实验报告

实验一 入门

Lab1 INTRO

罗晏宸
PB17000297
2019.9.7

实验目的

1. **入门Wireshark**
   熟悉Wireshark软件界面、功能，学习基本的分组捕获与分析方法，尝试阅读网络信息

实验内容

1. 列举捕获的分组中若干不同的网络协议

NBNS, DNS, UDP, SSL, SSDP, TCP, HTTP, WebSocket, TLSv1.2, TLSv1.3, ARP, ICMPv6, LLMNR, MDNS

2. 获取网络请求发出到接受的间隔时间

$$23:06:25.295585 - 23:06:24.993846 = 0.301739s$$

3. 获取本机与目标站点的网络地址

- 目标站点 Host: pixel.fonexsoftware.com:1453

- 本机 Origin: chrome-extension://npmleadjnlojpinmkhnepddhlplealpg

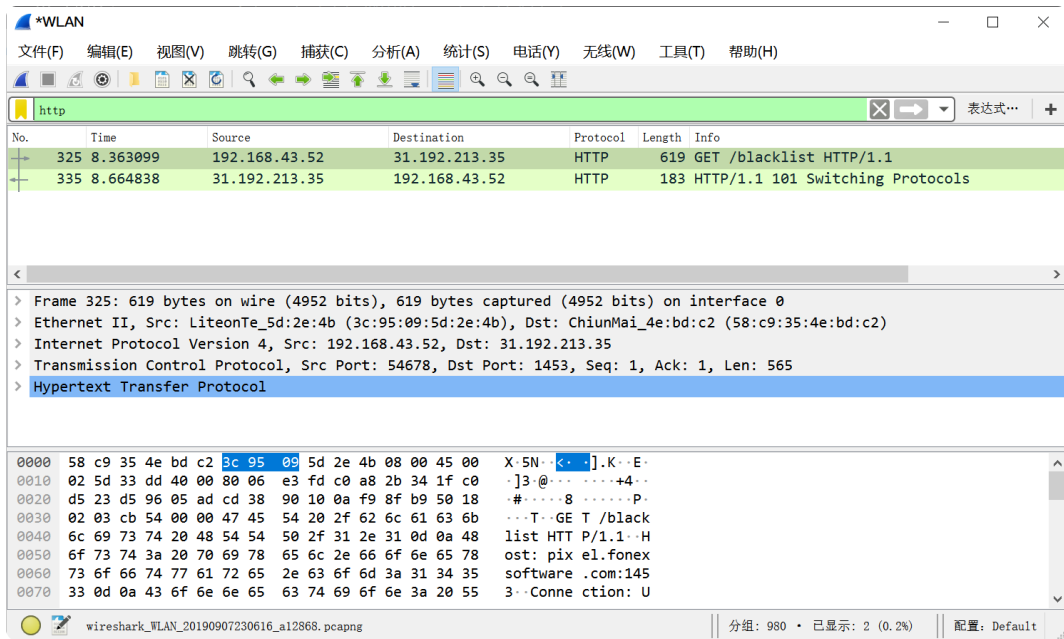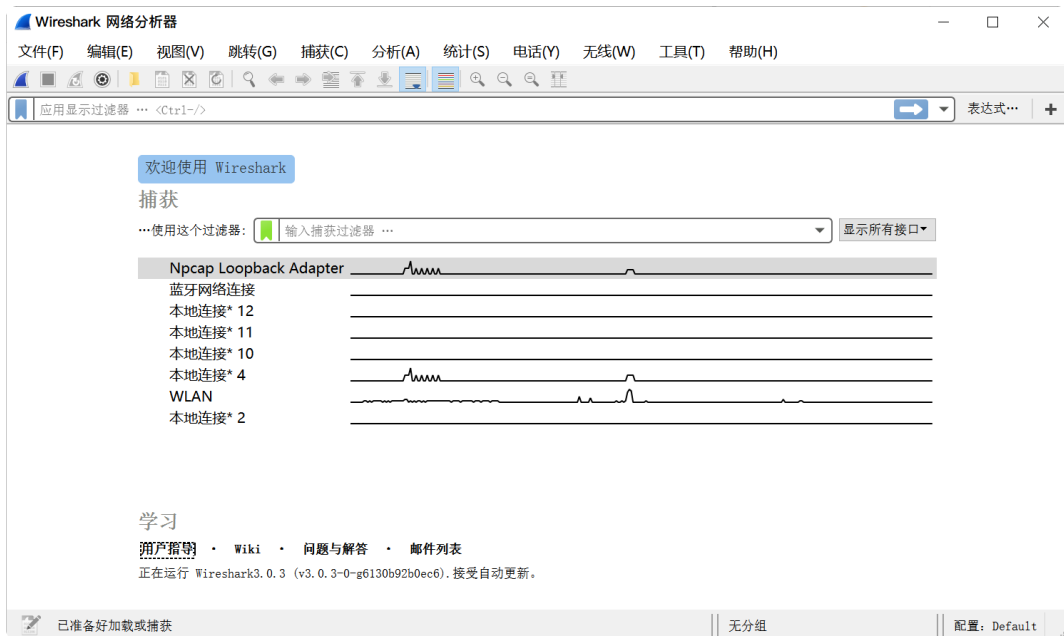### 4. 打印输出捕获结果

```
No.     Time          Source               Destination         Protocol Length Info
    325 23:06:24.993846  192.168.43.52        31.192.213.35       HTTP     619    GET /blackli
HTTP/1.1
Frame 325: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface 0
Ethernet II, Src: LiteonTe_5d:2e:4b (3c:95:09:5d:2e:4b), Dst: ChiunMai_4e:bd:c2 (58:c9:35:4e:bd:c2)
Internet Protocol Version 4, Src: 192.168.43.52, Dst: 31.192.213.35
Transmission Control Protocol, Src Port: 54678, Dst Port: 1453, Seq: 1, Ack: 1, Len: 565
Hypertext Transfer Protocol
    GET /blacklist HTTP/1.1\r\n
    Host: pixel.fonexsoftware.com:1453\r\n
    Connection: Upgrade\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
76.0.3809.132 Safari/537.36\r\n
    Upgrade: websocket\r\n
    Origin: chrome-extension://npmleadjnlojpinmkhnepddhlplealpg\r\n
    Sec-WebSocket-Version: 13\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
    Sec-WebSocket-Key: 0tEcDnOLs1oQUuXwnj76ng==\r\n
    Sec-WebSocket-Extensions: permessage-deflate; client_max_window_bits\r\n
    \r\n
    [Full request URI: http://pixel.fonexsoftware.com:1453/blacklist]
    [HTTP request 1/1]
    [Response in frame: 335]
```
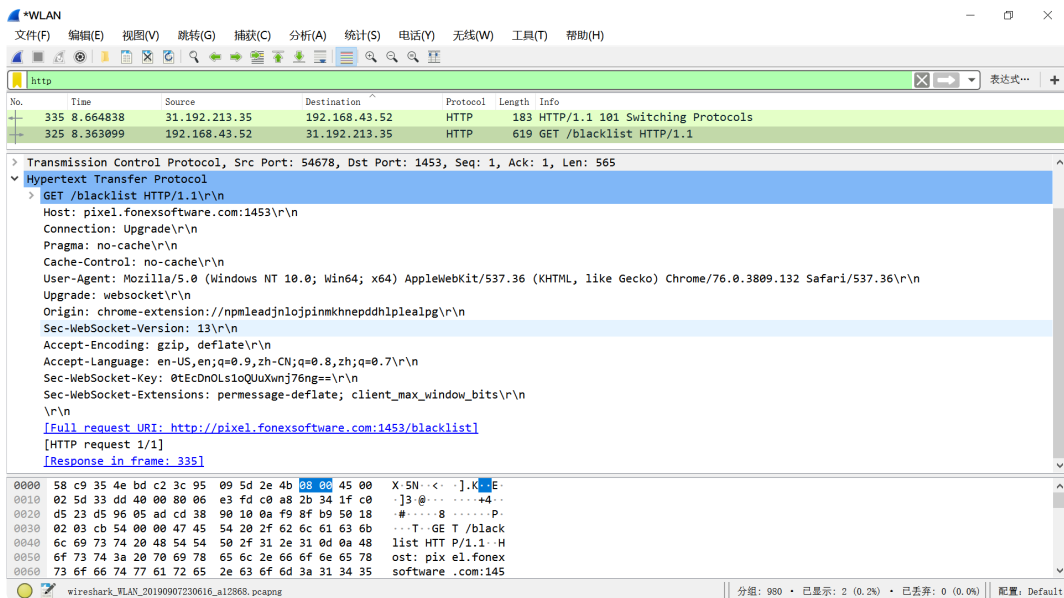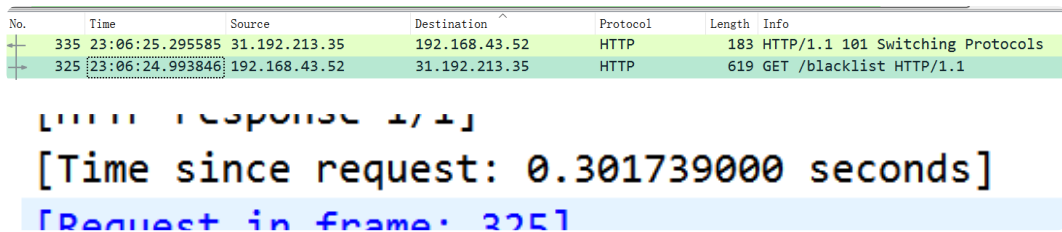
实验截图

1. 软件界面

2. 按协议过滤

3. 查看分组细节

4. 查看请求与接受间隔

实验总结

    作为本学期计算机网络课程的第一次观察实验，通过对于Wireshark软件的尝试与摸索，掌握了其基本功能及部分使用方法，包括捕获分组、查看分组头部细节、打印输出捕获结果等。进一步地，通过一个简单HTTP协议的例子，观察了实际分组的细节，回顾了已学习的相关知识。经过本次入门实验，引入了本学期观察实验的重要工具Wireshark，为今后的实验学习与实践提供了背景与工具。

附

    本报告中出现的所有设计与测试源代码文件以及相关截图与照片可见
GitHub@lyc0930