Joel Benjamin Castillo (jc5383) CS6843 - Computer Networking Prof. Rafail Portnoy

Wireshark Lab - Getting Started

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
    - TCP
    - UDP
    - DNS
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*.) `13:29:37.899814-13:29:37.695367 = .204447 S`
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? gaia.cs.umass.edu: `128.119.245.12` Computer: `192.168.1.3`
4. Print the two `HTTP` messages (`GET` and `OK`) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "*Selected Packet Only*" and "*Print as displayed*" radial buttons, and then click OK.

```
No.     Time               Source                Destination
Protocol Length Info
  48794 13:29:37.695367    192.168.1.3           128.119.245.12
HTTP     507    GET /
wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 48794: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bits)
on interface 0
Ethernet II, Src: Apple_75:4b:d3 (88:e9:fe:75:4b:d3), Dst:
NovatelW_9e:f2:db (00:15:ff:9e:f2:db)
Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50694, Dst Port: 80, Seq: 1, Ack:
1, Len: 441
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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6)
AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/69.0.3497.92 Safari/537.36\r\n
    Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apn
g,*/
*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,es;q=0.8\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: 48800]
No.      Time               Source                Destination
Protocol Length Info
  48800 13:29:37.899814    128.119.245.12        192.168.1.3
HTTP     504    HTTP/1.1
200 OK  (text/html)
Frame 48800: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits)
on interface 0
Ethernet II, Src: NovatelW_9e:f2:db (00:15:ff:9e:f2:db), Dst:
Apple_75:4b:d3 (88:e9:fe:75:4b:d3)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.3
Transmission Control Protocol, Src Port: 80, Dst Port: 50694, Seq: 1, Ack:
442, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sat, 15 Sep 2018 17:29:37 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: Sat, 15 Sep 2018 05:59:01 GMT\r\n
    ETag: "51-575e2a2ff0dc3"\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: 0.204447000 seconds]
    [Request in frame: 48794]
    [Next response in frame: 48805]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```