Linux下USB抓包及数据解析

1.配置内核使能 usbmon

修改内核配置文件.config，将usbmon模块编译进内核

```
CONFIG_USB_MON=y
```

2.安装 tcpdump 抓包工具

3.查看可抓取接口是否有usbmon

Linux shell界面输入下述指令：

```
tcpdump -D
```

显示如下usbmon1 / usbmon2 / usbmon3则已打开usbmon模块

```
1.eth0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.usbmon1 (USB bus number 1)
5.usbmon2 (USB bus number 2)
6.usbmon3 (USB bus number 3)
```

4. 查看usb挂载总线

Linux shell界面输入下述指令：

```
lsusb
```

```
Bus 003 Device 002: ID 2109:0713
Bus 001 Device 001: ID 1d6b:0002
Bus 002 Device 001: ID 1d6b:0002
Bus 003 Device 001: ID 1d6b:0003
```

获取usb设备总线号及设备号，如目标usb设备为Bus 003 Device 002: ID 2109:0713，总线号为3，使用usbmon3接口抓取，设备号为2。

5.抓取特定接口的usb包

根据步骤2获取的目标usb总线号选择对应usbmon接口，Linux shell界面输入下述指令：（root权限下运行）

```
tcpdump -i usbmon3 -w ~/usb.pcap
```

开始记录usb包传输信息，log路径位置 `/root/usb.pcap` 。

6.查看usb抓包信息

若在无图形界面开发板上抓取usb包信息，则需将usb.pcap文件拷贝至具有图形界面Linux虚拟机下。

安装wireshark应用程序：

```
sudo apt-get install wireshark-qt
```

查看usb抓包信息：

```
wireshark ~/usb.pcap
```

在过滤框中输入要分析的设备地址：

```
usb.device_address == 设备号
```