

Wireshark Lab: Getting Started

Copyright (c) 2020 Minaduki Shigure.

南京大学 电子科学与工程学院 吴康正 171180571

实验环境

Ubuntu 19.10 eoan w/ x86_64 Linux 5.3.0-40-generic

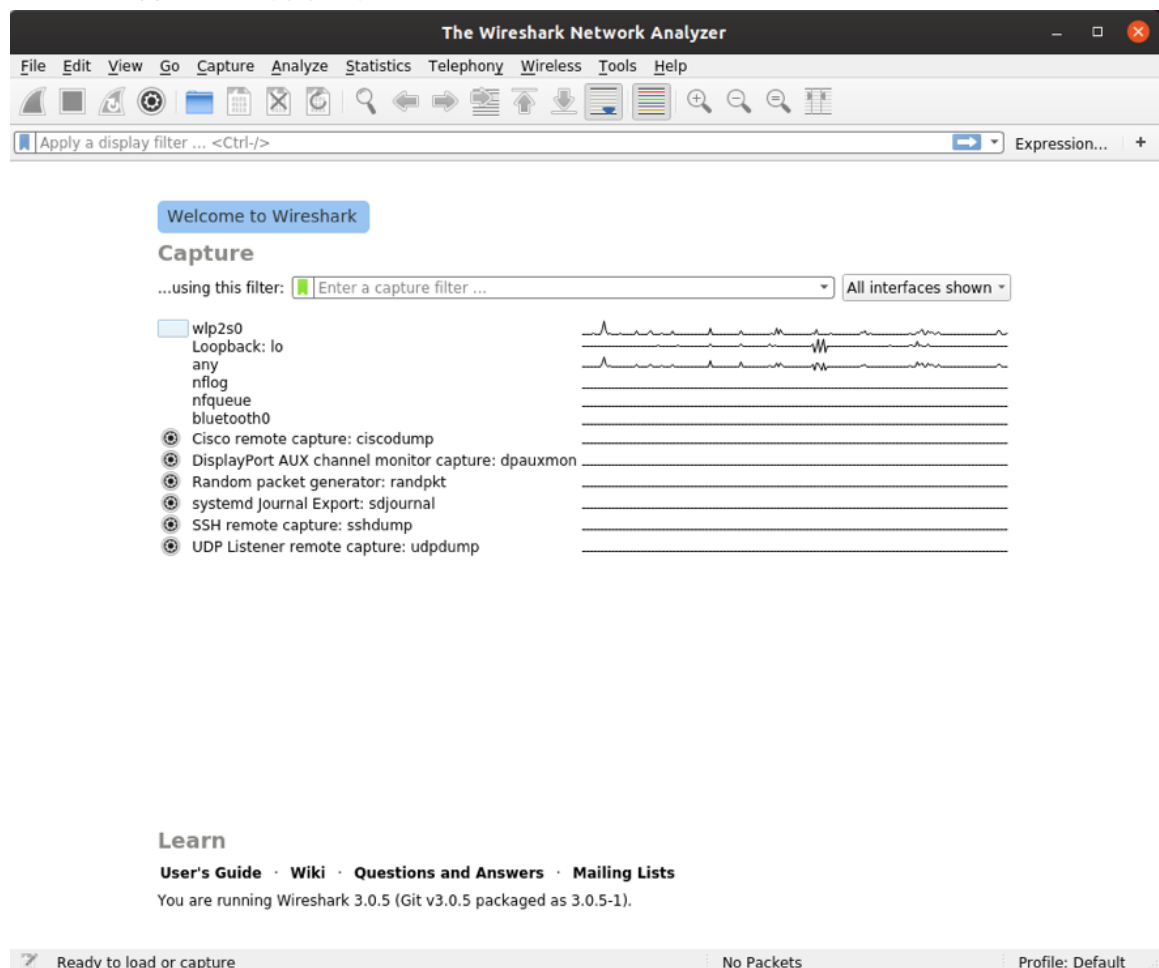
Broadcom BCM4352 Wireless Network Adapter

Wireshark Version 3.0.5 (Git v3.0.5 packaged as 3.0.5-1)

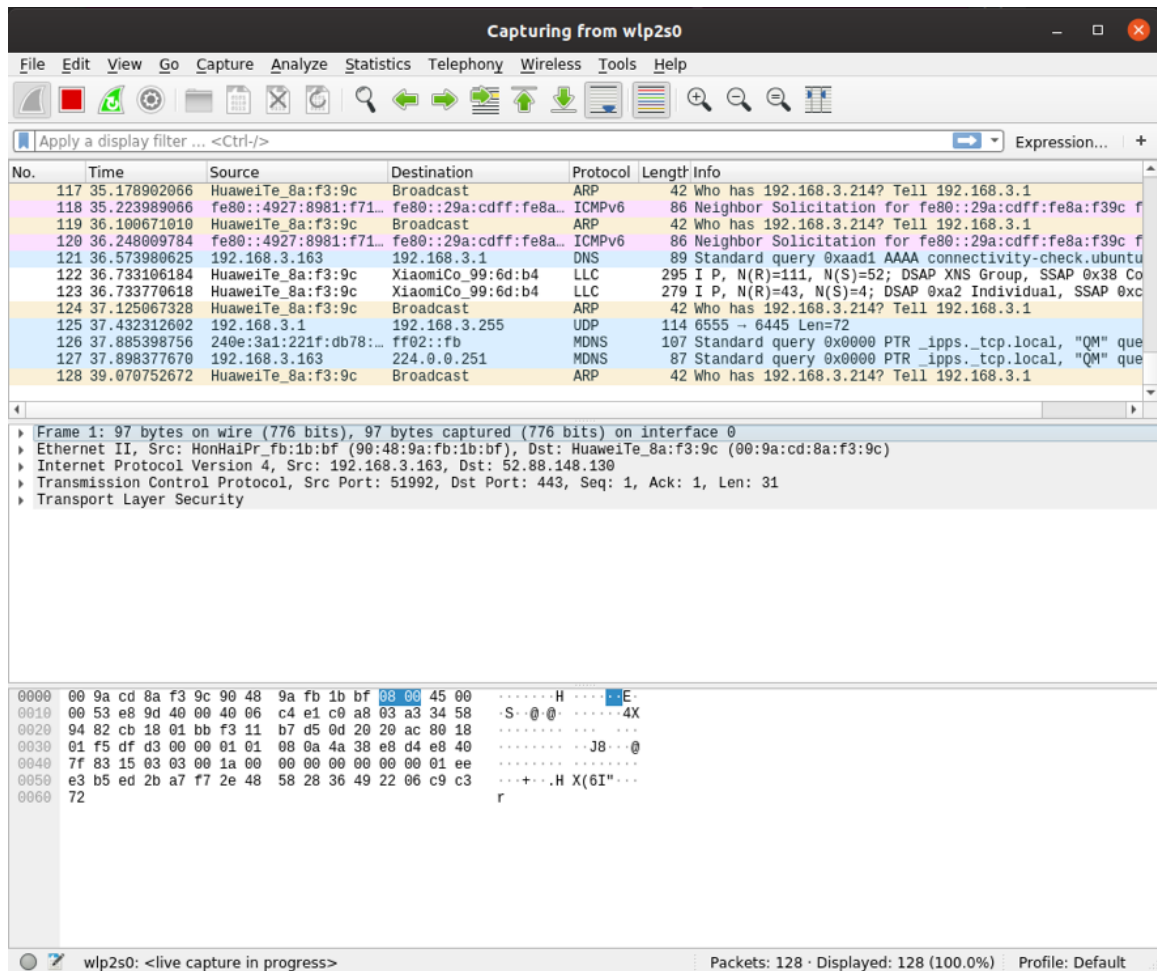
实验内容：你好，世界！

1. 首先运行Wireshark，从原则上来说，不应该允许任何非root用户拥有抓包的权限，因此切换到超级用户，然后再运行程序。

可以看到启动后的界面如下所示：



2. 启动后的界面列出了电脑上可供监听的端口，选择wlp2s0来监听此电脑无线网卡上的所有通讯，可以看见图示中就捕获到了一些不同协议的通讯，比如路由器广播的ARP询问、电脑系统更新时查询服务器DNS的请求等。



3. 按照课本上的要求，访问网页<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>，在Wireshark中找到了如下和此次请求有关联的封包：

The screenshot shows the Wireshark interface with a capture on interface 0. The packet list displays the following traffic:

No.	Time	Source	Destination	Protocol	Length	Info
7	1.464585612	192.168.3.163	192.168.3.1	DNS	77	Standard query 0x0f0c A gaia.cs.umass.edu
8	1.467307100	192.168.3.1	192.168.3.163	DNS	93	Standard query response 0x0f0c A gaia.cs.umass.edu
9	1.468319722	192.168.3.163	128.119.245.12	TCP	74	37294 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
10	1.536080882	HuaweiTe_8a:f3:9c	Broadcast	ARP	42	Who has 192.168.3.214? Tell 192.168.3.1
11	1.718501933	192.168.3.163	128.119.245.12	TCP	74	37298 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
12	1.727865622	128.119.245.12	192.168.3.163	TCP	74	80 → 37294 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
13	1.727908401	192.168.3.163	128.119.245.12	TCP	66	37294 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=
14	1.728137969	192.168.3.163	128.119.245.12	HTTP	554	GET /wireshark-labs/INTRO-wireshark-file1.html
15	2.049510397	128.119.245.12	192.168.3.163	TCP	74	80 → 37298 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
16	2.049601343	192.168.3.163	128.119.245.12	TCP	66	37298 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=
17	2.049518647	128.119.245.12	192.168.3.163	TCP	66	80 → 37294 [ACK] Seq=1 Ack=489 Win=30080 Len=0
18	2.050217356	128.119.245.12	192.168.3.163	HTTP	305	HTTP/1.1 304 Not Modified
19	2.050240816	192.168.3.163	128.119.245.12	TCP	66	37294 → 80 [ACK] Seq=489 Ack=240 Win=64128 Len=0

The packet details for frame 18 show the following structure:

- Frame 18: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface 0
- Ethernet II, Src: HuaweiTe_8a:f3:9c (00:9a:cd:8a:f3:9c), Dst: HonHaiPr_fb:1b:bf (90:48:9a:fb:1b:bf)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.3.163
- Transmission Control Protocol, Src Port: 80, Dst Port: 37294, Seq: 1, Ack: 489, Len: 239
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```

0000  90 48 9a fb 1b bf 00 9a cd 8a f3 9c 08 00 45 00  H.....E
0010  01 23 cb 5c 40 00 2c 06 48 a9 80 77 f5 0c c9 a8  #\@, H-w...
0020  03 a3 00 50 91 ae f2 9b 36 f8 c3 71 50 e1 80 18  .P...6-qP...
0030  00 eb 9b b0 00 00 01 01 08 0a 20 54 fd a9 c1 4f  .....T...O
0040  b4 09 48 54 54 50 2f 31 2e 31 20 33 30 34 20 4e  .HTTP/1.1 304 N
0050  6f 74 20 4d 6f 64 69 66 69 65 64 0d 0a 44 61 74  ot Modif led Dat
0060  65 3a 20 57 65 64 2c 20 32 35 20 4d 61 72 20 32  e: Wed, 25 Mar 2
0070  30 32 30 20 31 34 3a 30 31 3a 35 34 20 47 4d 54  020 14:0 1:54 GMT
0080  0d 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68 65  .Server: Apache
0090  2f 32 2e 34 2e 36 20 28 43 65 6e 74 4f 53 29 20  /2.4.6 (CentOS)
00a0  4f 70 65 6e 53 53 4c 2f 31 2e 30 2e 32 6b 2d 66  OpenSSL/ 1.0.2k-f
00b0  69 70 73 20 50 48 50 2f 35 2e 34 2e 31 36 20 6d  ips PHP/ 5.4.16 m
00c0  6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 31 31 20 50  od_perl/ 2.0.11 P
00d0  65 72 6c 2f 76 35 2e 31 36 2e 33 0d 0a 43 6f 6e  erl/v5.1 6.3 Con
00e0  6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c  nection: Keep-AL
  
```

4. 可以看见，本地计算机首先向DNS服务器（在本例中配置为路由器）发送了一个DNS请求，得到了网页服务器的IP地址，然后与远程服务器建立了TCP连接，发送HTTP GET请求，远程服务器收到请求后建立TCP连接将HTTP响应发回本地计算机，完成了网页的访问。

另外，可以使用Wireshark的过滤器功能筛选出所有的HTTP请求，列出如下：

The screenshot displays the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets, with the first three highlighted. The middle pane shows the details of the selected packet (Frame 18), including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

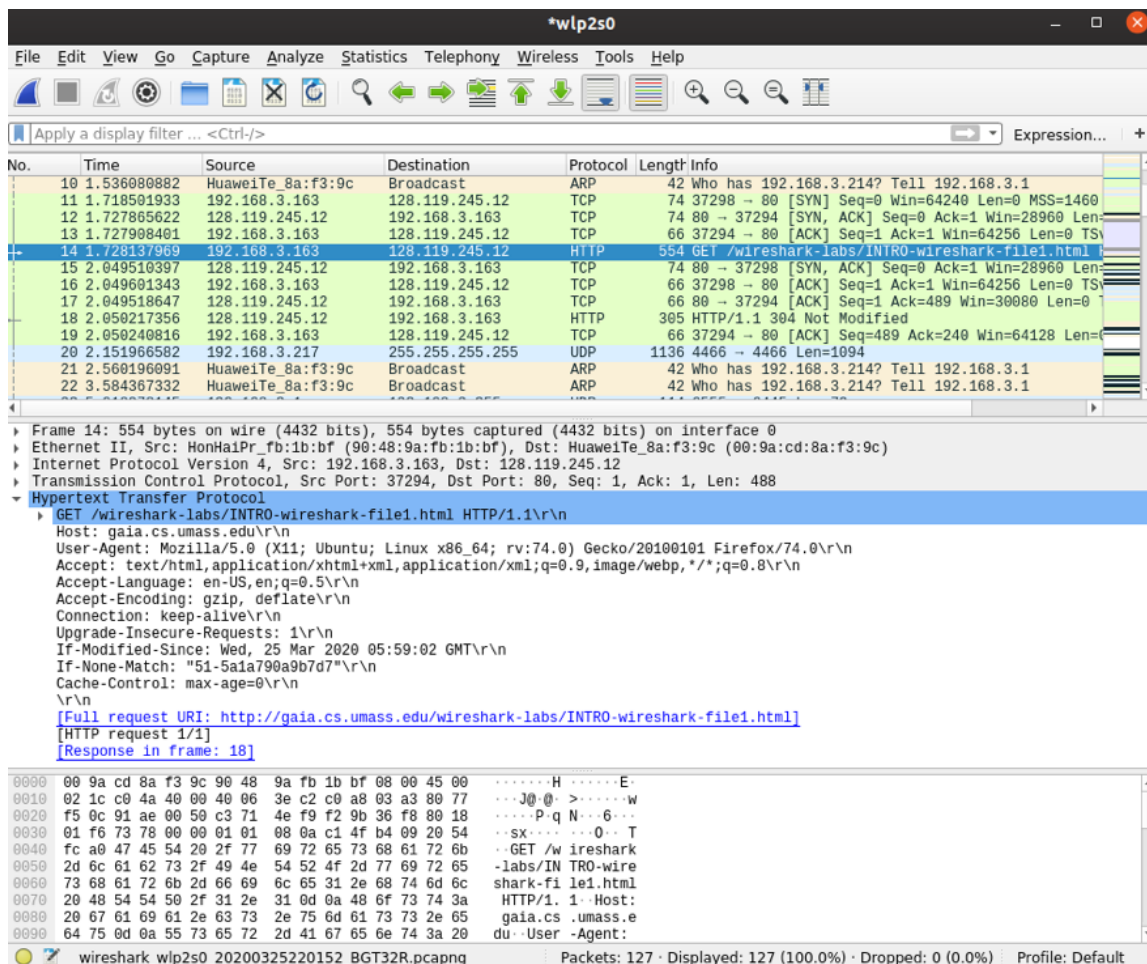
No.	Time	Source	Destination	Protocol	Length	Info
14	1.728137969	192.168.3.163	128.119.245.12	HTTP	554	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
18	2.050217356	128.119.245.12	192.168.3.163	HTTP	305	HTTP/1.1 304 Not Modified
83	16.421682160	192.168.3.163	128.119.245.12	HTTP	554	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
87	16.695656469	128.119.245.12	192.168.3.163	HTTP	305	HTTP/1.1 304 Not Modified
116	22.223138679	192.168.3.163	128.119.245.12	HTTP	554	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 18: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface 0
 Ethernet II, Src: HuaweiTe_8a:f3:9c (08:9a:cd:8a:f3:9c), Dst: HonHaiPr_fb:1b:bf (90:48:9a:fb:1b:bf)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.3.163
 Transmission Control Protocol, Src Port: 80, Dst Port: 37294, Seq: 1, Ack: 489, Len: 239
 Hypertext Transfer Protocol

0000 90 48 9a fb 1b bf 00 9a cd 8a f3 9c 00 00 45 00 H... ..E
 0010 01 23 cb 5c 40 00 2c 06 48 a9 80 77 f5 0c c0 a8 #\@, H-w...
 0020 03 a3 00 50 91 ae f2 9b 36 f8 c3 71 50 e1 80 18 P... 6-qP...
 0030 00 eb 9b b0 00 00 01 01 08 0a 20 54 fd a9 c1 4f T...0
 0040 b4 09 48 54 54 50 2f 31 2e 31 20 33 30 34 20 4e ..HTTP/1.1 304 N
 0050 6f 74 20 4d 6f 64 69 66 69 65 64 0d 0a 44 61 74 ot Modif ied Dat
 0060 65 3a 20 57 65 64 2c 20 32 35 20 4d 61 72 20 32 e: Wed, 25 Mar 2
 0070 30 32 30 20 31 34 3a 30 31 3a 35 34 20 47 4d 54 020 14:0 1:54 GMT
 0080 0d 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68 65 ..Server : Apache
 0090 2f 32 2e 34 2e 36 20 28 43 65 6e 74 4f 53 29 20 /2.4.6 (CentOS)
 00a0 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e 32 6b 2d 66 OpenSSL/ 1.0.2k-f
 00b0 69 70 73 20 50 48 50 2f 35 2e 34 2e 31 36 20 6d ips PHP/ 5.4.16 m
 00c0 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 31 31 20 50 od_perl/ 2.0.11 P
 00d0 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 0a 43 6f 6e erl/v5.1 6.3 Con
 00e0 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c nection: Keep-Al

wireshark_wlp2s0_20200325220152_BGT32R.pcapng Packets: 127 · Displayed: 5 (3.9%) · Dropped: 0 (0.0%) Profile: Default

- 按照课本要求，找到本地计算机发出的HTTP GET请求，Wireshark对数据包进行了层次化的结构分析，展开HTTP层的内容，就可以看到具体的GET请求内容。



小结

对于上面获得的HTTP封包，可以看见由于之前已经访问过这个页面，因此此次访问的请求header中包含了“Modified After”的entry，而网页内容的确没有修改，因此收到的响应是“304 Not Modified”，而不是200，服务器也没有回传网页内容，本地浏览器使用了缓存的网页进行显示。

另外发现，在我的计算机上，在启动Wireshark抓包时，有时会完全无法连接网络，询问同学得知，这似乎是Linux上Wireshark的一个普遍Bug，因此在下面的打印请求部分和以后的实验会更换其他平台完成。

对实验要求问题的解答：

1. List 3 protocols: 比如有ARP、DNS、SSL、HTTP、DHCPv6、ICMPv6、TCP、UDP、SMB2等。
2. How Long: 发送HTTP GET请求的时间戳是1.728137696，接收到返回新消息的时间戳是2.050217356，总共耗时0.32207966秒。
3. IP: 服务器的IP地址为128.119.245.12，本机地址由于存在NAT的关系，只能看见LAN地址为192.168.3.163。
4. 由于要求打印的是OK的响应，而之前实验时没有记录到200 OK，因此这里的请求内容是在更换平台之后重新发出记录的。

打印出来的两个请求如下，同时PDF源文件Wireshark-HTTP-Capture1.pdf也在同一目录中提供：

No.	Time	Source	Destination
150	2.166290	192.168.3.163	128.119.245.12

HTTP 465 GET /
 wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 Frame 150: 465 bytes on wire (3720 bits), 465 bytes captured (3720 bits) on interface en1, id 0
 Ethernet II, Src: HonHaiPr_fb:1b:bf (90:48:9a:fb:1b:bf), Dst: HuaweiTe_8a:f3:9c (00:9a:cd:8a:f3:9c)
 Internet Protocol Version 4, Src: 192.168.3.163, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 59856, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
 Hypertext Transfer Protocol
 GET /wireshark-labs/HTTP-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_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15\r\n
 Accept-Language: zh-cn\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: keep-alive\r\n

No.
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
 [HTTP request 1/1]
 [Response in frame: 168]

No.	Time	Source	Destination	P
168	2.404677	128.119.245.12	192.168.3.163	H

HTTP 552 HTTP/1.1
 200 OK (text/html)
 Frame 168: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en1, id 0
 Ethernet II, Src: HuaweiTe_8a:f3:9c (00:9a:cd:8a:f3:9c), Dst: HonHaiPr_fb:1b:bf (90:48:9a:fb:1b:bf)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.3.163

Transmission Control Protocol, Src Port: 80, Dst Port: 59856, Seq: 1, Ack: 400, Len: 486

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Thu, 26 Mar 2020 07:00:03 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Thu, 26 Mar 2020 05:59:03 GMT\r\n

ETag: "80-5a1bbae97fe64"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 128\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: 0.238387000 seconds]

[Request in frame: 150]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

File Data: 128 bytes

Line-based text data: text/html (4 lines)