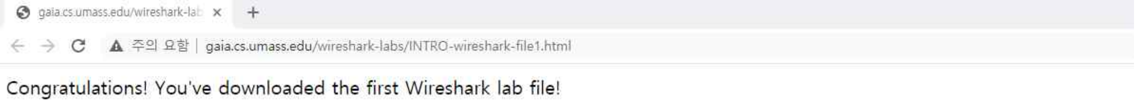
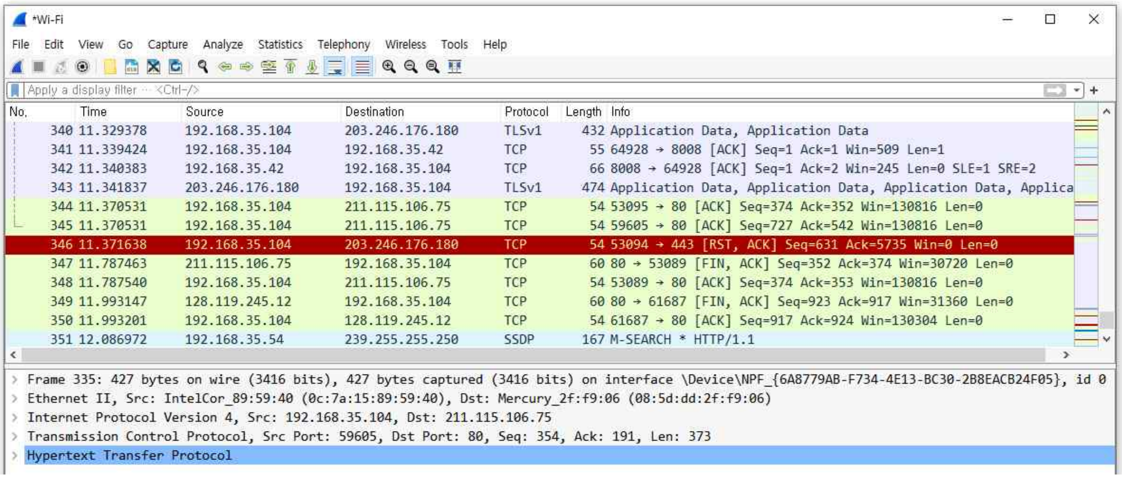
Homework #1 (Wireshark Introduction)

201724419 KimDongUk

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

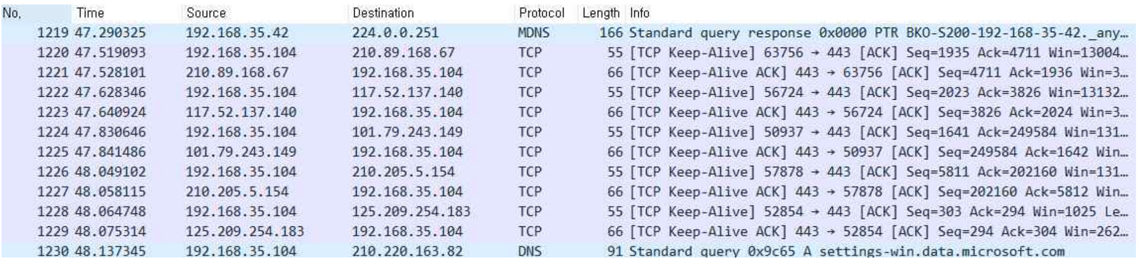

gaia.cs.umass.edu/wireshark-lab ×
+
주의 요함 | gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

Congratulations! You've downloaded the first Wireshark lab file!



No.	Time	Source	Destination	Protocol	Length	Info
340	11.329378	192.168.35.104	203.246.176.180	TLSv1	432	Application Data, Application Data
341	11.339424	192.168.35.104	192.168.35.42	TCP	55	64928 → 8008 [ACK] Seq=1 Ack=1 Win=509 Len=1
342	11.340383	192.168.35.42	192.168.35.104	TCP	66	8008 → 64928 [ACK] Seq=1 Ack=2 Win=245 Len=0 SLE=1 SRE=2
343	11.341837	203.246.176.180	192.168.35.104	TLSv1	474	Application Data, Application Data, Application Data, Applica
344	11.370531	192.168.35.104	211.115.106.75	TCP	54	53095 → 80 [ACK] Seq=374 Ack=352 Win=130816 Len=0
345	11.370531	192.168.35.104	211.115.106.75	TCP	54	59605 → 80 [ACK] Seq=727 Ack=542 Win=130816 Len=0
346	11.371638	192.168.35.104	203.246.176.180	TCP	54	53094 → 443 [RST, ACK] Seq=631 Ack=5735 Win=0 Len=0
347	11.787463	211.115.106.75	192.168.35.104	TCP	60	80 → 53089 [FIN, ACK] Seq=352 Ack=374 Win=30720 Len=0
348	11.787540	192.168.35.104	211.115.106.75	TCP	54	53089 → 80 [ACK] Seq=374 Ack=353 Win=130816 Len=0
349	11.993147	128.119.245.12	192.168.35.104	TCP	60	80 → 61687 [FIN, ACK] Seq=923 Ack=917 Win=31360 Len=0
350	11.993201	192.168.35.104	128.119.245.12	TCP	54	61687 → 80 [ACK] Seq=917 Ack=924 Win=130304 Len=0
351	12.086972	192.168.35.54	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1

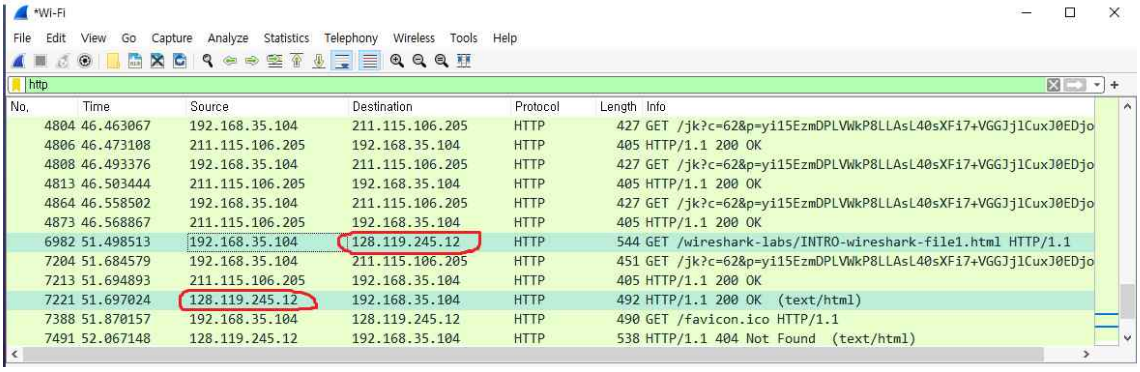
```
> Frame 335: 427 bytes on wire (3416 bits), 427 bytes captured (3416 bits) on interface \Device\NPF_{6A8779AB-F734-4E13-BC30-2B8EACB24F05}, id 0
> Ethernet II, Src: IntelCor_89:59:40 (0c:7a:15:89:59:40), Dst: Mercury_2f:f9:06 (08:5d:dd:2f:f9:06)
> Internet Protocol Version 4, Src: 192.168.35.104, Dst: 211.115.106.75
> Transmission Control Protocol, Src Port: 59605, Dst Port: 80, Seq: 354, Ack: 191, Len: 373
> Hypertext Transfer Protocol
```



No.	Time	Source	Destination	Protocol	Length	Info
1219	47.290325	192.168.35.42	224.0.0.251	MDNS	166	Standard query response 0x0000 PTR BKO-S200-192-168-35-42._any…
1220	47.519093	192.168.35.104	210.89.168.67	TCP	55	[TCP Keep-Alive] 63756 → 443 [ACK] Seq=1935 Ack=4711 Win=13004…
1221	47.528101	210.89.168.67	192.168.35.104	TCP	66	[TCP Keep-Alive ACK] 443 → 63756 [ACK] Seq=4711 Ack=1936 Win=3…
1222	47.628346	192.168.35.104	117.52.137.140	TCP	55	[TCP Keep-Alive] 56724 → 443 [ACK] Seq=2023 Ack=3826 Win=13132…
1223	47.640924	117.52.137.140	192.168.35.104	TCP	66	[TCP Keep-Alive ACK] 443 → 56724 [ACK] Seq=3826 Ack=2024 Win=3…
1224	47.830646	192.168.35.104	101.79.243.149	TCP	55	[TCP Keep-Alive] 50937 → 443 [ACK] Seq=1641 Ack=249584 Win=131…
1225	47.841486	101.79.243.149	192.168.35.104	TCP	66	[TCP Keep-Alive ACK] 443 → 50937 [ACK] Seq=249584 Ack=1642 Win…
1226	48.049102	192.168.35.104	210.205.5.154	TCP	55	[TCP Keep-Alive] 57878 → 443 [ACK] Seq=5811 Ack=202160 Win=131…
1227	48.058115	210.205.5.154	192.168.35.104	TCP	66	[TCP Keep-Alive ACK] 443 → 57878 [ACK] Seq=202160 Ack=5812 Win…
1228	48.064748	192.168.35.104	125.209.254.183	TCP	55	[TCP Keep-Alive] 52854 → 443 [ACK] Seq=303 Ack=294 Win=1025 Le…
1229	48.075314	125.209.254.183	192.168.35.104	TCP	66	[TCP Keep-Alive ACK] 443 → 52854 [ACK] Seq=294 Ack=304 Win=262…
1230	48.137345	192.168.35.104	210.220.163.82	DNS	91	Standard query 0x9c65 A settings-win.data.microsoft.com

Answer : This picture shows that when enter the site “gaia.cs.umass.edu”, wiresharks’s unfiltered packet-listing window shows these protocols like **TCP, TLSv1, SSDP, MDNS, 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.)


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time       Source           Destination      Protocol  Length Info
 4804 46.463067  192.168.35.104   211.115.106.205  HTTP       427 GET /jk?c=62&p=yi15EzmDPLVWkP8LLAsL40sXFi7+VGGJjlCuxJ0EDjo
 4806 46.473108  211.115.106.205  192.168.35.104   HTTP       405 HTTP/1.1 200 OK
 4808 46.493376  192.168.35.104   211.115.106.205  HTTP       427 GET /jk?c=62&p=yi15EzmDPLVWkP8LLAsL40sXFi7+VGGJjlCuxJ0EDjo
 4813 46.503444  211.115.106.205  192.168.35.104   HTTP       405 HTTP/1.1 200 OK
 4864 46.558502  192.168.35.104   211.115.106.205  HTTP       427 GET /jk?c=62&p=yi15EzmDPLVWkP8LLAsL40sXFi7+VGGJjlCuxJ0EDjo
 4873 46.568867  211.115.106.205  192.168.35.104   HTTP       405 HTTP/1.1 200 OK
 6982 51.498513  192.168.35.104   128.119.245.12   HTTP       544 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 7204 51.684579  192.168.35.104   211.115.106.205  HTTP       451 GET /jk?c=62&p=yi15EzmDPLVWkP8LLAsL40sXFi7+VGGJjlCuxJ0EDjo
 7213 51.694893  211.115.106.205  192.168.35.104   HTTP       405 HTTP/1.1 200 OK
 7221 51.697024  128.119.245.12   192.168.35.104   HTTP       492 HTTP/1.1 200 OK  (text/html)
 7388 51.870157  192.168.35.104   128.119.245.12   HTTP       490 GET /favicon.ico HTTP/1.1
 7491 52.067148  128.119.245.12   192.168.35.104   HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

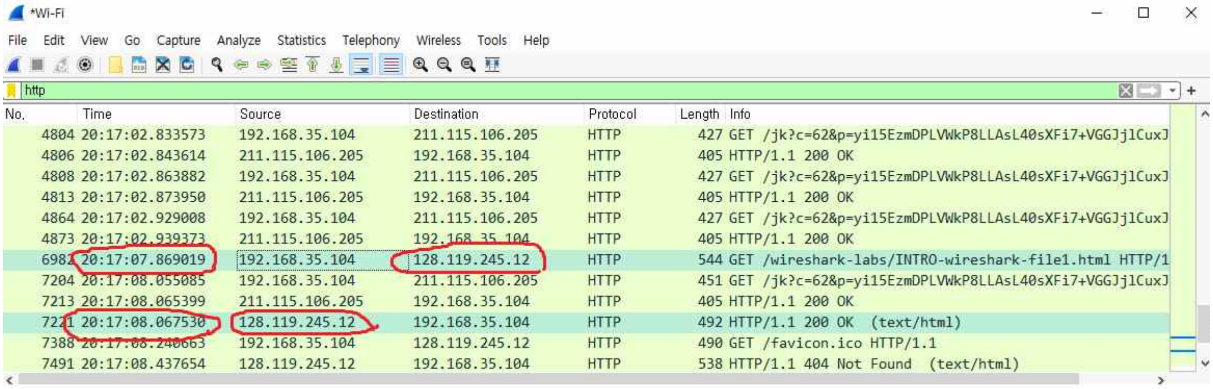
(second version)

Answer : This picture shows that 192.168.35.104(PC) <-> 128.119.245.12([http://gaia.cs.umass.edu/)](http://gaia.cs.umass.edu/) communicates each other

Get Time : 51.498513(s)

OK Time : 51.697024(s)

The time gap is 0.198511(s)


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time             Source           Destination      Protocol  Length Info
 4804 20:17:02.833573  192.168.35.104   211.115.106.205  HTTP       427 GET /jk?c=62&p=yi15EzmDPLVWkP8LLAsL40sXFi7+VGGJjlCuxJ
 4806 20:17:02.843614  211.115.106.205  192.168.35.104   HTTP       405 HTTP/1.1 200 OK
 4808 20:17:02.863882  192.168.35.104   211.115.106.205  HTTP       427 GET /jk?c=62&p=yi15EzmDPLVWkP8LLAsL40sXFi7+VGGJjlCuxJ
 4813 20:17:02.873950  211.115.106.205  192.168.35.104   HTTP       405 HTTP/1.1 200 OK
 4864 20:17:02.929008  192.168.35.104   211.115.106.205  HTTP       427 GET /jk?c=62&p=yi15EzmDPLVWkP8LLAsL40sXFi7+VGGJjlCuxJ
 4873 20:17:02.939373  211.115.106.205  192.168.35.104   HTTP       405 HTTP/1.1 200 OK
 6982 20:17:07.869019  192.168.35.104   128.119.245.12   HTTP       544 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1
 7204 20:17:08.055085  192.168.35.104   211.115.106.205  HTTP       451 GET /jk?c=62&p=yi15EzmDPLVWkP8LLAsL40sXFi7+VGGJjlCuxJ
 7213 20:17:08.065399  211.115.106.205  192.168.35.104   HTTP       405 HTTP/1.1 200 OK
 7221 20:17:08.067530  128.119.245.12   192.168.35.104   HTTP       492 HTTP/1.1 200 OK  (text/html)
 7388 20:17:08.240663  192.168.35.104   128.119.245.12   HTTP       490 GET /favicon.ico HTTP/1.1
 7491 20:17:08.437654  128.119.245.12   192.168.35.104   HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

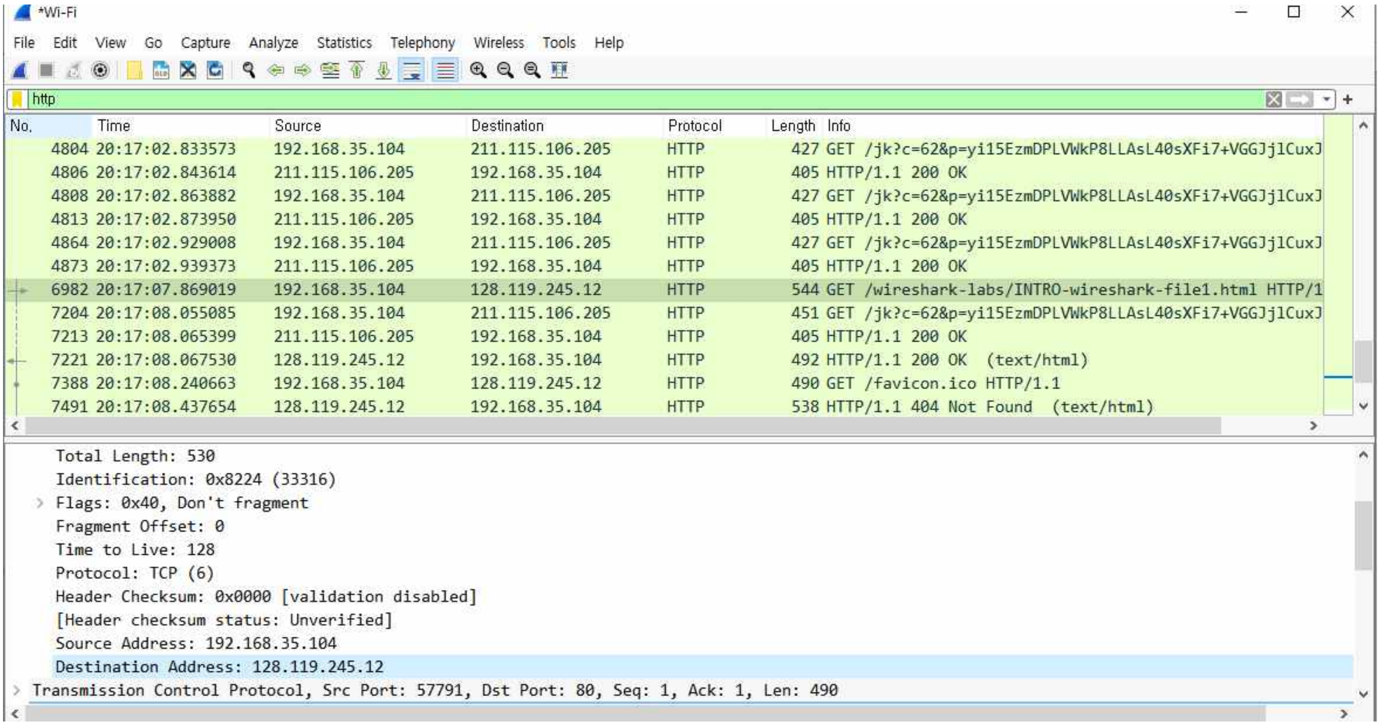
(Time-of-day version)

Get time: 20:17:07.869019

OK time: 20:17:08.067530

The time gap is 0.198511(s)

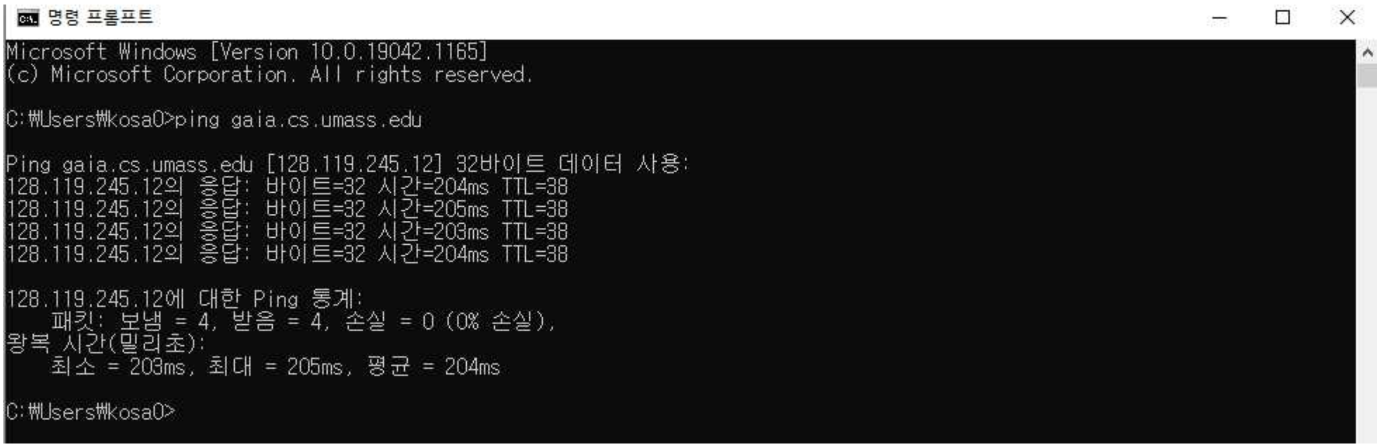
3. What is the Internet address of the gaia.cs.umass.edu (also known as www.net.cs.umass.edu)? What is the Internet address of your computer?



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.   Time             Source           Destination      Protocol  Length Info
 4804 20:17:02.833573  192.168.35.104   211.115.106.205  HTTP      427 GET /jk?c=62&p=yi15EzmDPLVWkP8LLAsL40sXFi7+VGGJjlCuxJ
 4806 20:17:02.843614  211.115.106.205  192.168.35.104   HTTP      405 HTTP/1.1 200 OK
 4808 20:17:02.863882  192.168.35.104   211.115.106.205  HTTP      427 GET /jk?c=62&p=yi15EzmDPLVWkP8LLAsL40sXFi7+VGGJjlCuxJ
 4813 20:17:02.873950  211.115.106.205  192.168.35.104   HTTP      405 HTTP/1.1 200 OK
 4864 20:17:02.929008  192.168.35.104   211.115.106.205  HTTP      427 GET /jk?c=62&p=yi15EzmDPLVWkP8LLAsL40sXFi7+VGGJjlCuxJ
 4873 20:17:02.939373  211.115.106.205  192.168.35.104   HTTP      405 HTTP/1.1 200 OK
 6982 20:17:07.869019  192.168.35.104   128.119.245.12   HTTP      544 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1
 7204 20:17:08.055085  192.168.35.104   211.115.106.205  HTTP      451 GET /jk?c=62&p=yi15EzmDPLVWkP8LLAsL40sXFi7+VGGJjlCuxJ
 7213 20:17:08.065399  211.115.106.205  192.168.35.104   HTTP      405 HTTP/1.1 200 OK
 7221 20:17:08.067530  128.119.245.12   192.168.35.104   HTTP      492 HTTP/1.1 200 OK  (text/html)
 7388 20:17:08.240663  192.168.35.104   128.119.245.12   HTTP      490 GET /favicon.ico HTTP/1.1
 7491 20:17:08.437654  128.119.245.12   192.168.35.104   HTTP      538 HTTP/1.1 404 Not Found  (text/html)

    Total Length: 530
    Identification: 0x8224 (33316)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.35.104
    Destination Address: 128.119.245.12
> Transmission Control Protocol, Src Port: 57791, Dst Port: 80, Seq: 1, Ack: 1, Len: 490
```



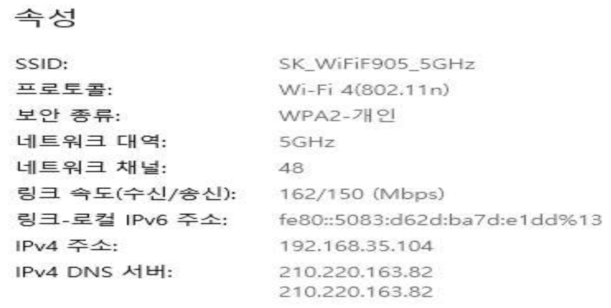
```
Microsoft Windows [Version 10.0.19042.1165]
(c) Microsoft Corporation. All rights reserved.

C:₩Users₩kosa0>ping gaia.cs.umass.edu

Ping gaia.cs.umass.edu [128.119.245.12] 32바이트 데이터 사용:
128.119.245.12의 응답: 바이트=32 시간=204ms TTL=38
128.119.245.12의 응답: 바이트=32 시간=205ms TTL=38
128.119.245.12의 응답: 바이트=32 시간=203ms TTL=38
128.119.245.12의 응답: 바이트=32 시간=204ms TTL=38

128.119.245.12에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 203ms, 최대 = 205ms, 평균 = 204ms

C:₩Users₩kosa0>
```



속성

SSID:	SK_WiFiF905_5GHz
프로토콜:	Wi-Fi 4(802.11n)
보안 종류:	WPA2-개인
네트워크 대역:	5GHz
네트워크 채널:	48
링크 속도(수신/송신):	162/150 (Mbps)
링크-로컬 IPv6 주소:	fe80::5083:d62d:ba7d:e1dd%13
IPv4 주소:	192.168.35.104
IPv4 DNS 서버:	210.220.163.82 210.220.163.82

Answer : The first picture shows that In wiresharks Http message, HTTP Get messages tell that the **Destination address (gaia.cs.umass.edu) is 128.119.245.12**

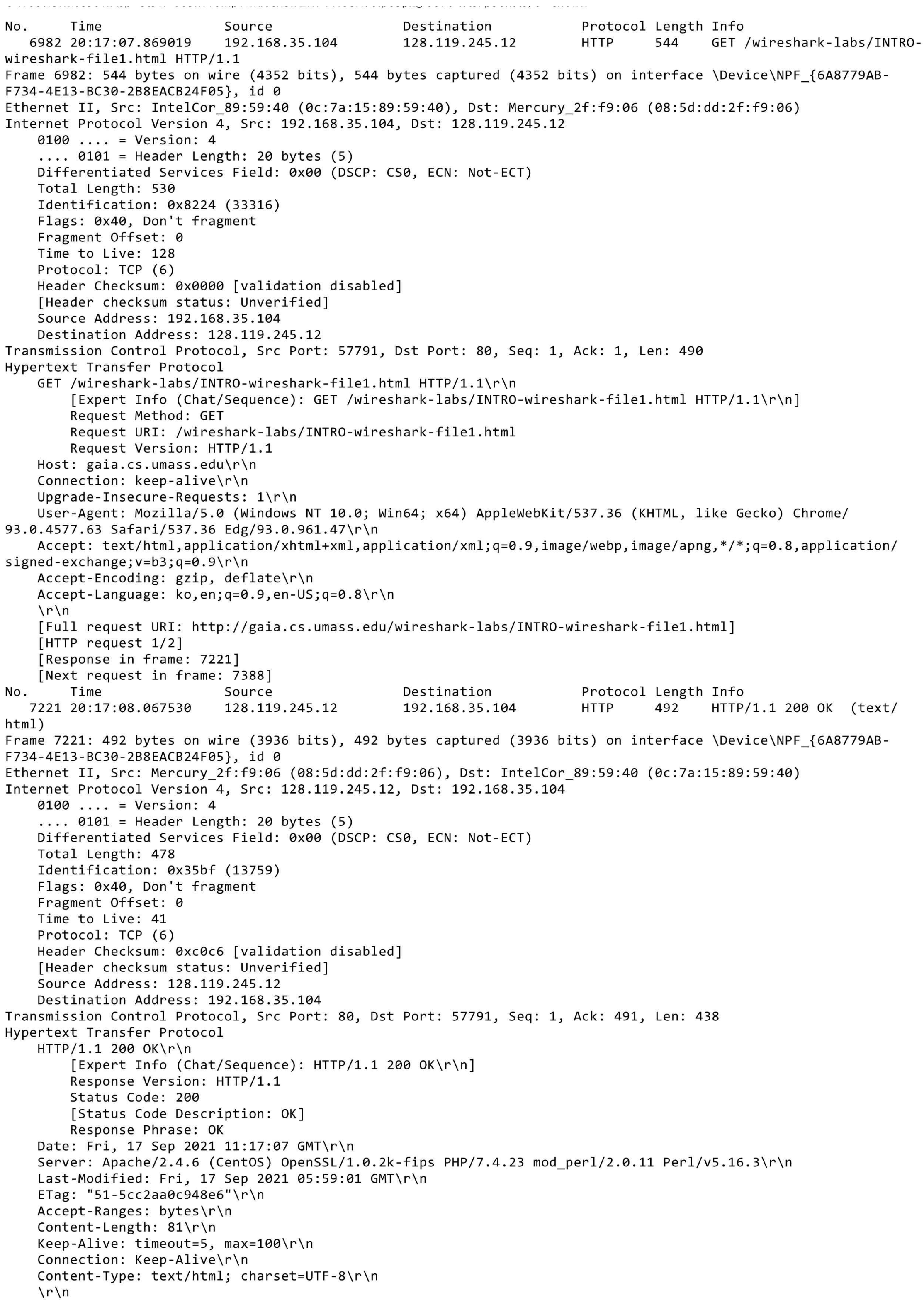
Source Address(my computer) is 192.168.35.104

The second picture is to check the internet address of gaia.cs.umass.edu using ping command

The third picture is to check the ip address of my computer

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.

Answer : HTTP GET and OK message (GET NO. 6982 / OK NO. 7221)



```
No.     Time             Source                Destination           Protocol Length Info
   6982 20:17:07.869019    192.168.35.104        128.119.245.12        HTTP     544    GET /wireshark-labs/INTRO-
wireshark-file1.html HTTP/1.1
Frame 6982: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface \Device\NPF_{6A8779AB-
F734-4E13-BC30-2B8EACB24F05}, id 0
Ethernet II, Src: IntelCor_89:59:40 (0c:7a:15:89:59:40), Dst: Mercury_2f:f9:06 (08:5d:dd:2f:f9:06)
Internet Protocol Version 4, Src: 192.168.35.104, 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: 530
    Identification: 0x8224 (33316)
    Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.35.104
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 57791, Dst Port: 80, Seq: 1, Ack: 1, Len: 490
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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
93.0.4577.63 Safari/537.36 Edg/93.0.961.47\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ko,en;q=0.9,en-US;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 7221]
    [Next request in frame: 7388]
No.     Time             Source                Destination           Protocol Length Info
   7221 20:17:08.067530    128.119.245.12        192.168.35.104        HTTP     492    HTTP/1.1 200 OK  (text/
html)
Frame 7221: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{6A8779AB-
F734-4E13-BC30-2B8EACB24F05}, id 0
Ethernet II, Src: Mercury_2f:f9:06 (08:5d:dd:2f:f9:06), Dst: IntelCor_89:59:40 (0c:7a:15:89:59:40)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.35.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 478
    Identification: 0x35bf (13759)
    Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 41
    Protocol: TCP (6)
    Header Checksum: 0xc0c6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 192.168.35.104
Transmission Control Protocol, Src Port: 80, Dst Port: 57791, Seq: 1, Ack: 491, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Fri, 17 Sep 2021 11:17:07 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.23 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Fri, 17 Sep 2021 05:59:01 GMT\r\n
    ETag: "51-5cc2aa0c948e6"\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 1/2]
    [Time since request: 0.198511000 seconds]
    [Request in frame: 6982]
    [Next request in frame: 7388]
    [Next response in frame: 7491]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```