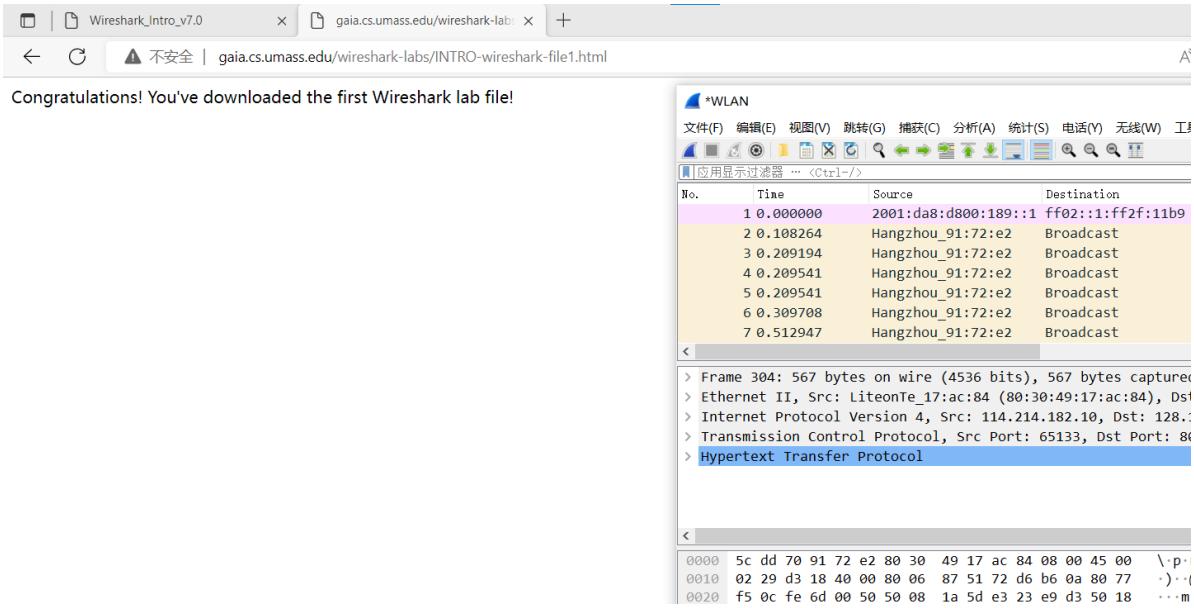
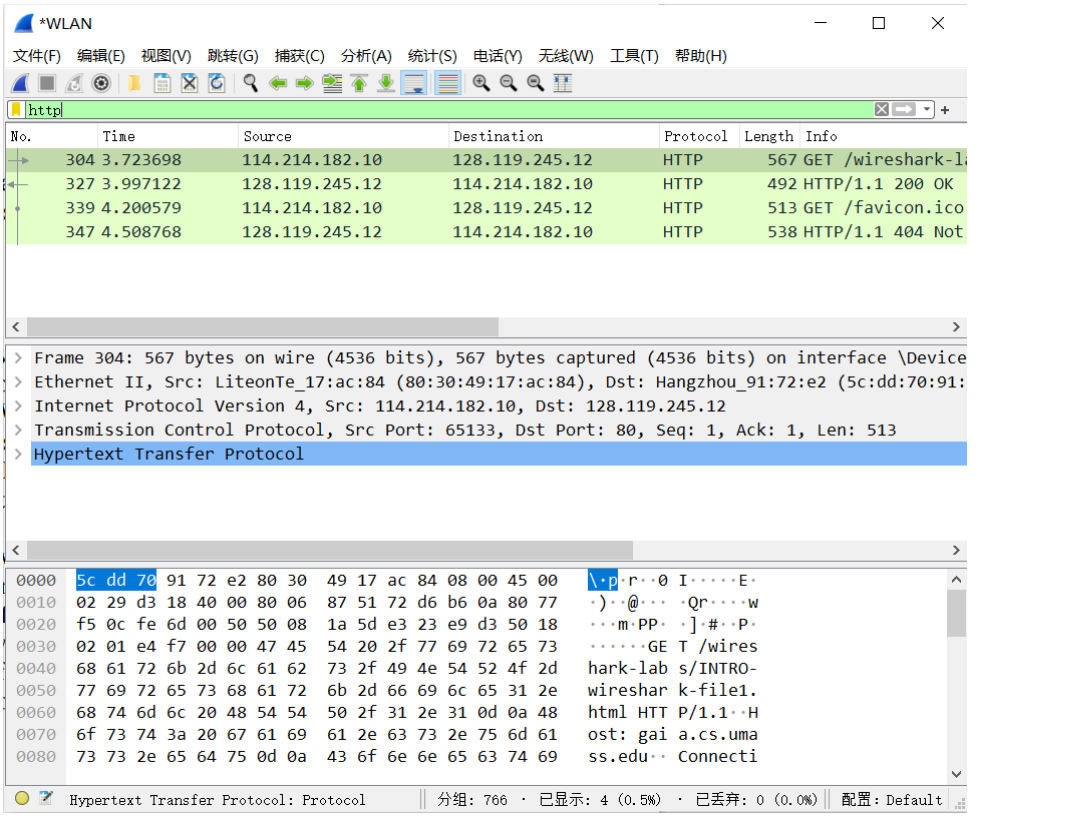
入门实验 实验报告

实验步骤

首先根据文档提示，先运行 Wireshark 软件，然后访问 gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html，就可以获取报文信息。



接着我们筛选出 HTTP 协议的报文信息：



然后就可以看到 HTTP GET 的报文信息：

```
> Frame 304: 567 bytes on wire (4536 bits), 567 bytes captured (4536 bits) on interface \Device\NPF_{78348DFD-6104-46FE-923D-EF83B9D90DB2}, id 0
> Ethernet II, Src: LiteonTe_17:ac:84 (80:30:49:17:ac:84), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 114.214.182.10, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 65133, Dst Port: 80, Seq: 1, Ack: 1, Len: 513
v Hypertext Transfer Protocol
  v 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/105.0.0.0 Safari/537.36 Edg/105.0.1343.27\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: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,en-GB;q=0.6\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: 327]
    [Next request in frame: 339]
```

实验问题

1. 实验过程中出现过 TCP, HTTP, ARP 这三种协议。

Time	Source	Destination	Protocol
3.722842	20.42.65.84	114.214.182.10	TCP
3.722842	128.119.245.12	114.214.182.10	TCP
3.722842	128.119.245.12	114.214.182.10	TCP
3.723090	114.214.182.10	128.119.245.12	TCP
3.723186	114.214.182.10	128.119.245.12	TCP
3.723698	114.214.182.10	128.119.245.12	HTTP
3.724246	20.42.65.84	114.214.182.10	TCP
3.724246	20.42.65.84	114.214.182.10	TCP
3.724246	20.42.65.84	114.214.182.10	TCP
3.724246	20.42.65.84	114.214.182.10	TCP
3.724246	20.42.65.84	114.214.182.10	TLSv1.2
3.724354	114.214.182.10	20.42.65.84	TCP
3.726625	Hangzhou_91:72:e2	Broadcast	ARP
3.736358	Hangzhou_91:72:e2	Broadcast	ARP
3.771644	40.90.184.73	114.214.182.10	TCP

2. 从上面筛选出 HTTP 协议报文信息的那张图片可以看到，HTTP GET 和 HTTP OK 信息之间的时间间隔为 $t = 3.997122s - 3.723698s = 0.273424s$

3. 通过筛选出 DNS 协议的报文信息，可以看到：

```
  223 3.169587 114.214.182.10  202.38.64.17    DNS      77 Standard query 0xafe9 A gaia.cs.umass.edu
  224 3.169589 114.214.182.10  202.38.64.17    DNS      77 Standard query 0xb254 AAAA gaia.cs.umass.edu
  282 3.500571 202.38.64.17    114.214.182.10  DNS      93 Standard query response 0xafe9 A gaia.cs.umass.edu A 128.119.245.12
  283 3.500571 202.38.64.17    114.214.182.10  DNS     130 Standard query response 0xb254 AAAA gaia.cs.umass.edu SOA unix1.cs.um
  286 3.517492 114.214.182.10  202.38.64.56    DNS      94 Standard query 0x3bbf A nav-edge.smartscreen.microsoft.com
```

```
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v gaia.cs.umass.edu: type A, class IN, addr 128.119.245.12
        Name: gaia.cs.umass.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 600 (10 minutes)
        Data length: 4
        Address: 128.119.245.12
    [Request In: 223]
    [Time: 0.330984000 seconds]
```

返回得到 http://gaia.cs.umass.edu 的 IP 地址为 128.119.245.12 。