

Wireshark

数据包分析实战详解

王晓卉 李亚伟 编著

通过80个实例，详细讲解了Wireshark数据包分析实施的8大类技巧
基于Wireshark抓取的数据包，层层剥茧地剖析了12种常见网络协议的构成

- ✓ 全面涵盖Wireshark基础知识和应用技巧，以及使用Wireshark对网络协议进行分析
- ✓ 遵循规范，从专业的角度循序渐进地讲解了Wireshark抓包及分析的实施流程
- ✓ 针对海量数据问题，详细讲解了捕获过滤器、显示过滤器和着色规则等专业技术
- ✓ 以图表结合的形式直观地展示了协议报结构，帮助读者快速掌握各种抽象的网络协议
- ✓ 对抓取的数据包按照协议层次，逐层讲解了各个协议在数据包中的体现

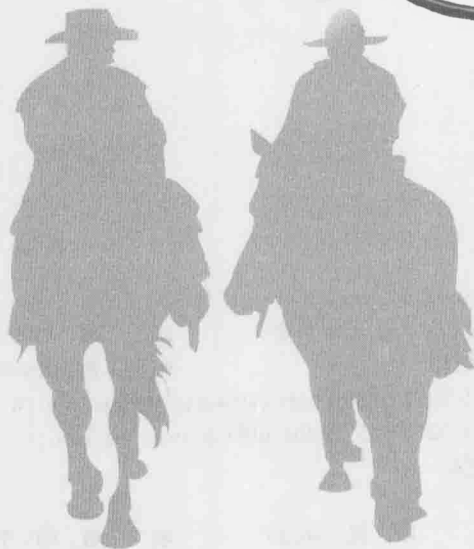


清华大学出版社

Wireshark

数据包分析实战详解

王晓卉 李亚伟 编著



清华大学出版社

北 京

内 容 简 介

本书由浅入深,全面系统地介绍了 Wireshark 数据包和数据包分析。本书提供了大量实例,供读者实战演练 Wireshark 的各项功能。同时,对抓取的数据包按照协议层次,逐层讲解各个协议在数据包中的体现。这样,读者就可以掌握数据包抓取到信息获取的每个环节。

本书共分 3 篇。第 1 篇介绍 Wireshark 的各项功能,包括基础知识、Wireshark 的定制、捕获过滤器和显示过滤器的使用、数据包的着色、导出和重组等;第 2 篇介绍基于 Wireshark 对 TCP/IP 协议族中常用协议的详细分析,如 ARP、IP、UDP、TCP、HTTP、HTTPS 和 FTP 等;第 3 篇介绍借助 Wireshark 分析操作系统启动过程中的网络通信情况。

本书涉及面广,内容包括工具使用、网络协议和应用。本书适合各类读者群体,如想全面学习 Wireshark 的初学者、网络管理员、渗透测试人员及网络安全专家等。对于网络数据分析人士,本书更是一本不可多得的案头必备参考书。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

Wireshark 数据包分析实战详解 / 王晓卉, 李亚伟编著. —北京: 清华大学出版社, 2015
ISBN 978-7-302-38871-5

I. ①W… II. ①王… ②李… III. ①统计数据—统计分析—应用软件 IV. ①O212.1-39

中国版本图书馆 CIP 数据核字(2015)第 004772 号

责任编辑: 杨如林

封面设计: 欧振旭

责任校对: 徐俊伟

责任印制: 宋 林

出版发行: 清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址: 北京清华大学学研大厦 A 座 邮 编: 100084

社 总 机: 010-62770175 邮 购: 010-62786544

投稿与读者服务: 010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈: 010-62772015, zhiliang@tup.tsinghua.edu.cn

印 装 者: 北京嘉实印刷有限公司

经 销: 全国新华书店

开 本: 185mm×260mm

印 张: 26.25

字 数: 656 千字

版 次: 2015 年 3 月第 1 版

印 次: 2015 年 3 月第 1 次印刷

印 数: 1~3000

定 价: 79.00 元

前言

网络的普及给人们的生活带来了极大的便利，同时网络的安全问题也成为公众热点。网络数据抓包和分析作为网络管理和监控最有效的措施，越来越受到网络管理人员和网络安全人员的重视。

Wireshark 作为一款开源的专业数据抓包和分析工具，深受业内人士欢迎。它提供了强大的数据抓取功能和丰富的数据分析方式。面对 Wireshark 强大的功能和海量的数据包，初学者往往无从下手。

笔者结合网络数据传输及安全方面存在的各种问题，经过分析及总结，编写了本书。本书通过专业的数据抓包流程，逐步讲解 Wireshark 各项强大的功能。同时，基于 Wireshark 抓取的数据包，以层层剥茧的形式，讲解常见的各种网络协议。这样读者可以更直接地掌握各种协议类型的数据包。

通过本书的学习，读者不仅可以轻松掌握 Wireshark 的使用，踏入网络数据分析的大门，还可以更为直观地理解 TCP/IP 各个协议，以及这些协议在数据包中的表现。掌握这些技术，再加以充分的练习，就可以轻松应对网络数据分析等各项工作。

本书特色

1. 内容全面、系统、深入

本书介绍了 Wireshark 的基础知识、捕获过滤器和显示过滤器的使用、对数据包进行导出或重组等。然后，介绍了使用 Wireshark 对各种协议的详细分析。最后，还详细分析了操作系统启动过程的数据包。

2. 贴近实际，专业讲解

本书按照 Wireshark 专业使用流程，对其功能进行详细讲解，帮助读者掌握最高效的数据抓包、分析技术，以解决各种复杂的网络问题。同时，针对围绕海量数据包处理问题，本书详细介绍相关技术，如抓取过滤器、显示过滤器、着色规则等功能。

3. 直观讲解网络协议

对于网络数据包涉及的网络协议，本书给以最直观的讲解。首先分析协议的工作原理以及相关数据包的构成，然后对照 Wireshark 数据包视图进行逐条比对，帮助读者以最直观的形式学习和掌握各个网络协议。

4. 提供多种学习和交流的方式

为了方便大家学习和交流，我们提供了多种方式。读者可以在论坛 www.wanjuanchina.com。

net 上发帖讨论 Wireshark 相关技术；也可以通过 QQ 群 336212690 转入对应的 Wireshark 技术群；还可以就图书阅读中遇到的问题致信 book@wanjuanchina.net 或 bookservice2008@163.com，以获得帮助。

本书内容及体系结构

第1篇 Wireshark应用篇（第1~9章）

本篇主要包括：Wireshark 的基础知识、设置 Wireshark 视图、捕获过滤器技巧、显示过滤器技巧、着色规则和数据包导出、构建图表、重组数据、添加注释等。通过本篇的学习，读者可以掌握 Wireshark 的基本操作，灵活地使用捕获过滤器和显示过滤器，可以对 Wireshark 中的数据进行重组构建图表等。

第2篇 网络协议分析篇（第10~20章）

本篇主要包括：ARP 协议抓包分析、互联网协议（IP）抓包分析、UDP 协议抓包分析、TCP 协议抓包分析、ICMP 协议抓包分析、DHCP 数据抓包分析、DNS 抓包分析、HTTP 协议抓包分析、HTTPS 协议抓包分析、FTP 协议抓包分析和电子邮件抓包分析。通过本篇的学习，读者可以掌握 TCP/IP 协议族中每层中包括的协议、协议的格式及传输的数据等。

第3篇 实战篇（第21章）

本篇主要包括：操作系统启动过程抓包分析。通过本篇的学习，读者可以掌握一个操作系统启动过程中会自动开启哪些服务、获取地址的过程及启动的一些应用程序等。

本书配套资源获取方式

本书涉及的源程序、工具及接线图等资源需要读者自行下载。请登录清华大学出版社的网站 <http://www.tup.com.cn>，搜索到本书页面后按照提示下载即可。另外，读者也可以到 www.wanjuanchina.net 社区的相关版块下载。

本书读者对象

- ☐ Wireshark 初学者；
- ☐ 想全面学习 Wireshark 的人员；
- ☐ 各种兴趣爱好者；
- ☐ 网络管理员；
- ☐ 专业的安全渗透测试人员；
- ☐ 大中专院校的学生；
- ☐ 社会培训班学员。

本书作者

本书由王晓卉、李亚伟编写，其中营口职业技术学院的王晓卉负责编写第 1~9 章，李亚伟负责编写第 10~21 章。其他参与编写的人员有陈刚、陈世琼、黄点点、黄海力、黄绍斌、蒋春蕾、李国良、李俊娜、李晓娜、刘永纯、王书勇、王挺、王文强、张伟、张小华、胡丹萍、王以荣、徐阳。

阅读本书的过程中若有任何疑问，都可以发邮件或者在论坛和 QQ 群里提问，会有专人为您解答。最后顺祝各位读者读书快乐！

编者

目 录

第 1 篇 Wireshark 应用篇

第 1 章 Wireshark 的基础知识	2
1.1 Wireshark 的功能	2
1.1.1 Wireshark 主窗口界面	2
1.1.2 Wireshark 的作用	3
1.2 安装 Wireshark	4
1.2.1 获取 Wireshark	4
1.2.2 安装 Wireshark	6
1.3 Wireshark 捕获数据	10
1.4 认识数据包	10
1.5 捕获 HTTP 包	13
1.6 访问 Wireshark 资源	16
1.7 Wireshark 快速入门	18
1.8 分析网络数据	25
1.8.1 分析 Web 浏览数据	26
1.8.2 分析后台数据	28
1.9 打开其他工具捕获的文件	29
第 2 章 设置 Wireshark 视图	30
2.1 设置 Packet List 面板列	30
2.1.1 添加列	30
2.1.2 隐藏、删除、重新排序及编辑列	31
2.2 Wireshark 分析器及 Profile 设置	37
2.2.1 Wireshark 分析器	37
2.2.2 分析非标准端口号流量	39
2.2.3 设置 Wireshark 显示的特定数据类型	42
2.2.4 使用 Profile 定制 Wireshark	47
2.2.5 查找关键的 Wireshark Profile	48
2.3 数据包时间延迟	50
2.3.1 时间延迟	50
2.3.2 检查延迟问题	51
2.3.3 检查时间差延迟问题	53
第 3 章 捕获过滤器技巧	56
3.1 捕获过滤器简介	56

3.2	选择捕获位置	57
3.3	选择捕获接口	58
3.3.1	判断哪个适配器上的数据	58
3.3.2	使用多适配器捕获	59
3.4	捕获以太网数据	59
3.5	捕获无线数据	60
3.5.1	捕获无线网络数据的方式	60
3.5.2	使用 AirPcap 适配器	61
3.6	处理大数据	61
3.6.1	捕获过滤器	61
3.6.2	捕获文件集	62
3.7	处理随机发生的问题	64
3.8	捕获基于 MAC/IP 地址数据	66
3.8.1	捕获单个 IP 地址数据	66
3.8.2	捕获 IP 地址范围	68
3.8.3	捕获广播或多播地址数据	70
3.8.4	捕获 MAC 地址数据	70
3.9	捕获端口应用程序数据	73
3.9.1	捕获所有端口号的数据	73
3.9.2	结合基于端口的捕获过滤器	74
3.10	捕获特定 ICMP 数据	77
第 4 章	显示技巧	80
4.1	显示过滤器简介	80
4.2	使用显示过滤器	81
4.2.1	显示过滤器语法	81
4.2.2	检查语法错误	83
4.2.3	识别字段名	85
4.2.4	比较运算符	87
4.2.5	表达式过滤器	87
4.2.6	使用自动补全功能	89
4.2.7	手动添加显示列	90
4.3	编辑和使用默认显示过滤器	93
4.4	过滤显示 HTTP	94
4.5	过滤显示 DHCP	97
4.6	根据地址过滤显示	98
4.6.1	显示单个 IP 地址或主机数据	98
4.6.2	显示一个地址范围的数据	100
4.6.3	显示一个子网 IP 的数据	101
4.7	过滤显示单一的 TCP/UDP 会话	102
4.8	使用复杂表达式过滤	106
4.8.1	使用逻辑运算符	106
4.8.2	使用括号	108
4.8.3	使用关键字	110
4.8.4	使用通配符	112

4.9 发现通信延迟	114
4.9.1 时间过滤器 (frame.time_delta)	114
4.9.2 基于 TCP 的时间过滤 (tcp.time_delta)	115
4.10 设置显示过滤器按钮	117
4.10.1 创建显示过滤器表达式按钮	118
4.10.2 编辑、添加、删除显示过滤器按钮	118
4.10.3 编辑 preferences 文件	119
第 5 章 着色规则和数据包导出	122
5.1 认识着色规则	122
5.2 禁用着色规则	123
5.2.1 禁用指定类型数据包彩色高亮	123
5.2.2 禁用所有包彩色高亮	125
5.3 创建用户着色规则	125
5.3.1 创建时间差着色规则	125
5.3.2 快速查看 FTP 用户名密码着色规则	127
5.3.3 创建单个会话着色规则	130
5.4 导出数据包	131
5.4.1 导出显示包	131
5.4.2 导出标记包	133
5.4.3 导出包的详细信息	134
第 6 章 构建图表	139
6.1 数据统计表	139
6.1.1 端点统计	139
6.1.2 网络会话统计	141
6.1.3 快速过滤会话	142
6.1.4 地图化显示端点统计信息	144
6.2 协议分层统计	147
6.3 图表化显示带宽使用情况	148
6.3.1 认识 IO Graph	148
6.3.2 应用显示过滤器	149
6.4 专家信息	152
6.5 构建各种网络错误图表	154
6.5.1 构建所有 TCP 标志位包	154
6.5.2 构建单个 TCP 标志位包	155
第 7 章 重组数据	157
7.1 重组 Web 会话	157
7.1.1 重组 Web 浏览会话	157
7.1.2 导出 HTTP 对象	162
7.2 重组 FTP 会话	165
7.2.1 重组 FTP 数据	165
7.2.2 提取 FTP 传输的文件	167
第 8 章 添加注释	170
8.1 捕获文件注释	170

8.2 包注释	170
8.2.1 添加包注释	171
8.2.2 查看包注释	171
8.3 导出包注释	173
8.3.1 使用 Export Packet Dissections 功能导出	173
8.3.2 使用复制功能导出包	175
第9章 捕获、分割和合并数据	177
9.1 将大文件分割为文件集	177
9.1.1 添加 Wireshark 程序目录到自己的位置	177
9.1.2 使用 Capinfos 获取文件大小和包数	177
9.1.3 分割文件	178
9.2 合并多个捕获文件	183
9.3 命令行捕获数据	184
9.3.1 Dumpcap 和 Tshark 工具	184
9.3.2 使用捕获过滤器	187
9.3.3 使用显示过滤器	188
9.4 导出字段值和统计信息	189
9.4.1 导出字段值	189
9.4.2 导出数据统计	191

第2篇 网络协议分析篇

第10章 ARP 协议抓包分析	196
10.1 ARP 基础知识	196
10.1.1 什么是 ARP	196
10.1.2 ARP 工作流程	196
10.1.3 ARP 缓存表	197
10.2 捕获 ARP 协议包	200
10.2.1 Wireshark 位置	200
10.2.2 使用捕获过滤器	201
10.3 分析 ARP 协议包	203
10.3.1 ARP 报文格式	203
10.3.2 ARP 请求包	204
10.3.3 ARP 响应包	205
第11章 互联网协议 (IP) 抓包分析	207
11.1 互联网协议 (IP) 概述	207
11.1.1 互联网协议地址 (IP 地址) 的由来	207
11.1.2 IP 地址	208
11.1.3 IP 地址的构成	208
11.2 捕获 IP 数据包	209
11.2.1 什么是 IP 数据报	209
11.2.2 Wireshark 位置	210

11.2.3 捕获 IP 数据包	210
11.2.4 捕获 IP 分片数据包	213
11.3 IP 数据报首部格式	215
11.3.1 存活时间 TTL	216
11.3.2 IP 分片	217
11.4 分析 IP 数据包	218
11.4.1 分析 IP 首部	218
11.4.2 分析 IP 数据包中 TTL 的变化	220
11.4.3 IP 分片数据包分析	223
第 12 章 UDP 协议抓包分析	229
12.1 UDP 协议概述	229
12.1.1 什么是 UDP 协议	229
12.1.2 UDP 协议的特点	229
12.2 捕获 UDP 数据包	230
12.3 分析 UDP 数据包	232
12.3.1 UDP 首部格式	233
12.3.2 分析 UDP 数据包	233
第 13 章 TCP 协议抓包分析	236
13.1 TCP 协议概述	236
13.1.1 TCP 协议的由来	236
13.1.2 TCP 端口	236
13.1.3 TCP 三次握手	237
13.1.4 TCP 四次断开	239
13.1.5 TCP 重置	239
13.2 捕获 TCP 数据包	240
13.2.1 使用捕获过滤器	240
13.2.2 使用显示过滤器	242
13.2.3 使用着色规则	243
13.3 TCP 数据包分析	249
13.3.1 TCP 首部	249
13.3.2 分析 TCP 的三次握手	251
13.3.3 分析 TCP 的四次断开	257
13.3.4 分析 TCP 重置数据包	263
第 14 章 ICMP 协议抓包分析	266
14.1 ICMP 协议概述	266
14.1.1 什么是 ICMP 协议	266
14.1.2 学习 ICMP 的重要性	266
14.1.3 Echo 请求与响应	267
14.1.4 路由跟踪	267
14.2 捕获 ICMP 协议包	267
14.2.1 捕获正常 ICMP 数据包	268
14.2.2 捕获请求超时的数据包	269
14.2.3 捕获目标主机不可达的数据包	271

14.3 分析 ICMP 数据包	272
14.3.1 ICMP 首部	272
14.3.2 分析 ICMP 数据包——Echo Ping 请求包	274
14.3.3 分析 ICMP 数据包——Echo Ping 响应包	275
14.3.4 分析 ICMP 数据包——请求超时数据包	277
14.3.5 分析 ICMP 数据包——目标主机不可达的数据包	279
第 15 章 DHCP 数据抓包分析	281
15.1 DHCP 概述	281
15.1.1 什么是 DHCP	281
15.1.2 DHCP 的作用	281
15.1.3 DHCP 工作流程	282
15.2 DHCP 数据抓包	284
15.2.1 Wireshark 位置	284
15.2.2 使用捕获过滤器	284
15.2.3 过滤显示 DHCP	289
15.3 DHCP 数据包分析	291
15.3.1 DHCP 报文格式	291
15.3.2 DHCP 报文类型	292
15.3.3 发现数据包	293
15.3.4 响应数据包	296
15.3.5 请求数据包	298
15.3.6 确认数据包	301
第 16 章 DNS 抓包分析	304
16.1 DNS 概述	304
16.1.1 什么是 DNS	304
16.1.2 DNS 的系统结构	305
16.1.3 DNS 系统解析过程	305
16.1.4 DNS 问题类型	307
16.2 捕获 DNS 数据包	307
16.3 分析 DNS 数据包	311
16.3.1 DNS 报文格式	311
16.3.2 分析 DNS 数据包	312
第 17 章 HTTP 协议抓包分析	317
17.1 HTTP 协议概述	317
17.1.1 什么是 HTTP	317
17.1.2 HTTP 请求方法	317
17.1.3 HTTP 工作流程	318
17.1.4 持久连接和非持久连接	319
17.2 捕获 HTTP 数据包	320
17.2.1 使用捕获过滤器	320
17.2.2 显示过滤 HTTP 协议包	323
17.2.3 导出数据包	326
17.3 分析 HTTP 数据包	332

17.3.1	HTTP 报文格式	332
17.3.2	HTTP 的头域	333
17.3.3	分析 GET 方法的 HTTP 数据包	335
17.3.4	分析 POST 方法的 HTTP 数据包	339
17.4	显示捕获文件的原始内容	343
17.4.1	安装 Xplico	343
17.4.2	解析 HTTP 包	344
第 18 章 HTTPS 协议抓包分析		351
18.1	HTTPS 协议概述	351
18.1.1	什么是 HTTPS 协议	351
18.1.2	HTTP 和 HTTPS 协议的区别	351
18.1.3	HTTPS 工作流程	352
18.2	SSL 概述	352
18.2.1	什么是 SSL	353
18.2.2	SSL 工作流程	353
18.2.3	SSL 协议的握手过程	353
18.3	捕获 HTTPS 数据包	354
18.3.1	使用捕获过滤器	354
18.3.2	显示过滤数据包	356
18.4	分析 HTTPS 数据包	359
18.4.1	客户端发出请求 (Client Hello)	360
18.4.2	服务器响应 (Server Hello)	362
18.4.3	证书信息	363
18.4.4	密钥交换	365
18.4.5	应用层信息通信	367
第 19 章 FTP 协议抓包分析		368
19.1	FTP 协议概述	368
19.1.1	什么是 FTP 协议	368
19.1.2	FTP 的工作流程	368
19.1.3	FTP 常用控制命令	369
19.1.4	应答格式	370
19.2	捕获 FTP 协议数据包	372
19.3	分析 FTP 协议数据包	375
19.3.1	分析控制连接的数据	375
19.3.2	分析数据连接的数据	376
第 20 章 电子邮件抓包分析		380
20.1	邮件系统工作原理	380
20.1.1	什么邮件客户端	380
20.1.2	邮件系统的组成及传输过程	380
20.2	邮件相关协议概述	381
20.2.1	SMTP 协议	382
20.2.2	POP 协议	383
20.2.3	IMAP 协议	384

20.3 捕获电子邮件数据包	386
20.3.1 Wireshark 捕获位置	386
20.3.2 Foxmail 邮件客户端的使用	387
20.3.3 捕获电子邮件数据包	389
20.4 分析发送邮件的数据包	390
20.4.1 分析 SMTP 工作流程	391
20.4.2 查看邮件内容	392
20.5 分析接收邮件的数据包	393
20.5.1 分析 POP 工作流程	393
20.5.2 查看邮件内容	395

第 3 篇 实战篇

第 21 章 操作系统启动过程抓包分析	398
21.1 操作系统概述	398
21.2 捕获操作系统启动过程产生的数据包	399
21.3 分析数据包	401
21.3.1 获取 IP 地址	401
21.3.2 加入组播组	402
21.3.3 发送 NBNS 协议包	402
21.3.4 ARP 协议包的产生	403
21.3.5 访问共享资源	404
21.3.6 开机自动运行的程序	404

第 1 篇 Wireshark 应用篇

» 第 1 章 Wireshark 的基础知识

» 第 2 章 设置 Wireshark 视图

» 第 3 章 捕获过滤器技巧

» 第 4 章 显示技巧

» 第 5 章 着色规则和数据包导出

» 第 6 章 构建图表

» 第 7 章 重组数据

» 第 8 章 添加注释

» 第 9 章 捕获、分割和合并数据

第 1 章 Wireshark 的基础知识

Wireshark（前称 Ethereal）是一个网络包分析工具。该工具主要是用来捕获网络包，并显示包的详细情况。本章将介绍 Wireshark 的基础知识。

1.1 Wireshark 的功能

在学习 Wireshark 之前，首先介绍一下它的功能。了解它的功能，可以帮助用户明确借助该工具能完成哪些工作。本节将介绍 Wireshark 的基本功能。

1.1.1 Wireshark 主窗口界面

在学习使用 Wireshark 之前，首先需要了解该工具主窗口界面中每部分的作用。Wireshark 主窗口界面如图 1.1 所示。

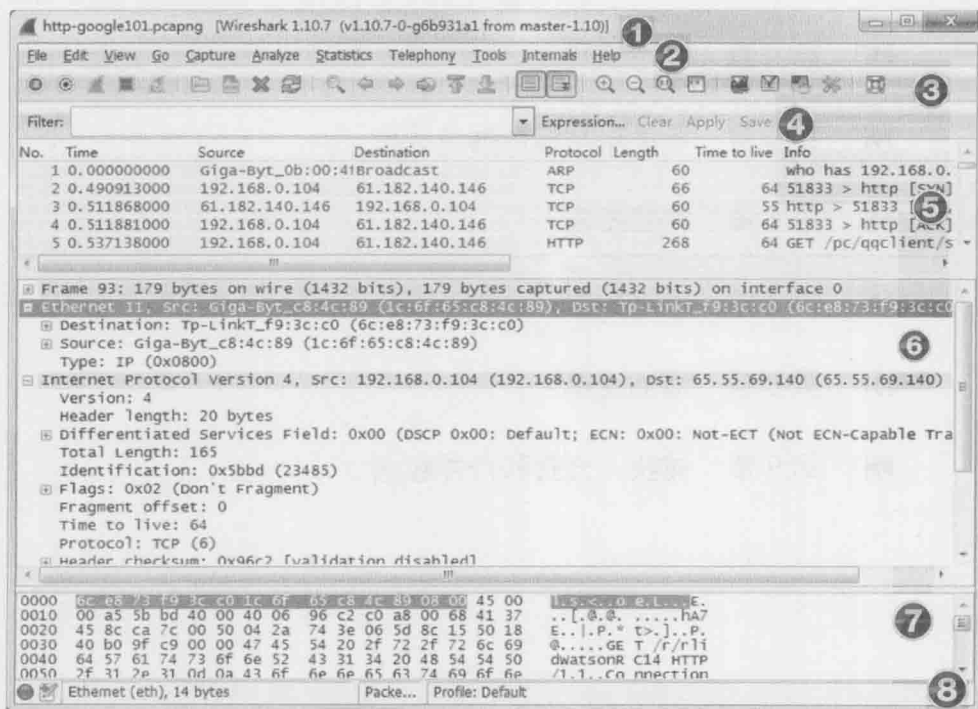


图 1.1 Wireshark 主窗口界面

在图 1.1 中,以编号的形式已将 Wireshark 主窗口每部分标出。下面分别介绍每部分的含义,如下所示。

- ☐ ① 标题栏——用于显示文件名称、捕获的设备名称和 Wireshark 版本号。
- ☐ ② 菜单栏——Wireshark 的标准菜单栏。
- ☐ ③ 工具栏——常用功能快捷图标按钮。
- ☐ ④ 显示过滤区域——减少查看数据的复杂度。
- ☐ ⑤ Packet List 面板——显示每个数据帧的摘要。
- ☐ ⑥ Packet Details 面板——分析封包的详细信息。
- ☐ ⑦ Packet Bytes 面板——以十六进制和 ASCII 格式显示数据包的细节。
- ☐ ⑧ 状态栏——专家信息、注释、包数和 Profile。

1.1.2 Wireshark 的作用

Wireshark 是一个广受欢迎的网络数据包分析软件。网络数据包分析软件的功能是截取网络数据包,并尽可能显示出最为详细的网络数据包数据。它是一个最知名的开源应用程序安全工具。Wireshark 可以运行在 Windows、MAC OS X、Linux 和 UNIX 操作系统上,它甚至可以作为一个 Portable App 运行。本小节将介绍 Wireshark 的常用功能。使用 Wireshark 可以快速分析一些任务,如下所示。

1. 一般分析任务

- ☐ 找出在一个网络内发送数据包最多的主机。
- ☐ 查看网络通信。
- ☐ 查看某个主机使用了哪些程序。
- ☐ 基本正常的网络通信。
- ☐ 验证特有的网络操作。
- ☐ 了解尝试连接无线网络的用户。
- ☐ 同时捕获多个网络的数据。
- ☐ 实施无人值守数据捕获。
- ☐ 捕获并分析到/来自一个特定主机或子网的数据。
- ☐ 通过 FTP 或 HTTP 查看和重新配置文件传输。
- ☐ 从其他捕获工具导入跟踪文件。
- ☐ 使用最少的资源捕获数据。

2. 故障任务

- ☐ 为故障创建一个自定义的分析环境。
- ☐ 确定路径、客户端和服务延迟。
- ☐ 确定 TCP 问题。
- ☐ 检查 HTTP 代理问题。
- ☐ 检查应用程序错误响应。
- ☐ 通过查看图形显示的结果,找出相关的网络问题。