计算机网络lab0实验报告

PB19071535徐昊天

一.实验目的

1. 观察协议实体之间交换的消息序列，深入研究协议操作的细节。
2. 了解Wireshark,并进行一些简单的抓包和观察。

二.实验工具

wireshark数据包嗅探器，可用于计算机中的数据包捕获库，它由两部分组成：

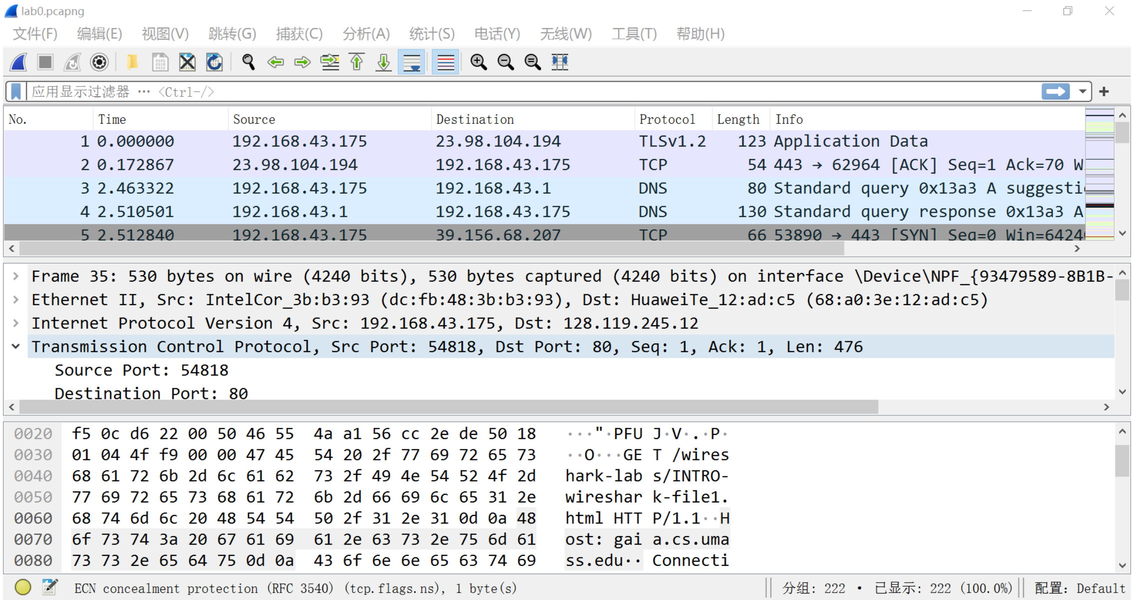
捕获库接收从计算机发送或接收的每个链路层帧的副本；

数据包分析仪在协议消息中显示所有字段的内容。

三.实验步骤

1. 下载并安装wireshark。
2. 启动wireshark并开始抓包。

   wireshark界面如下图所示：



```
No.     Time        Source            Destination       Protocol  Length Info
      1 0.000000    192.168.43.175    23.98.104.194     TLSv1.2     123 Application Data
      2 0.172867    23.98.104.194     192.168.43.175    TCP          54 443 → 62964 [ACK] Seq=1 Ack=70 W
      3 2.463322    192.168.43.175    192.168.43.1      DNS          80 Standard query 0x13a3 A suggesti
      4 2.510501    192.168.43.1      192.168.43.175    DNS         130 Standard query response 0x13a3 A
      5 2.512840    192.168.43.175    39.156.68.207     TCP          66 53890 → 443 [SYN] Seq=0 Win=6424
```

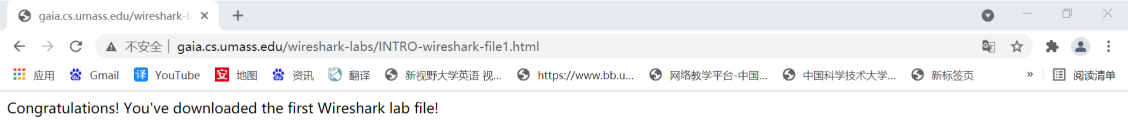
```
> Frame 35: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface \Device\NPF_{93479589-8B1B-
> Ethernet II, Src: IntelCor_3b:b3:93 (dc:fb:48:3b:b3:93), Dst: HuaweiTe_12:ad:c5 (68:a0:3e:12:ad:c5)
> Internet Protocol Version 4, Src: 192.168.43.175, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 54818, Dst Port: 80, Seq: 1, Ack: 1, Len: 476
    Source Port: 54818
    Destination Port: 80
```

```
0020  f5 0c d6 22 00 50 46 55  4a a1 56 cc 2e de 50 18   ···"·PFU J·V·.·P·
0030  01 04 4f f9 00 00 47 45  54 20 2f 77 69 72 65 73   ··O···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63 74 69   ss.edu·· Connecti
```

ECN concealment protection (RFC 3540) (tcp.flags.ns), 1 byte(s) ‖ 分组: 222 · 已显示: 222 (100.0%) ‖ 配置: Default

3. 当Wireshark运行时，输入URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html，并在浏览器中显示该页面。
4. 在浏览器中显示了"introduction - Wireshark -file1.html"页面后，在抓包窗口中选择"stop"停止抓包。

   页面如下图所示：

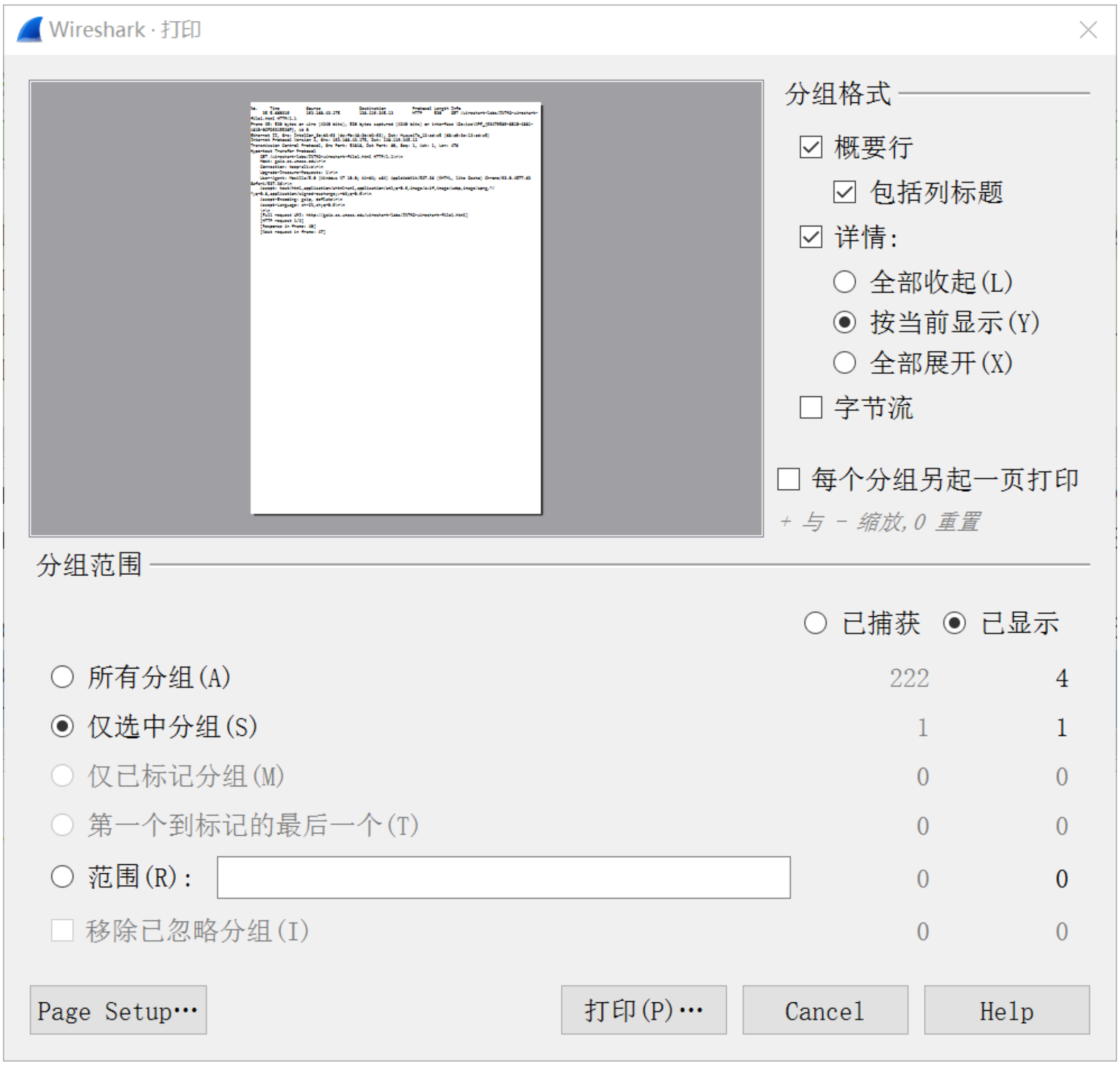


Congratulations! You've downloaded the first Wireshark lab file!

5. 在Wireshark主窗口顶部的显示过滤器规范窗口中输入“http”，使列表窗口中只显示HTTP消息。

6. 找到从计算机发送到gaia.cs.umass.edu HTTP服务器的HTTP GET消息。点击包详细信息窗口左侧的“+”和“-”向右和向下箭头，最小化显示的帧、以太网、Internet协议和传输控制协议信息的数量。最大化显示HTTP协议的信息量。

   打印HTTP消息时界面如下图:



Wireshark · 打印

分组格式

☑ 概要行

☑ 包括列标题

☑ 详情:

○ 全部收起(L)

● 按当前显示(Y)

○ 全部展开(X)

□ 字节流

□ 每个分组另起一页打印

+ 与 − 缩放，0 重置

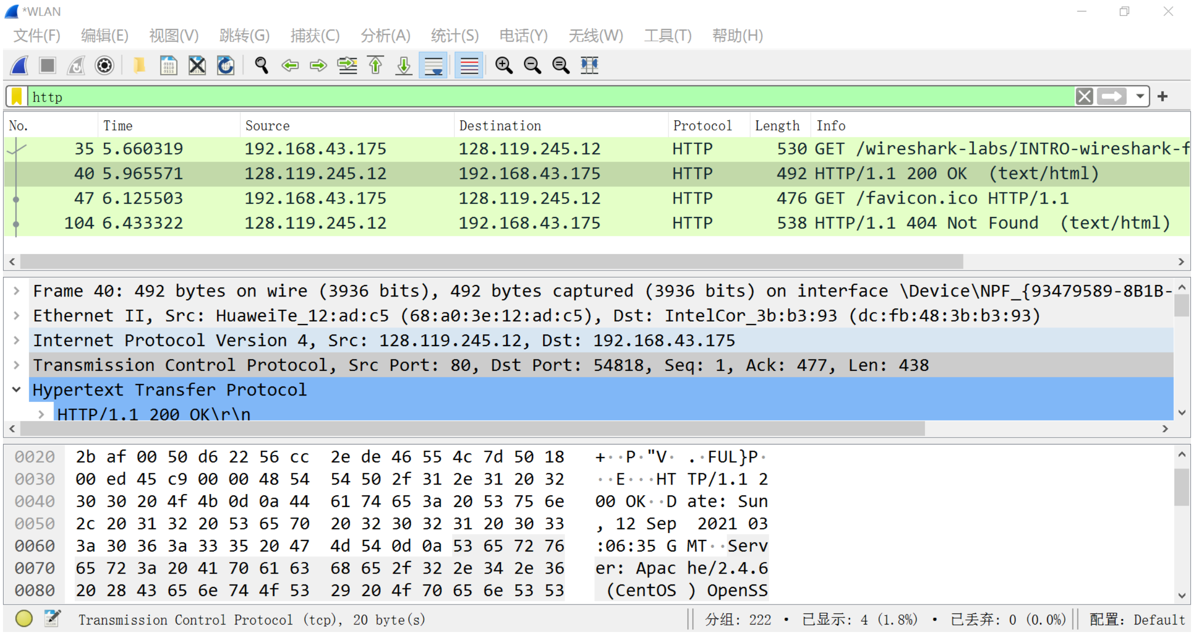
分组范围

	○ 已捕获	● 已显示
○ 所有分组(A)	222	4
● 仅选中分组(S)	1	1
○ 仅已标记分组(M)	0	0
○ 第一个到标记的最后一个(T)	0	0
○ 范围(R):	0	0
□ 移除已忽略分组(I)	0	0

7. 退出Wireshark。

四.实验结果

抓包并筛选后结果如图所示：


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
http
```

```
No.    Time        Source           Destination      Protocol  Length  Info
  35 5.660319      192.168.43.175   128.119.245.12   HTTP        530 GET /wireshark-labs/INTRO-wireshark-f
  40 5.965571      128.119.245.12   192.168.43.175   HTTP        492 HTTP/1.1 200 OK  (text/html)
  47 6.125503      192.168.43.175   128.119.245.12   HTTP        476 GET /favicon.ico HTTP/1.1
 104 6.433322      128.119.245.12   192.168.43.175   HTTP        538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 40: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{93479589-8B1B-
> Ethernet II, Src: HuaweiTe_12:ad:c5 (68:a0:3e:12:ad:c5), Dst: IntelCor_3b:b3:93 (dc:fb:48:3b:b3:93)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.43.175
> Transmission Control Protocol, Src Port: 80, Dst Port: 54818, Seq: 1, Ack: 477, Len: 438
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
```

```
0020  2b af 00 50 d6 22 56 cc  2e de 46 55 4c 7d 50 18   +··P·"V· .·FUL}P·
0030  00 ed 45 c9 00 00 48 54  54 50 2f 31 2e 31 20 32   ··E···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 75 6e   00 OK··D ate: Sun
0050  2c 20 31 32 20 53 65 70  20 32 30 32 31 20 30 33   , 12 Sep  2021 03
0060  3a 30 36 3a 33 35 20 47  4d 54 0d 0a 53 65 72 76   :06:35 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
```

```
Transmission Control Protocol (tcp), 20 byte(s)    分组: 222 · 已显示: 4 (1.8%) · 已丢弃: 0 (0.0%)    配置: Default
```

1. 列出上面第7步未过滤的包列表窗口中的协议列中出现的3个不同的协议。

答：所求协议如下表所示：

No	Time	Source	Destination	Protocol	Length	Info
36	5.667218	128.119.245.12	192.168.43.175	TCP	66	80 → 51705 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM=1 WS=128
37	5.667342	192.168.43.175	128.119.245.12	TCP	54	51705 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
1	0.000000	192.168.43.175	23.98.104.194	TLSv1.2	123	Application Data

2.从发送HTTP GET消息到收到HTTP OK应答花了多长时间?

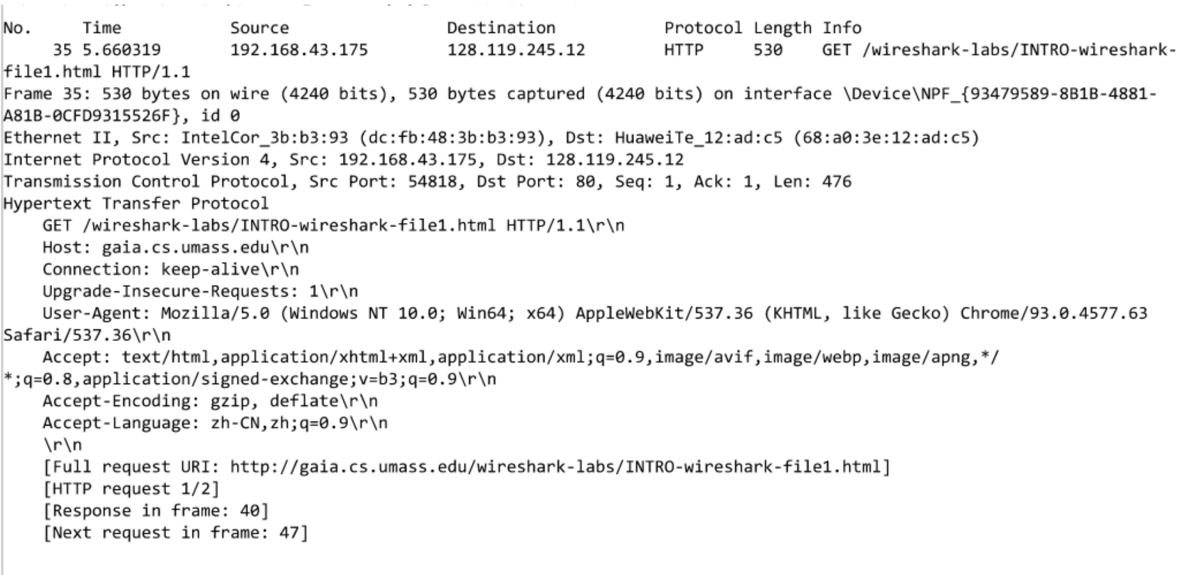
答：如上图所示，时间t=5.965571s-5.660319s=0.305252s

3.gaia.c.s.umass.edu的互联网地址是什么?你的电脑的互联网地址是什么?

答：如上图所示，gaia.c.s.umass.edu的ip地址为“128.119.245.12”，我的电脑ip地址为“192.168.43.175”。

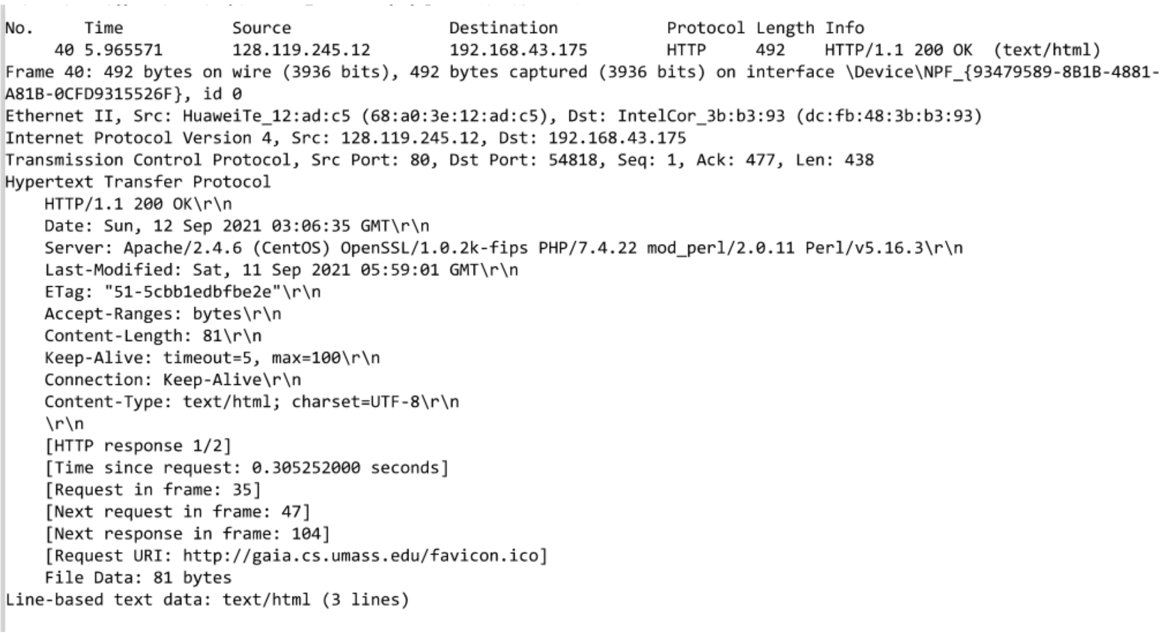
4.打印上面问题2中提到的两个HTTP消息(GET和OK).

答：将GET消息打印成pdf后如下图所示：



```
No.     Time           Source                Destination           Protocol Length Info
     35 5.660319       192.168.43.175        128.119.245.12        HTTP     530    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 35: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface \Device\NPF_{93479589-8B1B-4881-
A81B-0CFD9315526F}, id 0
Ethernet II, Src: IntelCor_3b:b3:93 (dc:fb:48:3b:b3:93), Dst: HuaweiTe_12:ad:c5 (68:a0:3e:12:ad:c5)
Internet Protocol Version 4, Src: 192.168.43.175, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54818, Dst Port: 80, Seq: 1, Ack: 1, Len: 476
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
    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\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: zh-CN,zh;q=0.9\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: 40]
    [Next request in frame: 47]
```

OK消息打印成pdf后如下图所示：



```
No.     Time           Source                Destination           Protocol Length Info
     40 5.965571       128.119.245.12        192.168.43.175        HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 40: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{93479589-8B1B-4881-
A81B-0CFD9315526F}, id 0
Ethernet II, Src: HuaweiTe_12:ad:c5 (68:a0:3e:12:ad:c5), Dst: IntelCor_3b:b3:93 (dc:fb:48:3b:b3:93)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.43.175
Transmission Control Protocol, Src Port: 80, Dst Port: 54818, Seq: 1, Ack: 477, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sun, 12 Sep 2021 03:06:35 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 11 Sep 2021 05:59:01 GMT\r\n
    ETag: "51-5cbb1edbfbe2e"\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: 0.305252000 seconds]
    [Request in frame: 35]
    [Next request in frame: 47]
    [Next response in frame: 104]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

五.实验收获

1. 学习并了解了一些wireshark的入门操作，为后续实验打下了基础。
2. 深入理解了网络协议，在实践中学习了网络协议的“实际运行”。
3. 学习了嗅探器的结构，理解了wireshark的工作原理。