**链路层、网络层及传输层协议报文分析**

# 1．链路层协议分析

# [分析Ethernet标准和Ieee802.3标准规定的MAC层帧结构](http://www.cnblogs.com/leftshine/p/5698809.html)

分析所用软件下载：[Wireshark-win32-1.10.2.exe](https://pan.baidu.com/s/1pLH6gUB)

任务：

[1. 学习Wireshark的安装与使用](http://www.cnblogs.com/leftshine/p/5698809.html#_1.__学习Wireshark的安装与使用)

[2. 熟悉Wireshark的操作界面与功能](http://www.cnblogs.com/leftshine/p/5698809.html#_2.__熟悉Wireshark的操作界面与功能)

[3. 设计应用以获取以太网链路数据帧](http://www.cnblogs.com/leftshine/p/5698809.html#_3.__设计应用以获取以太网链路数据帧)

[4. 分析以太网链路数据帧格式与内容](http://www.cnblogs.com/leftshine/p/5698809.html#_4.__分析以太网链路数据帧格式与内容)

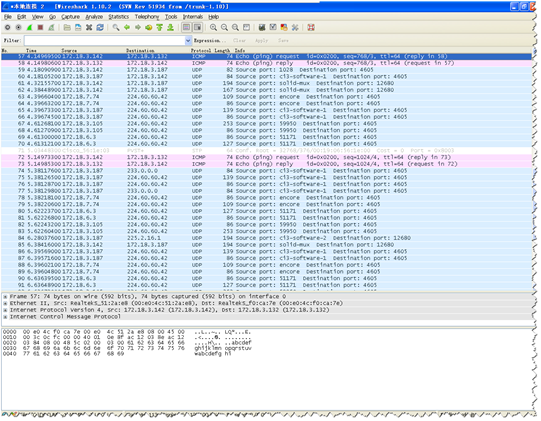
## 1.1 学习Wireshark的安装与使用

下载并安装网络装包软件Wireshark-win32-1.10.2

安装软件所需环境 WinPcap

## 1.2 熟悉Wireshark的操作界面与功能

打开Wireshark软件，熟悉操作界面及功能



## 1.3 设计应用以获取以太网链路数据帧

（1）抓取 ping 应用报文，获取以太网链路数据帧

开始抓包

Ping 当前实验室某计算机的ip：172.18.3.132

停止抓包，获取ping 应用的获取以太网链路数据帧

（2）抓取 http 应用的以太网链路数据帧

开始抓包

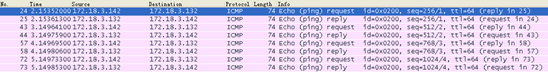
访问西南大学主页：www.swu.edu.cn

停止抓包，筛选并获取http 应用的以太网链路数据帧

## 1.4 分析以太网链路数据帧格式与内容

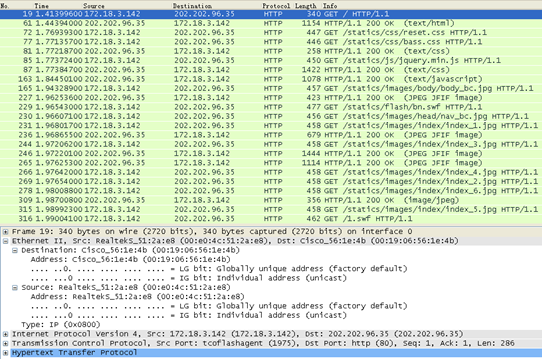
1. 获取以太网链路数据帧的结果

（1）获取到ping 应用的以太网链路数据帧：





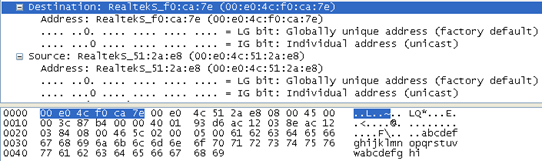
（2）获取到http应用的以太网链路数据帧：



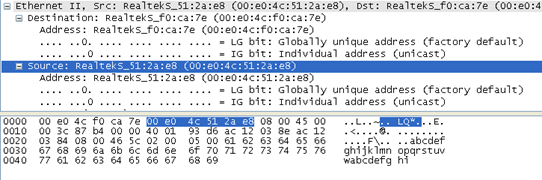
4. 分析以太网链路数据帧格式与内容

（1）ping 应用的以太网链路数据帧

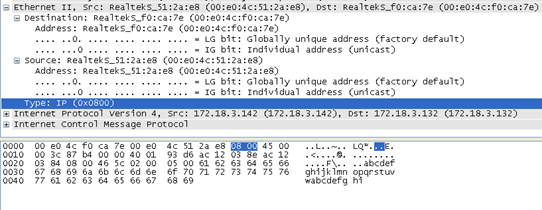
目的地址：00 e0 4c f0 ca 7e(6个字节)



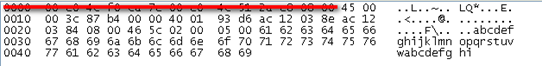
源地址：00 e0 4c 51 2a e8（6个字节）



类型：08 00（2个字节）

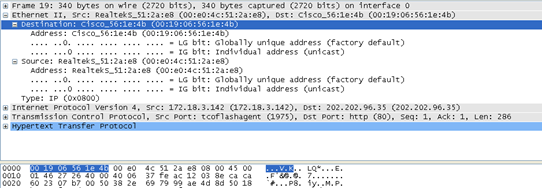


数据： 4500003c87b40000400193d6ac12038eac1203840800465c020005006162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

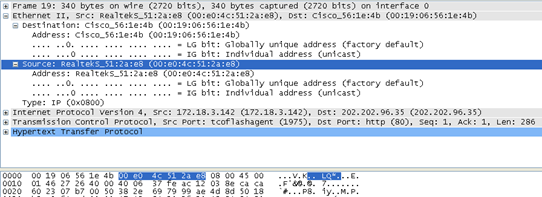


（2）http应用的以太网链路数据帧

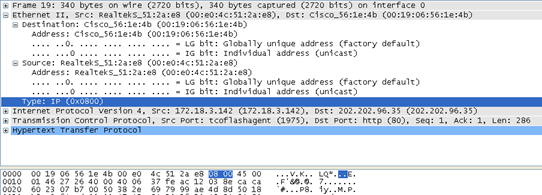
目的地址：00 19 06 56 1e 4b（6个字节）



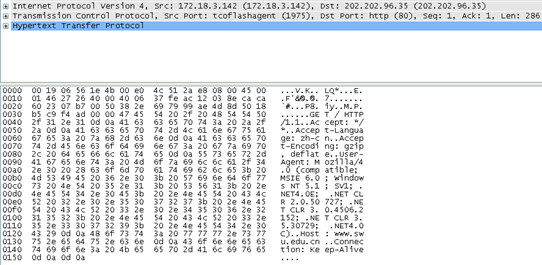
源地址：00 e0 4c 51 2a e6（6个字节）



类型：08 00类型（2个字节）



数据： 4500014627264000400637feac12038ecaca602307b70050382e697999ae4d8d5018b5c9f4ad0000474554202f20485454502f312e310d0a4163636570743a202a2f2a0d0a4163636570742d4c616e67756167653a207a682d636e0d0a4163636570742d456e636f64696e673a20677a69702c206465666c6174650d0a557365722d4167656e743a204d6f7a696c6c612f342e302028636f6d70617469626c653b204d53494520362e303b2057696e646f7773204e5420352e313b205356313b202e4e4554342e30453b202e4e455420434c5220322e302e35303732373b202e4e455420434c5220332e302e343530362e323135323b202e4e455420434c5220332e352e33303732393b202e4e4554342e3043290d0a486f73743a207777772e7377752e6564752e636e0d0a436f6e6e656374696f6e3a204b6565702d416c6976650d0a0d0a



（3）校园网登录过程的以太网链路数据帧格式与内容

目的地址：00 19 06 56 1e 4b (6个字节)

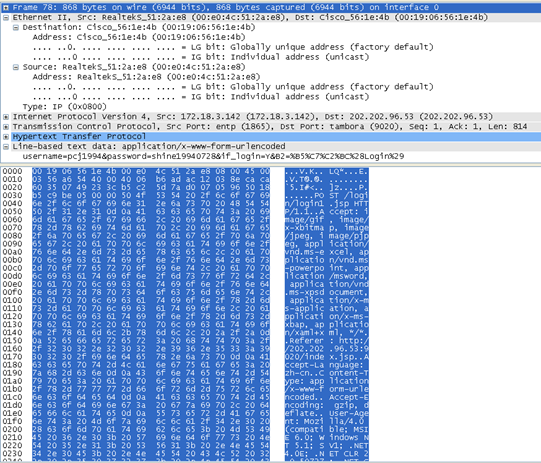
源地址：00 e0 4c 51 2a e8(6个字节)

类型：08 00（2个字节）

数据：

**757365726e616d653d70636a313939342670617373776f72643d7368696e6531393934303732382669\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*42323d2542352543372543322542432532384c6f67696e253239**

**其中加粗部分为抓取到得用户名与密码，该方式传输的密码字段为明文传输，未加密，不安全！**



（4）校园网退出登录过程的以太网链路数据帧格式与内容

目的地址：00 19 06 56 1e 4b (6个字节)

源地址：00 e0 4c 51 2a e8 (6个字节)

类型：08 00（2个字节）

数据：





（3）与（4）的网页一样，目的地址与源地址一样，只是传输数据不同，（3）是登录，（4）是退出

（5）FTP登录过程的以太网链路数据帧格式与内容

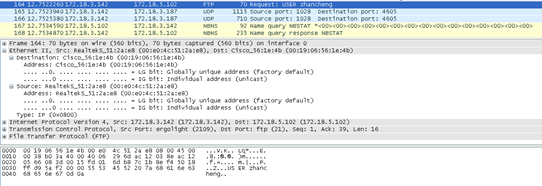
目的地址：00 19 06 56 1e 4b (6个字节)

源地址：00 e0 4c 51 2a e8 (6个字节)

类型：08 00（2个字节）

数据：

45000038b03a40004006296dac12038eac120566083d0015fd016db87c1b8ef45018ffd95af2000055534552207a68616e6368656e670d0a



从以上分析以太网链路数据帧格式与内容的过程中，发现部分网站的用户名密码采用明文传输，很容易被抓取到，非常不安全，这些网站应该改进传输方式！

# 2．网络层协议分析

# [地址解析协议ARP，网络层协议IP、ICMP协议](http://www.cnblogs.com/leftshine/p/5698848.html)

分析所用软件下载：[Wireshark-win32-1.10.2.exe](https://pan.baidu.com/s/1pLH6gUB)

任务：

[1. 分析IP协议](http://www.cnblogs.com/leftshine/p/5698848.html#_1.分析arp报文的格式与内容)

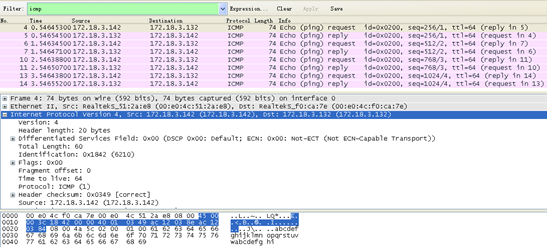
[2．分析ARP协议](http://www.cnblogs.com/leftshine/p/5698848.html#_2._分析ip报文的格式与内容)

[3．分析ICMP协议](http://www.cnblogs.com/leftshine/p/5698848.html#_3._分析icmp报文的格式与内容)

## 2.1分析ip报文的格式与内容

(1)ping 172.18.3.132 过程中icmp回送请求的ip报文：

4500003c1842000040010349ac12038eac120384



版本（Version）：4

首部长度（Header length）： 5 - 20 bytes

服务类型（Differentiated Services Field）：00

-0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

总长度（Total Length）：003c - 60

标识（Identification）：18 42 - 0x1842 (6210)

标志（Flags）：00 - 0x00

片偏移量（Fragment offset）：0000 - 0

寿命（Time to live）：40 - 64

协议（Protocol）：01 - ICMP (1)

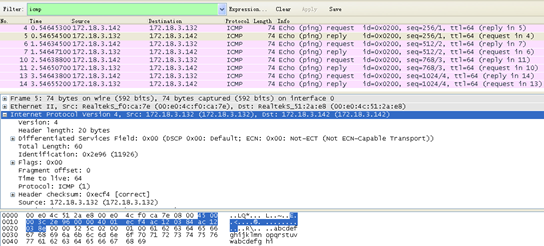
首部校验和（Header checksum）：03 49 - 0x0349 [correct]

源IP地址（Source）：ac 12 03 8e - 172.18.3.142 (172.18.3.142)

目的ip地址（Destination）：ac 12 03 84 -172.18.3.132 (172.18.3.132)

(2)ping 172.18.3.132 过程中icmp回送应答的ip报文：

4500003c2e9600004001ecf4ac120384ac12038e



版本（Version）：4

首部长度（Header length）： 5 - 20 bytes

服务类型（Differentiated Services Field）：00

-0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

总长度（Total Length）：003c - 60

标识（Identification）：2e 96 - 0x2e96 (11926)

标志（Flags）：00 - 0x00

片偏移量（Fragment offset）：0000 - 0

寿命（Time to live）：40 - 64

协议（Protocol）：01 - ICMP (1)

首部校验和（Header checksum）：ec f4 - 0xecf4 [correct]

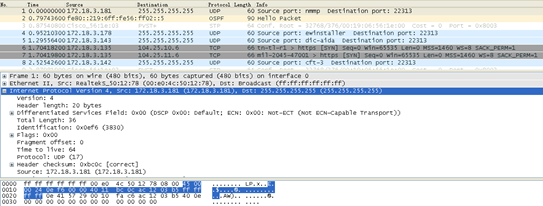
源IP地址（Source）：ac 12 03 84 -172.18.3.132 (172.18.3.132)

目的ip地址（Destination）：ac 12 03 8e - 172.18.3.142 (172.18.3.142)

数据：为icmp报文

(3)访问swu.edu.cn 过程中某UDP协议的ip报文：

450000240ef600004011bc0cac1203b5ffffffff



以太帧类型 TYPE=0800

版本（Version）：4

首部长度（Header length）： 5 - 20 bytes

服务类型（Differentiated Services Field）：00

-0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

总长度（Total Length）：00 24 - 36

标识（Identification）：0e f6 - 0x0ef6 (3830)

标志（Flags）：00 - 0x00

片偏移量（Fragment offset）：0000 - 0

寿命（Time to live）：40 - 64

协议（Protocol）：11 - UDP (17)

首部校验和（Header checksum）：bc 0c - 0xbc0c [correct]

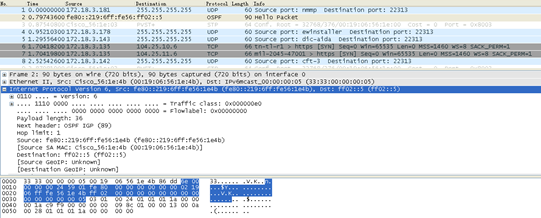
源IP地址（Source）：ac 12 03 b5 -172.18.3.181 (172.18.3.181)

目的ip地址（Destination）：ff ff ff ff - 255.255.255.255 (255.255.255.255)

数据：为UDP报文

(4)访问swu.edu.cn 过程中某OSPF协议的ip报文：

6e00000000245901fe80000000000000021906fffe561e4bff020000000000000000000000000005



 以太帧类型 TYPE=86dd

版本（Version）：6

流量类型（Traffic class）： = e 0

位流标记（ Flowlabel）： 0 00 00

载荷长度(Payload length)：00 24 - 36

下一个报头（Next header）: 59 -OSPF IGP (89)

跳数限制（Hop limit）: 01 - 1

源ip地址(Source): fe 80 00 00 00 00 00 00 02 19 06 ff fe 56 1e 4b

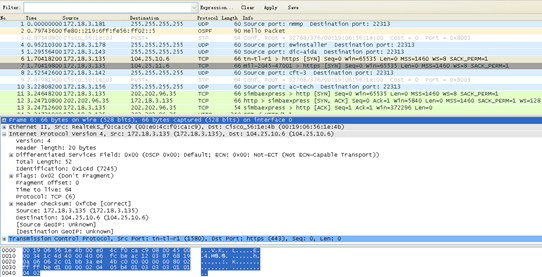
- fe80::219:6ff:fe56:1e4b

目的ip（Destination）: ff 02 00 00 00 00 00 00 00 00 00 00 00 00 00 05

- ff02::5

(5)访问swu.edu.cn 过程中某tcp协议的ip报文：

450000341c4d40004006fcbeac12038768190a06



版本（Version）：4

首部长度（Header length）： 5 - 20 bytes

服务类型（Differentiated Services Field）：00

-0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

总长度（Total Length）：00 34 - 52

标识（Identification）：1c 4d - 0x1c4d (7245)

标志（Flags）：40 - 0x02（ Don't Fragment)

片偏移量（Fragment offset）：0000 - 0

寿命（Time to live）：40 - 64

协议（Protocol）：06 - TCP (6)

首部校验和（Header checksum）：fc be - 0xfcbe [correct]

源IP地址（Source）：ac 12 03 87 -172.18.3.135

目的ip地址（Destination）：68 19 0a 06 - 104.25.10.6

数据：为TCP报文

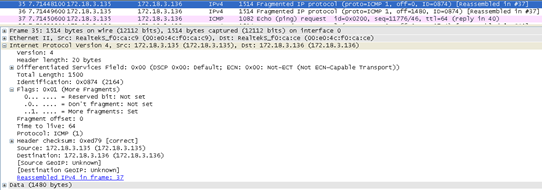
**分析ip分片报文的格式与内容**

（1） ping -l 4000 172.18.3.136 过程中icmp回送请求的ip分片报文：

本次ip报文被分成3片：

第一个分片

45000034087340004006cacdac120387246e937c



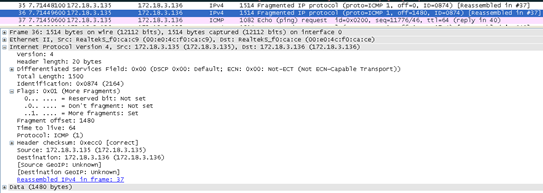
DF：0

MF：1

Fragment offset: 0

第二个分片：

450005dc087420b94001ecc0ac120387ac120388



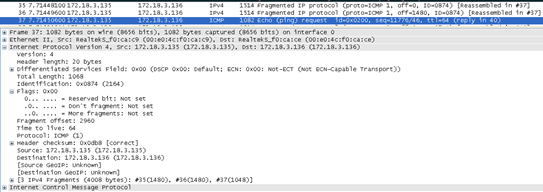
DF：0

MF：1

Fragment offset: 1480

第三个分片：

4500042c0874017240010db8ac120387ac120388



DF：0

MF：0

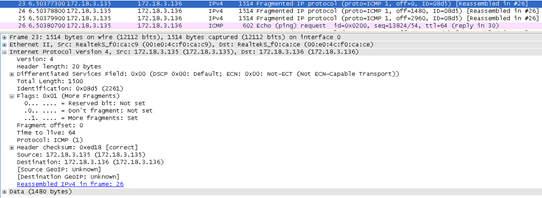
Fragment offset: 2960

（2） ping -l 5000 172.18.3.136 过程中icmp回送请求的ip分片报文

本次ip报文被分成4片：

第一个分片

450005dc08d520004001ed18ac120387ac120388



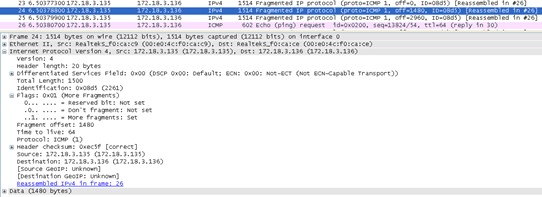
DF：0

MF：1

Fragment offset: 0

第二个分片：

450005dc08d520b94001ec5fac120387ac120388



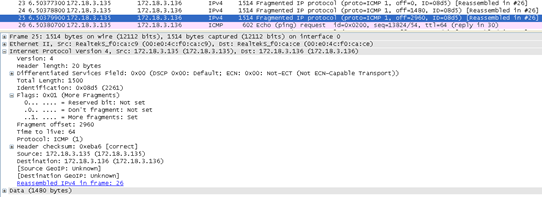
DF：0

MF：1

Fragment offset: 1480

第三个分片：

450005dc08d521724001eba6ac120387ac120388



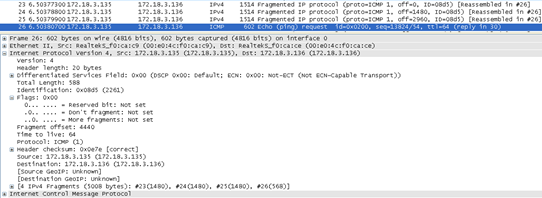
DF：0

MF：1

Fragment offset: 2960

第四个分片：

4500024c08d5022b40010e7eac120387ac120388



DF：0

MF：0

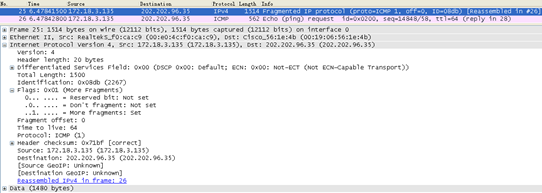
Fragment offset: 4440

（3）ping -l 2000 202.202.96.35 过程中icmp回送请求的ip分片报文

本次ip报文被分成2片：

第一个分片

450005dc08db2000400171bfac120387caca6023



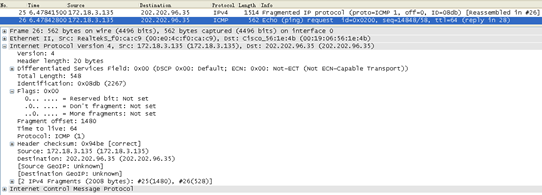
DF：0

MF：1

Fragment offset: 0

第二个分片：

4500022408db00b9400194beac120387caca6023



DF：0

MF：0

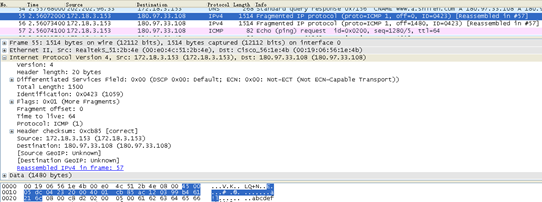
Fragment offset: 1480

（4）ping -l 3000 [www.baidu.com](http://www.baidu.com/)（未ping通） 过程中icmp回送请求1的ip分片报文

本次ip报文被分成3片：

第一个分片

450005dc042320004001cb85ac120399b461216c



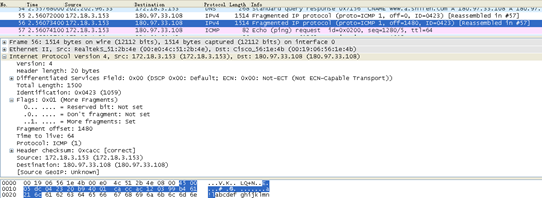
DF：0

MF：1

Fragment offset: 0

第二个分片：

450005dc042320b94001caccac120399b461216c



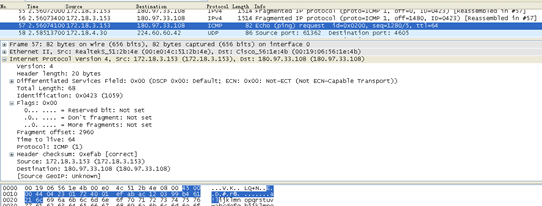
DF：0

MF：1

Fragment offset: 1480

第三个分片：

45000044042301724001efabac120399b461216c



DF：0

MF：0

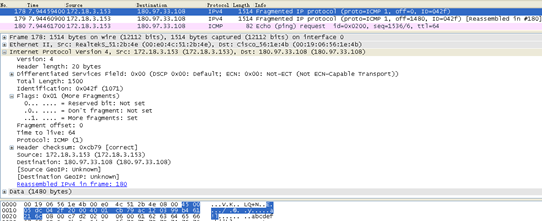
Fragment offset: 2960

（5）ping -l 3000 [www.baidu.com](http://www.baidu.com/)（未ping通） 过程中icmp回送请求2的ip分片报文

本次ip报文被分成3片：

第一个分片

450005dc042f20004001cb79ac120399b461216c



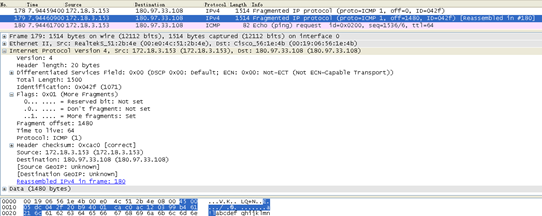
DF：0

MF：1

Fragment offset: 0

第二个分片：

450005dc042f20b94001cac0ac120399b461216c



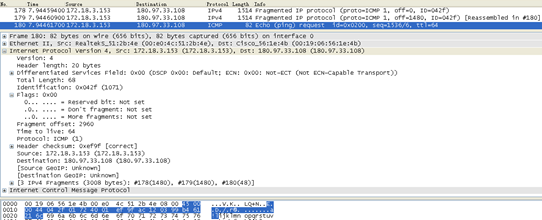
DF：0

MF：1

Fragment offset: 1480

第三个分片：

45000044042f01724001ef9fac120399b461216c



DF：0

MF：0

Fragment offset: 2960

在进行ip分片报文分析实验的时候，注意使用ping –l命令设置合适ip报文的长度以达到不同的分片效果。

## 2.2分析arp报文的格式与内容

(1)ping 172.18.3.132 的arp请求报文：

000108000604000100e04c512ae8ac12038e000000000000ac120384



物理网络类型Hardware type: 0001 - Ethernet (1)

协议类型Protocol type: 0800 - IP (0x0800)

物理地址长度Hardware size: 06 - 6

协议地址长度Protocol size: 04 - 4

操作Opcode: 0001 - request (1)：

发送方物理地址Sender MAC address:

00e04c512ae8 - RealtekS\_51:2a:e8 (00:e0:4c:51:2a:e8)

发送方IP地址Sender IP address:

ac12038e - 172.18.3.142 (172.18.3.142)

目标物理地址Target MAC address:

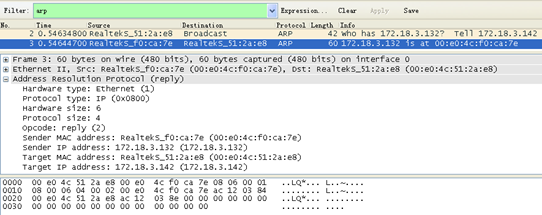
000000000000 - 00:00:00\_00:00:00 (00:00:00:00:00:00)

目标IP地址Target IP address:

ac120384 - 172.18.3.132 (172.18.3.132)

(2)ping 172.18.3.132 的arp响应报文：

000108000604000200e04cf0ca7eac12038400e04c512ae8ac12038e



物理网络类型Hardware type: 0001 - Ethernet (1)

协议类型Protocol type: 0800 - IP (0x0800)：

物理地址长度Hardware size: 06 - 6

协议地址长度Protocol size: 04 - 4

操作Opcode: 0002 - reply (2)

发送方物理地址Sender MAC address:

00e04cf0ca7e - RealtekS\_f0:ca:7e (00:e0:4c:f0:ca:7e)

发送方IP地址Sender IP address:

ac120384 - 172.18.3.132 (172.18.3.132)：

目标物理地址Target MAC address:

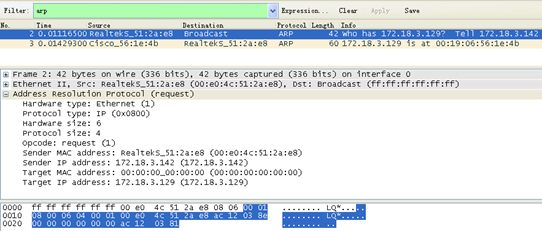
00e04c512ae8 - RealtekS\_51:2a:e8 (00:e0:4c:51:2a:e8)

目标IP地址Target IP address:

ac12038e - 172.18.3.142 (172.18.3.142)：

(3)ping 202.202.96.35（西南大学主页） 的arp请求报文：

000108000604000100e04c512ae8ac12038e000000000000ac120381



物理网络类型Hardware type: 0001 - Ethernet (1)

协议类型Protocol type: 0800 - IP (0x0800)

物理地址长度Hardware size: 06 - 6

协议地址长度Protocol size: 04 - 4

操作Opcode: 0001 - request (1)：

发送方物理地址Sender MAC address:

00e04c512ae8 - RealtekS\_51:2a:e8 (00:e0:4c:51:2a:e8)

发送方IP地址Sender IP address:

ac12038e - 172.18.3.142 (172.18.3.142)

目标物理地址Target MAC address:

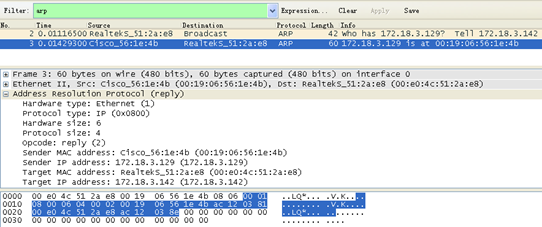
000000000000 - 00:00:00\_00:00:00 (00:00:00:00:00:00)

目标IP地址Target IP address:

ac120381 - 172.18.3.129(172.18.3.129)

(4)ping 202.202.96.35 的arp响应报文：

0001080006040002001906561e4bac12038100e04c512ae8ac12038e



物理网络类型Hardware type: 0001 - Ethernet (1)

协议类型Protocol type: 0800 - IP (0x0800)：

物理地址长度Hardware size: 06 - 6

协议地址长度Protocol size: 04 - 4

操作Opcode: 0002 - reply (2)

发送方物理地址Sender MAC address:

001906561e4b - Cisco\_56:1e:4b (00:19:06:56:1e:4b)

发送方IP地址Sender IP address:

ac120381 - 172.18.3.129 (172.18.3.129)：

目标物理地址Target MAC address:

00e04c512ae8 - RealtekS\_51:2a:e8 (00:e0:4c:51:2a:e8)

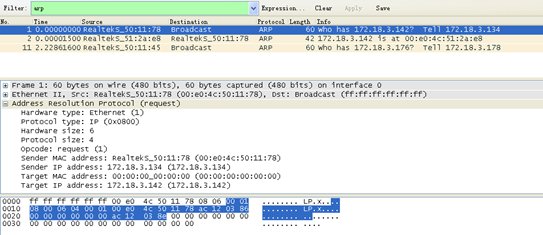
目标IP地址Target IP address:

ac12038e - 172.18.3.142 (172.18.3.142)：

因为202.202.96.35不是局域网内IP所以请求会通过网关送到外网，所以以上操作实际是在与网关通信获取网关的mac地址以建立arp缓存。

(5)由他机（172.18.3.134）ping本机IP（172.18.3.142） 的arp请求报文：

000108000604000100e04c501178ac120386000000000000ac12038e



物理网络类型Hardware type: 0001 - Ethernet (1)

协议类型Protocol type: 0800 - IP (0x0800)：

物理地址长度Hardware size: 06 - 6

协议地址长度Protocol size: 04 - 4

操作Opcode: 0001 - request (1)

发送方物理地址Sender MAC address:

00e04c501178 - RealtekS\_50:11:78 (00:e0:4c:50:11:78)

发送方IP地址Sender IP address:

ac120386 - 172.18.3.134 (172.18.3.134)：

目标物理地址Target MAC address:

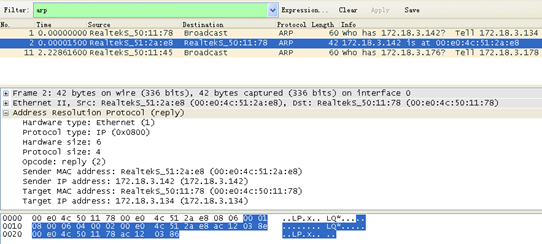
000000000000 - 00:00:00\_00:00:00 (00:00:00:00:00:00)

目标IP地址Target IP address:

ac12038e - 172.18.3.142 (172.18.3.142)：

(6) 由他机（172.18.3.134）ping本机IP（172.18.3.142） 的arp响应报文：

000108000604000200e04c512ae8ac12038e00e04c501178ac120386



物理网络类型Hardware type: 0001 - Ethernet (1)

协议类型Protocol type: 0800 - IP (0x0800)

物理地址长度Hardware size: 06 - 6

协议地址长度Protocol size: 04 - 4

操作Opcode: 0001 - request (1)：

发送方物理地址Sender MAC address:

00e04c512ae8 - RealtekS\_51:2a:e8 (00:e0:4c:51:2a:e8)

发送方IP地址Sender IP address:

ac12038e - 172.18.3.142 (172.18.3.142)

目标物理地址Target MAC address:

00e04c501178 - RealtekS\_50:11:78 (00:e0:4c:50:11:78)

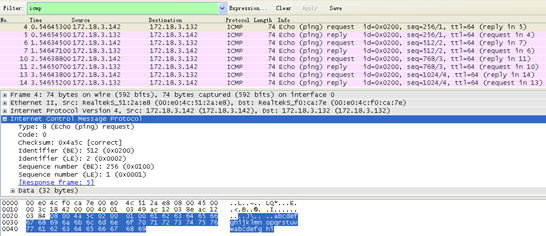
目标IP地址Target IP address:

ac120386 - 172.18.3.134(172.18.3.134)

## 2.3分析icmp报文的格式与内容

(1)ping 172.18.3.132 的icmp回送请求报文1：

08004a5c020001006162636465666768696a6b6c6d6e6f7071727374757677616263646566676869



类型（type）：08 -回送请求

代码（code）：00

校验和（Checksum）：4a 5c

标识Identifier (BE) Identifier (LE)：02 00

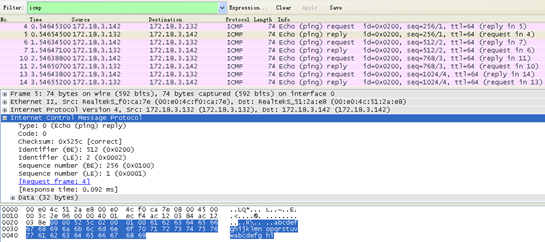
序号Sequence number (BE)、Sequence number (LE)：**01 00**

可选数据（Date）：

6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

(2)ping 172.18.3.132 的icmp回送应答报文1：

0000525c020001006162636465666768696a6b6c6d6e6f7071727374757677616263646566676869



类型（type）：00 -回送应答

代码（code）：00

校验和（Checksum）：52 5c

标识Identifier (BE) Identifier (LE)：02 00

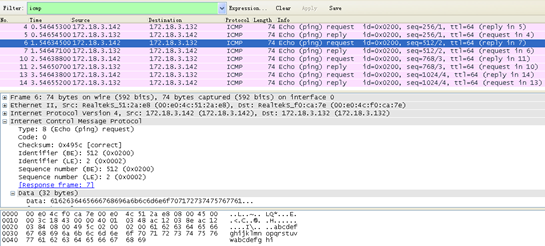
序号Sequence number (BE)、Sequence number (LE)：**01 00**

可选数据（Date）：

6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

(3)ping 172.18.3.132 的icmp回送请求报文2：

0800495c020002006162636465666768696a6b6c6d6e6f7071727374757677616263646566676869



类型（type）：08 -回送请求

代码（code）：00

校验和（Checksum）：49 5c

标识Identifier (BE) Identifier (LE)：02 00

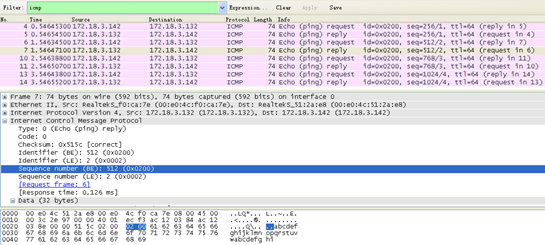
序号Sequence number (BE)、Sequence number (LE)：**02 00**

可选数据（Date）：

6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

(4)ping 172.18.3.132 的icmp回送应答报文2：

0000515c020002006162636465666768696a6b6c6d6e6f7071727374757677616263646566676869



类型（type）：00 -回送应答

代码（code）：00

校验和（Checksum）：51 5c

标识Identifier (BE) Identifier (LE)：02 00

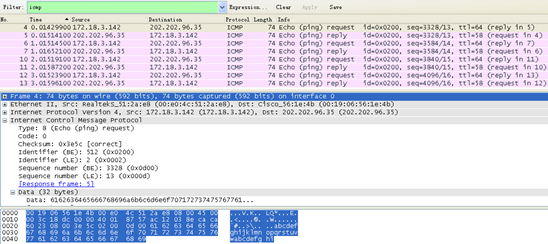
序号Sequence number (BE)、Sequence number (LE)：**02 00**

可选数据（Date）：

6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

(5) 202.202.96.35（西南大学主页） 的icmp回送请求报文1：

08003e5c02000d006162636465666768696a6b6c6d6e6f7071727374757677616263646566676869



类型（type）：08 -回送请求

代码（code）：00

校验和（Checksum）：3e 5c

标识Identifier (BE) Identifier (LE)：02 00

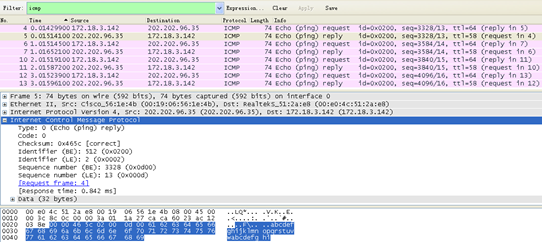
序号Sequence number (BE)、Sequence number (LE)：**0d 00**

可选数据（Date）：

6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

(6)ping202.202.96.35（西南大学主页） 的icmp回送应答报文1：

0000465c02000d006162636465666768696a6b6c6d6e6f7071727374757677616263646566676869



类型（type）：00 -回送应答

代码（code）：00

校验和（Checksum）：46 5c

标识Identifier (BE) Identifier (LE)：02 00

序号Sequence number (BE)、Sequence number (LE)：**0d 00**

可选数据（Date）：

6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

由上述实验看出：

成对的icmp请求和应答报文的标识和序号字段相同。

Ping命令基于icmp回送请求和应答报文工作，它的作用是检测一个目的站是否可达。

Icmp用于解决控制问题和实现报错机制，它可以帮助维护Internet的投递秩序。

# 3．传输层协议分析

# [传输层协议TCP和UDP分析](http://www.cnblogs.com/leftshine/p/5698867.html)

分析所用软件下载：[Wireshark-win32-1.10.2.exe](https://pan.baidu.com/s/1pLH6gUB)

任务：

1. 分析应用TCP协议，以及TCP链接管理

2. 分析应用UDP协议

分析要求

（1）TCP部分：

1. 学习3CDaemon FTP 服务器的配置和使用
2. 设计应用以获取tcp报文
3. 分析tcp报文的格式与内容（分析至少5个报文，并理解它们之间的关系）
4. 分析TCP 连接建立的 "三次握手"过程，找到 对应的报文

（2）UDP部分：

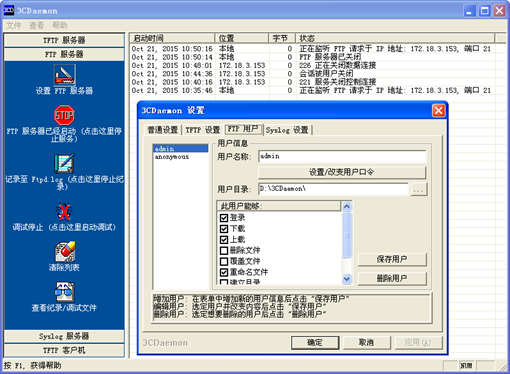
1. 学习Cisco TFTP Server的配置和使用
2. 设计应用以获取udp报文
3. 分析udp报文的格式与内容（分析至少5个报文，并理解它们之间的关系）
4. 分析UDP 报文与TCP 报文有何不同？体会UDP 协议和TCP 协议的区别

**分析内容**

（1）TCP部分：

1. 学习3CDaemon FTP 服务器的配置和使用

下载安装3CDaemon软件并配置FTP服务器部分



1. 设计应用以获取tcp报文

使用3CDaemon 系统内置的匿名帐户 "anonymous"登陆FTP 服务器以获取TCP报文

3．分析tcp报文的格式与内容（分析至少5个报文，并理解它们之间的关系）

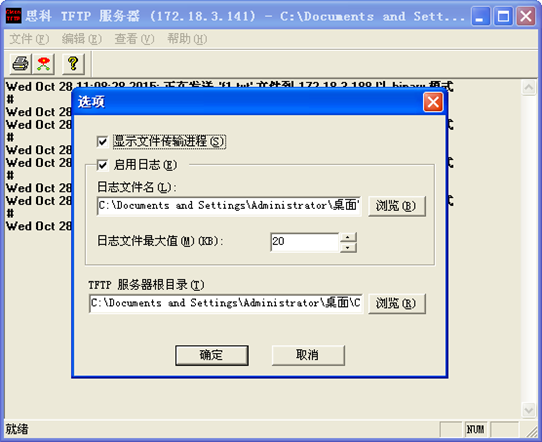
分析见第四部分

4.分析TCP 连接建立和释放连接的 "三次握手"过程，找到 对应的报文。分析见第四部分

（2）UDP部分：

1. 学习Cisco TFTP Server的配置和使用

配置Cisco TFTP Server



1. 设计应用以获取udp报文

使用Windows 命令行模式下的TFTP 客户端命令连接TFTP服务器，下载f1.txt文件：

TFTP –i 172.18.3.188 GET f1.txt

上传f2.txt文件：

TFTP -i 172.18.3.188 PUT f2.txt

同时抓包以获取UDP报文

3分析udp报文的格式与内容（分析至少5个报文，并理解它们之间的关系）

分析见第四部分

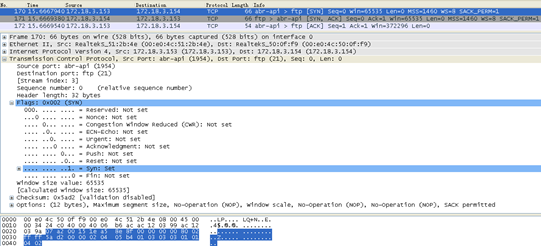
4.分析UDP 报文与TCP 报文有何不同？体会UDP 协议和TCP 协议的区别

分析结果及总结

## 3.1 获取并分析tcp报文

（1）登录ftp服务器：172.18.3.154建立TCP连接的第一次握手报文--SYN报文：

07a200151ea58e8f000000008002ffff5ad20000020405b40103030301010402



源端口：07a2

Source port: abr-api (1954)

目的端口：0015

Destination port: ftp (21)

序号：1e a5 8e 8f

Sequence number: 0 (relative sequence number)

首部长度：8

Header length: 32 bytes

码元比特：02

Flags: 0x002 (SYN)

窗口：ff ff

Window size value: 65535

Calculated window size: 65535

校验和：5ad2

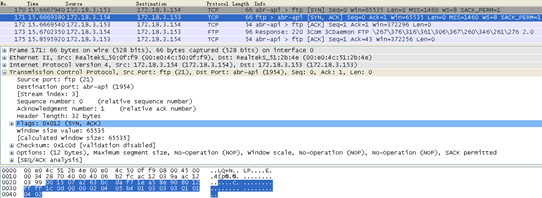
Checksum: 0x5ad2 [validation disabled]

选项：02 04 05 b4 01 03 03 03 01 01 04 02

Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted

（2）登录ftp服务器：172.18.3.154建立TCP连接的第二次握手报文--SYN+ACK报文：

00e04c512b4e00e04c500ff9080045000034287040004006b2fcac12039aac120399001507a263bcdaf71ea58e908012ffff1c0d0000020405b40103030301010402



源端口：00 15

Source port: ftp (21)

目的端口：07 a2

Destination port: abr-api (1954)

序号：63 bc da f7

Sequence number: 0 (relative sequence number)

确认号：1e a5 8e 90

Acknowledgment number: 1 (relative ack number)

首部长度：8

Header length: 32 bytes

码元比特：12

Flags: 0x012 (SYN, ACK)

窗口：ff ff

Window size value: 65535

Calculated window size: 65535

校验和：1c 0d

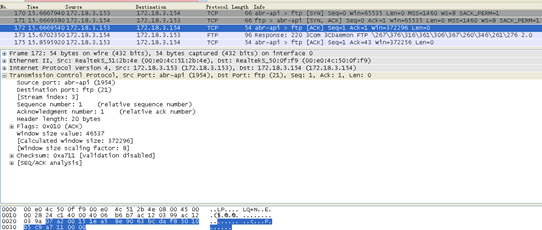
Checksum: 0x1c0d [validation disabled]

选项：020405b40103030301010402

Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted

（3）登录ftp服务器：172.18.3.154建立TCP连接的第三次握手报文--ACK报文：

07a200151ea58e9063bcdaf85010b5c9a7110000



源端口：07a2

Source port: abr-api (1954)

目的端口：0015

Destination port: ftp (21)

序号：1e a5 8e 90

Sequence number: 1 (relative sequence number)

确认号：63 bc da f8

Acknowledgment number: 1 (relative ack number)

首部长度：5

Header length: 20 bytes

码元比特：10

Flags: 0x010 (ACK)

窗口：b5 c9

Window size value: 46537

Calculated window size: 372296

Window size scaling factor: 8

校验和：a7 11

Checksum: 0xa711 [validation disabled]

（4）ftp服务器：172.18.3.154断开TCP连接的FIN+ACK seq=x报文：

00e04c512b4e00e04c500ff908004500002854fb40004006867dac12039aac12039900150966cb76f9c531de53865011b5b846a70000000000000000



源端口：00 15

Source port: ftp (21)

目的端口：09 66

Destination port: jediserver (2406)

序号：cb 76 f9 c5

Sequence number: 437 (relative sequence number)

确认号：31 de 53 86

Acknowledgment number: 135 (relative ack number)

首部长度：5

Header length: 20 bytes

码元比特：11

Flags: 0x011 (FIN, ACK)

窗口：b5 b8

Window size value: 46520

Calculated window size: 372160

Window size scaling factor: 8

校验和：46 a7

Checksum: 0x46a7 [validation disabled]

（5）ftp服务器：172.18.3.154断开TCP连接的ACK x+1报文：

0966001531de5386cb76f9c65010b59346cc0000



源端口：09 66

Source port: jediserver (2406)

目的端口：00 15

Destination port: ftp (21)

序号：31 de 53 86

Sequence number: 135 (relative sequence number)

确认号：cb 76 f9 c6

Acknowledgment number: 438 (relative ack number)

首部长度：5

Header length: 20 bytes

码元比特：10

Flags: 0x010 (ACK)

窗口：b5 93

Window size value: 46483

Calculated window size: 371864

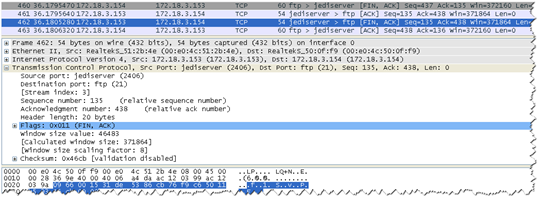
Window size scaling factor: 8

校验和：46 cc

Checksum: 0x46cc [validation disabled]

（6）ftp服务器：172.18.3.154断开TCP连接的FIN seq =y ，ACK +1报文：

0966001531de5386cb76f9c65011b59346cb0000



源端口：09 66

Source port: jediserver (2406)

目的端口：00 15

Destination port: ftp (21)

序号：31 de 53 86

Sequence number: 135 (relative sequence number)

确认号：cb 76 f9 c6

Acknowledgment number: 438 (relative ack number)

首部长度：5

Header length: 20 bytes

码元比特：11

Flags: 0x011 (FIN, ACK)

窗口：b5 93

Window size value: 46483

Calculated window size: 371864

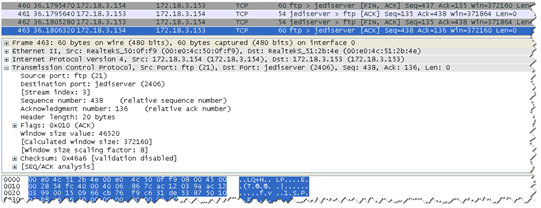
Window size scaling factor: 8

校验和：46 cb

Checksum: 0x46cb [validation disabled]

（7）ftp服务器：172.18.3.154断开TCP连接的ACK y+1报文：

00e04c512b4e00e04c500ff908004500002854fc40004006867cac12039aac12039900150966cb76f9c631de53875010b5b846a60000000000000000



源端口：00 15

Source port: ftp (21)

目的端口：09 66

Destination port: jediserver (2406)

序号：cb 76 f9 c6

Sequence number: 438 (relative sequence number)

确认号：31 de 53 87

Acknowledgment number: 136 (relative ack number)

首部长度：5

Header length: 20 bytes

码元比特：10

Flags: 0x010 (ACK)

窗口：b5 b8

Window size value: 46520

Calculated window size: 372160

Window size scaling factor: 8

校验和：46 a6

Checksum: 0x46a6 [validation disabled]

**TCP连接建立过程总结：**

**客户端发送序号为x的SYN报文，服务器接收后发送序号为y的SYN与序号为x+1 的ACK 报文，客户端接收后，发送序号为y+1的ACK报文，TCP以此顺序建立三次握手。**

**TCP连接的正常关闭总结：**

**网点1发送序号为x的FIN报文，网点2接收后发送序号为x+1的ACK 报文，网点2再发送序号为y的FIN与序号为x+1的ACK报文，网点1接收后发送序号为y+1的ACK报文，网点2接收该报文，连接正常关闭。如果将第二个报文与第三个报文合并，就变成为三次握手方法。**

## 3.2获取并分析UDP报文

（1）TFTP –i 172.18.3.188 GET f1.txt的第一个UDP报文：

0c3e00450017bd5c



源端口：0c 3e

Source Port: 3134 (3134)

目的端口：0045

Destination Port: 69 (69)

报文长度：00 17

Length: 23

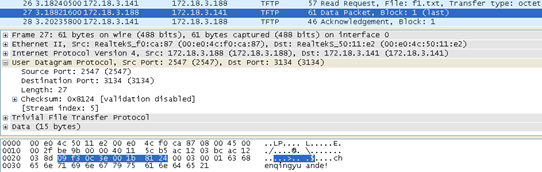
校验和：bd 5c

Checksum: 0xbd5c [validation disabled]

数据为TFTP报文

（2）TFTP –i 172.18.3.188 GET f1.txt的第二个UDP报文：

09f30c3e001b8124



源端口：09 f3

Source Port: 2547 (2547)

目的端口：0c3e

Destination Port: 3134 (3134)

报文长度：00 1b

Length: 27

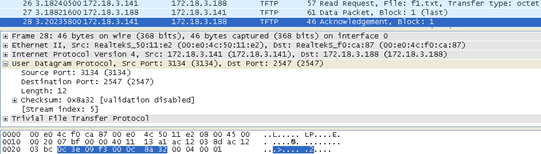
校验和：81 24

Checksum: 0x8124 [validation disabled]

数据为TFTP报文

（3）TFTP –i 172.18.3.188 GET f1.txt的第三个UDP报文：

0c3e09f3000c8a32



源端口：0c 3e

Source Port: 3134 (3134)

目的端口：09 f3

Destination Port: 2547 (2547)

报文长度：00 0c

Length: 12

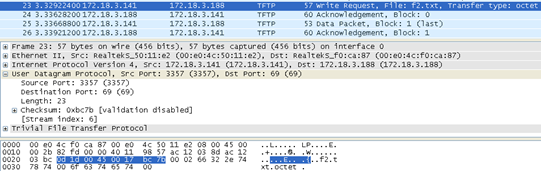
校验和：8a 32

Checksum: 0x8a32 [validation disabled]

数据为TFTP报文

（4）TFTP –i 172.18.3.188 PUT f2.txt的第一个UDP报文：

0d1d00450017bc7b



源端口：0d 1d

Source Port: 3357 (3357)

目的端口：00 45

Destination Port: 69 (69)

报文长度：00 17

Length: 23

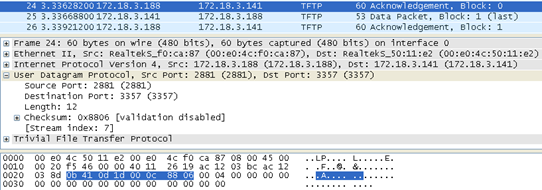
校验和：bc 7b

Checksum: 0xbc7b [validation disabled]

数据为TFTP报文

（5）TFTP –i 172.18.3.188 PUT f2.txt的第二个UDP报文：

0b410d1d000c8806



源端口：0b 41

Source Port: 2881 (2881)

目的端口：0d 1d

Destination Port: 3357 (3357)

报文长度：00 0c

Length: 12

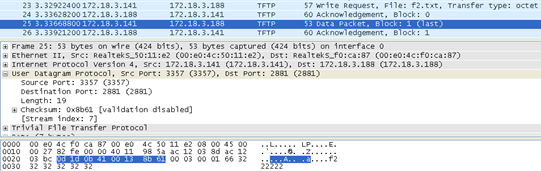
校验和：88 06

Checksum: 0x8806 [validation disabled]

数据为TFTP报文

（6）TFTP –i 172.18.3.188 PUT f2.txt的第三个UDP报文：

0d1d0b4100138b61



源端口：0d 1d

Source Port: 3357 (3357)

目的端口：0b 41

Destination Port: 2881 (2881)

报文长度：00 13

Length: 19

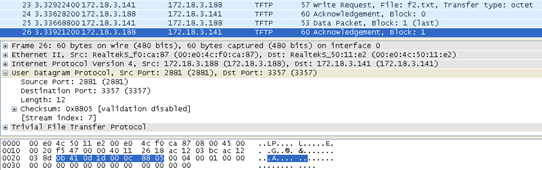
校验和：8b 61

Checksum: 0x8b61 [validation disabled]

数据为TFTP报文

（7）TFTP –i 172.18.3.188 PUT f2.txt的第四个UDP报文：

0b410d1d000c8805



源端口：0b 41

Source Port: 2881 (2881)

目的端口：0d 1d

Destination Port: 3357 (3357)

报文长度：00 0c

Length: 12

校验和：88 05

Checksum: 0x8805 [validation disabled]

数据为TFTP报文

**UDP 报文与TCP 报文有何不同：**

**UDP报文比TCP报文简短，且不用建立连接，TCP是可靠传输协议，UDP是不可靠传输协议。UDP传输速度比TCP快，适用于一些对速度要求高，精确度要求较低的连接。**