实验报告

院　系 数据科学与计算机学院　　学号 18340215　姓名　张天祎

班 级　18

【实验题目】WireShark **实验**

【实验目的】通过 WireShark 分析 IP 协议(Option)、ICMP 协议、ARP 协议、DHCP 协议、DNS 协议、TCP 协议。

【注意事项】

多个包要截一个**总图**（排序或用 ICMP 作为过滤条件），例如：

7	1.87487500	192.168.0.8	10.22.16.201	ICMP	114 Echo (ping) request id=0x0001, seq=11700/46125, ttl=64 (reply in 8)
8	1.88007700	10.22.16.201	192.168.0.8	ICMP	114 Echo (ping) reply id=0x0001, seq=11700/46125, ttl=252 (request in 7)
11	2.88836800	192.168.0.8	10.22.16.201	ICMP	114 Echo (ping) request id=0x0001, seq=11701/46381, ttl=64 (reply in 12)
12	2.89294600	10.22.16.201	192.168.0.8	ICMP	114 Echo (ping) reply id=0x0001, seq=11701/46381, ttl=252 (request in 11)
17	3.94400800	192.168.0.8	10.22.16.201	ICMP	114 Echo (ping) request id=0x0001, seq=11702/46637, ttl=64 (no response found!)
18	3.94981900	10.22.16.201	192.168.0.8	ICMP	114 Echo (ping) reply id=0x0001, seq=11702/46637, ttl=252 (request in 17)
20	4.99512300	192.168.0.8	10.22.16.201	ICMP	114 Echo (ping) request id=0x0001, seq=11703/46893, ttl=64 (reply in 21)
21	5.00011300	10.22.16.201	192.168.0.8	ICMP	114 Echo (ping) reply id=0x0001, seq=11703/46893, ttl=252 (request in 20)

所有截包要求展开 IP 协议和内部协议，如果有多个，只用选择其中一个，例如：

```
Ethernet II, Src: 60:6d:c7:c6:68:21 (60:6d:c7:c6:68:21), Dst: 1c:68:7e:c2:36:c5 (1c:68:7e:c2:36:c5)
Internet Protocol Version 4, Src: 192.168.0.8 (192.168.0.8), Dst: 10.22.16.201 (10.22.16.201)
    Version: 4
    Header Length: 60 bytes
  + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 100
    Identification: 0xd1e3 (53731)
  + Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
  + Header checksum: 0x7a01 [validation disabled]
    Source: 192.168.0.8 (192.168.0.8)
    Destination: 10.22.16.201 (10.22.16.201)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  - Options: (40 bytes), Time Stamp, End of Options List (EOL)
    - Time Stamp (36 bytes)
      + Type: 68
        Length: 36
        Pointer: 5
        Overflow: 0
        Flag: Time stamp and address
        Address = -, time stamp = 0
        Address = -, time stamp = 0
        Address = -, time stamp = 0
        Address = -, time stamp = 0
      + End of Options List (EOL)
- Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x1fa7 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 11700 (0x2db4)
    Sequence number (LE): 46125 (0xb42d)
    [Response frame: 81]
  - Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
      [Length: 32]
```

BE = 大端序

LE = 小端序

上面分别用 BE 和 LE 表示同一个数，这里是 BE 有效（本来 Intel 采用 LE，不知道这里为什么是 BE 有效）。

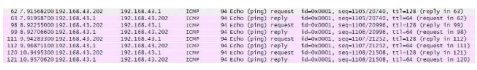
注意每一步都要保存截包文件

【实验任务】

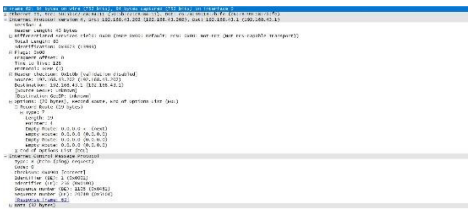
1、 (IP.pcapng)IP Option 和 ICMP 协议。

命令：ping -r 4 域名

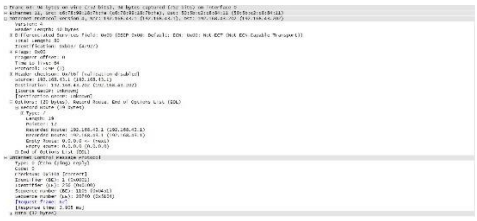
[Ping 总图]



[Ping 请求包截屏]



[Ping 响应包截屏]



[针对于所截包的问题]

IP 选项的长度：20B

ICMP 包的 Identifier：1（BE）

ICMP 包的序号：1105(BE)

ICMP 包的数据部分长度：32B

ICMP 包的数据部分的内容：

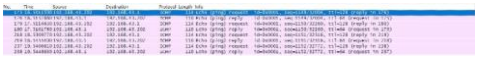
61:62:63:64:65:66:67:68:69:6a:6b:6c:6d:6e:6f:70:71:72:73:74:75:76:77:61:62:63:64:65:66:67:68:69

Identifier 是什么含义？

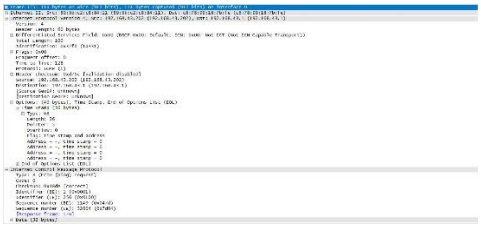
标识符，和序号一起标识出一个包

命令：ping -s 4 域名

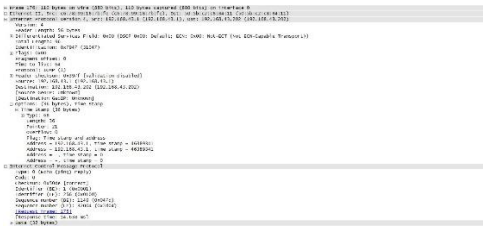
[Ping 总图]



[Ping 请求包截屏]



[Ping 响应包截屏]



[问题]

IP 选项的长度：40B/36B

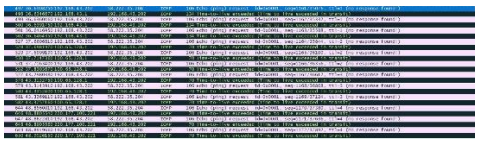
选项中的时间戳是否正确？正确

2、 (tracert.pcapng) ICMP 协议

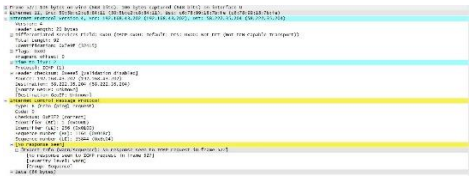
命令：tracert -h 4 域名

[tracert 总图截屏]

实验报告



[TTL=2 的第二个 Ping 请求包截屏]　*可以选其他包，但是要修改一下 *2 和二*



[对应响应包截屏]

3、 (arp.pcapng)ARP 协议。

命令：arp　-a

arp　-d　192.168.0.14

ping 家里另一台电脑或手机：先查看 ARP 缓存，删掉这台电脑的映射，然后启动截包，再 ping 它

[总图]

[ARP 请求包截屏] 用红线标出 ARP 协议中要查询的 IP 地址

[ARP 响应包截屏]用红线标出所查询的 IP 地址对应的 MAC 地址

[找到一个 Gratuitous ARP 包截屏]

＊ 如果没有，可以试一下可以重新配置一个新的 IP 地址，再找不到就算了。

[问题]

当 ARP 缓存没有映射时，系统对要发送的 IP 分组会怎么做？

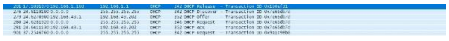
源主机先通过广播发 arp 包找到目的主机的 mac 地址，然后目的主机也会发一个 arp 包到源主机确定源主机的 mac 地址，接着两者的 arp 缓存中都有彼此，可以正常进行 ping 的过程。

ARP 协议是否采用了超时重传？没有

Gratuitous ARP 包有什么用途？可用于检测分配的 IP 是否冲突。

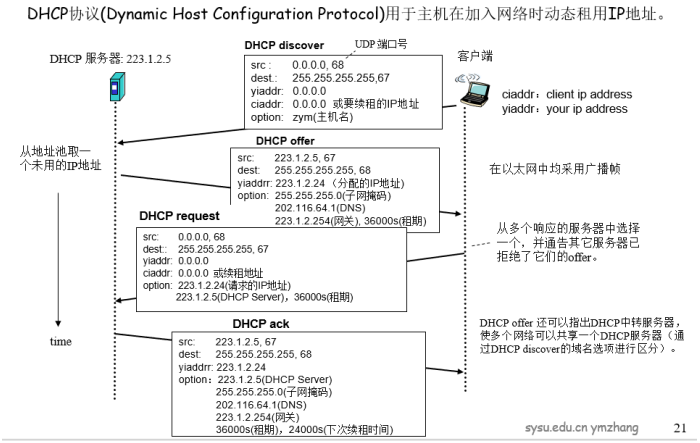
4、 (DHCP.pcapng)DHCP 协议

[总图]



[四个包]

[对照课件]



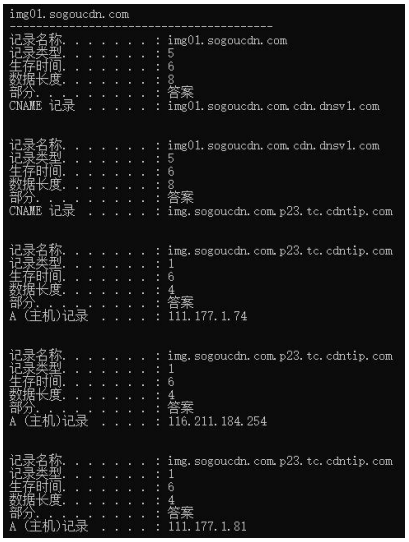
有没有可以纠正的内容？有的话写出来。

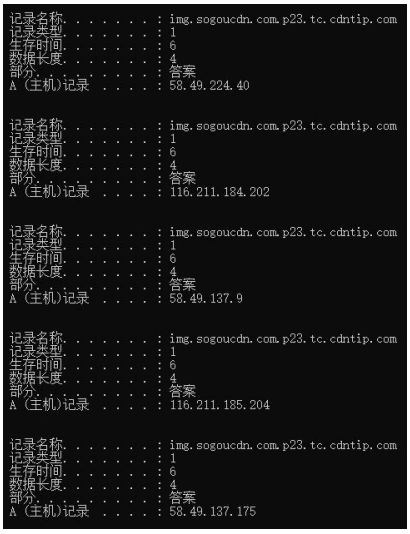
在 request 包内没有关于租期的信息，即 36000s 可能是默认的。

5、 (DNS.pcapng)DNS 协议

先 ping img01.sogoucdn.com 并截屏：

然后,在控制台用 C:>ipconfig /displaydns 查看 DNS 缓存,并截屏 img01.sogoucdn.com 的 DNS 记录：





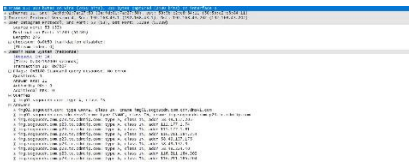
解释其中内容（说明如何可以从 DNS 记录中得到 img01.sogoucdn.com 的 IP 地址）：

首先通过两个 CNAME 记录获取域名的两个别名，然后通过大量的 A 记录解析别名获取 IP 地址。

清除 DNS 记录：C:>ipconfig /flushdns 后，再 ping img01.sogoucdn.com 并截包：

[DNS 查询包]

[DNS 响应包]



6、 (TCP.pcapng)截取完整的 TCP 三次握手建立连接和四次挥手关闭连接的包：

过滤条件： ip.addr==192.168.0.8 and ip.addr==103.26.79.35

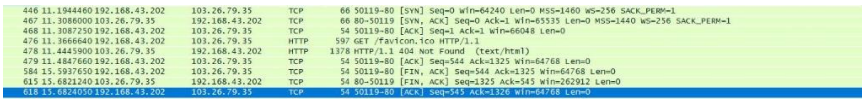
192.168.0.8 要用你的电脑的 IP 地址替换。

http://103.26.79.35/test/j1.html （刷新后要等很久才会关闭连接）

实验报告

如果需要传送完整的图(第二次开始 304 not modified)，可以采用其他图 sysu2.png~sysu24.png

[总图]



[分析]

过滤条件：ip.addr==103.26.79.35 and ip.addr==192.168.43.202 and tcp and tcp.port==50119

建立：

首先用户向服务器发送 SYN 包，Seq=0.然后服务器向用户发送 SYN+ACK 包，Seq=0，Ack=1。接着用户向服务器发送 ACK 包，Seq=1，Ack=1。

关闭：

首先用户向服务器发送 FIN+ACK 包（这里似乎没 PPT 中的 FIN 包，可能是含在了这里面），接着服务器向用户发送 FIN+ACK 包，最后用户再向服务器发送一个 ACK 包。

【完成情况】

是否完成以下步骤？（√完成 -未做完 ×未做）

(1) [√] (2) [√] (3) [√] (4) [√] 5[√] 6[√]

【实验体会】

写出实验过程中的问题，思考及解决方法，简述实验体会（如果有的话）。

【交实验报告】

上传网址：http://103.26.79.35/netdisk/default.aspx?vm=18net

截止日期（不迟于）：2020 年 7 月 23 日（周四）23:00

上传文件名：学号_姓名_WireShark.doc

学号_姓名_WireShark.rar （包含所有.pcapng 文件）