**武汉大学国际软件学院**

**实验报告**

**课程名称 网络及分布式计算实验**

**专业年级 2014级软件工程**

**姓 名**

**学 号**

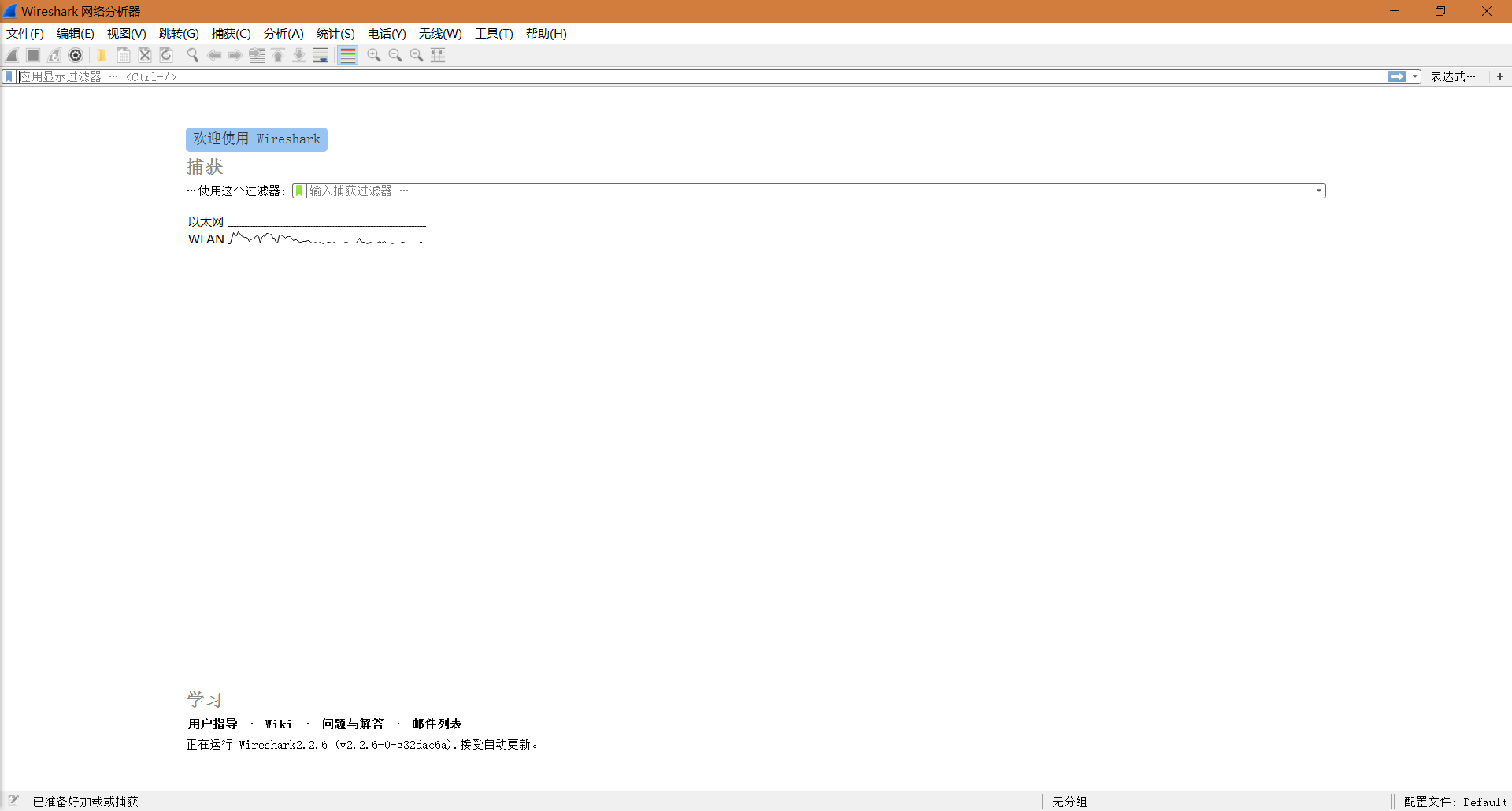
**实验学期 2016-2017　 学年 第1 学期**

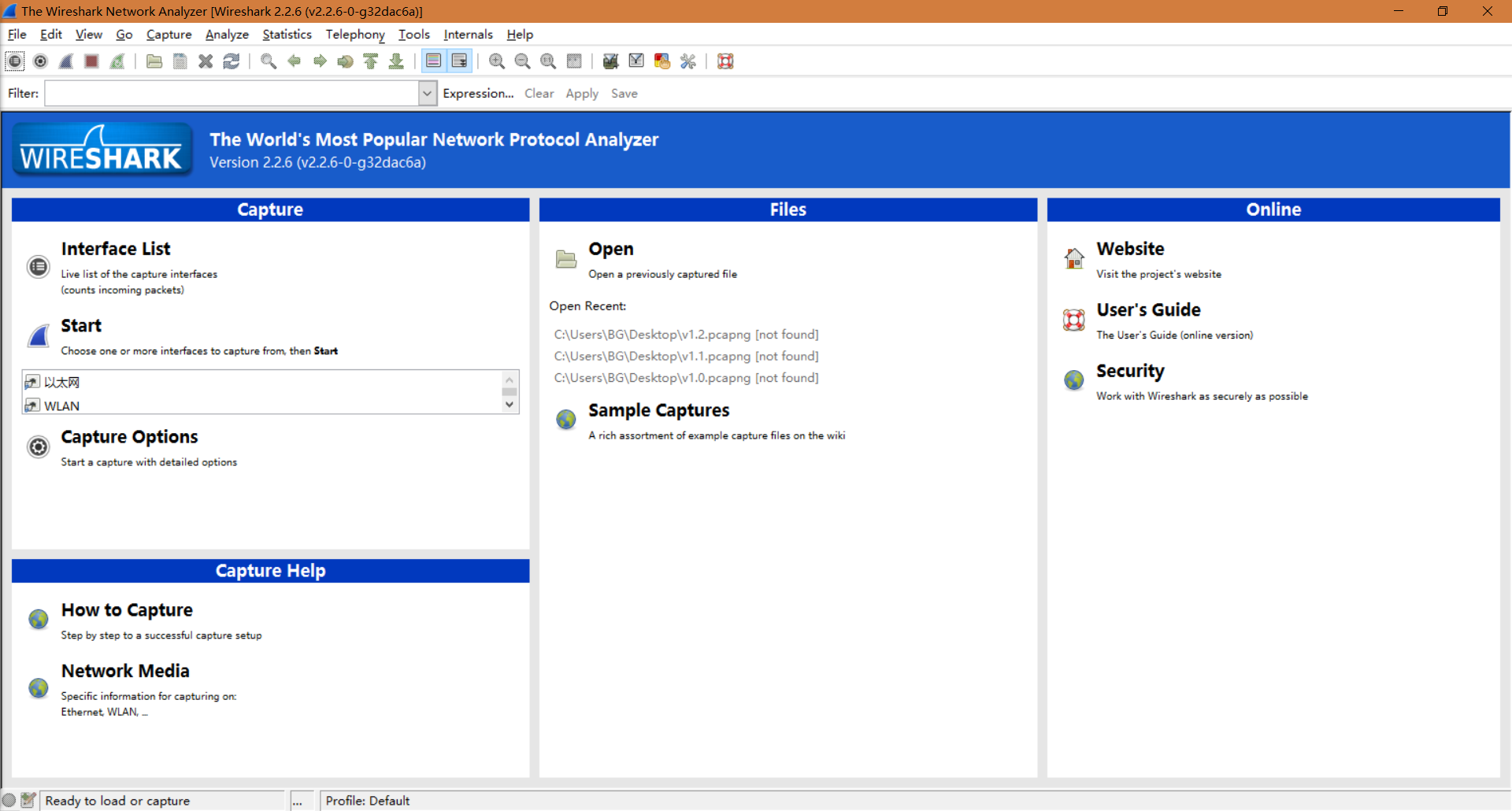
**课堂时数 课外时数**

**填写时间 2017 年 5 月 12 日**

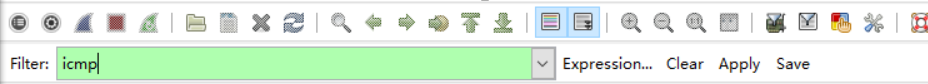
**实验任务四**

1. 下载安装Wireshark

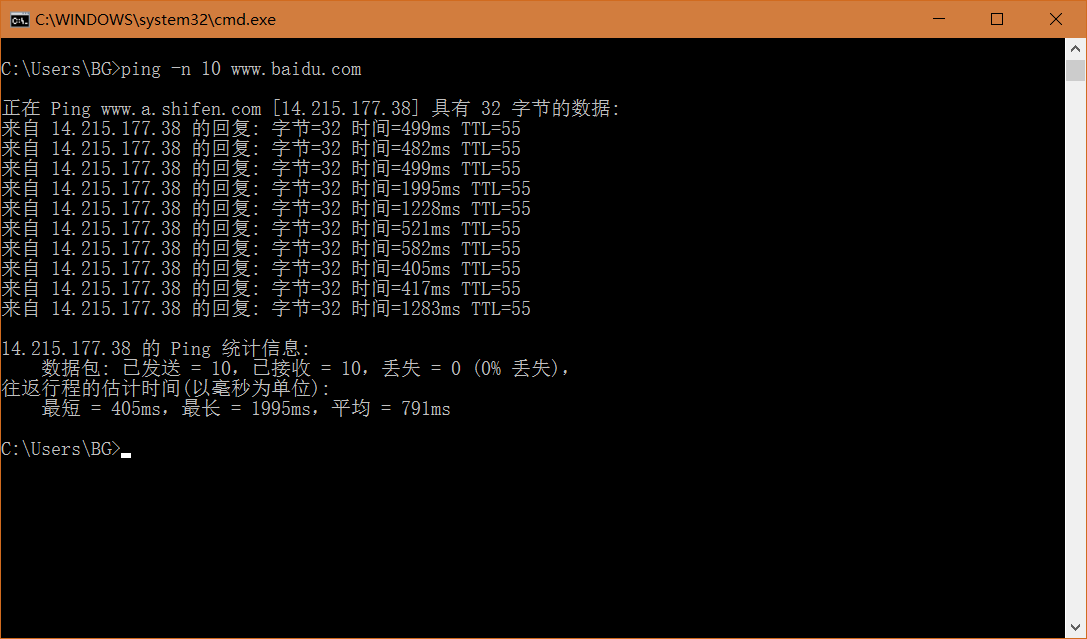




1. 利用ping程序产生ICMP分组，抓取ICMP数据包，具体过程如下：
   1. 打开Windows命令提示符窗口，启动Wireshark分组嗅探器，在过滤窗口输入ICMP：

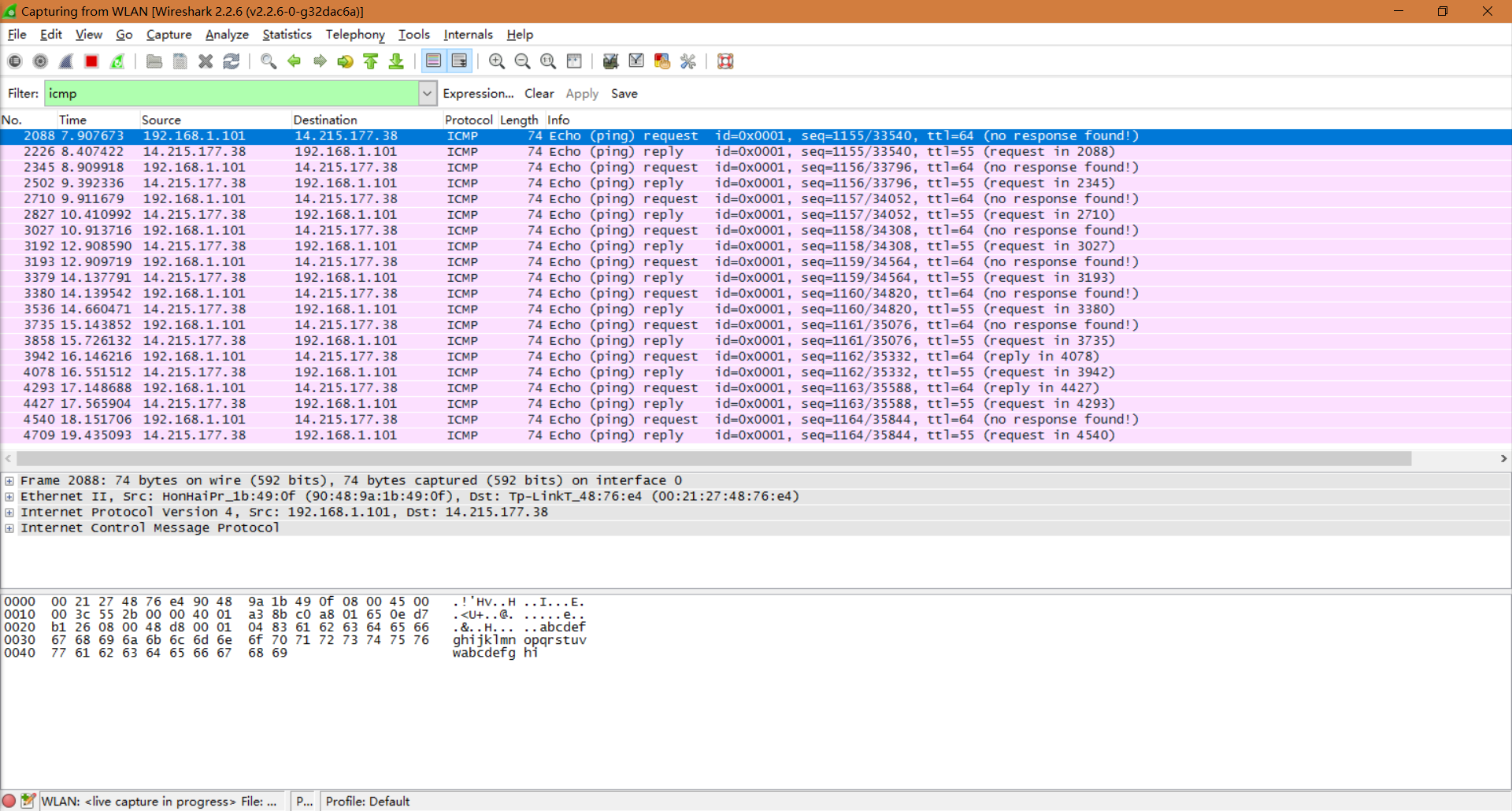


* 1. 在命令提示符界面输入“ping -n 10 www.baidu.com”，返回十条ping信息：



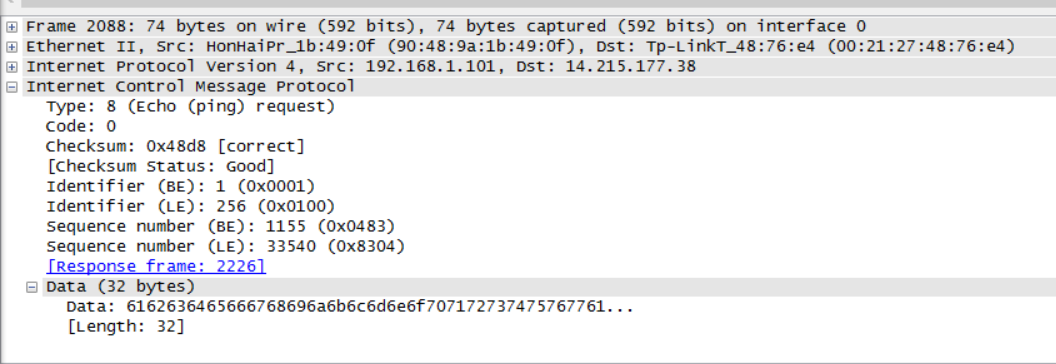
从图上可以看出连续收到了10个ping的恢复，每次ICMP通讯的过程都是一个ICMP request和ICMP reply，10次通讯加起来一共20个数据包。

* 1. 停止分组捕获后，Wireshark界面如下：

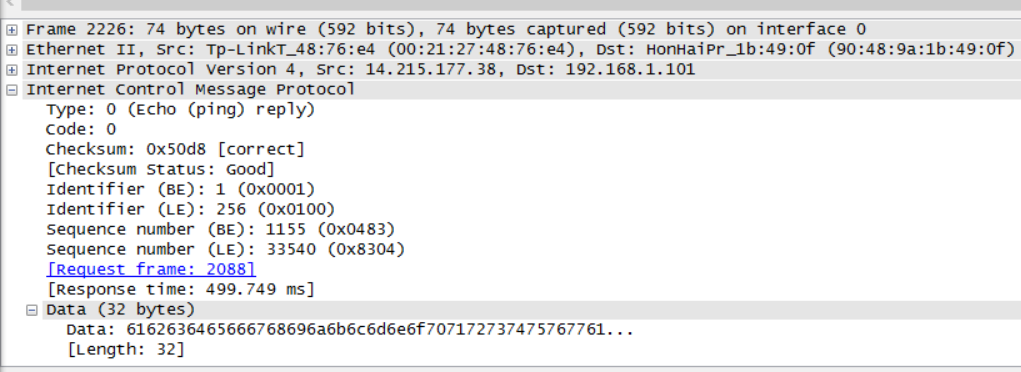


从图上可看到一共被Wireshark捕捉到了20个数据包。

这是一个展开了的ICMP request数据包：



这是一个展开了的ICMP reply数据包：

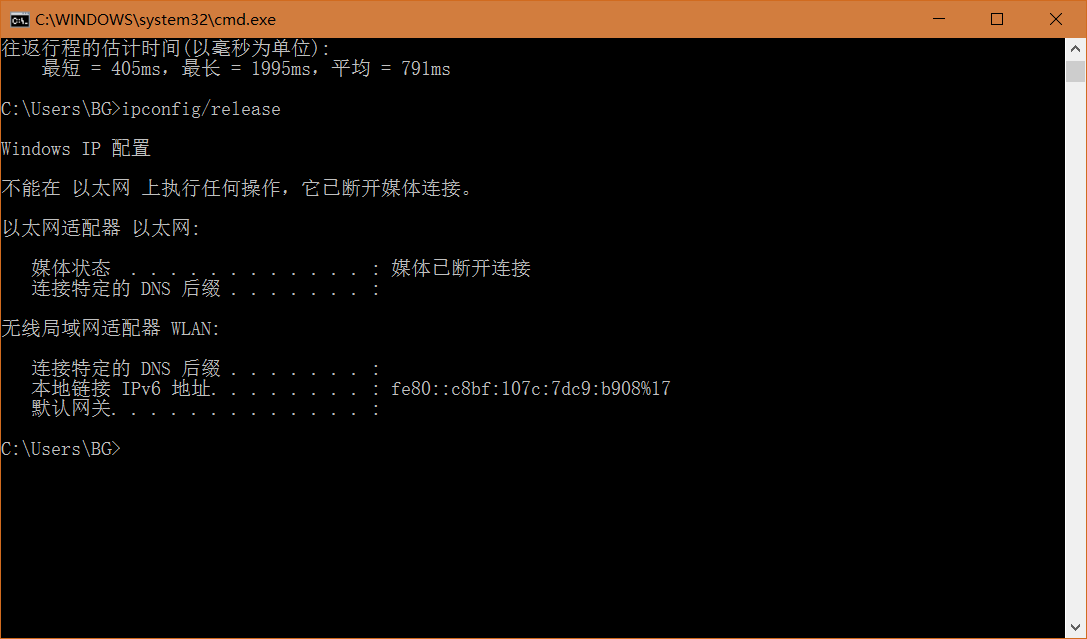


可以获取到信息有：

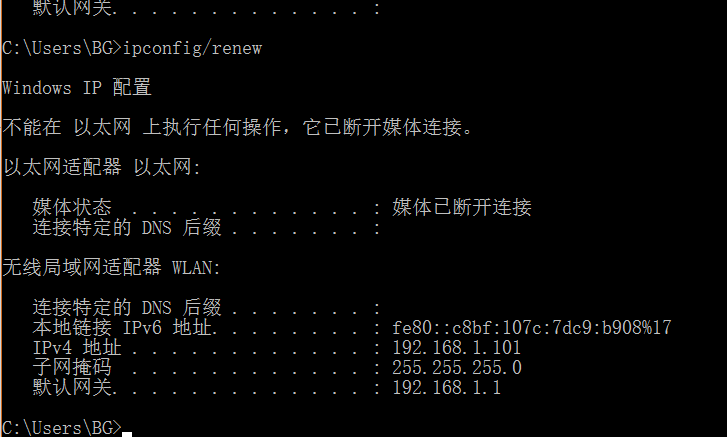
1. Type：类型字段，8代表ICMP的请求
2. Code：代码字段，0代表ICMP的请求
3. Checksum：对ICMP头部的校验值，如果传递过程中ICMP被篡改或损坏，与该值不匹配，接收方就将这个ICMP数据包作废
4. 进程ID标识，从哪个进程产生的ICMP数据包。
5. Sequence Number：序列号，同一个进程中会产生很多个ICMP数据包，用来描述当前这个数据包是哪一个，每一对ICMP request和ICMP reply这个字段应该是一样的
6. Data：ICMP中的数据，一般都是无意义的填充字段，这个部分可能会被黑客加入恶意代码，实施ICMP攻击
7. 利用ipconfig /release 和ipconfig /renew 产生DHCP分组，抓取DHCP数据包，具体过程如下：
   1. 启动Wireshark，启动Wireshark分组嗅探器，在过滤窗口输入bootp：



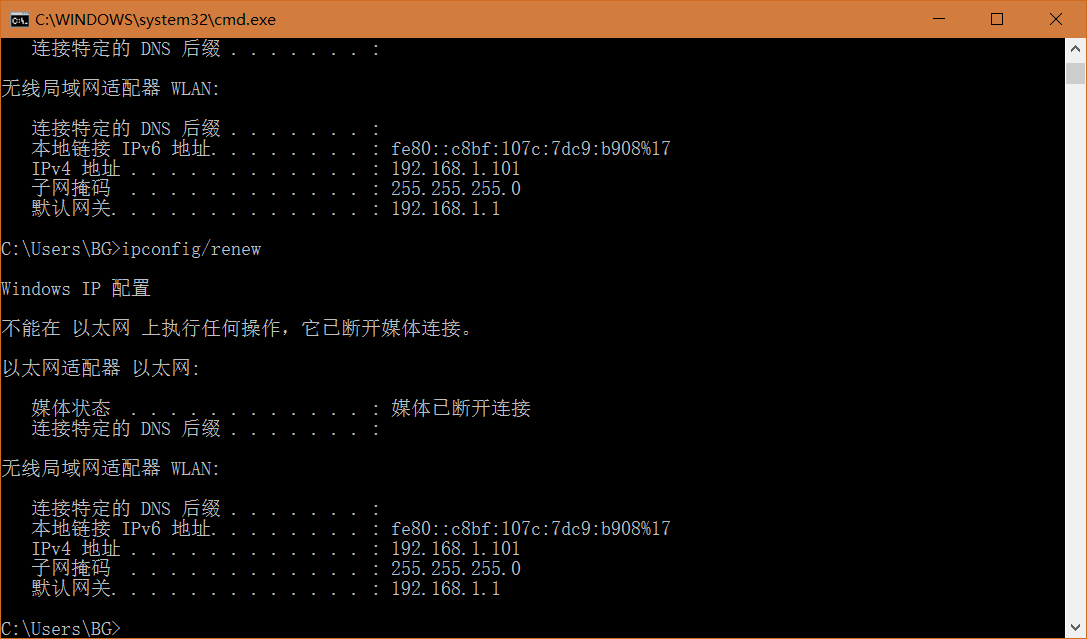
* 1. 打开Windows命令提示符窗口，输入ipconfig /release，释放IP



* 1. ipconfig /release终止后，输入ipconfig /renew，将发起一个DHCP过程



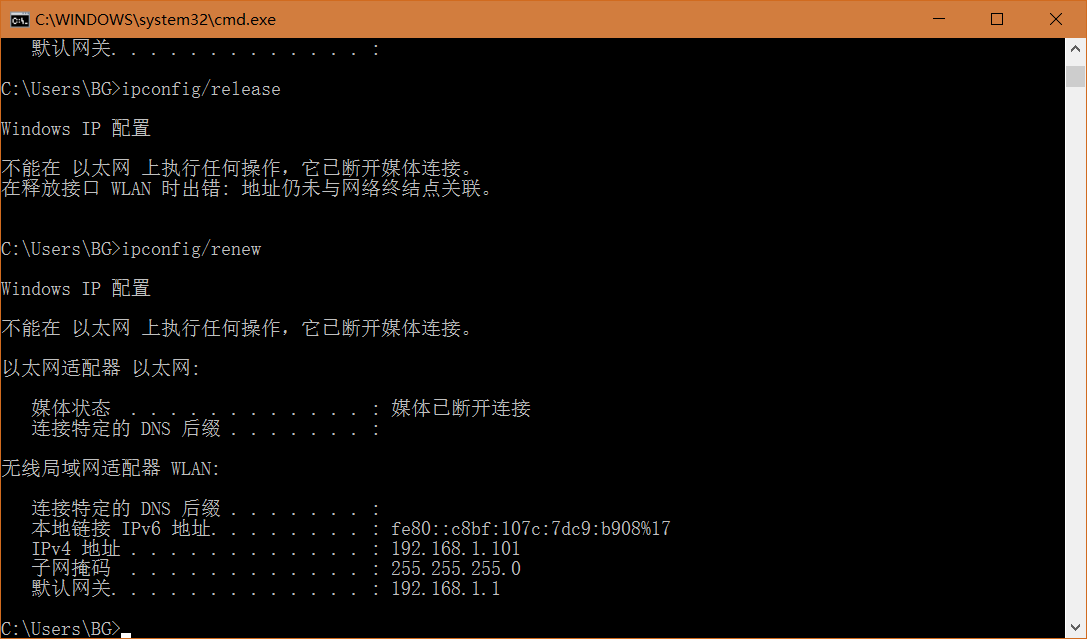
* 1. ipconfig /renew终止后，再次输入ipconfig /renew



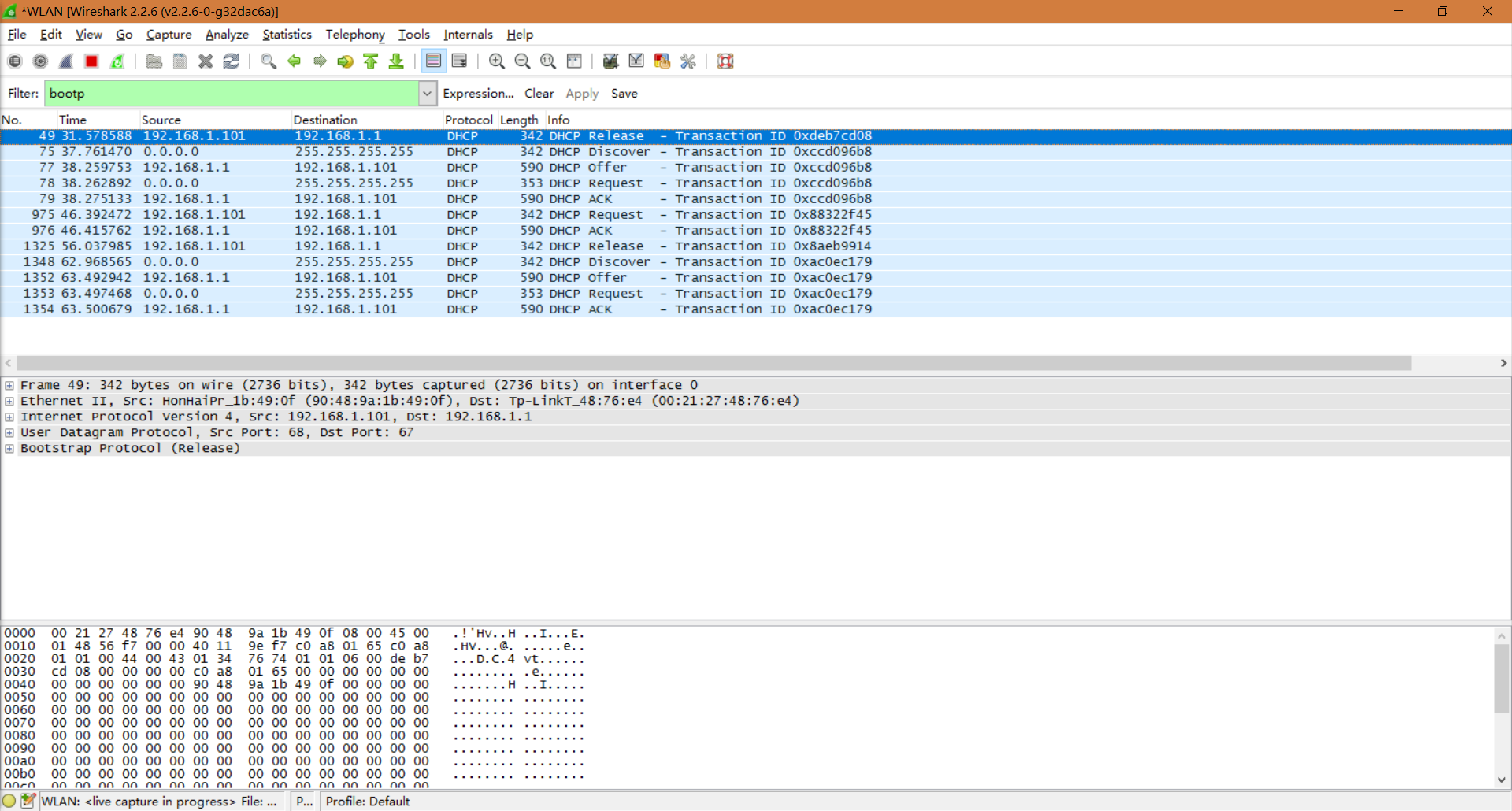
* 1. ipconfig /renew终止后，再次输入ipconfig /release



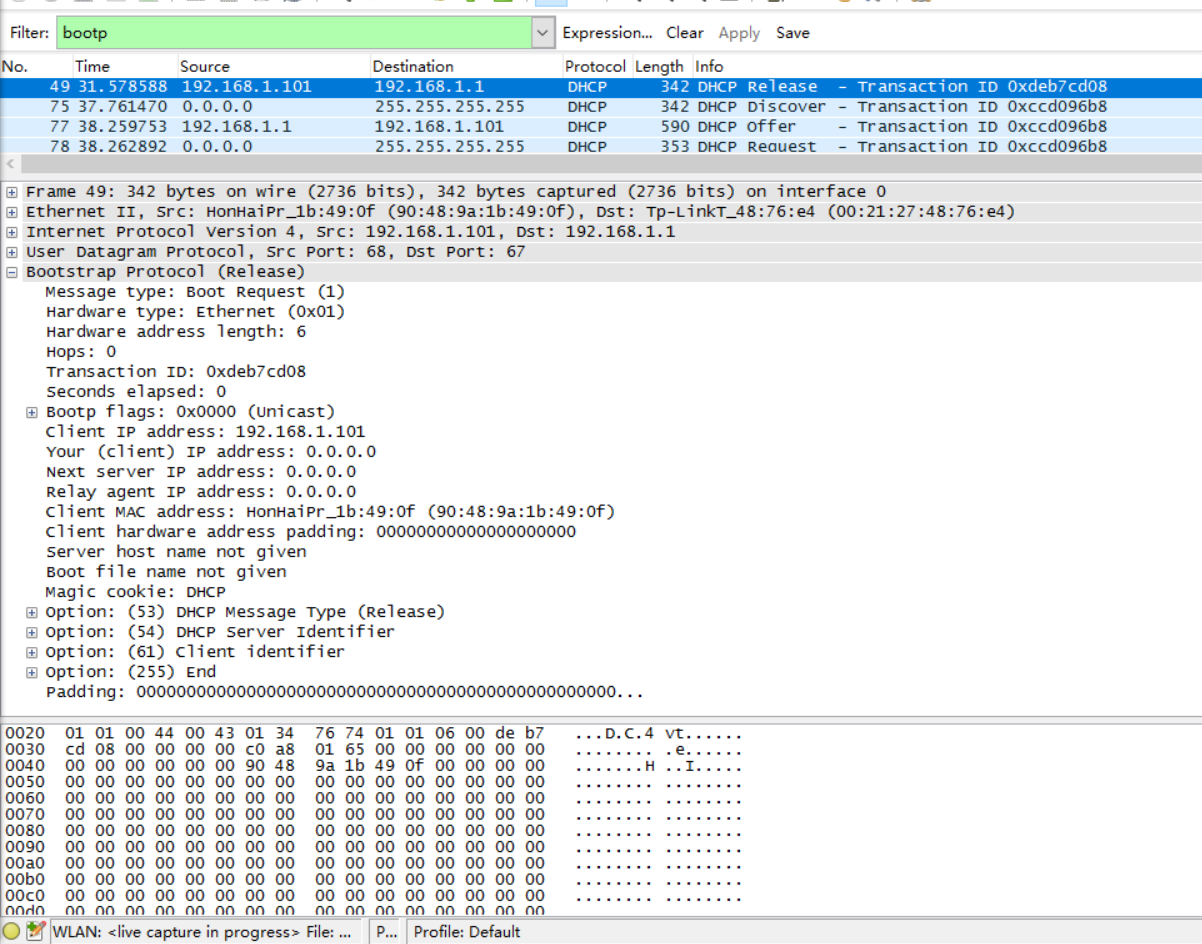
* 1. ipconfig /release终止后，再次输入ipconfig /renew



* 1. 停止分组捕获后，Wireshark界面如下：



* 1. 打开第一条DCHP数据包，由第一次执行ipconfig /release产生，结构如下：



DHCP的报文格式整理如下：

|  |  |  |  |
| --- | --- | --- | --- |
| OP(1) | Htype(1) | Hlen(1) | Hops(1) |
| Transaction ID(4) | | | |
| Seconds(2) | | Flags(2) | |
| Ciaddr（4） | | | |
| Yiaddr（4） | | | |
| Siaddr（4） | | | |
| Giaddr（4） | | | |
| Chaddr（16） | | | |
| Sname（64） | | | |
| File（128） | | | |
| Options（variable） | | | |

对应的含义分别是：

OP：若是client送给server的封包，设为1，反向为2；

Hard type：硬件类别，ethernet为1；

Hard address length：硬件长度，ethernet为6；

Hops：若数据包需经过router传送，每站加1，若在同一网内，为0；

Transaction ID：事务ID，是个随机数，用于客户和服务器之间匹配请求和相应消息；

Seconds：由用户指定的时间，指开始地址获取和更新进行后的时间；

Flags：从0-15bits，最左一bit为1时表示server将以广播方式传送封包给 client，其余尚未使用；

Ciaddr：用户IP地址；

Yiaddr：服务器分配给客户的IP地址；

Siaddr：用于bootstrap过程中的IP地址；（服务器的IP地址）

Giaddr：转发代理（网关）IP地址；

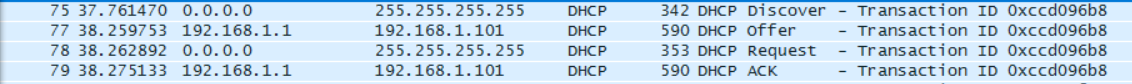
Chaddr：client的硬件地址；

Sname：可选server的名称，以0x00结尾；

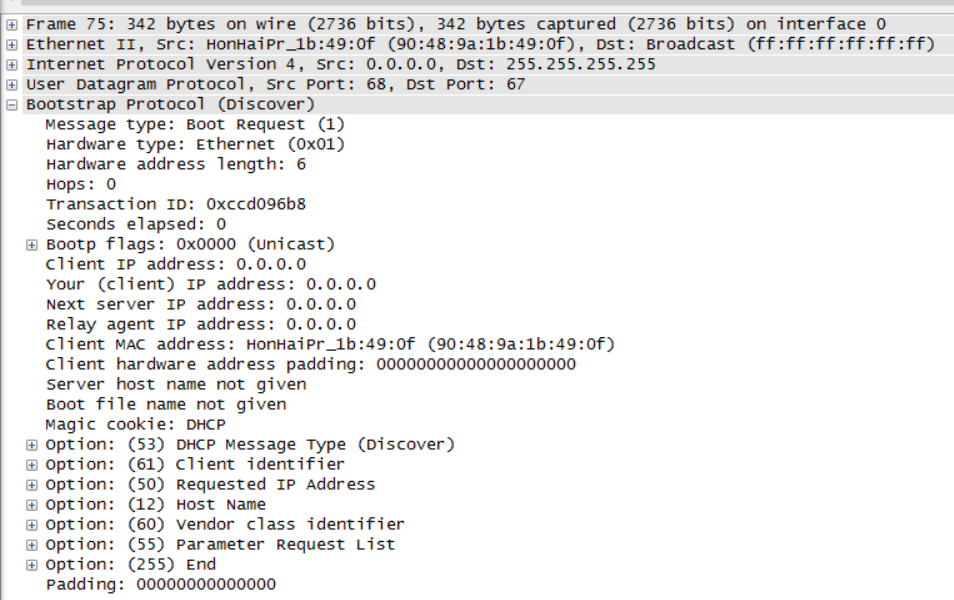
File：启动文件名；

Options：，厂商标识，可选的参数字段

* 1. 重点分析第一次执行ipconfig /renew产生的四条数据包：



* Discover



二层源地址：90:48:9a:1b:49:0f

二层目的地址：ff:ff:ff:ff:ff

Message type：Boot request（1），1是请求包，由client端发出的

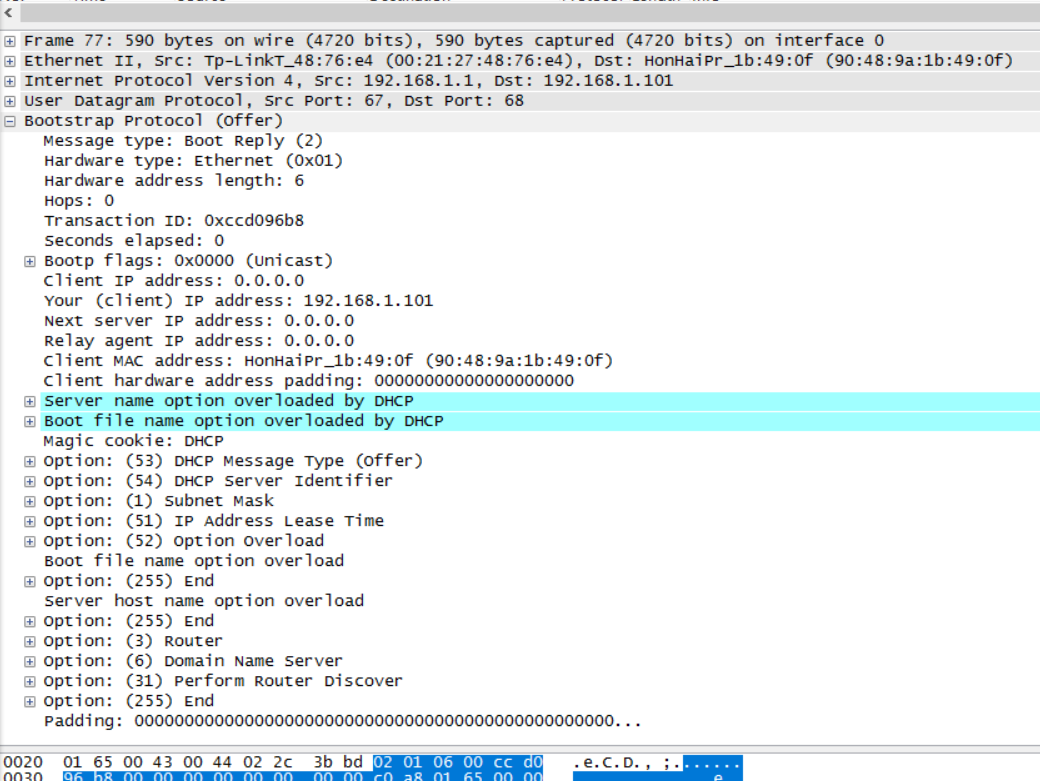
Hops：0，表示未经过处理

Client IP address：0.0.0.0，客户端的源IP，因为刚开始不知道ip地址是多少

Client MAC address：90:48:9a:1b:49:0f，客户端的MAC地址

Option：（53）DHCP Message Type（Discover），这是一个discover包

* Offer



二层源地址：00:21:27:48:76:e4

二层目的地址：90:48:9a:1b:49:0f

三层源地址：192.168.1.1

三层目的地址：192.168.1.101

User Datagran Protocol：通过udp来传输，端口号：68，67

Message type：Boot reply（2），1是回复包

Hops：0

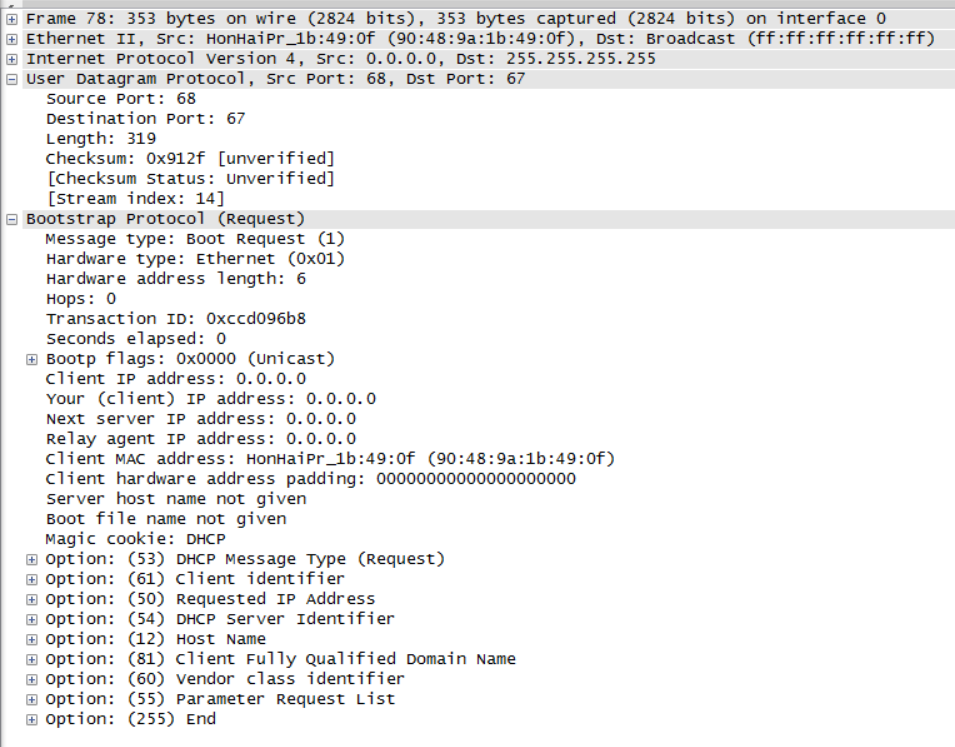
Boot flags：unicast

Your（client） IP address：192.168.1.101

Client MAC address：90:48:9a:1b:49:0f，客户端的MAC地址

Option：（53）DHCP Message Type（offer），这是一个offer包

* Request



二层源地址：90:48:9a:1b:49:0f

二层目的地址：ff:ff:ff:ff:ff

Message type：Boot request（1），1是请求包

Hops：0

Boot flags：unicast

Your（client） IP address：0.0.0.0

Client MAC address：90:48:9a:1b:49:0f，客户端的MAC地址

Option：（53）DHCP Message Type（request），这是一个request包

* ACK

