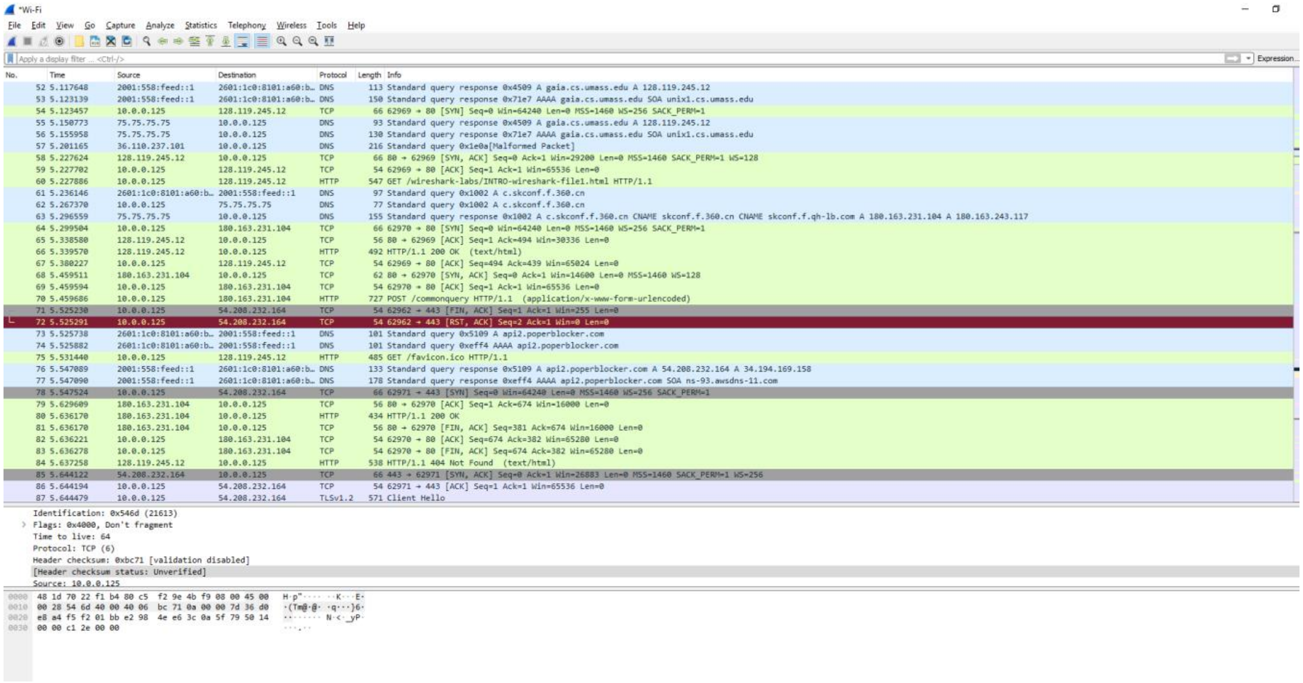
CS 372 – Lab 1

Hao (Jeff) Deng

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
   - The 3 different protocols are: DNS, TCP, and HTTP as you can see the screenshot below:

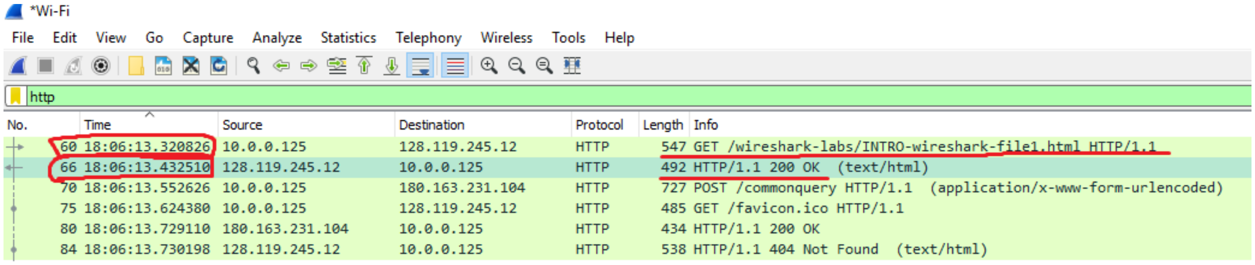

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

```
No.   Time      Source                Destination           Protocol  Length Info
   52 5.117648  2001:558:feed::1      2601:1c0:8101:a60:b… DNS       113 Standard query response 0x4509 A gaia.cs.umass.edu A 128.119.245.12
   53 5.123139  2001:558:feed::1      2601:1c0:8101:a60:b… DNS       150 Standard query response 0x71e7 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
   54 5.123457  10.0.0.125            128.119.245.12        TCP        66 62969 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   55 5.150773  75.75.75.75           10.0.0.125            DNS        93 Standard query response 0x4509 A gaia.cs.umass.edu A 128.119.245.12
   56 5.155958  75.75.75.75           10.0.0.125            DNS       130 Standard query response 0x71e7 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
   57 5.201165  36.110.237.101        10.0.0.125            DNS       216 Standard query 0x1e0a[Malformed Packet]
   58 5.227624  128.119.245.12        10.0.0.125            TCP        66 80 → 62969 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
   59 5.227702  10.0.0.125            128.119.245.12        TCP        54 62969 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   60 5.227886  10.0.0.125            128.119.245.12        HTTP      547 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   61 5.236146  2601:1c0:8101:a60:b… 2001:558:feed::1      DNS        97 Standard query 0x1002 A c.skconf.f.360.cn
   62 5.267370  10.0.0.125            75.75.75.75           DNS        77 Standard query 0x1002 A c.skconf.f.360.cn
   63 5.296559  75.75.75.75           10.0.0.125            DNS       155 Standard query response 0x1002 A c.skconf.f.360.cn CNAME skconf.f.360.cn CNAME skconf.f.qh-lb.com A 180.163.231.104 A 180.163.243.117
   64 5.299504  10.0.0.125            180.163.231.104       TCP        66 62970 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   65 5.338580  128.119.245.12        10.0.0.125            TCP        56 80 → 62969 [ACK] Seq=1 Ack=494 Win=30336 Len=0
   66 5.339570  128.119.245.12        10.0.0.125            HTTP      492 HTTP/1.1 200 OK  (text/html)
   67 5.380227  10.0.0.125            128.119.245.12        TCP        54 62969 → 80 [ACK] Seq=494 Ack=439 Win=65024 Len=0
   68 5.459511  180.163.231.104       10.0.0.125            TCP        62 80 → 62970 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=128
   69 5.459594  10.0.0.125            180.163.231.104       TCP        54 62970 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   70 5.459686  10.0.0.125            180.163.231.104       HTTP      727 POST /commonquery HTTP/1.1  (application/x-www-form-urlencoded)
   71 5.525230  10.0.0.125            54.208.232.164        TCP        54 62962 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
└  72 5.525291  10.0.0.125            54.208.232.164        TCP        54 62962 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
   73 5.525738  2601:1c0:8101:a60:b… 2001:558:feed::1      DNS       101 Standard query 0x5109 A api2.poperblocker.com
   74 5.525882  2601:1c0:8101:a60:b… 2001:558:feed::1      DNS       101 Standard query 0xeff4 AAAA api2.poperblocker.com
   75 5.531440  10.0.0.125            128.119.245.12        HTTP      485 GET /favicon.ico HTTP/1.1
   76 5.547089  2001:558:feed::1      2601:1c0:8101:a60:b… DNS       133 Standard query response 0x5109 A api2.poperblocker.com A 54.208.232.164 A 34.194.169.158
   77 5.547090  2001:558:feed::1      2601:1c0:8101:a60:b… DNS       178 Standard query response 0xeff4 AAAA api2.poperblocker.com SOA ns-93.awsdns-11.com
   78 5.547524  10.0.0.125            54.208.232.164        TCP        66 62971 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   79 5.629609  180.163.231.104       10.0.0.125            TCP        56 80 → 62970 [ACK] Seq=1 Ack=674 Win=16000 Len=0
   80 5.636170  180.163.231.104       10.0.0.125            HTTP      434 HTTP/1.1 200 OK
   81 5.636170  180.163.231.104       10.0.0.125            TCP        56 80 → 62970 [FIN, ACK] Seq=381 Ack=674 Win=16000 Len=0
   82 5.636221  10.0.0.125            180.163.231.104       TCP        54 62970 → 80 [ACK] Seq=674 Ack=382 Win=65280 Len=0
   83 5.636278  10.0.0.125            180.163.231.104       TCP        54 62970 → 80 [FIN, ACK] Seq=674 Ack=382 Win=65280 Len=0
   84 5.637258  128.119.245.12        10.0.0.125            HTTP      538 HTTP/1.1 404 Not Found  (text/html)
   85 5.644122  54.208.232.164        10.0.0.125            TCP        66 443 → 62971 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM=1 WS=256
   86 5.644194  10.0.0.125            54.208.232.164        TCP        54 62971 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   87 5.644479  10.0.0.125            54.208.232.164        TLSv1.2   571 Client Hello

    Identification: 0x546d (21613)
  > Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xbc71 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.0.125

0000  48 1d 70 22 f1 b4 80 c5  f2 9e 4b f9 08 00 45 00   H·p"····  ··K···E·
0010  00 28 54 6d 40 00 40 06  bc 71 0a 00 00 7d 36 d0   ·(Tm@·@·  ·q···}6·
0020  e8 a4 f5 f2 01 bb e2 98  4e e6 3c 0a 5f 79 50 14   ········  N·<·_yP·
0030  00 00 c1 2e 00 00                                  ···.··
```

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*.)
   - The amount of time it took to receive HTTP OK replay was 0.11 seconds.

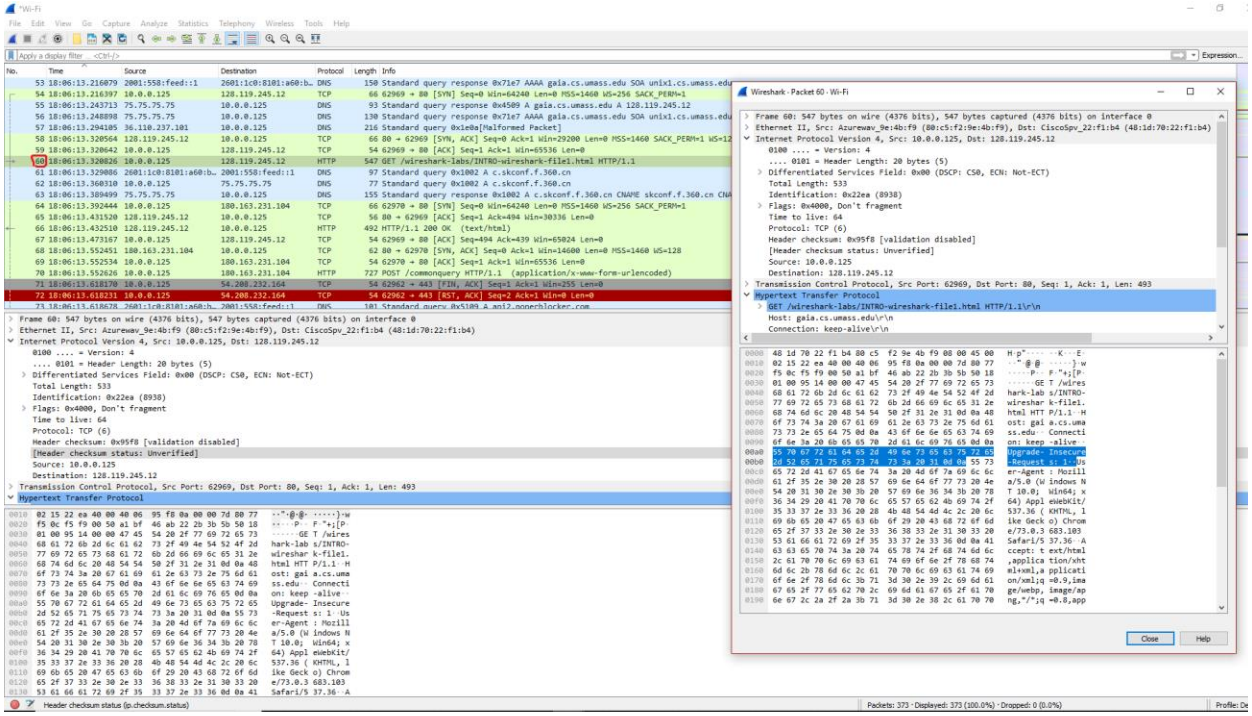

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http

No.  Time             Source           Destination      Protocol  Length Info
60 18:06:13.320826 10.0.0.125       128.119.245.12   HTTP      547 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
66 18:06:13.432510 128.119.245.12   10.0.0.125       HTTP      492 HTTP/1.1 200 OK  (text/html)
70 18:06:13.552626 10.0.0.125       180.163.231.104  HTTP      727 POST /commonquery HTTP/1.1  (application/x-www-form-urlencoded)
75 18:06:13.624380 10.0.0.125       128.119.245.12   HTTP      485 GET /favicon.ico HTTP/1.1
80 18:06:13.729110 180.163.231.104  10.0.0.125       HTTP      434 HTTP/1.1 200 OK
84 18:06:13.730198 128.119.245.12   10.0.0.125       HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?
    - The Internet address of the website is **128.119.245.12** and the address for my computer is **10.0.0.125**. The image above can support this with detail.

4. Screenshot the two HTTP messages (GET and OK) referred to in question 2 above. Make sure to include all pertinent information in the screenshot (Time field, Internet addresses, etc). Paste these screenshots into your lab report.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
Wireshark · Packet 60 · Wi-Fi
Close
Help

```
No.  Time               Source                 Destination        Protocol Length Info
  53 18:06:13.216079    2001:558:feed::1       2601:1c0:8101:a60:b… DNS      150 Standard query response 0x71e7 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
  54 18:06:13.216397    10.0.0.125             128.119.245.12     TCP       66 62969 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  55 18:06:13.243713    75.75.75.75            10.0.0.125         DNS       93 Standard query response 0x4509 A gaia.cs.umass.edu A 128.119.245.12
  56 18:06:13.248898    75.75.75.75            10.0.0.125         DNS      130 Standard query response 0x71e7 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
  57 18:06:13.294105    36.110.237.101         10.0.0.125         DNS      216 Standard query 0x1e0a[Malformed Packet]
  58 18:06:13.320564    128.119.245.12         10.0.0.125         TCP       66 80 → 62969 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=12
  59 18:06:13.320642    10.0.0.125             128.119.245.12     TCP       54 62969 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  60 18:06:13.320826    10.0.0.125             128.119.245.12     HTTP     547 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  61 18:06:13.329086    2601:1c0:8101:a60:b…   2001:558:feed::1   DNS       97 Standard query 0x1002 A c.skconf.f.360.cn
  62 18:06:13.360310    10.0.0.125             75.75.75.75        DNS       77 Standard query 0x1002 A c.skconf.f.360.cn
  63 18:06:13.389499    75.75.75.75            10.0.0.125         DNS      155 Standard query response 0x1002 A c.skconf.f.360.cn CNAME skconf.f.360.cn CNA
  64 18:06:13.392444    10.0.0.125             180.163.231.104    TCP       66 62970 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  65 18:06:13.431520    128.119.245.12         10.0.0.125         TCP       56 80 → 62969 [ACK] Seq=1 Ack=494 Win=30336 Len=0
  66 18:06:13.432510    128.119.245.12         10.0.0.125         HTTP     492 HTTP/1.1 200 OK  (text/html)
  67 18:06:13.473167    10.0.0.125             128.119.245.12     TCP       54 62969 → 80 [ACK] Seq=494 Ack=439 Win=65024 Len=0
  68 18:06:13.552451    180.163.231.104        10.0.0.125         TCP       62 80 → 62970 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=128
  69 18:06:13.552534    10.0.0.125             180.163.231.104    TCP       54 62970 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  70 18:06:13.552626    10.0.0.125             180.163.231.104    HTTP     727 POST /commonquery HTTP/1.1  (application/x-www-form-urlencoded)
  71 18:06:13.618170    10.0.0.125             54.208.232.164     TCP       54 62962 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
  72 18:06:13.618231    10.0.0.125             54.208.232.164     TCP       54 62962 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
  73 18:06:13.618678    2601:1c0:8101:a60:b…   2001:558:feed::1   DNS      101 Standard query 0x5109 A api2.popcrblocker.com
```

```
> Frame 60: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface 0
> Ethernet II, Src: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9), Dst: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4)
v Internet Protocol Version 4, Src: 10.0.0.125, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 533
    Identification: 0x22ea (8938)
  > Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x95f8 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.0.125
    Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 62969, Dst Port: 80, Seq: 1, Ack: 1, Len: 493
v Hypertext Transfer Protocol
```

```
0010  02 15 22 ea 40 00 40 06  95 f8 0a 00 00 7d 80 77   ··"·@·@· ·····}·w
0020  f5 0c f5 f9 00 50 a1 bf  46 ab 22 2b 3b 5b 50 18   ·····P·· F·"+;[P·
0030  01 00 95 14 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  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 55 73   -Request s: 1··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
00d0  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows N
00e0  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b 20 78   T 10.0;  Win64; x
00f0  36 34 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   64) Appl eWebKit/
0100  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
0110  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
0120  65 2f 37 33 2e 30 2e 33  36 38 33 2e 31 30 33 20   e/73.0.3 683.103 
0130  53 61 66 61 72 69 2f 35  33 37 2e 33 36 0d 0a 41   Safari/5 37.36··A
```

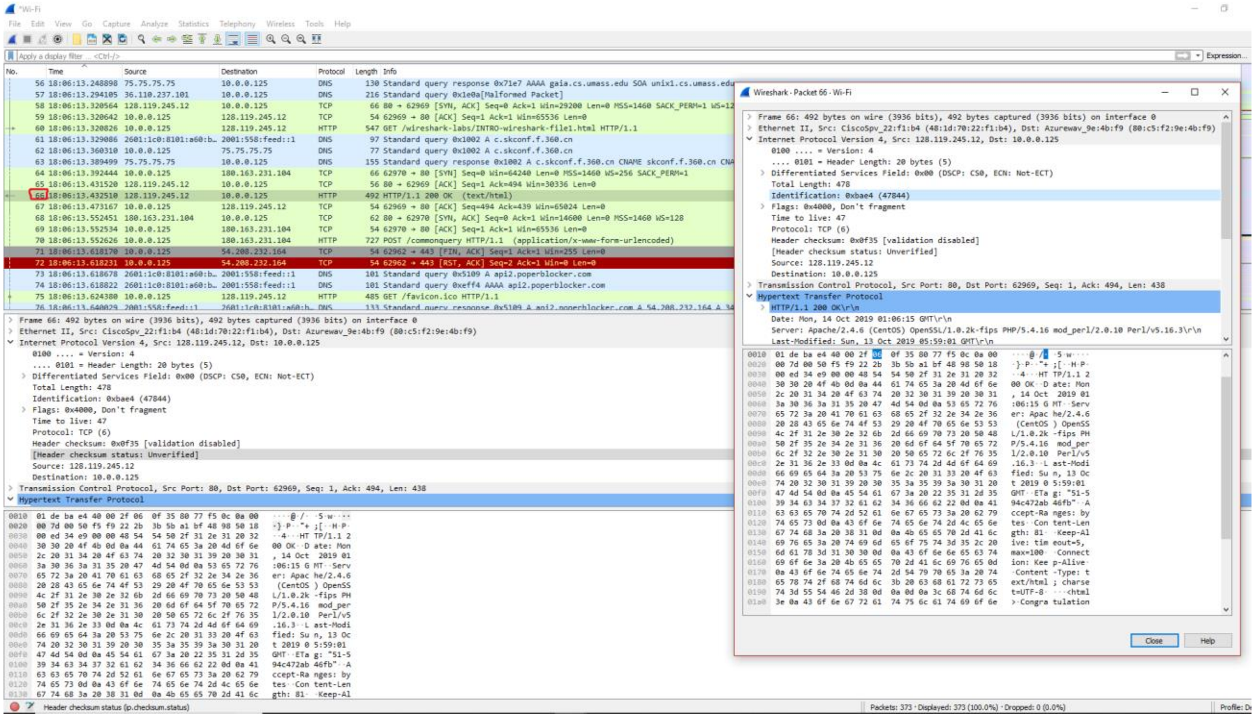
Header checksum status (ip.checksum.status)

```
> Frame 60: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface 0
> Ethernet II, Src: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9), Dst: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4)
v Internet Protocol Version 4, Src: 10.0.0.125, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 533
    Identification: 0x22ea (8938)
  > Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x95f8 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.0.125
    Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 62969, Dst Port: 80, Seq: 1, Ack: 1, Len: 493
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
```

```
0000  48 1d 70 22 f1 b4 80 c5  f2 9e 4b f9 08 00 45 00   H·p"···· ··K···E·
0010  02 15 22 ea 40 00 40 06  95 f8 0a 00 00 7d 80 77   ··"·@·@· ·····}·w
0020  f5 0c f5 f9 00 50 a1 bf  46 ab 22 2b 3b 5b 50 18   ·····P·· F·"+;[P·
0030  01 00 95 14 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  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 55 73   -Request s: 1··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
00d0  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows N
00e0  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b 20 78   T 10.0;  Win64; x
00f0  36 34 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   64) Appl eWebKit/
0100  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
0110  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
0120  65 2f 37 33 2e 30 2e 33  36 38 33 2e 31 30 33 20   e/73.0.3 683.103 
0130  53 61 66 61 72 69 2f 35  33 37 2e 33 36 0d 0a 41   Safari/5 37.36··A
0140  63 63 65 70 74 3a 20 74  65 78 74 2f 68 74 6d 6c   ccept: t ext/html
0150  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74   ,applica tion/xht
0160  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63 61 74 69   ml+xml,a pplicati
0170  6f 6e 2f 78 6d 6c 3b 71  3d 30 2e 39 2c 69 6d 61   on/xml;q =0.9,ima
0180  67 65 2f 77 65 62 70 2c  69 6d 61 67 65 2f 61 70   ge/webp, image/ap
0190  6e 67 2c 2a 2f 2a 3b 71  3d 30 2e 38 2c 61 70 70   ng,*/*;q =0.8,app
```

Packets: 373 · Displayed: 373 (100.0%) · Dropped: 0 (0.0%)

Profile: De


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
Wireshark · Packet 66 · Wi-Fi
Close
Help

```
No.   Time               Source                 Destination            Protocol Length Info
   56 18:06:13.248898    75.75.75.75            10.0.0.125             DNS      130 Standard query response 0x71e7 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
   57 18:06:13.294105    36.110.237.101         10.0.0.125             DNS      216 Standard query 0x1e0a[Malformed Packet]
   58 18:06:13.320564    128.119.245.12         10.0.0.125             TCP       66 80 → 62969 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=12
   59 18:06:13.320642    10.0.0.125             128.119.245.12         TCP       54 62969 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   60 18:06:13.320826    10.0.0.125             128.119.245.12         HTTP     547 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   61 18:06:13.329086    2601:1c0:8101:a60:b…   2001:558:feed::1       DNS       97 Standard query 0x1002 A c.skconf.f.360.cn
   62 18:06:13.360310    10.0.0.125             75.75.75.75            DNS       77 Standard query 0x1002 A c.skconf.f.360.cn
   63 18:06:13.389499    75.75.75.75            10.0.0.125             DNS      155 Standard query response 0x1002 A c.skconf.f.360.cn CNAME skconf.f.360.cn CNA
   64 18:06:13.392444    10.0.0.125             180.163.231.104        TCP       66 62970 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   65 18:06:13.431520    128.119.245.12         10.0.0.125             TCP       56 80 → 62969 [ACK] Seq=1 Ack=494 Win=30336 Len=0
   66 18:06:13.432510    128.119.245.12         10.0.0.125             HTTP     492 HTTP/1.1 200 OK  (text/html)
   67 18:06:13.473167    10.0.0.125             128.119.245.12         TCP       54 62969 → 80 [ACK] Seq=494 Ack=439 Win=65024 Len=0
   68 18:06:13.552451    180.163.231.104        10.0.0.125             TCP       62 80 → 62970 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=128
   69 18:06:13.552534    10.0.0.125             180.163.231.104        TCP       54 62970 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   70 18:06:13.552626    10.0.0.125             180.163.231.104        HTTP     727 POST /commonquery HTTP/1.1  (application/x-www-form-urlencoded)
   71 18:06:13.618170    10.0.0.125             54.208.232.164         TCP       54 62962 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
   72 18:06:13.618231    10.0.0.125             54.208.232.164         TCP       54 62962 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
   73 18:06:13.618678    2601:1c0:8101:a60:b…   2001:558:feed::1       DNS      101 Standard query 0x5109 A api2.poperblocker.com
   74 18:06:13.618822    2601:1c0:8101:a60:b…   2001:558:feed::1       DNS      101 Standard query 0xeff4 AAAA api2.poperblocker.com
   75 18:06:13.624380    10.0.0.125             128.119.245.12         HTTP     485 GET /favicon.ico HTTP/1.1
   76 18:06:13.640029    2001:558:feed::1       2601:1c0:8101:a60:b…   DNS      133 Standard query response 0x5109 A api2.poperblocker.com A 54.208.232.164 A 34
```

```
> Frame 66: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
> Ethernet II, Src: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4), Dst: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9)
v Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.125
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 478
    Identification: 0xbae4 (47844)
  > Flags: 0x4000, Don't fragment
    Time to live: 47
    Protocol: TCP (6)
    Header checksum: 0x0f35 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 10.0.0.125
> Transmission Control Protocol, Src Port: 80, Dst Port: 62969, Seq: 1, Ack: 494, Len: 438
v Hypertext Transfer Protocol
```

```
0010  01 de ba e4 40 00 2f 06  0f 35 80 77 f5 0c 0a 00   ····@·/· ·5·w···
0020  00 7d 00 50 f5 f9 22 2b  3b 5b a1 bf 48 98 50 18   ·}·P··"+ ;[··H·P·
0030  00 ed 34 e9 00 00 48 54  54 50 2f 31 2e 31 20 32   ··4···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D ate: Mon
0050  2c 20 31 34 20 4f 63 74  20 32 30 31 39 20 30 31   , 14 Oct  2019 01
0060  3a 30 36 3a 31 35 20 47  4d 54 0d 0a 53 65 72 76   :06:15 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 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16  mod_per
00b0  6c 2f 32 2e 30 2e 31 30  20 50 65 72 6c 2f 76 35   l/2.0.10  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 53 75  6e 2c 20 31 33 20 4f 63   fied: Su n, 13 Oc
00e0  74 20 32 30 31 39 20 30  35 3a 35 39 3a 30 31 20   t 2019 0 5:59:01
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 35 31 2d 35   GMT··ETa g: "51-5
0100  39 34 63 34 37 32 61 62  34 36 66 62 22 0d 0a 41   94c472ab 46fb"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 38 31 0d  0a 4b 65 65 70 2d 41 6c   gth: 81· ·Keep-Al
```

Header checksum status (ip.checksum.status)

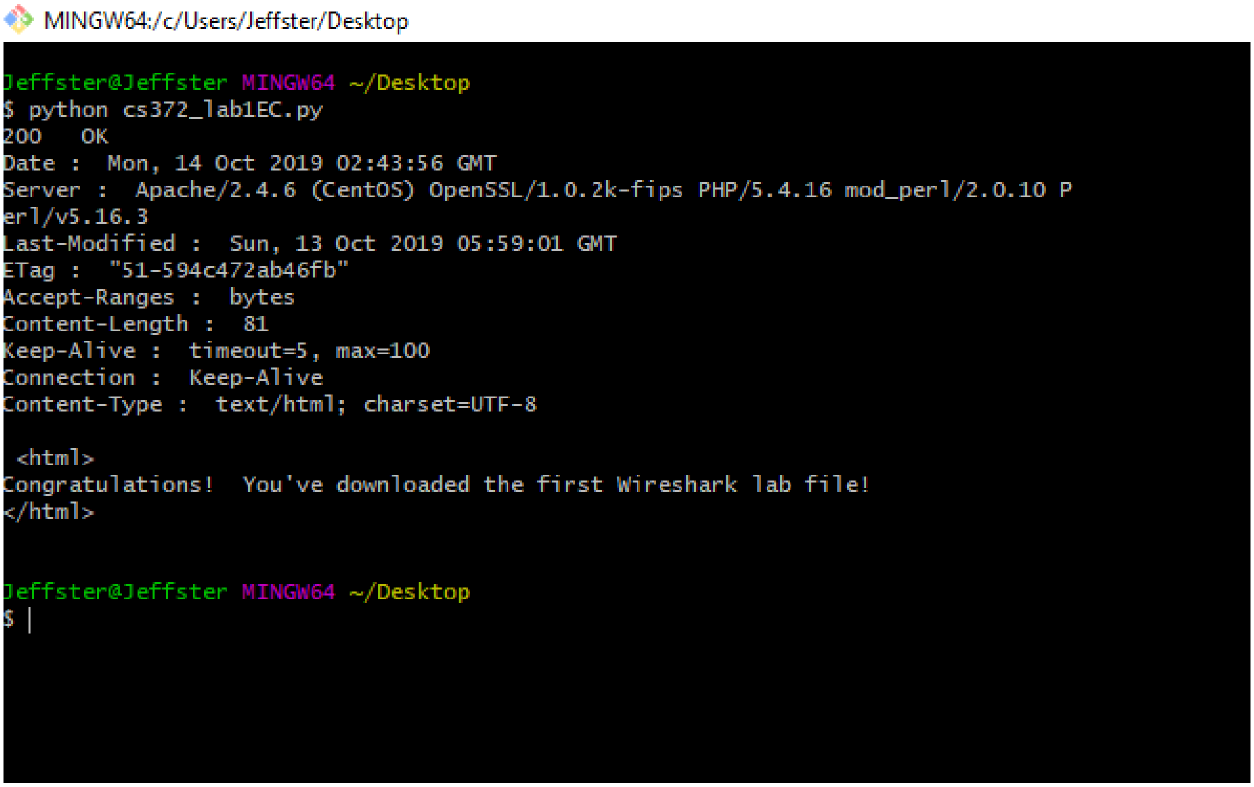
Packets: 373 · Displayed: 373 (100.0%) · Dropped: 0 (0.0%)

Profile: De

```
> Frame 66: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
> Ethernet II, Src: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4), Dst: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9)
v Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.125
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 478
    Identification: 0xbae4 (47844)
  > Flags: 0x4000, Don't fragment
    Time to live: 47
    Protocol: TCP (6)
    Header checksum: 0x0f35 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 10.0.0.125
> Transmission Control Protocol, Src Port: 80, Dst Port: 62969, Seq: 1, Ack: 494, Len: 438
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 14 Oct 2019 01:06:15 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: Sun, 13 Oct 2019 05:59:01 GMT\r\n
```

```
0010  01 de ba e4 40 00 2f 06  0f 35 80 77 f5 0c 0a 00   ····@·/· ·5·w···
0020  00 7d 00 50 f5 f9 22 2b  3b 5b a1 bf 48 98 50 18   ·}·P··"+ ;[··H·P·
0030  00 ed 34 e9 00 00 48 54  54 50 2f 31 2e 31 20 32   ··4···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D ate: Mon
0050  2c 20 31 34 20 4f 63 74  20 32 30 31 39 20 30 31   , 14 Oct  2019 01
0060  3a 30 36 3a 31 35 20 47  4d 54 0d 0a 53 65 72 76   :06:15 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 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16  mod_per
00b0  6c 2f 32 2e 30 2e 31 30  20 50 65 72 6c 2f 76 35   l/2.0.10  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 53 75  6e 2c 20 31 33 20 4f 63   fied: Su n, 13 Oc
00e0  74 20 32 30 31 39 20 30  35 3a 35 39 3a 30 31 20   t 2019 0 5:59:01
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 35 31 2d 35   GMT··ETa g: "51-5
0100  39 34 63 34 37 32 61 62  34 36 66 62 22 0d 0a 41   94c472ab 46fb"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 38 31 0d  0a 4b 65 65 70 2d 41 6c   gth: 81· ·Keep-Al
0140  69 76 65 3a 20 74 69 6d  65 6f 75 74 3d 35 2c 20   ive: tim eout=5,
0150  6d 61 78 3d 31 30 30 0d  0a 43 6f 6e 6e 65 63 74   max=100· ·Connect
0160  69 6f 6e 3a 20 4b 65 65  70 2d 41 6c 69 76 65 0d   ion: Kee p-Alive·
0170  0a 43 6f 6e 74 65 6e 74  2d 54 79 70 65 3a 20 74   ·Content -Type: t
0180  65 78 74 2f 68 74 6d 6c  3b 20 63 68 61 72 73 65   ext/html ; charse
0190  74 3d 55 54 46 2d 38 0d  0a 0d 0a 3c 68 74 6d 6c   t=UTF-8· ···<html
01a0  3e 0a 43 6f 6e 67 72 61  74 75 6c 61 74 69 6f 6e   >·Congra tulation
```

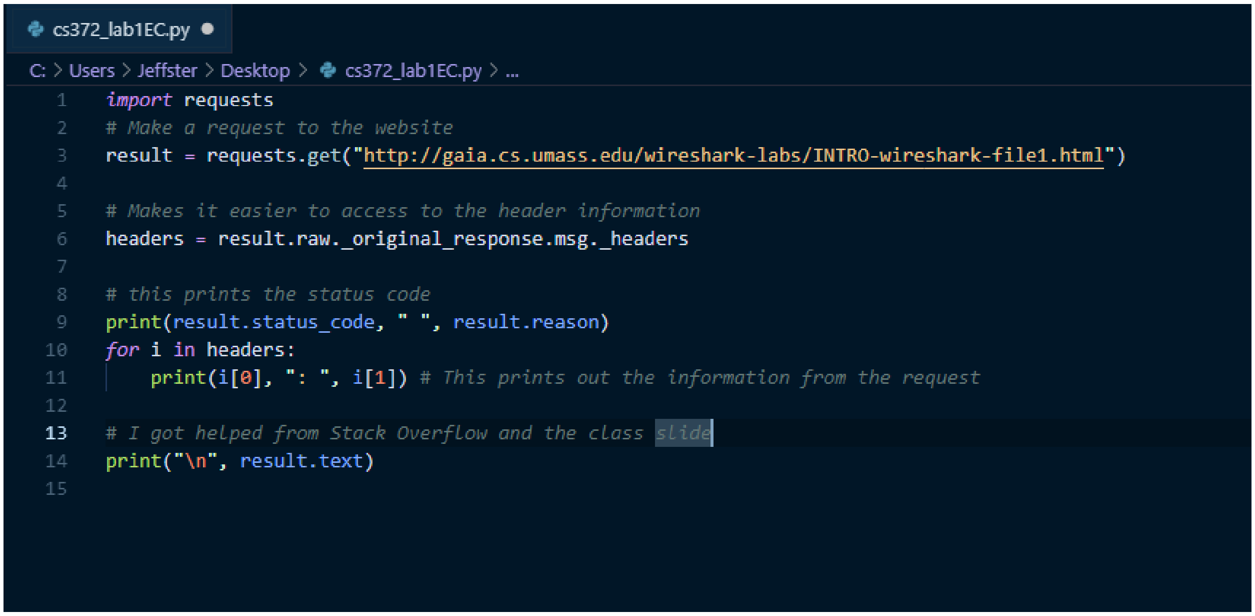
Extra Credit:



```
Jeffster@Jeffster MINGW64 ~/Desktop
$ python cs372_lab1EC.py
200   OK
Date :  Mon, 14 Oct 2019 02:43:56 GMT
Server :  Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 P
erl/v5.16.3
Last-Modified :  Sun, 13 Oct 2019 05:59:01 GMT
ETag :  "51-594c472ab46fb"
Accept-Ranges :  bytes
Content-Length :  81
Keep-Alive :  timeout=5, max=100
Connection :  Keep-Alive
Content-Type :  text/html; charset=UTF-8

 <html>
Congratulations!  You've downloaded the first Wireshark lab file!
</html>


Jeffster@Jeffster MINGW64 ~/Desktop
$ |
```



```python
import requests
# Make a request to the website
result = requests.get("http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html")

# Makes it easier to access to the header information
headers = result.raw._original_response.msg._headers

# this prints the status code
print(result.status_code, " ", result.reason)
for i in headers:
    print(i[0], ": ", i[1]) # This prints out the information from the request

# I got helped from Stack Overflow and the class slide
print("\n", result.text)

```