VishwaCTF

CHALLENGE NAME : [WIRED SECRETS]

DEV : [ADITYA JASORIYA, PRANAV BHOSALE , AMEY GULHANE]

CATEGORY : [DIGITAL FORENSCIS]

LEVEL : [MEDIUM]

2024

QUESTION:

You are an intern at the Cyber Security Department of India and you have been assigned your first case. The Department has finally caught a notorious Hacker who communicates online in a Secretive manner. It is suspected that this file might contain clues to unlock critical information. Your task is to analyse the file and decipher any hidden messages or patterns to progress further in the investigation

Flag Format: VishwaCTF{}

Writeup:

1) Upon opening the Evidence File you will see a number of packets that are captured by some USB device, there are DESCRIPTOR COMMUNICATIONS And USB INTERRUPTS.

2) See the Descriptor Communication To Know The Device Used To Inject Malicious Code.

3) URB transfer type: URB_CONTROL (0x02) this indicated that the device which is recorded is a USB Mouse.

4) The actual information transfer packets are of Length 31 and they have a Leftover Data Called as HID DATA which is displayed in Wireshark.

5) So to Filter the actual Data out of the file you need to run this filter in Wireshark

”frame.len == 31 && usbhid.data[:1] == 01”

the **frame.len** in filter is for the packet length and the **usbhid.data** is for when the mouse click is held down.

6) After the filter is applied to get the data into format tshark is used, the prompt is

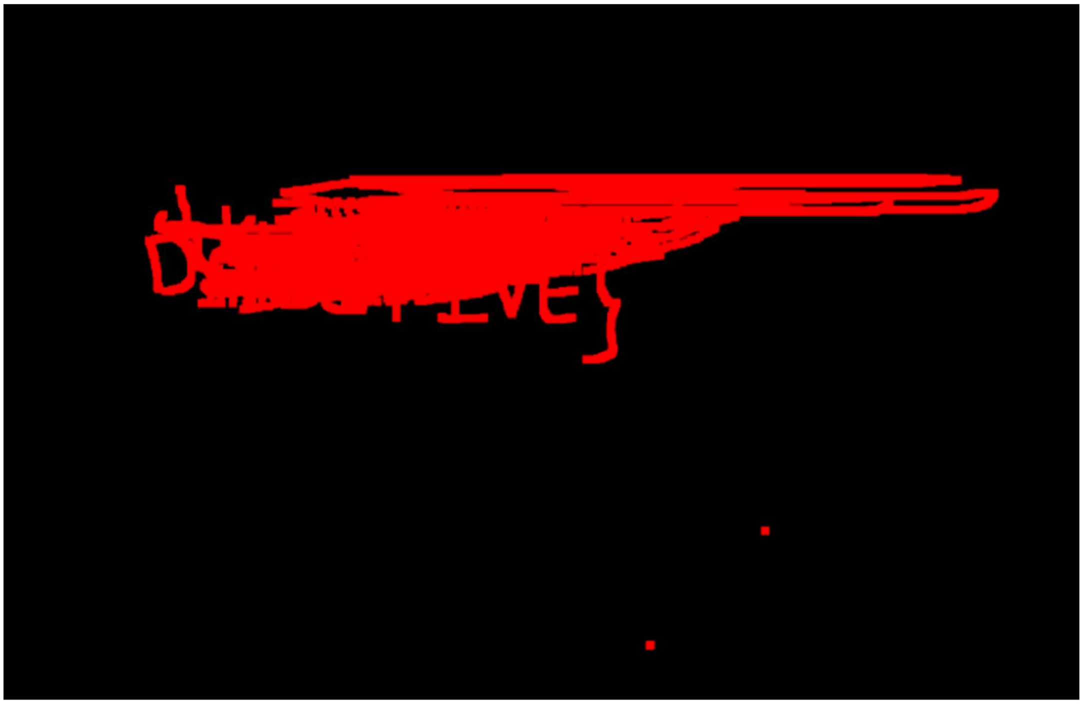
“tshark -r "draw" -T fields -e usbhid.data -Y usbhid.data > mouse.txt”

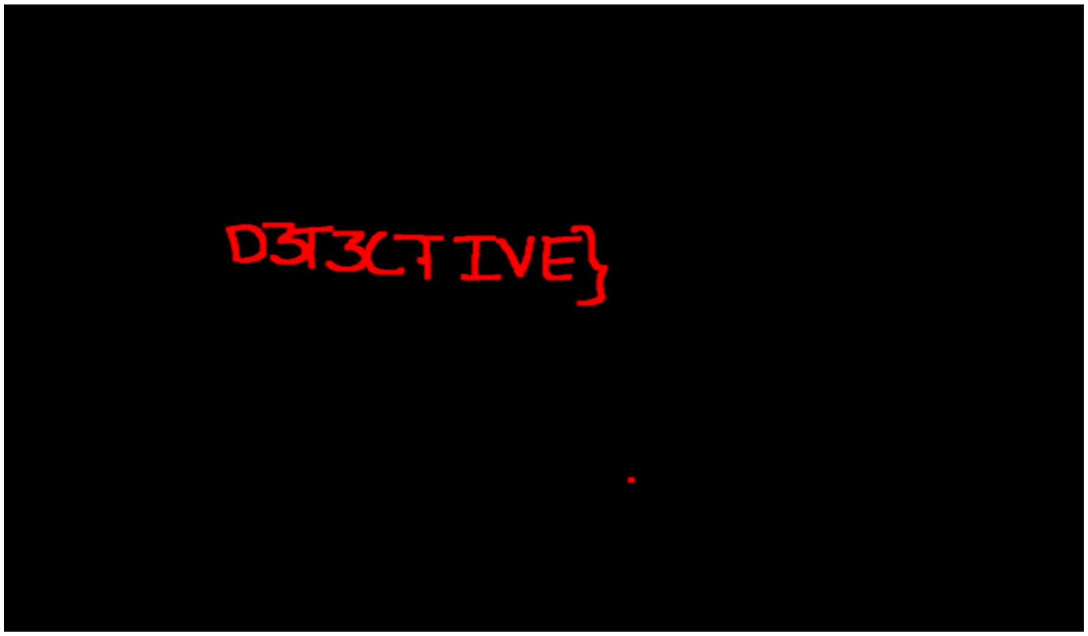
7) This will extract all the mouse movement into a txt file named mouse.txt

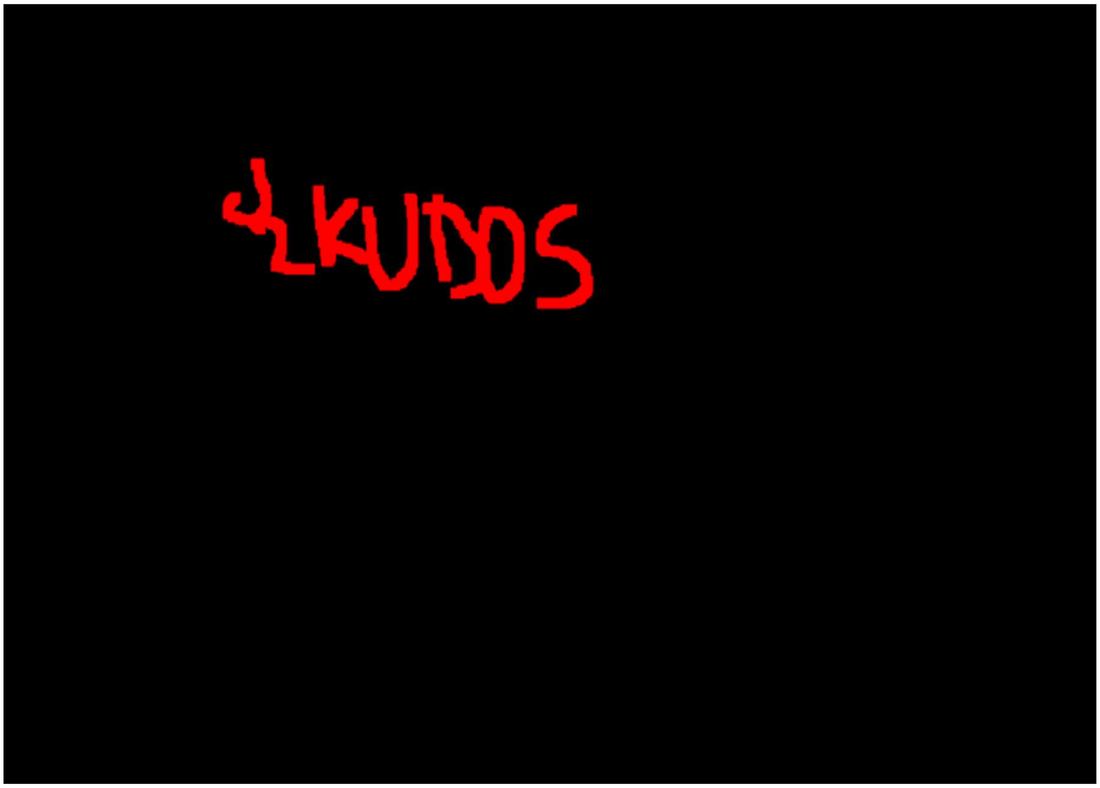
8) Now that you’ve extracted the movement it’s time to plot it you can plot the extracted data easily using python,the code is given below

```
#!/usr/bin/env python

from PIL import Image
import ctypes

def draw_line(image, x, y, color, line_width=1):
    for i in range(-line_width, (line_width+1)):
        for j in range(-line_width, (line_width+1)):
            image.putpixel((x + i, y + j), color)

width = 3920
height = 3080
img = Image.new("RGB", (width, height))

red = (255, 0, 0) # Skipping Right Mouse Btn, its not needed at all
green = (0, 255, 0)
blue = (0, 0, 255)
default = (0, 0, 0)

colormap = {
    0: green,
    1: red,
    2: blue
}
x = int(width/2)
y = int(height/2)
sum1 = 0
sum2 = 0
count = 0
with open('mouse3.txt') as f:
    for line in f:
        b0 = int(line[0: 2], 16)
        b1 = int(line[2: 4], 16)
        b2 = int(line[4: 6], 16)
        b3 = int(line[6: 8], 16)

        # byte0: 0==LBM, 1=RBM, 2=MBM
        color = colormap.get(b0, default)

        # byte1: X displacement
        x_dis  = ctypes.c_int8(b1).value

        # byte2: Y displacement
        y_dis = ctypes.c_int8(b2).value

        x = x + x_dis
        y = y + y_dis
        sum1 = sum1 + x_dis
        sum2 = sum2 + y_dis
        if(b0 == 1):
        print(x, y)
        count = count+1
        #print "line = ", line, "bytes =", bytes, x, y

        if(b0 == 1 and (count > 6530)):
```

```
    # 5870 to 6530 --> {KUD0S and 6530 to end --> D3T3CTIVE}
    draw_line(img, x, y, color, line_width=5)
print("count", count)
img.save("image.png")
```






{KUDOS

{KUDOS
PIVE}