《网络与通信》课程实验报告

实验三：数据包结构分析

姓名	汪江豪	院系	计算机学院	学号	22121630
任课教师	何冰		指导教师	何冰	
实验地点	计算机楼 708		实验时间	周三 7-8	
实验课表现	出勤、表现得分(10)		实验报告得分(40)		实验总分	
	操作结果得分(50)					

实验目的：

1. 了解 Sniffer 的工作原理，掌握 Sniffer 抓包、记录和分析数据包的方法；
2. 在这个实验中，你将使用抓包软件捕获数据包，并通过数据包分析每一层协议。

实验内容：

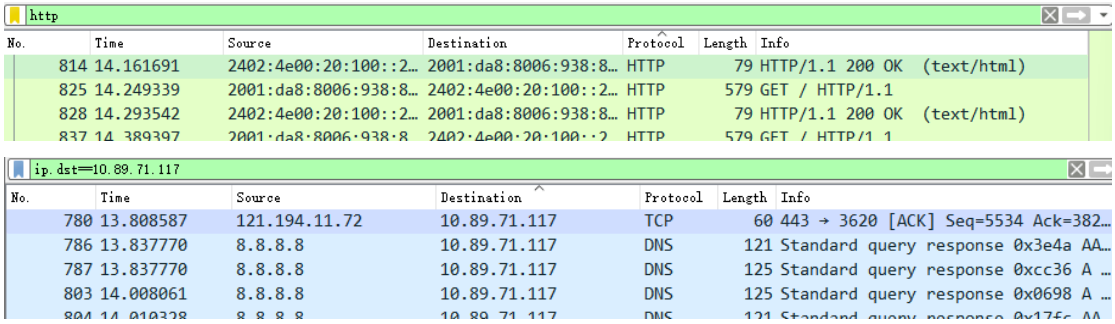
使用抓包软件捕获数据包，并通过数据包分析每一层协议。

实验要求：（学生对预习要求的回答）（10 分）　　得分：

- 常用的抓包工具
- 1.wireshark一款网络协议分析器。用于网络调试、分析、软件和通信协议开发。Wireshark可以捕获运行在本地计算机上的网络接口上的数据包，并提供实时分析。
- 2.sniffer一款网管和应用故障诊断分析软件。能进行实时的网络监视、数据包捕获以及故障诊断分析能力。
- 3.Tcpdump一个命令行数据包捕获工具，广泛用于unix-like系统。

实验过程中遇到的问题如何解决的？（10 分）　　得分：

问题 1：使用 wireshark 进行抓包的时候，如何从成千上万的数据包中抓到自己想要的数据包？



答：我们可以从上方导航栏输入相应的关键字，来检索我们想要的数据包，如网页内容相关，输入 http，发送到本机 ip 相关的数据包，输入 ip.dst==[本地 ip]。

问题 2：当我在捕获分组时，打开一个网页成功后，却看不到相关的数据包？

答：搜不到相关的数据包，第一次导航栏搜索的关键词有误。第二次原因可能是访问的网页内容在之前已经被浏览器缓存了，浏览器可能不会发送新的 http 请求来获取数据，因此 wireshark 无法捕获到新的数据包。

问题 3：抓取数据包的过程中，为什么能抓取 http 协议的网页内容，不能抓取 https 协议的

网页内容？

答：HTTP 时，数据以明文形式传输，在网络中可以被任何拥有网络访问点的人轻易截获和查看。HTTPS 是 HTTP 的安全版本，在客户端和服务器之间 通信过程中 加入 了 SSL/TLS 加密层，数据包即使被截获，也无法直接解读数据内容。

本次实验的体会（结论）（10 分） 得分：

本次使用 wireshark 进行数据包抓包实验，不仅加深了我对于网络协议的理解，还提高了我的实际操作能力。实验中，我直观地观察到各种网络协议的实际运作情况，包括 TCP,UDP,IP 等核心协议，在课堂上学习理论知识时，可能比较抽象，但通过 wireshark 的实时数据流分析，我能够看到每个数据包的具体信息，让我更好理解了协议规范和网络数据的流动。本次实验也让我认识到了网络安全的重要性，网络数据在传输过程中是可以被截获和查看的，需要注重加密和安全措施。

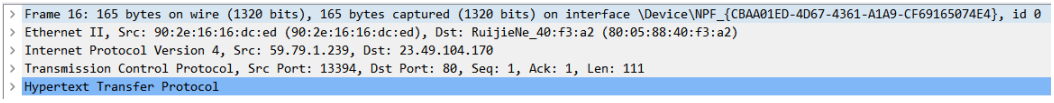
总之，本次实验让我加深了对网络分层的理解，学会了如何查看数据包的相关信息，让我受益匪浅。

10.89.71.117

思考题：（10 分）

思考题 1：（4 分） 得分：

写出捕获的数据包格式。



Frame：物理层的数据帧信息

Ethernet II：数据链路层以太网帧信息，ethernet II 表示以太网协议版本；Src 显示了源网卡的厂名_序号和物理地址；Dst 显示了目标网卡的相关信息；

Internet Protocol Version 4:表示了网络层 IP 数据报头部信息，包括 IP 协议版本，源 IP 地址，目标 IP 地址。

Transmission Control Protocol：传输层 TCP 头部。

Hypertext Transfer Protocol:应用层协议，此处是超文本传输协议，也即 http 协议。

思考题2：（6分） 得分：

写出实验过程并分析实验结果。

以登录上海大学统一身份认证平台为例：

首先开始捕获分组，然后在浏览器中打开上海大学统一身份认证平台登录，等页面加载成功后，停止捕获分组。在wireshark搜索栏输入http，可发现如下数据包：

```
4187 9.333911    59.79.1.239      140.210.69.130   HTTP    498 GET /sso/shu HTTP/1.1
4191 9.366191    140.210.69.130   59.79.1.239      HTTP    710 HTTP/1.1 302
```

一个是本地ip发向目的ip的请求，一个是目的ip发向本地ip的回应。打开第二个数据包：

```
Frame 4191: 710 bytes on wire (5680 bits), 710 bytes captured (5680 bits) on interface \Device\NPF_{CBAA01ED-4D67-4361-A1A9-CF69165074E4}, id 0
  Interface id: 0 (\Device\NPF_{CBAA01ED-4D67-4361-A1A9-CF69165074E4})
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 11, 2024 19:40:53.950756000 中国标准时间
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1726054853.950756000 seconds
  [Time delta from previous captured frame: 0.005388000 seconds]
  [Time delta from previous displayed frame: 0.032280000 seconds]
  [Time since reference or first frame: 9.366191000 seconds]
  Frame Number: 4191
  Frame Length: 710 bytes (5680 bits)
  Capture Length: 710 bytes (5680 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
```

以上是物理层，从第一行往下依次为：

接口编号为0，后面为网卡具体参数；

封装类型为以太网帧；

捕获时间为2024年9月11日19点40分53秒；

与前一包间隔时间；

信息出现时间；

与上一次被捕获帧的时间间隔；

与上一次显示帧的时间间隔；

与参考帧或第一帧的时间间隔；

帧号；

帧长为710字节；

捕获长度为710字节等。

```
Ethernet II, Src: RuijieNe_40:f3:a2 (80:05:88:40:f3:a2), Dst: 90:2e:16:16:dc:ed (90:2e:16:16:dc:ed)
  Destination: 90:2e:16:16:dc:ed (90:2e:16:16:dc:ed)
  Source: RuijieNe_40:f3:a2 (80:05:88:40:f3:a2)
  Type: IPv4 (0x0800)
```

以上是数据链路层，展示了源mac地址和目的mac地址Type:IPv4(0x0800)表示帧内封装的上层协议类型为IPv4，并在括号内显示了IP的十六进制码。

```
Internet Protocol Version 4, Src: 140.210.69.130, Dst: 59.79.1.239
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 696
  Identification: 0xa073 (41075)
  Flags: 0x4000, Don't fragment
  Fragment offset: 0
  Time to live: 49
  Protocol: TCP (6)
  Header checksum: 0x973a [validation disabled]
  [Header checksum status: Unverified]
  Source: 140.210.69.130
  Destination: 59.79.1.239
```

以上是网络层IP数据报头部信息，从上到下依次是：

IP协议版本；

IP报头长度；

区别服务域；

IP数据报总长度；

标示字段；

标记字段；

分段偏移量；

数据报有效存活时间；

数据报封装的上层协议为TCP；

首部检验和0x973a确认不可用；

源ip地址；

目标ip地址；

```
Transmission Control Protocol, Src Port: 80, Dst Port: 3808, Seq: 1, Ack: 445, Len: 656
    Source Port: 80
    Destination Port: 3808
    [Stream index: 153]
    [TCP Segment Len: 656]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 3145485689
    [Next sequence number: 657    (relative sequence number)]
    Acknowledgment number: 445    (relative ack number)
    Acknowledgment number (raw): 4247100562
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 60
    [Calculated window size: 30720]
    [Window size scaling factor: 512]
    Checksum: 0x9d67 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (656 bytes)
```

以上为传输层，传输控制协议，源端口80，目标端口3808，流端口号153，封包相对序号1，确认号445，window size value：窗口字段，控制对方发送的数据量等等。

```
Hypertext Transfer Protocol
 > HTTP/1.1 302 \r\n
   Date: Wed, 11 Sep 2024 11:40:57 GMT\r\n
 > Content-Length: 0\r\n
   Connection: keep-alive\r\n
   Set-Cookie: INGRESSCOOKIE=1726054859.593.65391.345023; Expires=Fri, 13-Sep-24 11:40:58 GMT; Max-Age=172800; Path=/; HttpOnly\r\n
   Rose: fanya-ssoboot-1\r\n
   Set-Cookie: jrose=D2858D7AF097481718F52C9AEC884C73.fanya-ssoboot-1; Path=/; HttpOnly\r\n
   Location: https://oauth.shu.edu.cn/oauth/authorize?response_type=code&scope=1&client_id=P3WnKUneBMDRwskNeO8wgo7b&redirect_uri=http%3A%2F%2Fshu.fysso.chaoxing.com%2Fsso%2Fshu\r\n
   upstreamdocker: 172.30.19.8:7085\r\n
   Set-Cookie: route=4b226ffea725727ea05ead170662c3b5; Path=/\r\n
   Origin-Agent-Cluster: ?0\r\n
   X-Frame-Options: SAMEORIGIN\r\n
   \r\n
   [HTTP response 1/2]
   [Time since request: 0.032280000 seconds]
   [Request in frame: 4187]
   [Next request in frame: 5616]
   [Next response in frame: 5622]
   [Request URI: http://shu.fysso.chaoxing.com/sso/shu]
```

以上为应用层内容，302为状态码，表示客户端请求的页面已经转移到另一个位置。该码通常用于重定向，告诉浏览器应该访问另一个URL以获取请求的资源。访问的网址的统一资源标识符(uniform resource identifier: URI)为：http://shu.fysso.chaoxing.com/sso/shu.

指导教师评语：

日期：