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.

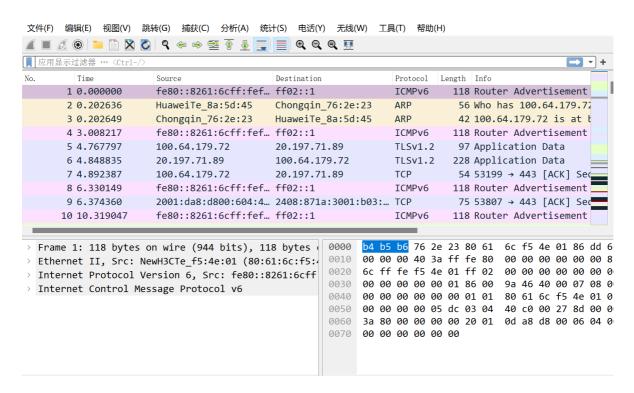
- **▼ Stable Release: 4.0.8**
- **Windows** x64 Installer
- **Windows x64 PortableApps®**
- macOS Arm Disk Image
- macOS Intel Disk Image
- </> Source Code

2、 利用 Wireshark 观察 http 报文

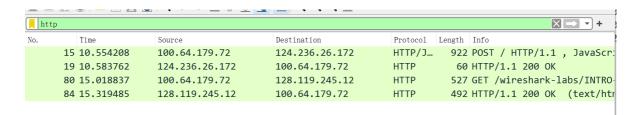
利用过滤筛选出http报文信息并分析

- (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



设置过滤http筛选出http条目,得到下图:



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, Ler [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≈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