华东师范大学计算机科学技术系上机实践报告

课程名称：计算机网络	**年级：**2022	**上机实践成绩：**
指导教师：洪道诚	**姓名：**朱宇笑	**创新实践成绩：**
实验名称：远程登陆与文件传输协议	**学号：**10225001410	**上机实践日期：**2023/12/29
座位编号：F	**组号：**6	**上机实践时间：**2 学时

一、 实验目的

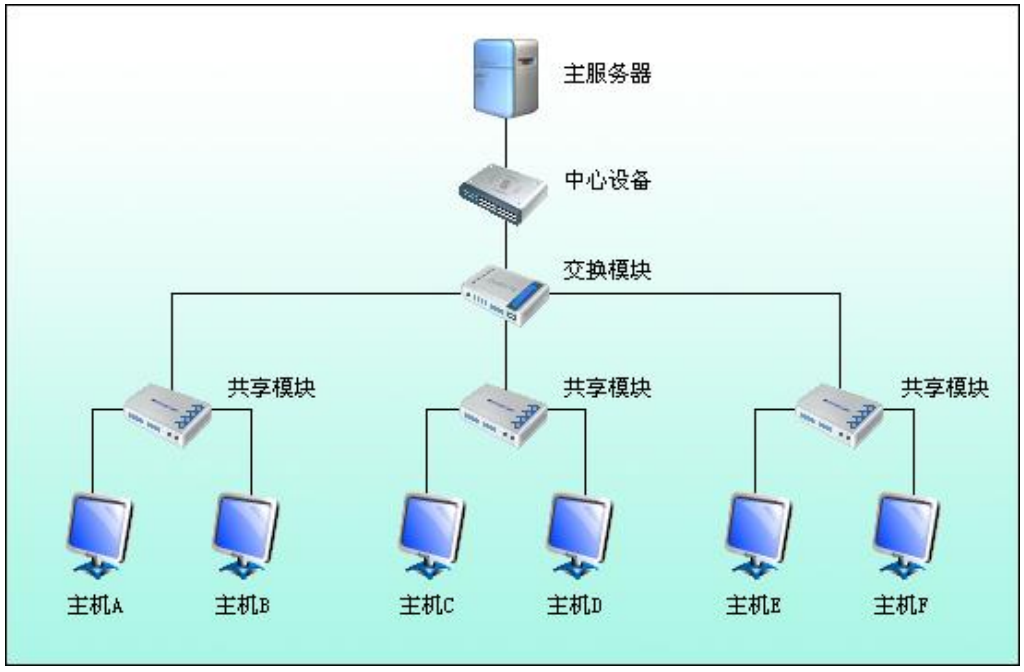
1. 掌握ARP协议的报文格式掌握TELNET的工作过程
2. 理解TELNET选项协商
3. 掌握FTP的工作原理
4. 掌握FTP一些常用命令的使用方法及用途

二、 实验设备

1. PC机
2. 仿真编辑器
3. 协议分析器

三、 实验原理

实验采用网络结构一



一．分时系统

在分时系统中，计算机支持多个用户。用户使用由键盘、鼠标和监视器组成的终端与分时系统进行交互。中央计算机进行所有的计算。当用户在键盘上键入字符时，这个字符发送到计算机，同时回送到监视器。分时系统使用户有专用计算机的感觉。用户可以运行程序，使用系统资源，从一个程序切换到另一个程序，等等。

二．本地登录与远程登录

在分时系统中，用户是系统的一部分，具有使用资源的权利。每一个授权用户都有一个标识，也可能还有一个口令。用户标识定义用户是系统的一部分。要接入到系统，用户要使用用户标识或登录名字登录到系统。系统对用户口令进行检查以防止非授权用户使用资源。

I．本地登录

用户登录到本地的分时系统叫做本地登录。用户在终端上进行操作，该操作被终端驱动程序接受。接着操作系统就解释字符的组合，并调用所需的应用程序，如下图所示：

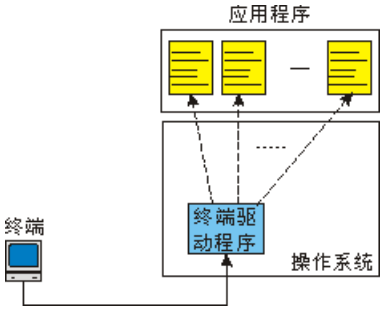


图 13-1 本地登录

2．远程登录

用户登录到远程主机并使用远程主机的应用程序，这叫做远程登录。远程登录一般要使用 TELNET 客户程序和服务器程序。用户把自己的击键发送给终端驱动程序，本地操作系统接受这些字符，但并不解释它们。这些字符被送到 TELNET 客户。然后，TELNET 客户把这些字符转换成叫做网络虚拟终端字符的通用字符集，再把它放入本地 TCP/IP 栈，如下图所示：

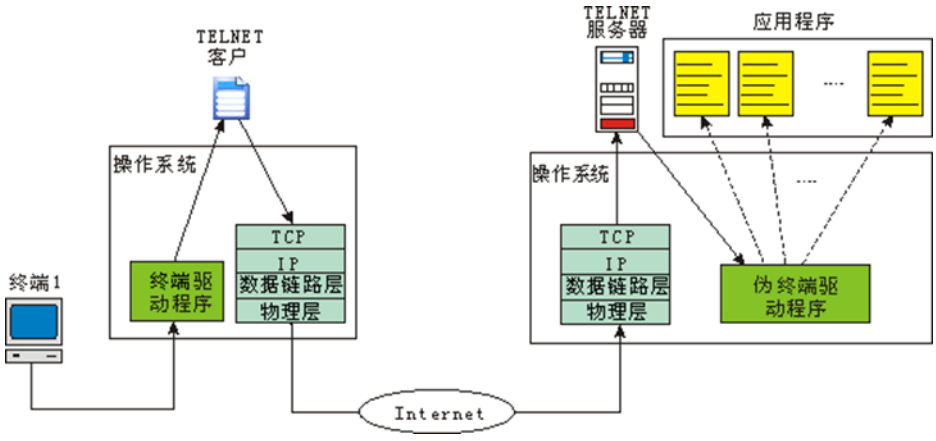


图 13-2 远程登陆

网络虚拟终端形式的命令或文字，通过Internet到达远程主机的TCP/IP栈。字符被交付给操作系统，

然后递交给TELNET服务器，TELNET服务器再把这些字符转换为远程计算机可理解的相应字符。这些字符不能直接交给操作系统，远程的操作系统不能接收来自TELNET服务器的字符（它只能接收来自终端驱动程序的字符）。TELNET服务器使用伪终端驱动程序将这些字符伪装成好像是从一个终端发来的。然后操作系统将这些字符传递给适当的应用程序。

三．网络虚拟终端

接入到远程计算机的过程是很复杂的，这是因为不同的操作系统接受特殊的字符组合是不同的。例如，在 Windows 操作系统的计算机中，文件结束标记是 Ctrl+z，而在 UNIX 操作系统中则是 Ctrl+d。

TELNET 使用网络虚拟终端(NVT)字符集来处理异构系统的远程登录问题。网络虚拟终端(NVT)字符集是一个通用接口，通过这个接口，客户 TELNET 把来自本地终端的字符（数据或命令）转换成 NVT 形式，然后交付给网络。而服务 TELNET 把来自 NVT 形式的字符（数据或命令）转换成计算机可接受的形式。下图给出了 NVT 字符集的概念。

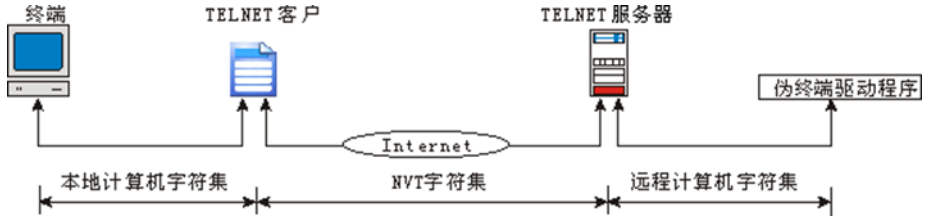


图 13-3 NVT 的概念

四．TELNET 简介

TELNET 是一种终端仿真技术，它提供了一种通过网络操作远程主机方法。TELNET 使用面向字节的双向通信，服务器通常使用 TCP 的 23 端口，客户端使用动态端口。TELNET 协议可以工作在任何主机和任何终端之间，它使用 TCP/IP 在远程计算机上登录并执行命令。

五．NVT 字符集

NVT 使用两个字符集，一个为数据字符集，另一个为远程控制字符集。

1．数据字符

对于数据，NVT 通常使用 NVTASCII。这是 8 位字符集，其中低 7 位和 USASCII 是一样的，但是最高位是 0。虽然这也可以使用 8 位的 ASCII（最高位可以是 0 或 1），但这必须在客户和服务器之间使用选项协商取得一致，如下图所示：

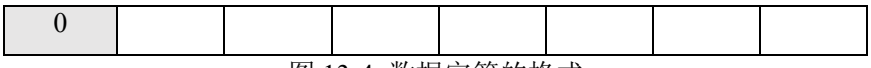


图 13-4 数据字符的格式

2．远程控制字符

远程控制字符用千在客户与服务器之间发送控制字符，NVT 使用 8 位字符集，其最高位置为 1。如下图所示：

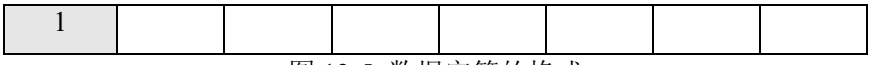


图 13-5 数据字符的格式

下表列举了一些远程控制字符及其意义。

表 13-1 某些 NVT 远程控制字符

字符	十进制	十六进制	意义
Echo	1	0x01	回显
Suppressgo_ahead	3	0x03	向前抑制
Status	5	0x05	状态
Terminal_type	24	0x18	终端类型
Negotiateaboutwindowsize	31	0x1f	窗口尺寸协商
Terminalspeed	32	0x20	终端速度
Remoteflowcontrol	33	0x21	远程溢出控制
Xdisplaylocation	35	0x23	X 显示定位
authentication	37	0x25	认证
encrypt	38	0x26	数据加密
Newenvironment	39	0x27	新环境
EOF	236	0xEC	文件结束
EOR	239	0xEF	记录结束
SE	240	0xF0	子选项结束
NOP	241	0xF1	无操作
DM	242	0xF2	数据标记
BRK	243	0xF3	断开
IP	244	0xF4	中断过程
AO	245	0xF5	异常终止输出
AYT	246	0xF6	对方是否还在运行
EC	247	0xF7	擦除字符
EL	248	0xF8	擦除行
GA	249	0xF9	前进
SB	250	0xFA	子选项开始
WILL	251	0xFB	同意允许（enable）选项
WONT	252	0xFC	拒绝允许选项
DO	253	0xFD	认可选项请求
DONT	254	0xFE	拒绝选项请求
IAC	255	0xFF	解释（下一个字符）为控制

六．TELNET 选项协商

TELNET 允许客户与服务器在使用服务之前或使用服务过程中进行选项协商。对千复杂的终端用户，选项协商能提供额外的特性。对于较简单的终端用户，选项协商只能使用较少的特性。一些远程控制字符

可用来定义选项。

下面是选项的描述：

二进制：这个选项允许将收到的除 IAC 之外的每个 8 位字符解释为二进制数据。当收到 IAC 时，它的下一个或下几个字符被解释为命令。如果收到的两个连续的 IAC 字符， 则丢弃第一个 IAC 字符，然后把第二个解释为数据。

回显：这个选项允许服务器回显收到的来自客户的数据。客户向发送器发送的每一个字符都将回显到客户终端的屏幕上。这时，用户终端通常在字符被键入时并不回显，而要等到服务器收到它们后才回显。

抵制前进：这个选项抑制前进字符(GA)。

状态：这个选项允许用户或客户机器上运行的进程得到在服务器端被允许的选项状态。

定时标记：这个选项允许一方发出定时标记，指出所有以前收到的数据都已被处理。

终端类型：这个选项允许客户发送它的终端类型。

终端速率：这个选项允许客户发送它的终端速率。

行方式：这个选项允许客户切换到行方式。

1．选项协商

要使用前面介绍的选项，就需要在客户与服务器之间进行选项协商。选项协商需要使用四种控制字符。这些字符如下表所示：

表 13-3 选项协商控制字符

字符	十进制	二进制	意义
WILL	251	11111011	(1)提供允许选项 (2)接受请求允许选项
WONT	252	11111100	(1)拒绝请求允许选项 (2)提供禁止选项 (3)接受禁止选项
DO	253	11111101	(1)同意提供允许选项 (2)请求允许选项
DONT	254	11111110	(1)不同意提供允许选项 (2)同意提供禁止选项 (3)请求禁止选项

(1)允许选项

一些选项仅能由服务器允许，另一些仅能由客户允许，还有一些则可由服务器或客户允许。选项要被允许需通过提供允许或请求允许来实现。

·提供允许

如果一方有权限，它可以提供允许选项。对方可以同意或不同意这个提供。提供方发送 WILL 命令，表示“我能允许这个选项吗？”。另一方可以发送 DO 命令，表示“同意”或发送 DONT 命令，表示“不同意”。如下图所示：

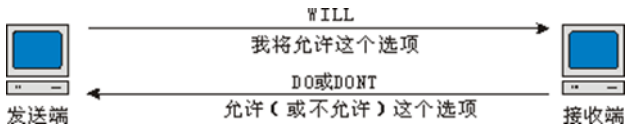


图 13-6 提供允许选项、

·请求允许

一方可以请求另一方允许选项。另一方可以接收或拒绝这个请求。请求方发送 DO 命令，表示“请允许这个选项”。另一方可以发送 WILL 命令，表示“同意”，或发送 WONT 命令，表示“我不同意”。如下图所示：

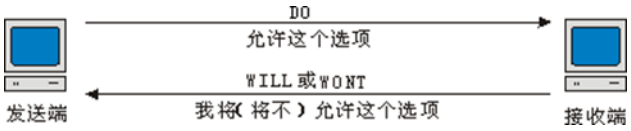


图 13-7 请求允许选项

(2)禁止选项

已经被允许的选项可以被一方禁止掉。可以通过提供禁止或请求禁止来禁止选项。

·提供禁止

一方可以提供禁止选项。另一方必须同意这个提供。提供方发送 WONT 命令，表示“我不再使用这个选项 " 。回答必须是 DONT 命令，表示“不要再使用这个选项”。如下图所示：

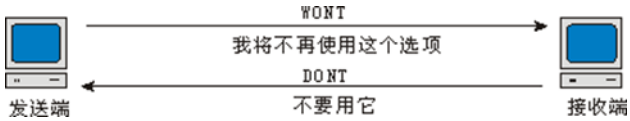


图 13-8 提供禁止选项

·请求禁止

一方可以请求另一方禁止选项。另一方必须接受这个请求。请求方发送 DONT 命令。表示“请不要再使用这个选项”。回答必须是 WONT 命令，表示“我不再使用它”。如下图所示：

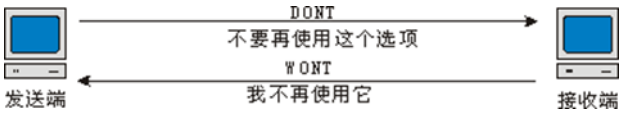


图 13-9 请求禁止选项

2. 子选项协商

一些选项需要附加的信息。例如，要定义终端的类型或速率，协商就要包括字符串或数字来定义类型或速率。下表所示的两个子选项字符是用来进行选项协商的。

表 13-4 子选项协商的 NVT 字符集

字符	十进制	二进制	意义
SE	240	11110000	子选项结束
SB	250	11111010	子选项开始

下图所示的例子中，客户将终端的类型设置为 VT。

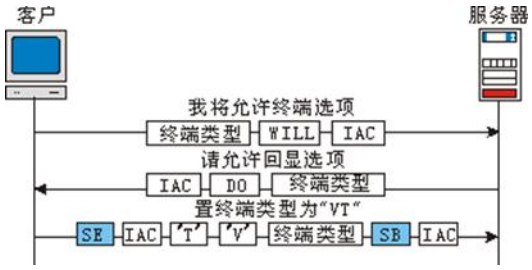


图 13-10 子选项协商的例子

七．FTP 协议简介

FTP（文件传输协议）提供了一种通过 TCP 传送文件的方法，可以将一个文件从一个系统复制到另一个系统中。FTP 使用两种 TCP 连接：一种是控制连接，一种是数据连接。控制连接一直持续到客户端和服务器端进程间的通信完成为止，用千传输控制命令，服务器使用 21 端口；数据连接根据通信的需要随时建立和释放，用于数据的传输，服务器常使用 20 端口。FTP 的连接模式有两种：主动模式(PORT)和被动模式(PASV)。

八．FTP 连接、通信与传送

I．连接

FTP 的控制连接和数据连接使用不同的方法和不同的端口号。

(1)控制连接

控制连接的创建步骤如下：

·服务器在熟知端口 21 发出被动打开，等待客户。

·客户使用临时端口发出主动打开。

在整个过程中这个连接一直是打开的。这是客户和服务器的交互式连接，所以 IP 协议使用的服务类型是最小延迟。用户键入命令并期望收到的响应延时不太大。下图给出了服务器和客户之间的初始连接：

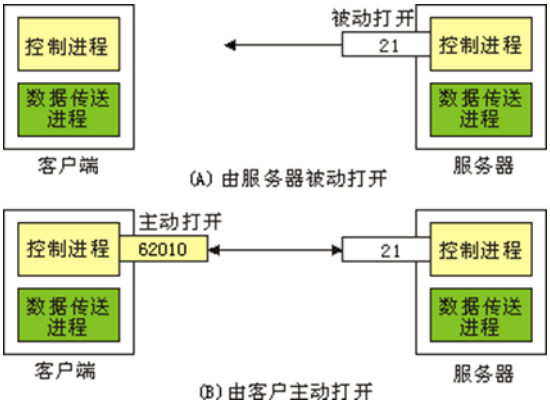


图 13-11 打开控制连接

(2) FTP 数据连接的两种模式

FTP 的数据连接存在两种模式：主动模式(PORT)和被动模式(PASV)。主动模式是从服务器端向客户端发起连接；被动模式是客户端向服务器端发起连接。

当 FTP 被设置为主动模式时，它的连接过程如下：首先客户端向服务器的 FTP 端口（默认是 21）发

送连接请求，服务器接受连接，建立一条控制连接。当需要传输数据时，客户端在控制连接上用 PORT 命令告诉服务器：“我打开了 XXXX 端口，你来连接我”。千是服务器从 20 端口向客户端的 XXXX 端口发送连接请求，最后建立一条数据连接来传输数据。

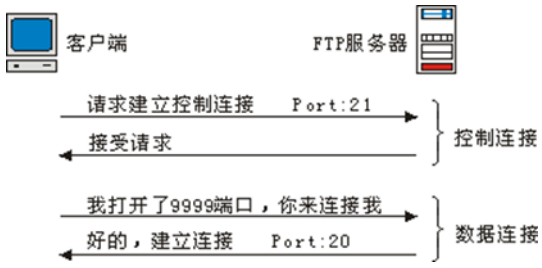


图 13-12 FTP 的主动模式

当 FTP 被设置为被动模式时，它的连接过程如下：首先客户端向服务器的 FTP 端口（默认是 21）发送连接请求，服务器接受连接，建立一条控制连接。当需要传输数据时，服务器在命令链路上用 PASV 命令告诉客户端：“我打开了 XXXX 端口，你来连接我”。于是客户端向服务器的 XXXX 端口发送连接请求，最后建立一条数据连接来传输数据。

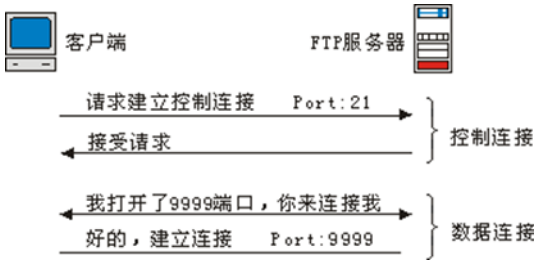


图 13-13 FTP 的被动模式

当进行 FTP 连接时，Internet Explorer 通常被设置为被动模式，而 FTP 客户端软件（如：Flash FXP，Cute FTP)一般为主动模式。如果服务器和客户端之间存在防火墙，主动模式经常会引起一些麻烦。例如：客户端位与防火墙之后，通常防火墙允许所有内部向外部的连接通过，但是对于外部向内部发起的连接却存在很多限制。在这种情况下，客户可以正常地和服务器建立控制连接，而如果使用主动模式的数据连接，一些数据传输命令就很难成功运行，因为防火墙会阻塞从服务器向客户端发起的数据传输连接。因此在使用主动模式的 FTP 数据连接时，防火墙上的配置会比较麻烦。

2．通信

(1)在控制连接上的通信

FTP 使用 NVTASCII 字符集在控制连接上通信，如下图所示。通信过程使用命令和响应来完成。命令和响应都是一个短行，因此不必考虑它的文件结构。每一行以回车和换行组成的结束记号结束。

图 13-14 使用控制连接

(2)在数据连接上的通信

数据连接用来传送数据，在传送数据之前，客户需要使用控制连接来做传输的准备。客户需要定义要传送的文件类型、数据结构以及传输方式。如下图所示：

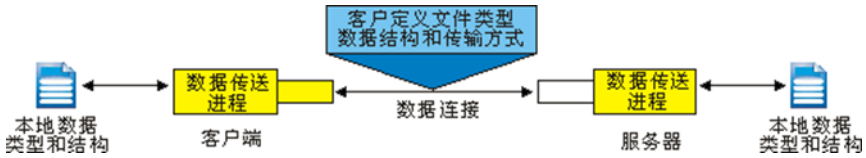


图 13-15 使用数据连接

①文件类型

FTP 能够在数据连接上传送下列文件类型中的一种：

• ASCII 文件：这是传送文本文件的默认格式。每一个字符使用 NVTASCII 进行编码。发送端把文件从它自己的表示转换成 NVTASCII 字符，而接收端从 NVTASCII 字符转换成它自己的字符。

• EBCDIC 文件：若连接的一端或两端使用 EBCDIC 编码，则可使用 EBCDIC 编码传送文件。

• 图像文件：这是传送二进制文件的默认格式。这种文件是作为连续的位流传送而没有任何解释或编码。在大多数情况下它用来传送二进制文件，如已编译的程序。

②数据结构

在数据连接上传送文件时，FTP 可以使用下列数据结构中的一种：

• 文件结构（默认）：这种文件没有结构。它是连续的字节流。

• 记录结构：这种文件划分为一些记录，这只能用千文本文件。

• 页面结构：这种文件划分为一些页面，每一个页面有页面号和页面首部。页面可以随机地或顺序地进行存取。

③传输方式

FTP 可以使用下列传输方式之一在数据连接上传送文件：

• 流方式：这是默认方式。数据作为连续的字节流从 FTP 交付给 TCP。TCP 负责把数据划分为适当大小的报文。若数据是简单的字节流（文件结构），就不需要文件结束符。若数据划分为记录（记录结构），则每一个记录有 1 字节的记录结束(EOR)字符，而在文件的结束处有文件结束(EOF)字符。

• 块方式：数据可以按块从 FTP 交付给 TCP。每一个块的前面有 3 字节首部。第一个字节叫做块描述符，后两个字节定义块的大小，以字节为单位。

• 压缩方式：若文件很大，数据可进行压缩。通常使用的压缩方法是游程长度编码。数据单元的连续出现数可以用一个“出现“和“重复数”来替换。在文本文件中，这通常是空格。在二进制文件中，空字符常常被压缩。

3．文件传送

在控制连接命令的控制下，在数据连接上进行文件传送，如下图所示：

图 13-16 文件传送

FTP 的文件传送有三种动作：

• 从服务器把文件复制到客户端叫做读取文件。读取文件是在 RETR 命令的监督下完成的。

• 从客户端把文件复制到服务器叫做存储文件。存储文件是在 STOR 命令的监督下完成的。

• 从服务器向客户端发送目录列表或文件名。这是在 LIST 命令的监督下完成的。FTP 把目录或文件名列表当作文件，在数据连接上发送。

九．FTP 命令与响应

FTP 使用控制连接在客户进程和服务器进程之间建立连接进行通信。在通信时，客户向服务器发送命令，服务器给客户返回响应，如下图所示：

图 13-17 命令的处理

四、 实验步骤

练习 1 运行 TELNET 命令，捕获数据并分析

在实验中每组 A~F 主机的接口 IP 地址分别设置为 172. 16. 0. n1、172. 16. 0. n2、172. 16. 0. n3、172. 16. 0. n4、172. 16. 0. n5、172. 16. 0. n6（其中 n 为组别号，取值范围为 1~12），子网掩码设置为 255. 255. 0. 0，默认网关设置为空。

本练习一人一组，现仅以主机 A 为例，其它主机参考主机 A 的操作。

1．主机 A 启动协议分析器进行数据捕获，并设置过滤条件（提取 TELNET 协议）。

2．主控中心服务器(IP 地址为 172. 16. 0. 253)上的 telnet 服务已经启动，使主控中心平台为本小组提供的帐号，其用户名：group1_1,密码：group1_1。

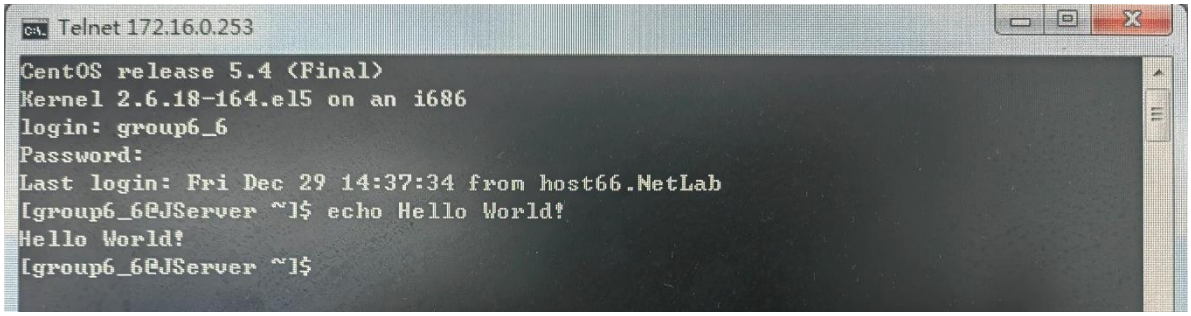
注：用户名、密码相同，规则是：groupx_y（这里 x 是组索引，y 是主机索引，例如第一组的主机 C 使用的用户名和密码为：group1_3）。

主机 A 在命令行提示符下运行：

(1) telnet 172. 16. 0. 253。

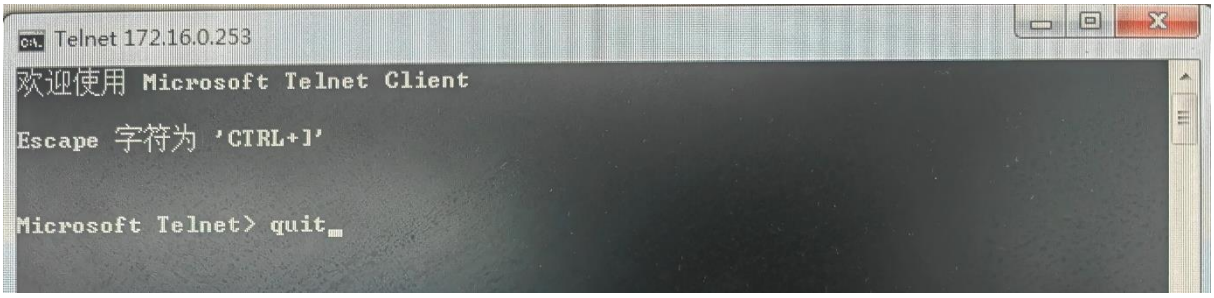
(2) 在“Login: ”提示符后输入用户名（group1_1）。在“Password: ”提示符后输入密码（group1_1）。

(3) 在虚拟终端上进行一些简单的操作（可不作）。



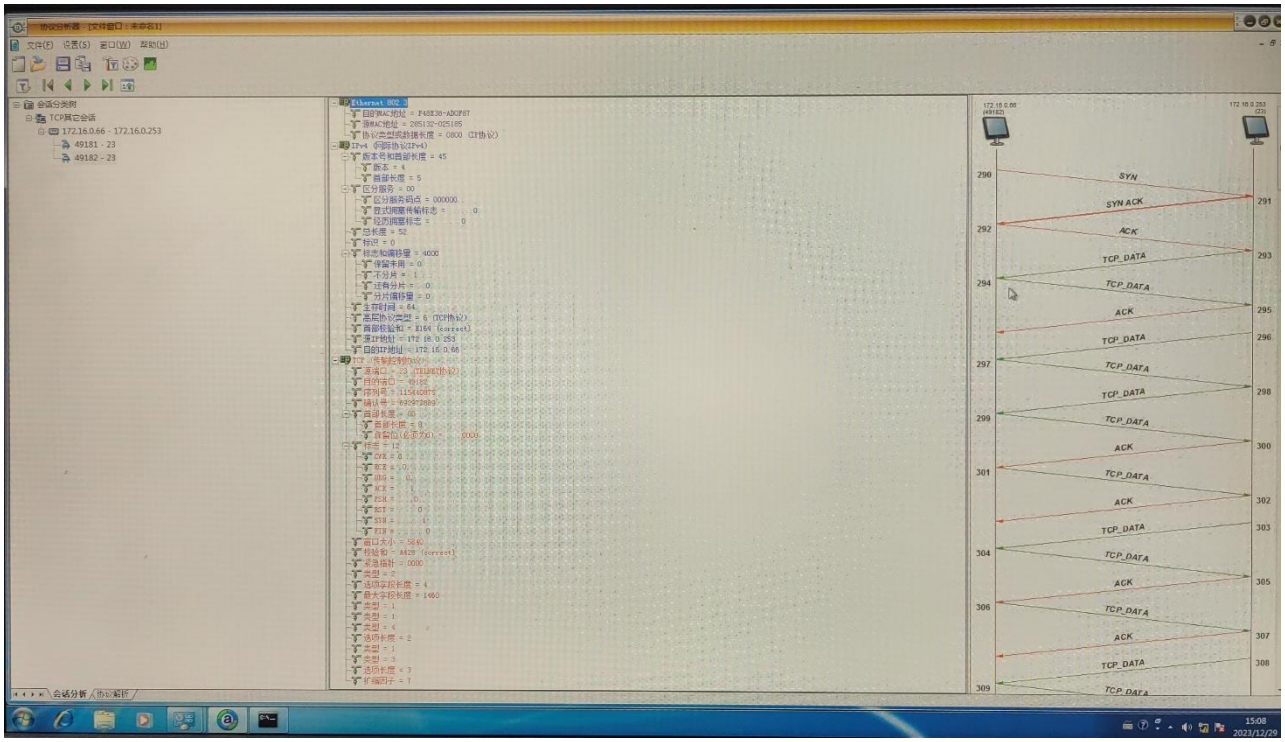
(4) 按“CTRL＋]”回到 telnet 提示符下。

(5) 输入“quit”退出 telnet。



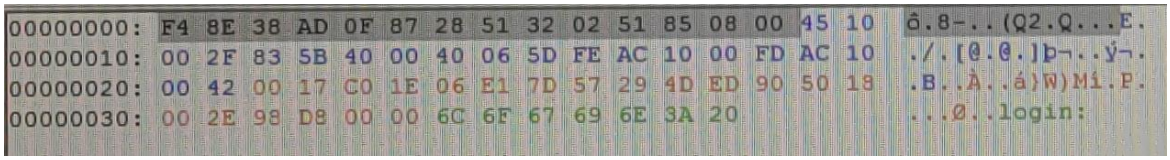
注：如果本机未安装 telnet 工具，请点击“开始→控制面板→程序和功能→打开或关闭 Windows 功能”，将“Telnet 客户端”前面打钩，点击“确定”便可。

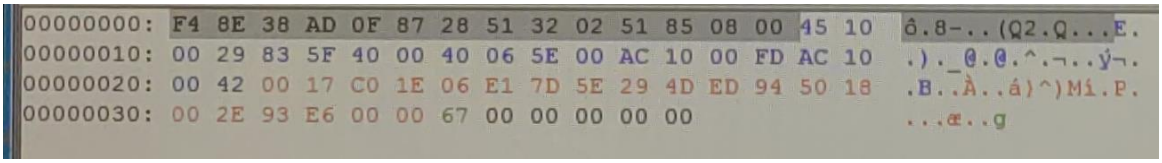
3．察看主机 A 捕获的数据，分析 TELNET 的工作过程。

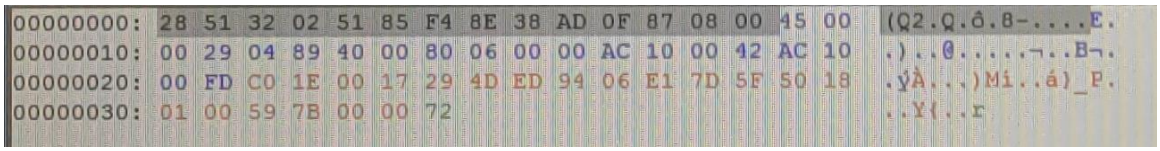


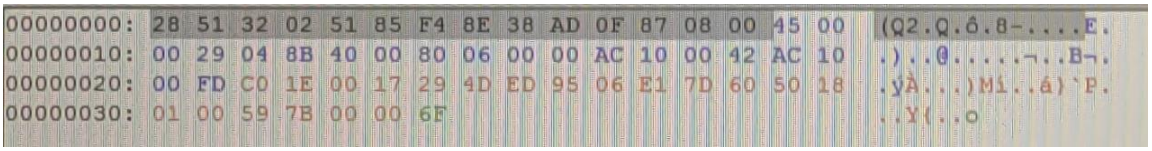
- TELNET 使用的 TCP 端口是___23___。
- 找出与选项协商有关的数据包，分析客户端与服务器端进行选项协商的过程。
- 在捕获的数据中，查找用户名和密码。

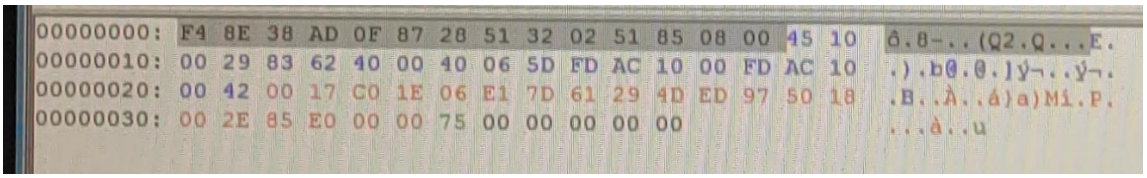
如下：

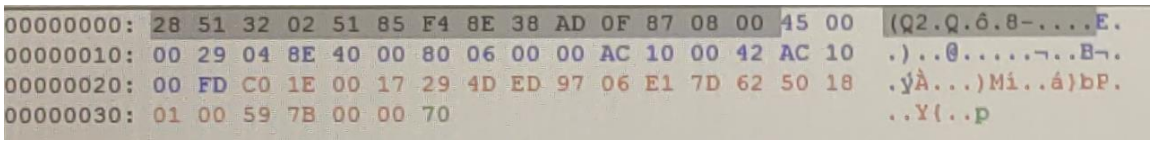


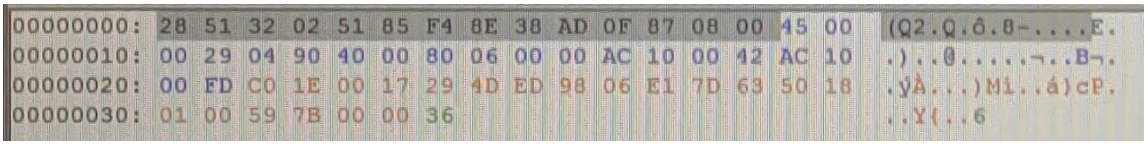


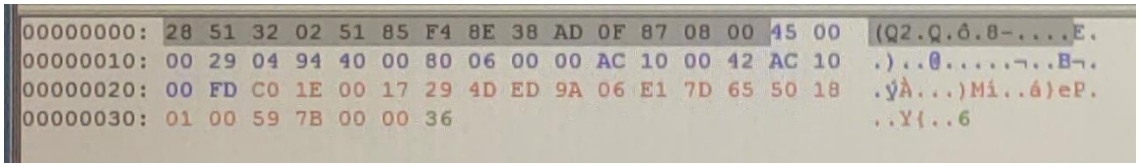












类似地，能够看到账号与密码。

- 结合分析结果，绘制 TELNET 交互图。
- 理解 TELNET 明文传输的不安全性，了解网络监听的可能。

练习 2 TELNET 选项协商的过程

本练习一人一组，现仅以主机 A 为例，其它主机参考主机 A 的操作。

1．主机 A 启动协议分析器进行数据捕获，并设置过滤条件（提取 TELNET 协议）。

2．主机 A 首先要与 TELNET 服务器建立一个 TCP 连接：

(1) 主机 A 上启动实验平台工具栏中的“TCP 工具”。

(2) 选中“客户端”单选框，在“地址”中填入服务器 IP 地址（默认 172. 16. 0. 253）。

(3) 在“端口”中填入 TELNET 协议的端口号 23。

(4) 点击［连接］按钮进行连接。

3．使用 TELNET 的 NVT 字符集实现选项协商。

在发送数据（十六进制）窗口编辑并发送以下数据：

FFFB18FFFB1F 点击“发送”按钮；

FFFC20FFFC23FFFB27 点击“发送”按钮；

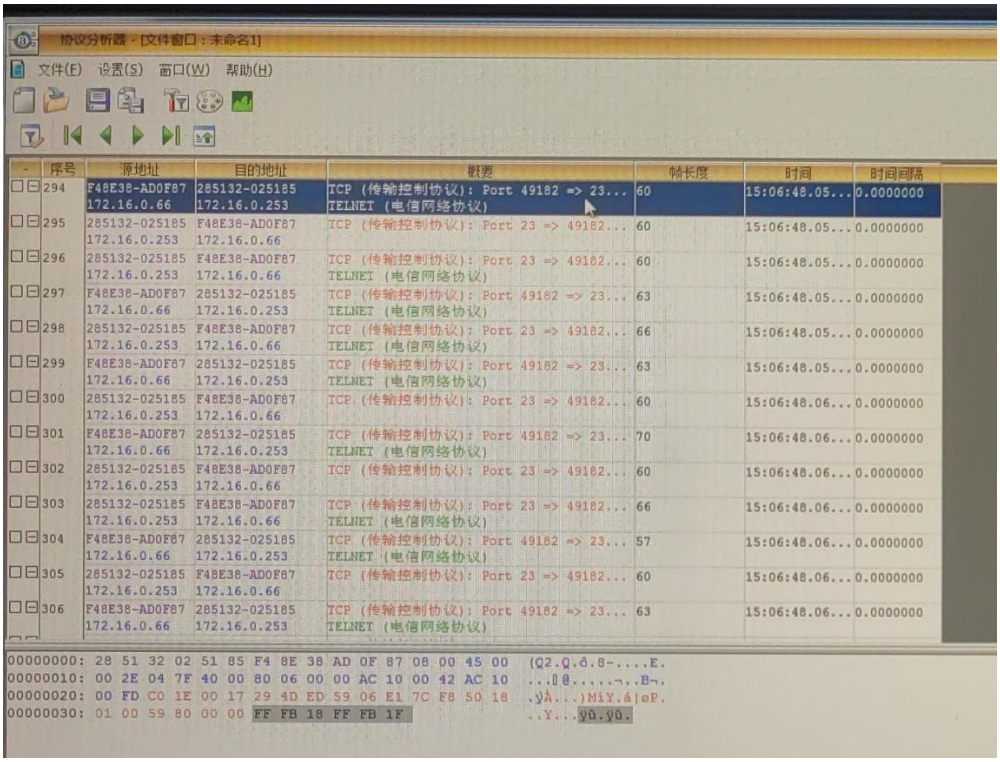
FFFD03 点击“发送”按钮；

FFFB01FFFE05FFFC21 点击“发送”按钮；

4．点击“断开”按钮，断开主机 A 与服务器的 TCP 连接。

5．察看主机 A 捕获到的数据，分析选项协商的过程。

- 写出步骤 3 中每个十六进制字符对应的 NVT 字符。
- 说明步骤 3 中发送的每个数据各自的作用和服务器端对其应答的内容。

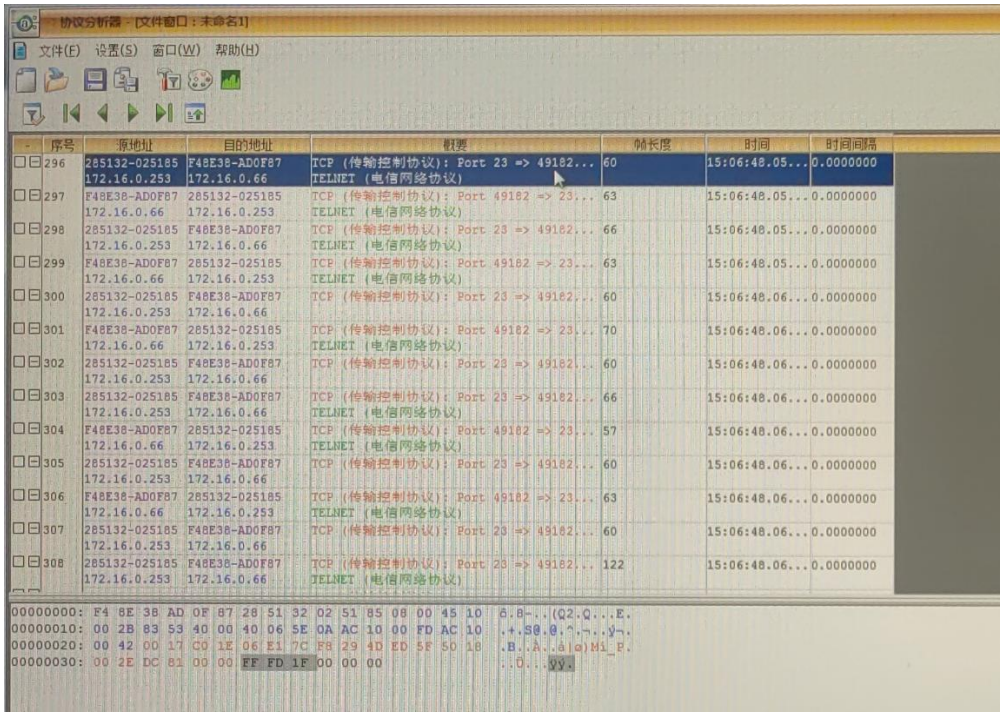


FF FB 18: IAC WILL Terminal_type

客户端将要允许使用终端类型选项。

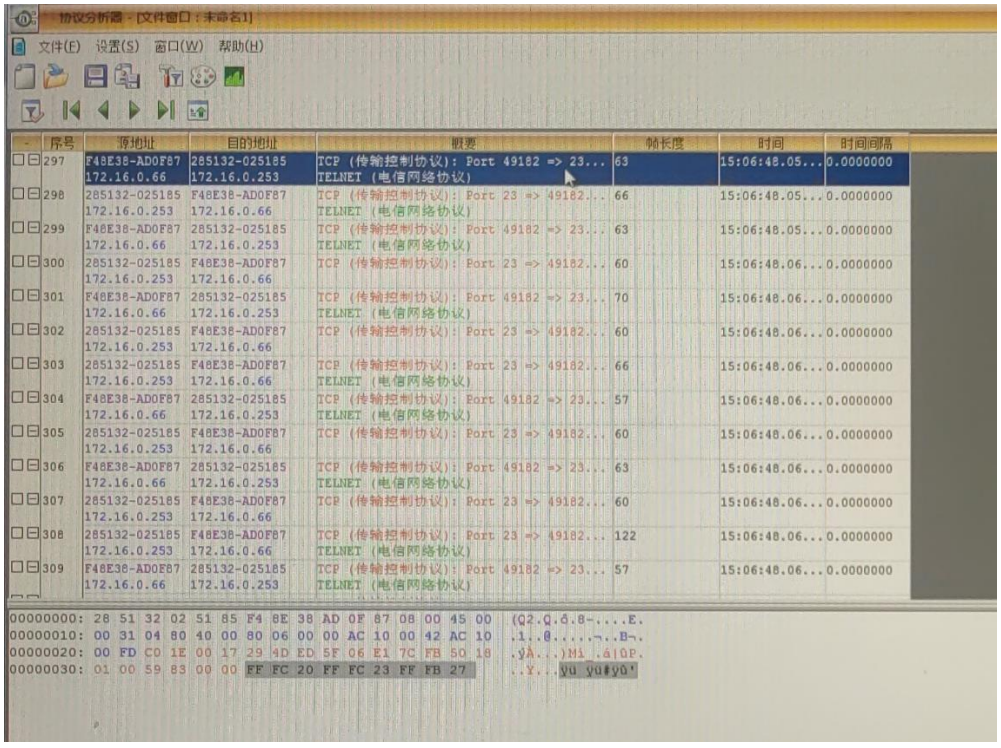
FF FB 1F: IAC WILL Negotiateaboutwindowsize

客户端将要允许使用窗口尺寸协商选项。



FF FD 1F: IAC DO Negotiateaboutwindowsize

服务器允许客户端使用窗口尺寸协商选项



FF FC 20: IAC WONT Terminalspeed

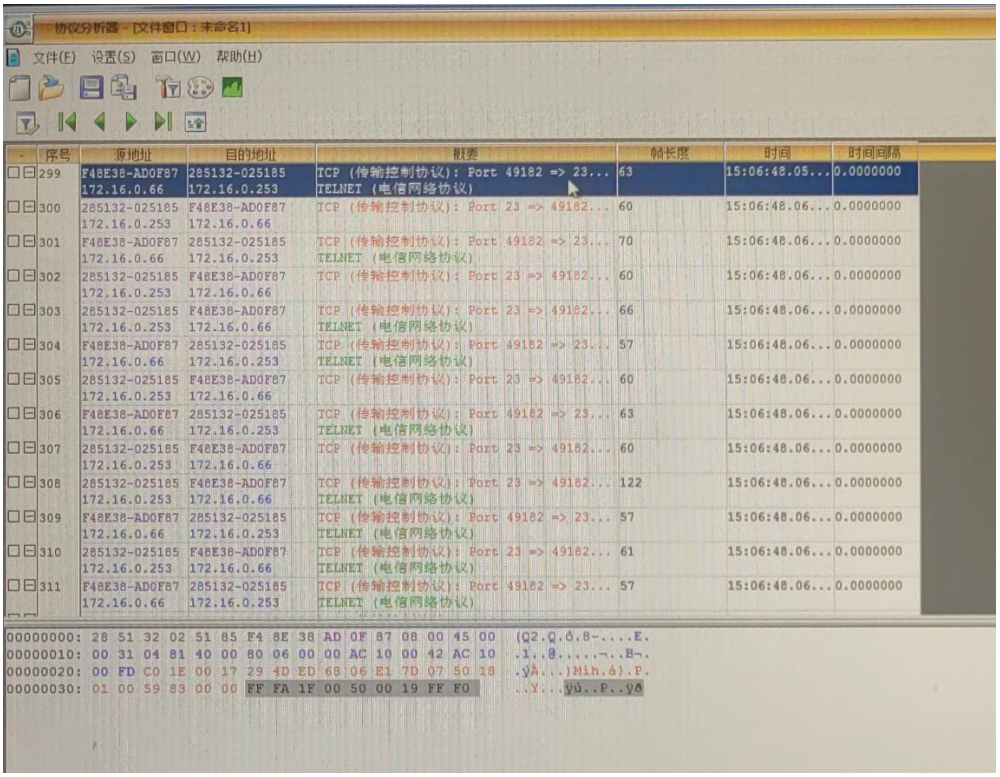
客户端将不再使用终端速度选项

FF FC 23: IAC WONT Xdisplaylocation

客户端将不再使用 X 显示定位选项

FF FB 27: IAC WILL Newenvironment

客户端将要允许使用新环境选项。

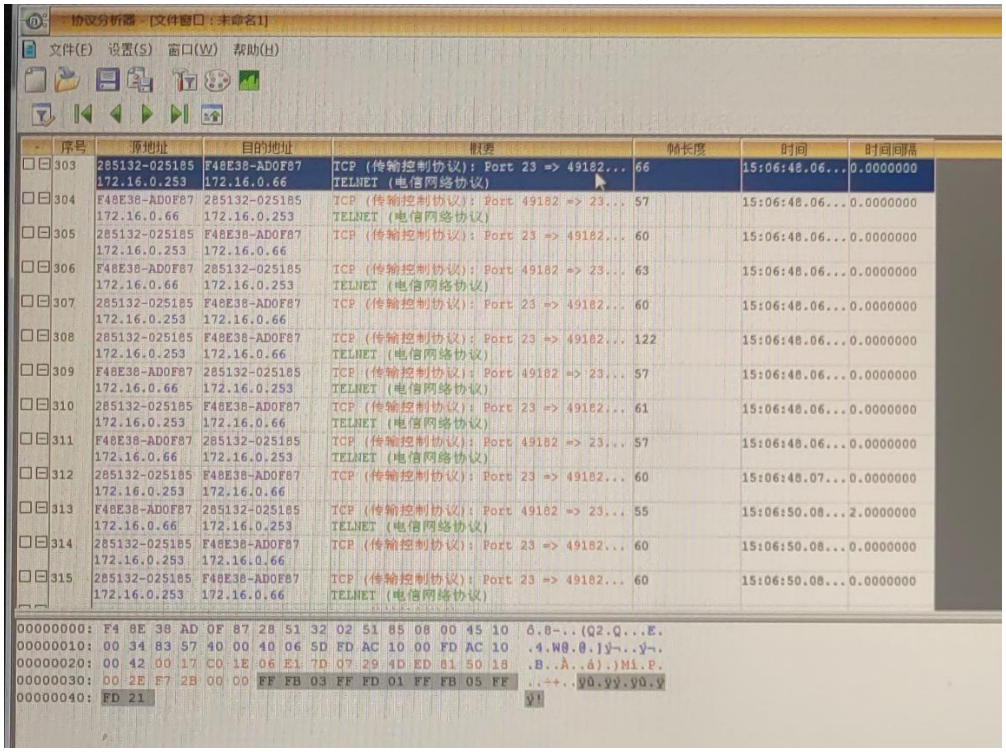


FF FA: IAC SB（子选项开始）

1F: Negotiateaboutwindowsize

00 50 00 19:（设置终端类型）

FF F0: IAC SE（子选项结束）



FF FB 03: IAC WILL Suppressgo_ahead

服务器将允许使用抑制前进选项

FF FD 01: IAC DO Echo

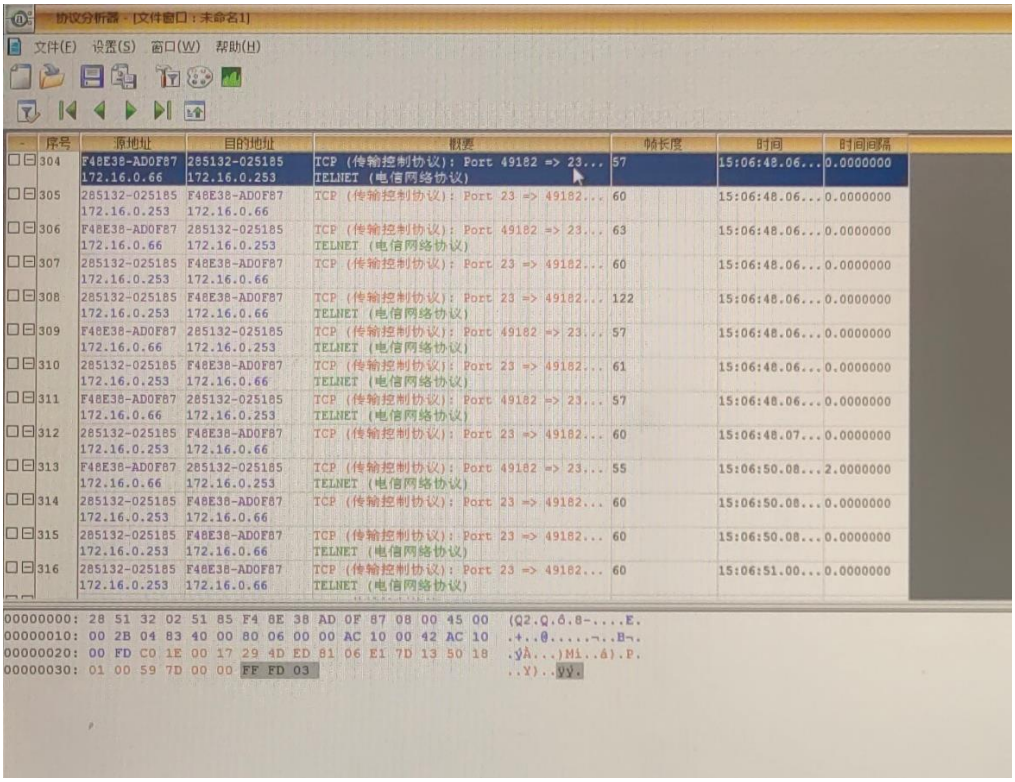
服务器允许客户端使用回显选项

FF FB 05: IAC WILL Status

服务器将允许使用状态选项

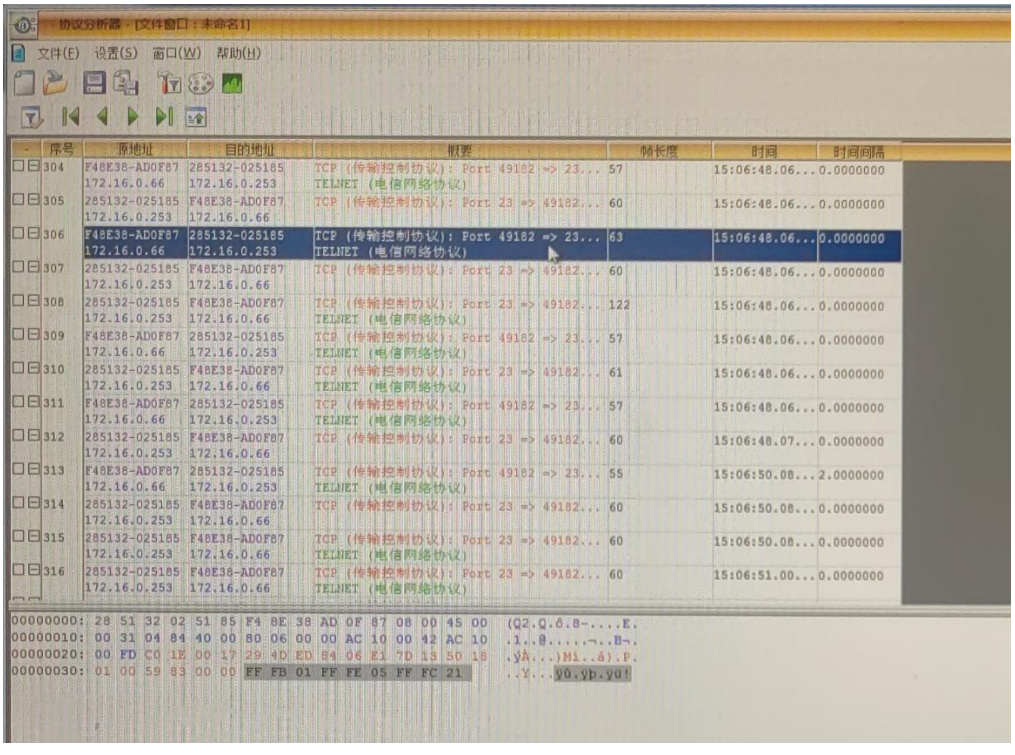
FF FD 21: IAC DO Remoteflowcontrol

服务器允许客户端远程溢出控制选项



FF FD 03: IAC DO Suppressgo_ahead

客户端允许服务器使用抑制前进选项



FF FB 01: IAC WILL Echo

客户端将允许使用回显选项

FF FE 05: IAC DONT Status

客户端不允许服务器状态选项

FF FC 21: IAC WONT Remoteflowcontrol

客户端不允许远程溢出控制选项

思考问题：

1．远程登录 TELNET 的主要特点是什么？什么叫做虚拟终端 NVT?

回答：

远程登录 TELNET 的主要特点是能够提供透明的远程连接服务。具体来说，用户可以在本地终端上通过 TCP 连接注册到远地的另一个主机上，TELNET 能将用户的击键传到远地主机，同时也能将远地主机的输出通过 TCP 连接返回到用户屏幕。这种服务是透明的，因为用户感觉到好像键盘和显示器是直接连在远地主机上。

网络虚拟终端 NVT 是网络上的所有终端对任何主机进程提供相似的接口，使网络所支持的任何终端和网络上的任何主机系统可被一起使用。它是一种虚拟的（即想象的）终端设备，被客户和服务器采用，用来建立数据表示和解释的一致性。本地终端数据在送到远程服务器之前，必须被映射（转换到）NVT。在服务器端，服务器再将 NVT 序列转化为本地格式传给应用程序。NVT 被想象为一个输出设备（显示器）和键盘，采用 8 比特字节数据，由 7 位数据加上一位标志位组成。当标志位为 1 时，表示这个字节是 NVT 命令，否则，表示这个字节为数据。NVT 能采用一些不同的终端特征，当通信开始时，通信双方都支持一个基本的终端特性子集，以便能进行最低层次的通信，在这个基础上，双方就可以协商其他的选项。在协商期间，NVT 命令在两个方向上互相发送，针对不同的选项，要用到两个基本的协商模式：“Will”和“Will not”（通告）、“Do”和“Do not”（请求或指示）。这些命令以命令解释字节（Interpret as command）开始。协商之后，数据传输的连接就建立了。

练习 3 FTP 的工作过程

本练习一人一组，现仅以主机 A 为例，其它主机参考主机 A 的操作。

1．主机 A 启动协议分析器进行数据捕获并设置过滤条件（提取 FTP data 和 FTP control 协议）。

2．主机 A 登录 FTP 服务器：

在实验环境中的服务器（默认为 172. 16. 0. 253）已经启动，并提供一个公共帐号，用户名是：anonymous，口令：无。

在命令行提示符下运行：

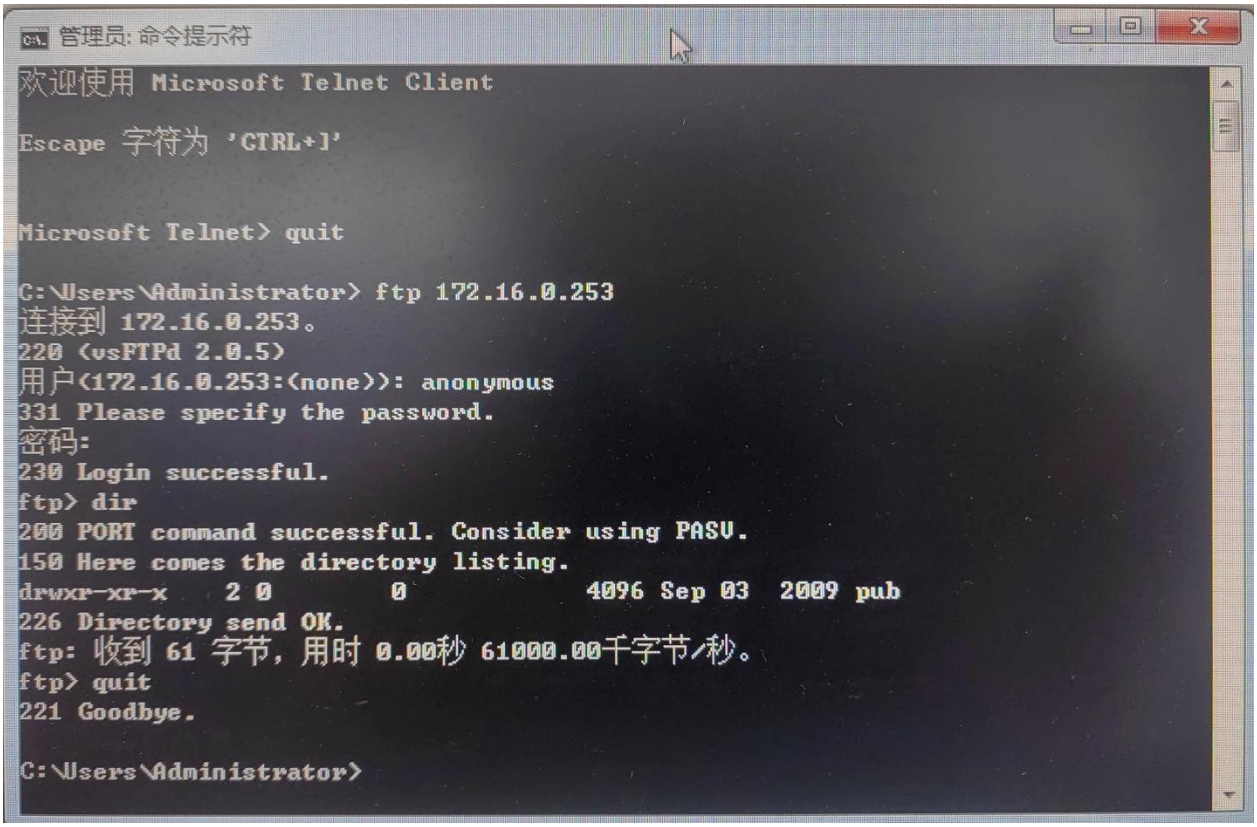
(1) C: \>ftp 172. 16. 0. 253

(2) 在“User: ”提示符后输入用户名：anonymous

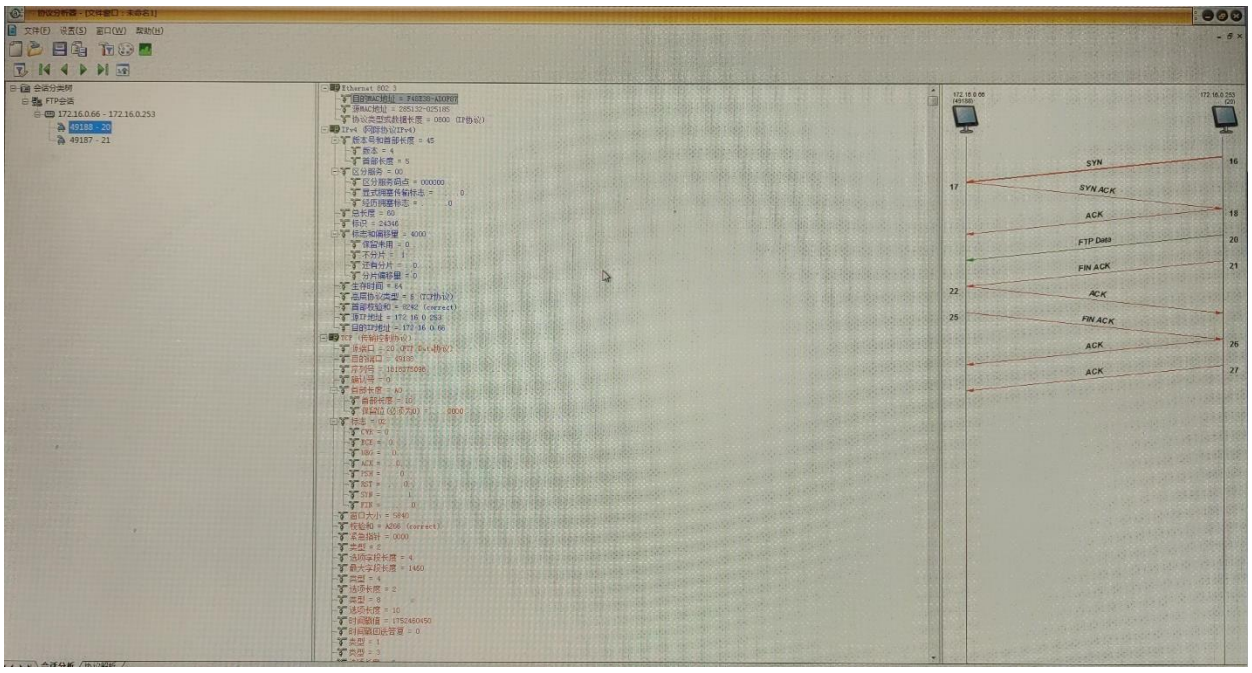
(3) 在“Password: ”提示符后输入密码：无

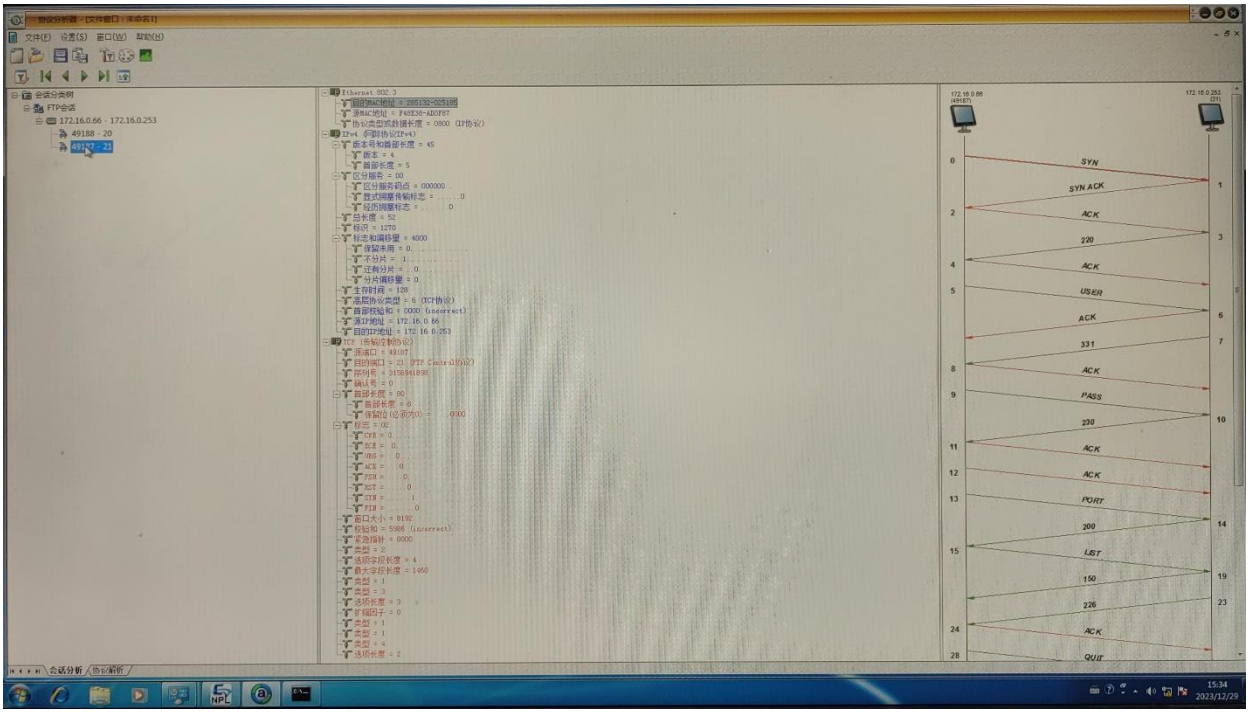
(4) 在客户端上运行一个简单的操作，如：ftp>dir

(5) 在 FTP 提示符下输入“quit”退出 FTP



3．察看主机 A 捕获的数据，通过会话交互视图分析 FTP 的工作过程：

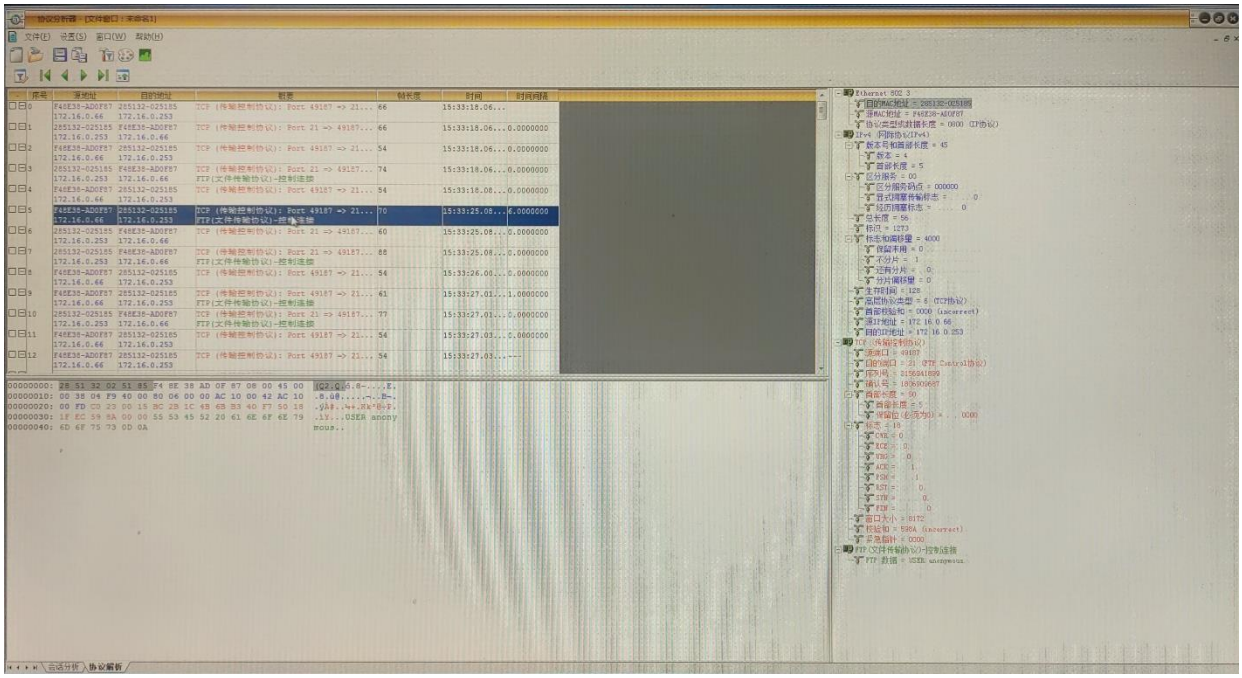


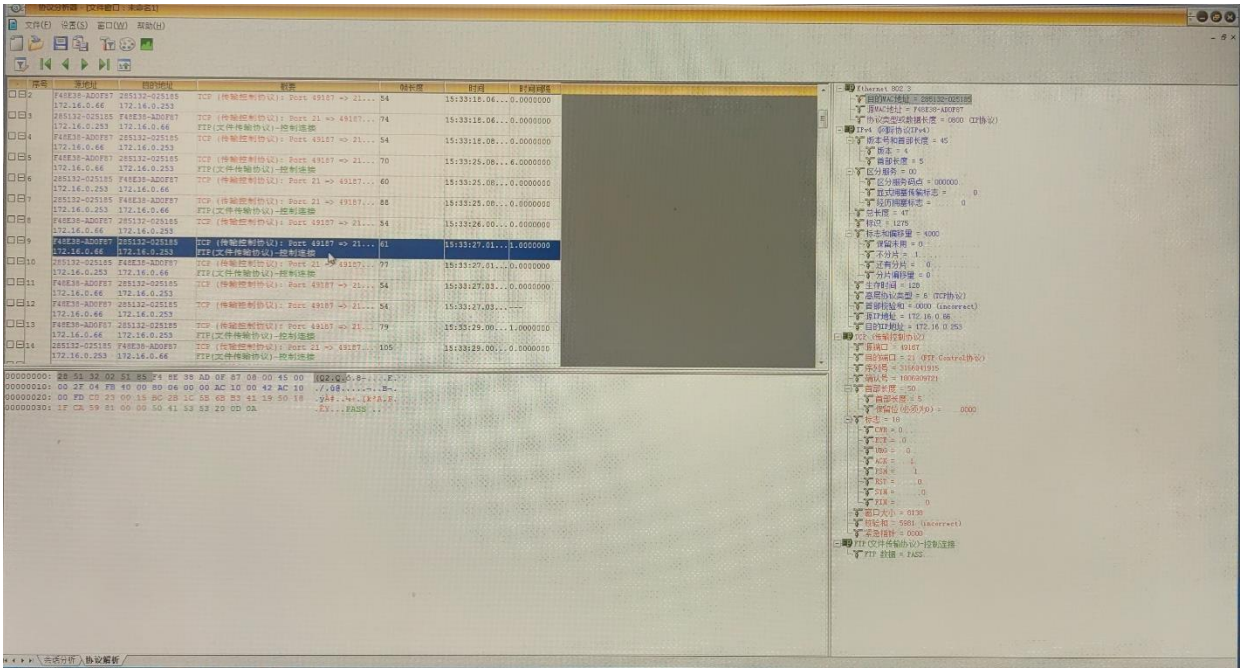


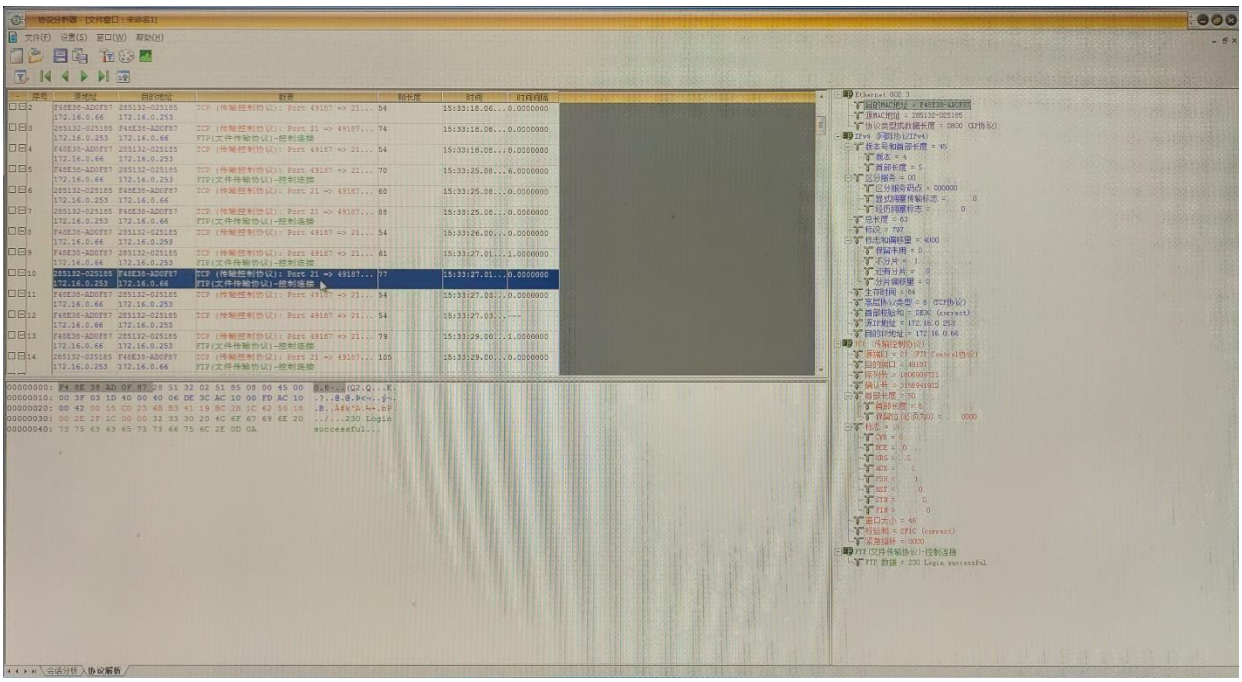
• FTP 使用的 TCP 端口有哪些？

回答：20 和 21。

• 分析 FTP 报文格式。指出在捕获的数据报文中含有用户名、密码的报文。是否可以看到用户名和密码？说明 FTP 的安全性。







回答：可以看到用户名和密码（如果有的话）。FTP 协议本身不提供加密，因此传输的数据（包括用户名和密码）都是明文的，可以被任何能够捕获网络数据包的人查看。

• 分析 FTP 的工作过程，分析控制连接和数据连接是如何工作的，绘制出控制连接和数据连接的交互过程图。

回答：在 FTP 的工作过程中，控制连接和数据连接的作用如下：

控制连接：用于传输 FTP 命令和响应。客户端通过控制连接向服务器发送命令（如“RETR”或“STOR”），并接收来自服务器的响应。控制连接在整个文件传输过程中一直保持打开状态。

数据连接：用于传输实际的数据（文件内容）。当客户端需要上传或下载文件时，它会通过数据连接进行传输。数据连接可以在主动模式或被动模式下建立。在主动模式下，客户端主动发起数据连接请求，服

务器响应请求并打开数据连接。在被动模式下，客户端发送命令到服务器，指示要传输的文件或目录，服务器响应命令并在其本地打开一个数据连接，然后客户端连接到服务器指定的端口进行文件传输。

思考问题：

1. 文件传送协议 FTP 的主要工作过程是怎样的？主进程和从属进程各起什么作用？

回答： FTP 工作过程可以分为三个阶段：建立连接、文件传输和关闭连接。在 FTP 工作过程中，首先需要建立两个连接：控制连接和数据连接。一旦控制连接建立并完成身份验证，客户端和服务器就可以开始文件传输。客户端发送一个命令（例如“RETR”或“STOR”），指示要传输的文件或目录。服务器响应这个命令，并打开一个数据连接。数据连接可以是主动模式或被动模式，这取决于 FTP 服务器的配置和网络环境。当文件传输完成后，客户端发送一个命令关闭数据连接。服务器收到命令后关闭数据连接。然后客户端和服务器之间的控制连接也关闭，完成整个 FTP 工作过程。

主进程负责监听客户端的连接请求，验证客户端的身份，并管理控制连接。主进程还负责处理客户端发送的 FTP 命令，并根据命令指示进行相应的操作，如打开数据连接、传输文件等。主进程通常运行在 FTP 服务器上，负责与客户端进行交互。从属进程负责与用户进行交互，发送用户名、密码和 FTP 命令给服务器。从属进程还负责接收服务器返回的响应和文件数据，并将结果显示给用户。从属进程通常运行在客户端计算机上，负责与 FTP 服务器进行通信。

练习 4 使用 TCP 连接工具与服务器进行命令交互

本练习一人一组，现仅以主机 A 为例，其它主机参考主机 A 的操作。

1．主机 A 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）。

2．主机 A 启动 TCP 工具连接 FTP 服务器。

(1) 主机 A 启动实验平台工具栏中的“TCP 工具”。

①选中“客户端”单选框。

②在“地址”文本框中填入 FTP 服务器的 IP 地址。

③在“端口”文本框中填入主机 FTP 服务器进程的端口号 21。

④点击“连接”按钮，建立与 FTP 服务器的 TCP 连接。

(2) 连接成功（将该次连接记为 w_cmd），在接收窗口会显示成功连接的信息；若不成功，再次尝试进行连接，直到成功。如图：

图 13-18 TCP 连接工具界面

2．使用 TCP 连接工具与服务器进行命令交互：

「注」

①<CRLF>是回车换行；

②文件名的生成规则是：file_X（x 是组索引，eg：第一组使用的文件名为：file_1）。

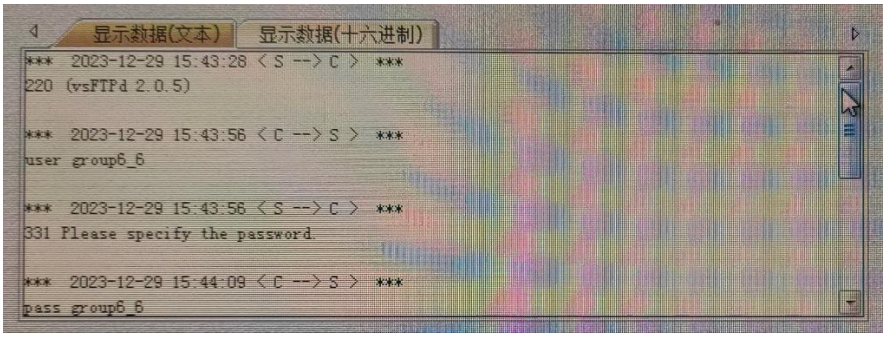
③用户名、密码相同，规则是：groupx_y（x 是组索引，y 是主机索引，例如第一组的主机 C 使用的用户名和密码为：group1_3)。

(1) w_cmd 的发送窗口：USER 用户名<CRLF>点击“发送”；

• 服务器回复的信息？

(2) w_cmd 的发送窗口：PASS 密码<CRLF>点击“发送”；

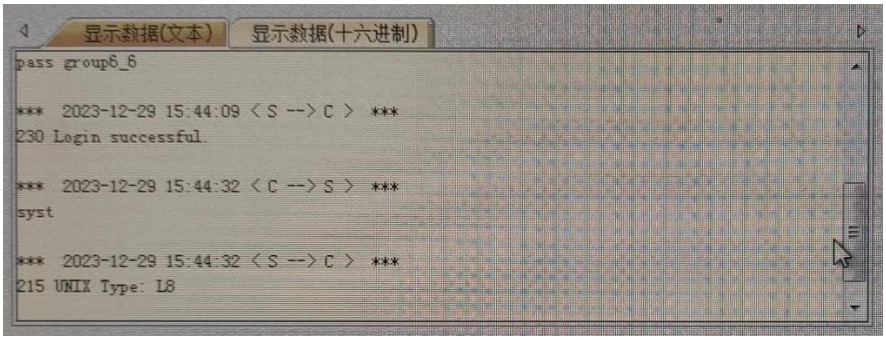
• 服务器回复的信息？



进入 FTP 服务器，与 FTP 服务器进行命令交互；

(3) w_cmd 的发送窗口：SYST<CRLF>点击“发送”；（询问服务器使用的操作系统）

• 服务器回复的信息？

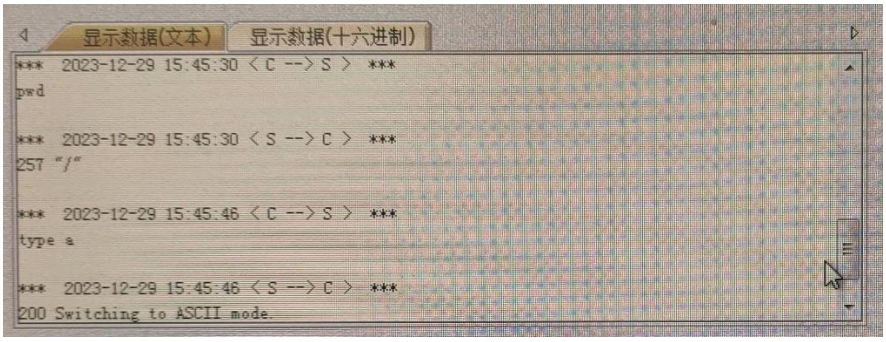


(4) w_cmd 的发送窗口：PWD<CRLF>点击“发送”;（显示当前路径）

• 服务器回复的信息？

(5) w_cmd 的发送窗口：TYPE A<CRLF>点击“发送”;（定义文件类型为 ASCII）

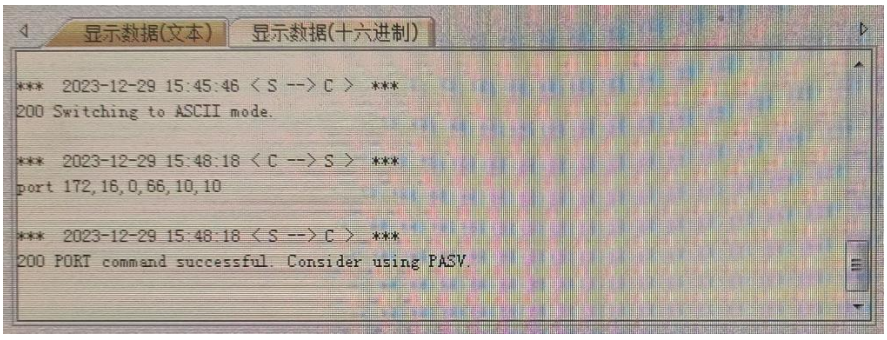
• 服务器回复的信息？

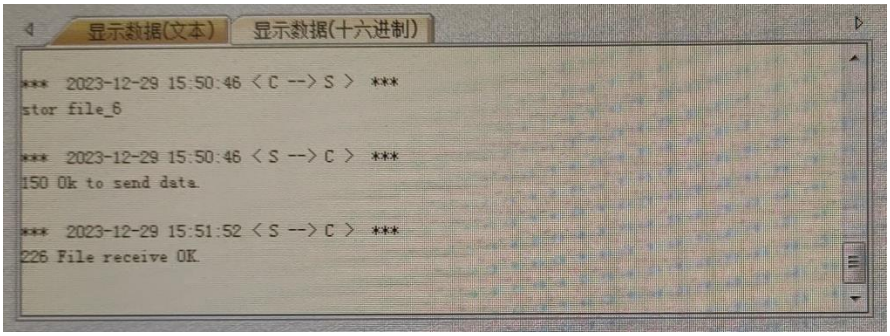


(6) w_cmd 的发送窗口：PORT x1,x2,x3,x4,x5,x6<CRLF>点击“发送”;

「注意」上面 x1-x4 的取值的规则为 x1,x2,x3,x4 携带的是本机的 IP 地址，x5,x6 为端口值，计算方法为 x5*256 + x6。例如本机的 IP 地址为 172. 16. 0. 35，则 xl、x2、x3、x4 分别为 172、16、0、35，端口号为 1025，则 x5 为 4，x6 为 1。本实验使用端口为 2570, 所以 x5 为 10，x6 为 10。

• 服务器回复的信息？





• PORT 命令对端口信息是怎样传递的？由上面发送的信息可知客户端使用的端口值为？

回答：2570。

• 解释一下 PORT 的格式，及该命令的用途。

回答：格式是：port port-number。其中，port-number 是指要使用的目的端口号，可以是一个具体的端口号，也可以是一个端口范围。用途是在设备上配置目的端口号，以便设备能够向 Portal 服务器发送报文。

• FTP 服务器是使用什么方式创建数据连接的？

回答：在这里使用了主动模式。客户端向 FTP 服务器的 TCP 21 端口发送 PORT 命令，请求建立连接，并告知服务器要使用的 X 端口接受数据。然后，服务器使用 TCP 20 端口主动与客户端指定的 X 端口建立数据连接。

(7)再次运行 TCP 连接工具，按下图的内容填写数据，按“创建”键，进入等待远程连接的侦听状态中（将该次创建的连接记为 w_datal）；

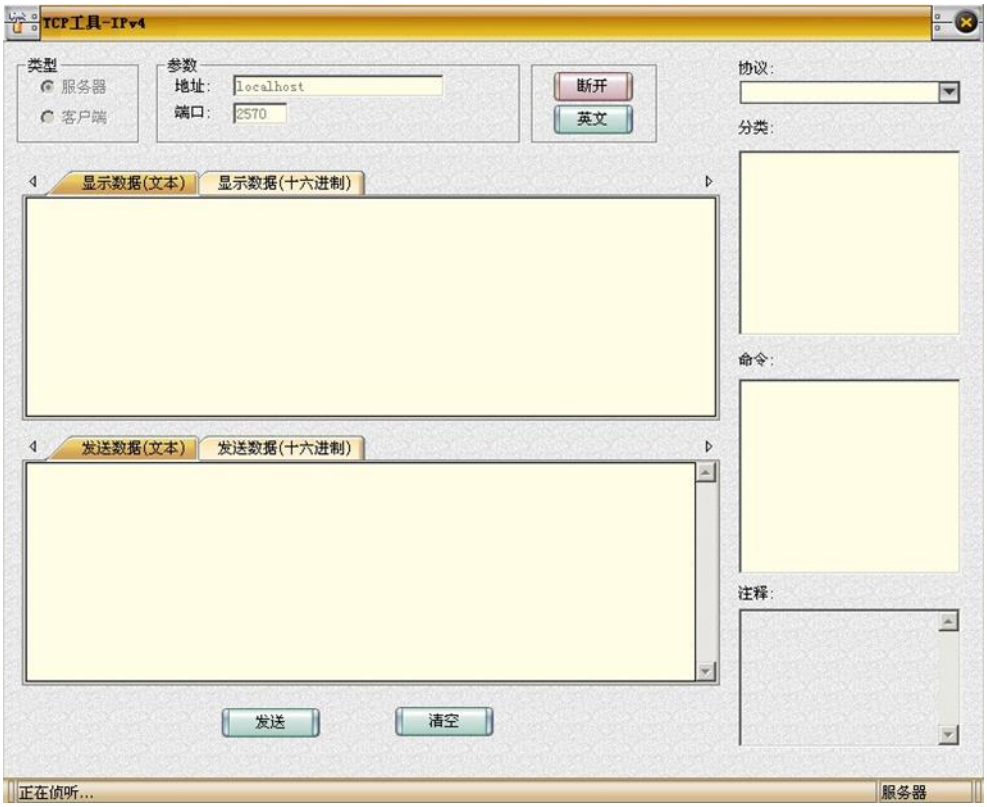
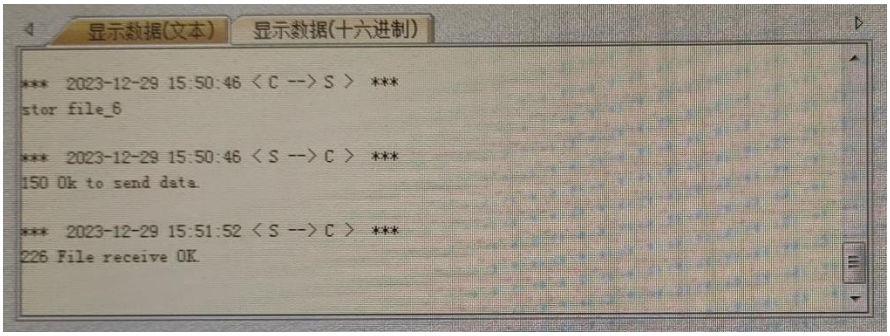


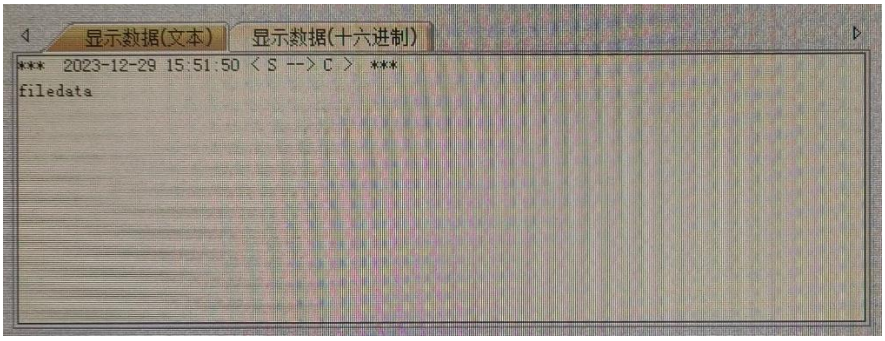
图 13-19 以服务器方式进行连接

(8) w_cmd 的发送窗口：STOR 文件名<CRLF>点击“发送”；（存储文件）

• 服务器回复的信息？

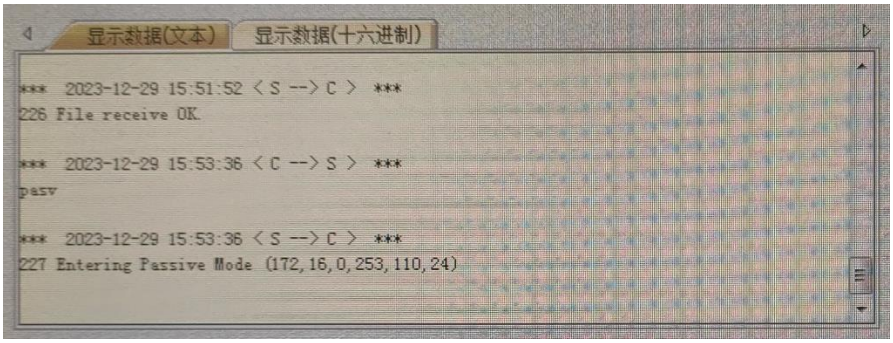


(9) w_datal 的发送窗口：filedata 点击“发送”，再按“断开”键关闭 w_datal；



(10) w_cmd 的发送窗口：PASV<CRLF>点击“发送”；

• 服务器回复的信息？



• 说明该命令的用途。

回答：以被动模式创建数据连接。

• FTP 服务器是使用什么方式创建数据连接的？

回答：被动模式。

• 在服务器回复的信息中可知服务器端使用的端口为？（记为 port）。

回答：110*256+24=28184。

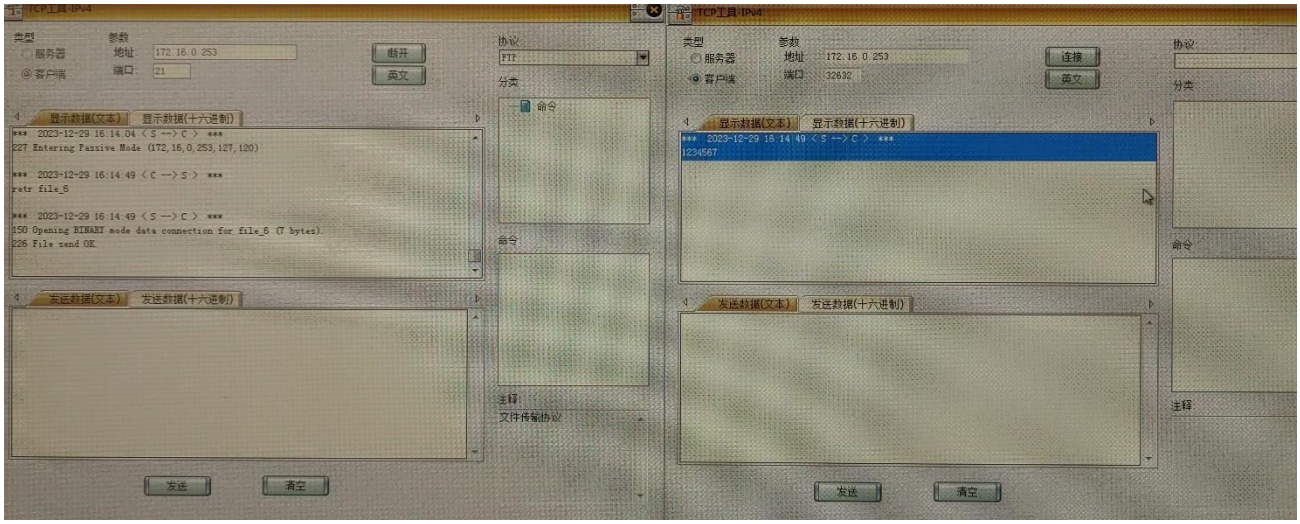
(11) 再次运行 TCP 工具，将其端口值 21 改为 port 的值，按“连接”键，进入 FTP 数据传输窗口（将该次连接记为 w—data2）；

(12) w_cmd 的发送窗口：RETR 文件名<CRLF>点击“发送”；（此为读取文件）

• 服务器回复的信息？

(13) 察看 w_data2 返回信息，并将其关闭；

• 其内容是步骤(9)输入的信息吗？



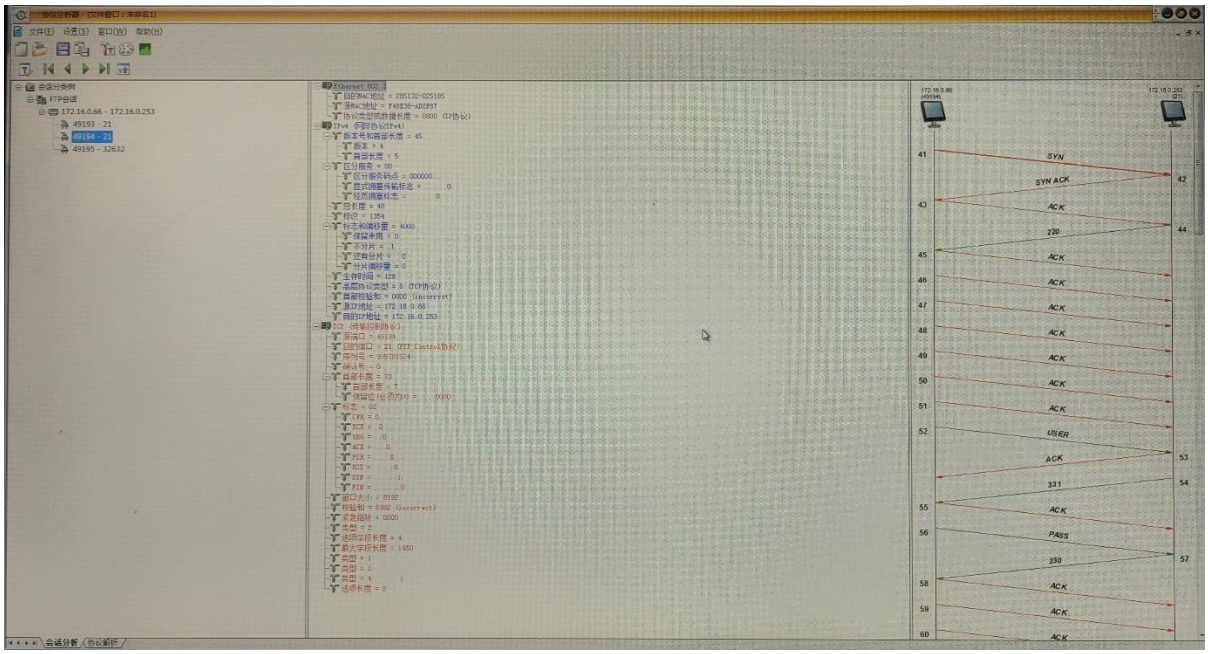
回答：不是。可能是其他人覆盖了信息。

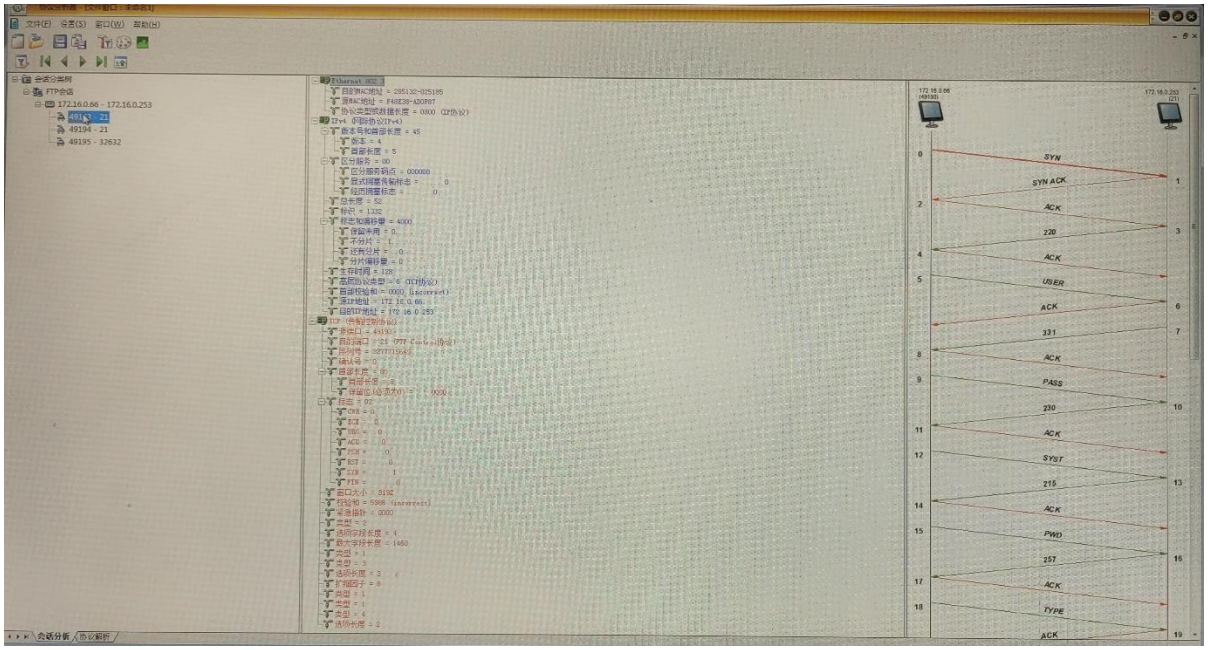
(14) w_cmd 的发送窗口：QUIT<CRLF>点击“发送”；（此为退出—终止命令连接）

• 服务器回复的信息？

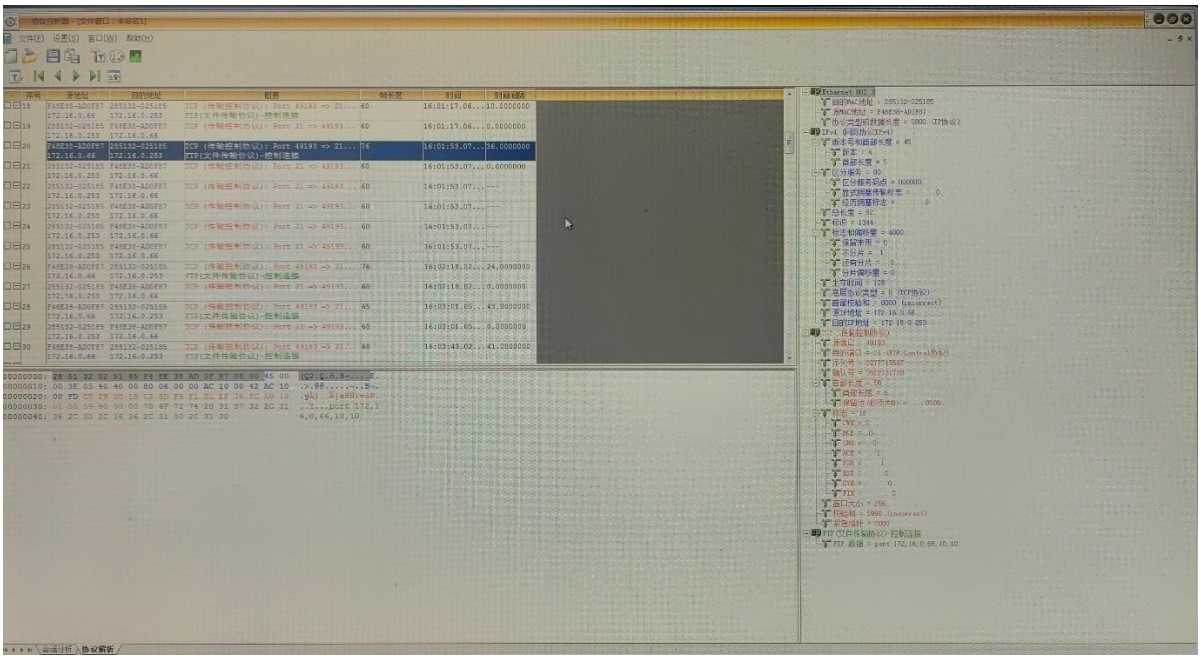
4．分析端停止数据捕获，并分析捕获的数据：

察看“FTP 会话”各会话中，建立 TCP 连接、数据传输、释放 TCP 连接的过程。

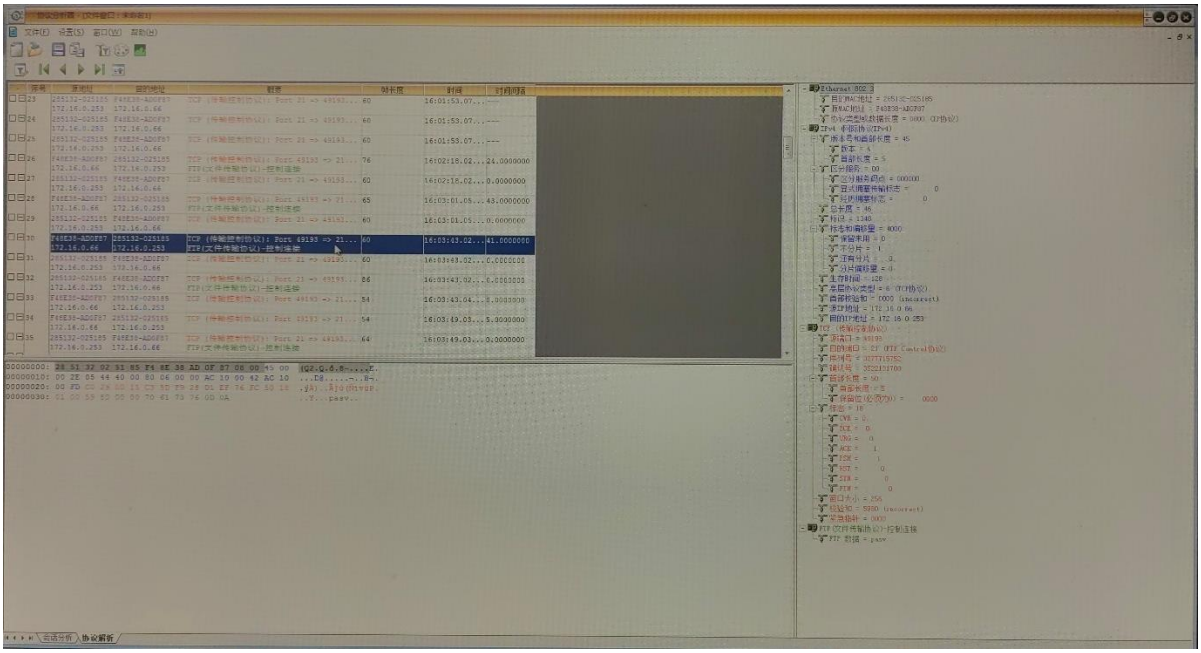




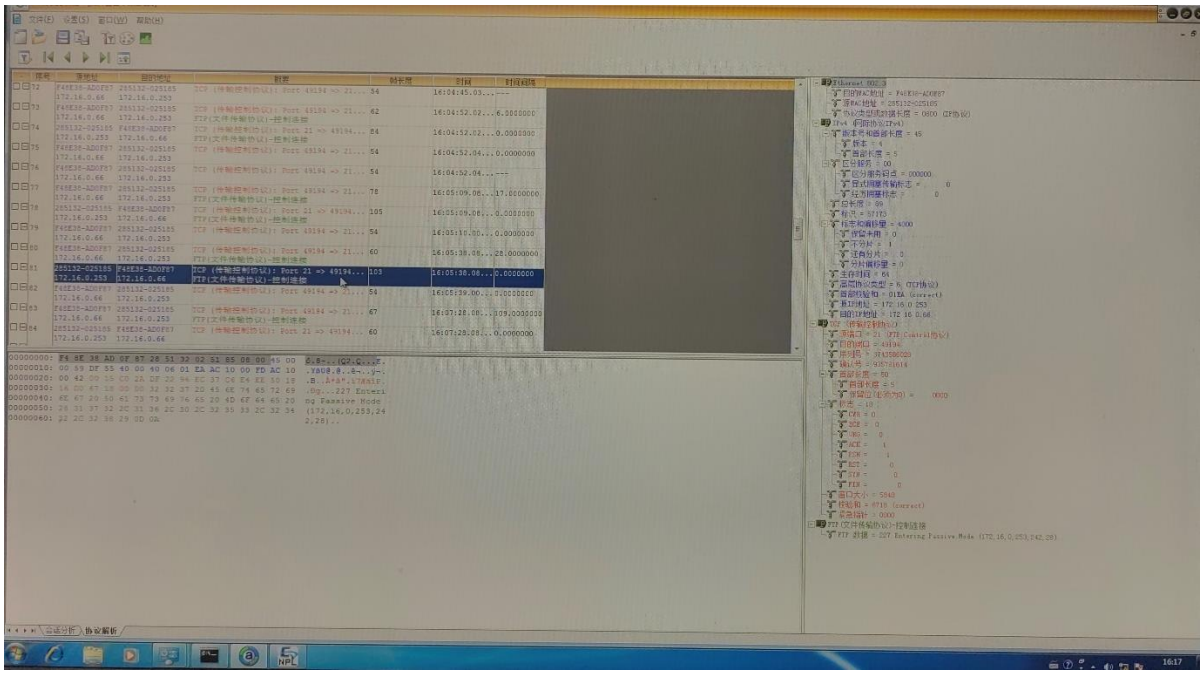
(1) 找出含有“PORT”命令的数据包，结合上下文理解该命令的作用。



(2) 找出含有“PASV”命令的数据包，结合上下文理解该命令的作用。



(3) 找出步骤 2 中涉及的数据连接（在“FTP 会话”中，由步骤 3 的(10)步 port 的值及 20 端口所区分的两个会话），分析数据传输的过程。



5．结合该实验的操作过程及实验结果，分别绘制出主动模式下、被动模式下 FTP 上传数据、下载数据的会话交互图。

回答：

主动模式（PORT）：

上传数据：

客户端 -> 服务器: PORT 172.16.0.253,32632

服务器 -> 客户端: 200 PORT command successful

客户端 -> 服务器:STOR filename

服务器 -> 客户端:150 File status okay; about to open data connection.

服务器 -> 客户端:226 Transfer complete

下载数据：

客户端 -> 服务器: RETR filename

服务器 -> 客户端:150 File status okay; about to open data connection.

客户端 <-> 服务器: Data connection for file transfer

服务器 -> 客户端:226 Transfer complete

被动模式（PASV）：

上传数据：

客户端 -> 服务器: PASV

服务器 -> 客户端:227 Entering Passive Mode (172.16.0.253,32632,1)

客户端 -> 服务器:STOR filename

服务器 -> 客户端:150 File status okay; about to open data connection.

服务器 <-> 客户端: Data connection for file transfer

服务器 -> 客户端:226 Transfer complete

下载数据：

客户端 -> 服务器: RETR filename

服务器 -> 客户端:150 File status okay; about to open data connection.

服务器 <-> 客户端: Data connection for file transfer

服务器 -> 客户端:226 Transfer complete

五、 思考问题:

1. FTP 的数据连接存在两种模式：主动模式和被动模式，说明各自的工作过程。如果服务器和客户端之间存在防火墙，使用哪种模式会引起一些麻烦？

回答：如果服务器和客户端之间存在防火墙，使用主动模式可能会引起一些麻烦。因为主动模式下，服务器会主动向客户端的随机端口发起连接，如果防火墙规则设置过于严格，可能会阻止这种主动连接，导致数据连接无法建立。而被动模式下，客户端会主动向服务器的随机端口发起连接，如果客户端的防火墙规则较为宽松，则一般不会影响数据连接的建立。因此，在存在防火墙的情况下，使用被动模式可能更为可靠。