

“网络安全综合实验（I）”实验指导

**题目：网络流量分析（高级）**

# 实验十：网络流量分析（高级）

## 实验环境及要求

### 实验平台及说明

实验软件：Wireshark 3.0.3；

操作系统：windows；

**参考资料**：

1. Chirs Sanders著，诸葛建伟等译，Wireshark数据包分析实战，人民邮电出版社，2018
2. Wireshark在线帮助
3. 课程群文件共享资料
4. 其他在线文档资源。

**提交时间及文件说明**：本实验环节，每位同学提交独立完成的实验报告电子版一份；按指导老师要求的时间和方式提交；文件名：U2019XXXX（学号）-姓名-网 络安全综合实验（I）网络流量分析实验。

**报告格式要求**：正文为宋体小 4 号，段首缩进 2 字符汉字，行间距 1 倍行距，字 符间距为标准；图保证清晰大小合适；每页尽量不留大段空白。图片需要编号及 命名；正文、图片、参考文献的格式，请参考华中科技大学毕业论文规范中关于排版的要求。

**文档中包含的内容**：

1 封面首页信息及作者、完成时间； 2 小结：总体感受、实验中遇到的最突出问题及收获、对实验环节的意见和建议；4 实验中为解决问题，查阅资料，请记录资料出处，包括资料名次、页码、网址，作为 参考文献部分列表给出； 5 参考网络上资料的，请通过浏览器的打印功能，以 pdf 文件方式保存；资料可归档为：参考资料.zip，与报告一并提交。

**学习通要求**：实验过程中，请各位同学按照实验指导手册中红色文字部分（例如：【验证实验1】）的要求截图和回答问题，并将问题的答案提交至“学习通软件”。

## 实验任务

本次实验主要对截获的网络流量进行分析，如何截获网络报文，可以参考其他老师的介绍。

### 任务1 无响应的气象服务

**【问题场景】**

仍然是那个Peter，他有众多的爱好，包括气象学——他自认为是一个业余的气象学家，每个几个小时就会查看天气现状和气象预报。他并不依赖本地新闻中的气象预报，他在自己家的外面运营了一个小型的气象站，并将数据上报至服务器用于数据汇总各查阅。

某一天Peter检查他的气象站的时候发现自物业开始，气象站已经有超过9个小时没有想服务器发送数据报告了。

这是怎么回事儿呢？

**【网络环境】**

在Peter的网络中，气象站被挂在房顶上，与屋内的设备通过射频链接。接收器通过路由器接入到网络中，然后将数据发送至互联网的服务器，这个结构如下图所示。



气象数据接收器有一个简易的Web管理界面，Peter登录到管理界面只发现了一条与上次同步时间相关的加密信息，除此之外 ，没有其他可用于故障处理的信息——这个系统不提供任何详细的错误日志。由于接收器是气象站设备的通信枢纽，因此抓取发往或来自于接收器的数据包对于诊断是有意义的。

但是，如何抓取数据呢？

抓取数据，通常有两种方式：

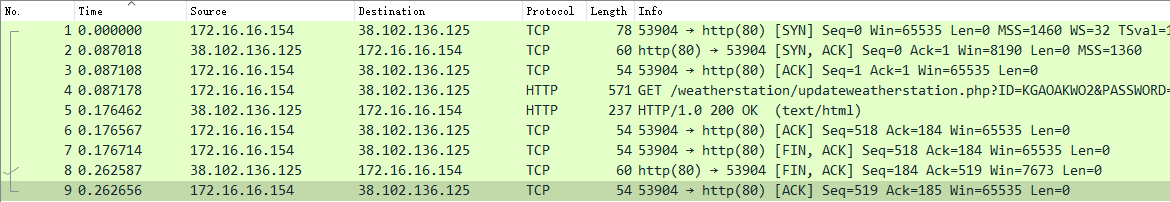
1. 抓取本机数据，打开Wireshark即可；
2. 抓取网络数据，使用网络设备（交换机/路由器）的镜像端口。

上面两种方式都不符合本次数据包数去的要求，只能使用ARP欺骗的方式进行数据包抓取的工作了（这个将在后续的内容进行讨论）。

**【发现问题】**

通过ARP欺骗的方式，我们个抓取到了网络数据包并将其保存在***weather\_borken.pcapng***文件中，下面开始对其进行分析。

使用Wireshark打开该捕获文件，发现交互得信息很简单。



从这些简单交互数据包，我们可以学习一些情况：

1. TCP建立连接使用三个交互数据包，俗称“三次握手”协议。他们分别是“SYN”、“SYN ACK”和“ACK”数据包；
2. HTTP数据包是在TCP连接上进行传输得，一定得TCP连接建立成功之后，才会进行HTTP得数据交互；
3. TCP拆除连接使用四个交互数据包，两个“FIN ACK”数据包，两个“ACK”数据包。

从上述分析来看，气象信息得数据交互在次序上面没有问题。先有“三次握手”建立 TCP连接，然后进行HTTP请求和应答，之后就是拆除TCP连接。既然HTTP数据通信能够开始，说明TCP连接没有问题，问题出在什么地方呢？

此时我们开始进行“合理”猜测，并注意进行验证：

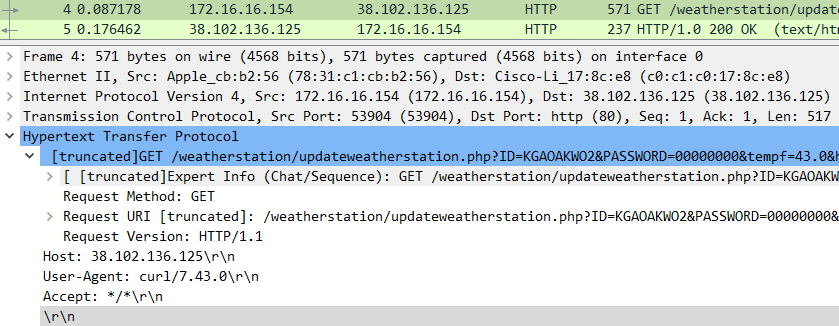
1. 通信得目的地址问题？

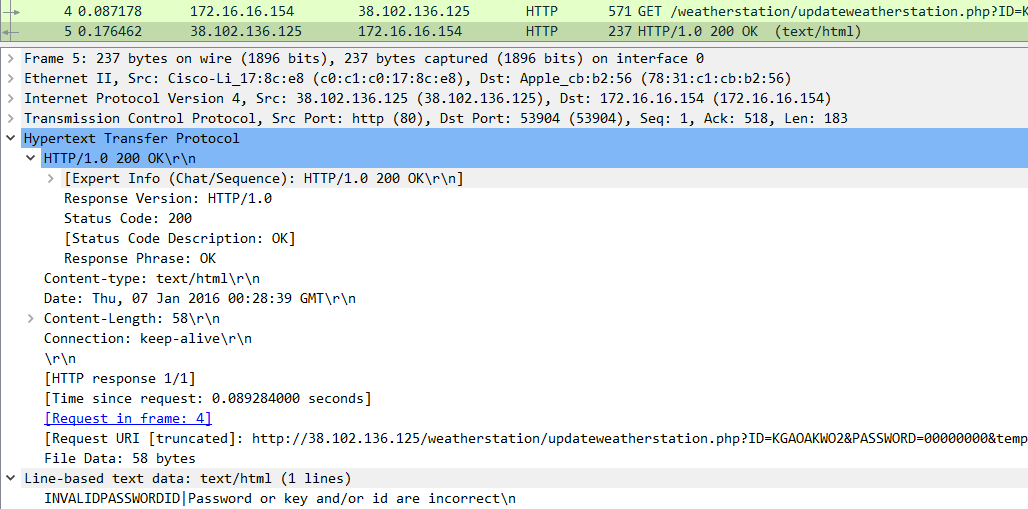
在本案例得通信过程中，除了Perter的气象数据接收器使用的地址外，出现了一个陌生的地址38.102.136.125，这个地址是不是正确的气象数据接收地址呢？通过WHOIS查询服务，我们至少发现这个地址与某一个气象组织相关，这个问题暂且得到验证吧。

1. TCP连接的问题？目前我们还没有学习具体的TCP协议以及TCP连接管理方面的知识。但是就我们目前了解的关于TCP连接管理的相关知识，“三次握手”是么有问题的，更何况后续的HTTP通信能够开始，我们也可以做出这样的判断，因为如果TCP连接连接有问题的话，HTTP通信是不会开始的。
2. 会不会是TCP连接拆除的过程出现了问题呢？感觉不像，因为就算TCP连接拆除出现问题，通过HTTP传输的数据也应该已经传输完成了，似乎不会影响到气象数据的传输。
3. 最后，我们把问题的焦点集中到了HTTP通信上，HTTP通信需要仔细得进行分析。

**【重点分析】**

从HTTP请求和应答得形式上看，HTTP得数据交互似乎也没有问题。仔细分析下，我们发现了问题：





1. 气象数据接收器是要像服务器发送数据得，但是HTTP请求数据包得数据部分是空的？这难道是问题所在么？

答案是否定得。一般而言，作为C/S结构得Web应用，都是浏览器从服务器获取数据，但是也不排除浏览器需要传输一些数据到服务器，遇到浏览器向服务器传输数据，会采用两种方式，一种是使用“POST”方法，将需要传送到服务器得数据作为表单放在请求数据包得数据部分传输到服务器；另一种方式是使用“GET”方法，将需要传输得参数放在URL中传输到服务器。仔细观察HTTP请求报文，我们发现其拥有一个长长的URL，而且这个URL得格式有些特殊。在URL的“？”字符之后，反复出现形如“XXX=XXX&”得字符形式，其实这就是HTTP协议使用“GET”方法向服务器传输参数的一种方法。

1609731066(1)

1609731149(1)

1609731184(1)

1. 再来分析HTTP响应数据包。HTTP响应数据包的状态码是200，状态短语是OK，表明与之对应的HTTP请求报文已经被服务器正确接收。但是我们从这个HTTP响应巴报文的数据部分发现了端倪，在数据部分有这样的字符串：

1609731545(1)

所有的同学应该都能够看出这个字符串的含义，“错误的用户ID或者口令”。难道请求数据包中的用户ID或者用户口令出现了错误？反过头来在仔细观察HTTP请求数据包，我们发现了问题所在：

1609731149(1)

**【结论】**

也许是由于固件升级，也许是由于设备其外重启导致用户口令丢失，气象数据接收器无法向服务器验证自己的身份，从而导致上传气象数据失败。Peter只需要接入他的数据接收器，重新输入用户名和口令，他的气象数据接收器就重新开始向服务器同步自己侦测到的气象数据了。

**【验证实验1】**

当Peter的气象数据接收器回复正常工作之后，我们又对气象数据接收器与服务器之间的通信进行了一次数据包捕获工作，捕获到的数据包保存在weather\_working.pcapng文件中，请分析该数据包，并将气象数据接收器与服务器通信时的用户ID和用户口令提取出来并截图证明之。

**【建议】**

很多开发者喜欢使用URL的方法向服务器传输一些参数信息，但是我们建议一般情况下不要像本案例一样将用户名、口令等参数写在URL中。因为在不适用加密措施，如HTTPS的情况下，HTTP通信将使用明文传输URL，这样容易导致用户敏感信息的泄露。

### 任务2 无法访问Internet

**【问题场景】**

这个问题的场景非常简单：用户不能访问Internet。我们已经确认该用户可以访问所有的内网资源，包括其他工作站的共享内容以及运行在本地服务器上的应用程序。

**【网络环境】**

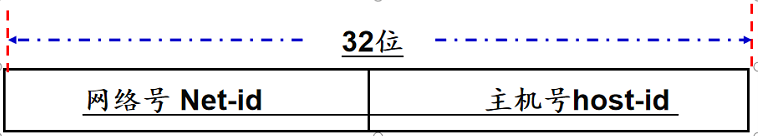
这个网络的环境也非常简单，所有客户机和服务器都连接到一系列的简单交换机上，Internet连接有一个路由器（作为默认网关）处理，IP地址信息有DHCP服务提供。由于网络上的交换机不支持镜像接口捕获网络数据包，我们不可避免的需要妨碍用户，在其PC捕获了网络数据包并保存在***nowebaccess1.pcapng***文件中。



**【预备知识】**

网络流量分析，从来都是人的事儿，之所以牵扯到Wireshark，只是因为Wireshark能够提供一些列的工具来帮助我们进行查看和统计，以提高网络流量分析的效率。所以在进行网络流量分析之前，有一些关于本次实验的计算机网络的预备知识需要大家提前了解下哟。

1. **IP地址的结构。**大家知道，IP地址是计算机网络中终端的唯一标识，它是一个32位的二进制数。为了能够方便寻址，他被设计成为一个具有层次结构的地址，这32位的二进制数，一部分表示局域网的网络号，另外一部分表示终端在这个网络内部的编号。



1. **内网通信过程：**这里所说的内网，一般来说是指局域网（LAN）。我们说两个终端在同一个内网中，其本质是指两个终端的网络号是相同的。如果两个终端在同一个内网中，那么其通信方式如下：

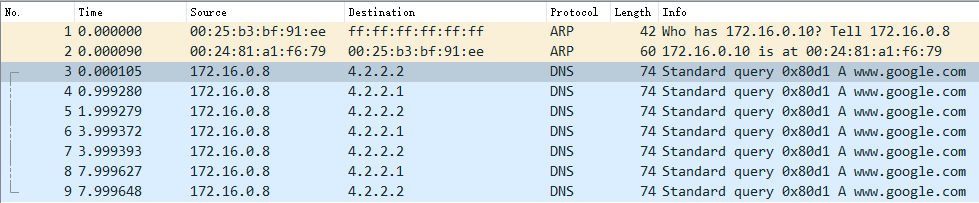


1. **Internet通信过程：**如果主机在Internet上，则目标地址与源地址不在同一个内网中，也就是说他们的IP地址的网络号部分并不一致，此时需要将数据包发送到“默认网关”上进行路由选择，具体的通信过程如下：

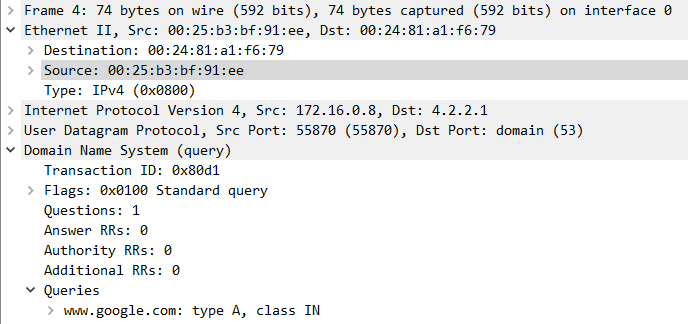


**【流量分析】**

使用Wireshark打开数据包捕获文件，我们看到如下的捕获数据包。从数据包协议来看，两个ARP数据包和7个DNS数据包，下面我们需要进行逐一分析。

****

1. **ARP数据包。**整个通信序列有两个ARP数据包开始是否正常呢？第一个ARP数据包，其目标地址是一个广播地址，这很符合ARP查询数据包的特征，它查询了172.16.0.10这个地址对应的MAC地址。从第二个ARP数据包来看，它是一个ARP应答包，其向主机172.16.0.8回应了172.16.0.10对应的MAC地址00:24:81:a1:f6:79。从表面上看，这一次ARP查询似乎是正常的，但是其查询的是谁的IP对应的MAC地址呢？
2. **DNS数据包。**在ARP之后紧接着DNS数据包，这个可以理解，因为访问网络之前通过DNS获取要访问的网站名称对应的IP地址是一件比较正常的事情，但是在捕获的数据包中我们发现几点比较奇怪的现象：一是我们只看到了DNS查询数据包，没有看到DNS回应数据包。通过whois查询，我们确认所有的DNS查询涉及的两个目标地址4.2.2.2和4.2.2.1的确是DNS服务器，同时，通过“ping”我们也确认这两个地址是在线的，那到底是什么原因导致DNS查询得不到回应呢？
3. **对DNS数据包重点分析。**选择一个DNS数据包查看其详细内容。DNS查询报文的目标IP地址是4.2.2.1或者4.2.2.2，查询的是www.google.com对应的IP地址。这些似乎都没有问题，那么问题出在什么地方呢？



回顾下我们前面学习的预备知识，很显然DNS服务器与出现问题的主机不在同一个内网中，那么这个DNS数据包会在第二层以默认网关的MAC地址进行封装并发送到默认网关进行路由转发。查看这个DNS查询报文的第二层信息，其目标MAC地址是00:24:81:a1:f6:79，这个地址正是ARP查询响应数据包响应的MAC地址，也就是说捕获数据包中开始的ARP实在查询默认网关的IP对应的MAC地址，因此我们可以判断用户主机配置的默认网关应该是172.16.0.10。

**【结论】**

问题分析到这里，应该可以做一个结论了。因为我们从用户网络管理员哪里获取的网络配置信息中，默认网关并不是172.16.0.10。进一步查看用户的本地网络网络配置，该用户使用了“静态配置IP参数”的方式，而没有采用DHCP方式，当网络的网关发生变化之后，他的网络参数没有同步进行更新，导致它法网Internet的数据被发送到了一个错误的“默认网关”，而这个网关又不具备路由转发的功能，所以他与Internet之间的数据交换就终止了。而内部通信是不需要默认网关参与，因此虽然配置了错误的“默认网关”，但是并不影响它的内网通信。

**【验证实验2】**

启动Wiresshark工具，对你访问某一个网站的数据交互进行捕获。对捕获的网络数据包进行分析，并回答下列问题：

1. 你的计算机配置的默认网关是什么？请截图证明之；
2. 你的计算机配置的DNS服务器是什么？请截图证明之；
3. 你访问的网站的IP地址是什么？请截图证明之。

### 任务3 推卸责任的程序员

在IT界，软件开发程序员经常和网络管理员争吵。程序员总是将应用程序的错误归咎于糟糕的网络设置和设备，而网络管理员总是倾向于将网络错误或者网络缓慢归咎于糟糕的应用程序代码。这时候就需要提出有利的证据，才能够说服对方。

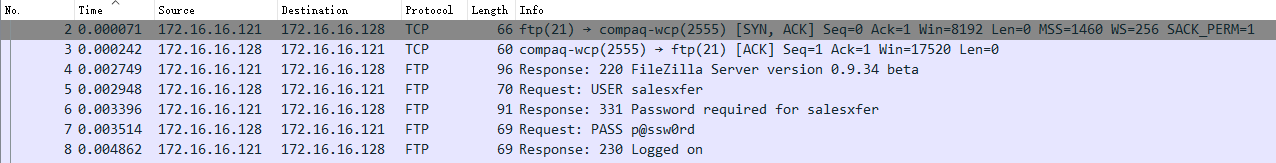
**【问题场景】**

这次是一个新开发的网络应用的 工作情况不太正常。服务器接收到了从各个卖场传回的文件，但是将这些文件中的数据插入到数据库中的时候却出现错误，导致数据无法插入到数据库中——有的数据丢失了，有的数据是错误的。当然，程序员一口咬定网络原因导致数据传输时被损坏了，而系统管理员却对他的网络非常自信。这个问题的场景非常简单：用户不能访问Internet。我们已经确认该用户可以访问所有的内网资源，包括其他工作站的共享内容以及运行在本地服务器上的应用程序。如果你是这个网络管理员，该怎样说服程序员应该好好好地修改他们地代码呢？

**【流量分析】**

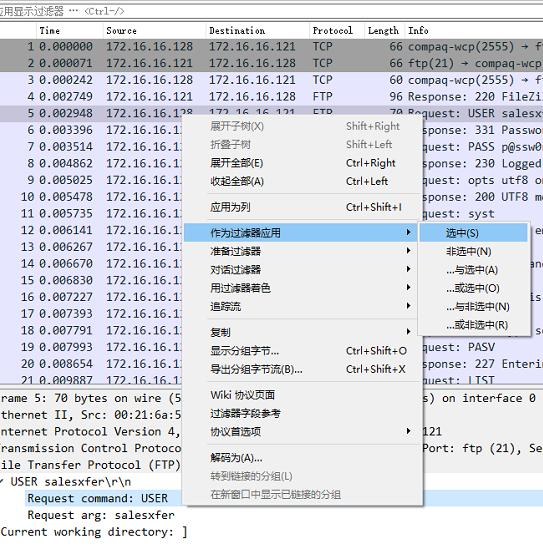
由于故障影响到了所有的卖场，如果这个问题的确由于网络的原因导致，我们应该在中心办公室捕获网络数据包，因为它是所有卖场数据通信的汇聚点。采用交换机镜像端口的方式，我们在中心办公室捕获到了网络数据包，并保存在***tickedoffdeveloper.pcap***文件中。

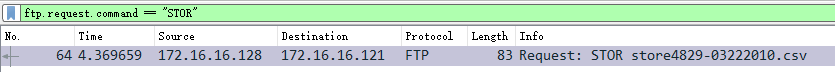
为了证明故障并不是由于网络传输导致的，我们只需要从中心办公室捕获的网络数据包中提取出需要传输的数据，证明他们和从卖场传输出来的数据一模一样就可以了。一次位目的，我么开始对网络流量进行分析。同时，除了在网络中捕获的网络数据包之外，我们完全不了解程序员开发的这个新的应用程序。从捕获的数据包来看，似乎是从一些FTP流量开始的。



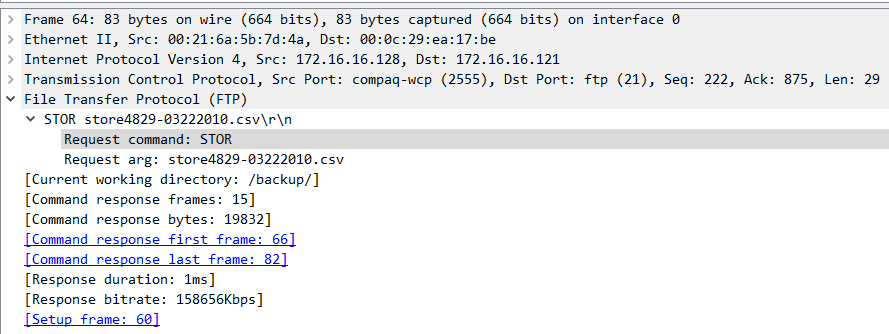
由于TCP连接是由172.16.16.121发起的，我们推测它是客户端，那么172.16.16.128就是数据服务器了。这个捕获文件中有非常多的FTP命令，但是我们真正关心的FTP命令是“STOR”命令，这个命令的出现，因为着正式的数据传输开始了。

如何在众多的网络数据包中找到“STOR”命令的数据包呢？当然是设置筛选过滤器啦。设置筛选过滤器的一个简单方法是：选中最开始出现的FTP命令报文，例如第5个报文，在详细信息面板中选中FTP Section中USER Seection，右击Request command：USER域，并选择“作为过滤器应用”，这将在数据包列表面板中产生一个过滤器。



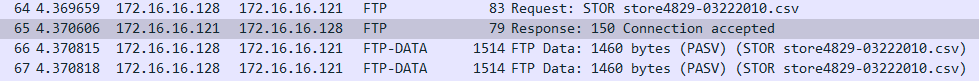
但是这个过滤器过滤的是数据包中使用FTP.USER命令的数据包，我们只需要将“USER”字符串修改为“STOR”字符串，就得到了一个过滤FTP.STOR命令的筛选过滤器。 

过滤结果只发现了一个带有FTP.STOR命令的FTP数据包，其顺序编号为64。这个数据包的详细信息如下。这个数据包非常重要，他的重要性主要体现在两个方面：首先，该数据包的出现意味着开始进行数据传输的数据包应该就在其附近；其次，该数据包明确了数据文件的名命，根据文件名称的扩展名，我们基本能够确定数据文件的类型，也就确定了我们该用什么方法去处理一个二进制表示的文件。

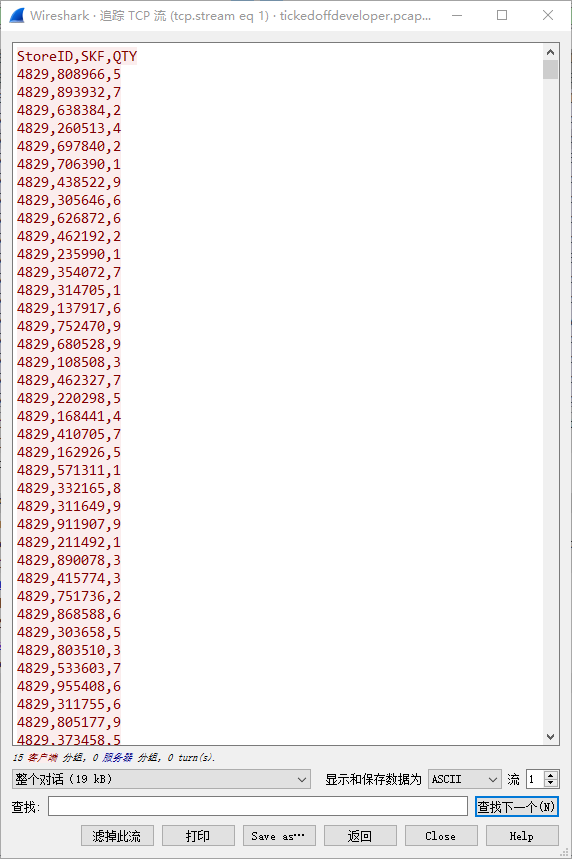
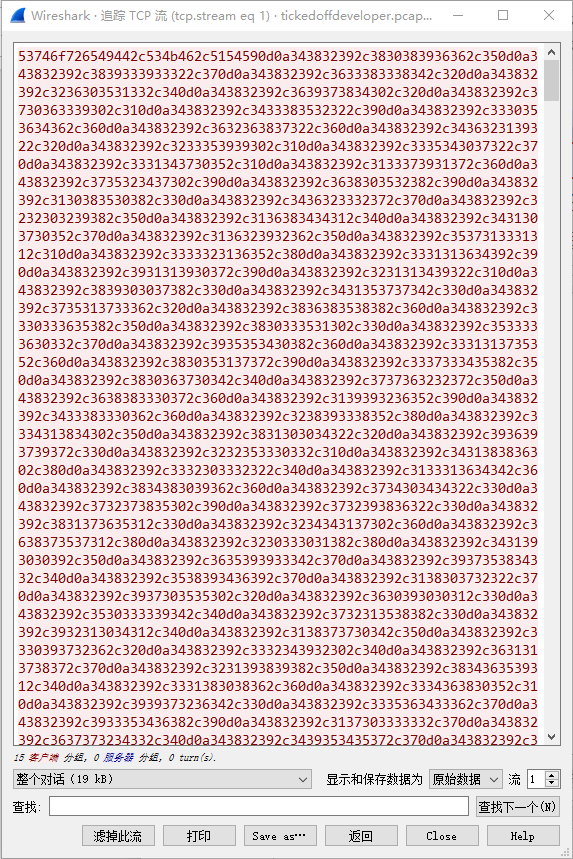


由于FTP传输命令和传输数据时使用两个不同的TCP连接进行的，因此此时我们需要清除掉筛选过滤器，并在64号报文附近搜索用于数据传输的FTP数据包。

很快，我们在66号数据包发现了用于传输数据的数据包。接下来要怎么把文件从数据包中提取出来呢？



右键选中FTP数据流中的任何一个数据包（66或者67号数据包），单击追踪TCP流，打开了“追踪TCP流”的对话框，如下：

将“显示和保存数据为”选择为“原始数据”，点击“Save as...”即可将FTP中传输的数据提取到文件中了。

**【结论】**

现在回答到底时网络设置或设备还是程序代码导致的故障这个问题已经不困难了，只需要比较原始文件和在中心办公室从数据包中提取的文件就可以了。如果二者相同，应该是程序代码出现了问题；如果不同，那就是网络传输出现了问题。

**【验证实验3】**

1. 安装Serv-U，这是一个FTP服务器软件。安装过程中注意配置相应的目录、用户名、口令等信息，其他参数可采用默认参数，不必修改，安装完成之后启动FTP服务器。
2. 两位同学为一组，A同学使用浏览器作为FTP客户端（地址栏中输入：[ftp://B同学的IP地址）访问B同学的FTP](ftp://另外一个为同学的IP地址）访问同组同学的FTP)服务器并上传一个文件。此时，B同学开启Wireshark捕获网络数据包，并从数据包中提取A同学上传的文件，查看并显示该文件。截图说明从捕获数据包中提取图片文件的过程。A、B同学角色互换，重复上述操作。

### 任务4 ARP欺骗攻击

前面我们已经学习过，ARP协议时如何将网络中的IP地址隐身成为MAC地址的，我们也讨论过ARP欺骗攻击可以改变网络中数据包的流量从而成为在交换网络中捕获网络数据包的一种方法，使ARP欺骗攻击成为网络工程师的一种非常高效使用的工具。然而，如果有恶意企图，它也成为了一个非常致命的“中间人攻击”的方法。它可以重定向两台主机之间的网络数据流量，试图在传输过程中拦截或者修改流量。中间人攻击包括会话劫持、DNS欺骗，SSL劫持等等，但是都是以ARP欺骗攻击作为基础。

数据包捕获文件***arppoison.pcap***文件中包含了ARP欺骗攻击的一个例子。其中受害的主机IP地址是172.16.0.107，它的默认网关是172.16.0.1。

试着分析一下这些捕获的数据包吧！！！

【验证实验4】

使用Wireshark打开捕获文件***arppoison.pcap***，对数据包进行分析，回答下列问题：

1. 从捕获的数据包分析，被攻击的主机MAC地址是什么？
2. 攻击发生在什么时候呢？那几个数据包是攻击的关键数据包？请说明攻击关键数据包的序号。
3. 正常情况下，被攻击主机的默认网关的MAC地址是什么？请截图证明之。
4. 被攻击之后，被攻击主机认为它的默认网关的MAC地址是什么呢？请截图证明之。
5. 这样的攻击，将导致什么样的后果？

# 小结：学习心得与体会

学生自己总结本次实验的内容，心得体会，意见和建议。

# 参考文献：

这部分要求学生把查阅的资料整理出来，并附上pdf归档包，作为积累的内容。