编程项目

网络流量查看器

演示文稿

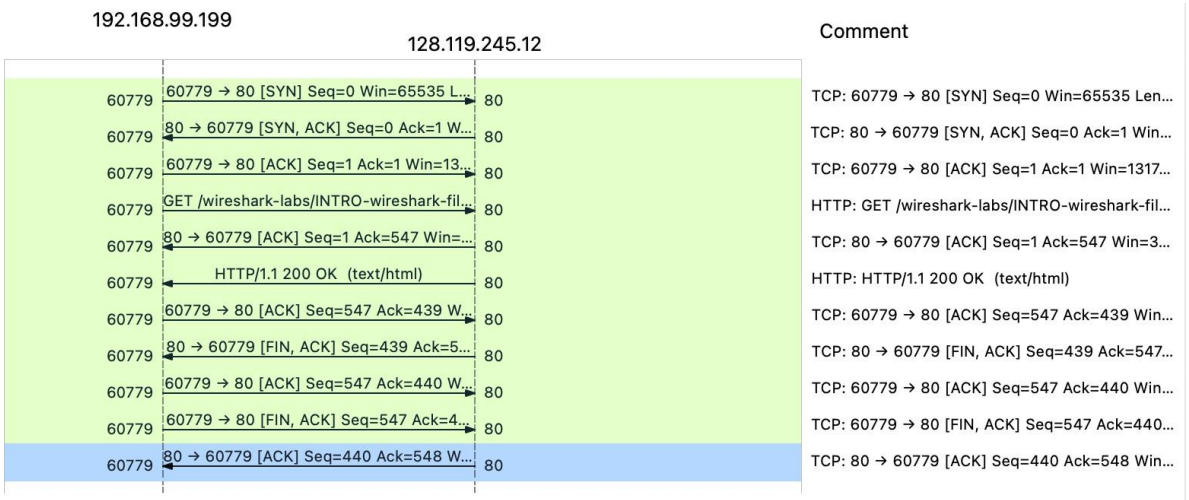
本项目的目标是对网络流量查看器进行编程。流量是指由两台机器执行的协议中交换的帧，每台机器由一个MAC地址、一个IP地址和可能的端口号来识别。

查看器将接受一个文本格式的跟踪文件作为输入，其中包含先前在以太网上捕获的字节。你的程序可以在命令窗口（终端类型）中运行，也可以在图形界面中运行。

你的分析仪能够理解的协议列表如下。

- 第二层：以太网
- 第三层：IPv4
- 第四层：TCP
- 第7层：HTTP

下面是一个预期结果的例子。



查看器按时间顺序显示一组帧，与它们在跟踪文件中出现的顺序相一致。对于每一帧，查看器都会显示以下信息。

- 所涉及的两台机器的IP地址。
- 使用的端口号。
- 封装的最高层协议的相关信息。

在每次运行时，查看器的结果必须保存在一个文本或pdf文件中，其格式要便于阅读。

提交

- 这个项目将分批进行。
- 你可以自由选择编程语言。
- 提交日期：**12月9日星期五23:59:00**。
- 需要提交的文件：

1. 在欧盟Moodle上提交一个**压缩档案**。
   a. 你的**源代码**。
   b. 一个**二进制文件**或**makefile文件**来开始运行你的扫描仪。
   c. 一个描述你的代码结构的**readme文件**。
   d. 一个解释如何安装和运行你的程序的**指南文件。**
2. 一段**10分钟的预录视频介绍**张贴在
   Youtube: 添加视频的链接。(你的视频将被添加到一个私人播放列表中）。不要点击 "这个视频是为儿童设计的"。

   在这个视频中，你将介绍:

   1. 对你的项目有一个**完整的概述**。
   2. 描述**你的个人选择、成就和贡献**。
   3. 你的观众在行动中的**演示。**

遵循的指示 1/ 在进入

时

你的程序接受一个跟踪文件（文本格式）作为输入，该文件包含在网络上捕获的 "原始 "字节。这些字节在Wireshark的 "捕获的字节 "面板中显示。这个文件可能包含几个按时间顺序排列的以太网帧（没有序言或FCS字段）。

- 每个字节都由两个十六进制的chiffres编码。
- 每个字节由一个空格分隔。
- 每一行都以同一行中第一个字节的off集开始。offset描述了这个字节在跟踪中的位置。
- 每个新的帧以0的off集开始，off集与位于它后面的捕获字节相隔三个空格。
- off集是以四个十六进制的chiff编码的。
- 十六进制字符可以是大写或小写。

2/ 退出时

你的程序的输出应该类似于Wireshark在 "流图 "工具中产生的信息。

查看器按时间顺序显示一组帧，与它们在跟踪文件中出现的顺序相一致。对于每一帧，查看器都会显示以下信息。

- 所涉及的两台机器的IP地址。
- 他们使用的端口号。
- 你认为与被封装的最高层协议有关的任何信息。这些信息将包括但不限于信息类型、序列号或识别号以及相关头字段的值。

查看器将通过选择发起特定流量和/或协议的机器的IP地址来查看一组过滤器，以查看其中的网络流。

在每次运行时，查看器的结果将被保存在一个文本或pdf文件中，其格式以方便阅读。