

计算机网络实验课

2020.9.26

实验安排

1. 网络协议分析（软件实验，10%）
2. 使用二层交换机组网（硬件实验，15%，**5人左右组队，必须来机房**）
3. 使用三层交换机组网（软件实验，10%）
4. 静态路由配置（软件实验，15%）
5. 动态路由协议OSPF配置（软件实验，20%）
6. 动态路由协议BGP配置（软件实验，20%）
7. 基于Socket接口实现自定义协议通信（编程实验，10%，可以2人一组完成）
8. 实现一个轻量级的WEB服务器（编程实验，bonus，5分）

总成绩：考试 * 50% + (实验 + 课后作业 + 平时分) * 50%

- 根据实验内容，一般两周一个实验，具体看通知
- **第二次硬件实验需要来实验教室做**，其他实验不用来
 - 想用实验教室的电脑做软件实验也行
- **除实验二和七，其他实验需要独立完成**

评分标准

- 实验评分

- 抄袭和没交：零分
- 没按时交：会扣分，迟一周扣0.5
- 部分没做：按比例扣分
 - 一两个步骤试了几次还是没做出来不用死磕，扣分其实很少（有些软件实验表现很迷）

- 实验数据记录和处理

- 按报告里的要求来，题目里没要求标注的话，截图里不用做标注
- 不要截图整个桌面或者软件

- 实验结果分析与思考

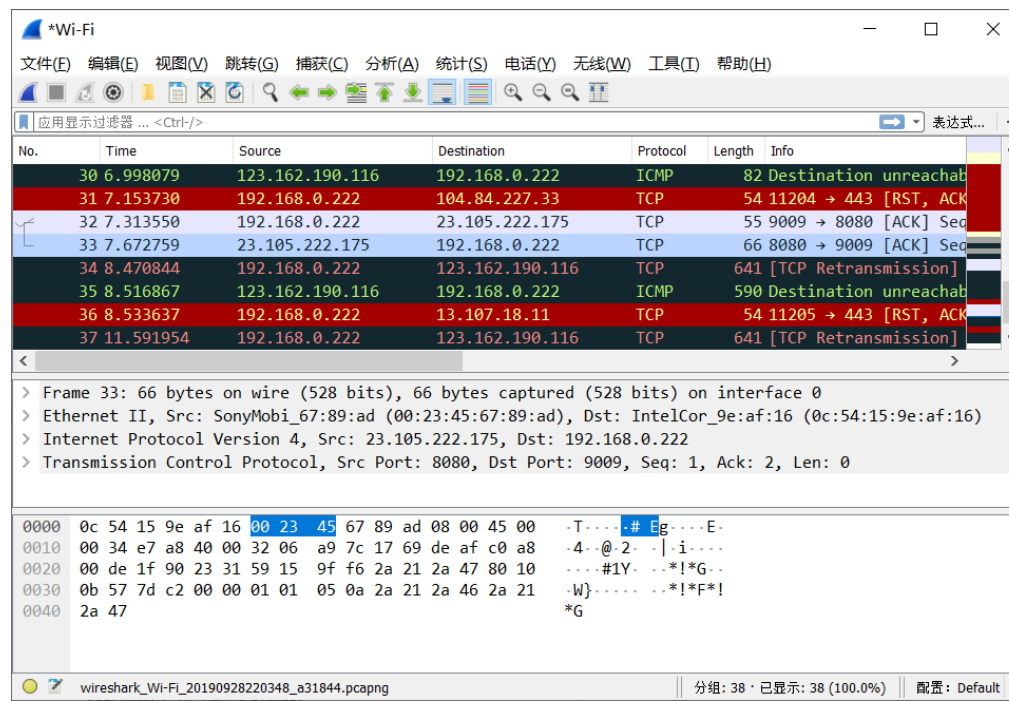
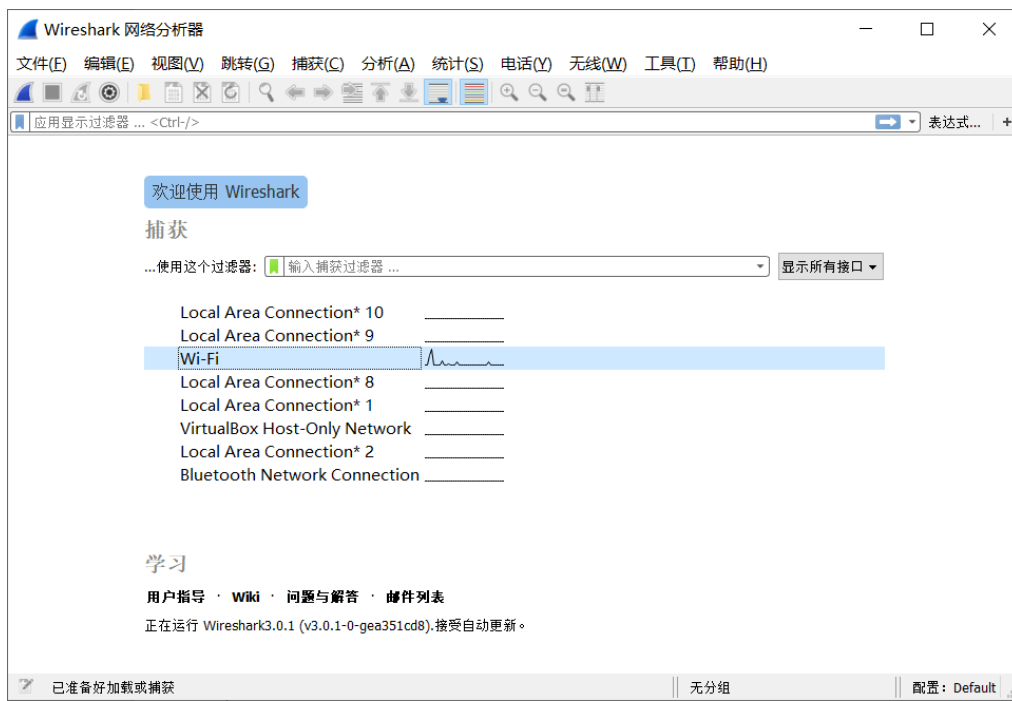
- 不要从网上复制答案，自己组织语言，用几句话就能答完
- 客观题答错扣分，主观题看逻辑有没有问题，关键点是否都回答到

- 讨论、心得

- 不要写“无”，简单几句描述一下
- 没遇到问题或者没想法：写大概花了多久做完实验

实验一：网络协议分析

- Deadline: 10月17号23:59
- 用Wireshark软件查看系统收到的网络数据包并进行分析
- Wireshark下载地址
 - 官网: <https://www.wireshark.org/download.html>
 - 浙大云盘: <https://pan.zju.edu.cn/share/a85b221212dda95ab723b6a795>
 - 没有Linux版本



Wireshark使用指导

1. 设置捕获过滤器（可选步骤）
2. 选择电脑上相应的接口
 - 接口 (interface): 可以简单理解为网卡
 - 有虚拟的, 也有物理的
3. 做一些操作（比如ping、打开网页）

欢迎使用 Wireshark

捕获

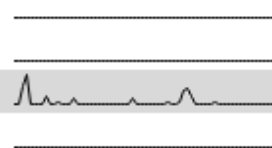
...使用这个过滤器:

Local Area Connection* 10

Local Area Connection* 9

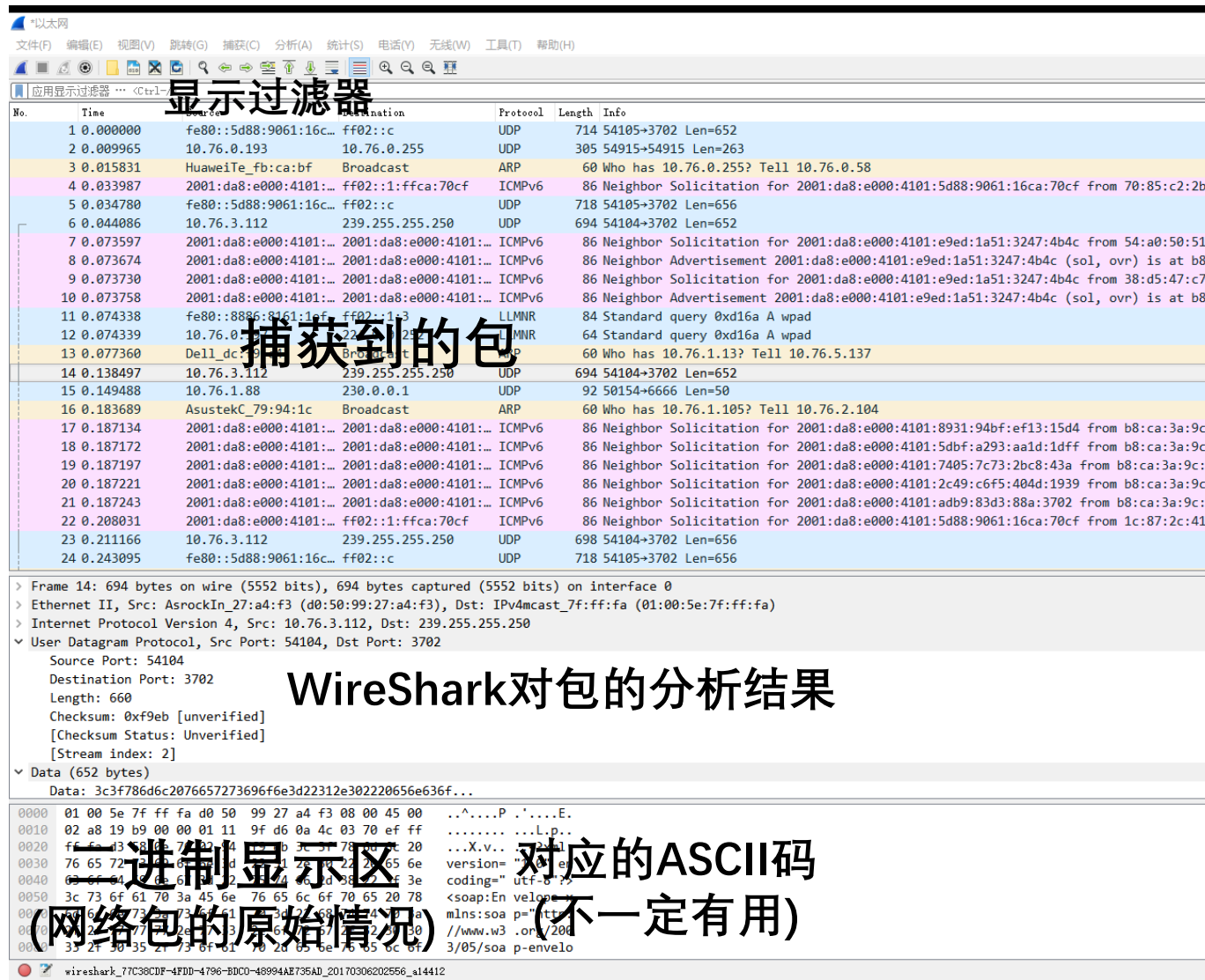
Wi-Fi

Local Area Connection* 8



Wireshark使用指导

1. 设置捕获过滤器 (可选步骤)
2. 选择电脑上相应的接口
 - 接口 (interface): 可以简单理解为网卡
 - 有虚拟的, 也有物理的
3. 做一些操作 (比如ping、打开网页)
4. 找到目标数据包进行分析



显示过滤器

捕获的包

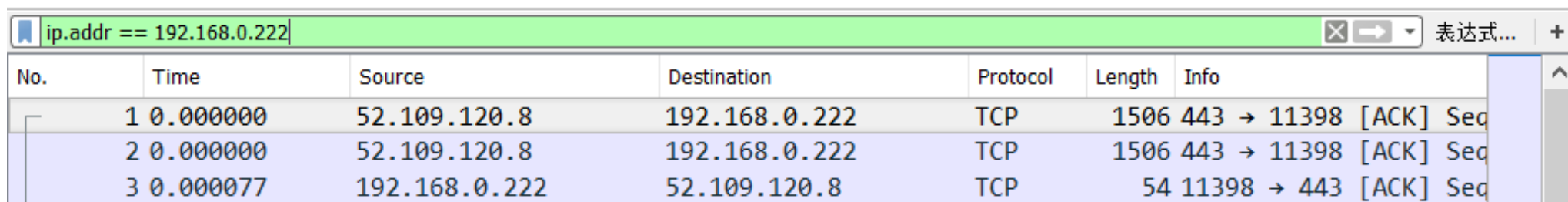
WireShark对包的分析结果

二进制的显示区
(网络包的原始情况)

对应的ASCII码
(不一定有用)

Wireshark使用指导

1. 设置捕获过滤器（可选步骤）
2. 选择电脑上相应的接口
 - 接口 (interface): 可以简单理解为网卡
 - 有虚拟的, 也有物理的
3. 做一些操作 (比如ping、打开网页)
4. 找到目标数据包进行分析
 - 可以设置显示过滤器, 方便查找

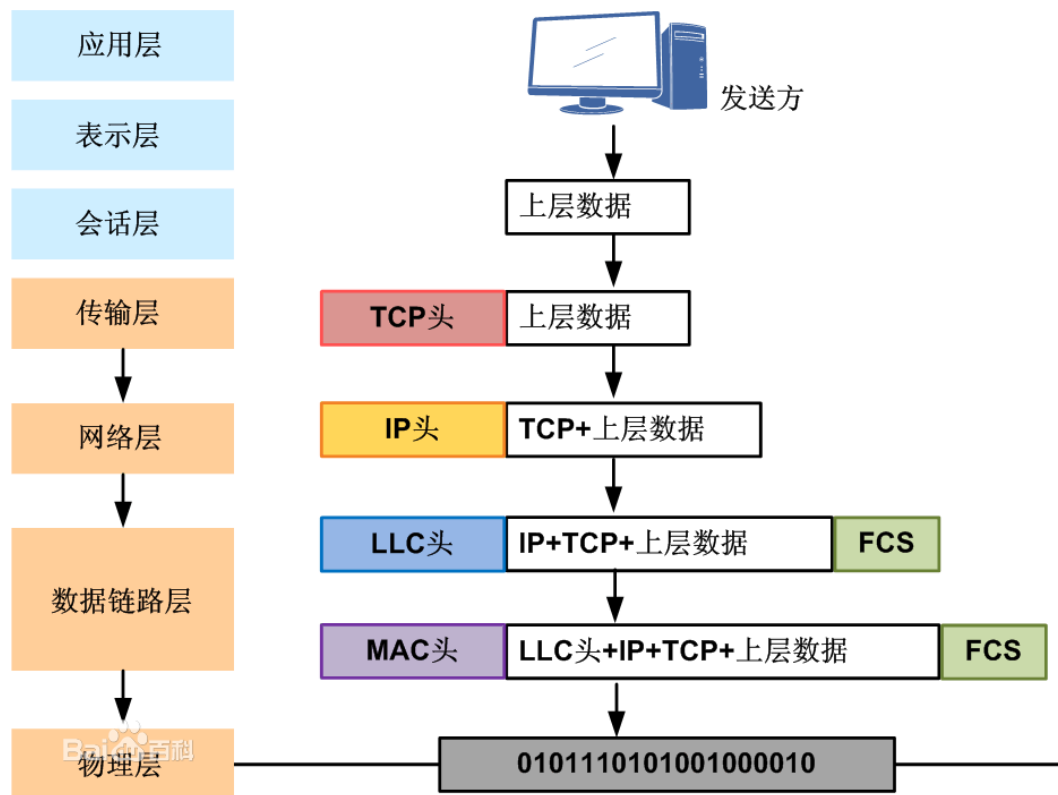


The screenshot shows the Wireshark interface. At the top, a green display filter bar contains the text 'ip.addr == 192.168.0.222'. Below this is a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. Three packets are visible, all of which are TCP ACKs from 192.168.0.222 to 52.109.120.8.

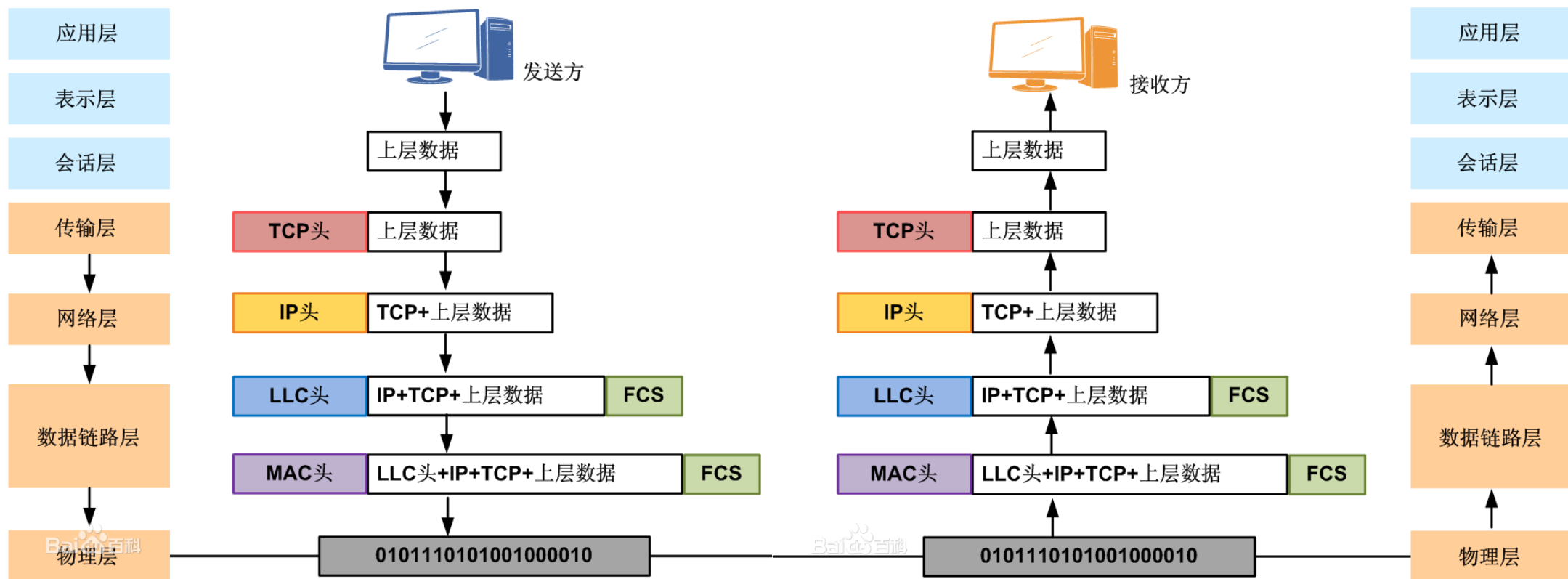
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	52.109.120.8	192.168.0.222	TCP	1506	443 → 11398 [ACK] Seq
2	0.000000	52.109.120.8	192.168.0.222	TCP	1506	443 → 11398 [ACK] Seq
3	0.000077	192.168.0.222	52.109.120.8	TCP	54	11398 → 443 [ACK] Seq

- 捕获过滤器和显示过滤器语法不一样, 有需求的自行上网搜, 不必完全掌握

如何看懂一个数据包



如何看懂一个数据包



- 数据链路层：根据**MAC地址**发给对应设备（路由器/交换机/电脑.....）
- 网络层：根据**IP**将封装的数据发给对应网络接口(一个设备可以有多个不同IP的接口，比如WiFi和有线)
- 传输层：根据**端口**将封装的数据发给对应应用（一个操作系统有很多联网应用）
- 应用层：数据到具体应用后，根据使用的协议解析（比如QQ可能自己设计了一套通信协议）

应用程序的开发者不用关心底层怎么封装，操作系统&网卡驱动会帮你处理

如何看懂一个数据包

- 是开始捕获后接受到的第88个数据帧(Frame)
- 数据链路层：使用了Ethernet II 协议传输，其中包含来源和目标设备的MAC地址
- 网络层：使用了IPV4协议，包含来源IP和目的地IP
- 传输层：使用了TCP协议，包含来源和目标端口
- 应用层：是HTTP协议，包含了一张GIF图片的数据

No.	Time	Source	Destination	Protocol	Length	Info
80	0.574309	192.168.0.222	210.32.0.113	HTTP	975	GET /images/main_bg1.gif
88	0.692977	210.32.0.113	192.168.0.222	HTTP	1180	HTTP/1.1 200 OK (GIF89a)
228	31.370962	23.105.222.175	192.168.0.222	TCP	1506	8080 → 12402 [ACK] Seq=15

>	Frame 88: 1180 bytes on wire (9440 bits), 1180 bytes captured (9440 bits) on interface 0
>	Ethernet II, Src: SonyMobi_67:89:ad (00:23:45:67:89:ad), Dst: IntelCor_9e:af:16 (0c:54:15:9e:af:16)
>	Internet Protocol Version 4, Src: 210.32.0.113, Dst: 192.168.0.222
>	Transmission Control Protocol, Src Port: 80, Dst Port: 13238, Seq: 1, Ack: 923, Len: 1126
>	Hypertext Transfer Protocol
>	Compuserve GIF, Version: GIF89a

0120	35 3a 35 34 3a 32 38 20 47 4d 54 0d 0a 0d 0a 47	5:54:28 GMT...	G
0130	49 46 38 39 61 84 03 14 00 c4 00 00 46 69 8d 47	IF89a...	Fi·G
0140	6a 8d 9f ba d4 6a 8d af eb ef f7 69 8d ae 7c a0	j...j...i..	
0150	c1 d3 df ec b9 cd e0 57 7a 9d 4a 6e 90 f6 f7 fcW z·Jn...	
0160	70 93 b5 74 98 ba da e4 f0 9e b9 d4 db e5 f0 5c	p..t....\	
0170	7e a1 5c 7f a2 74 97 b9 82 a6 c7 42 66 8a 42 65	~\..t...Bf·Be	
0180	89 43 67 8b 41 64 89 46 69 8c 45 68 8c 40 64 88	-Cg·Ad·F i·Eh·@d·	
0190	43 66 8a 41 65 89 44 67 8b f7 f8 fd 21 f9 04 00	Cf·Ae·Dg!	
01a0	00 00 00 00 2c 00 00 00 00 84 03 14 00 00 05 ff,...	

如何看懂一个数据包

Wireshark packet capture analysis of an ARP request. The interface shows a list of packets, with packet 1 selected. The packet details pane shows the Ethernet II header and the ARP request payload. Red boxes highlight the destination MAC address (0c:54:15:9e:af:16) and the target IP address (192.168.43.66). Red arrows point from these boxes to the corresponding hex values in the packet bytes pane: 0c 54 15 9e af 16 and c0 a8 2b 42.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	SonyMobi_04:a6:c8	IntelCor_9e:af:16	ARP	42	Who has 192.168.43.66
2	0.000015	IntelCor_9e:af:16	SonyMobi_04:a6:c8	ARP	42	192.168.43.66 is at 0
3	0.409910	117.18.232.200	192.168.43.66	TLSv1.2	240	Application Data

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

✓ Ethernet II, Src: SonyMobi_04:a6:c8 (38:78:62:04:a6:c8), Dst: IntelCor_9e:af:16 (0c:54:15:9e:af:16)

- > Destination: IntelCor_9e:af:16 (0c:54:15:9e:af:16)
- > Source: SonyMobi_04:a6:c8 (38:78:62:04:a6:c8)
- Type: ARP (0x0806)

✓ Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: SonyMobi_04:a6:c8 (38:78:62:04:a6:c8)
- Sender IP address: 192.168.43.3
- Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.43.66

0000 0c 54 15 9e af 16 38 78 62 04 a6 c8 08 06 00 01 .T....8x b.....
0010 08 00 06 04 00 01 38 78 62 04 a6 c8 c0 a8 2b 038x b.....+
0020 00 00 00 00 00 00 c0 a8 2b 42 +B

Destination Hardware Address (eth.dst), 6 字节 | 分组: 18 · 已显示: 18 (100.0%) | 配置: Default

Wireshark已经做了二进制的解析

可能会遇到的一些问题和疑惑

- 啥也没干捕获到好多包
 - 操作系统里有很多程序在“偷偷”联网，浏览器里的网页也一样，Wireshark只是全部呈现了出来
 - **推荐把可以关的应用、网页都关了**
- 新的网络包不断出现，会导致记录文件过大
 - 做完一个步骤可以点一下这个红色按钮停止网络



- 想重做一次可以使用同一行的重新开始捕获或者关闭捕获文件按钮，会清空之前捕获到的包
- 打开Wireshark 出现权限问题
 - 使用管理员权限打开（Windows下图标右键菜单里）

可能会遇到的一些问题和疑惑

- Mac OSX下多一层协议可能是因为VPN
- 不懂啥是IP, TCP, HTTP
 - 分别是网络层、传输层、应用层的名词，以后会学
 - WireShark已经做了解析，一般了解MAC地址、IP、端口、应用使用数据在哪里出现即可
- 啥是TCP流、HTTP流
 - 可以先理解为多个有关联的网络包
 - 使用TCP协议连接时，需要通过特定格式的内容表示连接的开始和结束，连接开始后到结束，同一端口收到的TCP包都属于同一个TCP流
 - HTTP包有请求和响应的概念，请求包和响应包属于一个HTTP流，请求和响应可能因为内容过大而被拆成多次发送/接收
- 用的无线网，但是第二层显示Ethernet协议(802.3)而不是802.11
 - 正常，无线网卡（驱动）为操作系统服务的时候以Ethernet的形式工作，WireShark也比较难绕过
 - <https://superuser.com/questions/1242454/why-do-i-see-ethernet-ii-protocol-in-wireshark-in-wireless-connection>
 - <https://wiki.wireshark.org/CaptureSetup/WLAN>
- 包的Frame格式和书上不一样（比如没有尾部的CRC/FCS校验值）
 - 正常，和适配器/驱动有关，WireShark能从硬件拿到的信息受操作系统和驱动控制
 - <https://serverfault.com/questions/521443/can-wireshark-capture-an-entire-ethernet-frame-including-preamble-crc-and-inter>