Theodore Kim
CS-GY 6843
Lab 1 – Getting Started with Wireshark

1. TCP, UDP, HTTP
2. 0.011369 seconds
3. (My computer) 192.168.0.100, (www.net.cs.umass.edu) 128.119.245.12
4.

GET Request

```
    1924 37.271656      192.168.0.100        128.119.245.12       HTTP     422    GET /wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1
Frame 1924: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface 0
Ethernet II, Src: RivetNet_e1:f0:cf (9c:b6:d0:e1:f0:cf), Dst: Tp-LinkT_97:5f:e8 (60:e3:27:97:5f:e8)
Internet Protocol Version 4, Src: 192.168.0.100, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50555, Dst Port: 80, Seq: 1, Ack: 1, Len: 368
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
            [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/3]
    [Response in frame: 1929]
    [Next request in frame: 1932]
```

OK Response

```
   1929 37.283025      128.119.245.12       192.168.0.100        HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 1929: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Ethernet II, Src: Tp-LinkT_97:5f:e8 (60:e3:27:97:5f:e8), Dst: RivetNet_e1:f0:cf (9c:b6:d0:e1:f0:cf)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.100
Transmission Control Protocol, Src Port: 80, Dst Port: 50555, Seq: 1, Ack: 369, Len: 438
Hypertext Transfer Protocol
    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]
        Request Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Thu, 01 Feb 2018 04:15:31 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, 31 Jan 2018 06:59:01 GMT\r\n
    ETag: "51-5640d03997b78"\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 1/3]
    [Time since request: 0.011369000 seconds]
    [Request in frame: 1924]
    [Next request in frame: 1932]
    [Next response in frame: 1933]
    File Data: 81 bytes
Line-based text data: text/html
```