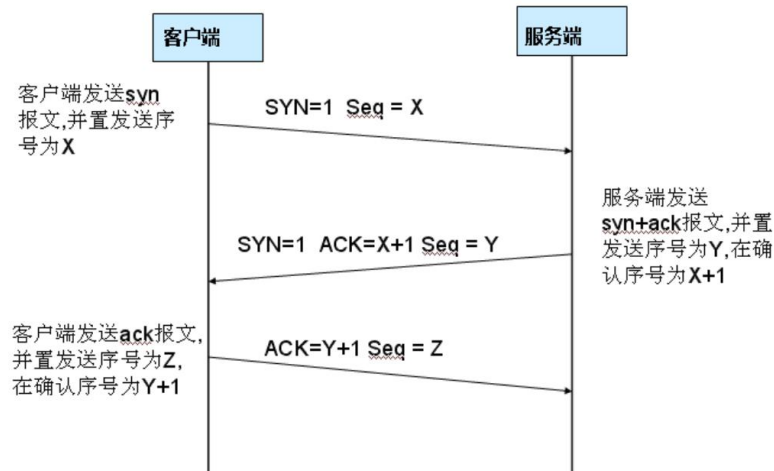


《网络与通信》课程实验报告

实验三：数据包结构分析

姓名	李昀哲	院系	计算机学院	学号	20123101
任课教师	刘通	指导教师	刘通		
实验地点	计 708	实验时间	2022.10.14		
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：
<ul style="list-style-type: none">● 常用的抓包工具 Fiddler 抓包工具、Charles 抓包工具、Firebug 抓包工具、httpwatch 抓包工具、Wireshark 抓包工具、SmartSniff 抓包工具。					
实验过程中遇到的问题如何解决的？（10 分）					得分：
<p>问题 1：不明确软件的使用过程和方法 结合 WireShark 官方 Document 以及课上所学知识，逐步上手尝试熟悉使用</p> <p>问题 2：不清楚如何筛选出自己想要的抓取到的数据包 使用软件中的“过滤语法”，具体语法包括：</p> <ol style="list-style-type: none">1. 比较操作符，如==, !=, >, <等；2. 协议过滤，如：tcp, http, icmp 等；3. Ip 过滤，如：ip.src ==, ip.dst ==, ip.addr ==4. 端口过滤，如 tcp.port, tcp.srcport, tcp.dstport; <p>问题 3：文档中提到的 TCP 三次握手并不了解（可能后续会学），这里简要了解了一下</p> <p>Step1: 客户端发送一个 SYN=1, ACK=0 标志的数据包给服务端，请求进行连接，这是第一次握手；</p> <p>Step2: 服务端收到请求并且允许连接的话，就会发送一个 SYN=1, ACK=1 标志的数据包给发送端，告诉它，可以通讯了，并且让客户端发送一个确认数据包，这是第二次握手；</p> <p>Step3: 服务端发送一个 SYN=0, ACK=1 的数据包给客户端，告诉它连接已被确认，这就是第三次握手。TCP 连接建立，开始通讯。</p>					

TCP 三次握手



本次实验的体会（结论）（10 分）

得分：

本次实验中了解了 wireshark 的工作原理，掌握 wireshark 抓包、记录和分析数据包的方法，通过软件的使用，对各个层次有了更清晰的了解，也对数据包中各层协议的格式有了直观的认识，为理论课的学习增添了实践的尝试。同时在学习软件过程中，了解到了 TCP 三次握手，也通过网络进行了检索和学习。

思考题：（10 分）

思考题 1：（4 分）

得分：

写出捕获的数据包格式。
选择其中一例进行分析：

67	20.773772	20.198.162.78	192.168.5.15	TLSv1.2	225 Application Data
68	20.824026	192.168.5.15	20.198.162.78	TCP	54 61305 → 443 [ACK] Seq=102 Ack=172 Win=512 Len=0

> Frame 67: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface \Device\NPF_{8EFB13B7-9754-4178-BA9E-C06A1534A7D0}, id 0
> Ethernet II, Src: Tp-LinkT_18:38:6b (80:ea:07:18:38:6b), Dst: IntelCor_da:62:bd (c8:b2:9b:da:62:bd)
> Internet Protocol Version 4, Src: 20.198.162.78, Dst: 192.168.5.15
> Transmission Control Protocol, Src Port: 443, Dst Port: 61305, Seq: 1, Ack: 102, Len: 171
> Transport Layer Security

总览：

Frame:物理层的数据帧概况；

Ethernet II：数据链路层以太网帧头部信息；

Internet Protocol Version 4：网络层IP包头部信息；

Transmission Control Protocol：运输层数据段头部信息，此处是TCP协议；

Transport Layer Security：应用层信息，此处是TLS协议；

物理层数据帧概况：

```
▼ Frame 67: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface \Device\NPF_{8EFB13B7-9754-417B-8A9E-C06A1534A7D0}, id 0
  Section number: 1
  > Interface id: 0 (\Device\NPF_{8EFB13B7-9754-417B-8A9E-C06A1534A7D0})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 15, 2022 12:19:56.774395000 中国标准时间
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1665807596.774395000 seconds
    [Time delta from previous captured frame: 0.066447000 seconds]
    [Time delta from previous displayed frame: 0.066447000 seconds]
    [Time since reference or first frame: 20.773772000 seconds]
    Frame Number: 67
    Frame Length: 225 bytes (1800 bits)
    Capture Length: 225 bytes (1800 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
```

Interface id: 接口 ID

Encapsulation type: Ethernet (1): 封装类型

Arrival Time: 捕获日期和时间

Frame Number: 帧序号

Frame Length: 帧长度

Capture Length: 捕获长度

此外还有帧内封装的协议层、着色标记的协议名等信息。

数据链路层以太网帧头部信息：

```
▼ Ethernet II, Src: Tp-LinkT_18:38:6b (80:ea:07:18:38:6b), Dst: IntelCor_da:62:bd (c8:b2:9b:da:62:bd)
  > Destination: IntelCor_da:62:bd (c8:b2:9b:da:62:bd)
  > Source: Tp-LinkT_18:38:6b (80:ea:07:18:38:6b)
  Type: IPv4 (0x0800)
```

Destination: 目标 MAC 地址

Source: 源 MAC 地址

网络层 IP 包头部信息：

```
▼ Internet Protocol Version 4, Src: 20.198.162.78, Dst: 192.168.5.15
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 211
    Identification: 0x6631 (26161)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 113
    Protocol: TCP (6)
    Header Checksum: 0x2628 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 20.198.162.78
    Destination Address: 192.168.5.15
```

Differentiated Services Field: 差分服务字段

Identification: 标记字段

Header Length: IP 包头部长度

还包括生存期 TTL，标志字段，分的偏移量等信息

运输层数据段头部信息：

```
Transmission Control Protocol, Src Port: 443, Dst Port: 61305, Seq: 1, Ack: 102, Len: 171
  Source Port: 443
  Destination Port: 61305
  [Stream index: 8]
  [Conversation completeness: Incomplete (12)]
  [TCP Segment Len: 171]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 3300716602
  [Next Sequence Number: 172 (relative sequence number)]
  Acknowledgment Number: 102 (relative ack number)
  Acknowledgment number (raw): 1536318907
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
  Window: 7990
  [Calculated window size: 7990]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x0a60 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
  TCP payload (171 bytes)
```

Source Port: 源端口

Destination Port: 目标端口

Stream Index: 流序号

Sequence Number: 序列号

还包括头部长度的、TCP 数据段校验、流量控制、确认序列号等信息。

应用层信息：

```
Transport Layer Security
  > TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
```

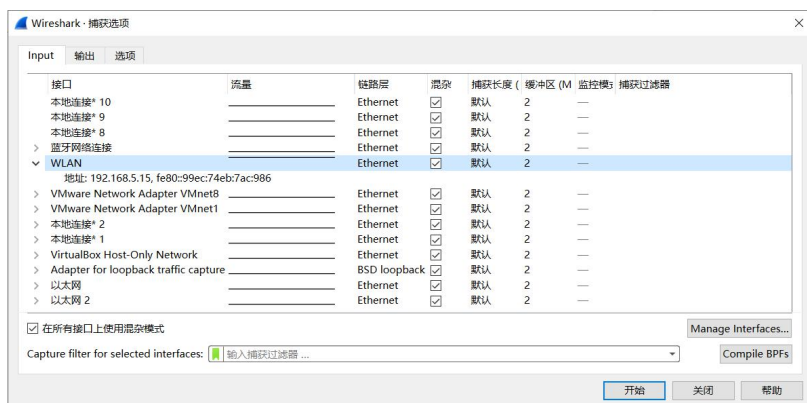
思考题2：（6分）

得分：

写出实验过程并分析实验结果。

1. 安装Wireshark抓包工具；

2. 打开后在“捕获” - “选项”中选择需要监视的网卡。这里我选择WLAN，点击开始后，wireshark启动且处于抓包状态；



选择捕获选项

正在捕获 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(I) 帮助(H)

应用显示过滤器: <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
23	6.496218	Tp-LinkT_18:38:6b	IntelCor_da:62:bd	ARP	60	192.168.5.15 → 192.168.5.1
24	10.000966	192.168.5.15	180.101.49.11	TCP	54	62054 → 443 [RST] Seq=192168515 Win=0 Len=0
25	10.390809	192.168.5.15	180.101.49.11	TCP	54	[TCP Retransmission] Seq=62054 → 443
26	11.047054	192.168.5.15	180.101.49.11	TCP	66	62056 → 443 [RST] Seq=192168515 Win=0 Len=0
27	11.058962	180.101.49.11	192.168.5.15	TCP	66	443 → 62056 [RST] Seq=192168515 Win=0 Len=0
28	11.059086	192.168.5.15	180.101.49.11	TCP	54	62056 → 443 [RST] Seq=192168515 Win=0 Len=0
29	11.059370	192.168.5.15	180.101.49.11	TCP	54	62056 → 443 [RST] Seq=192168515 Win=0 Len=0
30	11.359114	192.168.5.15	180.101.49.11	TCP	54	[TCP Retransmission] Seq=62056 → 443
31	11.969165	192.168.5.15	180.101.49.11	TCP	54	[TCP Retransmission] Seq=62056 → 443

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{8EFB13B7-9754-417B-BA9E-C06A1534A7D0}, id 0

> Ethernet II, Src: IntelCor_da:62:bd (c8:b2:9b:da:62:bd), Dst: 192.168.5.15 (08:00:2b:4c:00:00), id 0

> Internet Protocol Version 4, Src: 192.168.5.15, Dst: 180.101.49.11

> Transmission Control Protocol, Src Port: 62056, Dst Port: 443, Seq: 62056, Len: 54

处于抓包状态的wireshark

3. 执行需要抓包的的操作，试一下ping百度，即在cmd中：ping www.baidu.com 可以看到源主机IP为180.101.49.12，就可以在wireshark中过滤出对应的数据包；

```
C:\Users\16690>ping www.baidu.com

正在 Ping www.a.shifen.com [180.101.49.12] 具有 32 字节的数据:
来自 180.101.49.12 的回复: 字节=32 时间=15ms TTL=52
来自 180.101.49.12 的回复: 字节=32 时间=12ms TTL=52
来自 180.101.49.12 的回复: 字节=32 时间=21ms TTL=52
来自 180.101.49.12 的回复: 字节=32 时间=11ms TTL=52

180.101.49.12 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 11ms, 最长 = 21ms, 平均 = 14ms
```

Ping命令连通网络

4. 在wireshark中设置过滤条件，得到所需的数据包；

ip.addr == 180.101.49.12 and icmp

No.	Time	Source	Destination	Protocol	Length	Info
1327	194.298544	192.168.5.15	180.101.49.12	ICMP	74	Echo (ping)
1328	194.314212	180.101.49.12	192.168.5.15	ICMP	74	Echo (ping)
1329	195.312710	192.168.5.15	180.101.49.12	ICMP	74	Echo (ping)
1330	195.324911	180.101.49.12	192.168.5.15	ICMP	74	Echo (ping)
1332	196.329269	192.168.5.15	180.101.49.12	ICMP	74	Echo (ping)
1333	196.350159	180.101.49.12	192.168.5.15	ICMP	74	Echo (ping)
1339	197.343951	192.168.5.15	180.101.49.12	ICMP	74	Echo (ping)
1340	197.355405	180.101.49.12	192.168.5.15	ICMP	74	Echo (ping)

过滤所需的数据包

5. 数据包详细信息部分

67	20.773772	20.198.162.78	192.168.5.15	TLSv1.2	225	Application Data
68	20.824026	192.168.5.15	20.198.162.78	TCP	54	61305 → 443 [ACK] Seq=102 Ack=172 Win=512 Len=0

> Frame 67: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface \Device\NPF_{8EFB13B7-9754-417B-BA9E-C06A1534A7D0}, id 0

> Ethernet II, Src: Tp-LinkT_18:38:6b (80:ea:07:18:38:6b), Dst: IntelCor_da:62:bd (c8:b2:9b:da:62:bd)

> Internet Protocol Version 4, Src: 20.198.162.78, Dst: 192.168.5.15

> Transmission Control Protocol, Src Port: 443, Dst Port: 61305, Seq: 1, Ack: 102, Len: 171

> Transport Layer Security

数据包详细信息

Frame:物理层的数据帧概况；

Ethernet II: 数据链路层以太网帧头部信息；

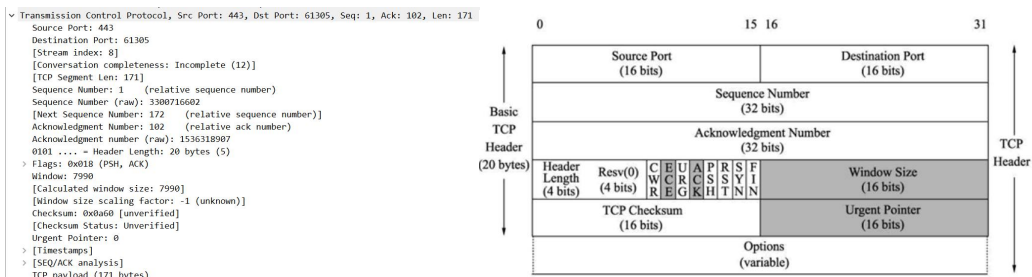
Internet Protocol Version 4: 网络层IP包头部信息；

Transmission Control Protocol: 运输层数据段头部信息；

Transport Layer Security: 应用层

6. TCP包中的具体内容

根据TCP的报文格式，可以在所获的TCP包中一一对应；



7. 分组字节流

从分组字节流中，可以找到对应的信息，以上述TCP中Source Port为例，对应了16字节的信息；

> Frame 67: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface \Device	0000	c8 b2 9b da 62 bd 80 ea 07 18 38 6b 08 00 45 00b....Bk-E-
> Ethernet II, Src: Tp-LinkT_18:38:6b (80:ea:07:18:38:6b), Dst: IntelCor_da:62:bd (c8:b2:9b:da)	0010	00 d3 66 31 40 00 71 06 26 28 14 c6 a2 4e c0 a8	..fig-q: 8(---N-
> Internet Protocol Version 4, Src: 20.198.162.78, Dst: 192.168.5.15	0020	05 9f 70 03 ef 79 c4 bc f0 3a 56 92 5d b6 50 18	..y...:[]-P-
> Transmission Control Protocol, Src Port: 443, Dst Port: 61305, Seq: 1, Ack: 102, Len: 171	0030	1f 36 0a 60 00 00 17 03 03 00 a5 00 00 00 00 00	..6.....
Source Port: 443	0040	00 00 20 a5 5b e5 1d 24 6c 91 13 a0 c8 7e a4 bc	...[]-\$ 1.....
Destination Port: 61305	0050	6b ec d5 6e 5c 7b 63 d6 3d 0d b8 5e d4 48 8e d7	k-m\(\c...^H-
[Stream index: 8]	0060	20 63 48 1f 36 a6 4c 5c 18 2c 97 09 08 1f e9 d5	..7x-KR...g...-
[Conversation completeness: Incomplete (12)]	0070	83 09 37 78 e0 cd 4b 52 ec da 67 e3 e2 3d f5 e4	...L]I...s...-
[TCP Segment Len: 171]	0080	a0 ed bd 4c c5 7d 49 05 b9 8e 8c 73 1e 3d 09 8c	...L]I...s...-
Sequence Number: 1 (relative sequence number)	0090	c8 ac 79 25 ef a9 5a 09 b9 f7 a2 d7 06 7b bc f0	..y%-Z.....
Sequence Number (raw): 3300716602	00a0	47 98 8d 5c 13 eb 20 a1 57 23 3d ca b4 d0 21 4b	G-\...-WM---IK
[Next Sequence Number: 172 (relative sequence number)]	00b0	71 21 89 5b 55 41 94 68 4d f4 cd f7 62 72 5f b4	q! [UA-h M---bE_
Acknowledgment Number: 102 (relative ack number)	00c0	82 2a 6d d4 35 a5 16 d6 b5 c0 c7 a3 8a fe f6 8a	*m-5.....
Acknowledgment number (raw): 1536318907	00d0	1c ec cb 00 74 ae 19 b0 6f 9a 6e 2b 16 29 a3 09	...t...o-n+...-
0101 = Header Length: 20 bytes (5)	00e0	62	b
> Flags: 0x018 (PSH, ACK)			

指导教师评语：

日期：