CSCE 560
2nd Lt David Crow

Wireshark Lab 1

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

   Among others, I see TCP, DNS, and HTTP.

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*.)

   $$12:24:13.056824 - 12:24:13.010346 = 0.046478\ seconds$$
   $$= 46.478\ milliseconds$$

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 IP address of the website is 128.119.245.12. The IP address of my computer - on my local network - is 192.168.1.5. I recognize that that's just my IP address on my local network, and that my router uses NAT to produce a public address.

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.

   Okay. It's on the back of this page.

```
No.     Time               Source                Destination           Protocol Length Info
    120 12:24:13.010346    192.168.1.5           128.119.245.12        HTTP     470    GET /
wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 120: 470 bytes on wire (3760 bits), 470 bytes captured (3760 bits) on interface 0
Ethernet II, Src: Apple_9e:e0:f8 (8c:85:90:9e:e0:f8), Dst: Sagemcom_30:b6:4a (34:6b:
46:30:b6:4a)
Internet Protocol Version 4, Src: 192.168.1.5, 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: 456
    Identification: 0x0000 (0)
    Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x01ff [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.5
    Destination: 128.119.245.12
Transmission Control Protocol, Src Port: 52221, Dst Port: 80, Seq: 1, Ack: 1, Len: 404
Hypertext Transfer Protocol
No.     Time               Source                Destination           Protocol Length Info
    133 12:24:13.056824    128.119.245.12        192.168.1.5           HTTP     504    HTTP/1.1
200 OK  (text/html)
Frame 133: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface 0
Ethernet II, Src: Sagemcom_30:b6:4f (34:6b:46:30:b6:4f), Dst: Apple_9e:e0:f8 (8c:
85:90:9e:e0:f8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 490
    Identification: 0xe0d6 (57558)
    Flags: 0x4000, Don't fragment
    Time to live: 46
    Protocol: TCP (6)
    Header checksum: 0x3306 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 192.168.1.5
Transmission Control Protocol, Src Port: 80, Dst Port: 52221, Seq: 1, Ack: 405, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```