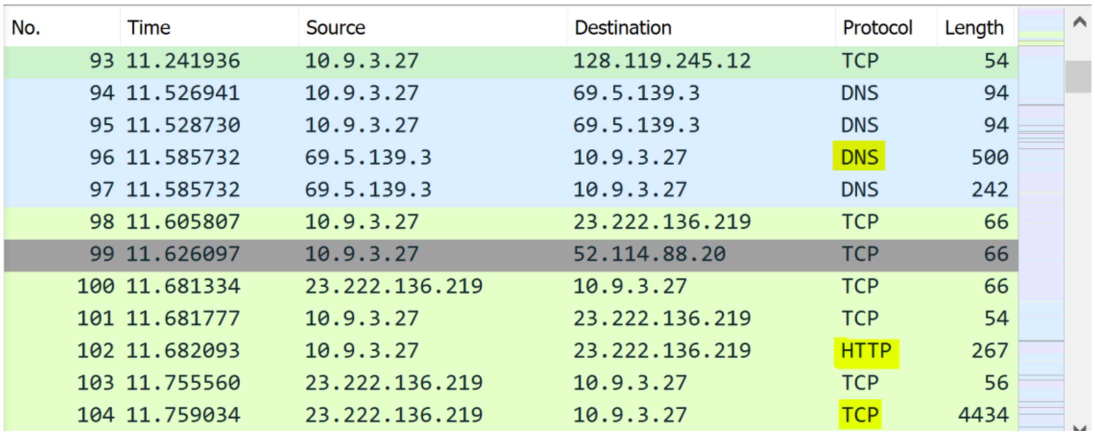
Gretel Rajamoney

Wireshark Lab #1

CS 372   4 – 4 – 2021

1. List 3 different protocols that appear in the protocol column in the unfiltered packet listing pane in step 7 above.

   = DNS, HTTP, and TCP

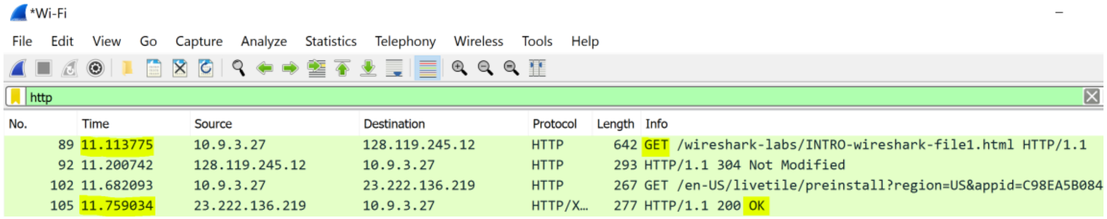


| No. | Time | Source | Destination | Protocol | Length |
|---|---|---|---|---|---|
| 93 | 11.241936 | 10.9.3.27 | 128.119.245.12 | TCP | 54 |
| 94 | 11.526941 | 10.9.3.27 | 69.5.139.3 | DNS | 94 |
| 95 | 11.528730 | 10.9.3.27 | 69.5.139.3 | DNS | 94 |
| 96 | 11.585732 | 69.5.139.3 | 10.9.3.27 | DNS | 500 |
| 97 | 11.585732 | 69.5.139.3 | 10.9.3.27 | DNS | 242 |
| 98 | 11.605807 | 10.9.3.27 | 23.222.136.219 | TCP | 66 |
| 99 | 11.626097 | 10.9.3.27 | 52.114.88.20 | TCP | 66 |
| 100 | 11.681334 | 23.222.136.219 | 10.9.3.27 | TCP | 66 |
| 101 | 11.681777 | 10.9.3.27 | 23.222.136.219 | TCP | 54 |
| 102 | 11.682093 | 10.9.3.27 | 23.222.136.219 | HTTP | 267 |
| 103 | 11.755560 | 23.222.136.219 | 10.9.3.27 | TCP | 56 |
| 104 | 11.759034 | 23.222.136.219 | 10.9.3.27 | TCP | 4434 |

2. How long did it take from when the HTTP GET message was sent until the HTTP OK 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. 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.)

   = 11.759034 – 11.113775

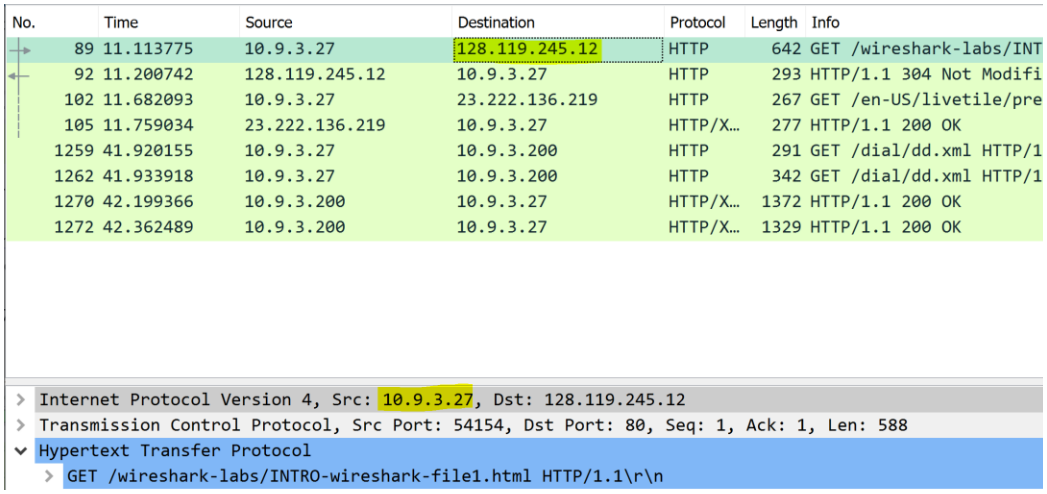
   = 0.645259 seconds



http

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 89 | 11.113775 | 10.9.3.27 | 128.119.245.12 | HTTP | 642 | GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |
| 92 | 11.200742 | 128.119.245.12 | 10.9.3.27 | HTTP | 293 | HTTP/1.1 304 Not Modified |
| 102 | 11.682093 | 10.9.3.27 | 23.222.136.219 | HTTP | 267 | GET /en-US/livetile/preinstall?region=US&appid=C98EA5B084 |
| 105 | 11.759034 | 23.222.136.219 | 10.9.3.27 | HTTP/X… | 277 | HTTP/1.1 200 OK |

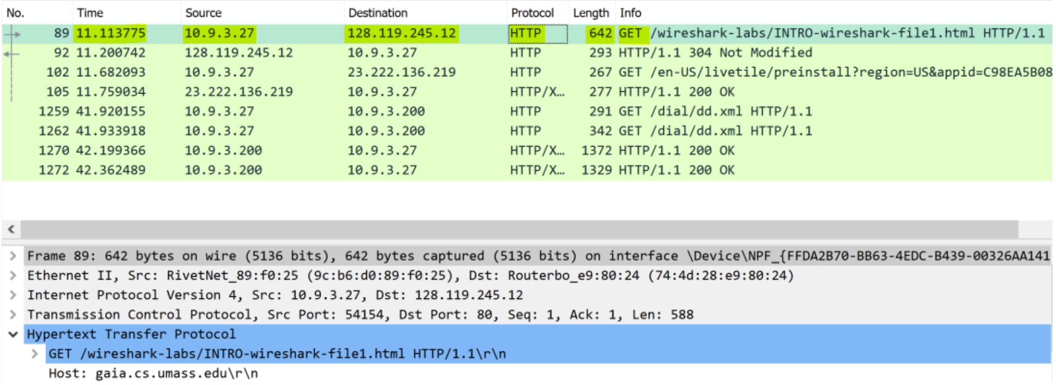
3. What is the Internet Protocol (IP) address of the gaia.cs.umass.edu? What is the Internet Protocol (IP) address of your computer?
   = The IP address of gaia.cs.umass.edu is: 128.119.245.12
   = The IP address of my computer is: 10.9.3.27



```
No.    Time       Source          Destination     Protocol Length Info
  89 11.113775   10.9.3.27       128.119.245.12  HTTP      642 GET /wireshark-labs/INT
  92 11.200742   128.119.245.12  10.9.3.27       HTTP      293 HTTP/1.1 304 Not Modifi
 102 11.682093   10.9.3.27       23.222.136.219  HTTP      267 GET /en-US/livetile/pre
 105 11.759034   23.222.136.219  10.9.3.27       HTTP/X…   277 HTTP/1.1 200 OK
1259 41.920155   10.9.3.27       10.9.3.200      HTTP      291 GET /dial/dd.xml HTTP/1
1262 41.933918   10.9.3.27       10.9.3.200      HTTP      342 GET /dial/dd.xml HTTP/1
1270 42.199366   10.9.3.200      10.9.3.27       HTTP/X…  1372 HTTP/1.1 200 OK
1272 42.362489   10.9.3.200      10.9.3.27       HTTP/X…  1329 HTTP/1.1 200 OK

> Internet Protocol Version 4, Src: 10.9.3.27, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54154, Dst Port: 80, Seq: 1, Ack: 1, Len: 588
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
```

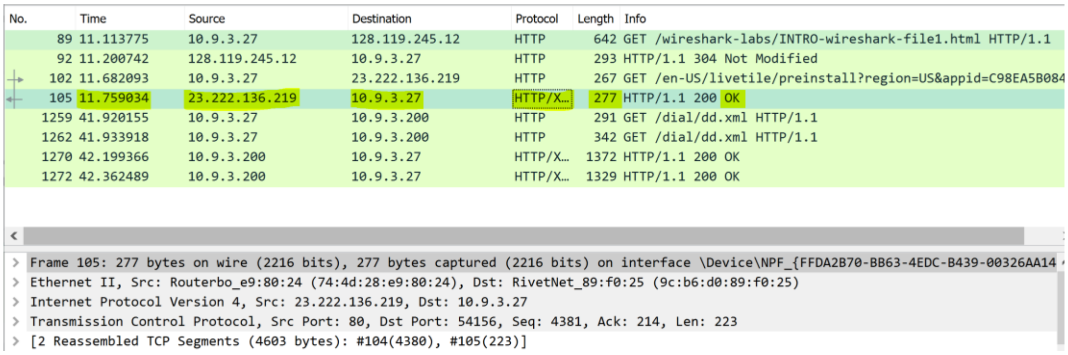
4. Include screenshots of the two HTTP messages (GET and OK) referred to in question 2 above. Make sure to include at least: Arrival Time, Total Length, Protocol, Source IP address, and Destination IP address.
   = GET HTTP message



```
No.    Time       Source          Destination     Protocol Length Info
  89 11.113775   10.9.3.27       128.119.245.12  HTTP      642 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  92 11.200742   128.119.245.12  10.9.3.27       HTTP      293 HTTP/1.1 304 Not Modified
 102 11.682093   10.9.3.27       23.222.136.219  HTTP      267 GET /en-US/livetile/preinstall?region=US&appid=C98EA5B08
 105 11.759034   23.222.136.219  10.9.3.27       HTTP/X…   277 HTTP/1.1 200 OK
1259 41.920155   10.9.3.27       10.9.3.200      HTTP      291 GET /dial/dd.xml HTTP/1.1
1262 41.933918   10.9.3.27       10.9.3.200      HTTP      342 GET /dial/dd.xml HTTP/1.1
1270 42.199366   10.9.3.200      10.9.3.27       HTTP/X…  1372 HTTP/1.1 200 OK
1272 42.362489   10.9.3.200      10.9.3.27       HTTP/X…  1329 HTTP/1.1 200 OK

> Frame 89: 642 bytes on wire (5136 bits), 642 bytes captured (5136 bits) on interface \Device\NPF_{FFDA2B70-BB63-4EDC-B439-00326AA141
> Ethernet II, Src: RivetNet_89:f0:25 (9c:b6:d0:89:f0:25), Dst: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
> Internet Protocol Version 4, Src: 10.9.3.27, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54154, Dst Port: 80, Seq: 1, Ack: 1, Len: 588
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
```

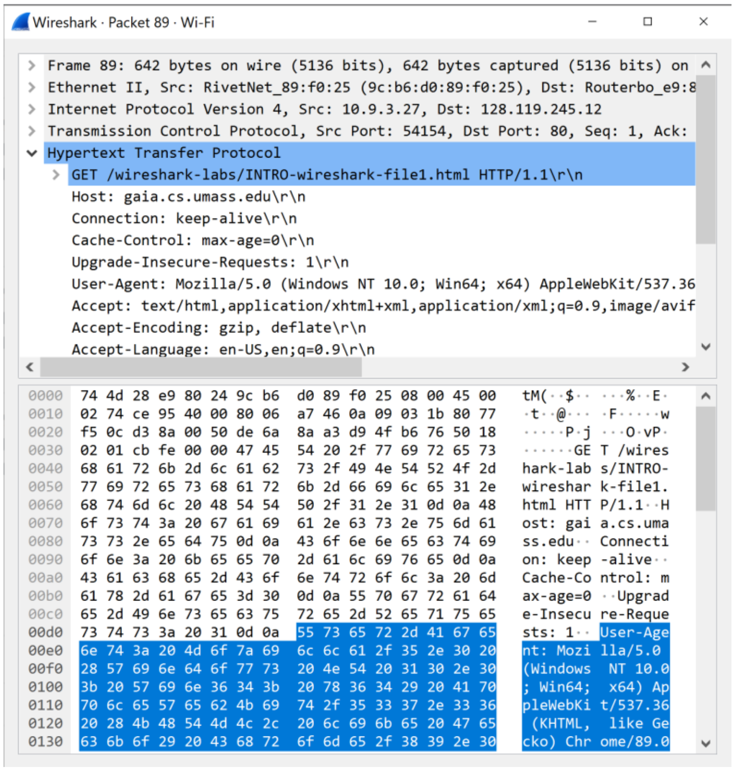
   = OK HTTP message



```
No.    Time       Source          Destination     Protocol Length Info
  89 11.113775   10.9.3.27       128.119.245.12  HTTP      642 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  92 11.200742   128.119.245.12  10.9.3.27       HTTP      293 HTTP/1.1 304 Not Modified
 102 11.682093   10.9.3.27       23.222.136.219  HTTP      267 GET /en-US/livetile/preinstall?region=US&appid=C98EA5B084
 105 11.759034   23.222.136.219  10.9.3.27       HTTP/X…   277 HTTP/1.1 200 OK
1259 41.920155   10.9.3.27       10.9.3.200      HTTP      291 GET /dial/dd.xml HTTP/1.1
1262 41.933918   10.9.3.27       10.9.3.200      HTTP      342 GET /dial/dd.xml HTTP/1.1
1270 42.199366   10.9.3.200      10.9.3.27       HTTP/X…  1372 HTTP/1.1 200 OK
1272 42.362489   10.9.3.200      10.9.3.27       HTTP/X…  1329 HTTP/1.1 200 OK

> Frame 105: 277 bytes on wire (2216 bits), 277 bytes captured (2216 bits) on interface \Device\NPF_{FFDA2B70-BB63-4EDC-B439-00326AA14
> Ethernet II, Src: Routerbo_e9:80:24 (74:4d:28:e9:80:24), Dst: RivetNet_89:f0:25 (9c:b6:d0:89:f0:25)
> Internet Protocol Version 4, Src: 23.222.136.219, Dst: 10.9.3.27
> Transmission Control Protocol, Src Port: 80, Dst Port: 54156, Seq: 4381, Ack: 214, Len: 223
> [2 Reassembled TCP Segments (4603 bytes): #104(4380), #105(223)]
```

= GET HTTP message (Packet in a New Window)

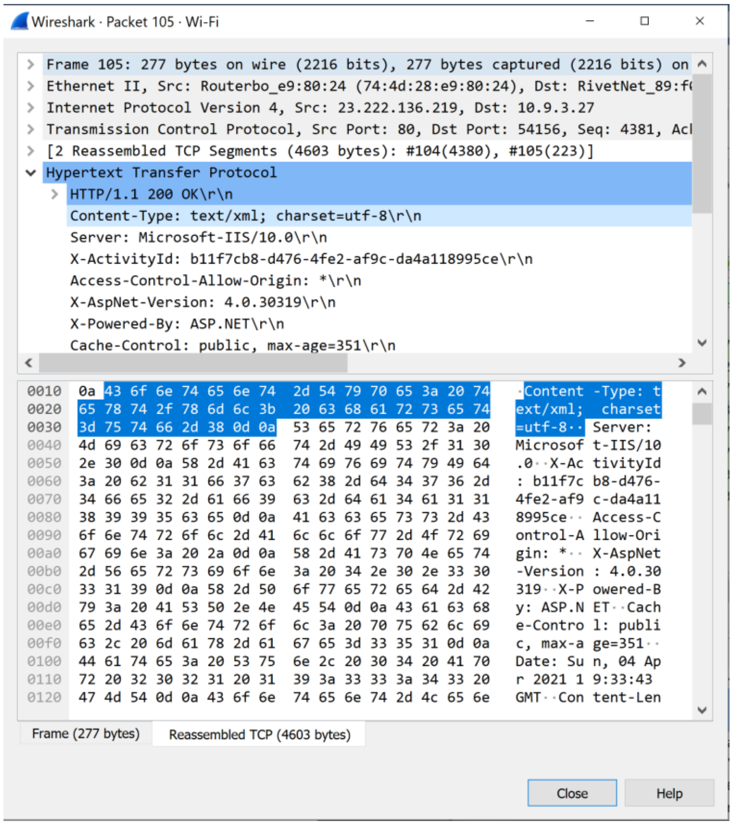


Wireshark · Packet 89 · Wi-Fi

```
> Frame 89: 642 bytes on wire (5136 bits), 642 bytes captured (5136 bits) on
> Ethernet II, Src: RivetNet_89:f0:25 (9c:b6:d0:89:f0:25), Dst: Routerbo_e9:8
> Internet Protocol Version 4, Src: 10.9.3.27, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54154, Dst Port: 80, Seq: 1, Ack:
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
```

```
0000  74 4d 28 e9 80 24 9c b6  d0 89 f0 25 08 00 45 00   tM(··$·· ···%··E·
0010  02 74 ce 95 40 00 80 06  a7 46 0a 09 03 1b 80 77   ·t··@··· ·F·····w
0020  f5 0c d3 8a 00 50 de 6a  8a a3 d9 4f b6 76 50 18   ·····P·j ···O·vP·
0030  02 01 cb fe 00 00 47 45  54 20 2f 77 69 72 65 73   ······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  43 61 63 68 65 2d 43 6f  6e 74 72 6f 6c 3a 20 6d   Cache-Co ntrol: m
00b0  61 78 2d 61 67 65 3d 30  0d 0a 55 70 67 72 61 64   ax-age=0 ··Upgrad
00c0  65 2d 49 6e 73 65 63 75  72 65 2d 52 65 71 75 65   e-Insecu re-Reque
00d0  73 74 73 3a 20 31 0d 0a  55 73 65 72 2d 41 67 65   sts: 1·· User-Age
00e0  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
00f0  28 57 69 6e 64 6f 77 73  20 4e 54 20 31 30 2e 30   (Windows  NT 10.0
0100  3b 20 57 69 6e 36 34 3b  20 78 36 34 29 20 41 70   ; Win64;  x64) Ap
0110  70 6c 65 57 65 62 4b 69  74 2f 35 33 37 2e 33 36   pleWebKi t/537.36
0120  20 28 4b 48 54 4d 4c 2c  20 6c 69 6b 65 20 47 65    (KHTML,  like Ge
0130  63 6b 6f 29 20 43 68 72  6f 6d 65 2f 38 39 2e 30   cko) Chr ome/89.0
```

= OK HTTP message (Packet in a New Window)



Wireshark · Packet 105 · Wi-Fi

```
> Frame 105: 277 bytes on wire (2216 bits), 277 bytes captured (2216 bits) on
> Ethernet II, Src: Routerbo_e9:80:24 (74:4d:28:e9:80:24), Dst: RivetNet_89:f0
> Internet Protocol Version 4, Src: 23.222.136.219, Dst: 10.9.3.27
> Transmission Control Protocol, Src Port: 80, Dst Port: 54156, Seq: 4381, Ack
> [2 Reassembled TCP Segments (4603 bytes): #104(4380), #105(223)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Content-Type: text/xml; charset=utf-8\r\n
    Server: Microsoft-IIS/10.0\r\n
    X-ActivityId: b11f7cb8-d476-4fe2-af9c-da4a118995ce\r\n
    Access-Control-Allow-Origin: *\r\n
    X-AspNet-Version: 4.0.30319\r\n
    X-Powered-By: ASP.NET\r\n
    Cache-Control: public, max-age=351\r\n
```

```
0010  0a 43 6f 6e 74 65 6e 74  2d 54 79 70 65 3a 20 74   ·Content -Type: t
0020  65 78 74 2f 78 6d 6c 3b  20 63 68 61 72 73 65 74   ext/xml;  charset
0030  3d 75 74 66 2d 38 0d 0a  53 65 72 76 65 72 3a 20   =utf-8·· Server: 
0040  4d 69 63 72 6f 73 6f 66  74 2d 49 49 53 2f 31 30   Microsof t-IIS/10
0050  2e 30 0d 0a 58 2d 41 63  74 69 76 69 74 79 49 64   .0··X-Ac tivityId
0060  3a 20 62 31 31 66 37 63  62 38 2d 64 34 37 36 2d   : b11f7c b8-d476-
0070  34 66 65 32 2d 61 66 39  63 2d 64 61 34 61 31 31   4fe2-af9 c-da4a11
0080  38 39 39 35 63 65 0d 0a  41 63 63 65 73 73 2d 43   8995ce·· Access-C
0090  6f 6e 74 72 6f 6c 2d 41  6c 6c 6f 77 2d 4f 72 69   ontrol-A llow-Ori
00a0  67 69 6e 3a 20 2a 0d 0a  58 2d 41 73 70 4e 65 74   gin: *·· X-AspNet
00b0  2d 56 65 72 73 69 6f 6e  3a 20 34 2e 30 2e 33 30   -Version : 4.0.30
00c0  33 31 39 0d 0a 58 2d 50  6f 77 65 72 65 64 2d 42   319··X-P owered-B
00d0  79 3a 20 41 53 50 2e 4e  45 54 0d 0a 43 61 63 68   y: ASP.N ET··Cach
00e0  65 2d 43 6f 6e 74 72 6f  6c 3a 20 70 75 62 6c 69   e-Contro l: publi
00f0  63 2c 20 6d 61 78 2d 61  67 65 3d 33 35 31 0d 0a   c, max-a ge=351··
0100  44 61 74 65 3a 20 53 75  6e 2c 20 30 34 20 41 70   Date: Su n, 04 Ap
0110  72 20 32 30 32 31 20 31  39 3a 33 33 3a 34 33 20   r 2021 1 9:33:43 
0120  47 4d 54 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   GMT··Con tent-Len
```