西湖论剑2020writeup

原创

FEARHF 于 2020-10-14 22:14:53 发布 922 收藏 2

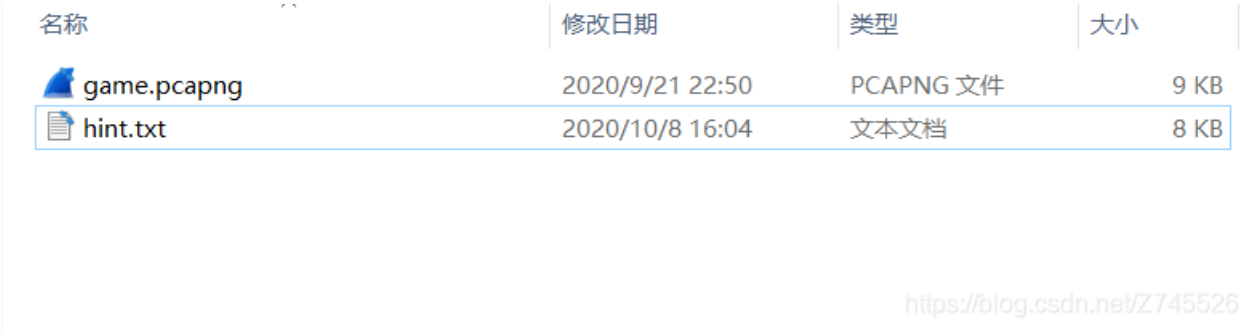
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/Z745526156/article/details/109038320
版权

2020西湖论剑 writeup（复现）

MISC

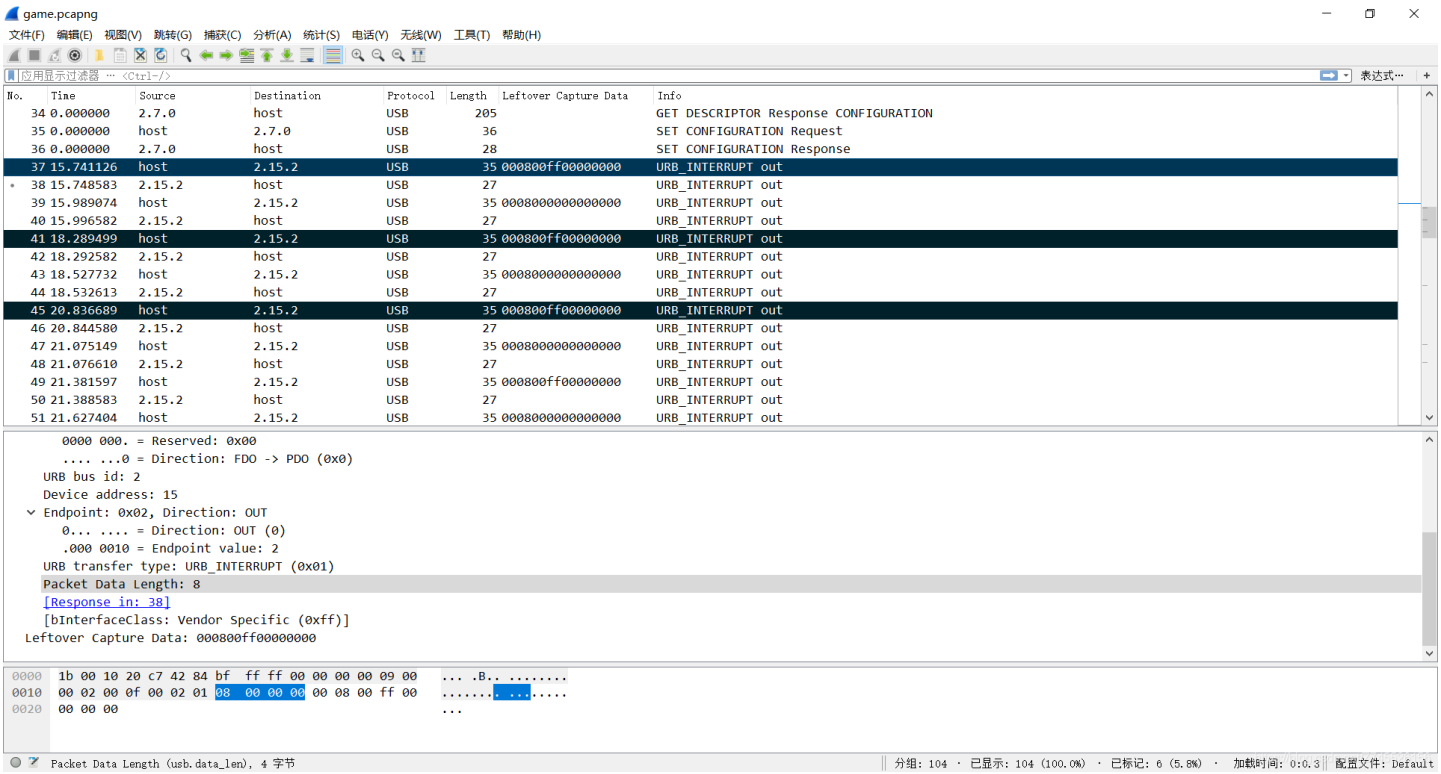
Yusa_yyds

下载附件得到



https://blog.csdn.net/Z745526156

观察game.pacp，发现本题为USB浏览分析题



观察有发送数据的字段（Leftover Capture Data字段），即IP==2.15.2与HOST之间通信的报文

```
USB URB
    [Source: host]
    [Destination: 2.15.2]
    USBPcap pseudoheader length: 27
    IRP ID: 0xffffbf8442c72010
    IRP USBD STATUS: USBD STATUS SUCCESS (0x00000000)
```

```
  URB Function: URB_FUNCTION_BULK_OR_INTERRUPT_TRANSFER (0x0009)
> IRP information: 0x00, Direction: FDO -> PDO
  URB bus id: 2
  Device address: 15
> Endpoint: 0x02, Direction: OUT
  URB transfer type: URB_INTERRUPT (0x01)
  Packet Data Length: 8
  [Response in: 40]
  [bInterfaceClass: Vendor Specific (0xff)]
Leftover Capture Data: 0008000000000000
```

https://blog.csdn.net/Z745526156

和网上的资料相对比

性能	应用	特性
低速(1.5Mbps): ✓交互式设备 ✓10-100kbps	➢键盘，鼠标 ➢手写笔 ➢游戏手柄 ➢虚拟设备 ➢外设	•极低的成本 •易于使用 •热插拔 •同时使用多个外设
全速(12Mbps): ✓电话，音频类 ✓压缩的视频类 ✓500kbps – 10Mbps	➢话音 ➢宽带 ➢音频 ➢麦克风	•较低的成本 •易于使用 •热插拔 •同时使用多个外设 •可保证的带宽 •可保证的延迟
高速(480Mbps): ✓视频，大容量存储 ✓25 – 400Mbps	➢视频 ➢大容量存储 ➢图像 ➢宽带	•低成本 •易于使用 •热插拔 •同时使用多个设备 •可保证的带宽 •可保证的延迟 •高带宽

这里我们只关注USB流量中的键盘流量和鼠标流量。

键盘数据包的数据长度为8个字节，击键信息集中在第3个字节，每次key stroke都会产生一个keyboard event usb packet。

鼠标数据包的数据长度为4个字节，第一个字节代表按键，当取0x00时，代表没有按键、为0x01时，代表按左键，为0x02时，代表当前按键为右键。第二个字节可以看成是一个signed byte类型，其最高位为符号位，当其值为正时，代表鼠标水平右移多少像素，为负时，代表水平左移多少像素。第三个字节与第二字节类似，代表垂直上下移动的偏移。

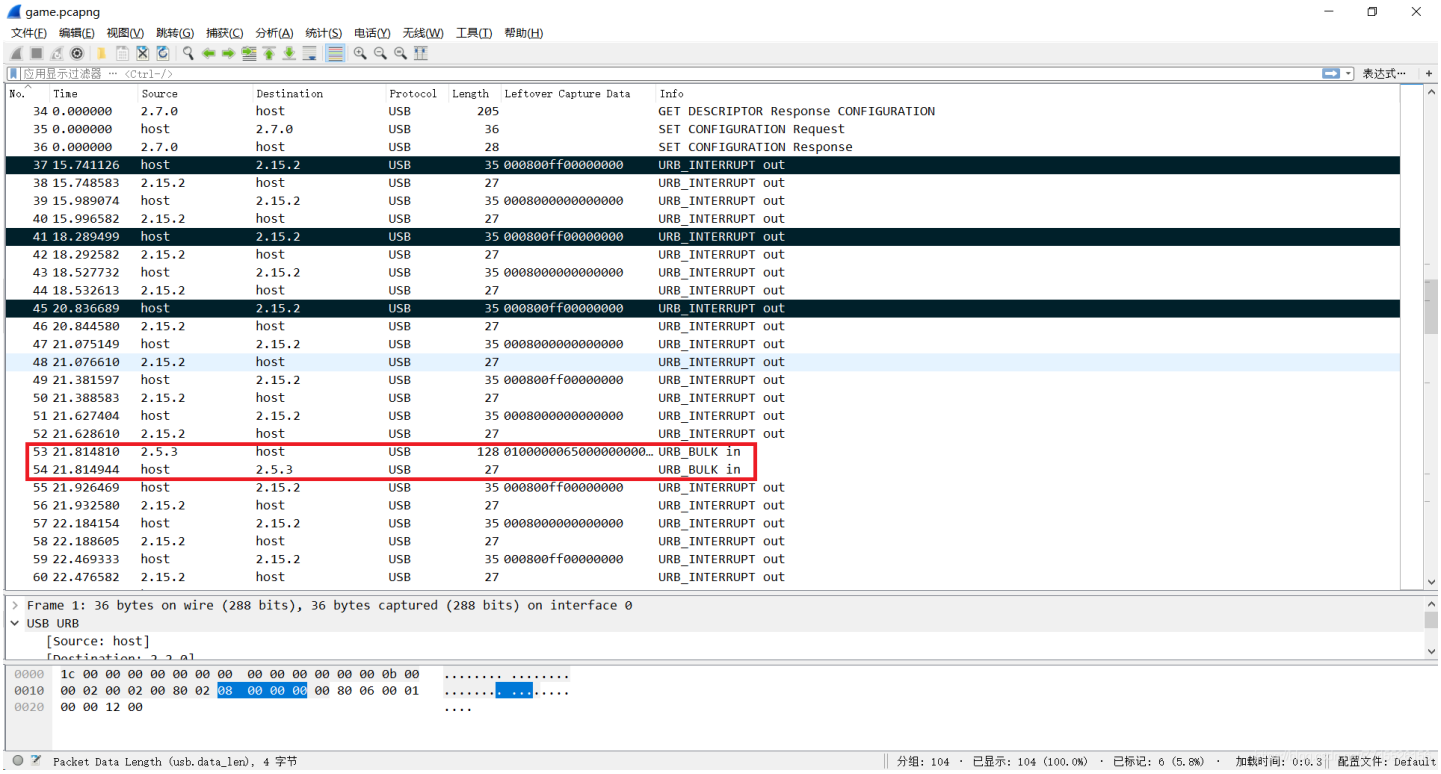
https://blog.csdn.net/Z745526156

分析该USB流量分析为键盘或者手柄

观察多个报文的时间间隔

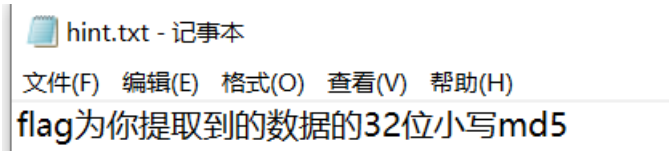
```
[Time delta from previous captured frame: 15.741126000 seconds]
[Time delta from previous displayed frame: 15.741126000 seconds]
[Time delta from previous captured frame: 0.240491000 seconds]
[Time delta from previous displayed frame: 0.240491000 seconds]
```

有一些报文时间间隔明显大于其他的时间间隔



观察除去红框中URB_BULK in其他数据包，发现以一个大时间间隔以及中间的四个包为一组（根据官方wp得到该USB流量分析为xbox手柄，时间间隔大的为震动，且一个震动会产生四个包），就会得到114514

再根据hint.txt的要求对其进行32位MD5



得到flag=c4d038b4bed09fdb1471ef51ec3a32cd