

Shouq Alamer
IT-520-LAB1
Jan 31 2019

```
MacBook-Air-alkhas-b-shoug:~ shouqalamer$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=3<RXCSUM,TXCSUM>
    inet6 ::1 prefixlen 128
    inet 127.0.0.1 netmask 0xff000000
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=1<PERFORMNUD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 7c:d1:c3:e0:c6:eb
    inet6 fe80::7ed1:c3ff:fee0:c6eb%en0 prefixlen 64 scopeid 0x4
    inet 192.168.0.74 netmask 0xfffff00 broadcast 192.168.0.255
    inet6 2001:579:a048:13:7ed1:c3ff:fee0:c6eb prefixlen 64 autoconf
    inet6 2001:579:a048:13:48bd:d32e:3467:a66d prefixlen 64 autoconf temporary
    inet6 2001:579:a048:13::a2f5 prefixlen 64 dynamic
    nd6 options=1<PERFORMNUD>
    media: autoselect
    status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=60<TS04,TS06>
    ether 32:00:11:60:a7:40
    media: autoselect <full-duplex>
    status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=63<RXCSUM,TXCSUM,TS04,TS06>
    ether 7e:d1:c3:0e:87:00
    Configuration:
        id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
        maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
        root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
        ipfilter disabled flags 0x2
    member: en1 flags=3<LEARNING,DISCOVER>
        ifmaxaddr 0 port 5 priority 0 path cost 0
    nd6 options=1<PERFORMNUD>
    media: <unknown type>
    status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    ether 0e:d1:c3:e0:c6:eb
    media: autoselect
    status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1452
    ether ea:01:31:9b:dc:11
    inet6 fe80::e801:31ff:fe9b:dc11%awdl0 prefixlen 64 scopeid 0x8
```

Questions:

1. What is the Internet address of your computer?

192.168.0.74

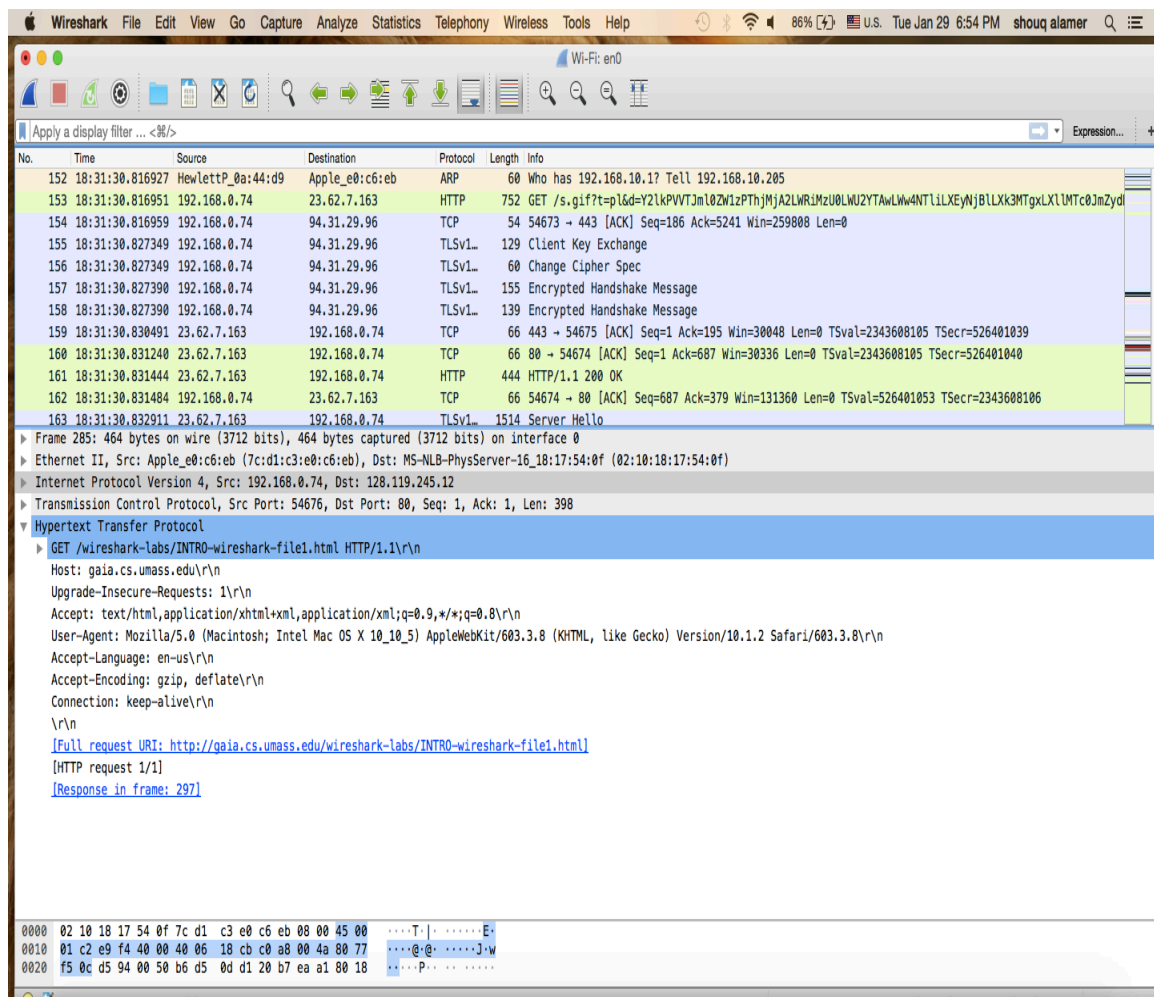
The image shows a Wireshark network traffic capture. The top toolbar includes buttons for File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right shows the date and time as Tue Jan 29 6:35 PM, the user as shouq alamer, and the network interface as Wi-Fi: en0. The main display area shows a list of captured packets. The selected packet is number 285, which is an HTTP GET request from 192.168.0.74 to 128.119.245.12. The packet details pane shows the following information:

- Frame 285: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface 0
- Ethernet II, Src: Apple_08:c6:eb (7c:d1:c3:e0:c6:eb), Dst: MS-NL8-PhysServer-16_18:17:54:0f (02:10:18:17:54:0f)
- Internet Protocol Version 4, Src: 192.168.0.74, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 54676, Dst Port: 80, Seq: 1, Ack: 1, Len: 398
- Hypertext Transfer Protocol
 - GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
 - Host: gaia.cs.umass.edu\r\n
 - Upgrade-Insecure-Requests: 1\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
 - User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.1.2 Safari/603.3.8\r\n
 - Accept-Language: en-us\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Connection: keep-alive\r\n

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, the IP header, the TCP header, and the HTTP request body.

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

ARP
HTTP
TCP



3. 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*.)

GET = 18:31:32:789328

OK = 18:31:32:816199

DIFFERENCE= 00:00:00:026871

Wireshark packet capture showing an HTTP GET request and its 200 OK response. The packet list shows the GET request at time 18:31:32.789328 and the OK response at 18:31:32.816199. The packet details pane shows the full HTTP request and response structure.

No.	Time	Source	Destination	Protocol	Length	Info
153	18:31:30.816951	192.168.0.74	23.62.7.163	HTTP	752	GET /s.gif?t=p1&d=Y2lkPVVTJm10ZW1zPThjMjA2LWR1MzU0LWU2YTAwLW44NTI1LXExNjB1LXk3MTgxLX1UMTc0JmZydl
161	18:31:30.831444	23.62.7.163	192.168.0.74	HTTP	444	HTTP/1.1 200 OK
285	18:31:32.789328	192.168.0.74	128.119.245.12	HTTP	464	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
297	18:31:32.816199	128.119.245.12	192.168.0.74	HTTP	504	HTTP/1.1 200 OK (text/html)

Frame 285: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface 0
Ethernet II, Src: Apple_eb:c6:eb (7c:d1:c3:e0:c6:eb), Dst: MS-NLB-PhysServer-16_18:17:54:0f (02:10:18:17:54:0f)
Internet Protocol Version 4, Src: 192.168.0.74, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54676, Dst Port: 80, Seq: 1, Ack: 1, Len: 398
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nUpgrade-Insecure-Requests: 1\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.1.2 Safari/603.3.8\r\nAccept-Language: en-us\r\nAccept-Encoding: gzip, deflate\r\nConnection: 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: 297]

0000 02 10 18 17 54 0f 7c d1 c3 e0 c6 eb 00 00 45 00T.....E
0010 01 c2 e9 f4 40 00 00 06 18 cb c0 a8 00 4a 80 77@.....J.W
0020 f5 0c d5 94 00 50 b6 d5 0d d1 20 b7 ea a1 80 18P.....

Internet Protocol Version 4 (ip), 20 bytes Packets: 1107 - Displayed: 41 (3.7%) - Dropped: 0 (0.0%) Profile: Default

4. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)?

128.119.245.12

The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right shows the date and time as Tuesday, January 29, 2019, at 6:35 PM, and the user as shouq alamer. The interface is set to capture on the Wi-Fi interface 'en0'.

The packet list on the left shows a series of HTTP requests. The selected packet is packet 285, which is an HTTP GET request to 'http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html'. The packet details pane on the right shows the following information:

- Frame 285: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface 0
- Ethernet II, Src: Apple_08:c6:eb (7c:d1:c3:e0:c6:eb), Dst: MS-NL0-PhysServer-16_18:17:54:0f (02:10:10:17:54:0f)
- Internet Protocol Version 4, Src: 192.168.0.74, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 54676, Dst Port: 80, Seq: 1, Ack: 1, Len: 398
- Hypertext Transfer Protocol
 - GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
 - Host: gaia.cs.umass.edu\r\n
 - Upgrade-Insecure-Requests: 1\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
 - User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.1.2 Safari/603.3.8\r\n
 - Accept-Language: en-us\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Connection: keep-alive\r\n

The packet bytes pane at the bottom shows the raw data of the selected packet, including the HTTP request line and headers.

5. 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.

GET

/var/folders/2p/1gs3fhtn08ncl7wj3dnnprn00000gn/T//wireshark_en0_20190129183128_mZfOFI.pcapng 1107 total packets, 41 shown

No.	Time	Source	Destination	Protocol	Length	Info
285	18:31:32.789328	192.168.0.74	128.119.245.12	HTTP	464	GET /

wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 285: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface 0
Ethernet II, Src: Apple_e0:c6:eb (7c:d1:c3:e0:c6:eb), Dst: MS-NLB-PhysServer-16_18:17:54:0f (02:10:18:17:54:0f)
Internet Protocol Version 4, Src: 192.168.0.74, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54676, Dst Port: 80, Seq: 1, Ack: 1, Len: 398
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Upgrade-Insecure-Requests: 1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.1.2 Safari/603.3.8\r\n
Accept-Language: en-us\r\n
Accept-Encoding: gzip, deflate\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: 297]

OK

/var/folders/2p/1gs3fhtn08ncl7wj3dnnprn00000gn/T//wireshark_en0_20190129183128_mZfOFI.pcapng 1107 total packets, 41 shown

No.	Time	Source	Destination	Protocol	Length	Info
200	18:31:32.816199	128.119.245.12	192.168.0.74	HTTP	504	HTTP/1.1

200 OK (text/html)
Frame 297: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface 0
Ethernet II, Src: MS-NLB-PhysServer-16_18:17:54:0f (02:10:18:17:54:0f), Dst: Apple_e0:c6:eb (7c:d1:c3:e0:c6:eb)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.74
Transmission Control Protocol, Src Port: 80, Dst Port: 54676, Seq: 1, Ack: 399, Len: 438
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Tue, 29 Jan 2019 23:31:30 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: Tue, 29 Jan 2019 06:59:01 GMT\r\n
ETag: "51-580935402e3a9"\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: 0.026871000 seconds]
[Request in frame: 285]
File Data: 81 bytes
Line-based text data: text/html (3 lines)
<html>\n
Congratulations! You've downloaded the first Wireshark lab file!\n
</html>\n