**《Internet协议分析实验报告》**

**实验单元： 传输层(2/6)**

**应用层**

**网络安全**

学号:031602507 姓名: 刘宏岩 实验机位: 9-B

小组成员:

学号: 031602507 姓名: 陈俞辛

学号: 031602523 姓名: 刘宏岩

学号：\_\_\_\_\_\_\_\_\_ 姓名: \_\_\_\_\_\_

学号：\_\_\_\_\_\_\_\_\_ 姓名: \_\_\_\_\_\_

学号：\_\_\_\_\_\_\_\_\_ 姓名: \_\_\_\_\_\_

学号：\_\_\_\_\_\_\_\_\_ 姓名: \_\_\_\_\_\_

实验时间： 2018 年 6 月 30 日实验目录

**第4部 传输层(2/6)(2个任务)**

**实验19 传输控制协议(TCP)分析**

*练习二 TCP重传机制*

任务一 TCP重传机制分析

*练习三 TCP拥塞控制机制分析*

任务一 TCP拥塞控制分析

**第5部分 应用层(5个任务)**

**实验20 域名服务协议（DNS）分析**

*练习二 域名查询与高速缓存*

任务一 DNS正向查询

任务三 DNS高速缓存

**实验23 超文本传输协议(HTTP)分析**

*练习一 HTTP报文分析*

任务一 页面访问

任务三 获取页面信息

*练习二 HTTP请求流程分析*

任务一 HTTP请求分析

**第6部分 网络安全(1个任务)**

**实验29 因特网中安全通信措施**

练习二 数据安全通信的实现

任务一 数据安全通信的实现

# 实验19 传输控制协议(TCP)分析

## 练习二 TCP重传机制

### 实验学时

0.5学时

### 实验目的

● 理解TCP重传机制

### 实验环境

网络拓扑结构一

### 实验工具

地址本工具

协议分析器

协议编辑器

TCP工具

启动TCP屏蔽

停止TCP屏蔽

### 实验任务

任务一 TCP重传机制分析

### 任务一 TCP重传机制分析

各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。

本任务将主机A和B作为一组，主机C和D作为一组，主机E和F作为一组。现仅以主机A、B所在组为例，其它组的操作参考主机A、B所在组的操作。

1. 主机B上启动“实验平台工具栏中的TCP工具”，作为服务端，监听端口设置为2483。

2. 主机B启动协议分析器开始捕获数据并设置过滤条件（提取TCP协议）。

3. 主机A启动TCP工具连接主机B。

（1）主机A启动“实验平台工具栏中的TCP工具”。

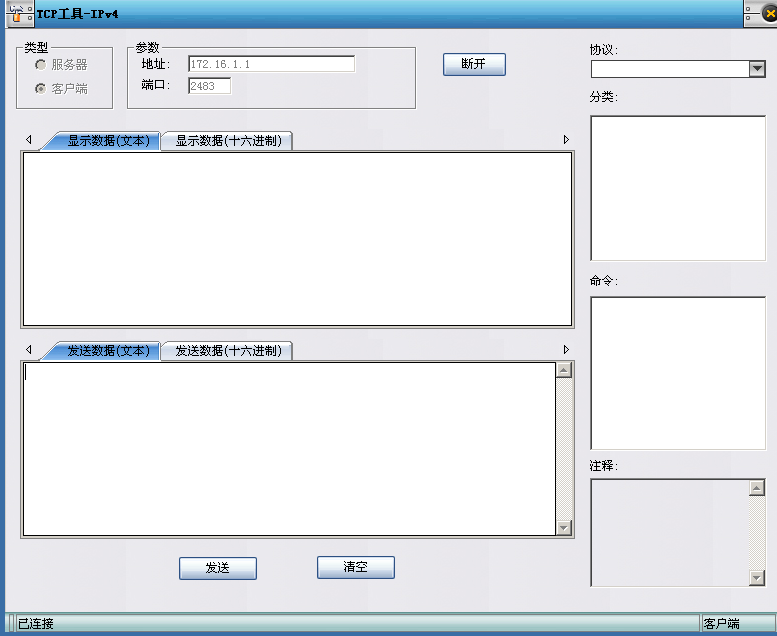
（2）选中“客户端”单选框。

（3）在“地址”文本框中填入主机B的IP地址。

（4）在“端口”文本框中填入主机B的TCP监听端口（2483）。

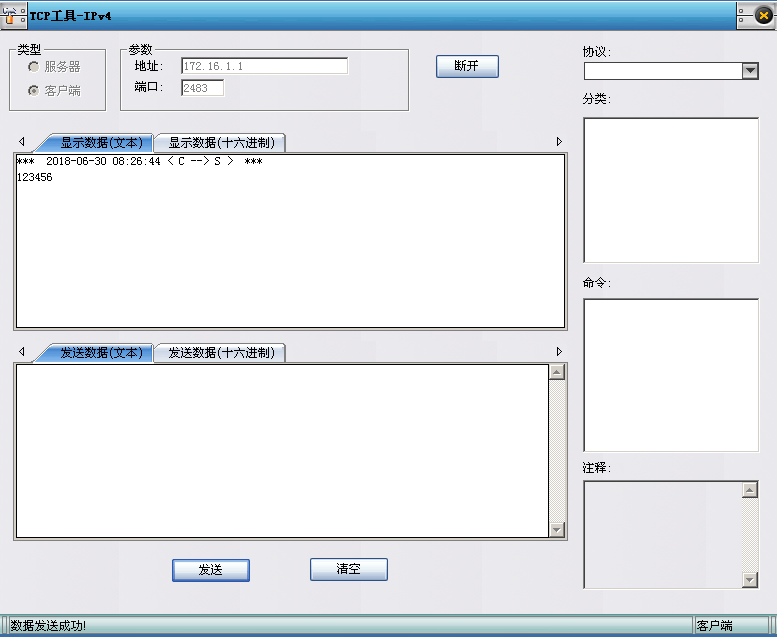
（5）点击[连接]按钮进行连接。

(贴图)



4. 主机A向主机B发送一条信息。

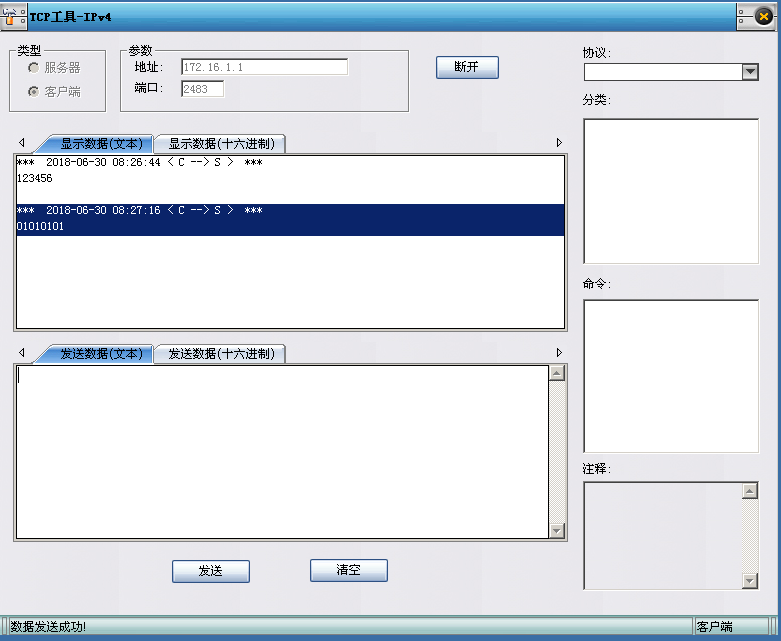
(贴图)



5. 主机B启动“实验平台工具栏中的启动TCP屏蔽”，过滤掉接收到的TCP数据。

6. 主机A向主机B再发送一条信息。

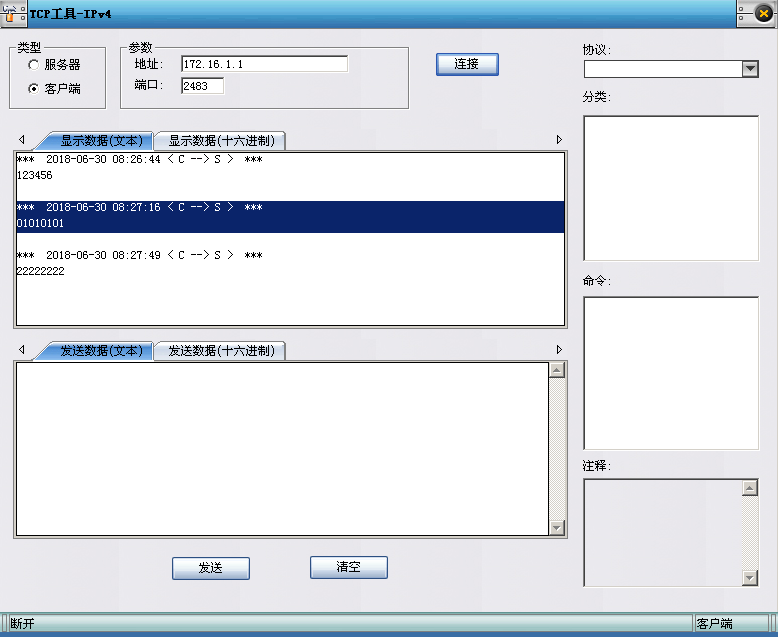
(贴图)



7. 主机B刷新捕获显示，当发现“会话分析视图”中有两条以上超时重传报文后，启动“实验平台工具栏中的停止TCP屏蔽”，恢复正常网络功能。

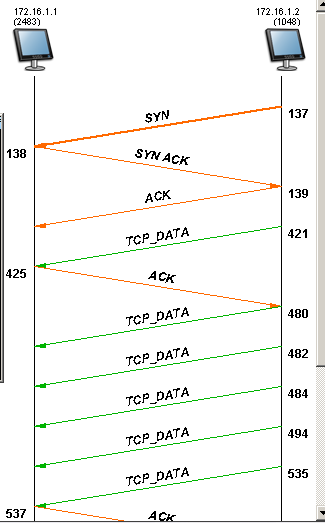
8. 主机A向主机B再发送一条信息，之后断开连接。

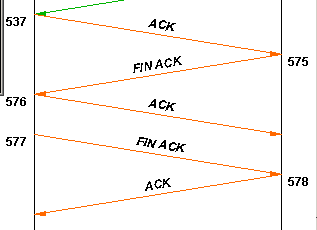
(贴图)



9. 主机B停止捕获数据。依据“会话分析视图”显示结果，绘制本任务的数据报交互图。

(贴图并分析实验结果)





做完实验后，请同学考虑以下问题：

◆ 根据实验，测试重传时间和重传次数。

五次，时间戳是从上午十点14分的5秒、11秒、22秒、43秒、15分的24秒。可以看到重传的间隔时间是逐渐增大的，而且不断翻倍。

## 练习三 TCP拥塞控制机制分析

### 实验学时

0.5学时

### 实验目的

● 了解拥塞窗口概念

● 理解TCP拥塞控制原理及控制过程

● 理解拥塞控制使用的策略

### 实验环境

网络拓扑结构一

### 实验工具

TCP拥塞控制演示工具

### 实验任务

任务一 TCP拥塞控制分析

### 任务一 TCP拥塞控制分析

本任务每台主机为一组。现仅以主机A所在组为例，其它组的操作参考主机A所在组的操作。

1. TCP拥塞控制演示工具按钮功能介绍。

（1）网络状态

分为三种情况：网络畅通、轻度拥塞和严重拥塞。

网络畅通：点击按钮后，云颜色变为绿色，网络状态为畅通，系统默认为网络畅通状态。

轻度拥塞：点击按钮后，云颜色变为黄色，网络状态改为轻度拥塞。

严重拥塞：点击按钮后，云颜色变为红色，网络状态改为严重拥塞。

（2）控制按钮

有发包、暂停和重置三种。

发包：点击按钮后，发送数据包，直到这次数据交互过程结束。

暂停：工具初始化时按钮为灰色，不可按。当发包按钮变为灰色时，暂停按钮变为可用，点击暂停按钮，数据收发演示部分停止数据交互过程，按钮显示继续，点击继续按钮后继续数据交互过程。

重置：工具恢复初始状态。当不可用时，按钮变为灰色。

2. 网络畅通状态的变化。

（1）选择网络状态为网络畅通，在这种情况下，首先注意窗口大小、阈值、超时定时器的初始值分别为多少。

（2）点击发包按钮，根据发包次数的不同，填写下表19-3-1。

● 记录实验数据。

|  |  |  |  |
| --- | --- | --- | --- |
| 发包次数 | 窗口大小 | 阀值 | 是否超时 |
| 初始状态 | 1 | 16 | 否 |
| 1 | 2 | 16 | 否 |
| 2 | 4 | 16 | 否 |
| 3 | 8 | 16 | 否 |
| 4 | 16 | 16 | 否 |
| 5 | 17 | 16 | 否 |
| 6 | 18 | 16 | 否 |

● 根据上面记录的数据，分析TCP拥塞窗口、阈值、超时定时器的变化规律，说明在这种状态下，TCP采取怎样的拥塞控制策略。

1-4阶段采用慢开始算法，因为窗口小于慢开始门限。

5-6阶段采用拥塞避免算法，窗口大于等于慢开始门限。

3. 轻度拥塞状态的变化。

（1）轻度拥塞有两种情况，我们分别进行演示分析。

（2）首先点击重置按钮，将网络置于初始状态。

（3）为了更好的观察轻度拥塞情况下的窗口大小和阈值的变化规律，我们可以先选择网络状态为网络畅通，发送1次数据。

（4）选择网络状态为轻度拥塞，观察在这种情况下，窗口大小、阈值、超时定时器的初始值分别为多少。并填写下表内容。

● 记录实验数据。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网络状态 | 发包次数 | 窗口大小 | 阀值 | 是否超时 |
| 网络畅通 | 初始状态 | 1 | 16 | 否 |
| 1 | 2 | 16 | 否 |
| 轻度拥塞 | 1 | 2 | 16 | 是 |

● 根据上面记录的数据，分析TCP拥塞窗口、阈值、超时定时器的变化规律，说明在这种状态下，是由于什么引起的拥塞，TCP又是采取怎样的拥塞控制策略。

由于网络情况为轻度拥塞，TCP发生了超时，把门限调低成窗口大小的一半（但最低是1），然后把窗口置为1。

（5）首先点击重置按钮，将网络置于初始状态。

（6）为了更好的观察轻度拥塞情况下的窗口大小和阈值的变化规律，我们可以先选择网络状态为网络畅通，发送2次数据。

（7）选择网络状态为轻度拥塞，观察在这种情况下，窗口大小、阈值、超时定时器的初始值分别为多少。并填写下表内容。

● 记录实验数据。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网络状态 | 发包次数 | 窗口大小 | 阀值 | 是否超时 |
| 网络畅通 | 初始状态 | 1 | 16 | 否 |
| 1 | 2 | 16 | 否 |
| 2 | 4 | 16 | 否 |
| 轻度拥塞 | 1 | 2 | 2 | 是 |

● 根据上面记录的数据，分析TCP拥塞窗口、阈值、超时定时器的变化规律，说明在这种状态下，是由于什么引起的拥塞，TCP又是采取怎样的拥塞控制策略。

收到了连续的三个ACK，此时不是超时，而是数据报丢失，采用快恢复算法，把门限调整为窗口大小即可。

4. 严重拥塞状态的变化。

（1）首先点击重置按钮，将网络置于初始状态。

（2）为了更好的观察严重拥塞情况下的窗口大小和阈值的变化规律，我们可以先选择网络状态为网络畅通，发送2次数据。

（3）选择网络状态为严重拥塞，观察在这种情况下，窗口大小、阈值、超时定时器的初始值分别为多少。并填写下表内容。

● 记录实验数据。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网络状态 | 发包次数 | 窗口大小 | 阀值 | 是否超时 |
| 网络畅通 | 初始状态 | 1 | 16 | 否 |
| 1 | 2 | 16 | 否 |
| 2 | 4 | 16 | 否 |
| 严重拥塞 | 1 | 1 | 2 | 是 |
| 2 | 2 | 2 | 否 |

● 根据上面记录的数据，分析TCP拥塞窗口、阈值、超时定时器的变化规律，说明在这种状态下，是由于什么引起的拥塞，TCP又是采取怎样的拥塞控制策略。

发生了严重拥塞， 因此将阈值减半并且将拥塞窗口置为1。可能是由于网络质量差引起的

# 实验20 域名服务协议（DNS）分析

## 练习二 域名查询与高速缓存

### 实验学时

1.5学时

### 实验目的

● 掌握DNS的报文格式

● 掌握DNS的工作原理

● 理解DNS高速缓存的作用

### 实验环境

网络拓扑结构一

### 实验工具

协议分析器

协议编辑器

命令行

### 实验任务

任务一 DNS正向查询

任务三 DNS高速缓存

### 任务一 DNS正向查询

各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。

本任务将主机A和B作为一组，主机C和D作为一组，主机E和F作为一组。现仅以主机A、B所在组为例，其它组的操作参考主机A、B所在组的操作。

【说明】

本任务中要求每台主机设置DNS服务器地址（即服务器的IP地址，默认为172.16.0.253）。

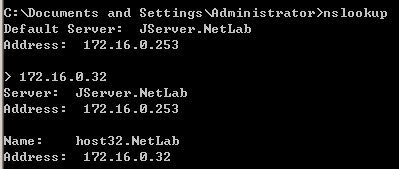
各组主机IP地址配置如下：

第一组六台主机IP地址依次为172.16.0.11，172.16.0.12 …… 172.16.0.16；

第二组六台主机IP地址依次为172.16.0.21，172.16.0.22 …… 172.16.0.26；

其它各组以此类推。

1. 在主机B上执行命令“nslookup 主机B的IP”获取主机B的域名，并告知主机A。



2. 主机A启动协议编辑器，编写一个DNS正向查询报文。其中：

MAC层：

源MAC地址：本机MAC地址

目的MAC地址：服务器的MAC地址

IP层：

源IP地址：本机IP地址

目的IP地址：服务器的IP地址（默认为172.16.0.253）

总长度：IP层及其上层协议总长度

校验和：IP层字段全部编辑完成后，计算IP层校验和

UDP层：

源端口：大于1024的端口

目的端口：53

有效负载长度：UDP层及其上层协议总长度

校验和：所有字段编辑完成后，计算校验和

DNS层：

标志：0100

问题记录数：1

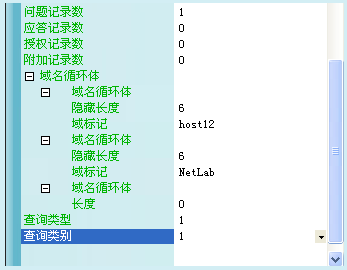
域名循环体：选中第一个“域名循环体”项，点击右边按钮[B]来追加域名块。按格式要求填写步骤1获取的主机B的域名。

例如：设步骤1中获取的域名为host12.Netlab，则追加2块。选中“域名循环体”下的“长度”项，修改长度值；出现“域标记”项，选中“域标记”项，点击右边按钮[E]输入相应的值。最后一块“长度”字段为0。

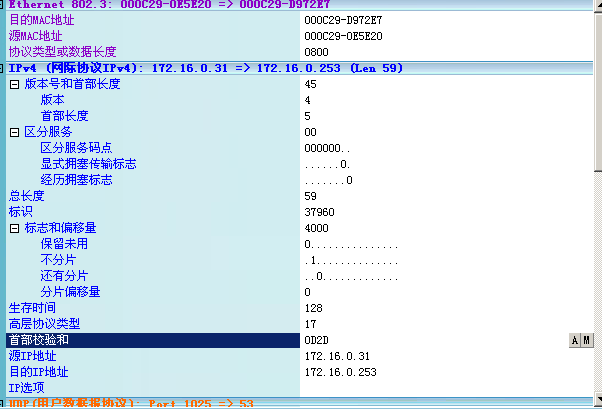
查询类型：1

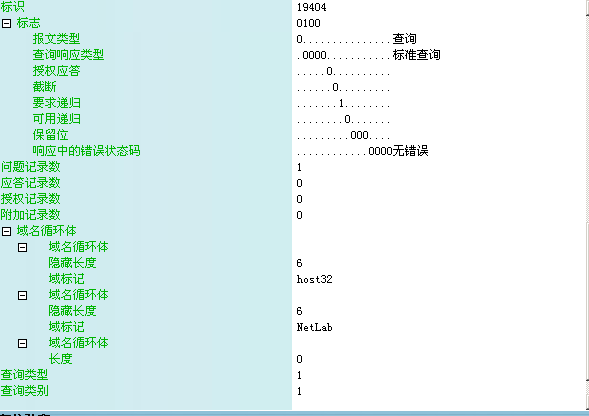
查询类别：1

设置如图所示：



(设置结果贴图)





3. 主机B启动协议分析器开始捕获数据，并设置过滤条件（提取DNS协议）。

4. 主机A发送已编辑好的报文。

5. 主机B停止捕获数据。在捕获到的数据中查找DNS响应报文。

「注」在响应报文中提取主机B的IP地址。

(找到的数据包贴图)



### 任务三 DNS高速缓存

各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。

本任务将主机A和B作为一组，主机C和D作为一组，主机E和F作为一组。现仅以主机A、B所在组为例，其它组的操作参考主机A、B所在组的操作。

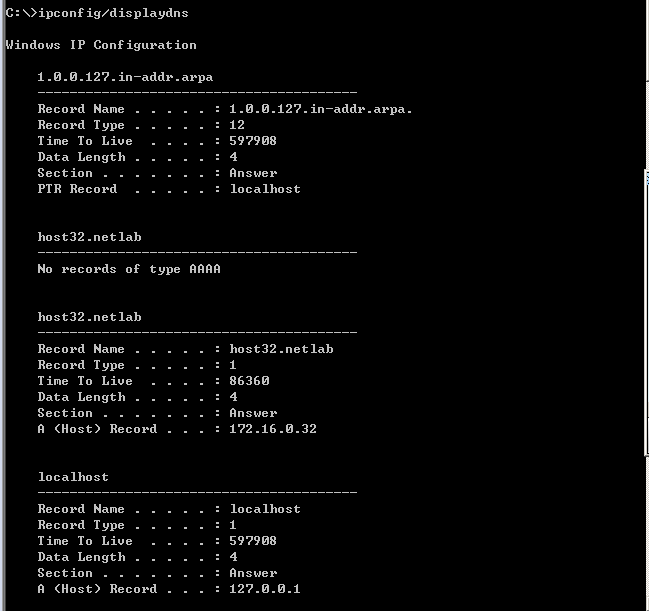
1. 该任务中，DNS服务器及各主机IP地址配置同任务一。

2. 主机A在命令行下执行“ipconfig /flushdns”命令来清空DNS高速缓存。

3. 主机B启动协议分析器开始捕获数据并设置过滤条件（提取DNS协议和ICMP协议）。

4. 主机A在命令行下执行“ping 主机B的域名”命令，然后执行“ipconfig /displaydns”命令来显示DNS高速缓存。在缓存中找到主机B的域名所对应的记录。

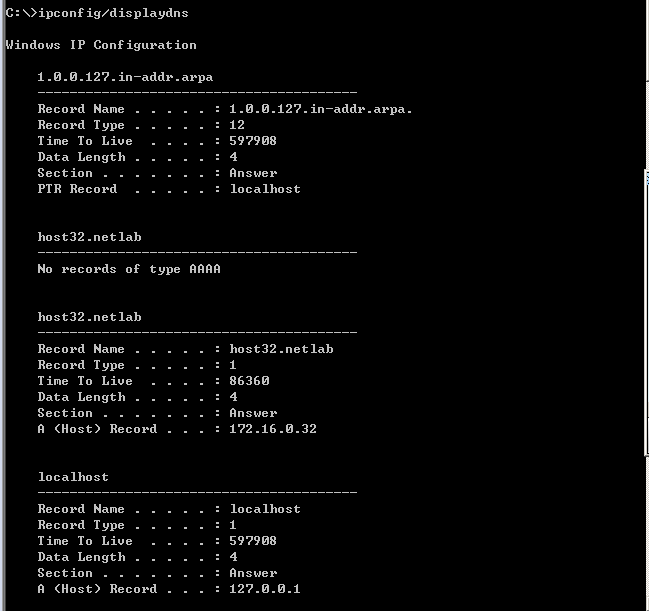
(缓存记录贴图)

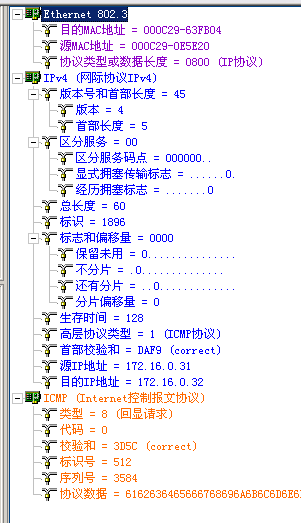
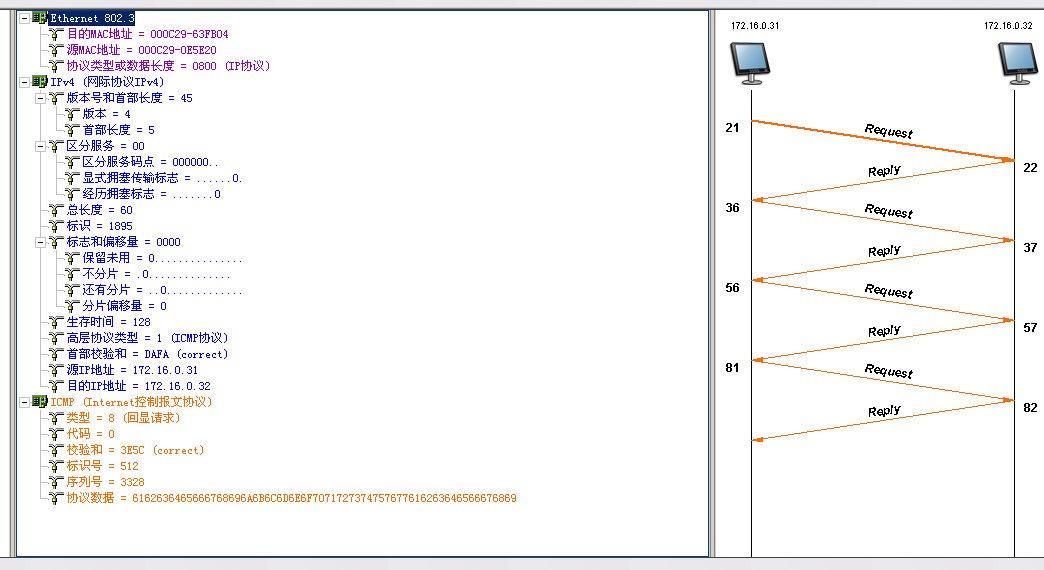


5. 主机A在命令行下再次执行“ping 主机B的域名”命令。

6. 主机B停止捕获，分析其捕获的数据及主机A的DNS高速缓存中的内容，回答问题：

(捕获的数据贴图)





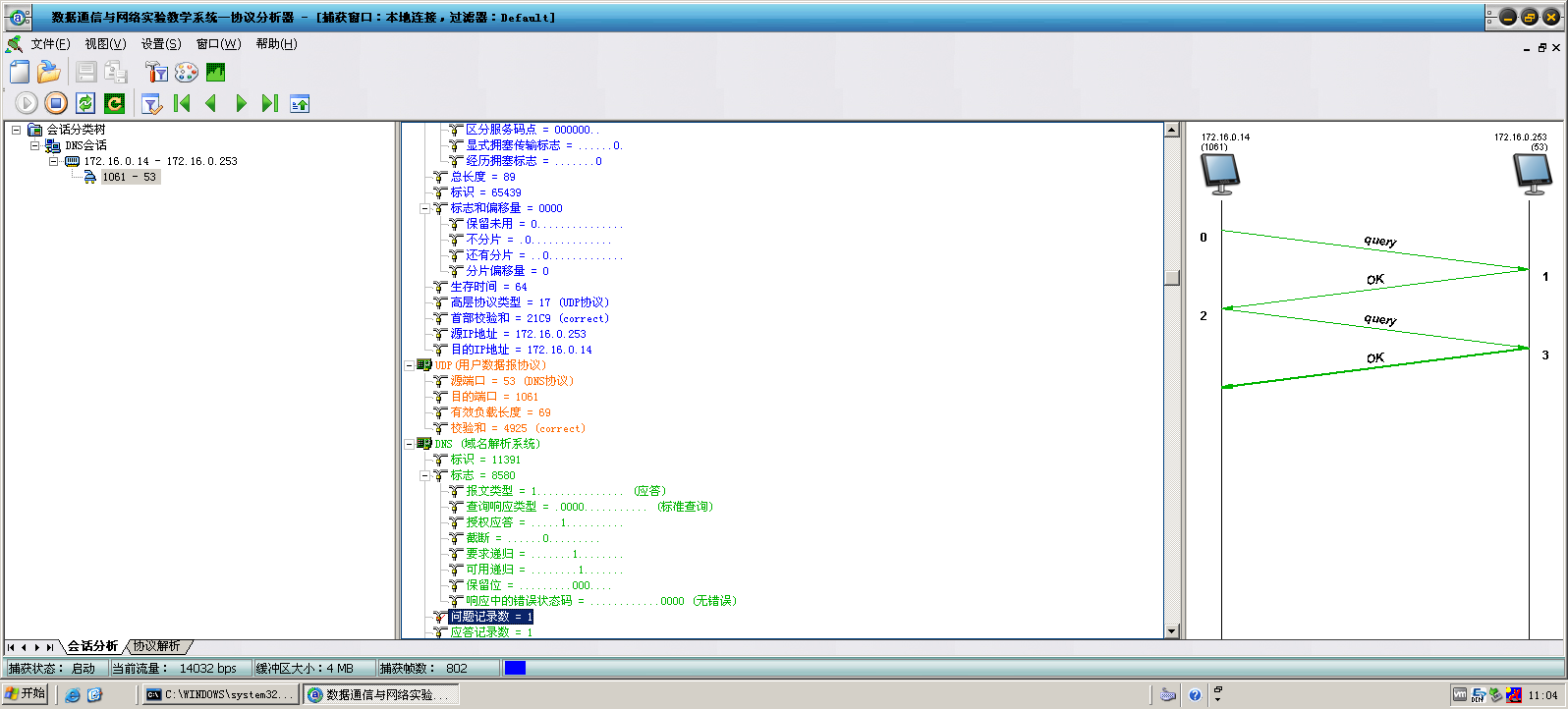
● 简述在使用域名完成的通信中，DNS协议所起到的作用。

将域名解析为IP地址

● 简述DNS高速缓存的作用。

可大大减轻根域名服务器的负荷,使因特网上的 DNS 查询请求和回答报文的数量大为减少。

● 参考主机B“会话分析”视图的显示结果，绘制此次访问过程的报文交互图（包括ICMP协议）。



7. 恢复网络环境，将“首选DNS服务器”清空。

# 实验23 超文本传输协议(HTTP)分析

## 练习一 HTTP报文分析

**实验学时**

1.5学时

**实验目的**

● 掌握HTTP的报文格式

● 掌握HTTP的工作原理

● 掌握HTTP常用方法

**实验环境**

网络拓扑结构一

**实验工具**

协议分析器

IE浏览器

TCP工具

**实验任务**

任务一 页面访问

任务三 获取页面信息

### 任务一 页面访问

各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。

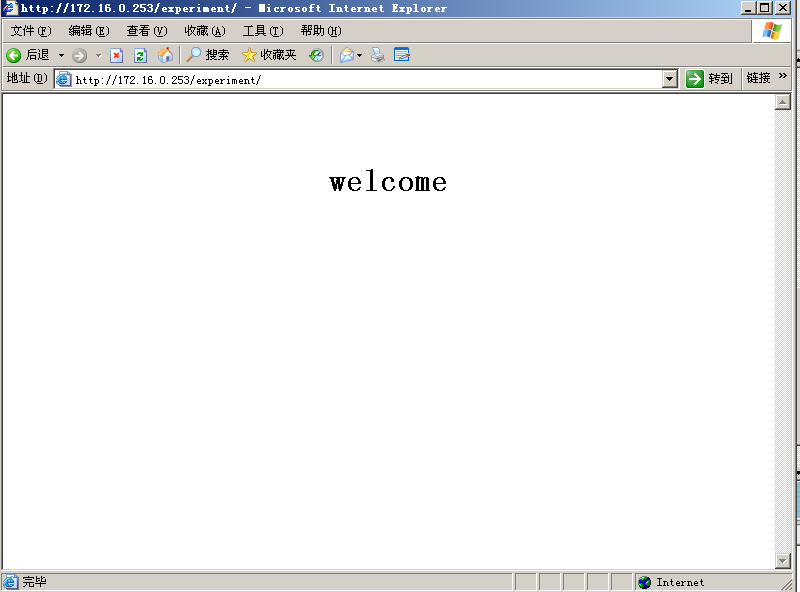
本任务将主机A和B作为一组，主机C和D作为一组，主机E和F作为一组。现仅以主机A、B所在组为例，其它组的操作参考主机A、B所在组的操作。

1. 主机A清空IE缓存。

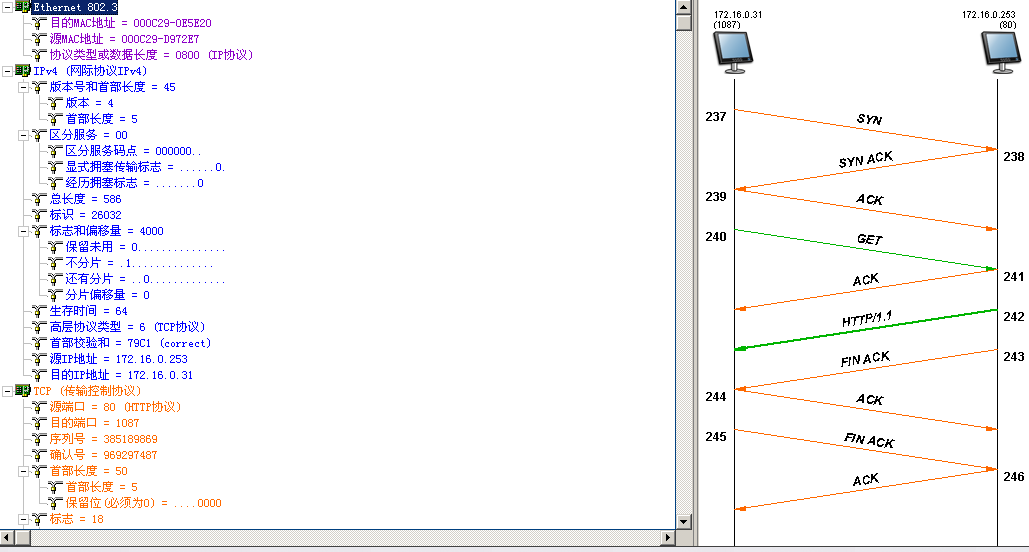
2. 主机B启动协议分析器开始捕获数据，并设置过滤条件（提取HTTP协议）。

3. 主机A启动IE浏览器，在“地址”框中输入http://服务器的ip/experiment，并连接，服务器的ip默认为172.16.0.253。

(贴图)

4. 主机B停止捕获数据，分析捕获到的数据，并回答以下问题：

(捕获的数据贴图)



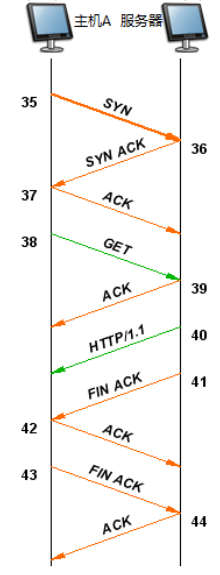
● 本练习使用HTTP协议的哪种方法？简述这种方法的作用。

GET方法,请求读取由URL所标志的信息。

● 根据本练习的报文内容，填写下表。

|  |  |
| --- | --- |
| 主机名 | 172.16.0.253 |
| URL | http://172.16.0.253/experiment/ |
| 服务器类型 | .Apache/2.2.3.(CentOS) |
| 传输文本类型 | .text/html |
| 访问时间 | .Tue,.22.May.2018.07:08:22.GMT. |

● 参考“会话分析”视图显示结果，绘制此次访问过程的报文交互图（包括TCP协议）。



● 简述TCP协议和HTTP协议之间的关系。

HTTP协议属于应用层协议，在运输层采用TCP协议实现数据无差错传输。HTTP协议是建立在TCP协议基础之上的。

◆ 一个主页是否只有一个连接？

一个主页可以对应多个链接

### 任务三 获取页面信息

各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。

本任务将主机A和B作为一组，主机C和D作为一组，主机E和F作为一组。现仅以主机A、B所在组为例，其它组的操作参考主机A、B所在组的操作。

1. 主机A启动“实验平台工具栏中的TCP工具”。

2. 主机B启动协议分析器开始捕获数据，并设置过滤条件（提取HTTP协议）。

3. 主机A在“TCP工具”上，选中“客户端”单选框，设置“IP地址”为服务器IP（默认为172.16.0.253）；设置“端口”为80；单击[连接]按钮来和服务器建立连接。

4. 主机A在“TCP工具”上，设置“发送数据（文本）”为以下内容：

HEAD /experiment/ HTTP/1.1<CRLF>

Host: 172.16.0.253<CRLF>

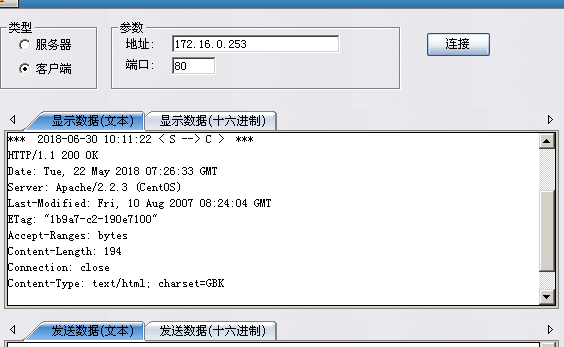
<CRLF>

点击[发送]按钮。 （注：<CRLF>是回车换行）

点击[断开]按钮，断开TCP连接（由于不同http版本所遵循的规范不同，有些HTTP服务器不需要断开操作）。

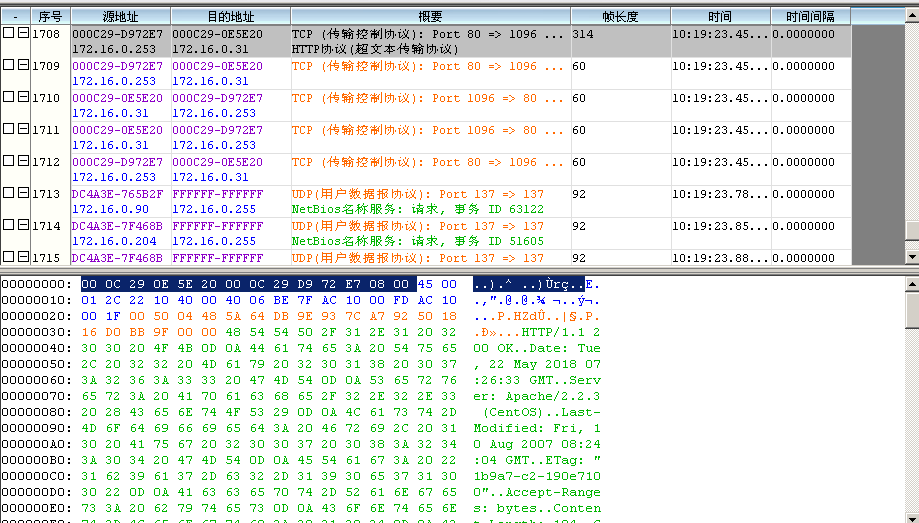
5. 主机A在“TCP工具”上的“显示数据（文本）”中察看服务器返回信息。

(贴图)



6. 主机B停止捕获数据，分析捕获到的数据。

(捕获的数据贴图,并分析其内容)



做完实验后，请同学考虑以下问题：

◆ 同时打开多个浏览器窗口并访问一个WEB站点的不同页面时，系统是根据什么把返回的页面正确地显示到相应窗口的？

使用多个浏览器窗口访问一个WEB站点的不同页面时，每一个浏览器窗口可能对应一个或多个连接，每一个连接和数据报中的一个端口相对应，系统是根据这种对应关系把返回的页面正确地显示到相应窗口中。

## 练习二 HTTP请求流程分析

### 实验学时

0.5学时

### 实验目的

● 掌握HTTP请求流程

### 实验环境

网络拓扑结构一

### 实验工具

协议分析器

TCP工具

IE浏览器

命令行

### 实验任务

任务一 HTTP请求分析

### 任务一 HTTP请求分析

各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。

本任务将主机A和B作为一组，主机C和D作为一组，主机E和F作为一组。现仅以主机A、B所在组为例，其它组的操作参考主机A、B所在组的操作。

1. 本任务中要求主机A设置DNS服务器地址（即服务器的IP地址，默认为172.16.0.253）。

2. 主机A使用“ipconfig /flushdns”命令清空DNS高速缓存。

3. 主机B启动协议分析器开始捕获数据并设置过滤条件（提取DNS、HTTP协议）。

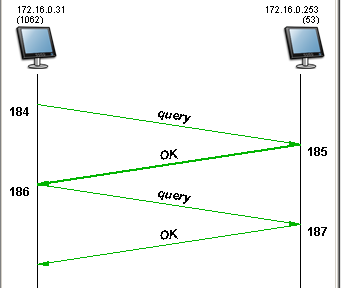
4. 主机A启动IE浏览器，在地址框中输入http://JServer.NetLab/complexpage.htm。

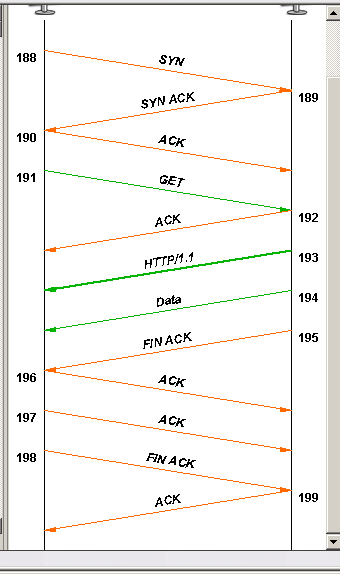
(页面贴图)



5. 主机B停止捕获数据，察看相关会话，分析捕获到的数据，并回答以下问题：

(捕获的数据贴图, 并分析)





● 结合本次实验结果，简述浏览器是如何处理一个访问请求的。

用户在浏览器的地址栏中输入Web站点的URL，URL中的信息被浏览器提取出来打包到一个HTTP请求报文中，然后传输给底层的传输层、网络层和链路层协议。该请求报文由运行Web服务器软件的目标计算机接收。服务器处理该请求报文并且获取所需信息，然后创建一个HTTP响应报文再传输。这个响应由客户端接收，浏览器解释，然后再显示给用户

◆ 为什么HTTP不保持与客户端的TCP连接？

HTTP版本1.0指明了非持续连接，而在版本1.1中，持续连接是默认的策略。

非持续连接

在非持续连接中，对每一个请求/响应都要建立一次TCP连接。下面列出这种策略的步骤：

(1) 客户打开TCP连接，并发送请求。

(2) 服务器发送响应，并关闭连接。

(3) 客户读取数据，直到它遇到文件结束；然后它关闭连接。

使用这种策略时，对于在不同文件中的N个不同资源，连接必须打开和关闭N次。非持续连接策略给服务器造成了很大的开销，因为服务器需要N个不同的缓存，而每次打开连接时都要使用慢开始过程。

持续连接

HTTP版本1.1指明持续连接是默认的策略。在使用持续连接时，服务器在发送响应后，让连接继续为一些请求打开。服务器可以在客户请求或到达超时时限时,关闭这个连接。发送端通常在每一个响应中都发送数据的长度。但是，在某些情况下，发送端并不知道数据的长度。这种情况就是当文档是动态文档或活动文档时。在这些情况下，服务器把不知道长度这件事通知客户，并在发送数据后关闭这个连接，因此客户就知道数据结束的地方已经到了。

6. 恢复网络环境，将“首选DNS服务器”清空。

# 实验29 因特网中安全通信措施

## 练习二 数据安全通信的实现

### 实验学时

1学时

### 实验目的

● 掌握安全通信中常用的加密算法

● 掌握安全文件传输基本步骤

### 实验环境

网络拓扑结构一

### 实验工具

协议分析器

密码工具

### 实验任务

任务一 数据安全通信的实现

### 任务一 数据安全通信的实现

各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。

本任务将主机A和B作为一组，主机C和D作为一组，主机E和F作为一组。现仅以主机A、B所在组为例，其它组的操作参考主机A、B所在组的操作。

说明：实验应用密码工具实现信息的安全传输，其实现流程参见实验原理二，下面以主机A为数据发送方，主机B为数据接收方为例，说明实验过程。

1. 主机A与主机B协商实验中用到的加密算法: DES(对称加密算法)、RSA(非对称加密算法)和MD5(哈希函数);

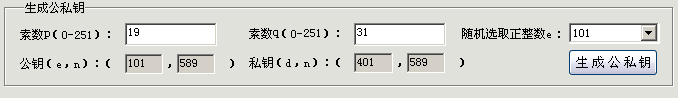
2. 主机A、B分别生成公私钥对。

进入“密码工具”|“RSA加密算法”|“公私钥”页签，在生成公钥区输入素数p和素数q，这里要求p和q不能相等，并且p与q的乘积也不能小于127。

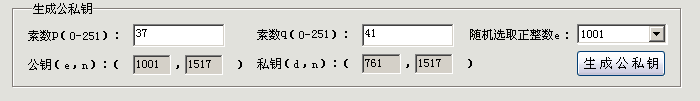
点击“随机选取正整数e”下拉按钮，随机选取e的值。

点击“生成公私钥”按钮生成公私钥，并将公钥通告给对方。

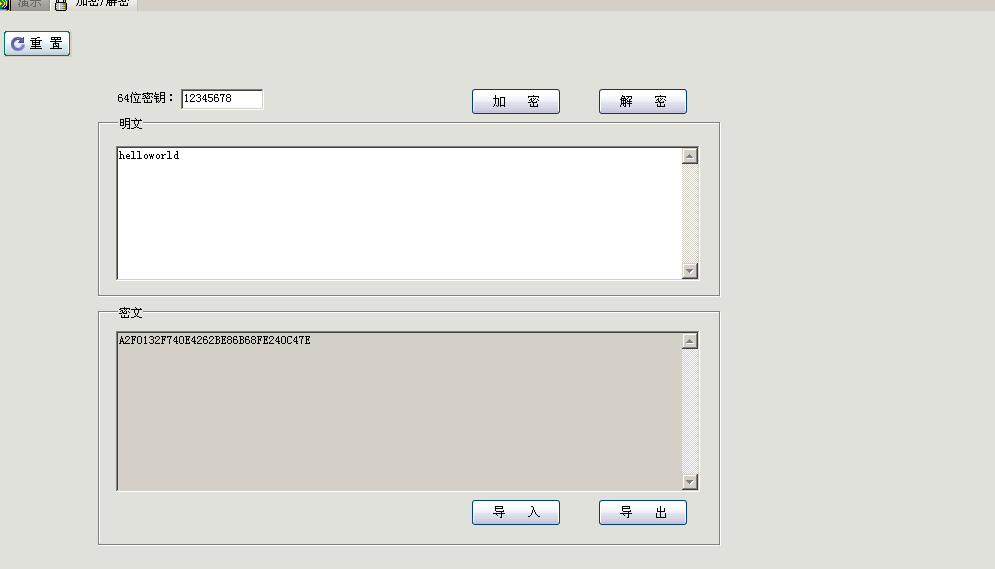
主机A



主机B



3. 主机A使用DES对称加密算法对源文件进行加密。



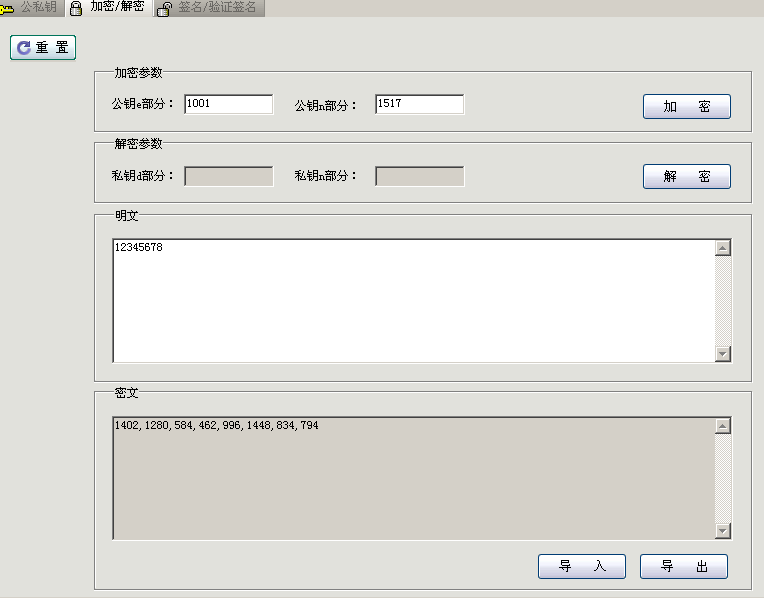
创建名为s.txt，内容任意的文件，作为传输的源文件。

进入“DES机密算法”|“加密、解答”页签，在密钥窗口输入8(64位)个字符的密钥k（会话密钥）。

在明文输入区输入s.txt文件的内容，单击“加密”按钮，对明文进行加密，单击“导出”按钮将密文保存到数据加密文件夹(work\FileEncrypt\)中，命名为“源文件密文”。

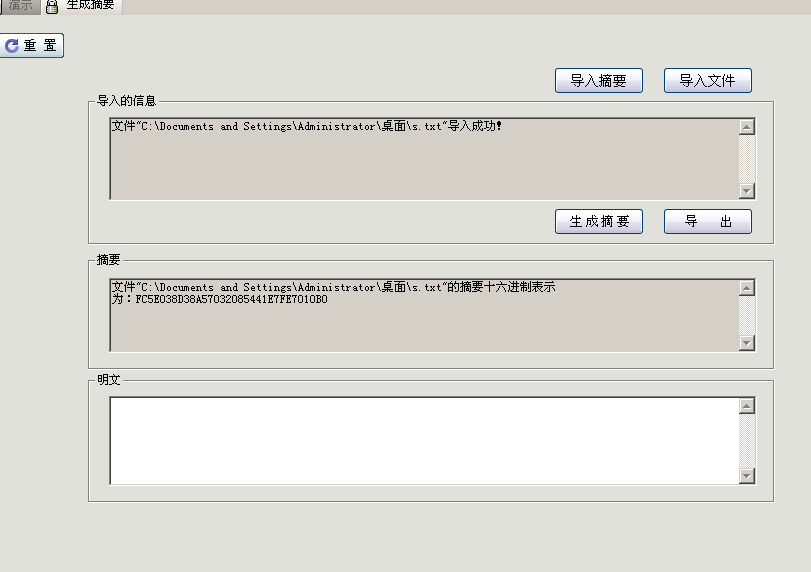
4. 主机A使用主机B的公钥对会话密钥进行加密。

进入“RSA加密算法”|“加密/解密”页签，在“在公钥e部分”和“公钥n部分”输入主机B的公钥，在明文输入区输入会话密钥k的内容，单击“加密”按钮进行加密，单击“导出”按钮将密文保存到数据加密文件夹中，命名为“会话密钥k密文”。



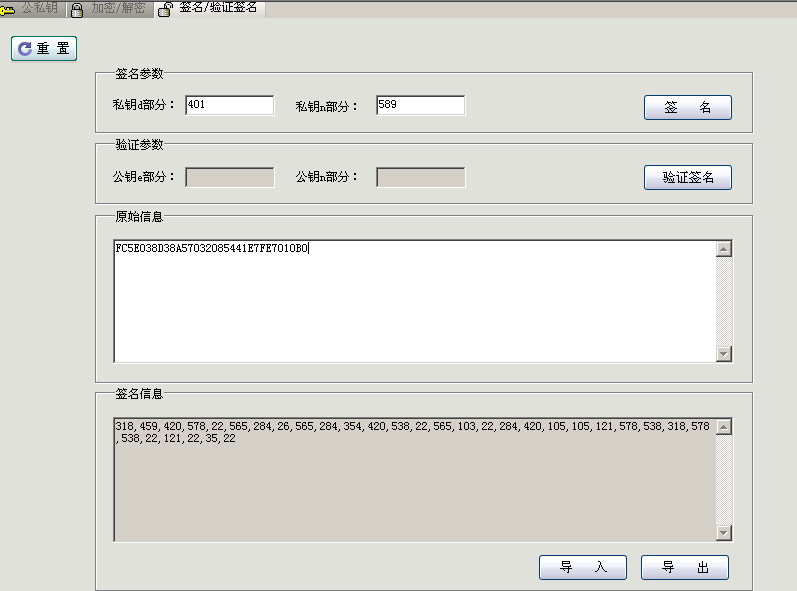
5. 主机A对源文件进行数字摘要。

进入“MD5哈希函数”|“生成摘要”页签，单击“导入文件”按钮导入s.txt文件，单击“生成摘要”按钮，生成文件摘要。单击“导出”按钮，将摘要保存到数据加密文件夹中，命名为“源文件MD5摘要”。



6. 主机A对文件摘要进行数字签名。

进入“RSA加密算法”|“签名/验证签名”页签，在“签名参数”区输入自己的“私钥d”和“私钥n”,在“原始信息”中输入步骤5生成的“源文件MD5摘要”内容，单击“签名”按钮，生成签名信息。

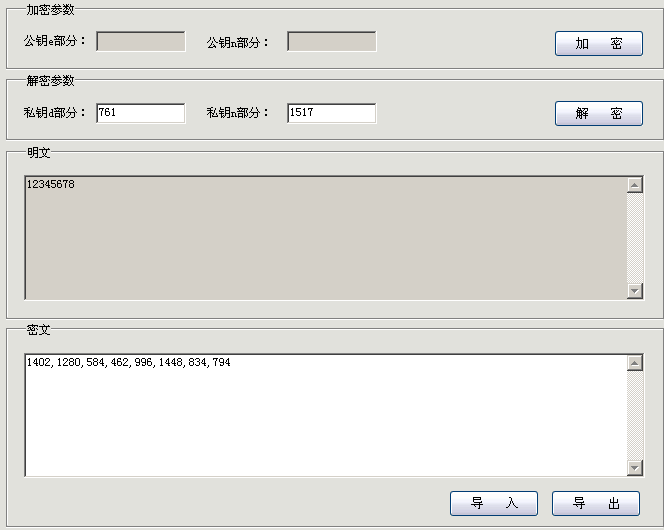


单击“导出”按钮，将签名文件保存到数据加密文件夹中，命名为“源文件数字签名”。

7. 主机A将密文“源文件密文”、加密后的会话密钥“会话密钥k密文”和数字签名“源文件数字签名”传给主机B。

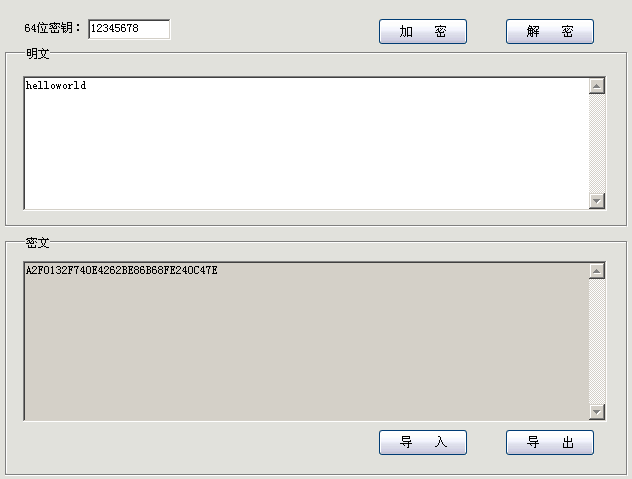
8. 主机B使用自己的私钥对会话密钥进行解密。

进入“RSA加密算法”|“加密/解密”页签，点击“解密”按钮 ，切换到解密模式，在“私钥d部分”和“私钥n部分”输入自己的私钥，单击“导入”按钮，将“会话密钥k密文”文件导入，再次点击“解密”按钮进行解密，得到准会话密钥。

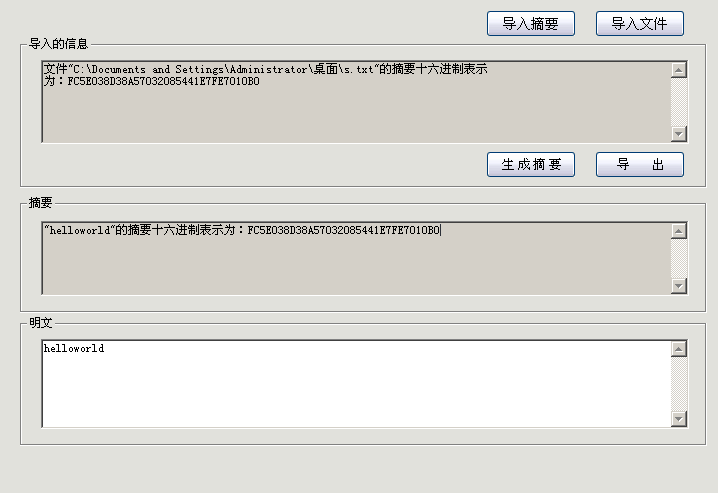


9. 主机B使用准会话密钥对得到的密文进行解密。

进入“DES加密算法”|“加密/解密”页签，在密钥窗口输入步骤8中解密后的准会话密钥，单击“导入”按钮，将“源文件密文”文件导入，点击“解密”按钮进行解密，得到准明文。

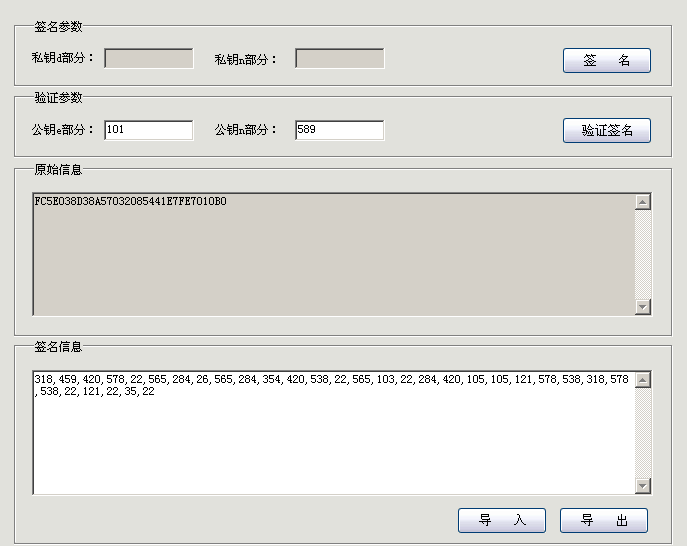


10. 主机B使用MD5哈希函数对得到的准明文进行数字摘要。



11. 主机B使用主机A的公钥验证数字签名。

进入“RSA加密算法”|“签名/验证签名”页签，单击“验证签名”按钮，切换到验证签名模式，在“验证参数”区输入主机A的“公钥e”和“公钥n”，单击“导入”按钮，导入“源文件数字签名”文件，单击“验证签名”，得到准明文摘要。



12. 将步骤10计算得到的摘要与准明文摘要进行比较，若相同则表明文件安全传输成功。

(对以上过程贴图并进行说明)

思考问题：

1. 实验步骤中，哪些步骤实现了信息传输的保密性、完整性和不可否认性。

在A中步骤1,2体现了信息传输的保密性；

在B中3体现了传输信息的不可否认性；

在B中的5体现了信息的完整性

2. 为什么不直接应用非对称加密算法对明文进行加密传输，而是使用对称加密算法完成对明文的加密工作。

1. 因为直接使用非对称加密算法进行加密不能保证通信双方的身份，因为公钥有可能被第三方知道，从而违背了信息传输中不可否认性的要求；
2. 使用对称加密算法对明文加密是因为它能更好的实现数字签名，从而保证信息的完整性，并且可以保证传输信息的不可否认；