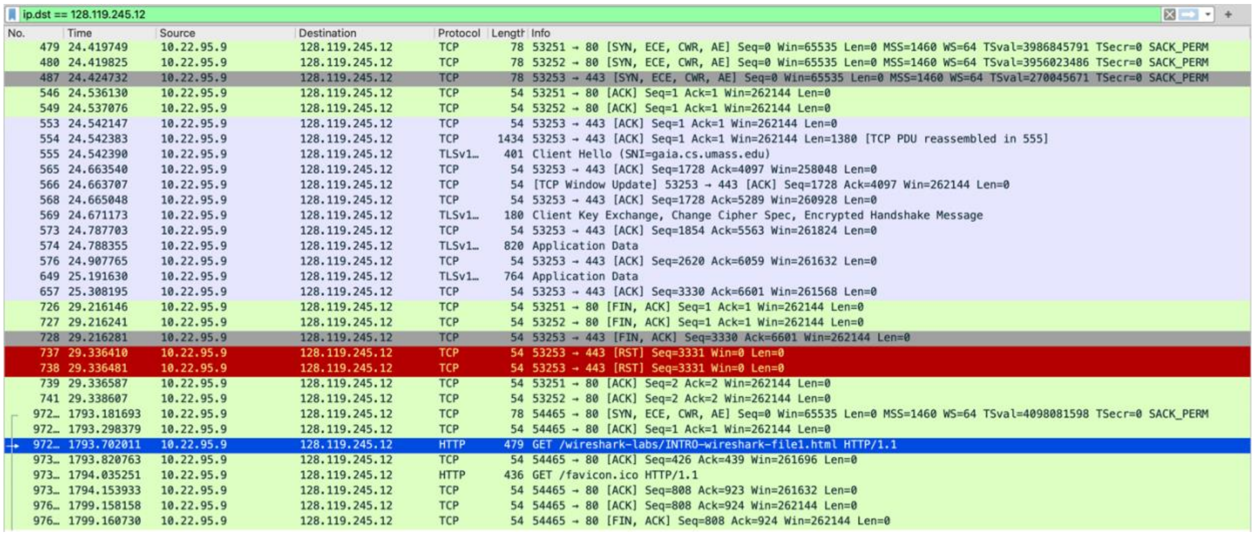
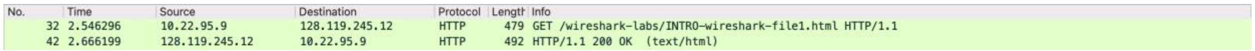
TTM4100 – Assignment 1

1. 

```
ip.dst == 128.119.245.12
No.     Time          Source        Destination      Protocol  Length Info
   479  24.419749     10.22.95.9    128.119.245.12   TCP          78 53251 → 80 [SYN, ECE, CWR, AE] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3986845791 TSecr=0 SACK_PERM
   480  24.419825     10.22.95.9    128.119.245.12   TCP          78 53252 → 80 [SYN, ECE, CWR, AE] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3956023486 TSecr=0 SACK_PERM
   487  24.424732     10.22.95.9    128.119.245.12   TCP          78 53253 → 443 [SYN, ECE, CWR, AE] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=270045671 TSecr=0 SACK_PERM
   546  24.536130     10.22.95.9    128.119.245.12   TCP          54 53251 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   549  24.537076     10.22.95.9    128.119.245.12   TCP          54 53252 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   553  24.542147     10.22.95.9    128.119.245.12   TCP          54 53253 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   554  24.542383     10.22.95.9    128.119.245.12   TCP        1434 53253 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=1380 [TCP PDU reassembled in 555]
   555  24.542390     10.22.95.9    128.119.245.12   TLSv1…      401 Client Hello (SNI=gaia.cs.umass.edu)
   565  24.663540     10.22.95.9    128.119.245.12   TCP          54 53253 → 443 [ACK] Seq=1728 Ack=4097 Win=258048 Len=0
   566  24.663707     10.22.95.9    128.119.245.12   TCP          54 [TCP Window Update] 53253 → 443 [ACK] Seq=1728 Ack=4097 Win=262144 Len=0
   568  24.665048     10.22.95.9    128.119.245.12   TCP          54 53253 → 443 [ACK] Seq=1728 Ack=5289 Win=260928 Len=0
   569  24.671173     10.22.95.9    128.119.245.12   TLSv1…      180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   573  24.787703     10.22.95.9    128.119.245.12   TCP          54 53253 → 443 [ACK] Seq=1854 Ack=5563 Win=261824 Len=0
   574  24.788355     10.22.95.9    128.119.245.12   TLSv1…      820 Application Data
   576  24.907765     10.22.95.9    128.119.245.12   TCP          54 53253 → 443 [ACK] Seq=2620 Ack=6059 Win=261632 Len=0
   649  25.191630     10.22.95.9    128.119.245.12   TLSv1…      764 Application Data
   657  25.308195     10.22.95.9    128.119.245.12   TCP          54 53253 → 443 [ACK] Seq=3330 Ack=6601 Win=261568 Len=0
   726  29.216146     10.22.95.9    128.119.245.12   TCP          54 53251 → 80 [FIN, ACK] Seq=1 Ack=1 Win=262144 Len=0
   727  29.216241     10.22.95.9    128.119.245.12   TCP          54 53252 → 80 [FIN, ACK] Seq=1 Ack=1 Win=262144 Len=0
   728  29.216281     10.22.95.9    128.119.245.12   TCP          54 53253 → 443 [FIN, ACK] Seq=3330 Ack=6601 Win=262144 Len=0
   737  29.336410     10.22.95.9    128.119.245.12   TCP          54 53253 → 443 [RST] Seq=3331 Win=0 Len=0
   738  29.336481     10.22.95.9    128.119.245.12   TCP          54 53253 → 443 [RST] Seq=3331 Win=0 Len=0
   739  29.336587     10.22.95.9    128.119.245.12   TCP          54 53251 → 80 [ACK] Seq=2 Ack=2 Win=262144 Len=0
   741  29.338607     10.22.95.9    128.119.245.12   TCP          54 53252 → 80 [ACK] Seq=2 Ack=2 Win=262144 Len=0
  972…  1793.181693   10.22.95.9    128.119.245.12   TCP          78 54465 → 80 [SYN, ECE, CWR, AE] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4098081598 TSecr=0 SACK_PERM
  972…  1793.298379   10.22.95.9    128.119.245.12   TCP          54 54465 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
  972…  1793.702011   10.22.95.9    128.119.245.12   HTTP        479 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  973…  1793.820763   10.22.95.9    128.119.245.12   TCP          54 54465 → 80 [ACK] Seq=426 Ack=439 Win=261696 Len=0
  973…  1794.035251   10.22.95.9    128.119.245.12   HTTP        436 GET /favicon.ico HTTP/1.1
  973…  1794.153933   10.22.95.9    128.119.245.12   TCP          54 54465 → 80 [ACK] Seq=808 Ack=923 Win=261632 Len=0
  976…  1799.158158   10.22.95.9    128.119.245.12   TCP          54 54465 → 80 [ACK] Seq=808 Ack=924 Win=262144 Len=0
  976…  1799.160730   10.22.95.9    128.119.245.12   TCP          54 54465 → 80 [FIN, ACK] Seq=808 Ack=924 Win=262144 Len=0
```

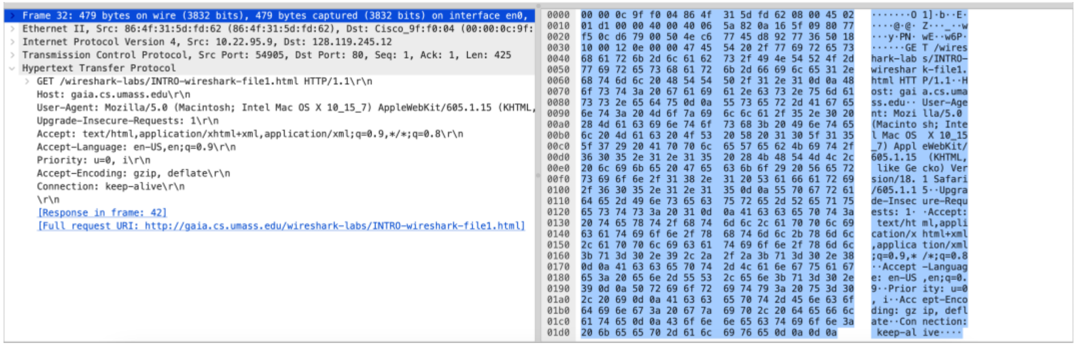
The protocols used when visiting the site in step 7 are: TCP, HTTP and TLS

2. 

```
No.     Time          Source          Destination      Protocol  Length Info
    32  2.546296      10.22.95.9      128.119.245.12   HTTP        479 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    42  2.666199      128.119.245.12  10.22.95.9       HTTP        492 HTTP/1.1 200 OK  (text/html)
```

It took 0.12 seconds between the http get request, and the http 200 response

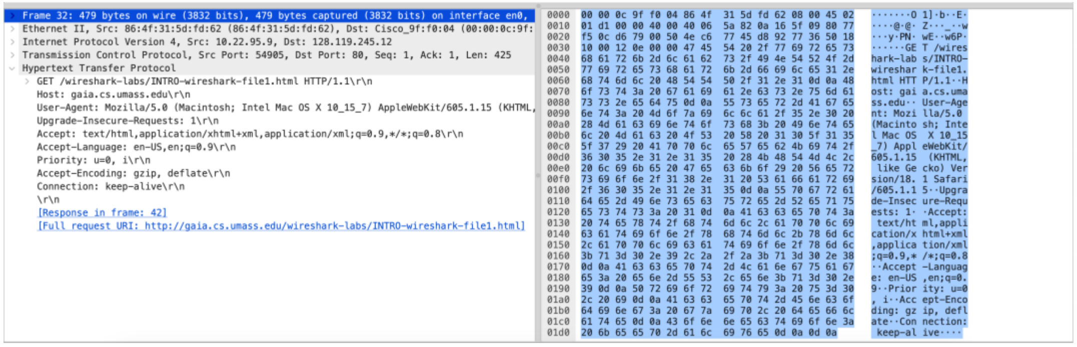
3. In the previous screenshots, we can see that the ip address of http://gaia.cs.umass.edu is 128.22.95.9

4. 

```
> Frame 32: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface en0,
> Ethernet II, Src: 86:4f:31:5d:fd:62 (86:4f:31:5d:fd:62), Dst: Cisco_9f:f0:04 (00:00:0c:9f:
> Internet Protocol Version 4, Src: 10.22.95.9, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54905, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML,
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    Priority: u=0, i\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Response in frame: 42]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

```
0000  00 00 0c 9f f0 04 86 4f  31 5d fd 62 08 00 45 02   ·······O 1]·b··E·
0010  01 d1 00 00 40 00 40 06  5a 82 0a 16 5f 09 80 77   ····@·@· Z···_··w
0020  f5 0c d6 79 00 50 4e c6  77 45 d8 92 77 36 50 18   ···y·PN· wE··w6P·
0030  10 00 12 0e 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  55 73 65 72 2d 41 67 65   ss.edu·· User-Age
0090  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
00a0  28 4d 61 63 69 6e 74 6f  73 68 3b 20 49 6e 74 65   (Macinto sh; Inte
00b0  6c 20 4d 61 63 20 4f 53  20 58 20 31 30 5f 31 35   l Mac OS  X 10_15
00c0  5f 37 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   _7) Appl eWebKit/
00d0  36 30 35 2e 31 2e 31 35  20 28 4b 48 54 4d 4c 2c   605.1.15  (KHTML,
00e0  20 6c 69 6b 65 20 47 65  63 6b 6f 29 20 56 65 72    like Ge cko) Ver
00f0  73 69 6f 6e 2f 31 38 2e  31 20 53 61 66 61 72 69   sion/18. 1 Safari
0100  2f 36 30 35 2e 31 2e 31  35 0d 0a 55 70 67 72 61   /605.1.1 5··Upgra
0110  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
0120  65 73 74 73 3a 20 31 0d  0a 41 63 63 65 70 74 3a   ests: 1· ·Accept:
0130  20 74 65 78 74 2f 68 74  6d 6c 2c 61 70 70 6c 69    text/ht ml,appli
0140  63 61 74 69 6f 6e 2f 78  68 74 6d 6c 2b 78 6d 6c   cation/x html+xml
0150  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 6d 6c   ,applica tion/xml
0160  3b 71 3d 30 2e 39 2c 2a  2f 2a 3b 71 3d 30 2e 38   ;q=0.9,* /*;q=0.8
0170  0d 0a 41 63 63 65 70 74  2d 4c 61 6e 67 75 61 67   ··Accept -Languag
0180  65 3a 20 65 6e 2d 55 53  2c 65 6e 3b 71 3d 30 2e   e: en-US ,en;q=0.
0190  39 0d 0a 50 72 69 6f 72  69 74 79 3a 20 75 3d 30   9··Prior ity: u=0
01a0  2c 20 69 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   , i··Acc ept-Enco
01b0  64 69 6e 67 3a 20 67 7a  69 70 2c 20 64 65 66 6c   ding: gz ip, defl
01c0  61 74 65 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   ate··Con nection:
01d0  20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 0d 0a       keep-al ive····
```

The GET request ^



```
> Frame 32: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface en0,
> Ethernet II, Src: 86:4f:31:5d:fd:62 (86:4f:31:5d:fd:62), Dst: Cisco_9f:f0:04 (00:00:0c:9f:
> Internet Protocol Version 4, Src: 10.22.95.9, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54905, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML,
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    Priority: u=0, i\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Response in frame: 42]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

```
0000  00 00 0c 9f f0 04 86 4f  31 5d fd 62 08 00 45 02   ·······O 1]·b··E·
0010  01 d1 00 00 40 00 40 06  5a 82 0a 16 5f 09 80 77   ····@·@· Z···_··w
0020  f5 0c d6 79 00 50 4e c6  77 45 d8 92 77 36 50 18   ···y·PN· wE··w6P·
0030  10 00 12 0e 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  55 73 65 72 2d 41 67 65   ss.edu·· User-Age
0090  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
00a0  28 4d 61 63 69 6e 74 6f  73 68 3b 20 49 6e 74 65   (Macinto sh; Inte
00b0  6c 20 4d 61 63 20 4f 53  20 58 20 31 30 5f 31 35   l Mac OS  X 10_15
00c0  5f 37 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   _7) Appl eWebKit/
00d0  36 30 35 2e 31 2e 31 35  20 28 4b 48 54 4d 4c 2c   605.1.15  (KHTML,
00e0  20 6c 69 6b 65 20 47 65  63 6b 6f 29 20 56 65 72    like Ge cko) Ver
00f0  73 69 6f 6e 2f 31 38 2e  31 20 53 61 66 61 72 69   sion/18. 1 Safari
0100  2f 36 30 35 2e 31 2e 31  35 0d 0a 55 70 67 72 61   /605.1.1 5··Upgra
0110  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
0120  65 73 74 73 3a 20 31 0d  0a 41 63 63 65 70 74 3a   ests: 1· ·Accept:
0130  20 74 65 78 74 2f 68 74  6d 6c 2c 61 70 70 6c 69    text/ht ml,appli
0140  63 61 74 69 6f 6e 2f 78  68 74 6d 6c 2b 78 6d 6c   cation/x html+xml
0150  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 6d 6c   ,applica tion/xml
0160  3b 71 3d 30 2e 39 2c 2a  2f 2a 3b 71 3d 30 2e 38   ;q=0.9,* /*;q=0.8
0170  0d 0a 41 63 63 65 70 74  2d 4c 61 6e 67 75 61 67   ··Accept -Languag
0180  65 3a 20 65 6e 2d 55 53  2c 65 6e 3b 71 3d 30 2e   e: en-US ,en;q=0.
0190  39 0d 0a 50 72 69 6f 72  69 74 79 3a 20 75 3d 30   9··Prior ity: u=0
01a0  2c 20 69 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   , i··Acc ept-Enco
01b0  64 69 6e 67 3a 20 67 7a  69 70 2c 20 64 65 66 6c   ding: gz ip, defl
01c0  61 74 65 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   ate··Con nection:
01d0  20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 0d 0a       keep-al ive····
```

The HTTP Response ^