**江苏科技大学**

**课程实验报告**

课 程： 计算机网络与安全

课 题： 网络协议分析与漏洞扫描

学 院： 计算机学院

姓 名： 陈四贵

班 级： 1822107101

学 号： 182210710119

指导老师： 张笑非

目 录

[一、 实验目的 1](#_Toc58924054)

[二、 实验内容 1](#_Toc58924055)

[三、 实验原理 1](#_Toc58924056)

[四、 实验步骤 3](#_Toc58924057)

[五、 实验结果 3](#_Toc58924058)

[六、 思考题 6](#_Toc58924059)

# 实验目的

1.掌握利用网络协议的分析、检测软件对实际网络中的各种协议进行分析的方法；

2.通过各协议的分析，进一步理解各协议的工作原理及其相应的报文格式；

3.掌握基于Python的端口扫描程序设计方法；

4.掌握Socket包中相关类和函数的使用方法。

# 实验内容

1.使用 Wireshark 在网络上对数据报进行搜集；

2.对搜集到的数据包进行分析，重点分析 ARP、IP、ICMP、TCP、UDP 等协议数据单元。

# 实验原理

网络协议分析部分：

◎Wireshark 是一个网络数据包分析软件，它能够抓获网络数据包，并尽量显示数据包的所有细节。利用Wireshark，网络管理员可以找出网络故障的根源，网络安全工程师可以找出安全隐患，开发人员可以调试所写的协议，而更多人可以了解网络协议的内部。

◎Wireshark 最基本的功能就是从网络上抓获实时的数据包，通过选择菜单“Capture‐>Interface”，将出现CaptureInterface 对话框。通过点击某个接口的Option按钮，可以设置该接口在抓获数据包时的相关参数。注意，如果是以太网接口，通常可以选择工作在混杂promiscuous 模式，但如果是在一些其它类型的接口上，则必须不能工作在该模式下，如Wifi接口。

◎通过设置好相关参数后，便可以点击Start按钮，开始抓获数据包，通过双击数据包列表中所感兴趣的某个具体的数据包，可以查看该数据包的PDU信息，除此以外，Wireshark 还有一些高级特性，如跟踪指定的TCP 数据流、将相关的数据包进行组合、将数字地址解析为名字等。利用Wireshark的统计特性，可以显示抓获的数据包总体信息、协议层次分布图、特定对话信息、端点信息、IO图等。这些功能可以参考Wireshark自带的UserGuide。

漏洞扫描部分：

端口扫描可以定义为一种监视技术，用于定位特定主机上可用的开放端口。 网络管理员，渗透测试人员或黑客可以使用此技术。 我们可以根据我们的要求配置端口扫描程序，以从目标系统获取最大的信息。

现在，考虑我们在运行端口扫描后可以获得的信息:有关开放端口的信息；有关在每个端口上运行的服务的信息；有关目标主机的OS和MAC地址的信息。

端口扫描就像一个窃贼，他想通过检查每扇门和窗户看哪些打开来进入房屋。如前所述，用于Internet通信的TCP / IP协议簇由TCP和UDP两个协议组成，这两个协议都有0到65535端口。由于始终建议关闭我们系统的不必要端口，因此实际上有65000多个门（端口）需要锁定，这些65535端口可以分为以下三个范围:

|  |  |
| --- | --- |
| 端口类型 | 端口范围 |
| 系统端口/知名端口 | [0, 1023] |
| 用户端口/注册端口 | [1024, 49151] |
| 动态端口/私有端口 | [49152, 65535] |

当使用ICMP进行扫描时，ICMP不是端口扫描，但它用于ping远程主机以检查主机是否已启动。 当我们必须检查网络中的多个活动主机时，此扫描很有用。 它涉及向主机发送ICMP ECHO请求，如果该主机处于活动状态，它将返回ICMP ECHO回复。

port\_scanner\_using\_icmp.jpg

Ping Sweep的概念: 实际上，从某种意义上讲，ping sweep也称为ping sweeping。 唯一的区别是ping扫描是在特定网络范围内查找多台计算机可用性的过程。 例如，假设我们要测试IP地址的完整列表，然后通过使用ping扫描（即操作系统的ping命令）来一次扫描IP地址将非常耗时。 这就是为什么我们需要使用ping扫描脚本的原因。

当使用TCP scan进行端口扫描时，我们要理解TCP的工作原理。要建立TCP连接，主机必须执行三向握手。请按照以下步骤执行操作：步骤1 设置了SYN标志的数据包，在此步骤中，尝试启动连接的系统从设置了SYN标志的数据包开始。步骤2 设置了SYN-ACK标志的数据包，在此步骤中，目标系统返回带有SYN和ACK标志集的数据包。步骤3 设置了ACK标志的数据包。最后，启动系统将把设置了ACK标志的数据包返回到原始目标系统。

但是，这里出现的问题是，如果我们可以使用ICMP回显请求和应答方法(ping scanner)进行端口扫描，那么为什么需要TCP扫描呢？其背后的主要原因是，假设如果我们关闭ICMP ECHO答复功能或对ICMP数据包使用防火墙，则ping扫描扫描程序将无法工作，我们需要TCP扫描。

# 实验步骤

网络协议分析部分：

1.运行 Wireshark，接着选择并设置好某接口的参数，最后开始抓获数据包。

2.分别抓获 5 个TCP、UDP、ICMP、HTTP 的PDU，以及5 个其它类型的PDU，记录这些数据包的信息并作分析。

3.跟踪某个特定的 TCP 流，并对它的特征进行描述和分析。

4.对所有抓获的数据包进行统计并作分析。

漏洞扫描部分：

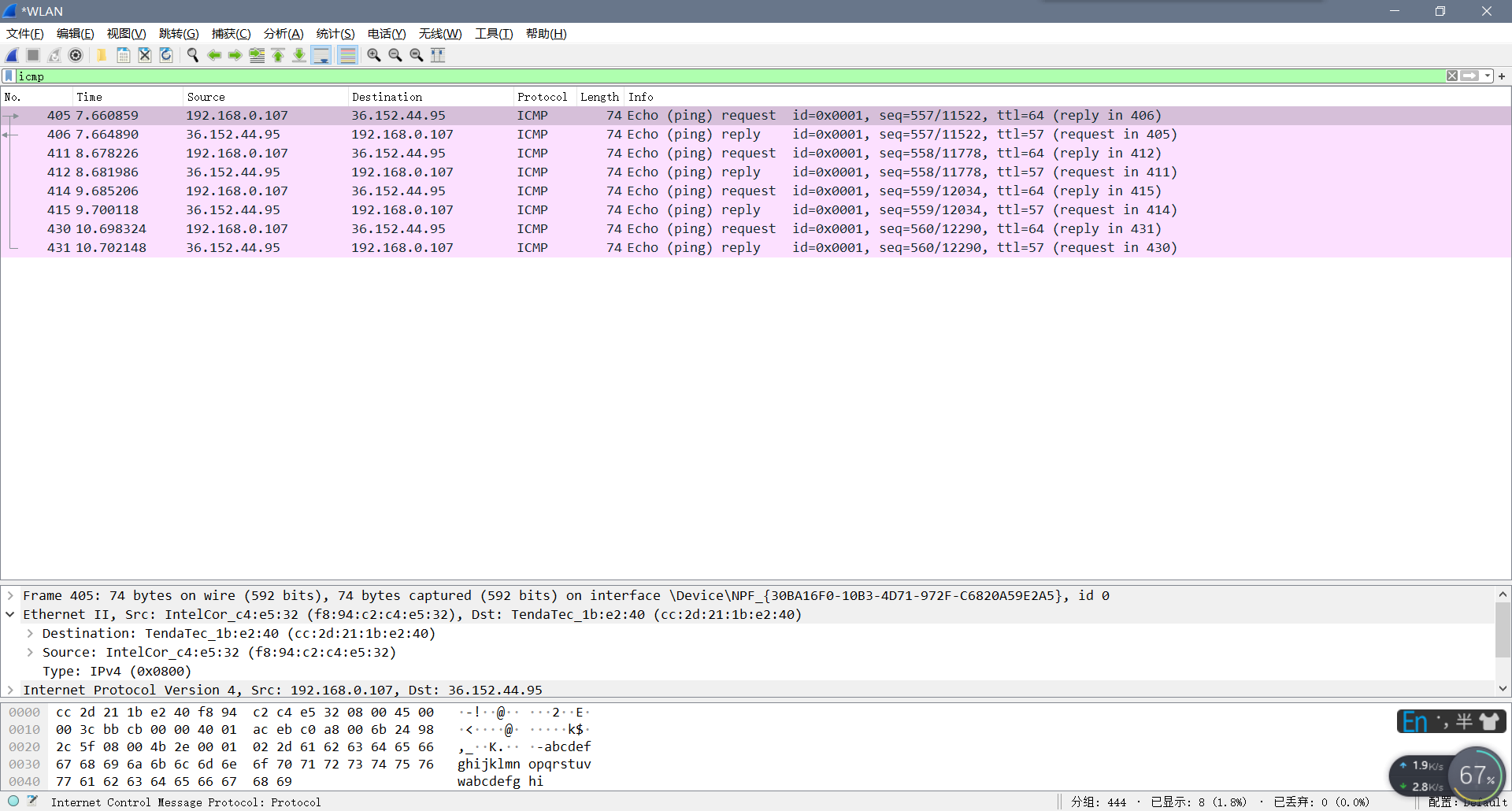
步骤一: 利用套接字扫描端口

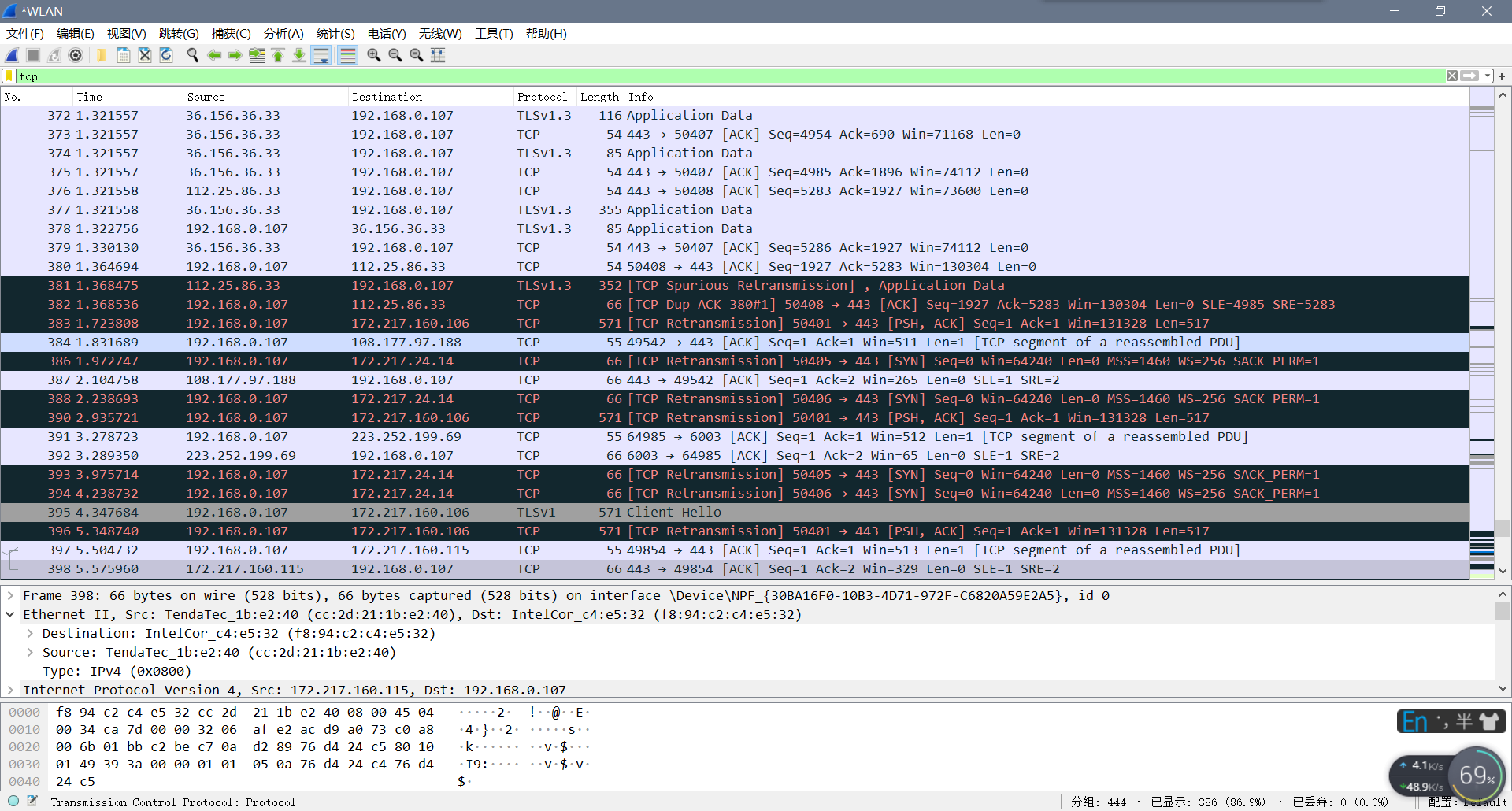
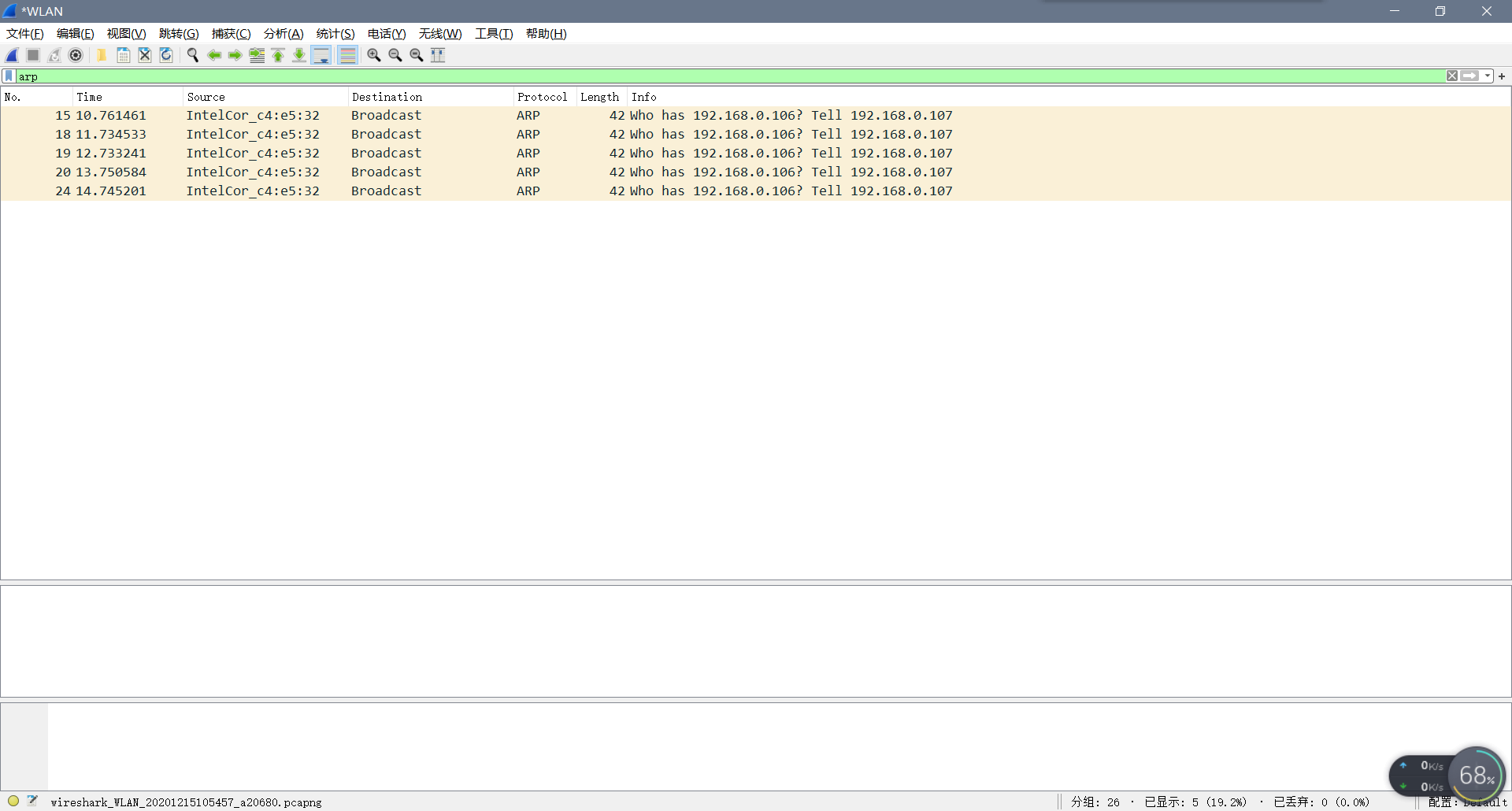
步骤二: 利用ICMP进行扫描

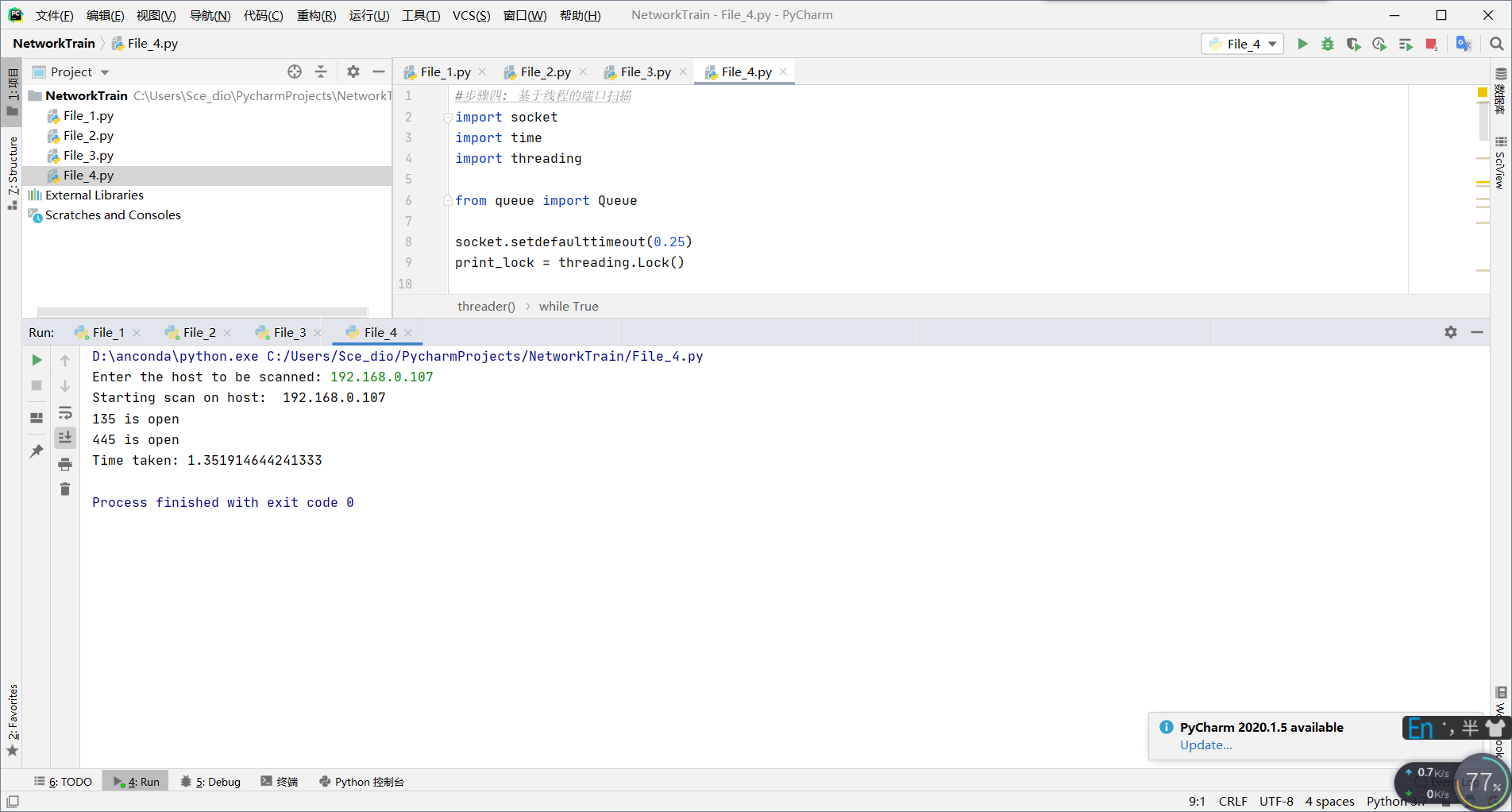
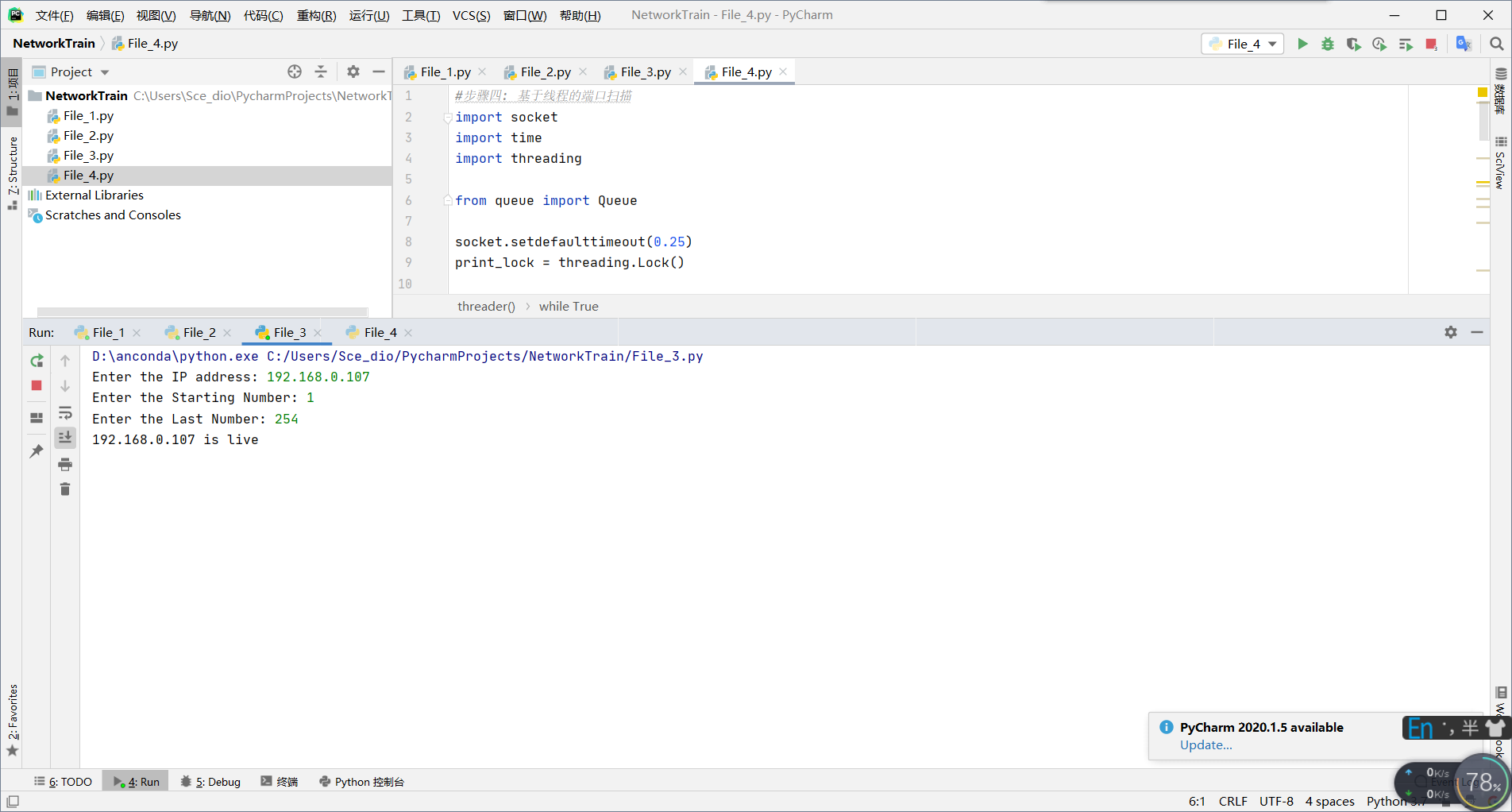
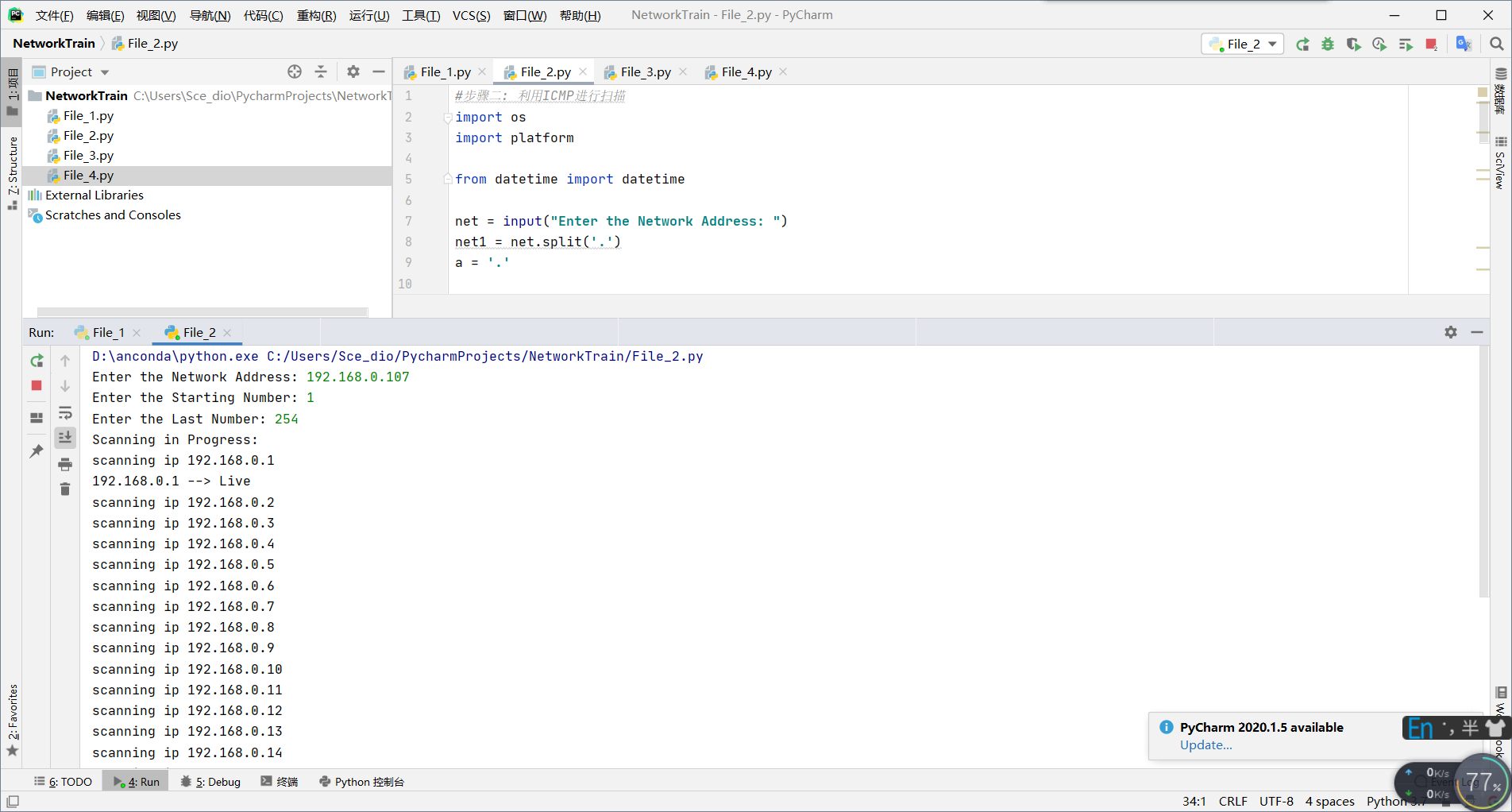
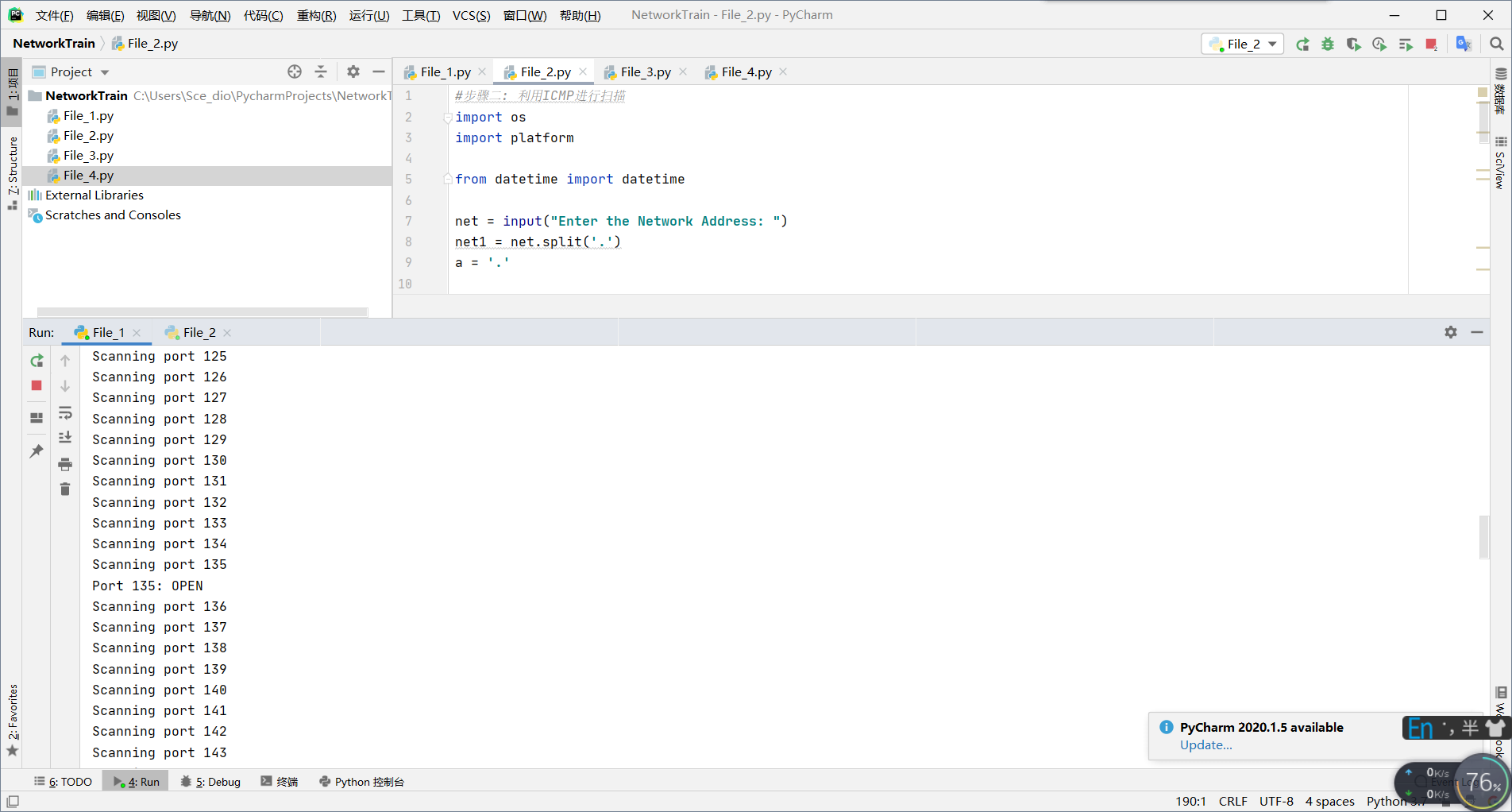
步骤三: 利用TCP scan进行端口扫描

步骤四: 基于线程的端口扫描

# 实验结果







# 思考题

1. 利用 Wireshark 所抓获的PDU 都属于OSI 的哪些层次，有什么共性，以及为什么会这样的共性？

答：网络层，都是数据包.因为wireshark是对各端口扫描抓包。

2. 如何能够抓获 FTP、SMTP 等类型的PDU？

答：在主机上发送、下载邮件等使用FTP、SMTP协议的应用，即可抓获FTP、SMTP等类型的数据包。