

一、实验目的:

通过 Wireshark 分析 IP 协议并了解 IP 数据报的组成及各部分的含义。

IP 是英文 Internet Protocol ([网络之间互连的协议](#)) 的缩写, 中文简称为“网协”, 也就是为计算机网络相互连接进行通信而设计的协议。在因特网中, 它是能使连接到网上的所有计算机网络实现相互通信的一套规则, 规定了计算机在因特网上进行通信时应当遵守的规则。

二、实验准备:

下载并安装本实验使用的软件: wget (<http://www.gnu.org/software/wget/>)、wireshark (www.wireshark.org)

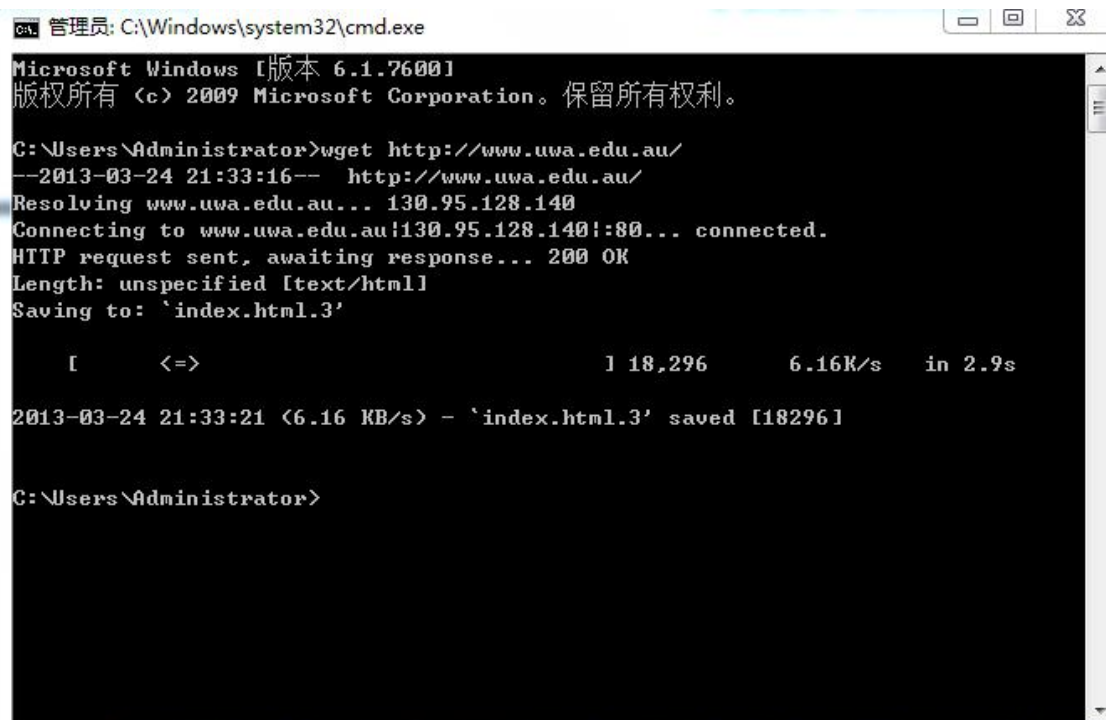
Windows 下相关命令: tracert、wget

三、实验步骤:

1、捕获数据

在 DOS 命令行下使用 wget 命令得到如下数据:

```
wget http://www.uwa.edu.au/
```



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>wget http://www.uwa.edu.au/
--2013-03-24 21:33:16-- http://www.uwa.edu.au/
Resolving www.uwa.edu.au... 130.95.128.140
Connecting to www.uwa.edu.au|130.95.128.140|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: `index.html.3'

  [      <=>          ] 1 18,296      6.16K/s   in 2.9s

2013-03-24 21:33:21 (6.16 KB/s) - `index.html.3' saved [18296]

C:\Users\Administrator>
```

在 DOS 命令行下使用 tracert 命令得到如下数据:

```
tracert www.uwa.edu.au
```

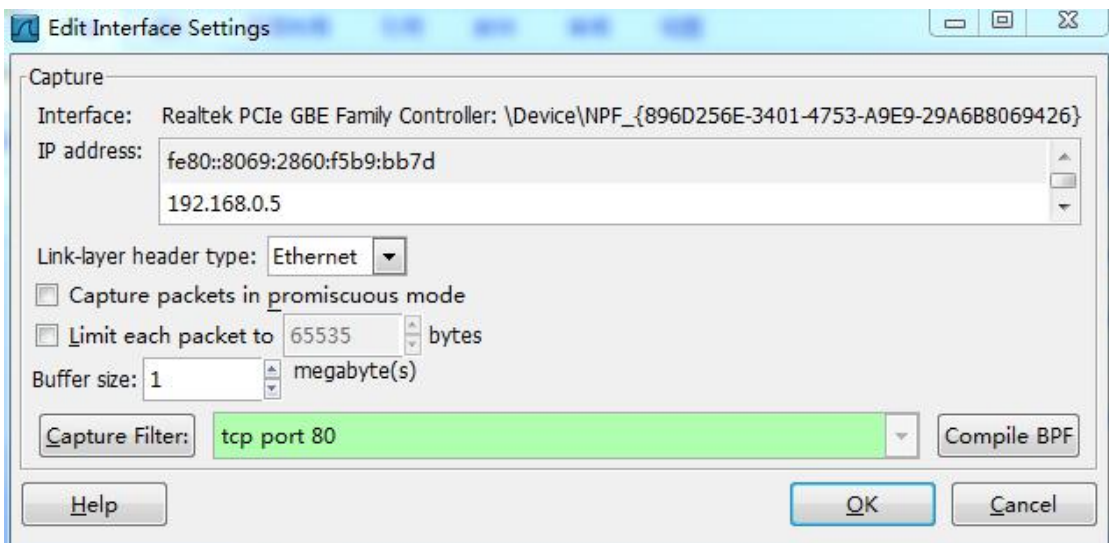
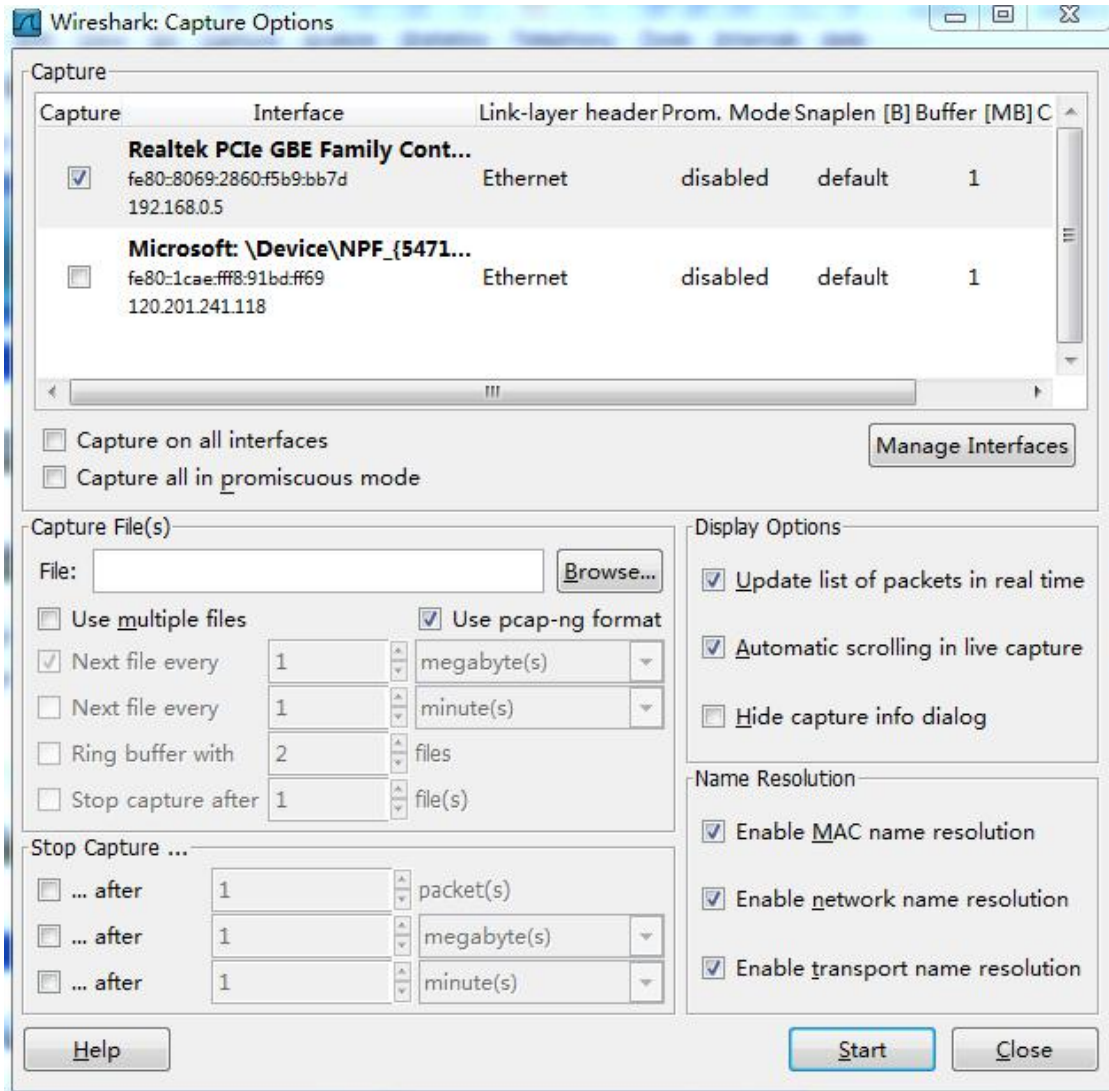
```
C:\Windows\system32\cmd.exe
C:\Users\Administrator>tracert www.uwa.edu.au

通过最多 30 个跃点跟踪
到 www.uwa.edu.au [130.95.128.140] 的路由:

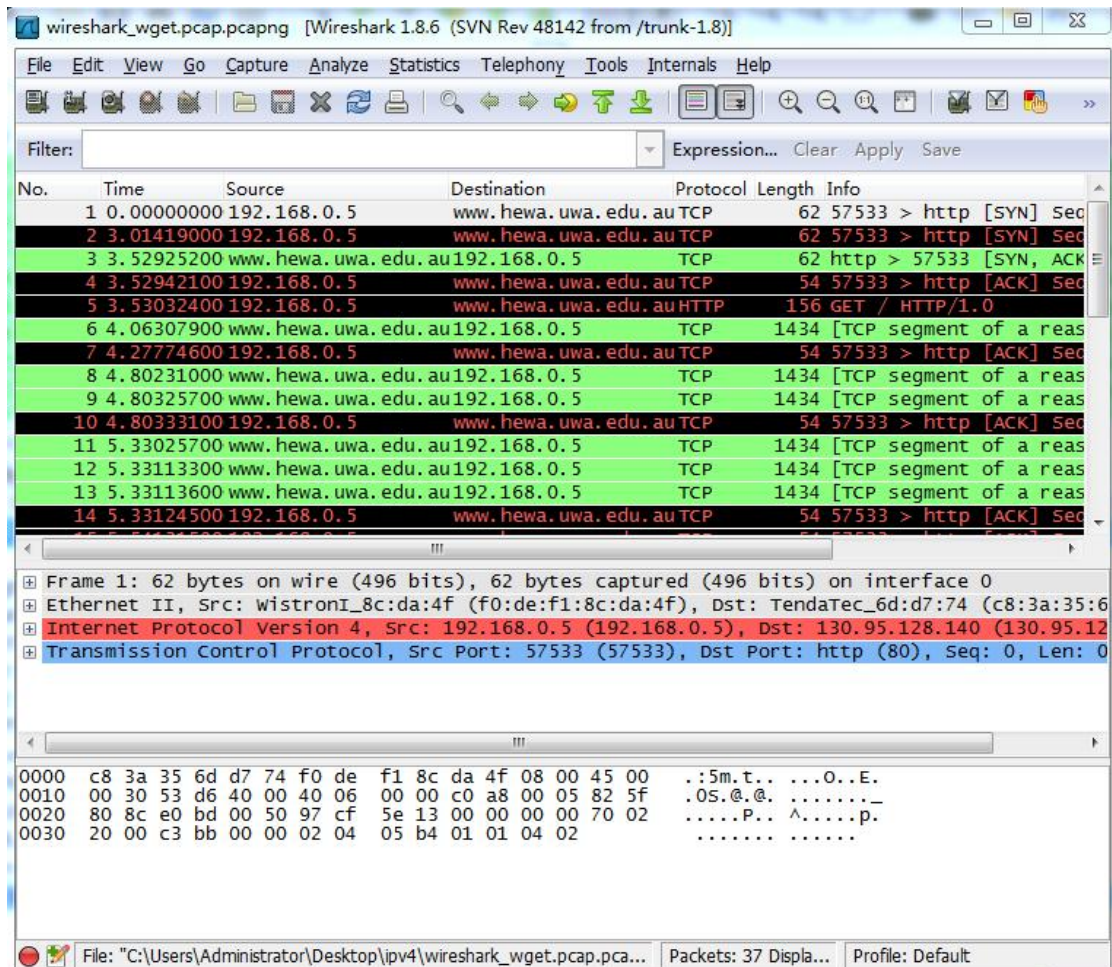
  1  <1 毫秒      1 ms      1 ms      192.168.0.1
  2   3 ms      12 ms     8 ms      10.22.0.1
  3   3 ms       3 ms     3 ms      172.17.5.1
  4   2 ms       3 ms     4 ms      124.93.197.9
  5   5 ms       5 ms     5 ms      61.189.79.141
  6   8 ms       *         10 ms     113.230.185.5
  7  56 ms      59 ms    55 ms     219.158.15.109
  8  114 ms     114 ms   114 ms     219.158.3.122
  9  115 ms     112 ms   129 ms     219.158.96.242
 10  323 ms     320 ms   313 ms     219.158.25.118
 11  290 ms     292 ms   302 ms     sl-st20-sj-11-1-2.sprintlink.net [144.223.242.69]
 12  353 ms     *         358 ms     sl-above4-228560-0.sprintlink.net [144.228.111.90]
 13  306 ms     303 ms   303 ms     xe-0-3-0.cr1.sjc2.us.above.net [64.125.24.1]
 14  357 ms     357 ms   358 ms     xe-0-1-0.mpr1.pao1.us.above.net [64.125.31.65]
 15  475 ms     474 ms   473 ms     64.124.200.214.allocated.above.net [64.124.200.214]
 16  471 ms     468 ms   466 ms     so-3-3-1.bb1.a.syd.aarnet.net.au [202.158.194.173]
 17  487 ms     485 ms   484 ms     so-2-0-0.bb1.a.mel.aarnet.net.au [202.158.194.33]
 18  493 ms     494 ms   493 ms     so-2-0-0.bb1.a.adl.aarnet.net.au [202.158.194.171]
 19  514 ms     521 ms   518 ms     so-0-1-0.bb1.a.per.aarnet.net.au [202.158.194.5]
 20  512 ms     514 ms   523 ms     tengigabitethernet1-4.er2.uwa.cpe.aarnet.net.au [202.158.198.10]
 21  529 ms     526 ms   529 ms     gw1.er2.uwa.cpe.aarnet.net.au [113.197.9.118]
 22  *           *         *         请求超时。
 23  *           *         *         请求超时。
 24  524 ms     522 ms   536 ms     staff.uwa.edu.au [130.95.128.140]

跟踪完成。
C:\Users\Administrator>
```

wireshark 中的设置项如下图所示，过滤掉其它类型的数据包只捕获 ip 数据包：



wireshark 设置完成后开始捕获数据，捕获到的数据如下：



2、数据分析：

- Internet Protocol Version 4, Src: 192.168.0.5 (192.168.0.5), Dst: 130.95.128.140 (130.95.128.140)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable))
 - Total Length: 40
 - Identification: 0x53dc (21468)
 - Flags: 0x02 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 64
 - Protocol: TCP (6)
 - Header checksum: 0x0000 [incorrect, should be 0x235b (may be caused by "IP checksum offload")]
 - Source: 192.168.0.5 (192.168.0.5)
 - Destination: 130.95.128.140 (130.95.128.140)
 - [Source GeoIP: Unknown]
 - [Destination GeoIP: Unknown]

上图所示即为 IP 数据报的格式：

Version: “4”说明此数据报通过 ipv4 发送/接收

Header length: IP 数据包头部的长度

Differentiated Services : 区分服务

Total Length: 数据包的总长度

Identification : 标示

Flags: 标志

Fragment offset : 片偏移量

Time to live/TTL :生存周期

Protocol : 协议

Header checksum : 首部检验和

Source/ Destination :源/目的地址