California State University, Monterey Bay

Week 1 – Lab 1

Clarence Mitchell

CST331

Introduction to Computer Networks

SUMMER 2015

Instructor: Dr. Anand Seetharam

Problem

The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running, and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation:

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
    a. HTTP
    b. TCP
    c. 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 packetlisting 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.)
    a. 11 Seconds
3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?
    a. IP Address of gaia.cs.umass.edu is 128.119.245.12
    b. IP Address of my computer is 10.32.89.137 (from wifi using dynamic IP address assignment)
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

Print 1

```
No.     Time                           Source                Destination
Protocol Length Info
    124 2015-05-06 00:18:24.596698000 10.32.89.137          128.119.245.12
HTTP     524    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 124: 524 bytes on wire (4192 bits), 524 bytes captured (4192 bits) on
interface 0
    Interface id: 0 (\Device\NPF_{A68CEA27-5F02-46C2-9106-5FBC1CDDB2EB})
    Encapsulation type: Ethernet (1)
    Arrival Time: May  6, 2015 00:18:24.596698000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1430896704.596698000 seconds
    [Time delta from previous captured frame: 0.273549000 seconds]
    [Time delta from previous displayed frame: 1.066990000 seconds]
    [Time since reference or first frame: 9.508020000 seconds]
    Frame Number: 124
    Frame Length: 524 bytes (4192 bits)
    Capture Length: 524 bytes (4192 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Number of per-protocol-data: 1]
    [Hypertext Transfer Protocol, key 0]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb), Dst: AsustekC_92:e5:90
(e0:3f:49:92:e5:90)
    Destination: AsustekC_92:e5:90 (e0:3f:49:92:e5:90)
        Address: AsustekC_92:e5:90 (e0:3f:49:92:e5:90)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb)
        Address: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.32.89.137 (10.32.89.137), Dst: 128.119.245.12
(128.119.245.12)
    Version: 4
    Header Length: 20 bytes
    Differentiated Services Field: 0xb8 (DSCP 0x2e: Expedited Forwarding; ECN:
0x00: Not-ECT (Not ECN-Capable Transport))
        1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (0x2e)
        .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable
Transport) (0x00)
    Total Length: 510
    Identification: 0x494f (18767)
    Flags: 0x02 (Don't Fragment)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
```

```
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xd5c5 [validation disabled]
        [Good: False]
        [Bad: False]
    Source: 10.32.89.137 (10.32.89.137)
    Destination: 128.119.245.12 (128.119.245.12)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 19499 (19499), Dst Port: 80 (80), Seq: 1,
Ack: 1, Len: 470
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]
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/42.0.2311.90 Safari/537.36\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    If-None-Match: "51-515637de88bb4"\r\n
    If-Modified-Since: Wed, 06 May 2015 05:59:01 GMT\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: 126]
```

Print 2

```
No.     Time                           Source                Destination
Protocol Length Info
    126 2015-05-06 00:18:24.700080000 128.119.245.12        10.32.89.137
HTTP     296    HTTP/1.1 304 Not Modified

Frame 126: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on
interface 0
    Interface id: 0 (\Device\NPF_{A68CEA27-5F02-46C2-9106-5FBC1CDDB2EB})
    Encapsulation type: Ethernet (1)
    Arrival Time: May  6, 2015 00:18:24.700080000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1430896704.700080000 seconds
    [Time delta from previous captured frame: 0.000051000 seconds]
    [Time delta from previous displayed frame: 0.103382000 seconds]
    [Time since reference or first frame: 9.611402000 seconds]
    Frame Number: 126
```

```
    Frame Length: 296 bytes (2368 bits)
    Capture Length: 296 bytes (2368 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Number of per-protocol-data: 1]
    [Hypertext Transfer Protocol, key 0]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: AsustekC_92:e5:90 (e0:3f:49:92:e5:90), Dst: HonHaiPr_62:0a:cb
(ac:d1:b8:62:0a:cb)
    Destination: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb)
        Address: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: AsustekC_92:e5:90 (e0:3f:49:92:e5:90)
        Address: AsustekC_92:e5:90 (e0:3f:49:92:e5:90)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
10.32.89.137 (10.32.89.137)
    Version: 4
    Header Length: 20 bytes
    Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00:
Not-ECT (Not ECN-Capable Transport))
        0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
        .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable
Transport) (0x00)
    Total Length: 282
    Identification: 0x3290 (12944)
    Flags: 0x02 (Don't Fragment)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 47
    Protocol: TCP (6)
    Header checksum: 0x3f01 [validation disabled]
        [Good: False]
        [Bad: False]
    Source: 128.119.245.12 (128.119.245.12)
    Destination: 10.32.89.137 (10.32.89.137)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 19499 (19499), Seq: 1,
Ack: 471, Len: 242
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        Request Version: HTTP/1.1
        Status Code: 304
        Response Phrase: Not Modified
    Date: Wed, 06 May 2015 07:17:26 GMT\r\n
```

```
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9-dev
Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "51-515637de88bb4"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.103382000 seconds]
    [Request in frame: 124]
```