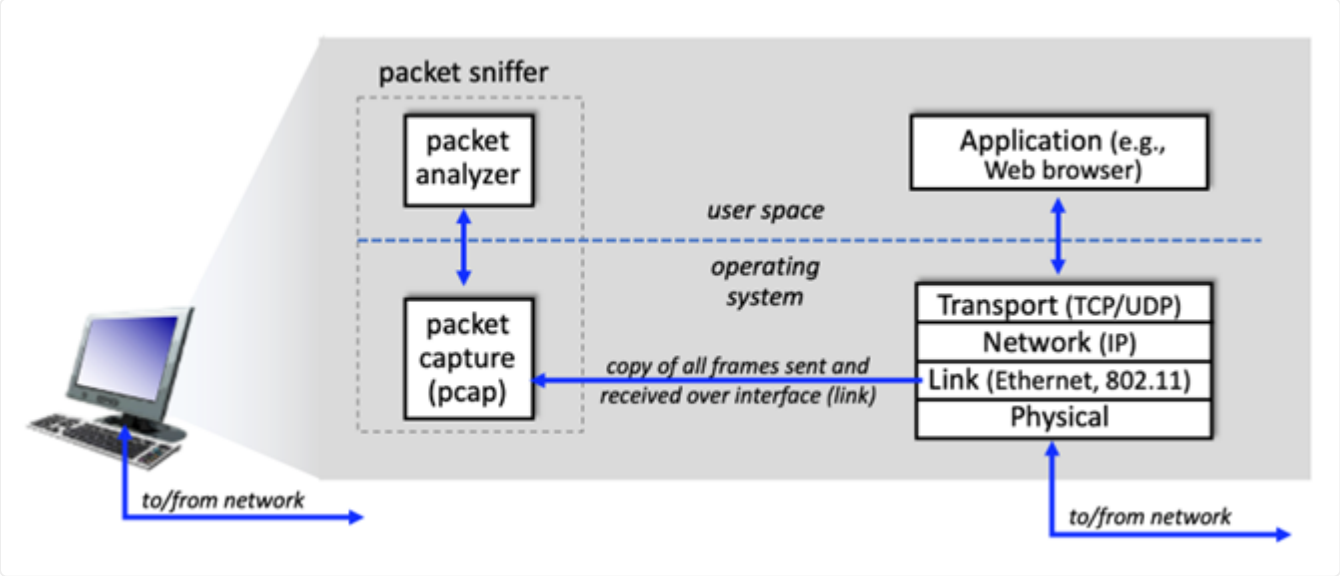
Lab 1: 使用Wireshark观察分组

一、实验目的

1. 掌握使用Wireshark捕获分组、分析分组内容的方法；
2. 观察网络协议运行情况，对分组的首部、载荷等基本结构形成直观认识；
3. 通过观察不同协议的分组，加深对网络协议层次模型的理解；
4. 体会重要信息在网络中明文传输的危险性，增强网络安全意识。

二、实验原理

网络嗅探器（Network Sniffer）是一种软件或硬件工具，用于捕获、分析和监视通过计算机网络传输的分组。网络嗅探器可以被用来监视网络流量、分析网络通信、识别潜在的安全问题，以及进行网络故障排除。嗅探器被动工作，它本身不发送分组，也没有分组明确以嗅探器为目的地。



网络嗅探器结构

上图展示了网络嗅探器的结构。右侧是通常在计算机上运行的协议（本例中为互联网协议）和应用程序（如网络浏览器或电子邮件客户端）。 虚线矩形内所示的网络嗅探器由两部分组成。第一部分是**分组捕获库**，它接收计算机通过给定接口（链路层，如以太网或 WiFi）发送或接收的每个链路层帧的副本。由于HTTP、FTP、TCP、UDP、DNS 或 IP 等高层协议交换的信息最

终都封装在链路层帧中，通过以太网电缆或 802.11 WiFi 无线电等物理介质传输。 因此，通过捕获所有链路层帧，就可以获得计算机中执行的所有协议和应用程序通过受监控链路发送/接收的所有信息。

分组嗅探器的第二个组成部分是**分组分析器**，它可以显示协议信息中所有字段的内容。 为此，分组分析器必须 “理解 ”协议交换的所有报文结构。 例如，假设我们想显示上图中 HTTP 协议交换的报文中的各个字段。分组分析仪了解以太网帧的格式，因此可以识别以太网帧中的 IP 数据报。 它还了解 IP 数据报格式，因此可以提取 IP 数据报中的 TCP 段。 最后，它了解 TCP 报文段结构，因此可以提取 TCP 报文段中包含的 HTTP 报文。 最后，它还了解 HTTP 协议，例如，它知道 HTTP 报文的第一个字节将包含字符串 “GET”、“POST ”或 “HEAD”。

在本学期的课程中，我们使用的网络嗅探器是Wireshark，它的具体安装和使用说明请见 附录A：Wireshark 教程。如上文所述，网络嗅探器通过捕获链路层帧来工作；但是根据wireshark的命名习惯，我们使用“分组”这个不那么精确的术语来统称链路层帧、网络层数据报、传输层报文段和应用层报文，并将wireshark的工作笼统称为捕获分组。

三、实验任务

请打开Wireshark分组捕获，并访问http版本（注意不是https，有时浏览器自动重定向到https，需要在地址栏手动修改）的复旦信息办网站http://ecampus.fudan.edu.cn/，回答以下问题：

1. 请列出捕获到的5种不同类型的协议。
2. 用显示过滤器过滤出所有http消息，从发送第一条 HTTP GET 请求到收到对应的 HTTP OK 回复用了多长时间？默认情况下，数据包列表窗口中 “Time”列的值是自 Wireshark 捕获开始经过的秒数，也可以点击菜单栏“视图-时间显示格式”切换到其他格式。
3. 复旦信息办的 IP 地址是什么？你的计算机发送 HTTP GET 请求时的 IP 地址是什么？
4. 找到任意一个 HTTP 包，发出 HTTP 请求的网络浏览器是什么？你可以在分组详细信息中的 Hypertext Transfer Protocol（也即 HTTP ）部分，或者追踪流的页面中寻找“User-Agent"字段。
5. 找到任意一个 TCP 包，源端口号和目的端口号各自是什么？你可以发现，分组详细信息中的Transmission Control Protocol（也即 TCP）部分列出了 Src Port 和 Dst Port。
6. 找到一个由多个 TCP 报文段组合而成的 HTTP 响应分组，这个分组是由多少个 TCP 报文段组成的？在分组详细信息中，会有“[x Reassembled TCP Segments]”提示。
7. 找到一个带有明文图片的分组，通过“显示分组字节”在 wireshark中显示图片，并在浏览器中找到对应图片。
8. （确保你已经为以上问题保存了必要的截图后）重新开启分组捕获，在复旦信息办网站右上角的导航栏搜索任意内容，在捕获到的分组里寻找你输入的内容，观察 HTTP 如何通过 POST 方法发送数据。

以下问题的现象可能会受浏览器缓存影响，如果你第一次访问指定网页时操作失误，请关闭该网页、清除浏览器缓存后再重新操作。重新开启分组捕获，访问 http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html ，输入用户名 wireshark-students，密码 network

9. 在抓取的分组中找到输入的用户名和密码（提示：传输使用了base64编码）。将地址中的http改为https（https://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html），还能否通过捕获分组获得密码？

Previous
计算机网络（H）实验课简介

Next
附录A：Wireshark 教程

Last updated 3 days ago