《计算机网络》实验指导书

实验一 应用层协议消息的捕获和解析

北京邮电大学网络空间安全学院

2025 年 3 月

目　　录

实验一：应用层协议消息的捕获和解析

1. 实验类别

协议分析验证型

2. 实验内容和实验目的

本次实验主要包含下列内容：

1） 使用 Wireshark 软件捕获 HTTP 消息，分析其消息头，理解 HTTP 的通信原理；

2） 使用 Wireshark 软件捕获一次从客户端发送 Email 的过程，分析 SMTP 消息，理解 Email 系统中发送邮件的通信原理；

3）使用 Telnet 软件访问 Email 服务器，输入 SMTP 命令与 Email 服务器交互，理解 SMTP 的通信过程和 Base64 编码的概念。

通过本实验，学生可以深入理解典型的应用层协议——HTTP 和 SMTP 的要点。

3. 实验学时

4 学时。

4. 实验组人数

每组 1 人，独立完成数据捕获工作、进行分析并撰写实验报告。

5. 实验设备环境

一台装有 MS Windows 系列操作系统、Linux 或 Mac 操作系统的计算机，能够连接到因特网，并安装 Wireshark 软件。

6. 教学要点与学习难点

在课堂教学和教材中，涵盖了 DNS、HTTP、SMTP 等应用层协议的工作原理和主要通信过程，但是学生对于通信的细节和消息的关键字段及其作用缺乏感性认识，理解不足。在本实验中，学生通过使用 Wireshark 软件来捕获网络上实际传输的数据，可以加深对于上述协议的要点的理解；并且对于教材中没有包含或阐述不够详细的内容，例如 DNS 请求/应答消息中关于问题和回答的描述、常用的 HTTP 消息头、SMTP 消息中关于用户名和密码的命令和 Base64 的应用等，均可以通过分析数据格式和协议流程进行自学和了解。

在本实验中，熟悉 Wireshark 软件并进行消息捕获的工作比较简单，实验的重点和难点在于协议的分析工作。此外，学生应学会使用 telnet 程序远程访问邮件服务器，输入 SMTP 命令与服务器通信。

7. 实验步骤

7.1 准备工作

1. 下载 Wireshark 软件并了解其功能和使用方法。
2. 确保计算机已经连接到网络。

3. 启动 Wireshark，选择捕获接口为联网的本机网卡（本地连接或 WLAN），设置合适的捕获过滤器：
   - 对于 HTTP 消息，设置捕获过滤器为 `tcp port 80`
   - 对于 SMTP 消息，设置捕获过滤器为 `tcp port 25`
4. 开始捕获。

7.2 数据捕获

7.2.1 捕获 HTTP 协议数据

打开浏览器，从设置中清除 cookie 数据（访问记录），选择一个非 HTTPS 协议的网站，在地址栏里输入其 URL，如 www.xinhuanet.com，网页全部显示后停止捕获。

7.2.3 捕获 SMTP 协议数据

下载并安装邮件客户端软件（如 Foxmail），配置用户账户，设置发件服务器不选择 SSL，端口为 25。配置 wireshark，开始捕获，用 Foxmail 发送一封邮件，邮件发送成功后停止捕获。

7.2.4 使用 SMTP 命令与邮件服务器交互

在命令行模式，使用 telnet 程序连接到发件服务器，如 c:>telnet smtp.qq.com 25
在新窗口中，输入 SMTP 命令，与邮件服务器交互，常用的 SMTP 命令如表 1 所示
（注：命令不区分大写和小写，<SP>表示空格，<CRLF>表示回车换行——按下 Enter 键）。

表 1 常用的 SMTP 命令

SMTP 命令及格式	功能
EHLO<SP><domain><CRLF>	SMTP 客户端与 SMTP 服务器端建立连接后必须发送的第一条命令。 参数<domain>为 SMTP 服务器的域名。
AUTH<SP>LOGIN<CRLF>	SMTP 客户端向 SMTP 服务器端说明身份认证的方式。 注意：此命令得到的响应信息和后续的用户名及密码都必须以 Base64 编码。
MAIL<SP>FROM:<reverse-path><CRLF>	指定邮件发送者的邮箱地址，参数<reverse-path>表示发信人的邮箱地址。
RCPT<SP>TO:<forword-path><CRLF>	指定邮件接收者的邮箱地址，参数<forword-path>表示接收者的邮箱地址。 每条 RCPT 命令指定一个收信人。如果邮件要发送给多个收信人，应使用多条 RCPT 命令。
data<CRLF>	通知 SMTP 服务器端准备开始传送邮件内容。收到响应后，SMTP 客户端发送的所有数据都将被当做邮件内容，直至“<CRLF>.<CRLF>”标志符（即只有“.”的单独一行），则表示邮件内容结束。
QUIT<CRLF>	结束邮件发送过程，SMTP 服务器端收到此命令后，将关闭与 SMTP 客户端的 TCP 连接。

下图 1 显示了使用 telnet 与服务器 smtp.163.com 交互的示例。

图 1 使用 telnet 与 SMTP 服务器交互示例

注意：为确保命令正确，应使用与 wireshark 所捕获的相一致的命令及参数；因为要输入的

命令比较多，建议实现把各命令、及用户名/密码对应的 Base64 编码按顺序录入一个文本文件，然后复制到命令行窗口中，以避免输入错误。

7.3 协议分析

运行 Wireshark 软件，打开所捕获的数据文件，完成下列分析工作：

1. HTTP 消息分析：选择网页请求的 Get 消息及返回的 200 OK 应答消息，记录并分析消息头中各字段的值及其功能。
2. SMTP 消息分析：根据捕获到的消息，总结 SMTP 的各命令/响应消息的内容及功能，画出通信过程的消息序列图。

上述分析工作应在实验报告中进行详细描述，具体要求参见第 9 节。

7.4 撰写实验报告

按第 9 节的要求撰写实验报告，对于捕获到的数据进行认真分析，归纳各协议的工作原理和实现要点。

8. Wireshark 软件使用说明

本次实验使用的是 Wireshark 软件，其早期版本称为 Ethereal。Wireshark 是一个网络包分析工具，它可以捕获网络中传输的数据包，对于数据包进行解析，并显示包中各协议数据的详细内容，是目前最好的开源网络分析软件之一。Wireshark 可以应用在下列情形：

- 帮助网络管理员解决网络问题
- 帮助网络安全工程师检测安全隐患
- 帮助开发人员测试其开发的协议的执行情况
- 帮助学生学习网络协议

8.1 Wireshark 软件的安装

在 https://www.wireshark.org/download.html 下载 Wireshark 安装包并执行，安装选项可以选择默认配置。Wireshark 安装包中已包含 WinPcap，无需单独下载安装。

8.2 运行 Wireshark 并设置捕获条件

运行 Wireshark 软件，在启动页中选中活跃的网卡，如图 2 所示的 WLAN，然后设置捕获过滤器条件，可以设置需要捕获的协议和端口号，例如捕获 HTTP 消息时，应设为：tcp port 80。设置好后，点击左上角蓝色的图标即开始捕获。

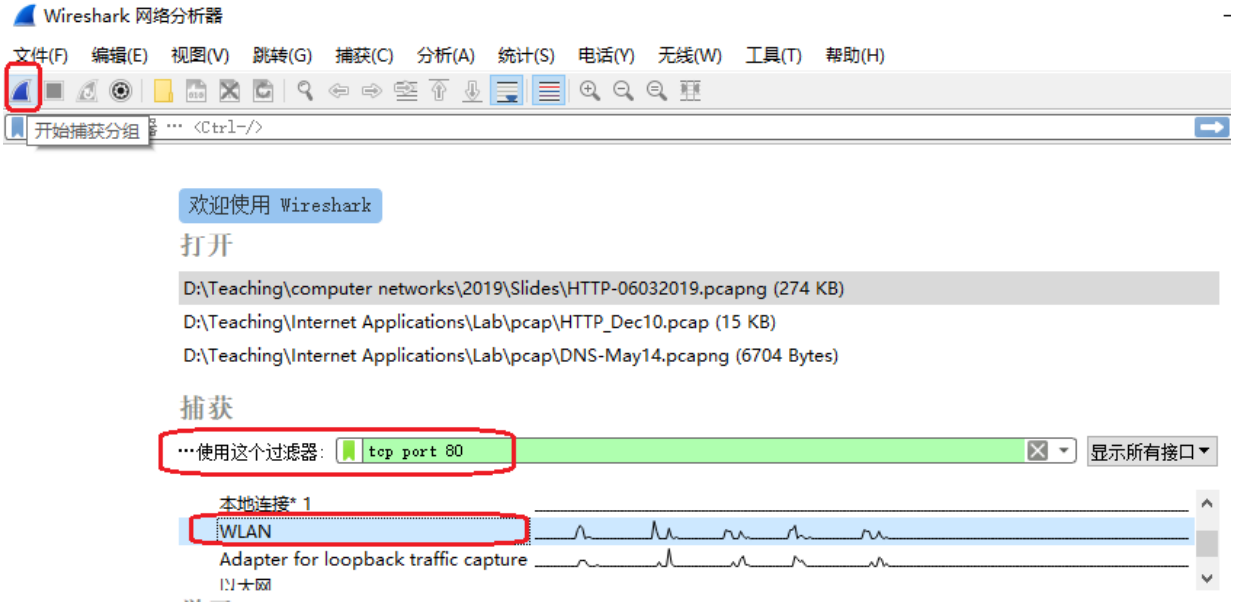

图 2　Wireshark 的捕获条件设置示例

8. 3 解码分析

启动捕获之后，运行相应的网络通信程序，Wireshark 即可以捕获到网卡发送和接收到的符合捕获条件的数据，并在显示在如图 4 所示的主窗口中。

注：在左上角的显示过滤器中进行设置，可以只显示需要的消息，例如图 4 中，左上角的 http 表示只显示 HTTP 消息。

Wireshark 的数据显示窗口分为 Packet List、Packet Detail 和 Packet Byte 三部分。

1. PacketList：显示所捕获到的所有数据包，每行显示一个数据包。如果选中一行，在下面的 Packet Detail 和 Packet Byte 窗口中显示对应的详细信息。

默认情况下，PacketList 显示包括下面各列：

- No. ：表示包的序号
- Time：表示包的时间戳
- Source：显示包的源 IP 地址
- Destination：显示包的目的 IP 地址
- Protocal：显示包内数据的协议类型
- Length：数据帧（不包括帧尾的校验字段）的长度
- Info：包内容的主要信息，例如对于 HTTP 消息，显示方法名、HTTP 版本、状态码等信息。

2. PacketDetail：显示在 PacketList 窗口中所选中的数据包解析后的详细信息，包括每个协议字段的含义及其值。PacketList 窗口中的显示是从数据链路层开始，每层协议显示一行概要信息，包括协议的源地址和目的地址。如图 4 示例的 TCP 消息，概要信息分别显示了以太网帧地址、IP 包地址和 TCP 数据报端口号。

每层协议的细节信息是以树状方式组织的，可以展开，如图 4 示例，对 HTTP 的协议消息进行了展开，可以看到命令行和每个消息头的名字、值和补充信息。

3. Packet Byte：以十六进制的方式在 PacketList 和 PacketDetail 窗口中所选中的部分对应的数据值。该窗口分为 3 部分，左侧分栏显示选中数据在整个帧中的偏移量，中间分栏显示 16 进制的对应值，右侧分栏显示对应的 ASCII 字符值。如图 3 所示，在 PacketDetail 窗口中选中了 HTTP 消息的命令行中的方法

名“GET”，Packet Byte 窗口则显示了其对应的二进制值和 ASCII 字符。

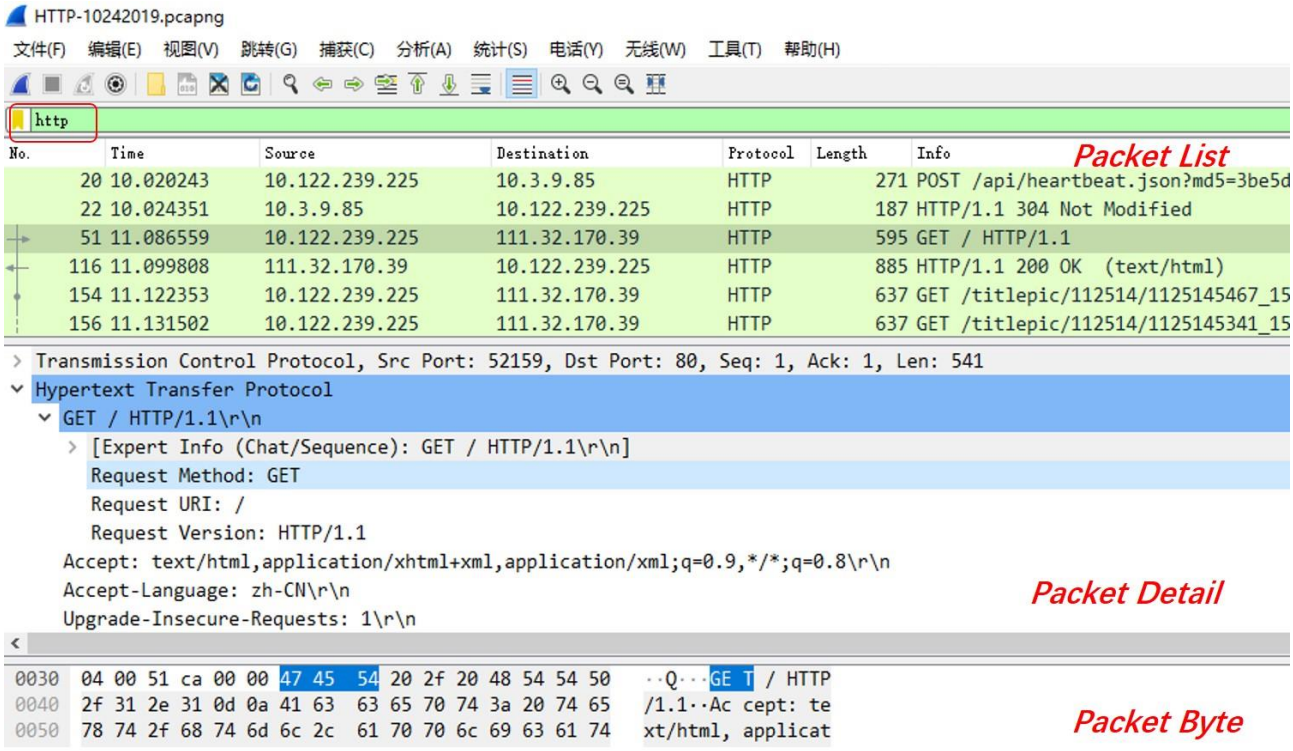

图 3 Wireshark 主窗口示例

关于 Wireshark 的详细功能和具体使用说明，请参照 Wireshark 用户手册。

9. 实验报告要求

本节描述了应提交实验报告的内容提纲和每项具体要求。实验完成后，应以电子版方式提交实验报告。

9.1 实验内容和实验步骤描述

描述本次实验的任务、内容、实验环境和实验步骤。

9.2 HTTP 协议分析

1） 根据捕获到的消息，对照讲义和教材，理解 HTTP 的功能和通信过程。
2） 观察 HTTP 请求/应答消息的各字段及消息头的内容，自己查找资料理解各消息头的功能，列表总结请求消息和应答消息中各字段及各消息头的功能及现有值的含义。

9.3 SMTP 协议分析

1） 根据捕获到的消息，对照讲义和教材，理解 SMTP 的功能和通信过程。
2） 观察 SMTP 命令消息和响应状态码，自己查资料理解命令和状态码的功能，并画出一次完整通信过程所对应的消息序列图。

9.4 实验结论和实验心得

总结实验中遇到的问题和解决方案，总结实验心得。