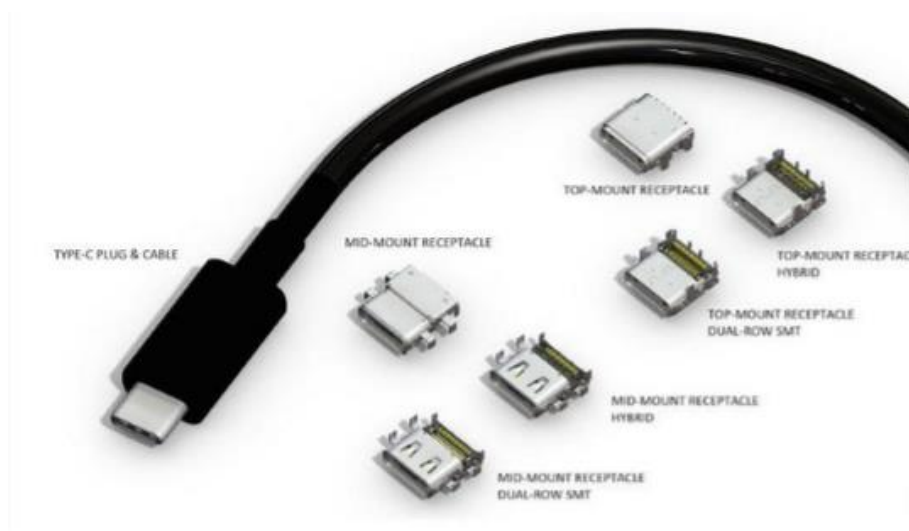
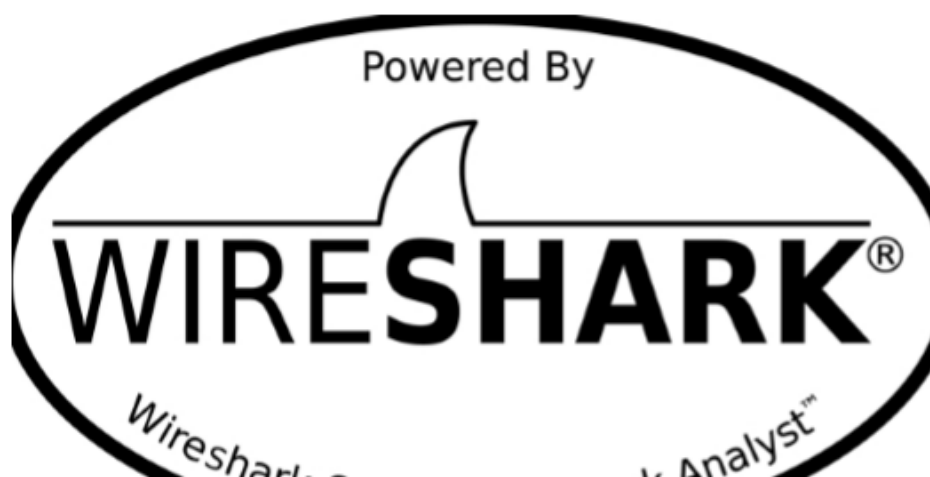


用 Wireshark 捕获 USB 数据

现在越来越多的电子设备采用 USB 接口进行通讯,通讯标准也在逐步提高。那么,我们就会好奇这些设备是如何工作的?而无论你是一个硬件黑客, 业余爱好者或者只是对它有一点兴趣的,USB 对我们都是具有挑战性的。



事实上通过 wireshark,我们可以捕获到 usb 设备发送给我们主机的数据,这样就可以进一步研究了。



本文中,我们将向大家介绍怎样通过 wireshark 捕获 usb 数据,使用的环境如下:

I Wireshark 2.0.1 (SVN)

I Linux kernel 4.1.6

你也可以用其他版本的 wireshark ,只要是 1.2.0 以上的都行。这里并没有 测试 window 上能不能行。

简介

在开始前 ,我们先介绍一些 USB 的基础知识。USB 有不同的规格 ,以下是 使用 USB 的三种方式 :

I USB UART

I USB HID

I USB Memory

UART 或者 Universal Asynchronous Receiver/Transmitter。这种方式 下 ,设备只是简单的将 USB 用于接受和发射数据 ,除此之外就再没有其他通讯 功能了。

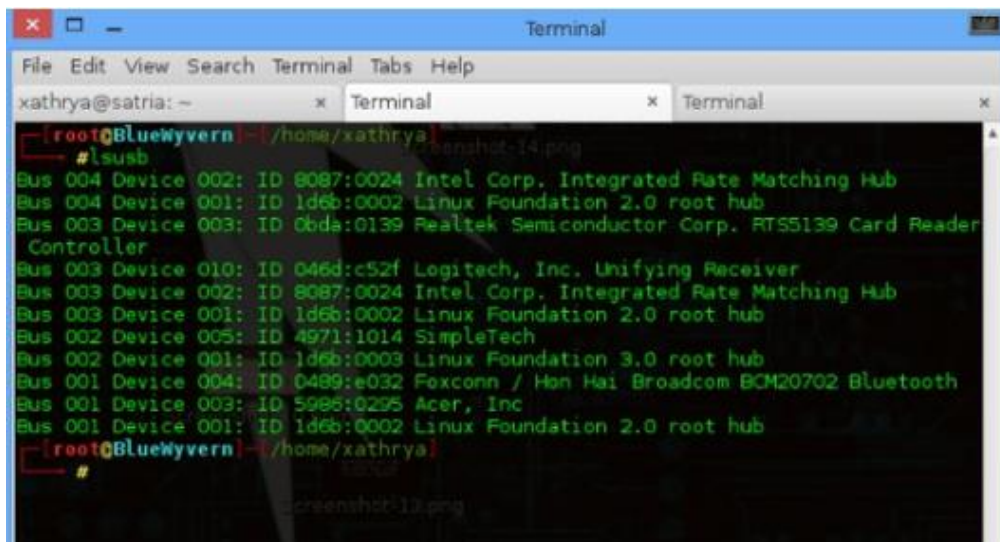
HID 是人性化的接口。这一类通讯适用于交互式 ,有这种功能的设备有 : 键盘 ,鼠标 ,游戏手柄和数字显示设备。

最后是 USB Memory ,或者说是数据存储。 External HDD, thumb drive / flash drive,等都是这一类的。

其中使用的最广的不是 USB HID 就是 USB Memory 了。

每一个 USB 设备 (尤其是 HID 或者 Memory)都有一个供应商 ID (Vendor Id) 和产品识别码 (Product Id)。 Vendor Id 是用来标记哪个厂

商生产了这个 USB 设备。 Product Id 用来标记不同的产品 ,他并不是一个特殊的数字 ,当然最好不同。如下图 :



```
root@BlueWyvern:~# lsusb
Bus 004 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub
Bus 004 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 003 Device 003: ID 0bda:0139 Realtek Semiconductor Corp. RTS5139 Card Reader Controller
Bus 003 Device 010: ID 046d:c52f Logitech, Inc. Unifying Receiver
Bus 003 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 005: ID 4971:1014 SimpleTech
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 004: ID 0489:e032 Foxconn / Hon Hai Broadcom BCM20702 Bluetooth
Bus 001 Device 003: ID 5986:0295 Acer, Inc
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@BlueWyvern:~#
```

上图是连接在我电脑上的 USB 设备列表，通过 lsusb 查看命令。

例如说，我有一个无线鼠标 Logitech。它是属于 HID 设备。这个设备正常的运行，并且通过 lsusb 这个命令查看所有 u s b 设备，现在大家能找出哪一条是这个鼠标吗？？没有错，就是第四个，就是下面这条：

Bus 003 Device 010: ID 046d:c52f Logitech, Inc. Unifying Receiver

其中，ID 046d:c52f 就是 Vendor-Product Id 对，Vendor Id 的值是 046d，并且 Product Id 的值是 c52f。Bus 003 Device 010 代表 usb 设备正常连接，这点需要记下来。

准备

我们用 root 权限运行 Wireshark 捕获 USB 数据流。但是通常来说我们不 建议这么做。我们需要给用户足够的权限来获取 linux 中的 usb 数据流。我们

可以用 udev 来达到我们的目的。我们需要创建一个用户组 usbmon，然后把 我们的账户添加到这个组中。

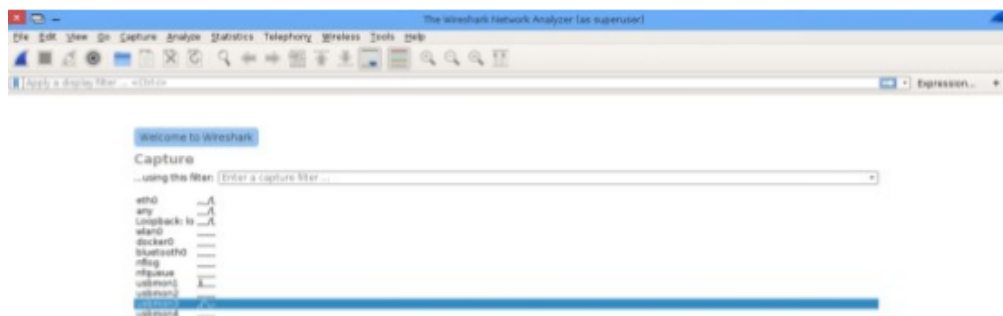
```
addgroup usbmon
gpasswd -a $USER usbmon
echo 'SUBSYSTEM=="usbmon", GROUP="usbmon", MODE="640" >
/etc/udev/rules.d/99-usbmon.rules
```

接下来 , 我们需要 usbmon 内核模块。如果该模块没有被加载 , 我们可以 通过以下命令加载该模块 :

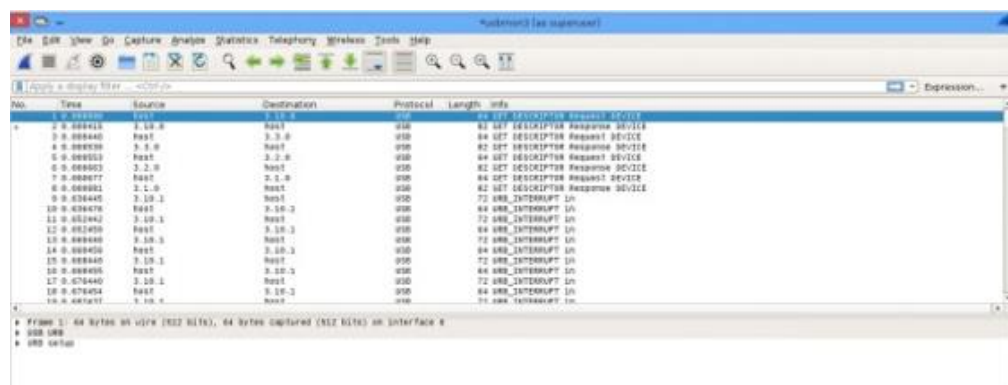
```
modprobe usbmon
```

捕获

打开 wireshark , 你会看到 usbmonX 其中 X 代表数字。下图是我们本次 的结果 (我使用的是 root) :



如果接口处于活跃状态或者有数据流经过的时候 , wireshark 的界面就会把它以波形图的方式显示出来。那么 , 我们该选那个呢 ? 没有错 , 就是我刚刚让大家记下来的 , 这个 X 的数字就是对应这 USB Bus。在本文中是 usbmon3。 打开他就可以观察数据包了。



最后

那么我们获取到了这些有什么用呢？通过这些，我们可以了解到 usb 设备与主机之间的通信过程和工作原理，也许我们就可以把这些知识用到逆向工程中，得到一些东西。