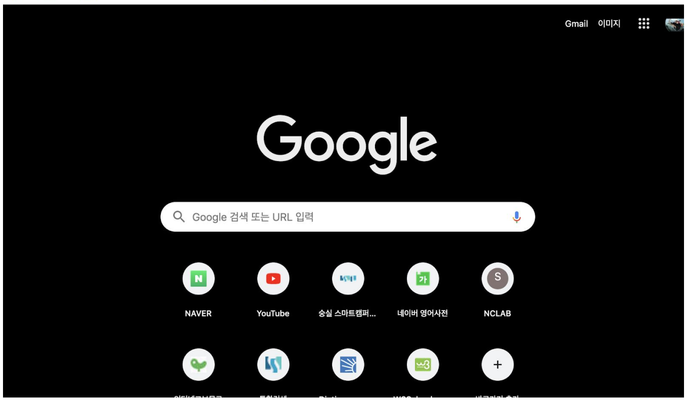
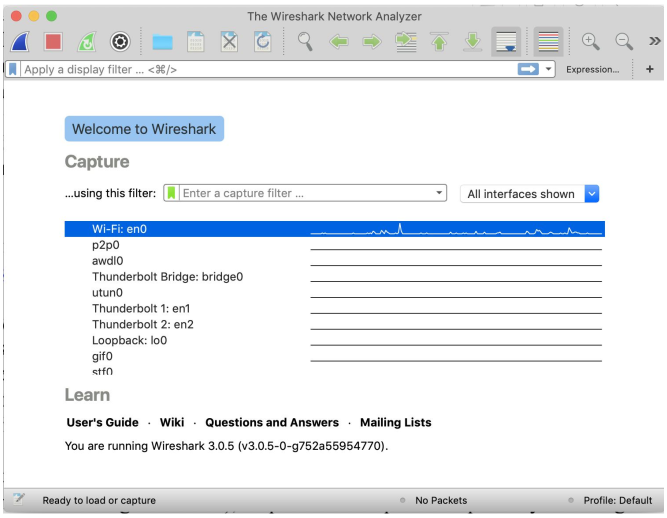
20132927_정재명_ wireshark_lab1_get_started

Taking Wireshark for a Test Run

1. 브라우저 실행.



2.와이어샤크 실행.


The Wireshark Network Analyzer
Apply a display filter … <⌘/>
Expression…
Welcome to Wireshark
Capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

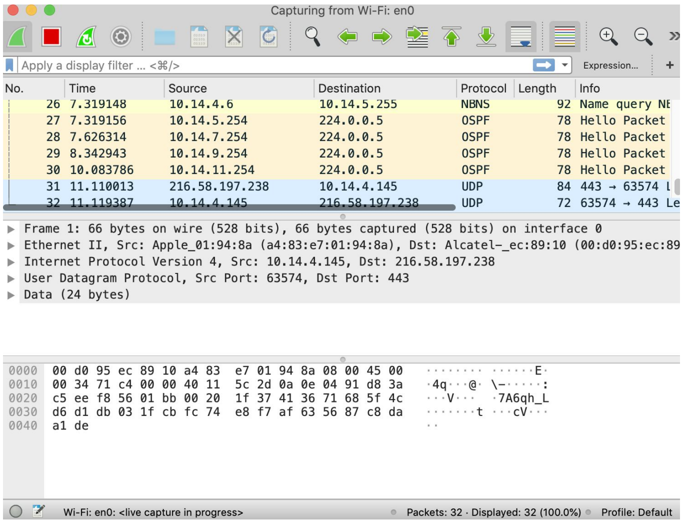
...using this filter: Enter a capture filter ... All interfaces shown

```
Wi-Fi: en0
p2p0
awdl0
Thunderbolt Bridge: bridge0
utun0
Thunderbolt 1: en1
Thunderbolt 2: en2
Loopback: lo0
gif0
stf0
```

You are running Wireshark 3.0.5 (v3.0.5-0-g752a55954770).

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

3. 캡쳐 시작.



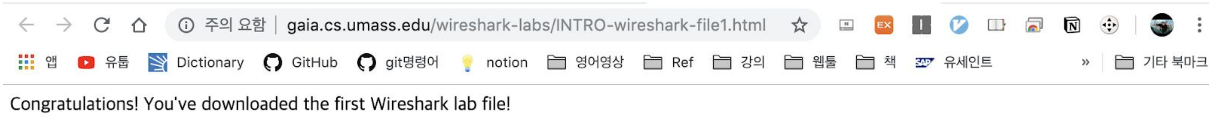
```
No.   Time        Source           Destination      Protocol  Length  Info
   26 7.319148    10.14.4.6        10.14.5.255      NBNS          92  Name query NE
   27 7.319156    10.14.5.254      224.0.0.5        OSPF          78  Hello Packet
   28 7.626314    10.14.7.254      224.0.0.5        OSPF          78  Hello Packet
   29 8.342943    10.14.9.254      224.0.0.5        OSPF          78  Hello Packet
   30 10.083786   10.14.11.254     224.0.0.5        OSPF          78  Hello Packet
   31 11.110013   216.58.197.238   10.14.4.145      UDP           84  443 → 63574 L
   32 11.119387   10.14.4.145      216.58.197.238   UDP           72  63574 → 443 Le
```

```
▶ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: Apple_01:94:8a (a4:83:e7:01:94:8a), Dst: Alcatel-_ec:89:10 (00:d0:95:ec:89
▶ Internet Protocol Version 4, Src: 10.14.4.145, Dst: 216.58.197.238
▶ User Datagram Protocol, Src Port: 63574, Dst Port: 443
▶ Data (24 bytes)
```

```
0000  00 d0 95 ec 89 10 a4 83  e7 01 94 8a 08 00 45 00   ········ ······E·
0010  00 34 71 c4 00 00 40 11  5c 2d 0a 0e 04 91 d8 3a   ·4q···@· \-·····:
0020  c5 ee f8 56 01 bb 00 20  1f 37 41 36 71 68 5f 4c   ···V···  ·7A6qh_L
0030  d6 d1 db 03 1f cb fc 74  e8 f7 af 63 56 87 c8 da   ·······t ···cV···
0040  a1 de                                              ··
```

Wi-Fi: en0: <live capture in progress> · Packets: 32 · Displayed: 32 (100.0%) · Profile: Default

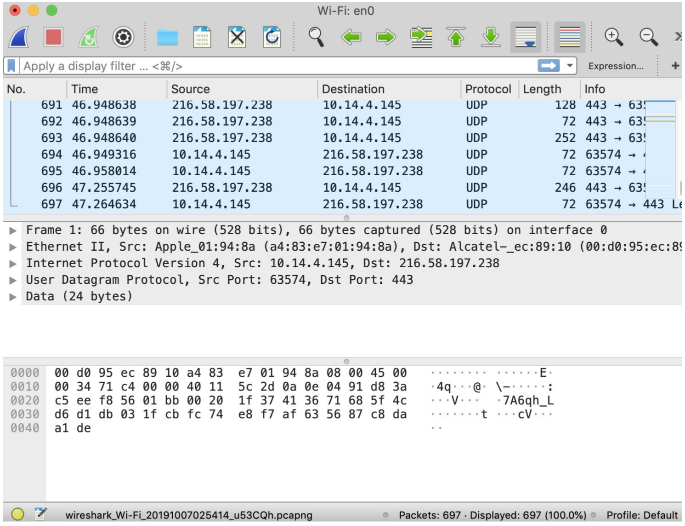
4. 브라우저 진입



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

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

5. 캡쳐 중단.



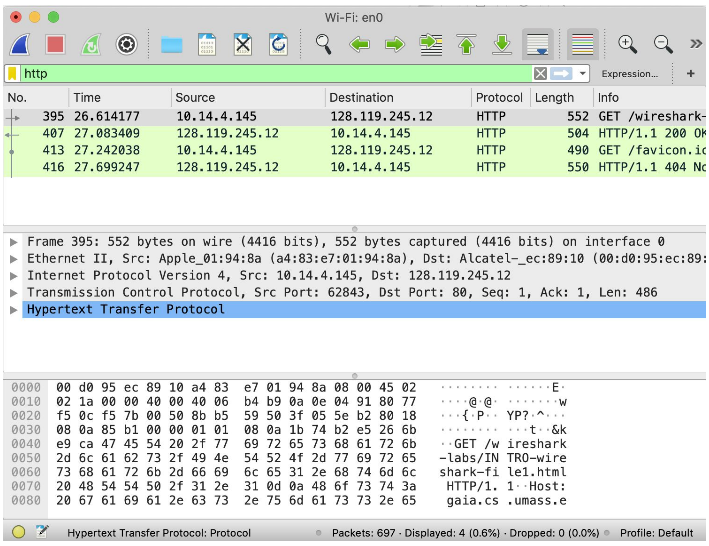
```
No.   Time       Source          Destination     Protocol Length Info
  691 46.948638  216.58.197.238  10.14.4.145     UDP        128  443 → 63!
  692 46.948639  216.58.197.238  10.14.4.145     UDP         72  443 → 63!
  693 46.948640  216.58.197.238  10.14.4.145     UDP        252  443 → 63!
  694 46.949316  10.14.4.145     216.58.197.238  UDP         72  63574 → 4
  695 46.958014  10.14.4.145     216.58.197.238  UDP         72  63574 → 4
  696 47.255745  216.58.197.238  10.14.4.145     UDP        246  443 → 63!
  697 47.264634  10.14.4.145     216.58.197.238  UDP         72  63574 → 443 Le
```

```
▶ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: Apple_01:94:8a (a4:83:e7:01:94:8a), Dst: Alcatel-_ec:89:10 (00:d0:95:ec:8
▶ Internet Protocol Version 4, Src: 10.14.4.145, Dst: 216.58.197.238
▶ User Datagram Protocol, Src Port: 63574, Dst Port: 443
▶ Data (24 bytes)
```

```
0000  00 d0 95 ec 89 10 a4 83  e7 01 94 8a 08 00 45 00   ········ ······E·
0010  00 34 71 c4 00 00 40 11  5c 2d 0a 0e 04 91 d8 3a   ·4q···@· \-·····:
0020  c5 ee f8 56 01 bb 00 20  1f 37 41 36 71 68 5f 4c   ···V···   ·7A6qh_L
0030  d6 d1 db 03 1f cb fc 74  e8 f7 af 63 56 87 c8 da   ·······t ···cV···
0040  a1 de                                              ··
```

wireshark_Wi-Fi_20191007025414_u53CQh.pcapng · Packets: 697 · Displayed: 697 (100.0%) · Profile: Default

6. http 필터링.



http

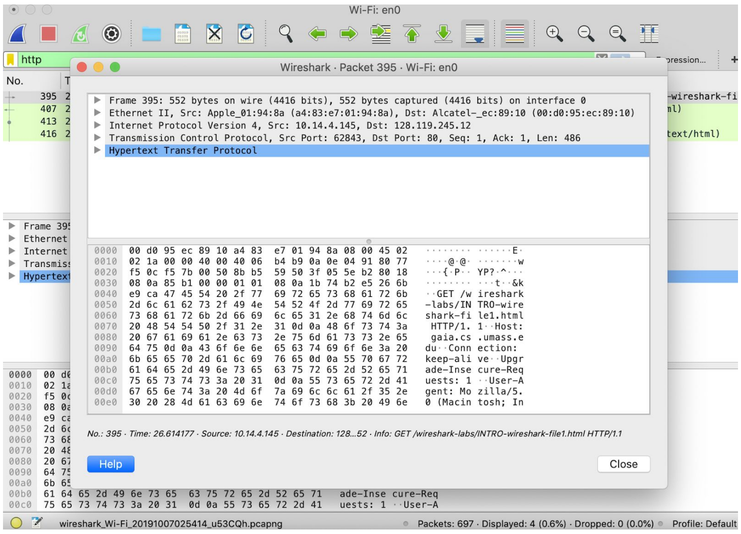
```
No.   Time       Source          Destination     Protocol Length Info
  395 26.614177  10.14.4.145     128.119.245.12  HTTP       552  GET /wireshark-
  407 27.083409  128.119.245.12  10.14.4.145     HTTP       504  HTTP/1.1 200 OK
  413 27.242038  10.14.4.145     128.119.245.12  HTTP       490  GET /favicon.ic
  416 27.699247  128.119.245.12  10.14.4.145     HTTP       550  HTTP/1.1 404 No
```

```
▶ Frame 395: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
▶ Ethernet II, Src: Apple_01:94:8a (a4:83:e7:01:94:8a), Dst: Alcatel-_ec:89:10 (00:d0:95:ec:89:
▶ Internet Protocol Version 4, Src: 10.14.4.145, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 62843, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
▶ Hypertext Transfer Protocol
```

```
0000  00 d0 95 ec 89 10 a4 83  e7 01 94 8a 08 00 45 02   ········ ······E·
0010  02 1a 00 00 40 00 40 06  b4 b9 0a 0e 04 91 80 77   ····@·@· ·······w
0020  f5 0c f5 7b 00 50 8b b5  59 50 3f 05 5e b2 80 18   ···{·P·· YP?·^···
0030  08 0a 85 b1 00 00 01 01  08 0a 1b 74 b2 e5 26 6b   ········ ···t··&k
0040  e9 ca 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 49 4e  54 52 4f 2d 77 69 72 65   -labs/IN TRO-wire
0060  73 68 61 72 6b 2d 66 69  6c 65 31 2e 68 74 6d 6c   shark-fi le1.html
0070  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
0080  20 67 61 69 61 2e 63 73  2e 75 6d 61 73 73 2e 65    gaia.cs .umass.e
```

Hypertext Transfer Protocol: Protocol · Packets: 697 · Displayed: 4 (0.6%) · Dropped: 0 (0.0%) · Profile: Default

7. GET 요청 패킷 분석



Wireshark · Packet 395 · Wi-Fi: en0

```
▶ Frame 395: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
▶ Ethernet II, Src: Apple_01:94:8a (a4:83:e7:01:94:8a), Dst: Alcatel-_ec:89:10 (00:d0:95:ec:89:10)
▶ Internet Protocol Version 4, Src: 10.14.4.145, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 62843, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
▶ Hypertext Transfer Protocol
```

```
0000  00 d0 95 ec 89 10 a4 83  e7 01 94 8a 08 00 45 02   ········ ······E·
0010  02 1a 00 00 40 00 40 06  b4 b9 0a 0e 04 91 80 77   ····@·@· ·······w
0020  f5 0c f5 7b 00 50 8b b5  59 50 3f 05 5e b2 80 18   ···{·P·· YP?·^···
0030  08 0a 85 b1 00 00 01 01  08 0a 1b 74 b2 e5 26 6b   ········ ···t··&k
0040  e9 ca 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 49 4e  54 52 4f 2d 77 69 72 65   -labs/IN TRO-wire
0060  73 68 61 72 6b 2d 66 69  6c 65 31 2e 68 74 6d 6c   shark-fi le1.html
0070  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
0080  20 67 61 69 61 2e 63 73  2e 75 6d 61 73 73 2e 65    gaia.cs .umass.e
0090  64 75 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   du··Conn ection: 
00a0  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 55 70 67 72   keep-ali ve··Upgr
00b0  61 64 65 2d 49 6e 73 65  63 75 72 65 2d 52 65 71   ade-Inse cure-Req
00c0  75 65 73 74 73 3a 20 31  0d 0a 55 73 65 72 2d 41   uests: 1 ··User-A
00d0  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
00e0  30 20 28 4d 61 63 69 6e  74 6f 73 68 3b 20 49 6e   0 (Macin tosh; In
```

No.: 395 · Time: 26.614177 · Source: 10.14.4.145 · Destination: 128...52 · Info: GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

wireshark_Wi-Fi_20191007025414_u53CQh.pcapng · Packets: 697 · Displayed: 4 (0.6%) · Dropped: 0 (0.0%) · Profile: Default

What to hand in

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

-> UDP, NBNS, SSDP

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*.)

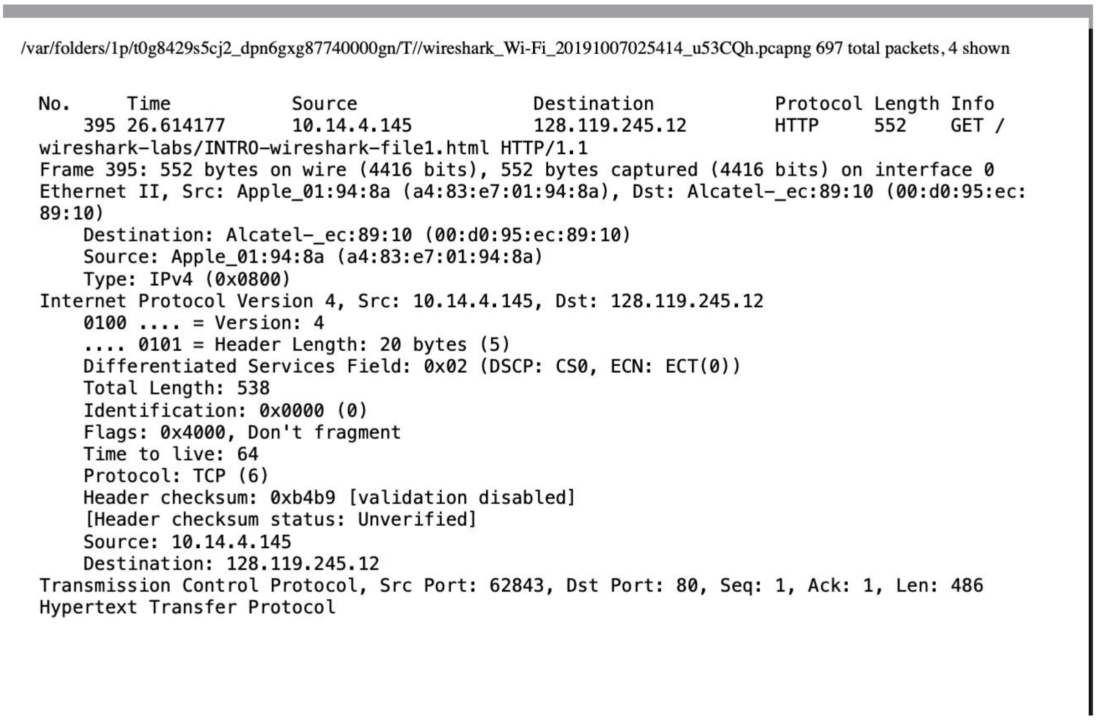
-> 0.469232 초.

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?

-> me : 10.14.4.145 / gaia.cs.umass.edu : 128.119.245.12

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.

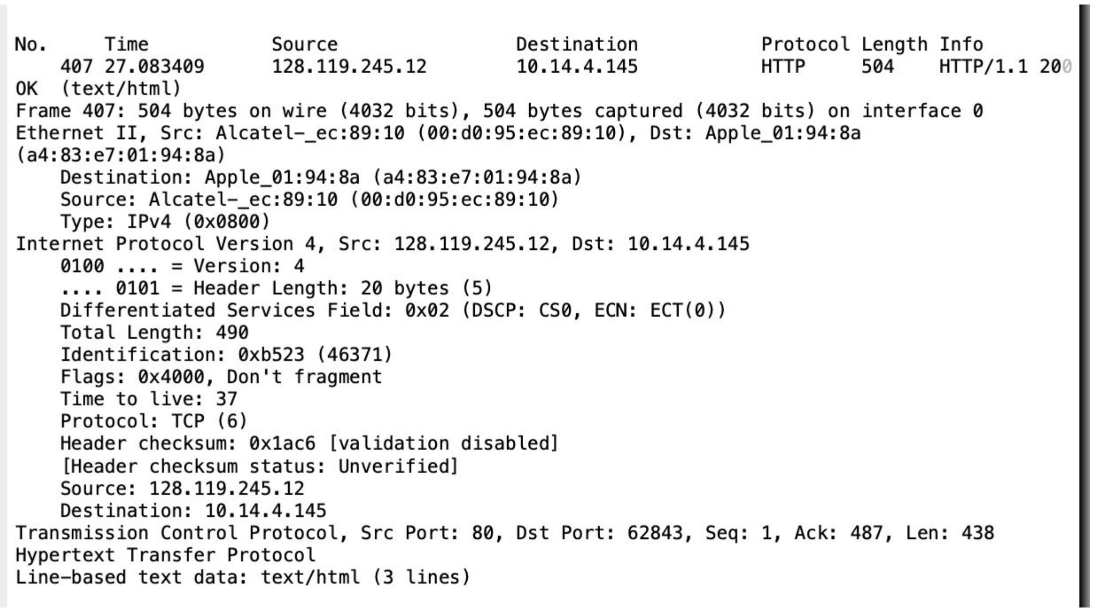
- GET



/var/folders/1p/t0g8429s5cj2_dpn6gxg87740000gn/T//wireshark_Wi-Fi_20191007025414_u53CQh.pcapng 697 total packets, 4 shown

```
No.     Time           Source                Destination           Protocol Length Info
    395 26.614177      10.14.4.145           128.119.245.12        HTTP     552    GET /
wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 395: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
Ethernet II, Src: Apple_01:94:8a (a4:83:e7:01:94:8a), Dst: Alcatel-_ec:89:10 (00:d0:95:ec:
89:10)
    Destination: Alcatel-_ec:89:10 (00:d0:95:ec:89:10)
    Source: Apple_01:94:8a (a4:83:e7:01:94:8a)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.14.4.145, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0))
    Total Length: 538
    Identification: 0x0000 (0)
    Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xb4b9 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.14.4.145
    Destination: 128.119.245.12
Transmission Control Protocol, Src Port: 62843, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
Hypertext Transfer Protocol
```

- OK



```
No.     Time           Source                Destination           Protocol Length Info
    407 27.083409      128.119.245.12        10.14.4.145           HTTP     504    HTTP/1.1 200
OK  (text/html)
Frame 407: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface 0
Ethernet II, Src: Alcatel-_ec:89:10 (00:d0:95:ec:89:10), Dst: Apple_01:94:8a
(a4:83:e7:01:94:8a)
    Destination: Apple_01:94:8a (a4:83:e7:01:94:8a)
    Source: Alcatel-_ec:89:10 (00:d0:95:ec:89:10)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.14.4.145
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0))
    Total Length: 490
    Identification: 0xb523 (46371)
    Flags: 0x4000, Don't fragment
    Time to live: 37
    Protocol: TCP (6)
    Header checksum: 0x1ac6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 10.14.4.145
Transmission Control Protocol, Src Port: 80, Dst Port: 62843, Seq: 1, Ack: 487, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```