


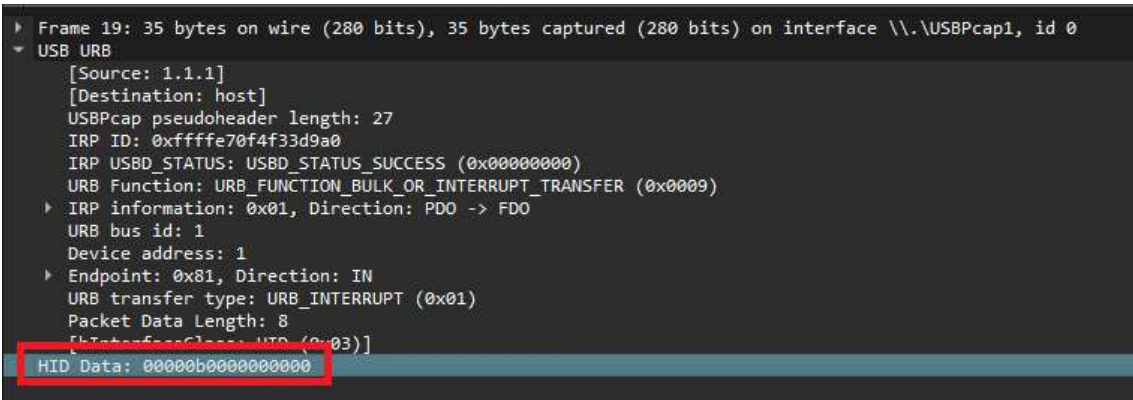


KEYBOARD HACKERS

Description:  
My hacker friend gave me this file saying that he hacked my keyboard. I have no idea what he means. Can you make sense of this file?

This packet capture (PCAP) shows the communication between a USB Human Interface Device (HID) and the host system. The captured data includes the exchange of HID reports, which are the primary method for transmitting input data such as keystrokes or mouse movements between the device and the computer. Example the image shown below.



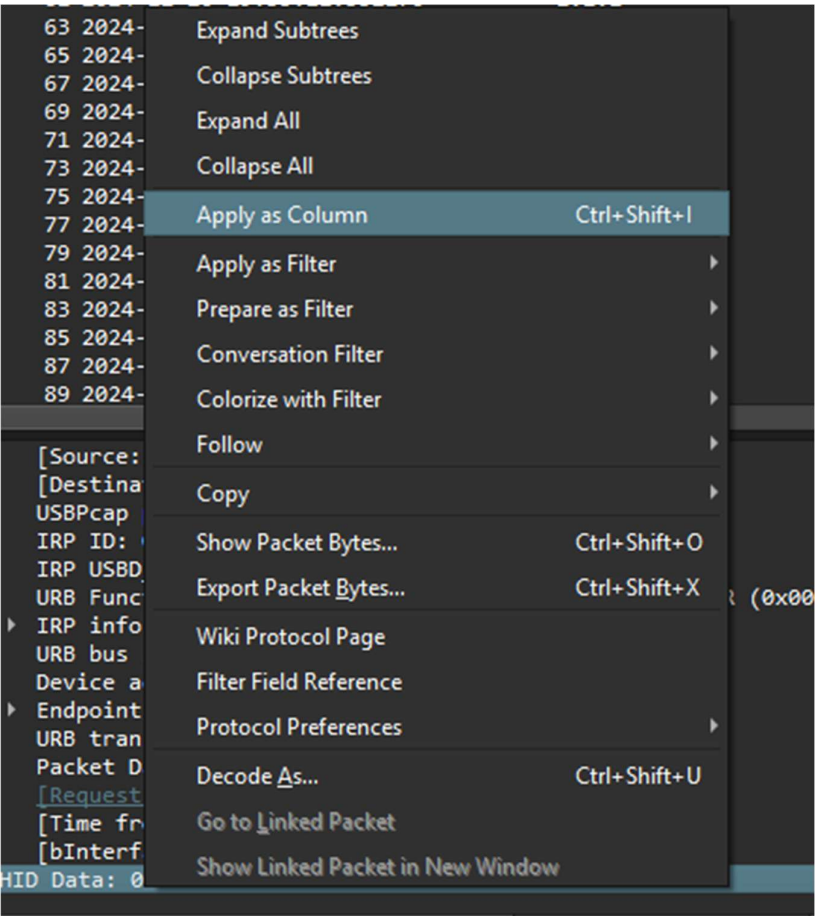


usb.src=="1.1.1"

HackersKeyboard.pcap			
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help			
usb.src=="1.1.1"			
No.	Time	Source	Destination
43	2024-12-20 19:35:10.648183	1.1.1	host
45	2024-12-20 19:35:10.728178	1.1.1	host
47	2024-12-20 19:35:10.992176	1.1.1	host
49	2024-12-20 19:35:11.080185	1.1.1	host
51	2024-12-20 19:35:11.160175	1.1.1	host
53	2024-12-20 19:35:11.240174	1.1.1	host
55	2024-12-20 19:35:11.344175	1.1.1	host
57	2024-12-20 19:35:11.432168	1.1.1	host



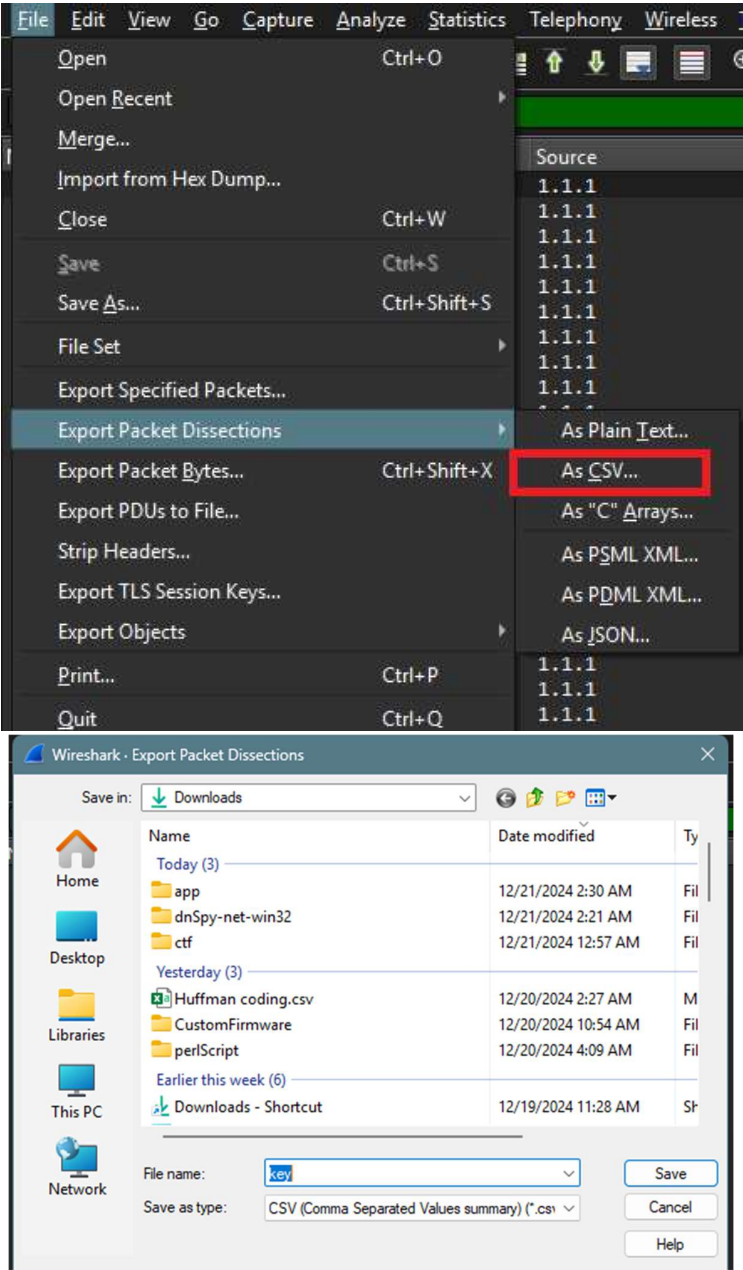
HID devices communicate by sending packets that contain data in specific report formats. These packets are transmitted using periodic transfer types and are typically acknowledged by the host system. Hence we can put it in column to see the HID Data



Now we can see the HID Data on the column.

usb.src==1.1.1							
Time	Source	Destination	Protocol	Length	HID Data	Info	
19 2024-12-20 19:35:07.672186	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
21 2024-12-20 19:35:07.776186	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
23 2024-12-20 19:35:08.024185	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
25 2024-12-20 19:35:08.128185	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
27 2024-12-20 19:35:08.384177	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
29 2024-12-20 19:35:08.472183	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
31 2024-12-20 19:35:08.528194	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
33 2024-12-20 19:35:08.616183	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
35 2024-12-20 19:35:08.712173	1.1.1	host	USB	35	0000120000000000	URB_INTERRUPT	in
37 2024-12-20 19:35:08.808337	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
39 2024-12-20 19:35:09.800177	1.1.1	host	USB	35	00002C0000000000	URB_INTERRUPT	in
41 2024-12-20 19:35:09.896175	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
43 2024-12-20 19:35:10.648183	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
45 2024-12-20 19:35:10.728178	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
47 2024-12-20 19:35:10.992176	1.1.1	host	USB	35	0000120000000000	URB_INTERRUPT	in
49 2024-12-20 19:35:11.080185	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
51 2024-12-20 19:35:11.160175	1.1.1	host	USB	35	0000130000000000	URB_INTERRUPT	in
53 2024-12-20 19:35:11.240174	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
55 2024-12-20 19:35:11.344175	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
57 2024-12-20 19:35:11.432168	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
59 2024-12-20 19:35:11.472171	1.1.1	host	USB	35	00002C0000000000	URB_INTERRUPT	in
61 2024-12-20 19:35:11.552170	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
63 2024-12-20 19:35:11.728173	1.1.1	host	USB	35	00001C0000000000	URB_INTERRUPT	in
65 2024-12-20 19:35:11.816171	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
67 2024-12-20 19:35:12.048172	1.1.1	host	USB	35	0000120000000000	URB_INTERRUPT	in
69 2024-12-20 19:35:12.152168	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
71 2024-12-20 19:35:12.280168	1.1.1	host	USB	35	0000180000000000	URB_INTERRUPT	in
73 2024-12-20 19:35:12.384180	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
75 2024-12-20 19:35:12.504171	1.1.1	host	USB	35	00002C0000000000	URB_INTERRUPT	in
77 2024-12-20 19:35:12.584173	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
79 2024-12-20 19:35:12.752169	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
81 2024-12-20 19:35:12.896167	1.1.1	host	USB	35	0000000000000000	URB_INTERRUPT	in
83 2024-12-20 19:35:13.192167	1.1.1	host	USB	35	00002C0000000000	URB_INTERRUPT	in

Save as CSV



Name to anything you like example ‘key’



E	F	G	H	I
ocol	Length	HID Data	Info	
	35	00000b0000000000	URB_INTERRUPT in	
	35	0000000000000000	URB_INTERRUPT in	
	35	0000080000000000	URB_INTERRUPT in	
	35	0000000000000000	URB_INTERRUPT in	
	35	00000f0000000000	URB_INTERRUPT in	
	35	0000000000000000	URB_INTERRUPT in	
	35	00000f0000000000	URB_INTERRUPT in	
	35	0000000000000000	URB_INTERRUPT in	
	35	0000120000000000	URB_INTERRUPT in	
	35	0000000000000000	URB_INTERRUPT in	
	35	00002c0000000000	URB_INTERRUPT in	
	35	0000000000000000	URB_INTERRUPT in	
	35	00000b0000000000	URB_INTERRUPT in	
	35	0000000000000000	URB_INTERRUPT in	
	35	0000120000000000	URB_INTERRUPT in	

Copy the HID Data only and save it in `.txt`

For the script. I'm using the script getting from this: [Decoding Mixed Case USB Keystrokes from PCAP](#)

```
(osiris@ALICE) - [~/Downloads/CTF/STOUTCTF/Hacker_Keyboard]
$ cat hidcap.txt | head
00000b0000000000
0000000000000000
0000080000000000
0000000000000000
00000f0000000000
0000000000000000
00000f0000000000
0000000000000000
0000000000000000
0000120000000000
0000000000000000

(osiris@ALICE) - [~/Downloads/CTF/STOUTCTF/Hacker_Keyboard]
$ python solver.py hidcap.txt
hello hope you can get this flag:) stoutctf{by3yfbitp3vs1ecx6ery}good luck
(osiris@ALICE) - [~/Downloads/CTF/STOUTCTF/Hacker_Keyboard]
$
```

<b>Flag</b>	STOUTCTF{BY3YFBITP3VS1ECX6ERY}
-------------	--------------------------------