네트워크실험 1주차
Experiments on Communication Networks

Contents

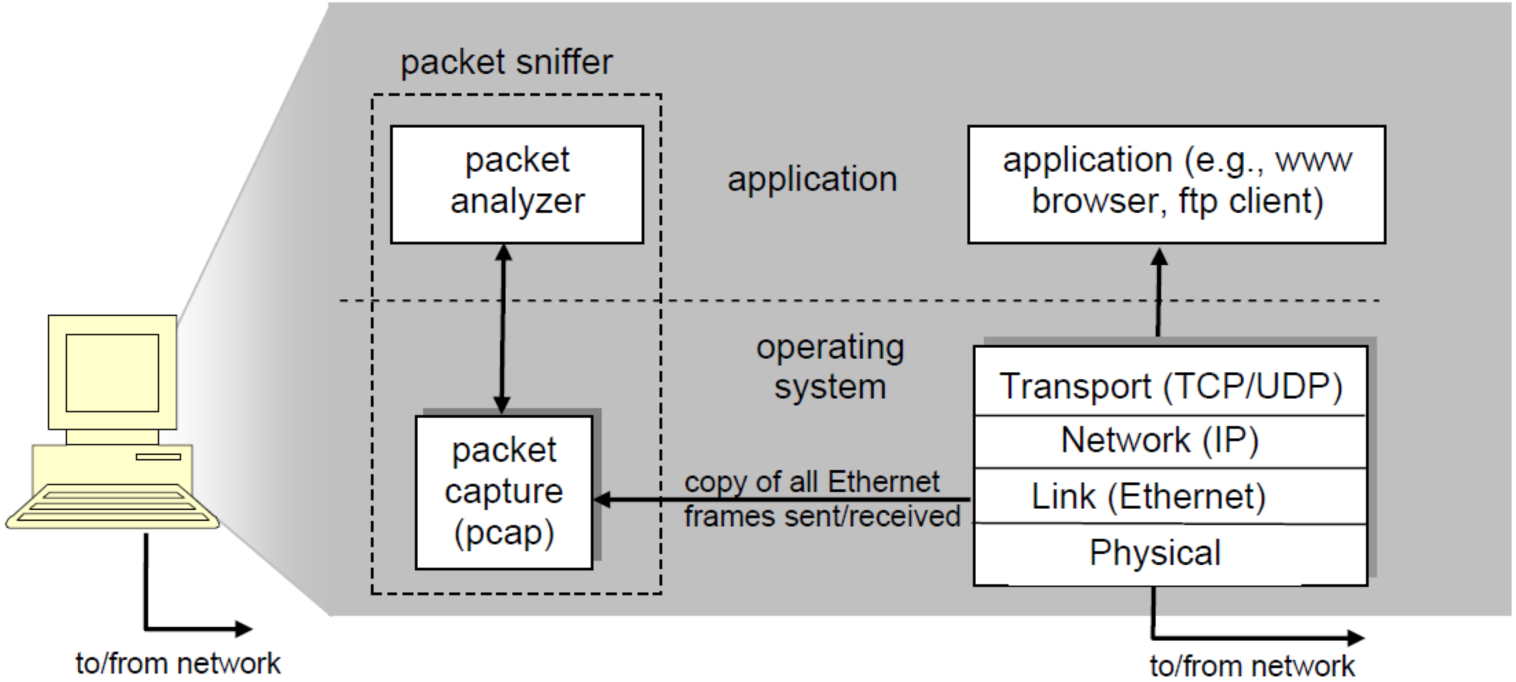
- **실험 1: Getting Started**
  - Getting Wireshark
  - Running Wireshark
  - Taking Wireshark for a Test Run

- **실험 2: HTTP**
  - The Basic HTTP GET/response interaction
  - The HTTP CONDITIONAL GET/response interaction
  - Retrieving Long Documents

- **실험 3: DNS**
  - nslookup
  - ipconfig
  - Tracing DNS with Wireshark

실험 1: Getting Started

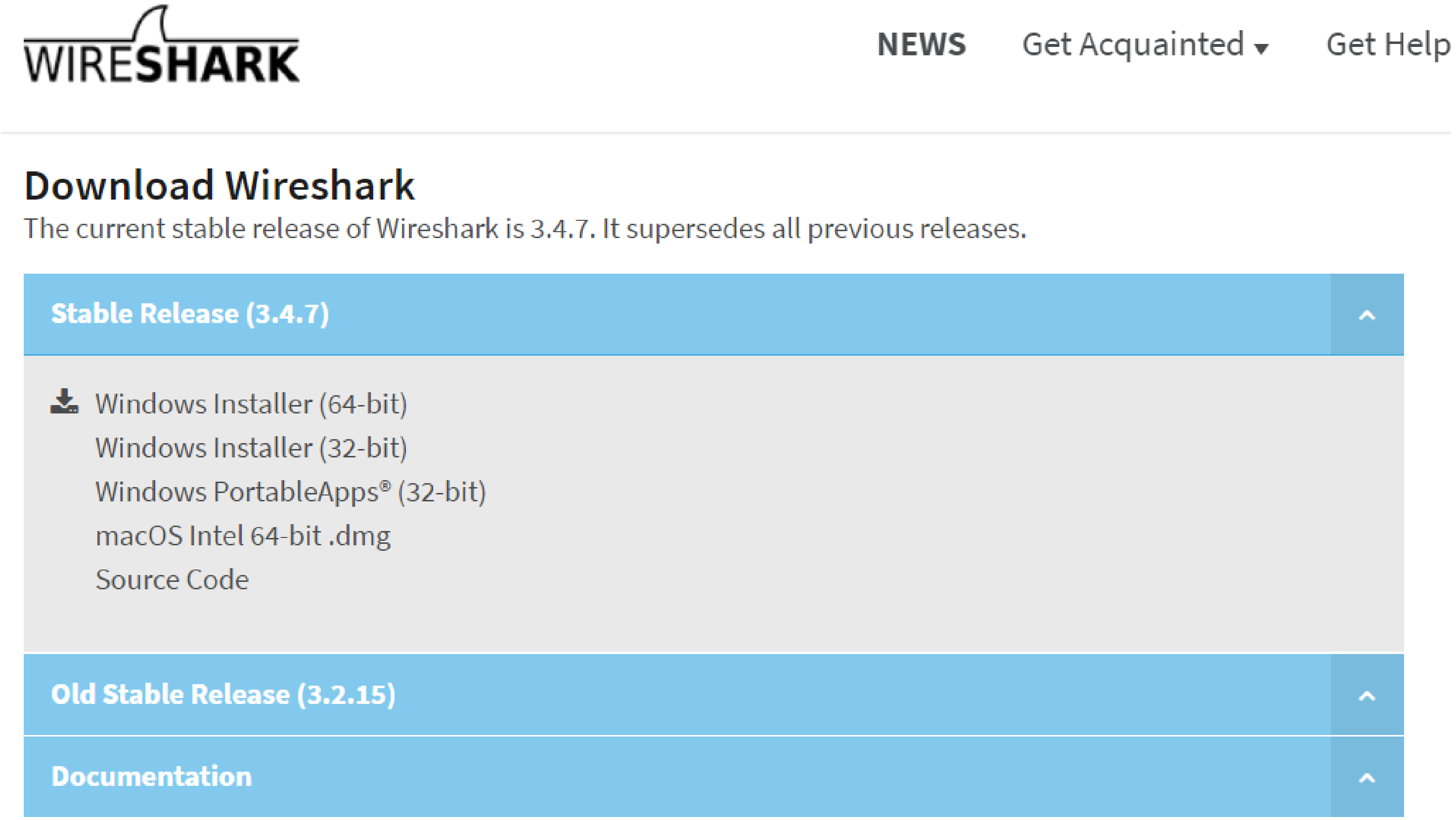
- **Wireshark**
  - a **packet sniffer** : the basic tool for observing the messages exchanged between executing protocol entities
    - to capture ("sniff") messages being sent/received from/by your computer
    - to store and/or display the contents of the various protocol fields in these captured messages
    - to receive a copy of packets that are sent/received from/by application and protocols executing on your machine



실험 1: Getting Started

Getting Wireshark

- Download and install the Wireshark software:
  - Go to http://www.wireshark.org/download.html and download and install the Wireshark binary for your computer.



Download Wireshark

The current stable release of Wireshark is 3.4.7. It supersedes all previous releases.

Stable Release (3.4.7)

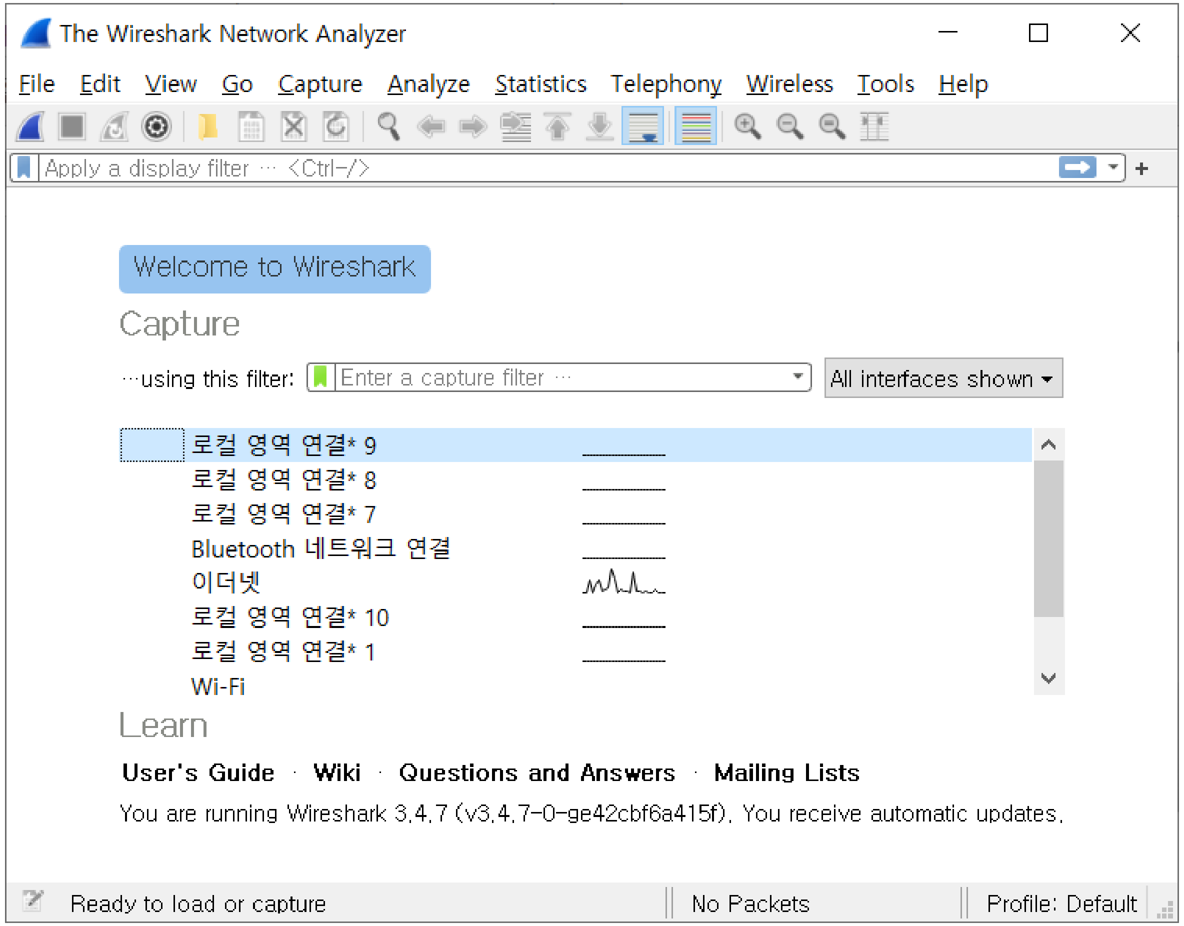
- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- macOS Intel 64-bit .dmg
- Source Code

Old Stable Release (3.2.15)

Documentation

실험 1: Getting Started

- **Running Wireshark**
  - Run the Wireshark program.



You are running Wireshark 3.4.7 (v3.4.7-0-ge42cbf6a415f). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

실험 1: Getting Started

- **Running Wireshark**
  - Click on one of these interfaces to start packet capture.

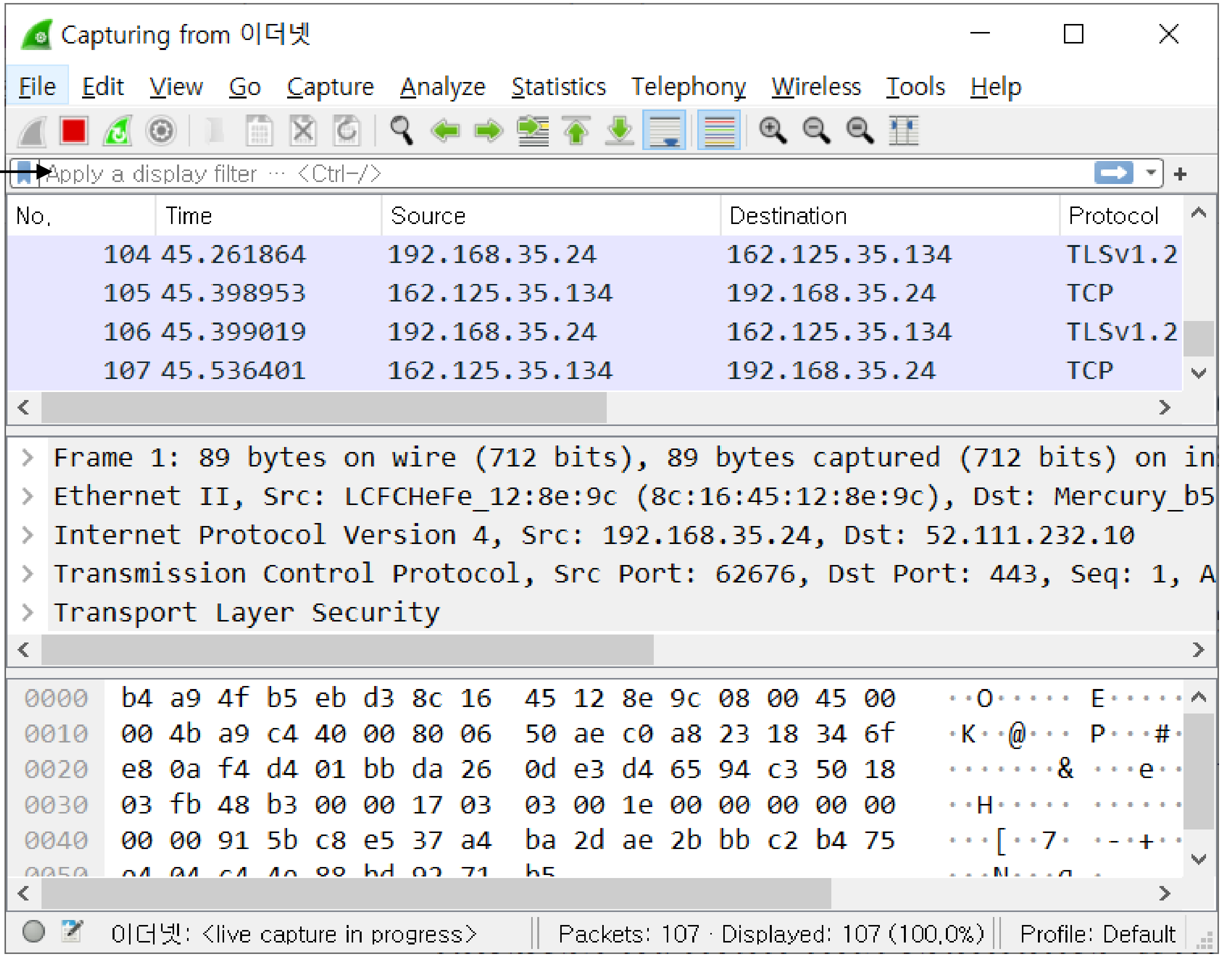
command menus

display filter specification

listing of captured packets

details of selected packet header

packet content in hexadecimal and ASCII



```
No.       Time       Source           Destination      Protocol
      104 45.261864  192.168.35.24    162.125.35.134   TLSv1.2
      105 45.398953  162.125.35.134   192.168.35.24    TCP
      106 45.399019  192.168.35.24    162.125.35.134   TLSv1.2
      107 45.536401  162.125.35.134   192.168.35.24    TCP
```

```
> Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on in
> Ethernet II, Src: LCFCHeFe_12:8e:9c (8c:16:45:12:8e:9c), Dst: Mercury_b5
> Internet Protocol Version 4, Src: 192.168.35.24, Dst: 52.111.232.10
> Transmission Control Protocol, Src Port: 62676, Dst Port: 443, Seq: 1, A
> Transport Layer Security
```

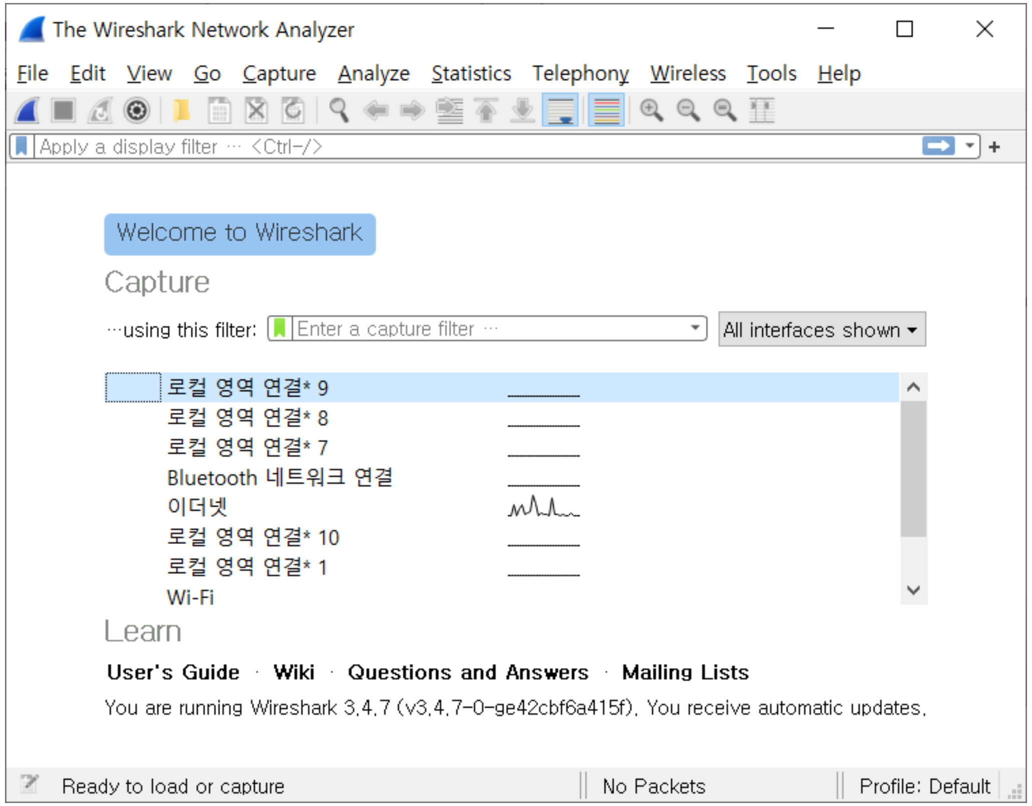
```
0000  b4 a9 4f b5 eb d3 8c 16  45 12 8e 9c 08 00 45 00   ··O·····  E·····
0010  00 4b a9 c4 40 00 80 06  50 ae c0 a8 23 18 34 6f   ·K··@···  P···#·
0020  e8 0a f4 d4 01 bb da 26  0d e3 d4 65 94 c3 50 18   ·······&  ···e·
0030  03 fb 48 b3 00 00 17 03  03 00 1e 00 00 00 00 00   ··H·····  ······
0040  00 00 91 5b c8 e5 37 a4  ba 2d ae 2b bb c2 b4 75   ···[··7·  ·-·+··
```

이더넷: <live capture in progress> | Packets: 107 · Displayed: 107 (100.0%) | Profile: Default

실험 1: Getting Started

Taking Wireshark for a Test Run

- Start up your favorite web browser, which will display your selected homepage.
- Start up the Wireshark software. You will initially see a window similar to that shown in the figure below. Wireshark has not yet begun capturing packets.



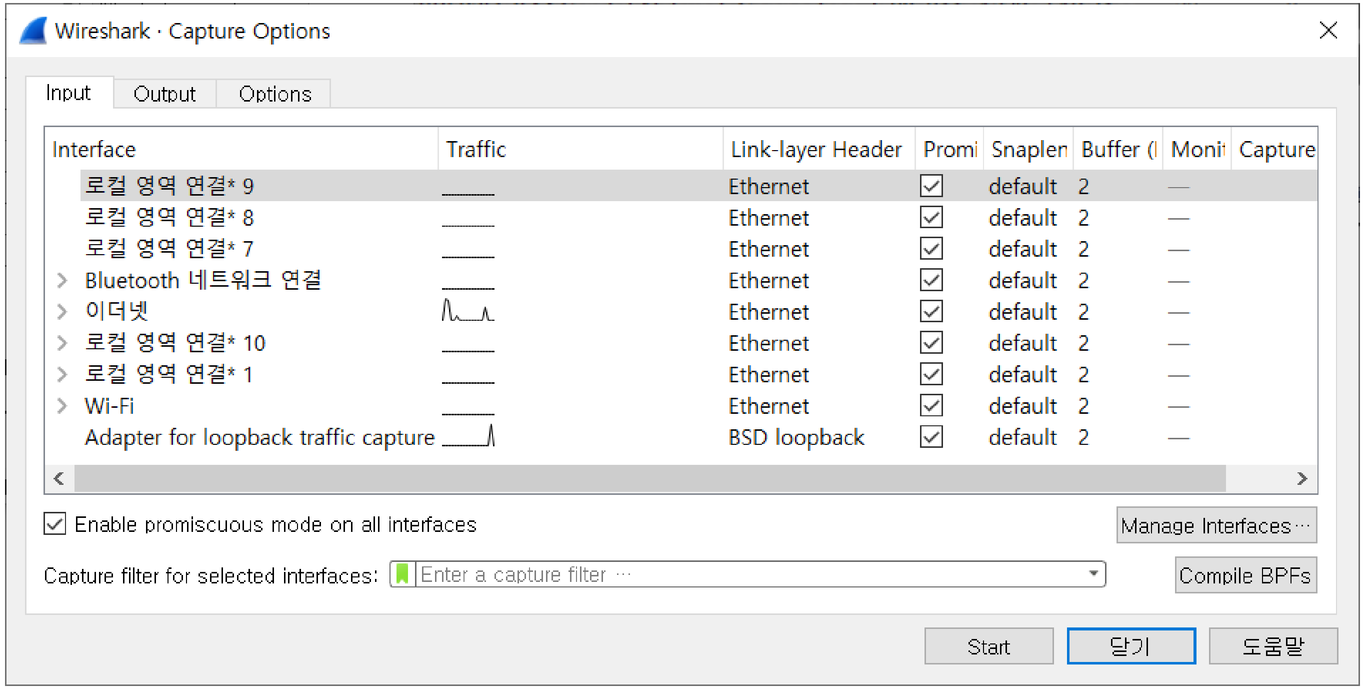
You are running Wireshark 3.4.7 (v3.4.7-0-ge42cbf6a415f). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

실험 1: Getting Started

Taking Wireshark for a Test Run

- To begin packet capture, select the Capture pull down menu and select *Interfaces*. This will cause the “Wireshark: Capture Interfaces” window to be displayed, as shown in the figure below.



Wireshark · Capture Options

Interface	Traffic	Link-layer Header	Promi	Snaplen	Buffer (I	Moni	Capture
로컬 영역 연결* 9		Ethernet	☑	default	2	—	
로컬 영역 연결* 8		Ethernet	☑	default	2	—	
로컬 영역 연결* 7		Ethernet	☑	default	2	—	
› Bluetooth 네트워크 연결		Ethernet	☑	default	2	—	
› 이더넷		Ethernet	☑	default	2	—	
› 로컬 영역 연결* 10		Ethernet	☑	default	2	—	
› 로컬 영역 연결* 1		Ethernet	☑	default	2	—	
› Wi-Fi		Ethernet	☑	default	2	—	
Adapter for loopback traffic capture		BSD loopback	☑	default	2	—	

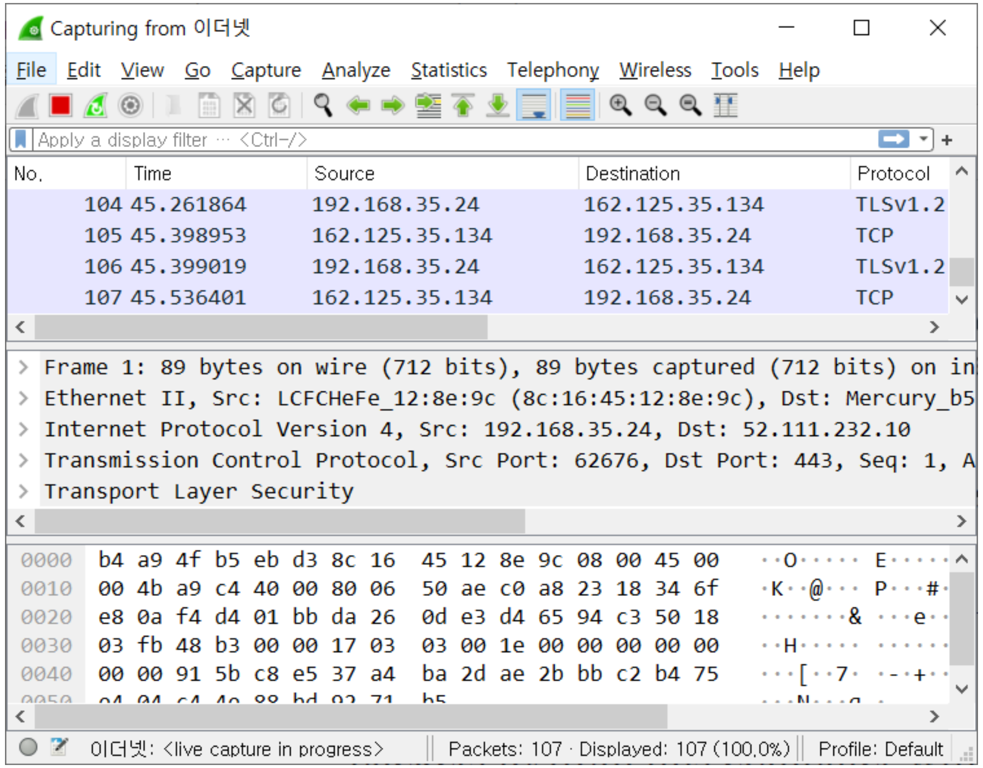
☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

- You’ll see a list of the interfaces on your computer as well as a count of the packets that have been observed on that interface so far. Click on *Start* for the interface on which you want to begin packet capture. Packet capture will now begin - Wireshark is now capturing all packets being sent/received from/by your computer!

실험 1: Getting Started

- **Taking Wireshark for a Test Run**
  - Once you begin packet capture, a window similar to that shown in the figure below will appear. This window shows the packets being captured. By selecting *Capture* pulldown menu and selecting *Stop*, you can stop packet capture. But don't stop packet capture yet. Let's capture some interesting packets first. To do so, we'll need to generate some network traffic. Let's do so using a web browser, which will use the HTTP protocol that we will study in detail in class to download content from a website.



Capturing from 이더넷
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.        Time           Source            Destination       Protocol
       104 45.261864      192.168.35.24     162.125.35.134    TLSv1.2
       105 45.398953      162.125.35.134    192.168.35.24     TCP
       106 45.399019      192.168.35.24     162.125.35.134    TLSv1.2
       107 45.536401      162.125.35.134    192.168.35.24     TCP
```

```
> Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on in
> Ethernet II, Src: LCFCHeFe_12:8e:9c (8c:16:45:12:8e:9c), Dst: Mercury_b5
> Internet Protocol Version 4, Src: 192.168.35.24, Dst: 52.111.232.10
> Transmission Control Protocol, Src Port: 62676, Dst Port: 443, Seq: 1, A
> Transport Layer Security
```

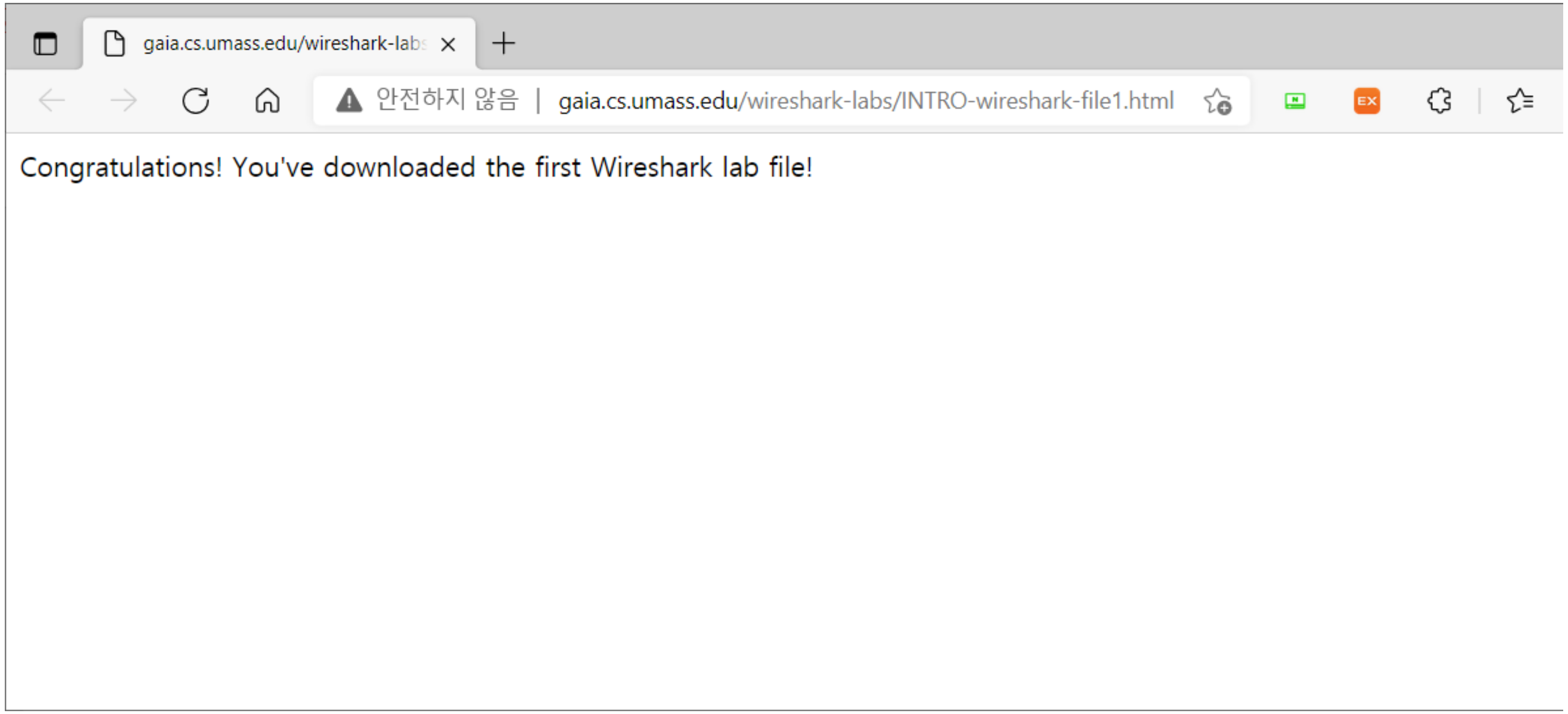
```
0000  b4 a9 4f b5 eb d3 8c 16  45 12 8e 9c 08 00 45 00   ··O·····  E·····
0010  00 4b a9 c4 40 00 80 06  50 ae c0 a8 23 18 34 6f   ·K··@···  P···#·
0020  e8 0a f4 d4 01 bb da 26  0d e3 d4 65 94 c3 50 18   ·······&  ···e··
0030  03 fb 48 b3 00 00 17 03  03 00 1e 00 00 00 00 00   ··H·····  ······
0040  00 00 91 5b c8 e5 37 a4  ba 2d ae 2b bb c2 b4 75   ···[··7·  ·-·+··
```

```
이더넷: <live capture in progress> || Packets: 107 · Displayed: 107 (100.0%) || Profile: Default
```

실험 1: Getting Started

■ Taking Wireshark for a Test Run

- While Wireshark is running, enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html and have that page displayed in your browser. In order to display this page, your browser will contact the HTTP server at gaia.cs.umass.edu and exchange HTTP messages with the server in order to download this page. The Ethernet frames containing these HTTP messages (as well as all other frames passing through your Ethernet adapter) will be captured by Wireshark.



gaia.cs.umass.edu/wireshark-labs
안전하지 않음 | gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

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

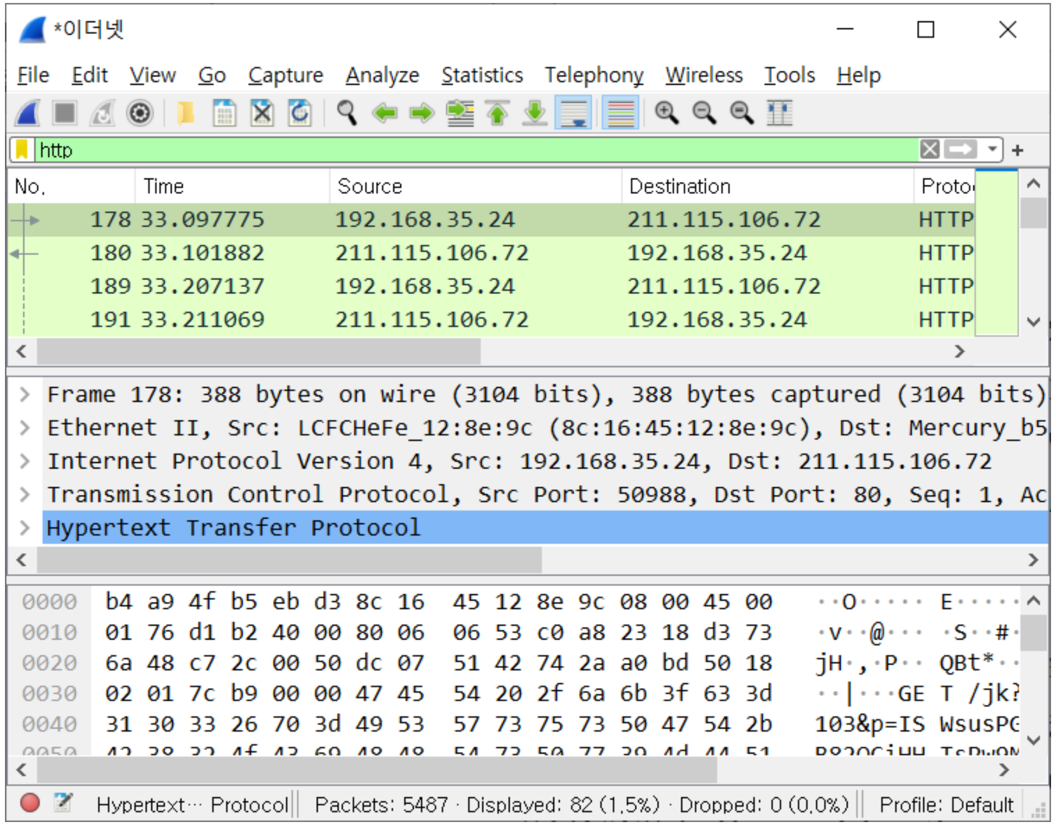
실험 1: Getting Started

- **Taking Wireshark for a Test Run**
  - After your browser has displayed the INTRO-wireshark-file1.html page (it is a simple one line of congratulations), stop Wireshark packet capture by selecting stop in the Wireshark capture window. The main Wireshark window should now look similar to the previous figure. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the gaia.cs.umass.edu web server should appear somewhere in the listing of packets captured. But there will be many other types of packets displayed as well (see, e.g., the many different protocol types shown in the *Protocol* column in the previous figure). Even though the only action you took was to download a web page, there were evidently many other protocols running on your computer that are unseen by the user. We'll learn much more about these protocols as we progress through the text! For now, you should just be aware that there is often much more going on than "meet's the eye"!

실험 1: Getting Started

■ Taking Wireshark for a Test Run

- Type in “http” (without the quotes, and in lower case – all protocol names are in lower case in Wireshark) into the display filter specification window at the top of the main Wireshark window. Then select *Apply* (to the right of where you entered “http”). This will cause only HTTP message to be displayed in the packet-listing window.


*이더넷
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.    Time          Source           Destination      Proto
178 33.097775   192.168.35.24    211.115.106.72   HTTP
180 33.101882   211.115.106.72   192.168.35.24    HTTP
189 33.207137   192.168.35.24    211.115.106.72   HTTP
191 33.211069   211.115.106.72   192.168.35.24    HTTP
```

```
> Frame 178: 388 bytes on wire (3104 bits), 388 bytes captured (3104 bits)
> Ethernet II, Src: LCFCHeFe_12:8e:9c (8c:16:45:12:8e:9c), Dst: Mercury_b5
> Internet Protocol Version 4, Src: 192.168.35.24, Dst: 211.115.106.72
> Transmission Control Protocol, Src Port: 50988, Dst Port: 80, Seq: 1, Ac
> Hypertext Transfer Protocol
```

```
0000  b4 a9 4f b5 eb d3 8c 16  45 12 8e 9c 08 00 45 00   ··O····· E·····
0010  01 76 d1 b2 40 00 80 06  06 53 c0 a8 23 18 d3 73   ·v··@··· ·S··#·
0020  6a 48 c7 2c 00 50 dc 07  51 42 74 2a a0 bd 50 18   jH·,·P·· QBt*··
0030  02 01 7c b9 00 00 47 45  54 20 2f 6a 6b 3f 63 3d   ··|···GE T /jk?
0040  31 30 33 26 70 3d 49 53  57 73 75 73 50 47 54 2b   103&p=IS WsusPG
0050  42 38 32 4f 43 69 48 48  54 73 50 77 39 4d 44 51   B82OCiHH TsPwQM
```

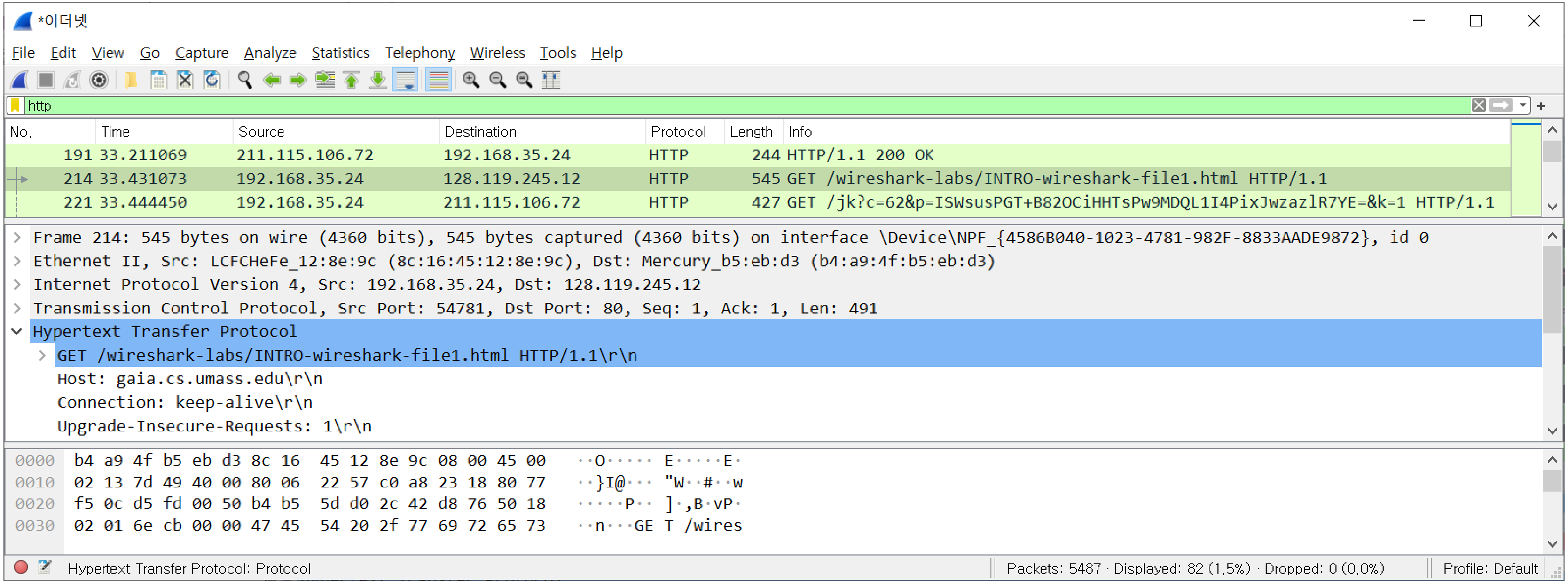
Hypertext··· Protocol | Packets: 5487 · Displayed: 82 (1.5%) · Dropped: 0 (0.0%) | Profile: Default

실험 1: Getting Started

- **Taking Wireshark for a Test Run**
  - Find the HTTP GET message that was sent from your computer to the gaia.cs.umass.edu HTTP server. (Look for an HTTP GET message in the "listing of captured packets" portion of the Wireshark window that shows "GET" followed by the gaia.cs.umass.edu URL that you entered. When you select the HTTP GET message, the Ethernet frame, IP datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window. By clicking on '+' and '-' right-pointing and down-pointing arrowheads to the left side of the packet details window, *minimize* the amount of Frame, Ethernet, Internet Protocol, and Transmission Control Protocol information displayed. *Maximize* the amount information displayed about the HTTP protocol. Your Wireshark display should now look roughly as shown in the previous figure. (Note, in particular, the minimized amount of protocol information for all protocols except HTTP, and the maximized amount of protocol information for HTTP in the packet-header window).
    - Recall that the HTTP GET message that is sent to the gaia.cs.umass.edu web server is contained within a TCP segment, which is contained (encapsulated) in an IP datagram, which is encapsulated in an Ethernet frame.

실험 1: Getting Started

■ Taking Wireshark for a Test Run


*이더넷
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.       Time        Source           Destination      Protocol  Length Info
      191 33.211069   211.115.106.72   192.168.35.24    HTTP         244 HTTP/1.1 200 OK
      214 33.431073   192.168.35.24    128.119.245.12   HTTP         545 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
      221 33.444450   192.168.35.24    211.115.106.72   HTTP         427 GET /jk?c=62&p=ISWsusPGT+B82OCiHHTsPw9MDQL1I4PixJwzazlR7YE=&k=1 HTTP/1.1
```

```
> Frame 214: 545 bytes on wire (4360 bits), 545 bytes captured (4360 bits) on interface \Device\NPF_{4586B040-1023-4781-982F-8833AADE9872}, id 0
> Ethernet II, Src: LCFCHeFe_12:8e:9c (8c:16:45:12:8e:9c), Dst: Mercury_b5:eb:d3 (b4:a9:4f:b5:eb:d3)
> Internet Protocol Version 4, Src: 192.168.35.24, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54781, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
v 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
```

```
0000  b4 a9 4f b5 eb d3 8c 16  45 12 8e 9c 08 00 45 00   ··O····· E·····E·
0010  02 13 7d 49 40 00 80 06  22 57 c0 a8 23 18 80 77   ··}I@··· "W··#··w
0020  f5 0c d5 fd 00 50 b4 b5  5d d0 2c 42 d8 76 50 18   ·····P·· ]·,B·vP·
0030  02 01 6e cb 00 00 47 45  54 20 2f 77 69 72 65 73   ··n···GE T /wires
```

```
Hypertext Transfer Protocol: Protocol    Packets: 5487 · Displayed: 82 (1.5%) · Dropped: 0 (0.0%)    Profile: Default
```

– Exit Wireshark.

실험 1: Getting Started

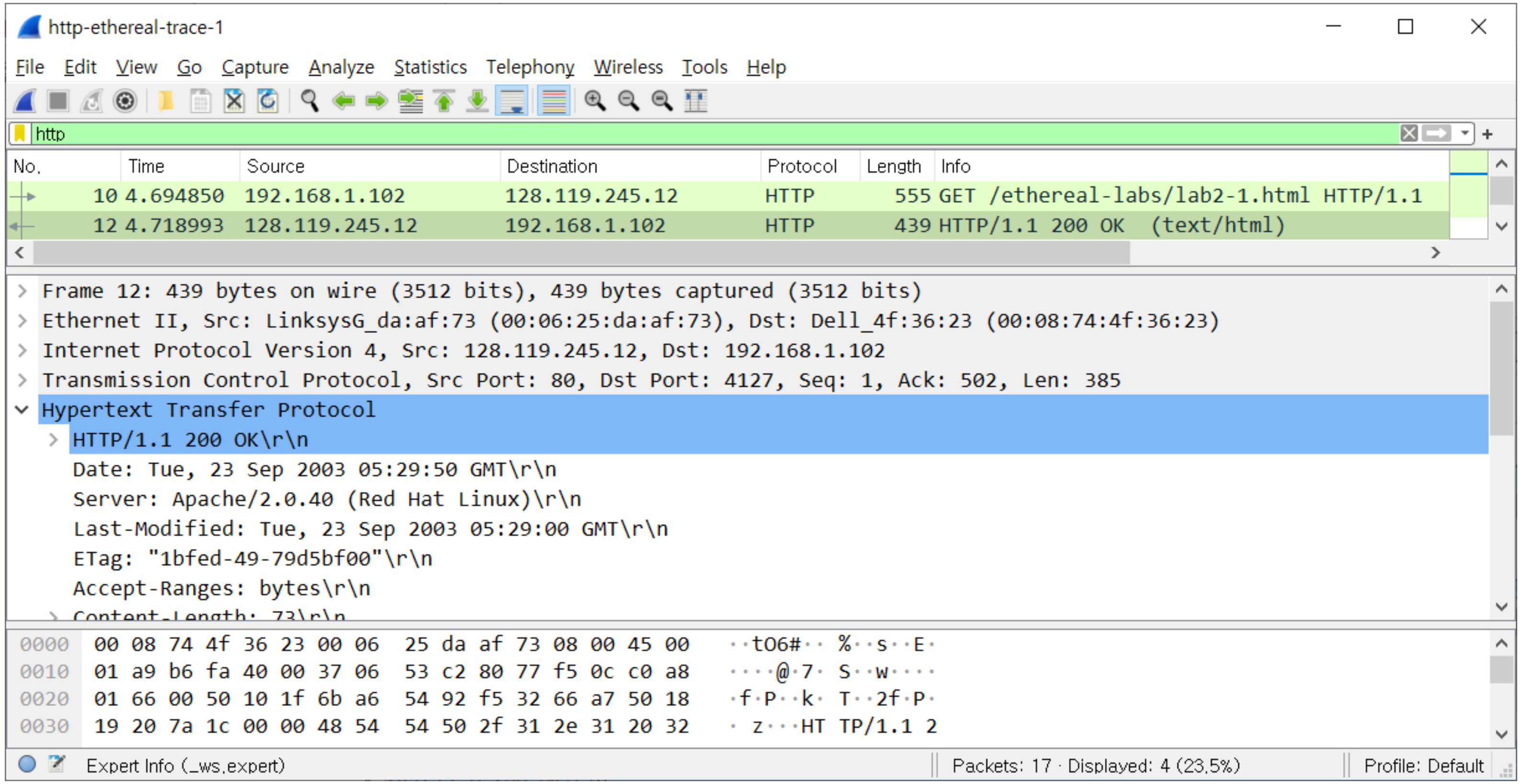
- **Taking Wireshark for a Test Run**
  - 1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
  - 2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time 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*.)
  - 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?
  - 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.

실험 2: HTTP

- **The Basic HTTP GET/response interaction**
  - Start up your web browser.
  - Start up the Wireshark packet sniffer, as described in the Introductory lab (but don’t yet begin packet capture). Enter “http” (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We’re only interested in the HTTP protocol here, and don’t want to see the clutter of all captured packets).
  - Wait a bit more than one minute (we’ll see why shortly), and then begin Wireshark packet capture.
  - Enter the following to your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html. Your browser should display the very simple, one-line HTML file.
  - Stop Wireshark packet capture.

실험 2: HTTP

■ The Basic HTTP GET/response interaction


http-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

No.	Time	Source	Destination	Protocol	Length	Info
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)

```
> Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1, Ack: 502, Len: 385
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
    ETag: "1bfed-49-79d5bf00"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 73\r\n
```

```
0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ··tO6#·· %··s··E·
0010  01 a9 b6 fa 40 00 37 06  53 c2 80 77 f5 0c c0 a8   ····@·7· S··w····
0020  01 66 00 50 10 1f 6b a6  54 92 f5 32 66 a7 50 18   ·f·P··k· T··2f·P·
0030  19 20 7a 1c 00 00 48 54  54 50 2f 31 2e 31 20 32   · z···HT TP/1.1 2
```

Expert Info (_ws.expert) | Packets: 17 · Displayed: 4 (23.5%) | Profile: Default

– If you are unable to run Wireshark on a live network connection, you can download a packet trace that was created when the steps above were followed. Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file http-ethereal-trace-1.

실험 2: HTTP

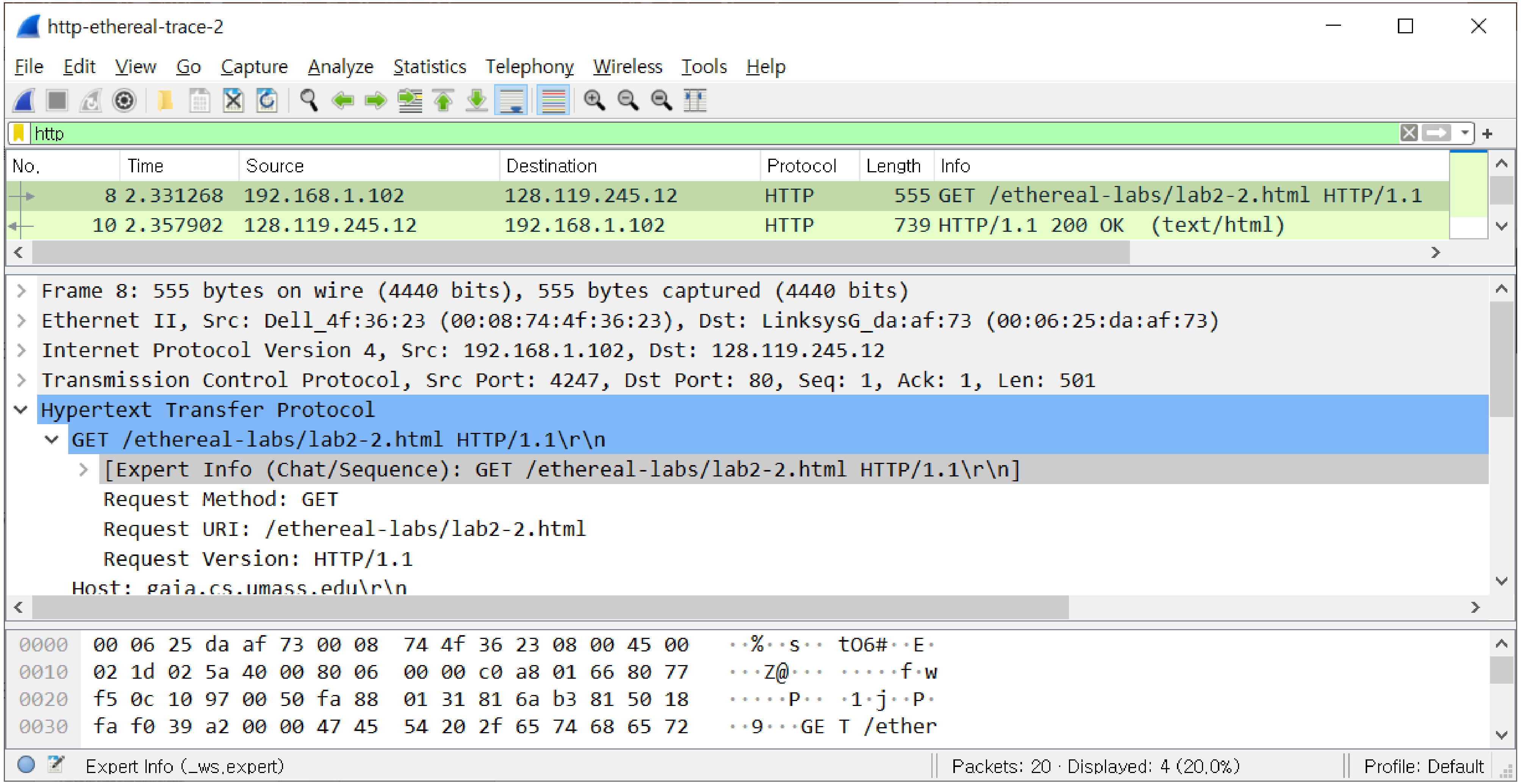
- **The Basic HTTP GET/response interaction**
  - 1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
  - 2. What languages (if any) does your browser indicate that it can accept to the server?
  - 3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
  - 4. What is the status code returned from the server to your browser?
  - 5. When was the HTML file that you are retrieving last modified at the server?
  - 6. How many bytes of content are being returned to your browser?
  - 7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

실험 2: HTTP

- **The HTTP CONDITIONAL GET/response interaction**
  - Start up your web browser, and make sure your browser’s cache is cleared.
  - Start up the Wireshark packet sniffer.
  - Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html. Your browser should display a very simple five-line HTML file.
  - Quickly enter the same URL into your browser again (or simply select the refresh button on your browser).
  - Stop Wireshark packet capture, and enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.
  - If you are unable to run Wireshark on a live network connection, you can use the http-ethereal-trace-2 packet trace to answer the questions below.

실험 2: HTTP

■ The HTTP CONDITIONAL GET/response interaction



http-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.    Time       Source          Destination     Protocol  Length Info
     8 2.331268   192.168.1.102   128.119.245.12  HTTP       555 GET /ethereal-labs/lab2-2.html HTTP/1.1
    10 2.357902   128.119.245.12  192.168.1.102   HTTP       739 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 8: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
v Hypertext Transfer Protocol
  v GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /ethereal-labs/lab2-2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
```

```
0000  00 06 25 da af 73 00 08  74 4f 36 23 08 00 45 00   ··%··s·· tO6#··E·
0010  02 1d 02 5a 40 00 80 06  00 00 c0 a8 01 66 80 77   ···Z@··· ·····f·w
0020  f5 0c 10 97 00 50 fa 88  01 31 81 6a b3 81 50 18   ·····P·· ·1·j··P·
0030  fa f0 39 a2 00 00 47 45  54 20 2f 65 74 68 65 72   ··9···GE T /ether
```

Expert Info (_ws.expert) | Packets: 20 · Displayed: 4 (20.0%) | Profile: Default

실험 2: HTTP

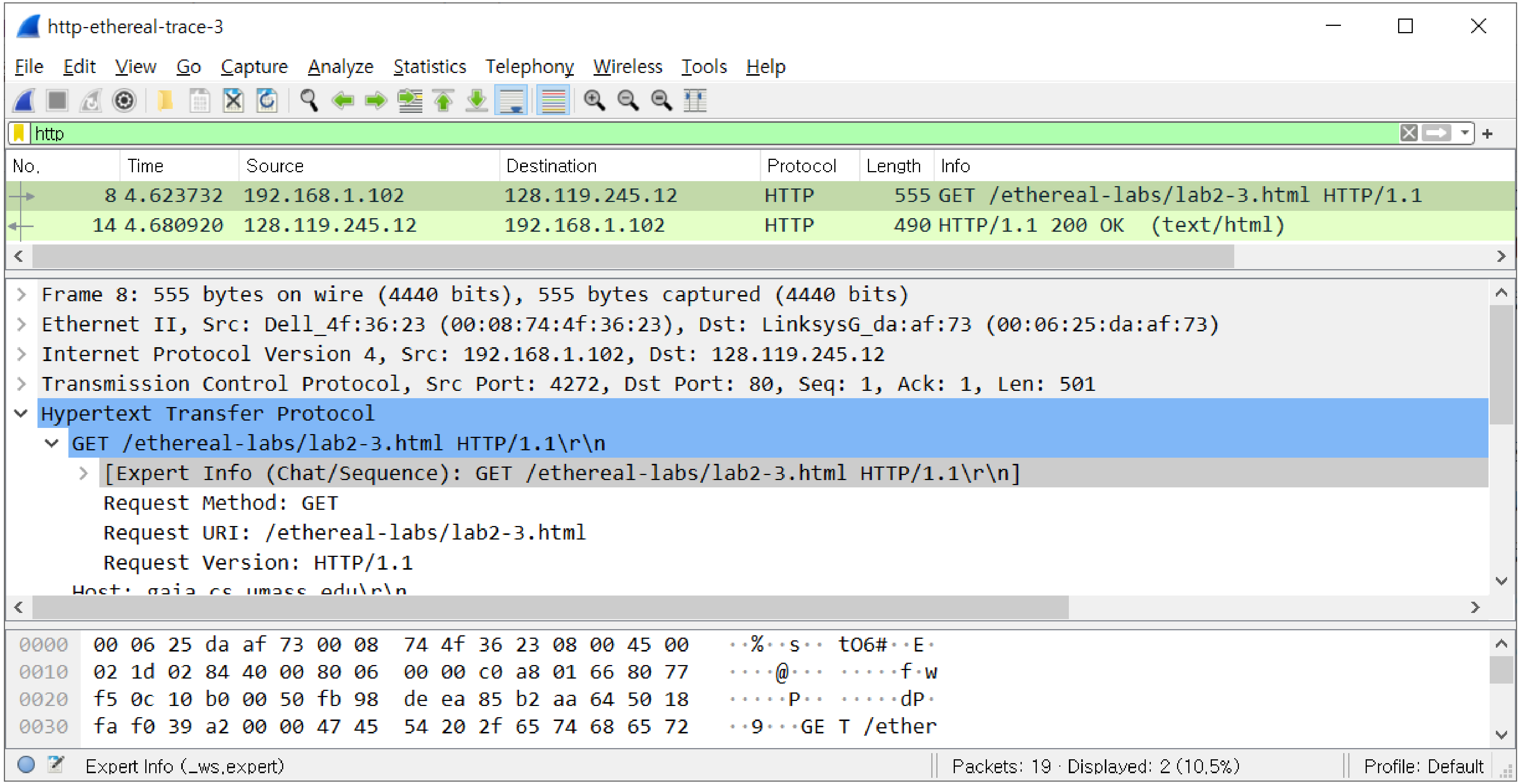
- **The HTTP CONDITIONAL GET/response interaction**
  - 8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
  - 9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
  - 10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?
  - 11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

실험 2: HTTP

- **Retrieving Long Documents**
  - Start up your web browser, and make sure your browser's cache is cleared.
  - Start up the Wireshark packet sniffer.
  - Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html. Your browser should display the rather lengthy US Bill of Rights.
  - Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.
  - If you are unable to run Wireshark on a live network connection, you can use the http-ethereal-trace-3 packet trace to answer the questions below.

실험 2: HTTP

■ Retrieving Long Documents


http-ethereal-trace-3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.   Time      Source          Destination     Protocol  Length Info
    8 4.623732  192.168.1.102   128.119.245.12  HTTP         555 GET /ethereal-labs/lab2-3.html HTTP/1.1
   14 4.680920  128.119.245.12  192.168.1.102   HTTP         490 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 8: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4272, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
v Hypertext Transfer Protocol
  v GET /ethereal-labs/lab2-3.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /ethereal-labs/lab2-3.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
```

```
0000  00 06 25 da af 73 00 08  74 4f 36 23 08 00 45 00   ··%··s·· tO6#··E·
0010  02 1d 02 84 40 00 80 06  00 00 c0 a8 01 66 80 77   ····@··· ·····f·w
0020  f5 0c 10 b0 00 50 fb 98  de ea 85 b2 aa 64 50 18   ·····P·· ·····dP·
0030  fa f0 39 a2 00 00 47 45  54 20 2f 65 74 68 65 72   ··9···GE T /ether
```

Expert Info (_ws.expert) | Packets: 19 · Displayed: 2 (10.5%) | Profile: Default

실험 2: HTTP

- **Retrieving Long Documents**
  - 12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

  - 13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

  - 14. What is the status code and phrase in the response?

  - 15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

실험 3: DNS

- **nslookup**
  - Consider the first command:

```
nslookup www.mit.edu
```

    - "Please send me the IP address for the host www.mit.edu."

  - Now consider the second command:

```
nslookup –type=NS mit.edu
```

    - "Please send me the host names of the authoritative DNS for mit.edu."

  - Now finally consider the third command:

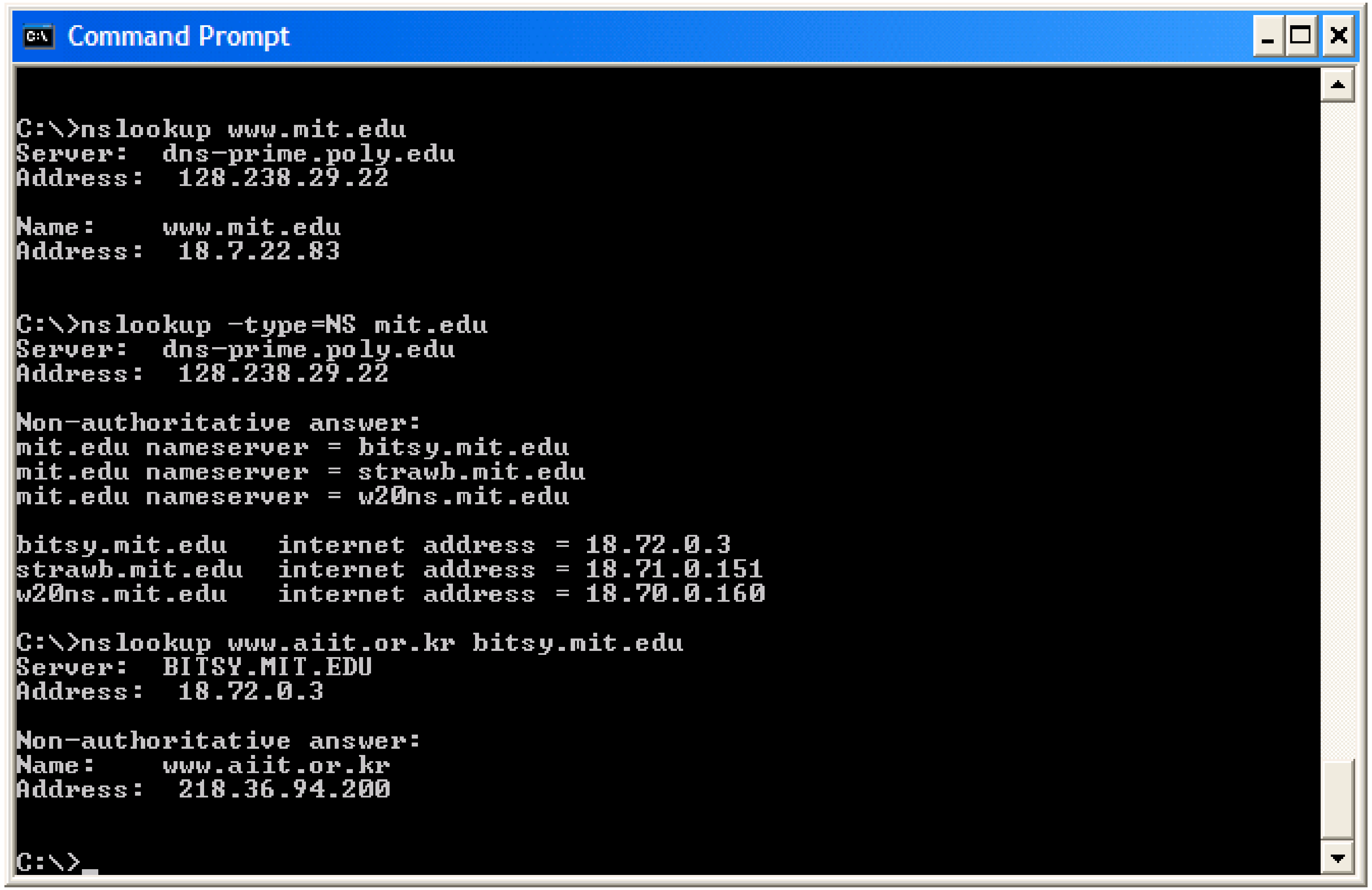
```
nslookup www.aiit.or.kr bitsy.mit.edu
```

    - The query and reply transaction takes place directly between our querying host and bitsy.mit.edu.

```
nslookup –option1 –option2 host-to-find dns-server
```

실험 3: DNS

- nslookup



```
C:\>nslookup www.mit.edu
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Name:    www.mit.edu
Address:  18.7.22.83


C:\>nslookup -type=NS mit.edu
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Non-authoritative answer:
mit.edu nameserver = bitsy.mit.edu
mit.edu nameserver = strawb.mit.edu
mit.edu nameserver = w20ns.mit.edu

bitsy.mit.edu   internet address = 18.72.0.3
strawb.mit.edu  internet address = 18.71.0.151
w20ns.mit.edu   internet address = 18.70.0.160

C:\>nslookup www.aiit.or.kr bitsy.mit.edu
Server:  BITSY.MIT.EDU
Address:  18.72.0.3

Non-authoritative answer:
Name:    www.aiit.or.kr
Address:  218.36.94.200


C:\>_
```

실험 3: DNS

- **ipconfig**
  - Enter

```
ipconfig /all
```

    - to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on

  - Enter

```
ipconfig /displaydns
```

    - Each entry shows the remaining Time to Live (TTL) in seconds.

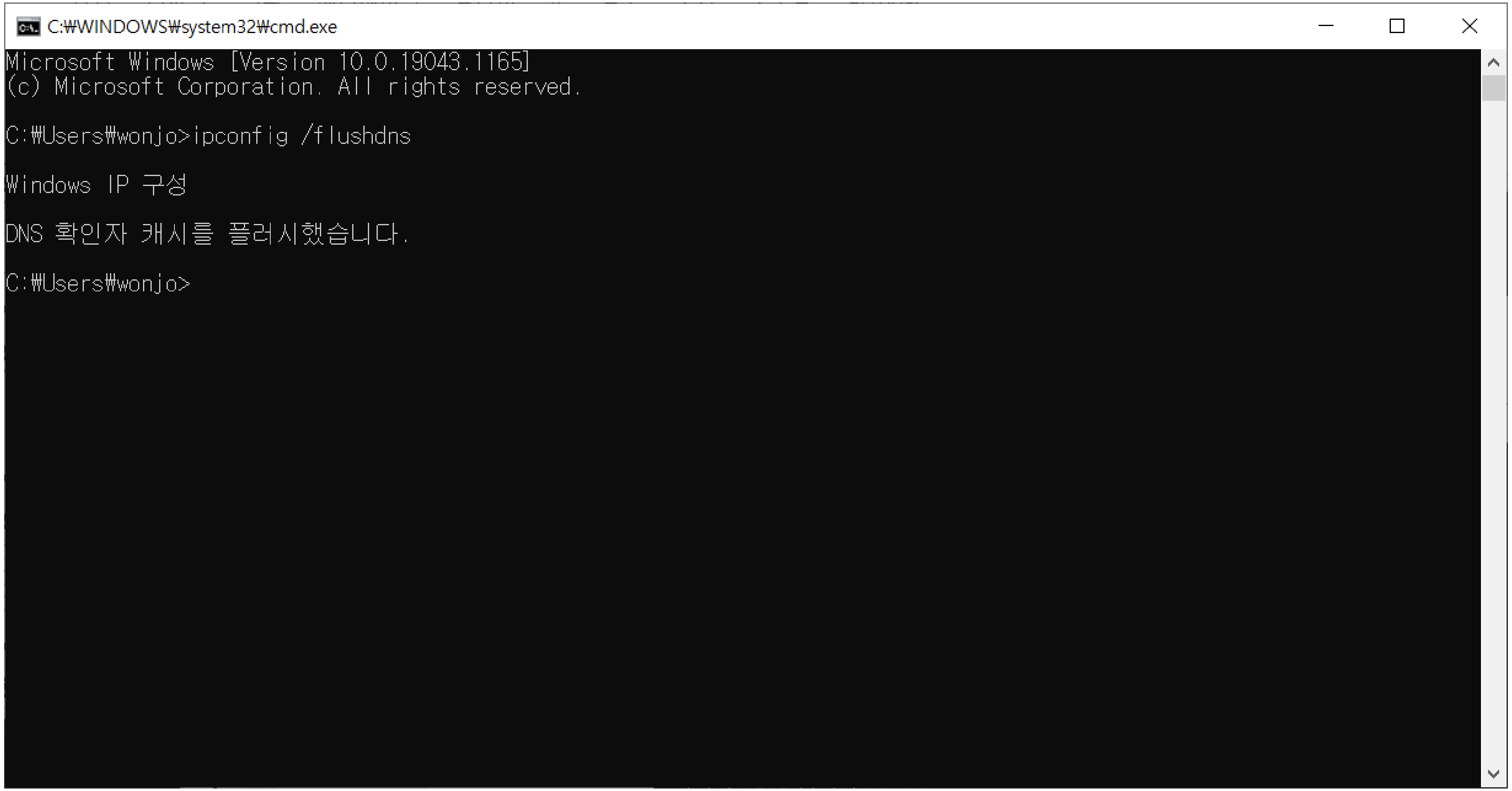
  - Enter

```
ipconfig /flushdns
```

    - Flushing the DNS cache clears all entries and reloads the entries from the hosts file.

실험 3: DNS

- ipconfig



C:₩WINDOWS₩system32₩cmd.exe

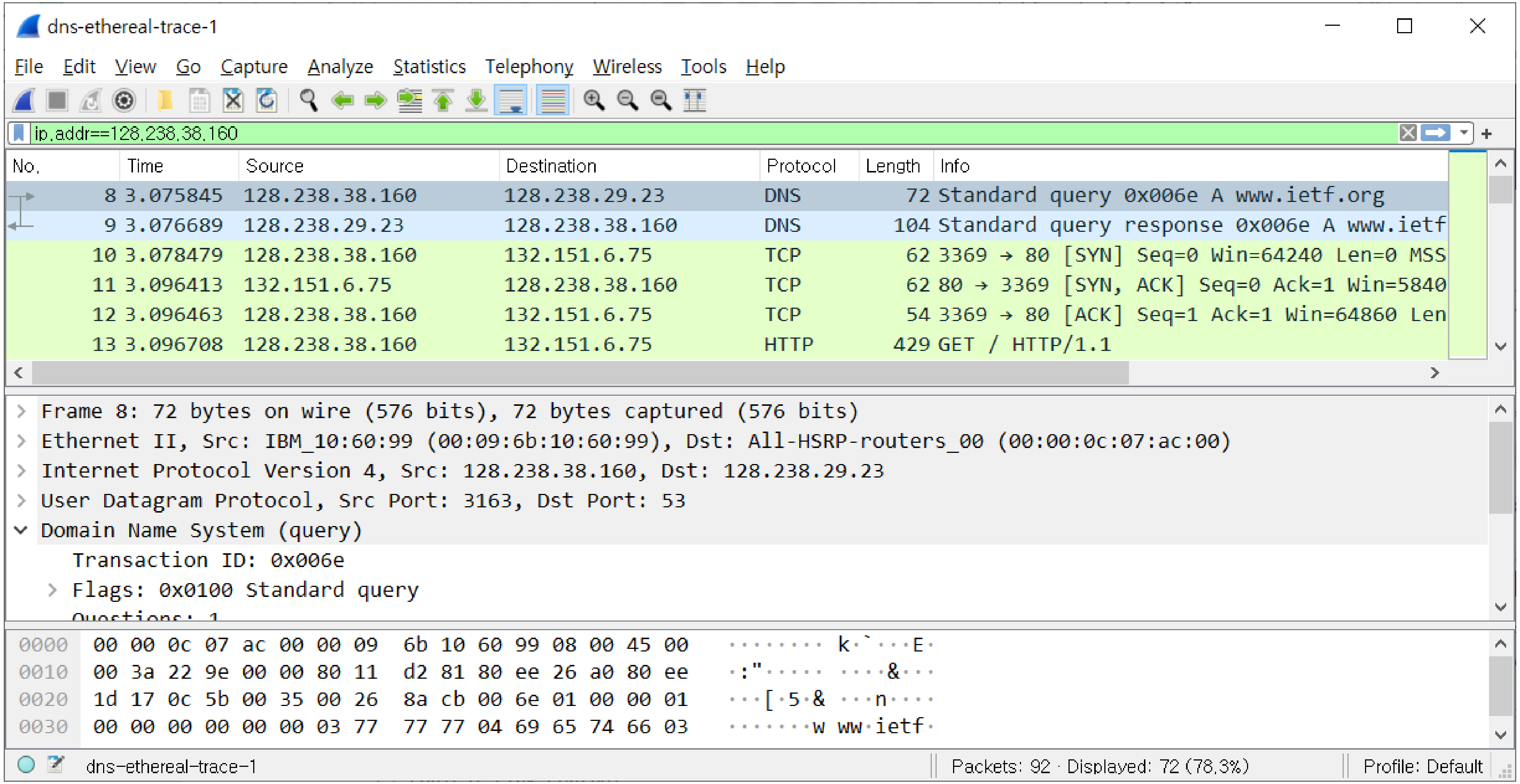
```
Microsoft Windows [Version 10.0.19043.1165]
(c) Microsoft Corporation. All rights reserved.

C:₩Users₩wonjo>ipconfig /flushdns

Windows IP 구성

DNS 확인자 캐시를 플러시했습니다.

C:₩Users₩wonjo>
```

실험 3: DNS

- **Tracing DNS with Wireshark**
  - Use *ipconfig* to empty the DNS cache in your host.
  - Open your browser and empty your browser cache. (With Internet Explorer, go to Tools menu and select Internet Options; then in the General tab select Delete Files.)
  - Open Wireshark and enter “ip.addr == your_IP_address” into the filter, where you obtain your_IP_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.
  - Start packet capture in Wireshark.
  - With your browser, visit the Web page: http://www.ietf.org.
  - Stop packet capture.
  - If you are unable to run Wireshark on a live network connection, you can download a packet trace file. Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file dns-ethereal-trace-1.

실험 3: DNS

- **Tracing DNS with Wireshark**


dns-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==128.238.38.160

No.	Time	Source	Destination	Protocol	Length	Info
8	3.075845	128.238.38.160	128.238.29.23	DNS	72	Standard query 0x006e A www.ietf.org
9	3.076689	128.238.29.23	128.238.38.160	DNS	104	Standard query response 0x006e A www.ietf
10	3.078479	128.238.38.160	132.151.6.75	TCP	62	3369 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS
11	3.096413	132.151.6.75	128.238.38.160	TCP	62	80 → 3369 [SYN, ACK] Seq=0 Ack=1 Win=5840
12	3.096463	128.238.38.160	132.151.6.75	TCP	54	3369 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len
13	3.096708	128.238.38.160	132.151.6.75	HTTP	429	GET / HTTP/1.1

```
> Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
> User Datagram Protocol, Src Port: 3163, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x006e
  > Flags: 0x0100 Standard query
    Questions: 1
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········ k·`···E·
0010  00 3a 22 9e 00 00 80 11  d2 81 80 ee 26 a0 80 ee   ·:"····· ····&···
0020  1d 17 0c 5b 00 35 00 26  8a cb 00 6e 01 00 00 01   ···[·5·& ···n····
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·
```

dns-ethereal-trace-1 | Packets: 92 · Displayed: 72 (78.3%) | Profile: Default

실험 3: DNS

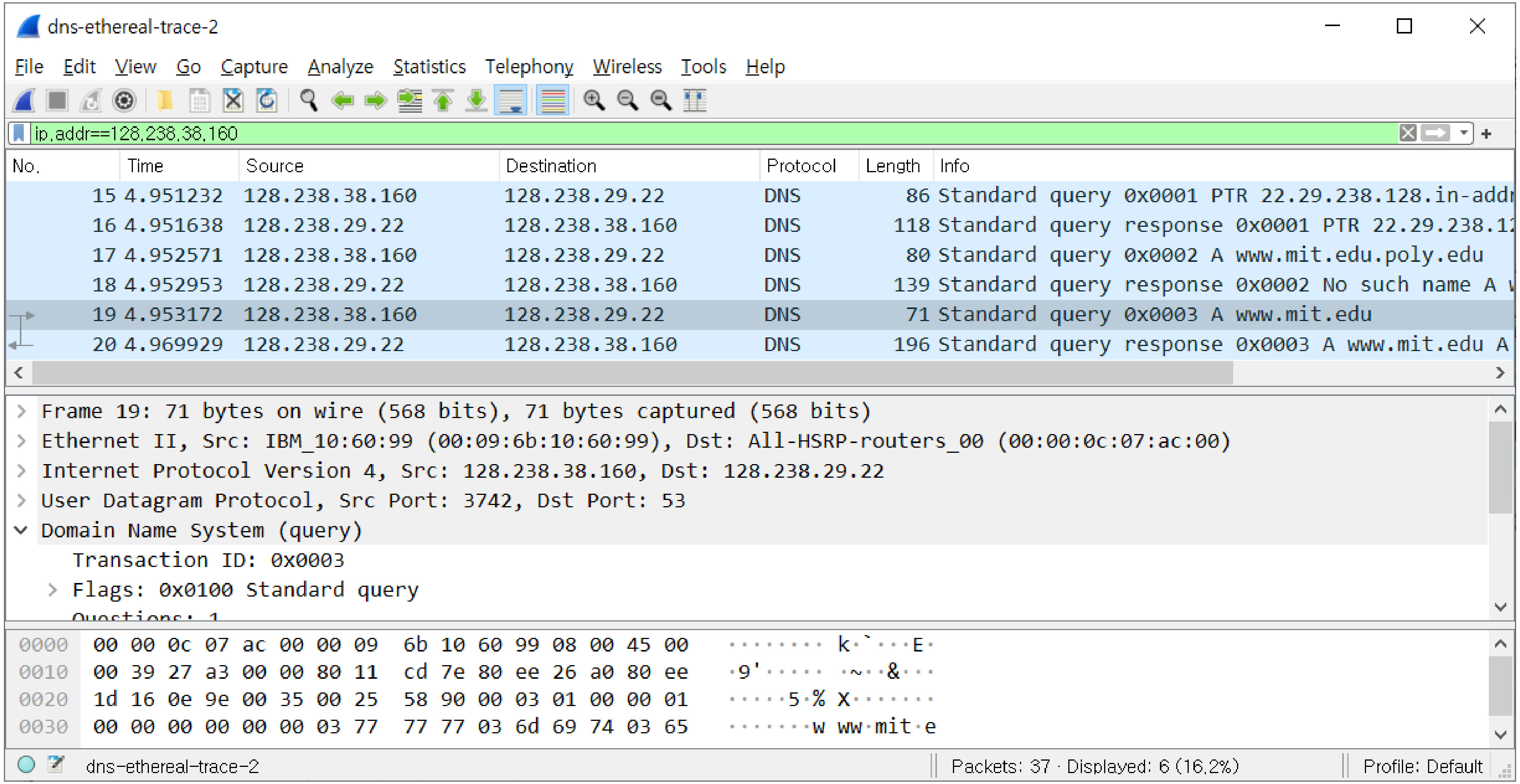
- **Tracing DNS with Wireshark**
  - 1. Locate the DNS query and response messages. Are then sent over UDP or TCP?
  - 2. What is the destination port for the DNS query message? What is the source port of DNS response message?
  - 3. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
  - 4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
  - 5. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
  - 6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
  - 7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

실험 3: DNS

- **Tracing DNS with Wireshark**
  - Start packet capture.
  - Do an *nslookup* on www.mit.edu.
  - Stop packet capture.
  - If you are unable to run Wireshark and capture a trace file, use the trace file dns-ethereal-trace-2 in the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip.
  - We see from the above screenshot that *nslookup* actually sent three DNS queries and received three DNS responses. For the purpose of this assignment, in answering the following questions, ignore the first two sets of queries/responses, as they are specific to *nslookup* and are not normally generated by standard Internet applications. You should instead focus on the last query and response messages.

실험 3: DNS

■ Tracing DNS with Wireshark



dns-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==128.238.38.160

```
No.   Time      Source          Destination     Protocol  Length Info
   15 4.951232  128.238.38.160  128.238.29.22   DNS           86 Standard query 0x0001 PTR 22.29.238.128.in-addr
   16 4.951638  128.238.29.22   128.238.38.160  DNS          118 Standard query response 0x0001 PTR 22.29.238.12
   17 4.952571  128.238.38.160  128.238.29.22   DNS           80 Standard query 0x0002 A www.mit.edu.poly.edu
   18 4.952953  128.238.29.22   128.238.38.160  DNS          139 Standard query response 0x0002 No such name A w
   19 4.953172  128.238.38.160  128.238.29.22   DNS           71 Standard query 0x0003 A www.mit.edu
   20 4.969929  128.238.29.22   128.238.38.160  DNS          196 Standard query response 0x0003 A www.mit.edu A
```

```
> Frame 19: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3742, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········k·`···E·
0010  00 39 27 a3 00 00 80 11  cd 7e 80 ee 26 a0 80 ee   ·9'······~··&···
0020  1d 16 0e 9e 00 35 00 25  58 90 00 03 01 00 00 01   ·····5·%X·······
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······www·mit·e
```

dns-ethereal-trace-2 | Packets: 37 · Displayed: 6 (16.2%) | Profile: Default

실험 3: DNS

- **Tracing DNS with Wireshark**
  - 8. What is the destination port for the DNS query message? What is the source port of DNS response message?
  - 9. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
  - 10. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
  - 11. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

실험 3: DNS

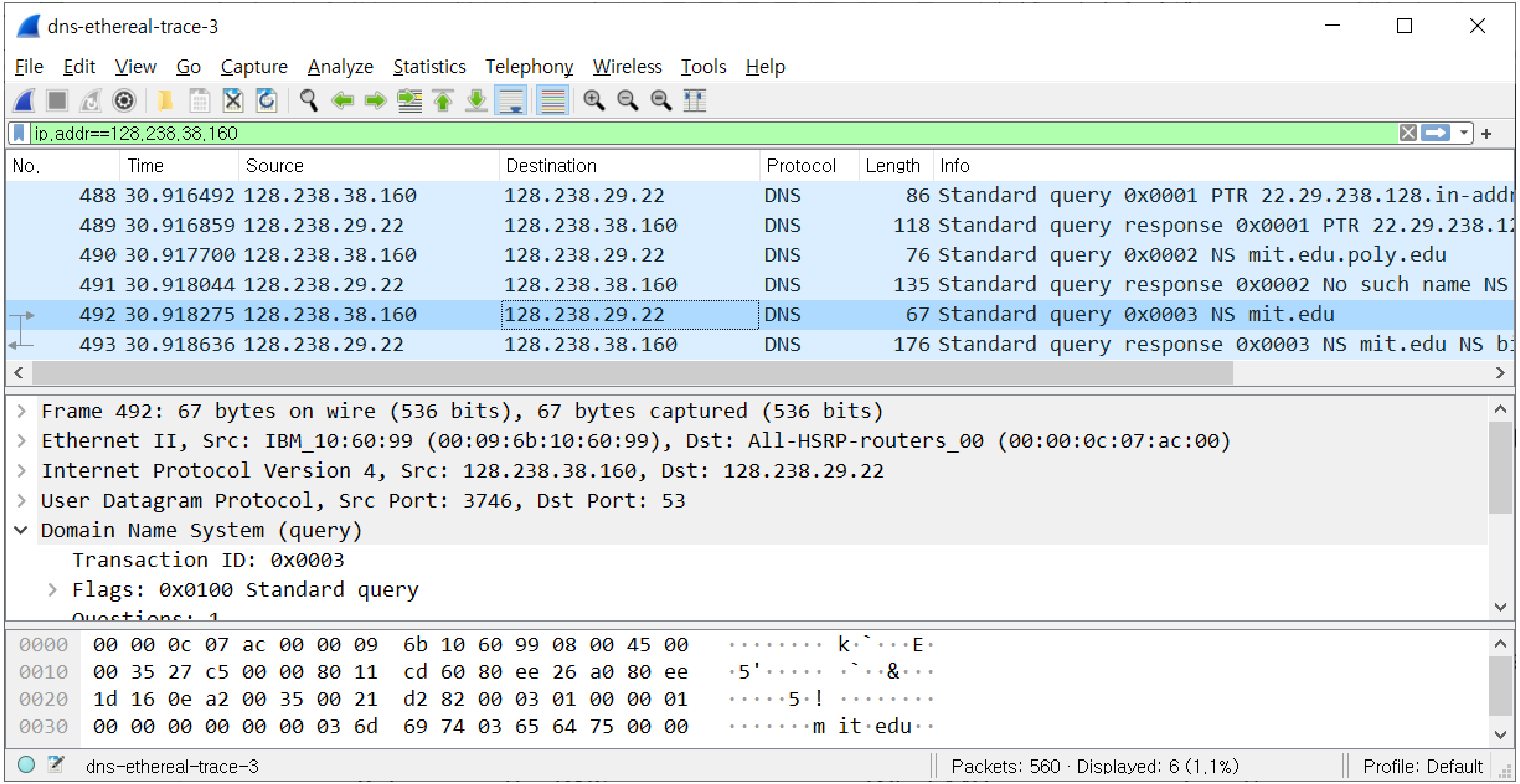
- **Tracing DNS with Wireshark**
  - Now repeat the previous experiment, but instead issue the command:

    ```
    nslookup –type=NS mit.edu
    ```

  - If you are unable to run Wireshark and capture a trace file, use the trace file dns-ethereal-trace-3 in the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip.
  - 12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
  - 13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
  - 14. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

실험 3: DNS

■ Tracing DNS with Wireshark



dns-ethereal-trace-3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==128.238.38.160

```
No.   Time       Source          Destination     Protocol  Length Info
  488 30.916492 128.238.38.160  128.238.29.22    DNS          86 Standard query 0x0001 PTR 22.29.238.128.in-addr
  489 30.916859 128.238.29.22   128.238.38.160   DNS         118 Standard query response 0x0001 PTR 22.29.238.12
  490 30.917700 128.238.38.160  128.238.29.22    DNS          76 Standard query 0x0002 NS mit.edu.poly.edu
  491 30.918044 128.238.29.22   128.238.38.160   DNS         135 Standard query response 0x0002 No such name NS
  492 30.918275 128.238.38.160  128.238.29.22    DNS          67 Standard query 0x0003 NS mit.edu
  493 30.918636 128.238.29.22   128.238.38.160   DNS         176 Standard query response 0x0003 NS mit.edu NS bi
```

```
> Frame 492: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3746, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········ k·`···E·
0010  00 35 27 c5 00 00 80 11  cd 60 80 ee 26 a0 80 ee   ·5'····· ·`··&···
0020  1d 16 0e a2 00 35 00 21  d2 82 00 03 01 00 00 01   ·····5·! ········
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
```

실험 3: DNS

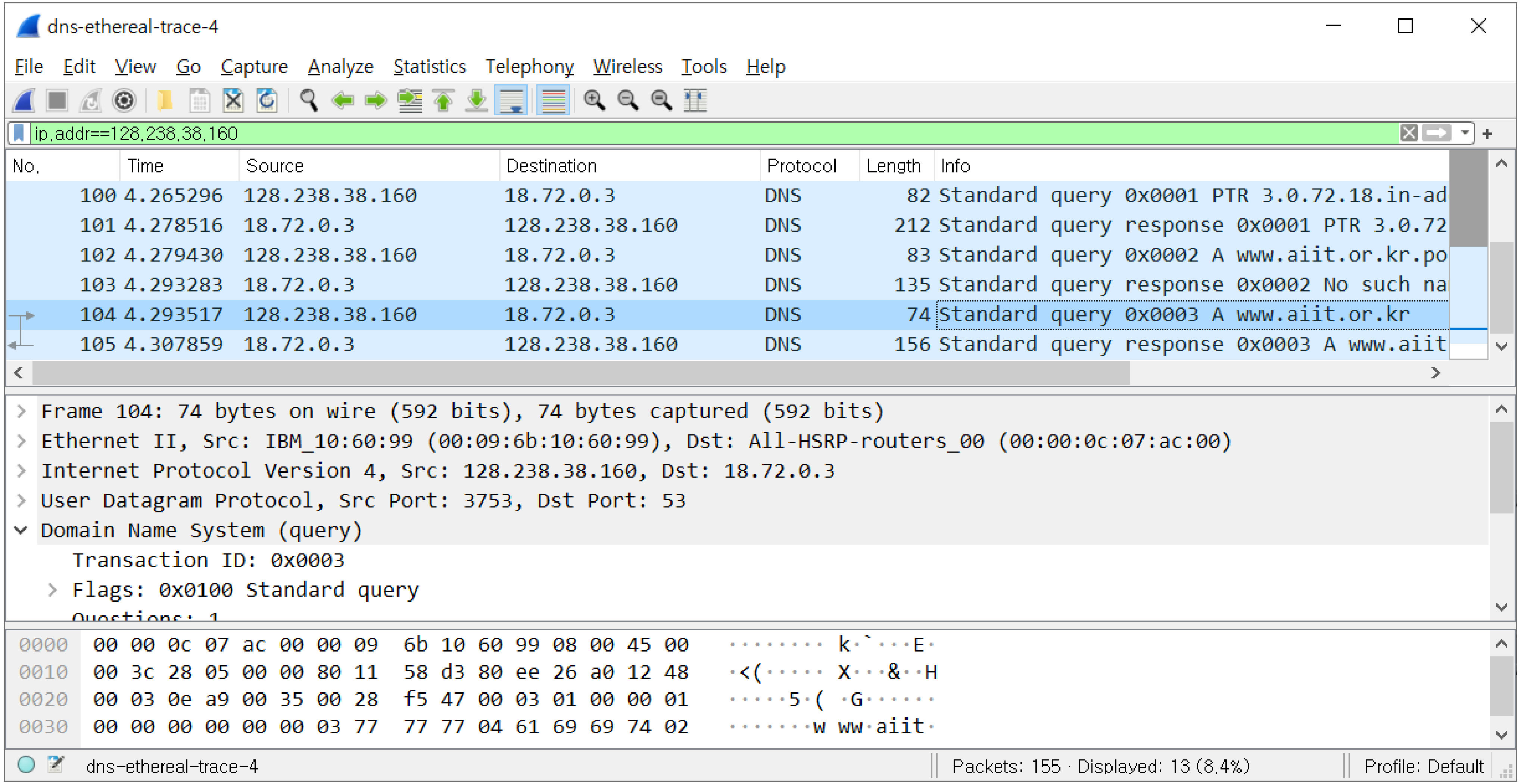
- **Tracing DNS with Wireshark**
  - Now repeat the previous experiment, but instead issue the command:

    ```
    nslookup www.aiit.or.kr bitsy.mit.edu
    ```

  - If you are unable to run Wireshark and capture a trace file, use the trace file dns-ethereal-trace-4 in the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip.
  - 15. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
  - 16. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
  - 17. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

실험 3: DNS

- **Tracing DNS with Wireshark**


dns-ethereal-trace-4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==128.238.38.160

No.	Time	Source	Destination	Protocol	Length	Info
100	4.265296	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-ad
101	4.278516	18.72.0.3	128.238.38.160	DNS	212	Standard query response 0x0001 PTR 3.0.72
102	4.279430	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.aiit.or.kr.po
103	4.293283	18.72.0.3	128.238.38.160	DNS	135	Standard query response 0x0002 No such na
104	4.293517	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.aiit.or.kr
105	4.307859	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A www.aiit

```
> Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 3753, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········ k·`···E·
0010  00 3c 28 05 00 00 80 11  58 d3 80 ee 26 a0 12 48   ·<(····· X···&··H
0020  00 03 0e a9 00 35 00 28  f5 47 00 03 01 00 00 01   ·····5·( ·G······
0030  00 00 00 00 00 00 03 77  77 77 04 61 69 69 74 02   ·······w ww·aiit·
```

dns-ethereal-trace-4 | Packets: 155 · Displayed: 13 (8.4%) | Profile: Default

결과 보고서

- **실험 1: Getting Started**
  - 질문에 답하기 (15 슬라이드)
- **실험 2: HTTP**
  - 질문에 답하기 (18, 21, 24 슬라이드)
- **실험 3: DNS**
  - 질문에 답하기 (31, 34, 35, 37 슬라이드)

  - 모든 답변은 Wireshark를 통해 확인한 packet에서 근거를 찾을 것. (사진 첨부)

예비 보고서

- **TCP protocol에 대해 조사**
  - TCP packet의 구성
  - SYN segment와 SYNACK segment의 역할
  - window의 의미

- **UDP protocol에 대해 조사**
  - UDP packet의 구성

- **IP protocol에 대해 조사**
  - IP datagram의 구성
  - TTL의 의미
  - fragmentation의 의미