

计网入门实验

学号:PB21111723 姓名:王涵

一、实验目的

熟悉Wireshark，并做一些简单的抓包和观察。

二、实验原理

Wireshark是非常流行的网络封包分析软件，功能十分强大。可以截取各种网络封包，显示网络封包的详细信息。Wireshark使用Npcap 作为接口，直接与网卡进行数据报文交换，监听共享网络上传送的数据包。Npcap是替代WinPcap的新型Windows网络数据包截获软件。能够比原有的WinPcap数据包获得更好的抓包性能，并且稳定性更好。

三、实验环境

Windows、Wireshark

四、实验过程

1、Wireshark的安装

在网上下载安装最新Windows版本，按照引导完成安装

Download Wireshark

The current stable release of Wireshark is 4.0.8. It supersedes all previous releases. You can also download the latest development release (4.1.0) and documentation.

▼ Stable Release: 4.0.8

-  [Windows x64 Installer](#)
-  [Windows x64 PortableApps®](#)
-  [macOS Arm Disk Image](#)
-  [macOS Intel Disk Image](#)
-  [Source Code](#)

2、 利用 Wireshark 观察 http 报文

利用过滤筛选出http报文信息并分析

(1)启动浏览器(Google Chrome) , 清空浏览器缓存

(2)启动wireshark, 并启动捕获分组

(3)输入网址: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

(4)停止捕获并观察

The screenshot shows the Wireshark interface with a packet capture of ICMPv6 Router Advertisements. The top menu bar includes File(F), Edit(E), View(V), Transform(T), Capture(C), Analysis(A), Statistics(S), Network(W), Tools(T), and Help(H). Below the menu is a toolbar with various icons for file operations, navigation, and analysis. A filter bar at the top displays "应用显示过滤器 ... <Ctrl-/>" with a search icon and a plus sign.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::8261:6cff:fef...	ff02::1	ICMPv6	118	Router Advertisement
2	0.202636	HuaweiTe_8a:5d:45	Chongqin_76:2e:23	ARP	56	Who has 100.64.179.72
3	0.202649	Chongqin_76:2e:23	HuaweiTe_8a:5d:45	ARP	42	100.64.179.72 is at b
4	3.008217	fe80::8261:6cff:fef...	ff02::1	ICMPv6	118	Router Advertisement
5	4.767797	100.64.179.72	20.197.71.89	TLSv1.2	97	Application Data
6	4.848835	20.197.71.89	100.64.179.72	TLSv1.2	228	Application Data
7	4.892387	100.64.179.72	20.197.71.89	TCP	54	53199 → 443 [ACK] Seq
8	6.330149	fe80::8261:6cff:fef...	ff02::1	ICMPv6	118	Router Advertisement
9	6.374360	2001:da8:d800:604:4...	2408:871a:3001:b03:...	TCP	75	53807 → 443 [ACK] Seq
10	10.319047	fe80::8261:6cff:fef...	ff02::1	ICMPv6	118	Router Advertisement

The bottom pane shows the details of the selected packet (Frame 1). It lists the following fields:

- > Frame 1: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
- > Ethernet II, Src: NewH3CTe_f5:4e:01 (80:61:6c:f5:4e:01), Dst: ff02::1 (01:00)
- > Internet Protocol Version 6, Src: fe80::8261:6cff:fef... , Dst: ff02::1
- > Internet Control Message Protocol v6

The hex dump pane shows the raw data of the frame, with the first few bytes highlighted in blue:

```

0000  b4 b5 b6 76 2e 23 80 61 6c f5 4e 01 86 dd 6
0010  00 00 00 40 3a ff fe 80 00 00 00 00 00 00 8
0020  6c ff fe f5 4e 01 ff 02 00 00 00 00 00 00 0
0030  00 00 00 00 00 01 86 00 9a 46 40 00 07 08 0
0040  00 00 00 00 00 00 01 01 80 61 6c f5 4e 01 0
0050  00 00 00 00 05 dc 03 04 40 c0 00 27 8d 00 0
0060  3a 80 00 00 00 00 20 01 0d a8 d8 00 06 04 0
0070  00 00 00 00 00 00
  
```

设置过滤http筛选出http条目，得到下图：

No.	Time	Source	Destination	Protocol	Length	Info
15	10.554208	100.64.179.72	124.236.26.172	HTTP/J...	922	POST / HTTP/1.1 , JavaScr
19	10.583762	124.236.26.172	100.64.179.72	HTTP	60	HTTP/1.1 200 OK
80	15.018837	100.64.179.72	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO
84	15.319485	128.119.245.12	100.64.179.72	HTTP	492	HTTP/1.1 200 OK (text/ht

报文：

```
> Frame 15: 922 bytes on wire (7376 bits), 922 bytes captured (7376 bits) on interface
> Ethernet II, Src: Chongqin_76:2e:23 (b4:b5:b6:76:2e:23), Dst: HuaweiTe_8a:5d:45 (c8
> Internet Protocol Version 4, Src: 100.64.179.72, Dst: 124.236.26.172
> Transmission Control Protocol, Src Port: 53853, Dst Port: 80, Seq: 145, Ack: 1, Len
> [2 Reassembled TCP Segments (1012 bytes): #14(144), #15(868)]
> Hypertext Transfer Protocol
  JavaScript Object Notation: application/json
> Line-based text data: application/json (12 lines)
```

五、问题解答

1、DNS,HTTP,TCP

2、

80	15.018837	100.64.179.72	128.119.245.12	HTTP	527 GET /wireshark-labs/INTRO-wire
84	15.319485	128.119.245.12	100.64.179.72	HTTP	492 HTTP/1.1 200 OK (text/html)

所用时间 $t=15.319485-15.018837=0.300648\approx 0.3$ 秒

3、

128.119.245.12

100.64.179.72

4、见另一个PDF文件--打印结果.pdf