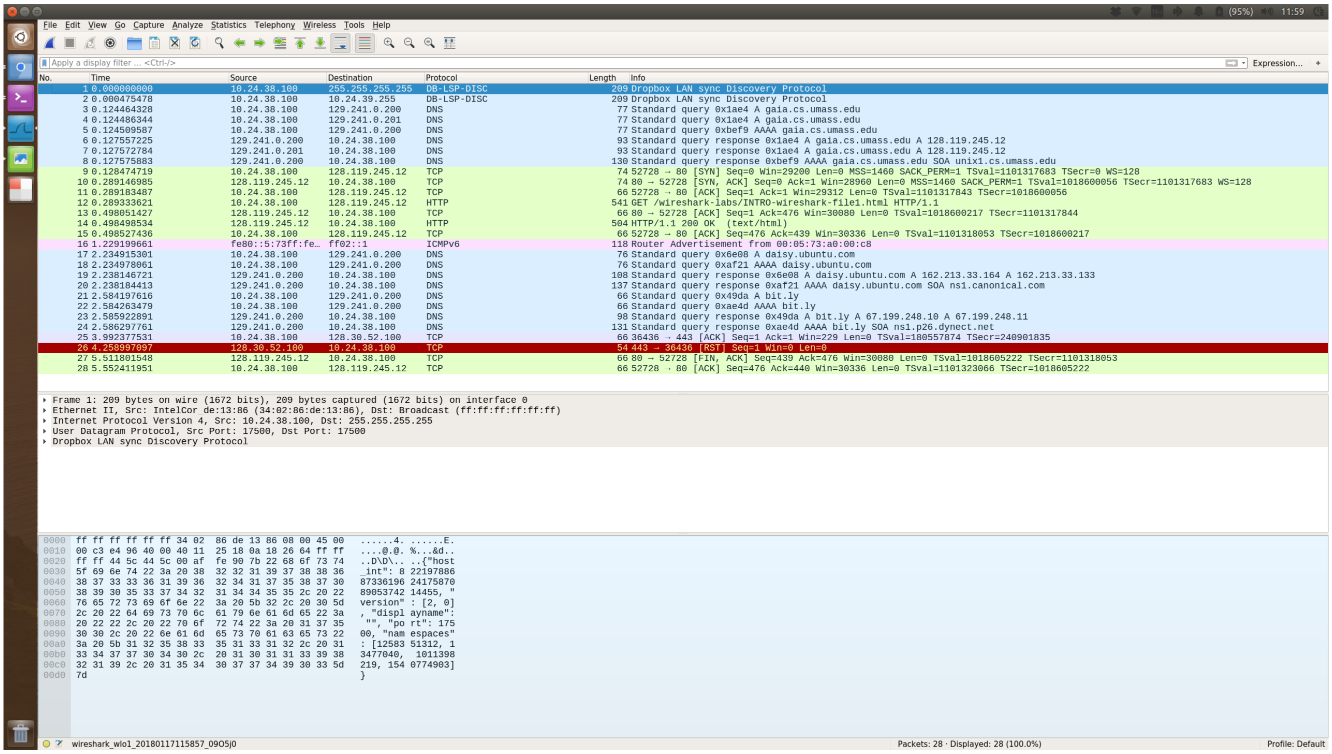
Excercise 1
Rendell Cale, February 23, 2018

Question 1



```
No.  Time         Source           Destination      Protocol      Length Info
   1 0.000000000  10.24.38.100     255.255.255.255  DB-LSP-DISC      209 Dropbox LAN sync Discovery Protocol
   2 0.000475478  10.24.38.100     10.24.39.255     DB-LSP-DISC      209 Dropbox LAN sync Discovery Protocol
   3 0.124464328  10.24.38.100     129.241.0.200    DNS               77 Standard query 0x1ae4 A gaia.cs.umass.edu
   4 0.124486344  10.24.38.100     129.241.0.201    DNS               77 Standard query 0x1ae4 A gaia.cs.umass.edu
   5 0.124509587  10.24.38.100     129.241.0.200    DNS               77 Standard query 0xbef9 AAAA gaia.cs.umass.edu
   6 0.127557225  129.241.0.200    10.24.38.100     DNS               93 Standard query response 0x1ae4 A gaia.cs.umass.edu A 128.119.245.12
   7 0.127572784  129.241.0.201    10.24.38.100     DNS               93 Standard query response 0x1ae4 A gaia.cs.umass.edu A 128.119.245.12
   8 0.127575883  129.241.0.200    10.24.38.100     DNS              130 Standard query response 0xbef9 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
   9 0.128474719  10.24.38.100     128.119.245.12   TCP               74 52728 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1101317683 TSecr=0 WS=128
  10 0.289146985  128.119.245.12   10.24.38.100     TCP               74 80 → 52728 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1018600056 TSecr=1101317683 WS=128
  11 0.289183487  10.24.38.100     128.119.245.12   TCP               66 52728 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1101317843 TSecr=1018600056
  12 0.289333621  10.24.38.100     128.119.245.12   HTTP             541 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  13 0.498051427  128.119.245.12   10.24.38.100     TCP               66 80 → 52728 [ACK] Seq=1 Ack=476 Win=30080 Len=0 TSval=1018600217 TSecr=1101317844
  14 0.498498534  128.119.245.12   10.24.38.100     HTTP             504 HTTP/1.1 200 OK  (text/html)
  15 0.498527436  10.24.38.100     128.119.245.12   TCP               66 52728 → 80 [ACK] Seq=476 Ack=439 Win=30336 Len=0 TSval=1101318053 TSecr=1018600217
  16 1.229199661  fe80::5:73ff:fe… ff02::1          ICMPv6           118 Router Advertisement from 00:05:73:a0:00:c8
  17 2.234915301  10.24.38.100     129.241.0.200    DNS               76 Standard query 0x6e08 A daisy.ubuntu.com
  18 2.234978061  10.24.38.100     129.241.0.200    DNS               76 Standard query 0xaf21 AAAA daisy.ubuntu.com
  19 2.238146721  129.241.0.200    10.24.38.100     DNS              108 Standard query response 0x6e08 A daisy.ubuntu.com A 162.213.33.164 A 162.213.33.133
  20 2.238184413  129.241.0.200    10.24.38.100     DNS              137 Standard query response 0xaf21 AAAA daisy.ubuntu.com SOA ns1.canonical.com
  21 2.584197616  10.24.38.100     129.241.0.200    DNS               66 Standard query 0x49da A bit.ly
  22 2.584263479  10.24.38.100     129.241.0.200    DNS               66 Standard query 0xae4d AAAA bit.ly
  23 2.585922891  129.241.0.200    10.24.38.100     DNS               98 Standard query response 0x49da A bit.ly A 67.199.248.10 A 67.199.248.11
  24 2.586297761  129.241.0.200    10.24.38.100     DNS              131 Standard query response 0xae4d AAAA bit.ly SOA ns1.p26.dynect.net
  25 3.992377531  10.24.38.100     128.30.52.100    TCP               66 36436 → 443 [ACK] Seq=1 Ack=1 Win=229 Len=0 TSval=180557874 TSecr=240901835
  26 4.258997097  128.30.52.100    10.24.38.100     TCP               54 443 → 36436 [RST] Seq=1 Win=0 Len=0
  27 5.511801548  128.119.245.12   10.24.38.100     TCP               66 80 → 52728 [FIN, ACK] Seq=439 Ack=476 Win=30080 Len=0 TSval=1018605222 TSecr=1101318053
  28 5.552411951  10.24.38.100     128.119.245.12   TCP               66 52728 → 80 [ACK] Seq=476 Ack=440 Win=30336 Len=0 TSval=1101323066 TSecr=1018605222
```

```
▸ Frame 1: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface 0
▸ Ethernet II, Src: IntelCor_de:13:86 (34:02:86:de:13:86), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 10.24.38.100, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 17500, Dst Port: 17500
▸ Dropbox LAN sync Discovery Protocol
```

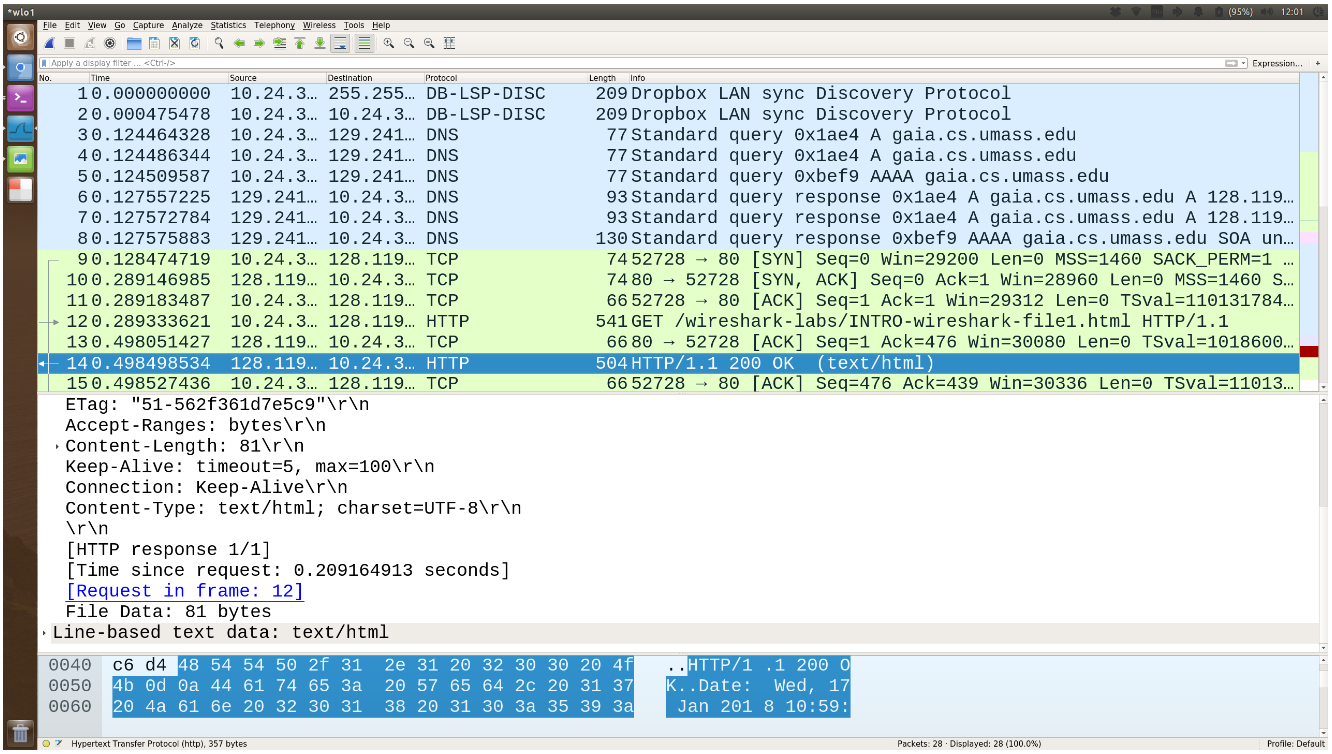
```
0000  ff ff ff ff ff ff 34 02  86 de 13 86 08 00 45 00   ......4. ......E.
0010  00 c3 e4 96 40 00 40 11  25 18 0a 18 26 64 ff ff   ....@.@. %...&d..
0020  ff ff 44 5c 44 5c 00 af  fe 90 7b 22 68 6f 73 74   ..D\D\.. ..{"host
0030  5f 69 6e 74 22 3a 20 38  32 32 31 39 37 38 38 36   _int": 8 22197886
0040  38 37 33 33 36 31 39 36  32 34 31 37 35 38 37 30   87336196 24175870
0050  38 39 30 35 33 37 34 32  31 34 34 35 35 2c 20 22   89053742 14455, "
0060  76 65 72 73 69 6f 6e 22  3a 20 5b 32 2c 20 30 5d   version" : [2, 0]
0070  2c 20 22 64 69 73 70 6c  61 79 6e 61 6d 65 22 3a   , "displ ayname":
0080  20 22 22 2c 20 22 70 6f  72 74 22 3a 20 31 37 35    "", "po rt": 175
0090  30 30 2c 20 22 6e 61 6d  65 73 70 61 63 65 73 22   00, "nam espaces"
00a0  3a 20 5b 31 32 35 38 33  35 31 33 31 32 2c 20 31   : [12583 51312, 1
00b0  33 34 37 37 30 34 30 2c  20 31 30 31 31 33 39 38   3477040,  1011398
00c0  32 31 39 2c 20 31 35 34  30 37 37 34 39 30 33 5d   219, 154 0774903]
00d0  7d                                                 }
```

wireshark_wlo1_20180117115857_09O5j0   Packets: 28 · Displayed: 28 (100.0%)   Profile: Default

Looks like the three protocols related to the website access are:

- DNS
- HTTP
- TCP

Question 2


*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
12:01
(95%)

```
No.   Time          Source       Destination  Protocol      Length Info
    1 0.000000000   10.24.3…     255.255…     DB-LSP-DISC   209 Dropbox LAN sync Discovery Protocol
    2 0.000475478   10.24.3…     10.24.3…     DB-LSP-DISC   209 Dropbox LAN sync Discovery Protocol
    3 0.124464328   10.24.3…     129.241…     DNS            77 Standard query 0x1ae4 A gaia.cs.umass.edu
    4 0.124486344   10.24.3…     129.241…     DNS            77 Standard query 0x1ae4 A gaia.cs.umass.edu
    5 0.124509587   10.24.3…     129.241…     DNS            77 Standard query 0xbef9 AAAA gaia.cs.umass.edu
    6 0.127557225   129.241…     10.24.3…     DNS            93 Standard query response 0x1ae4 A gaia.cs.umass.edu A 128.119…
    7 0.127572784   129.241…     10.24.3…     DNS            93 Standard query response 0x1ae4 A gaia.cs.umass.edu A 128.119…
    8 0.127575883   129.241…     10.24.3…     DNS           130 Standard query response 0xbef9 AAAA gaia.cs.umass.edu SOA un…
    9 0.128474719   10.24.3…     128.119…     TCP            74 52728 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 …
   10 0.289146985   128.119…     10.24.3…     TCP            74 80 → 52728 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 S…
   11 0.289183487   10.24.3…     128.119…     TCP            66 52728 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=110131784…
   12 0.289333621   10.24.3…     128.119…     HTTP          541 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   13 0.498051427   128.119…     10.24.3…     TCP            66 80 → 52728 [ACK] Seq=1 Ack=476 Win=30080 Len=0 TSval=1018600…
   14 0.498498534   128.119…     10.24.3…     HTTP          504 HTTP/1.1 200 OK  (text/html)
   15 0.498527436   10.24.3…     128.119…     TCP            66 52728 → 80 [ACK] Seq=476 Ack=439 Win=30336 Len=0 TSval=11013…
```

```
  ETag: "51-562f361d7e5c9"\r\n
  Accept-Ranges: bytes\r\n
› Content-Length: 81\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 1/1]
  [Time since request: 0.209164913 seconds]
  [Request in frame: 12]
  File Data: 81 bytes
› Line-based text data: text/html
```

```
0040  c6 d4 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   ..HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 57 65 64 2c 20 31 37   K..Date:  Wed, 17
0060  20 4a 61 6e 20 32 30 31  38 20 31 30 3a 35 39 3a    Jan 201 8 10:59:
```

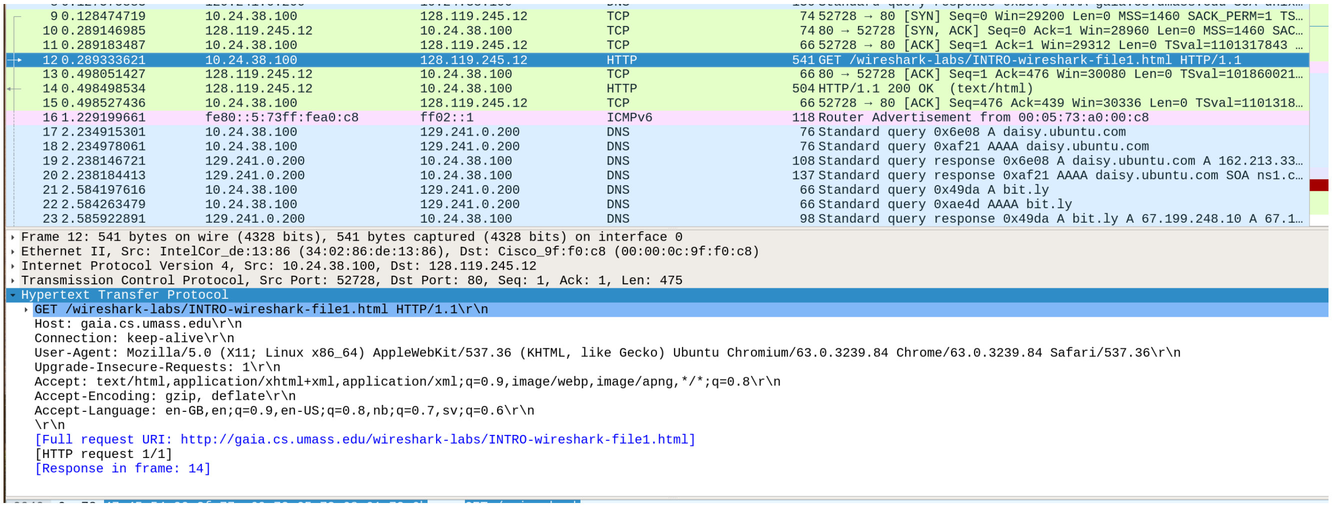
```
Hypertext Transfer Protocol (http), 357 bytes        Packets: 28 · Displayed: 28 (100.0%)        Profile: Default
```

Going into to response entry, we can see that the time passed since request was about 0.2092 s.

Question 3

Looking at the source and destination of the HTTP GET request, we see that the source (my computer) has internet address 10.24.38.100 and that the website has internet address 128.119.245.12.

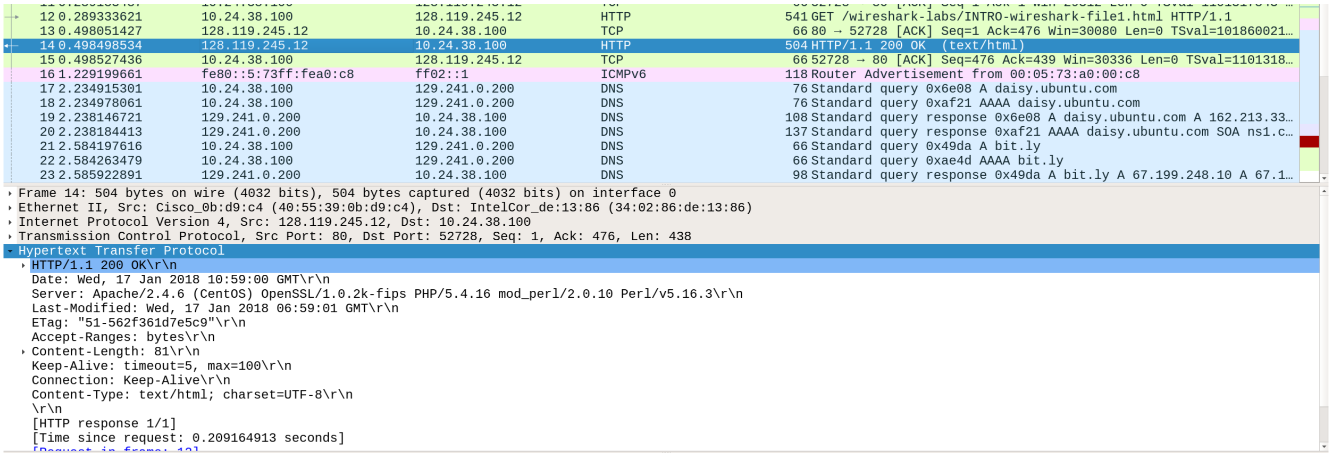
Question 4



```
    9 0.128474719   10.24.38.100             128.119.245.12     TCP        74 52728 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TS…
   10 0.289146985   128.119.245.12           10.24.38.100       TCP        74 80 → 52728 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SAC…
   11 0.289183487   10.24.38.100             128.119.245.12     TCP        66 52728 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1101317843 …
   12 0.289333621   10.24.38.100             128.119.245.12     HTTP      541 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   13 0.498051427   128.119.245.12           10.24.38.100       TCP        66 80 → 52728 [ACK] Seq=1 Ack=476 Win=30080 Len=0 TSval=101860021…
   14 0.498498534   128.119.245.12           10.24.38.100       HTTP      504 HTTP/1.1 200 OK  (text/html)
   15 0.498527436   10.24.38.100             128.119.245.12     TCP        66 52728 → 80 [ACK] Seq=476 Ack=439 Win=30336 Len=0 TSval=1101318…
   16 1.229199661   fe80::5:73ff:fea0:c8     ff02::1            ICMPv6    118 Router Advertisement from 00:05:73:a0:00:c8
   17 2.234915301   10.24.38.100             129.241.0.200      DNS        76 Standard query 0x6e08 A daisy.ubuntu.com
   18 2.234978061   10.24.38.100             129.241.0.200      DNS        76 Standard query 0xaf21 AAAA daisy.ubuntu.com
   19 2.238146721   129.241.0.200            10.24.38.100       DNS       108 Standard query response 0x6e08 A daisy.ubuntu.com A 162.213.33…
   20 2.238184413   129.241.0.200            10.24.38.100       DNS       137 Standard query response 0xaf21 AAAA daisy.ubuntu.com SOA ns1.c…
   21 2.584197616   10.24.38.100             129.241.0.200      DNS        66 Standard query 0x49da A bit.ly
   22 2.584263479   10.24.38.100             129.241.0.200      DNS        66 Standard query 0xae4d AAAA bit.ly
   23 2.585922891   129.241.0.200            10.24.38.100       DNS        98 Standard query response 0x49da A bit.ly A 67.199.248.10 A 67.1…
```

```
› Frame 12: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits) on interface 0
› Ethernet II, Src: IntelCor_de:13:86 (34:02:86:de:13:86), Dst: Cisco_9f:f0:c8 (00:00:0c:9f:f0:c8)
› Internet Protocol Version 4, Src: 10.24.38.100, Dst: 128.119.245.12
› Transmission Control Protocol, Src Port: 52728, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
˅ 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
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/63.0.3239.84 Chrome/63.0.3239.84 Safari/537.36\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en;q=0.9,en-US;q=0.8,nb;q=0.7,sv;q=0.6\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 14]
```

Figure 1: HTTP GET



```
   12 0.289333621   10.24.38.100          128.119.245.12        HTTP        541 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   13 0.498051427   128.119.245.12        10.24.38.100          TCP          66 80 → 52728 [ACK] Seq=1 Ack=476 Win=30080 Len=0 TSval=101860021…
   14 0.498498534   128.119.245.12        10.24.38.100          HTTP        504 HTTP/1.1 200 OK  (text/html)
   15 0.498527436   10.24.38.100          128.119.245.12        TCP          66 52728 → 80 [ACK] Seq=476 Ack=439 Win=30336 Len=0 TSval=1101318…
   16 1.229199661   fe80::5:73ff:fea0:c8  ff02::1               ICMPv6      118 Router Advertisement from 00:05:73:a0:00:c8
   17 2.234915301   10.24.38.100          129.241.0.200         DNS          76 Standard query 0x6e08 A daisy.ubuntu.com
   18 2.234978061   10.24.38.100          129.241.0.200         DNS          76 Standard query 0xaf21 AAAA daisy.ubuntu.com
   19 2.238146721   129.241.0.200         10.24.38.100          DNS         108 Standard query response 0x6e08 A daisy.ubuntu.com A 162.213.33…
   20 2.238184413   129.241.0.200         10.24.38.100          DNS         137 Standard query response 0xaf21 AAAA daisy.ubuntu.com SOA ns1.c…
   21 2.584197616   10.24.38.100          129.241.0.200         DNS          66 Standard query 0x49da A bit.ly
   22 2.584263479   10.24.38.100          129.241.0.200         DNS          66 Standard query 0xae4d AAAA bit.ly
   23 2.585922891   129.241.0.200         10.24.38.100          DNS          98 Standard query response 0x49da A bit.ly A 67.199.248.10 A 67.1…
```

```
▸ Frame 14: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface 0
▸ Ethernet II, Src: Cisco_0b:d9:c4 (40:55:39:0b:d9:c4), Dst: IntelCor_de:13:86 (34:02:86:de:13:86)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.24.38.100
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 52728, Seq: 1, Ack: 476, Len: 438
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Wed, 17 Jan 2018 10:59:00 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Wed, 17 Jan 2018 06:59:01 GMT\r\n
    ETag: "51-562f361d7e5c9"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 81\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 1/1]
    [Time since request: 0.209164913 seconds]
    [Request in frame: 12]
```

Figure 2: HTTP OK