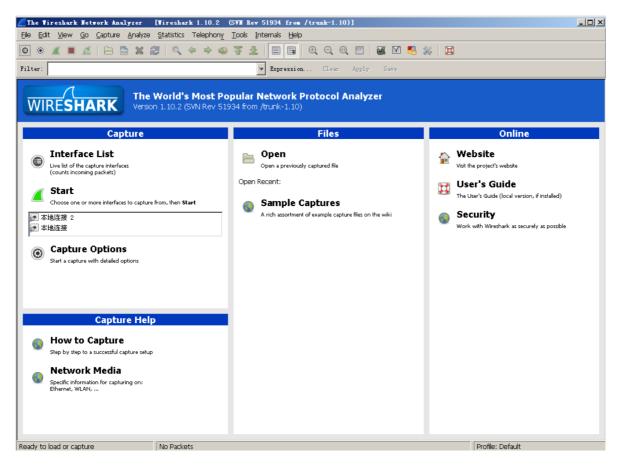
实验2 使用WireShark分析报文

实验要求

- 1. 掌握网络协议分析器与仿真编辑器的使用方法;
- 2. 用 wireshark 分析以数据链路层、网络层和传输层的网络协议单元的结构、理解网络 协议的工作 过程。

实验准备

Wireshark



上机实践

下面是使用Ubuntu来ping Windows Server的结果。

```
215 M-SEARCH * HTTP/1.1
216 M-SEARCH * HTTP/1.1
217 M-SEARCH * HTTP/1.1
218 Echo (ping) replust id=0x0844, seq=1/256, ttl=64
42 Who has 192.168.11.27 rell 192.168.11.3
60 192.168.11.2 is at 08:00:27:55:53:22
98 Echo (ping) reply id=0x0844, seq=1/256, ttl=128 (request in 19)
98 Echo (ping) request id=0x0844, seq=2/512, ttl=128 (request in 23)
98 Echo (ping) request id=0x0844, seq=3/768, ttl=64 (reply in 26)
98 Echo (ping) request id=0x0844, seq=4/1024, ttl=28 (request in 25)
98 Echo (ping) reply id=0x0844, seq=4/1024, ttl=28 (request in 27)
98 Echo (ping) reply id=0x0844, seq=5/1280, ttl=64 (reply in 30)
98 Echo (ping) reply id=0x0844, seq=5/1280, ttl=128 (request in 29)
98 Echo (ping) reply id=0x0844, seq=6/1536, ttl=64 (reply in 32)
98 Echo (ping) reply id=0x0844, seq=6/1536, ttl=128 (request in 31)
 12 75.825437000
13 76.826773000
14 77.827611000
                                                                                                                     192.168.11.1
192.168.11.1
192.168.11.1
                                                                                                                                                                                                                         239.255.255.250
239.255.255.250
239.255.255.250
                                                                                                                                                                                                                                                                                                                                SSDP
  15 194.826835000
                                                                                                                     192.168.11.1
                                                                                                                                                                                                                                                                                                                                SSDP
  16 195.828084000
                                                                                                                     192.168.11.1
                                                                                                                                                                                                                           239.255.255.250
                                                                                                                                                                                                                                                                                                                                SSDP
16 195.828084000
18 197.829948000
19 213.719262000
20 213.719276000
21 213.7958000
22 213.719558000
23 214.745549000
24 214.745624000
25 215.770821000
27 216.812332000
28 216.8123350000
                                                                                                                  192.168.11.1
192.168.11.1
192.168.11.1
192.168.11.2
CadmusCo_79:50:be
CadmusCo_55:53:c2
                                                                                                                                                                                                                                                                                                                                  SSDP
                                                                                                                                                                                                                        Decirios.1.3
Broadcast
CadmusCo_79:50:be
192.168.11.2
192.168.11.3
192.168.11.3
192.168.11.3
                                                                                                                                                                                                                                                                                                                                ARP
                                                                                                                    192.168.11.3
                                                                                                                                                                                                                                                                                                                                ICMP
                                                                                                                  192.168.11.2
192.168.11.3
192.168.11.2
192.168.11.3
                                                                                                                                                                                                                                                                                                                                ICMP
                                                                                                                     192.168.11.2
                                                                                                                                                                                                                         192.168.11.3
                                                                                                                                                                                                                                                                                                                                ICMP
27 216.812332000
28 216.812350000
29 217.818073000
30 217.818087000
31 218.839885000
32 218.839966000
                                                                                                        192.168.11.2
192.168.11.3
192.168.11.2
192.168.11.3
192.168.11.2
192.168.11.3
                                                                                                                                                                                                                     192.168.11.3
192.168.11.3
192.168.11.2
192.168.11.3
192.168.11.3
                                                                                                                                                                                                                                                                                                                                ICMP
```

对报文进行分解,前6位为源地址,之后是目的地址,在一些控制信息后出现真正的数据,长度大约占一般,数据是可读的符号数字序列。

Telnet

No. Time	Source	Destination	Protocol	Length Info
1 0.000000000	192.168.11.3	192.168.11.4	TCP	62 sbl > telnet [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
2 0.000280000	192.168.11.4	192.168.11.3	TCP	62 telnet > sbl [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1
3 0.000287000	192.168.11.3	192.168.11.4	TCP	54 sbl > telnet [ACK] Seq=1 Ack=1 Win=64240 Len=0
4 0.010184000	192.168.11.4	192.168.11.3	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00
5 0.010200000	192.168.11.3	192.168.11.4	NBNS	289 Name query response NBSTAT
6 0.010216000	10.0.2.15	192.168.11.3	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00
7 1.464420000	10.0.2.15	192.168.11.3	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00
8 2.923227000	10.0.2.15	192.168.11.3	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00
9 4.388288000	192.168.11.4	192.168.11.3	TELNET	75 Telnet Data
10 4.388367000	192.168.11.3	192.168.11.4	TELNET	57 Telnet Data
11 4.388688000	192.168.11.4	192.168.11.3	TELNET	62 Telnet Data
13 4 300607000	100 160 11 3	100 160 11 4	TEL NET	O1 Teleph Data

可以看到TCP协议三次握手的过程。

实验过程

1 0.000000000	10.0.2.15	192.168.31.1	DNS	77 Standard query 0x3298 A staff.ustc.edu.cn
2 0.001866000	192.168.31.1	10.0.2.15	DNS	93 Standard query response 0x3298 A 202.38.64.11
3 0.002131000	10.0.2.15	202.38.64.11	TCP	62 wfremotertm > http [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
4 0.017079000	202.38.64.11	10.0.2.15	TCP	60 http > wfremotertm [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
5 0.017090000	10.0.2.15	202.38.64.11	TCP	54 wfremotertm > http [ACK] Seq=1 Ack=1 win=64240 Len=0
6 0.017280000	10.0.2.15	202.38.64.11	HTTP	622 GET /~mfy/network.htm HTTP/1.1
7 0.017392000	202.38.64.11	10.0.2.15	TCP	60 http > wfremotertm [ACK] Seq=1 Ack=569 Win=65535 Len=0
8 0.046031000	202.38.64.11	10.0.2.15	HTTP	204 HTTP/1.1 304 Not Modified
9 0.046041000	202.38.64.11	10.0.2.15	TCP	60 http > wfremotertm [FIN, ACK] Seq=151 Ack=569 Win=65535 Len=0
10 0.046050000	10.0.2.15	202.38.64.11	TCP	54 wfremotertm > http [ACK] Seq=569 Ack=152 win=64090 Len=0
11 0.046249000	10.0.2.15	202.38.64.11	TCP	54 wfremotertm > http [FIN, ACK] Seq=569 Ack=152 win=64090 Len=0
12 0.046520000	202.38.64.11	10.0.2.15	TCP	60 http > wfremotertm [ACK] Seq=152 Ack=570 win=65535 Len=0

访问课程主页,得到的报文结果如下。

结果分析

首先分析各个报文的目的。

- 1. 报文1和2通过DNS服务器查询网址对应的ip地址
- 2. 345是TCP三次握手
- 3. 报文6由浏览器向服务器发送请求
- 4. 报文7发送控制协议
- 5. 由于此页面曾被加载过一遍,本地有缓存,因此报文8的内容是"自上次加载未进行更新",否则应该是报文内容
- 6.9到10四次握手断开连接