CHALLENGE NAME : 1NJ3CT0R
DEV : PRATIK PATIL
CATEGORY : DIGITAL FORENSICS
LEVEL : HARD

Challenge Description :

You Are Working As Digital Forensics Expert At Infosys India And Someone Reported That A PC Might Have Been Infected. Tech Team Already Collected All The Evidences From Workstation And Found That Someone Injected Malicious Code.It Is Your Job To Find , What Is Injected Into That PC.NOTE:Use Underscore(_) After Every Word.

Solution :

1)As You Go Through Evidence File You Will Get It ,There Are DESCRIPTOR COMMUNICATIONS And USB INTERRUPTS.
2)See The Descriptor Communication To Know The Device Used To Inject Malicious Code.
3)Then In USB INTERRUPTS (0x01) You Will Get It That Keystrokes Are Injected.
4)There Are Tons Of Ways To Extract Keystroke From Evidence File, But You Have To Analyse The File Carefully.Then Only You Will Get Pattern To Extract Keystrokes.
5)Use This Command To Extract Keystroke : **tshark -r ./usbforensics.pcapng -Y 'usbhid.data.array' -T fields -e usbhid.data.array | sed -e 's/^/0x/' > keystrokes.txt**
6)It Will Extract Keystrokes And Save It To "Keystrokes.txt"
7)Now Create Dictionary Of Hex Values To Convert It Into Characters.
8)Create Code Of Your Favourite Language It will Convert Hex Values Corresponding To Dictionary And Finally Print Out The Alphabets[FLAG].
9)**Flag :VishwaCTF{n0w_y0u_423_d0n3_w17h_u58_f023n51c5}**

References :
1)https://www.youtube.com/watch?v=EnOgRyio_9Q
2)https://www.youtube.com/watch?v=0HXL4RGmExo
3)https://www.usb.org/sites/default/files/documents/hut1_12v2.pdf (Page-53)

These Are The Extracted Keys :

1.

```
0x00
0x09
0x00
0x0f
0x00
0x04
0x00
0x0a
0x00
0x33
0x00
0x2f
0x00
0x11
0x00
0x27
0x00
0x1a
0x00
0x2d
0x00
0x1c
0x00
0x27
0x00
0x18
0x00
0x2d
0x00
0x21
0x00
0x1f
0x00
0x20
0x00
0x2d
0x00
0x07
0x00
0x27
0x00
0x11
0x00
0x20
0x00
0x2d
```

2.

```
0x00
0x1a
0x00
0x1e
0x00
0x24
0x00
0x0b
0x00
0x2d
0x00
0x18
0x00
0x22
0x00
0x25
0x00
0x2d
0x00
0x09
0x00
0x27
0x00
0x1f
0x00
0x20
0x00
0x11
0x00
0x22
0x00
0x1e
0x00
0x06
0x00
0x22
0x00
0x30
0x00
```

Here Is The Simple Code Used By Me :

```
#Keystroke Dictionary
KeystrokeDictionary = {
"0x00" :"","0x04" :"a","0x05" :"b","0x06" :"c","0x07" :"d","0x08":"e","0x09" :"f",
"0x0a" :"g","0x0b" :"h","0x0c" :"i","0x0d" :"j","0x0e":"k","0x0f" :"l",
"0x10" :"m","0x11" :"n","0x12" :"o","0x13" :"p","0x14":"q","0x15" :"r","0x16" :"
s","0x17" :"t","0x18" :"u","0x19" :"v","0x1a":"w","0x1b" :"x","0x1c" :"y","0x1d" :
"z","0x1e" :"1","0x1f" :"2","0x20":"3","0x21" :"4","0x22" :"5","0x23" :"6","0x24"
 :"7","0x25"  :"8","0x26":"9","0x27":"0","0x28":"Enter","0x29":"Escape","0x2a":"
Backspace","0x2b" :"\t","0x2c" :"","0x2d" :"_","0x2e" :"=","0x2f" :"{","0x30":"}",
"0x32":"#","0x33"  :":","0x34":"\'","0x36":",","0x37":".","0x38":"/","0x39":"Capsl
ock","0x4f":"RightArrow","0x50":"LeftArrow","0x51"  :"DownArrow","0x52":"Up
Arrow",
}

flag = []
keystroke= open("keystrokes.txt","r") #Enter keystroke-file
for x in keystroke:
original = x.replace("\n","")
flag.append(KeystrokeDictionary[original])
print("".join(flag))
```