Wireshark Lab 1

Suyi Liu, Yuan Jing Vincent Yan

February 4 2017

1

TCP, HTTP and UDP

2

It took 16:05:39.903836 - 16:05:39.848833 = 0.055003 seconds.

3

Internet address of the gaia.cs.umass.edu: 128.119.245.12
Internet address of my computer: 10.1.101.149

4

GET (2nd page):
OK (3rd page):

```
   7229 65.069982      10.1.101.149          128.119.245.12        HTTP     489    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 7229: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface 0
Ethernet II, Src: RivetNet_0d:65:85 (9c:b6:d0:0d:65:85), Dst: Sonicwal_06:2e:44 (18:b1:69:06:2e:44)
Internet Protocol Version 4, Src: 10.1.101.149, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50510, Dst Port: 80, Seq: 1, Ack: 1, Len: 435
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
    Accept-Language: en-US,en;q=0.8,zh-Hans-CN;q=0.7,zh-Hans;q=0.5,zh-Hant-HK;q=0.3,zh-Hant;q=0.2\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/
14.14393\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\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: 7250]
```

```
   7250 65.124985      128.119.245.12        10.1.101.149          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 7250: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Ethernet II, Src: Sonicwal_06:2e:44 (18:b1:69:06:2e:44), Dst: RivetNet_0d:65:85 (9c:b6:d0:0d:65:85)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.1.101.149
Transmission Control Protocol, Src Port: 80, Dst Port: 50510, Seq: 1, Ack: 436, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sat, 04 Feb 2017 21:05:41 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sat, 04 Feb 2017 06:59:01 GMT\r\n
    ETag: "51-547aeeee194c7"\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: 0.055003000 seconds]
    [Request in frame: 7229]
    File Data: 81 bytes
Line-based text data: text/html
```