: Default
```

My browser sent 3 HTTP GET messages.

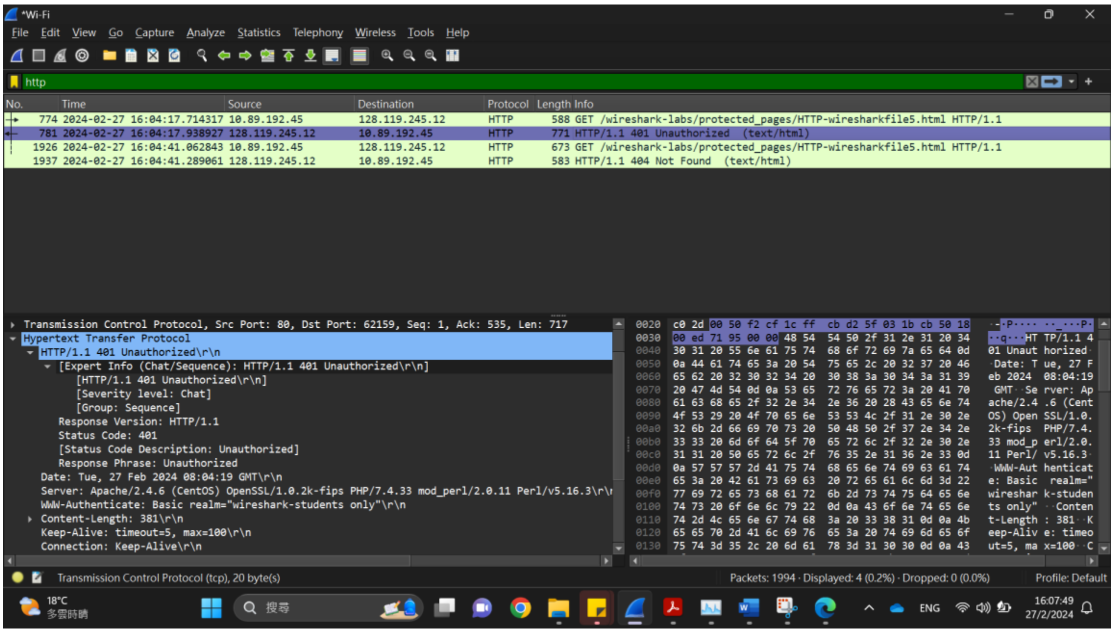
The first GET request is sent to the Internet address 128.119.245.12.

The second GET request is sent to the Internet address 128.119.245.12.

The third GET request is sent to the Internet address 178.79.137.164.

Part 5:

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?


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

```
No.  Time                        Source          Destination     Protocol Length Info
 774 2024-02-27 16:04:17.714317 10.89.192.45    128.119.245.12  HTTP      588 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
 781 2024-02-27 16:04:17.938927 128.119.245.12  10.89.192.45    HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
1926 2024-02-27 16:04:41.062843 10.89.192.45    128.119.245.12  HTTP      673 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
1937 2024-02-27 16:04:41.289061 128.119.245.12  10.89.192.45    HTTP      583 HTTP/1.1 404 Not Found  (text/html)
```

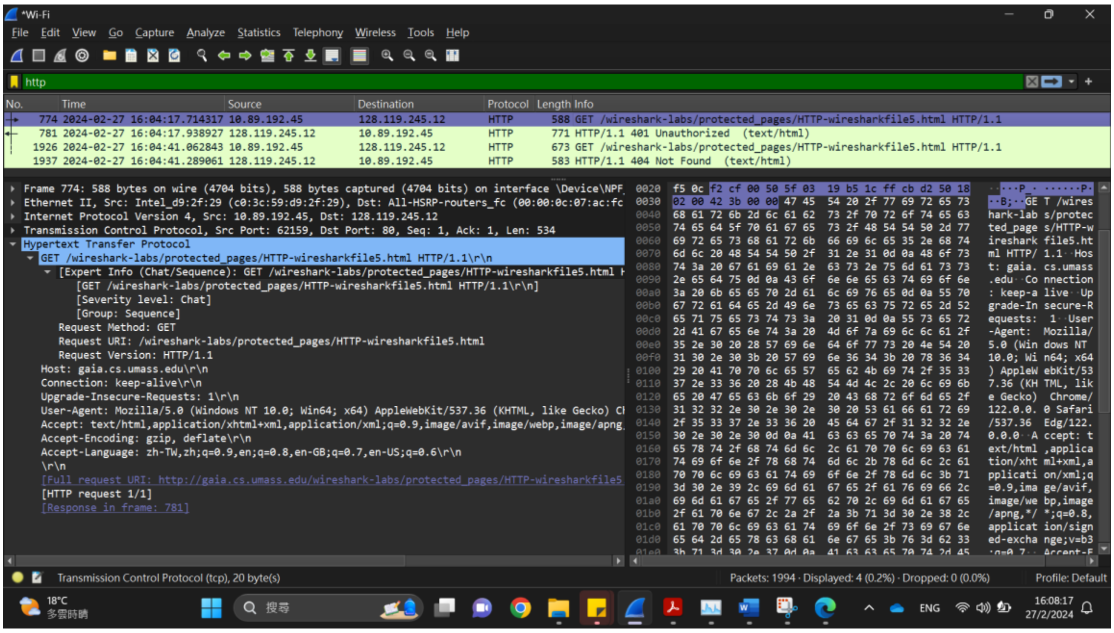
```
> Transmission Control Protocol, Src Port: 80, Dst Port: 62159, Seq: 1, Ack: 535, Len: 717
v Hypertext Transfer Protocol
  v HTTP/1.1 401 Unauthorized\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
        [HTTP/1.1 401 Unauthorized\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
    Date: Tue, 27 Feb 2024 08:04:19 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  > Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
```

```
0020  c0 2d 00 50 f2 cf 1c ff  cb d2 5f 03 1b cb 50 18   ·-·P···· ··_···P·
0030  00 ed 71 95 00 00 48 54  54 50 2f 31 2e 31 20 34   ··q···HT TP/1.1 4
0040  30 31 20 55 6e 61 75 74  68 6f 72 69 7a 65 64 0d   01 Unaut horized·
0050  0a 44 61 74 65 3a 20 54  75 65 2c 20 32 37 20 46   ·Date: T ue, 27 F
0060  65 62 20 32 30 32 34 20  30 38 3a 30 34 3a 31 39   eb 2024  08:04:19
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0080  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
00b0  33 33 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   33 mod_p erl/2.0.
00c0  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
00d0  0a 57 57 57 2d 41 75 74  68 65 6e 74 69 63 61 74   ·WWW-Aut henticat
00e0  65 3a 20 42 61 73 69 63  20 72 65 61 6c 6d 3d 22   e: Basic  realm="
00f0  77 69 72 65 73 68 61 72  6b 2d 73 74 75 64 65 6e   wireshar k-studen
0100  74 73 20 6f 6e 6c 79 22  0d 0a 43 6f 6e 74 65 6e   ts only" ··Conten
0110  74 2d 4c 65 6e 67 74 68  3a 20 33 38 31 0d 0a 4b   t-Length : 381··K
0120  65 65 70 2d 41 6c 69 76  65 3a 20 74 69 6d 65 6f   eep-Aliv e: timeo
0130  75 74 3d 35 2c 20 6d 61  78 3d 31 30 30 0d 0a 43   ut=5, ma x=100··C
```

```
Transmission Control Protocol (tcp), 20 byte(s)        Packets: 1994 · Displayed: 4 (0.2%) · Dropped: 0 (0.0%)        Profile: Default
```

The server's status code is 401, and the phrase is "Unauthorized".

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
18°C
多雲時晴
搜尋
ENG
16:08:17
27/2/2024

```
No.   Time                       Source          Destination     Protocol Length Info
  774 2024-02-27 16:04:17.714317 10.89.192.45    128.119.245.12  HTTP     588 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
  781 2024-02-27 16:04:17.938927 128.119.245.12  10.89.192.45    HTTP     771 HTTP/1.1 401 Unauthorized  (text/html)
 1926 2024-02-27 16:04:41.062843 10.89.192.45    128.119.245.12  HTTP     673 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
 1937 2024-02-27 16:04:41.289061 128.119.245.12  10.89.192.45    HTTP     583 HTTP/1.1 404 Not Found  (text/html)
```

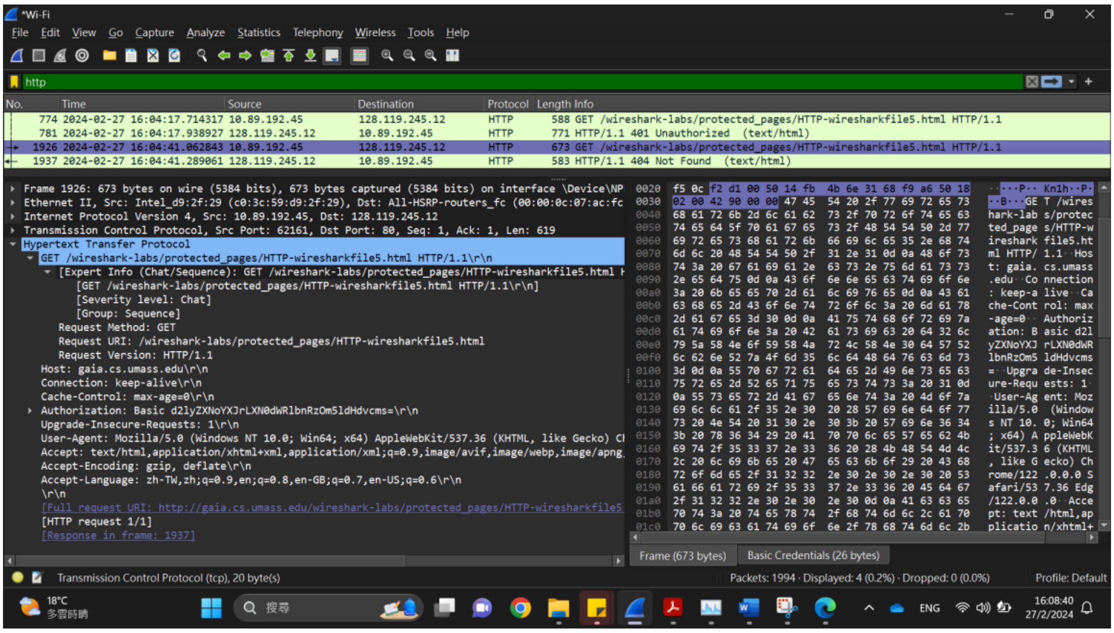
```
Frame 774: 588 bytes on wire (4704 bits), 588 bytes captured (4704 bits) on interface \Device\NPF_
Ethernet II, Src: Intel_d9:2f:29 (c0:3c:59:d9:2f:29), Dst: All-HSRP-routers_fc (00:00:0c:07:ac:fc
Internet Protocol Version 4, Src: 10.89.192.45, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62159, Dst Port: 80, Seq: 1, Ack: 1, Len: 534
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html H
      [GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\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) Ch
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-TW,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5
  [HTTP request 1/1]
  [Response in frame: 781]
```

```
0020  f5 0c f2 cf 00 50 5f 03  19 b5 1c ff cb d2 50 18   ·····P_· ······P·
0030  02 00 42 3b 00 00 47 45  54 20 2f 77 69 72 65 73   ··B;··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec
0050  74 65 64 5f 70 61 67 65  73 2f 48 54 54 50 2d 77   ted_page s/HTTP-w
0060  69 72 65 73 68 61 72 6b  66 69 6c 65 35 2e 68 74   ireshark file5.ht
0070  6d 6c 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   ml HTTP/ 1.1··Hos
0080  74 3a 20 67 61 69 61 2e  63 73 2e 75 6d 61 73 73   t: gaia. cs.umass
0090  2e 65 64 75 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .edu··Co nnection
00a0  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 55 70   : keep-a live··Up
00b0  67 72 61 64 65 2d 49 6e  73 65 63 75 72 65 2d 52   grade-In secure-R
00c0  65 71 75 65 73 74 73 3a  20 31 0d 0a 55 73 65 72   equests:  1··User
00d0  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00e0  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT 
00f0  31 30 2e 30 3b 20 57 69  6e 36 34 3b 20 78 36 34   10.0; Wi n64; x64
0100  29 20 41 70 70 6c 65 57  65 62 4b 69 74 2f 35 33   ) AppleW ebKit/53
0110  37 2e 33 36 20 28 4b 48  54 4d 4c 2c 20 6c 69 6b   7.36 (KH TML, lik
0120  65 20 47 65 63 6b 6f 29  20 43 68 72 6f 6d 65 2f   e Gecko)  Chrome/
0130  31 32 32 2e 30 2e 30 2e  30 20 53 61 66 61 72 69   122.0.0. 0 Safari
0140  2f 35 33 37 2e 33 36 20  45 64 67 2f 31 32 32 2e   /537.36  Edg/122.
0150  30 2e 30 2e 30 0d 0a 41  63 63 65 70 74 3a 20 74   0.0.0··A ccept: t
0160  65 78 74 2f 68 74 6d 6c  2c 61 70 70 6c 69 63 61   ext/html ,applica
0170  74 69 6f 6e 2f 78 68 74  6d 6c 2b 78 6d 6c 2c 61   tion/xht ml+xml,a
0180  70 70 6c 69 63 61 74 69  6f 6e 2f 78 6d 6c 3b 71   pplicati on/xml;q
0190  3d 30 2e 39 2c 69 6d 61  67 65 2f 61 76 69 66 2c   =0.9,ima ge/avif,
01a0  69 6d 61 67 65 2f 77 65  62 70 2c 69 6d 61 67 65   image/we bp,image
01b0  2f 61 70 6e 67 2c 2a 2f  2a 3b 71 3d 30 2e 38 2c   /apng,*/ *;q=0.8,
01c0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 73 69 67 6e   applicat ion/sign
01d0  65 64 2d 65 78 63 68 61  6e 67 65 3b 76 3d 62 33   ed-excha nge;v=b3
01e0  3b 71 3d 30 2e 37 0d 0a  41 63 63 65 70 74 2d 45   ;q=0.7·· Accept-E
```

Transmission Control Protocol (tcp), 20 byte(s)

Packets: 1994 · Displayed: 4 (0.2%) · Dropped: 0 (0.0%)

Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
18°C
多雲時晴
搜尋
ENG
16:08:40
27/2/2024

```
No.   Time                       Source          Destination     Protocol Length Info
  774 2024-02-27 16:04:17.714317 10.89.192.45    128.119.245.12  HTTP     588 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
  781 2024-02-27 16:04:17.938927 128.119.245.12  10.89.192.45    HTTP     771 HTTP/1.1 401 Unauthorized  (text/html)
 1926 2024-02-27 16:04:41.062843 10.89.192.45    128.119.245.12  HTTP     673 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
 1937 2024-02-27 16:04:41.289061 128.119.245.12  10.89.192.45    HTTP     583 HTTP/1.1 404 Not Found  (text/html)
```

```
Frame 1926: 673 bytes on wire (5384 bits), 673 bytes captured (5384 bits) on interface \Device\NP
Ethernet II, Src: Intel_d9:2f:29 (c0:3c:59:d9:2f:29), Dst: All-HSRP-routers_fc (00:00:0c:07:ac:fc
Internet Protocol Version 4, Src: 10.89.192.45, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62161, Dst Port: 80, Seq: 1, Ack: 1, Len: 619
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html H
      [GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\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) Ch
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-TW,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5
  [HTTP request 1/1]
  [Response in frame: 1937]
```

```
0020  f5 0c f2 d1 00 50 14 fb  4b 6e 31 68 f9 a6 50 18   ·····P·· Kn1h··P·
0030  02 00 42 90 00 00 47 45  54 20 2f 77 69 72 65 73   ··B···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec
0050  74 65 64 5f 70 61 67 65  73 2f 48 54 54 50 2d 77   ted_page s/HTTP-w
0060  69 72 65 73 68 61 72 6b  66 69 6c 65 35 2e 68 74   ireshark file5.ht
0070  6d 6c 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   ml HTTP/ 1.1··Hos
0080  74 3a 20 67 61 69 61 2e  63 73 2e 75 6d 61 73 73   t: gaia. cs.umass
0090  2e 65 64 75 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .edu··Co nnection
00a0  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
00b0  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
00c0  2d 61 67 65 3d 30 0d 0a  41 75 74 68 6f 72 69 7a   -age=0·· Authoriz
00d0  61 74 69 6f 6e 3a 20 42  61 73 69 63 20 64 32 6c   ation: B asic d2l
00e0  79 5a 58 4e 6f 59 58 4a  72 4c 58 4e 30 64 57 52   yZXNoYXJ rLXN0dWR
00f0  6c 62 6e 52 7a 4f 6d 35  6c 64 48 64 76 63 6d 73   lbnRzOm5 ldHdvcms
0100  3d 0d 0a 55 70 67 72 61  64 65 2d 49 6e 73 65 63   =··Upgra de-Insec
0110  75 72 65 2d 52 65 71 75  65 73 74 73 3a 20 31 0d   ure-Requ ests: 1·
0120  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
0130  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
0140  73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
0150  3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
0160  69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
0170  2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
0180  72 6f 6d 65 2f 31 32 32  2e 30 2e 30 2e 30 20 53   rome/122 .0.0.0 S
0190  61 66 61 72 69 2f 35 33  37 2e 33 36 20 45 64 67   afari/53 7.36 Edg
01a0  2f 31 32 32 2e 30 2e 30  2e 30 0d 0a 41 63 63 65   /122.0.0 .0··Acce
01b0  70 74 3a 20 74 65 78 74  2f 68 74 6d 6c 2c 61 70   pt: text /html,ap
01c0  70 6c 69 63 61 74 69 6f  6e 2f 78 68 74 6d 6c 2b   plicatio n/xhtml+
```

Frame (673 bytes) | Basic Credentials (26 bytes)

Transmission Control Protocol (tcp), 20 byte(s)

Packets: 1994 · Displayed: 4 (0.2%) · Dropped: 0 (0.0%)

Profile: Default

The new fields are Cache-Control and Authorization.

Wireshark Lab: DNS

Part 3:

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The DNS query message sent to a IP address 143.89.14.7.
This is the IP address of my default local DNS server.

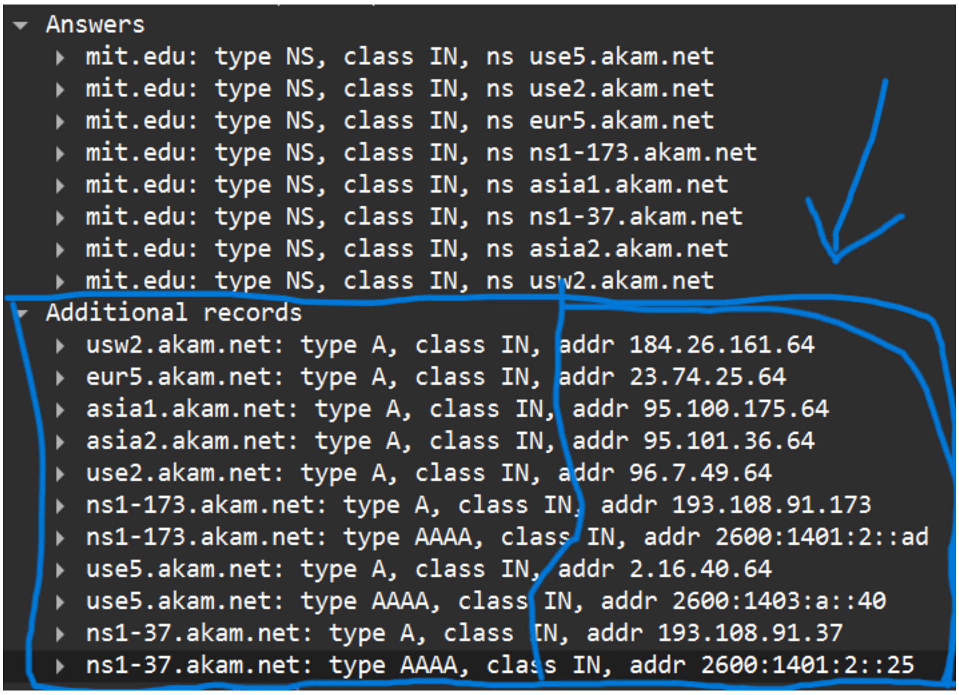
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The “type” of DNS query is NS.
The query message does not contain any “answers”.

18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

The response message provides 8 MIT nameservers, they are:
use5.akam.net
use2.akam.net
eur5.akam.net
ns1-173.akam.net
asia1.akam.net
ns1-37.akam.net
asia2.akam.net
usw2.akam.net

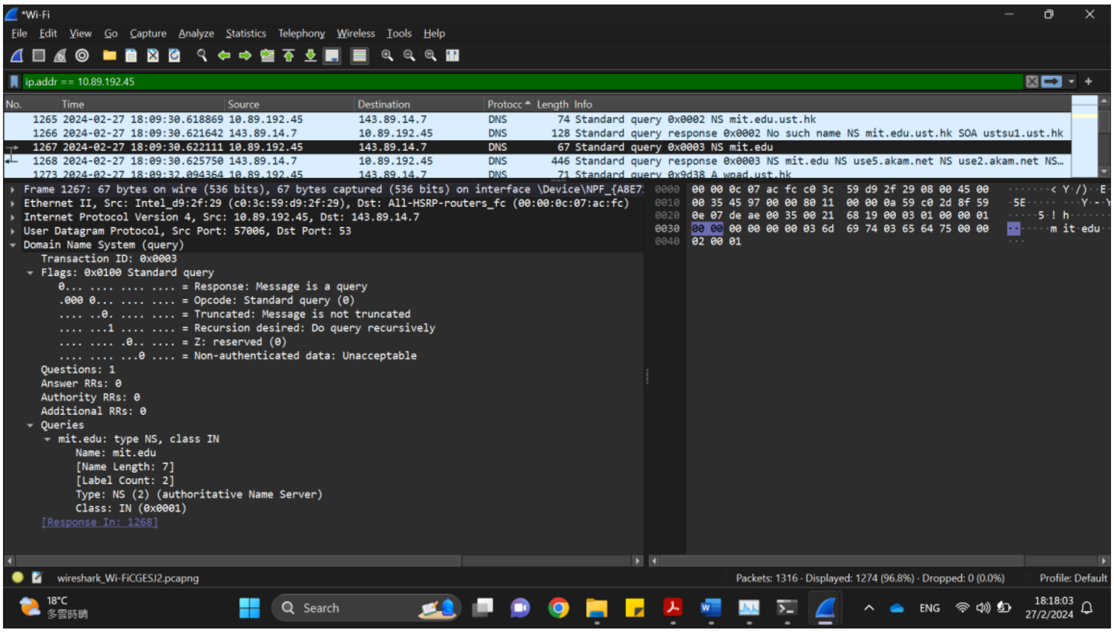
This response message also provides the IP address of the MIT nameservers, they are:



```
Answers
  mit.edu: type NS, class IN, ns use5.akam.net
  mit.edu: type NS, class IN, ns use2.akam.net
  mit.edu: type NS, class IN, ns eur5.akam.net
  mit.edu: type NS, class IN, ns ns1-173.akam.net
  mit.edu: type NS, class IN, ns asia1.akam.net
  mit.edu: type NS, class IN, ns ns1-37.akam.net
  mit.edu: type NS, class IN, ns asia2.akam.net
  mit.edu: type NS, class IN, ns usw2.akam.net
Additional records
  usw2.akam.net: type A, class IN, addr 184.26.161.64
  eur5.akam.net: type A, class IN, addr 23.74.25.64
  asia1.akam.net: type A, class IN, addr 95.100.175.64
  asia2.akam.net: type A, class IN, addr 95.101.36.64
  use2.akam.net: type A, class IN, addr 96.7.49.64
  ns1-173.akam.net: type A, class IN, addr 193.108.91.173
  ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
  use5.akam.net: type A, class IN, addr 2.16.40.64
  use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
  ns1-37.akam.net: type A, class IN, addr 193.108.91.37
  ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
```

19. Provide a screenshot.

(The first screenshot is for Q16 – Q17, while the second to the fourth screenshots are for Q18 – Q19)


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

ip.addr == 10.89.192.45

```
No.   Time                       Source        Destination   Protocol Length Info
1265 2024-02-27 18:09:30.618869 10.89.192.45  143.89.14.7   DNS       74 Standard query 0x0002 NS mit.edu.ust.hk
1266 2024-02-27 18:09:30.621642 143.89.14.7   10.89.192.45  DNS      128 Standard query response 0x0002 No such name NS mit.edu.ust.hk SOA ustsu1.ust.hk
1267 2024-02-27 18:09:30.622111 10.89.192.45  143.89.14.7   DNS       67 Standard query 0x0003 NS mit.edu
1268 2024-02-27 18:09:30.625750 143.89.14.7   10.89.192.45  DNS      446 Standard query response 0x0003 NS mit.edu NS use5.akam.net NS use2.akam.net NS…
1273 2024-02-27 18:09:32.094364 10.89.192.45  143.89.14.7   DNS       71 Standard query 0x9d38 A wpad.ust.hk
```

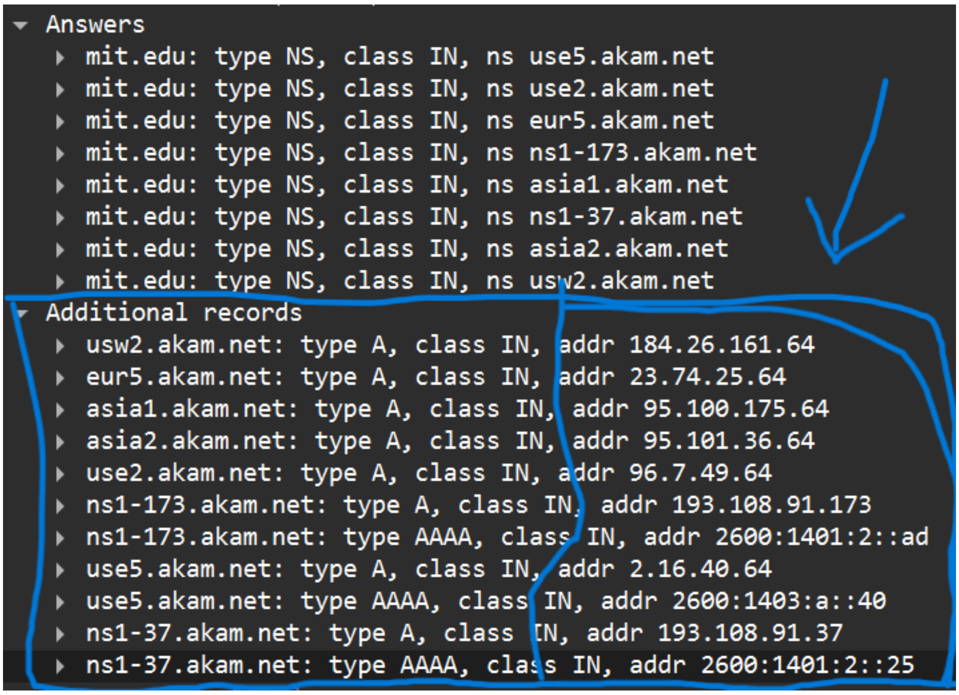
```
Frame 1267: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{A8E7
Ethernet II, Src: Intel_d9:2f:29 (c0:3c:59:d9:2f:29), Dst: All-HSRP-routers_fc (00:00:0c:07:ac:fc)
Internet Protocol Version 4, Src: 10.89.192.45, Dst: 143.89.14.7
User Datagram Protocol, Src Port: 57006, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x0003
    Flags: 0x0100 Standard query
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        mit.edu: type NS, class IN
            Name: mit.edu
            [Name Length: 7]
            [Label Count: 2]
            Type: NS (2) (authoritative Name Server)
            Class: IN (0x0001)
    [Response In: 1268]
```

```
0000  00 00 0c 07 ac fc c0 3c  59 d9 2f 29 08 00 45 00   ·······< Y·/)··E·
0010  00 35 45 97 00 00 80 11  00 00 0a 59 c0 2d 8f 59   ·5E·····  ···Y·-·Y
0020  0e 07 de ae 00 35 00 21  68 19 00 03 01 00 00 01   ·····5·! h·······
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  02 00 01                                           ···
```

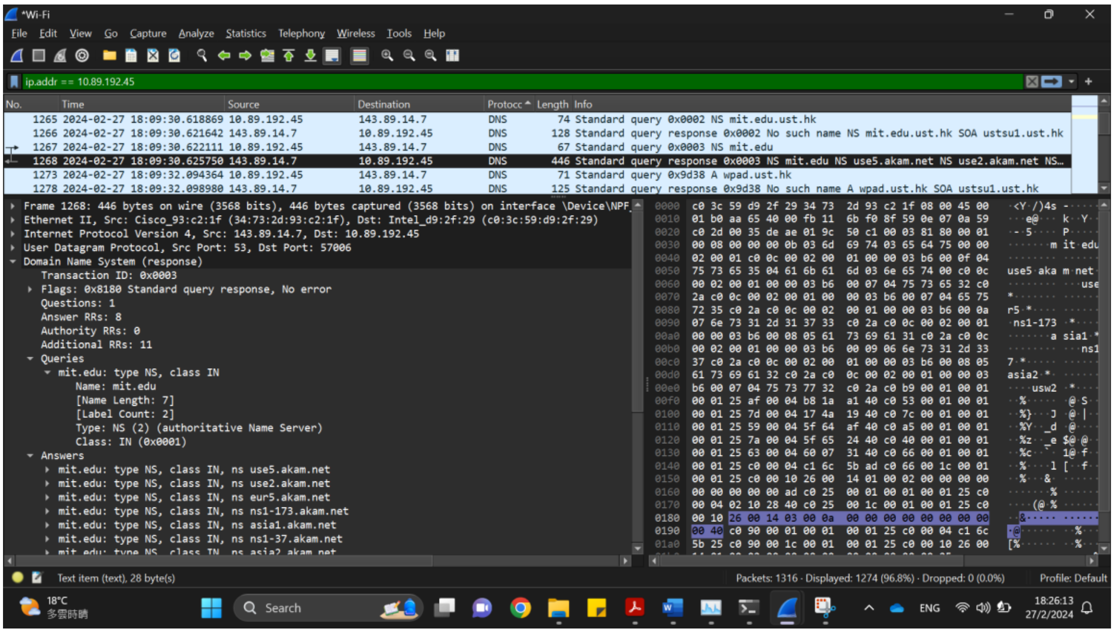
wireshark_Wi-FiCGESJ2.pcapng

Packets: 1316 · Displayed: 1274 (96.8%) · Dropped: 0 (0.0%)

Profile: Default



```
▾ Answers
    ▸ mit.edu: type NS, class IN, ns use5.akam.net
    ▸ mit.edu: type NS, class IN, ns use2.akam.net
    ▸ mit.edu: type NS, class IN, ns eur5.akam.net
    ▸ mit.edu: type NS, class IN, ns ns1-173.akam.net
    ▸ mit.edu: type NS, class IN, ns asia1.akam.net
    ▸ mit.edu: type NS, class IN, ns ns1-37.akam.net
    ▸ mit.edu: type NS, class IN, ns asia2.akam.net
    ▸ mit.edu: type NS, class IN, ns usw2.akam.net
▾ Additional records
    ▸ usw2.akam.net: type A, class IN, addr 184.26.161.64
    ▸ eur5.akam.net: type A, class IN, addr 23.74.25.64
    ▸ asia1.akam.net: type A, class IN, addr 95.100.175.64
    ▸ asia2.akam.net: type A, class IN, addr 95.101.36.64
    ▸ use2.akam.net: type A, class IN, addr 96.7.49.64
    ▸ ns1-173.akam.net: type A, class IN, addr 193.108.91.173
    ▸ ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
    ▸ use5.akam.net: type A, class IN, addr 2.16.40.64
    ▸ use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
    ▸ ns1-37.akam.net: type A, class IN, addr 193.108.91.37
    ▸ ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
```



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

ip.addr == 10.89.192.45

```
No.   Time                       Source         Destination    Protocc  Length Info
 1265 2024-02-27 18:09:30.618869 10.89.192.45   143.89.14.7    DNS          74 Standard query 0x0002 NS mit.edu.ust.hk
 1266 2024-02-27 18:09:30.621642 143.89.14.7    10.89.192.45   DNS         128 Standard query response 0x0002 No such name NS mit.edu.ust.hk SOA ustsu1.ust.hk
 1267 2024-02-27 18:09:30.622111 10.89.192.45   143.89.14.7    DNS          67 Standard query 0x0003 NS mit.edu
 1268 2024-02-27 18:09:30.625750 143.89.14.7    10.89.192.45   DNS         446 Standard query response 0x0003 NS mit.edu NS use5.akam.net NS use2.akam.net NS…
 1273 2024-02-27 18:09:32.094364 10.89.192.45   143.89.14.7    DNS          71 Standard query 0x9d38 A wpad.ust.hk
 1278 2024-02-27 18:09:32.098980 143.89.14.7    10.89.192.45   DNS         125 Standard query response 0x9d38 No such name A wpad.ust.hk SOA ustsu1.ust.hk
```

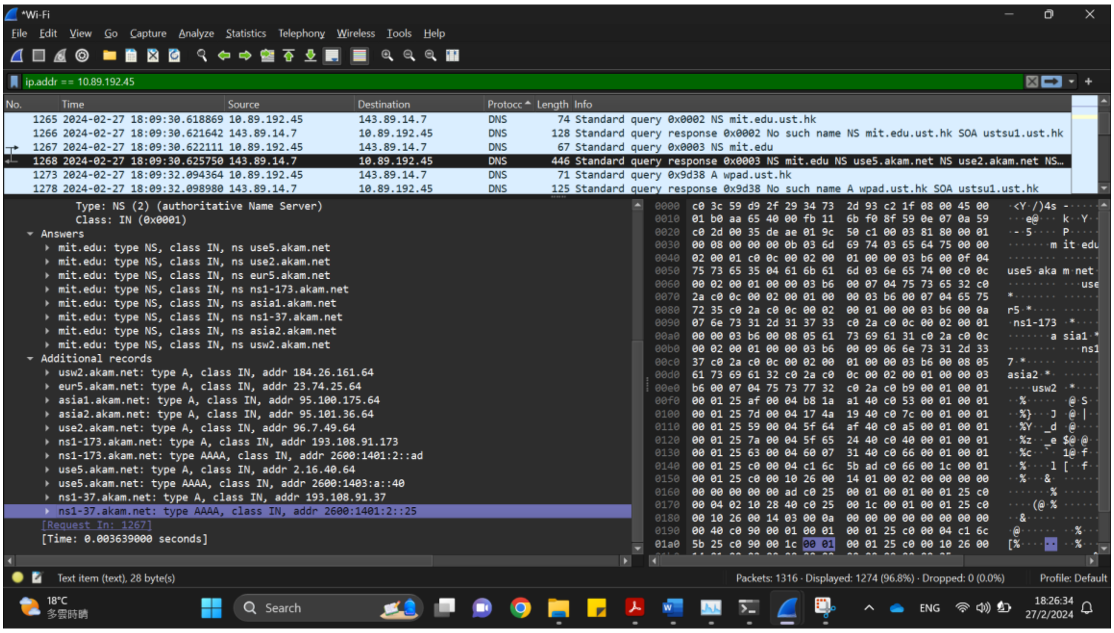
```
▸ Frame 1268: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface \Device\NPF_
▸ Ethernet II, Src: Cisco_93:c2:1f (34:73:2d:93:c2:1f), Dst: Intel_d9:2f:29 (c0:3c:59:d9:2f:29)
▸ Internet Protocol Version 4, Src: 143.89.14.7, Dst: 10.89.192.45
▸ User Datagram Protocol, Src Port: 53, Dst Port: 57006
▾ Domain Name System (response)
    Transaction ID: 0x0003
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 11
  ▾ Queries
    ▾ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
  ▾ Answers
    ▸ mit.edu: type NS, class IN, ns use5.akam.net
    ▸ mit.edu: type NS, class IN, ns use2.akam.net
    ▸ mit.edu: type NS, class IN, ns eur5.akam.net
    ▸ mit.edu: type NS, class IN, ns ns1-173.akam.net
    ▸ mit.edu: type NS, class IN, ns asia1.akam.net
    ▸ mit.edu: type NS, class IN, ns ns1-37.akam.net
    ▸ mit.edu: type NS, class IN, ns asia2.akam.net
```

```
0000  c0 3c 59 d9 2f 29 34 73  2d 93 c2 1f 08 00 45 00   ·<Y·/)4s -·····
0010  01 b0 aa 65 40 00 fb 11  6b f0 8f 59 0e 07 0a 59   ···e@···k··Y··
0020  c0 2d 00 35 de ae 01 9c  50 c1 00 03 81 80 00 01   ·-·5····P·····
0030  00 08 00 00 00 0b 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu
0040  02 00 01 c0 0c 00 02 00  01 00 00 03 b6 00 0f 04   ··············
0050  75 73 65 35 04 61 6b 61  6d 03 6e 65 74 00 c0 0c   use5·aka m·net·
0060  00 02 00 01 00 00 03 b6  00 07 04 75 73 65 32 c0   ···········use
0070  2a c0 0c 00 02 00 01 00  00 03 b6 00 07 04 65 75   *·············
0080  72 35 c0 2a c0 0c 00 02  00 01 00 00 03 b6 00 0a   r5·*··········
0090  07 6e 73 31 2d 31 37 33  c0 2a c0 0c 00 02 00 01   ·ns1-173 ·*····
00a0  00 00 03 b6 00 08 05 61  73 69 61 31 c0 2a c0 0c   ·······a sia1·*
00b0  00 02 00 01 00 00 03 b6  00 09 06 6e 73 31 2d 33   ···········ns1
00c0  37 c0 2a c0 0c 00 02 00  01 00 00 03 b6 00 08 05   7·*···········
00d0  61 73 69 61 32 c0 2a c0  0c 00 02 00 01 00 00 03   asia2·*·······
00e0  b6 00 07 04 75 73 77 32  c0 2a c0 b9 00 01 00 01   ····usw2 ·*····
00f0  00 01 25 af 00 04 b8 1a  a1 40 c0 53 00 01 00 01   ··%······@·S··
0100  00 01 25 7d 00 04 17 4a  19 40 c0 7c 00 01 00 01   ··%}···J ·@·|··
0110  00 01 25 59 00 04 5f 64  af 40 c0 a5 00 01 00 01   ··%Y··_d ·@····
0120  00 01 25 7a 00 04 5f 65  24 40 c0 40 00 01 00 01   ··%z··_e $@·@··
0130  00 01 25 63 00 04 60 07  31 40 c0 66 00 01 00 01   ··%c··`· 1@·f··
0140  00 01 25 c0 00 04 c1 6c  5b ad c0 66 00 1c 00 01   ··%····l [··f··
0150  00 01 25 c0 00 10 26 00  14 01 00 02 00 00 00 00   ··%···&·······
0160  00 00 00 00 00 ad c0 25  00 01 00 01 00 01 25 c0   ·······%······
0170  00 04 02 10 28 40 c0 25  00 1c 00 01 00 01 25 c0   ····(@·%······
0180  00 10 26 00 14 03 00 0a  00 00 00 00 00 00 00 00   ··&···········
0190  00 40 c0 90 00 01 00 01  00 01 25 c0 00 04 c1 6c   ·@········%··
01a0  5b 25 c0 90 00 1c 00 01  00 01 25 c0 00 10 26 00   [%········%··
```

Text item (text), 28 byte(s)

Packets: 1316 · Displayed: 1274 (96.8%) · Dropped: 0 (0.0%)

Profile: Default



*Wi-Fi

ip.addr == 10.89.192.45

```
No.   Time                       Source         Destination    Protocc Length Info
 1265 2024-02-27 18:09:30.618869 10.89.192.45   143.89.14.7    DNS      74 Standard query 0x0002 NS mit.edu.ust.hk
 1266 2024-02-27 18:09:30.621642 143.89.14.7    10.89.192.45   DNS     128 Standard query response 0x0002 No such name NS mit.edu.ust.hk SOA ustsu1.ust.hk
 1267 2024-02-27 18:09:30.622111 10.89.192.45   143.89.14.7    DNS      67 Standard query 0x0003 NS mit.edu
 1268 2024-02-27 18:09:30.625750 143.89.14.7    10.89.192.45   DNS     446 Standard query response 0x0003 NS mit.edu NS use5.akam.net NS use2.akam.net NS…
 1273 2024-02-27 18:09:32.094364 10.89.192.45   143.89.14.7    DNS      71 Standard query 0x9d38 A wpad.ust.hk
 1278 2024-02-27 18:09:32.098980 143.89.14.7    10.89.192.45   DNS     125 Standard query response 0x9d38 No such name A wpad.ust.hk SOA ustsu1.ust.hk
```

```
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
  Answers
    mit.edu: type NS, class IN, ns use5.akam.net
    mit.edu: type NS, class IN, ns use2.akam.net
    mit.edu: type NS, class IN, ns eur5.akam.net
    mit.edu: type NS, class IN, ns ns1-173.akam.net
    mit.edu: type NS, class IN, ns asia1.akam.net
    mit.edu: type NS, class IN, ns ns1-37.akam.net
    mit.edu: type NS, class IN, ns asia2.akam.net
    mit.edu: type NS, class IN, ns usw2.akam.net
  Additional records
    usw2.akam.net: type A, class IN, addr 184.26.161.64
    eur5.akam.net: type A, class IN, addr 23.74.25.64
    asia1.akam.net: type A, class IN, addr 95.100.175.64
    asia2.akam.net: type A, class IN, addr 95.101.36.64
    use2.akam.net: type A, class IN, addr 96.7.49.64
    ns1-173.akam.net: type A, class IN, addr 193.108.91.173
    ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
    use5.akam.net: type A, class IN, addr 2.16.40.64
    use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
    ns1-37.akam.net: type A, class IN, addr 193.108.91.37
    ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
  [Request In: 1267]
  [Time: 0.003639000 seconds]
```

```
0000  c0 3c 59 d9 2f 29 34 73  2d 93 c2 1f 08 00 45 00   ·<Y·/)4s -·····
0010  01 b0 aa 65 40 00 fb 11  6b f0 8f 59 0e 07 0a 59   ···e@··· k··Y··
0020  c0 2d 00 35 de ae 01 9c  50 c1 00 03 81 80 00 01   ·-·5···· P·····
0030  00 08 00 00 00 0b 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu
0040  02 00 01 c0 0c 00 02 00  01 00 00 03 b6 00 0f 04   ········ ·······
0050  75 73 65 35 04 61 6b 61  6d 03 6e 65 74 00 c0 0c   use5·aka m·net·
0060  00 02 00 01 00 00 03 b6  00 07 04 75 73 65 32 c0   ········ ···use
0070  2a c0 0c 00 02 00 01 00  00 03 b6 00 07 04 65 75   *······· ·······
0080  72 35 c0 2a c0 0c 00 02  00 01 00 00 03 b6 00 0a   r5·*···· ·······
0090  07 6e 73 31 2d 31 37 33  c0 2a c0 0c 00 02 00 01   ·ns1-173 ·*·····
00a0  00 00 03 b6 00 08 05 61  73 69 61 31 c0 2a c0 0c   ·······a sia1·*
00b0  00 02 00 01 00 00 03 b6  00 09 06 6e 73 31 2d 33   ········ ···ns1
00c0  37 c0 2a c0 0c 00 02 00  01 00 00 03 b6 00 08 05   7·*····· ·······
00d0  61 73 69 61 32 c0 2a c0  0c 00 02 00 01 00 00 03   asia2·*· ·······
00e0  b6 00 07 04 75 73 77 32  c0 2a c0 b9 00 01 00 01   ····usw2 ·*·····
00f0  00 01 25 af 00 04 b8 1a  a1 40 c0 53 00 01 00 01   ··%····· ·@·S···
0100  00 01 25 7d 00 04 17 4a  19 40 c0 7c 00 01 00 01   ··%}···J ·@·|···
0110  00 01 25 59 00 04 5f 64  af 40 c0 a5 00 01 00 01   ··%Y··_d ·@·····
0120  00 01 25 7a 00 04 5f 65  24 40 c0 40 00 01 00 01   ··%z··_e $@·@···
0130  00 01 25 63 00 04 60 07  31 40 c0 66 00 01 00 01   ··%c··`· 1@·f···
0140  00 01 25 c0 00 04 c1 6c  5b ad c0 66 00 1c 00 01   ··%····l [··f···
0150  00 01 25 c0 00 10 26 00  14 01 00 02 00 00 00 00   ··%···&· ·······
0160  00 00 00 00 00 ad c0 25  00 01 00 01 00 01 25 c0   ·······% ·······
0170  00 04 02 10 28 40 c0 25  00 1c 00 01 00 01 25 c0   ····(@·% ·······
0180  00 10 26 00 14 03 00 0a  00 00 00 00 00 00 00 00   ··&····· ·······
0190  00 40 c0 90 00 01 00 01  00 01 25 c0 00 04 c1 6c   ·@······ ··%····
01a0  5b 25 c0 90 00 1c 00 01  00 01 25 c0 00 10 26 00   [%······ ··%····
```

Text item (text), 28 byte(s)

Packets: 1316 · Displayed: 1274 (96.8%) · Dropped: 0 (0.0%)

Profile: Default