VishwaCTF

CHALLENGE NAME: [Data Trail]

DEV : [Pranav Bhosale]

CATEGORY: [Digital Forensics]

LEVEL: [Medium]

Challenge Description:

We have intercepted a modern military group while they were communicating their strategies. Inspired by the encryption methods of a famous Roman general who once declared ,"Veni","Vidi","Vici", they're using encrypted methods to protect their sensitive information. Your mission is to analyze the provided file, uncover the hidden message, and figure out what they are planning.

Solution:

Step 1)

We need to filter out the packets that are carrying data so we will apply a custom filter that looks at incoming packages with HID data present.

```
frame.len==35 and !(usb.capdata==00:00:00:00:00:00:00:00) and
!(usbhid.data == 00:00:00:00:00:00:00:00)
```

After applying the is filter we will save these packets into a new file called filtered.pcapng.

Step 2)

We then need to get the 2 important parts of the packets ie usb.capdata & usb.data_len==8 where we can anaylse the keystrokes by extracting them into a .txt file which we will later feed into a Python script to parse the data. We will use Tshark to extract data from our filtered.pcapng file.

```
tshark -r ./filtered.pcapng -Y 'usb.capdata && usb.data_len == 8' -T
fields -e usb.capdata | sed 's/../:&/g2'>filtered
```

Step 3)

A popular tool used to analyse keystrokes is https://github.com/TeamRocketIst/ctf-usb-keyboard-parser

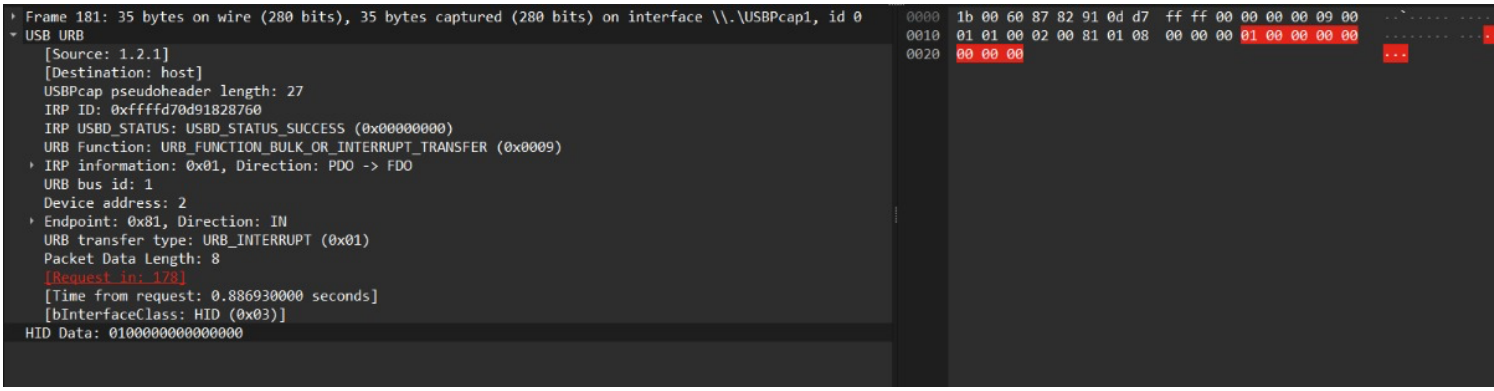
We used this tool to extract the following string:

```
BoznwfHAL{0v3y4a10s_I3z3ya_Za0yr}
```

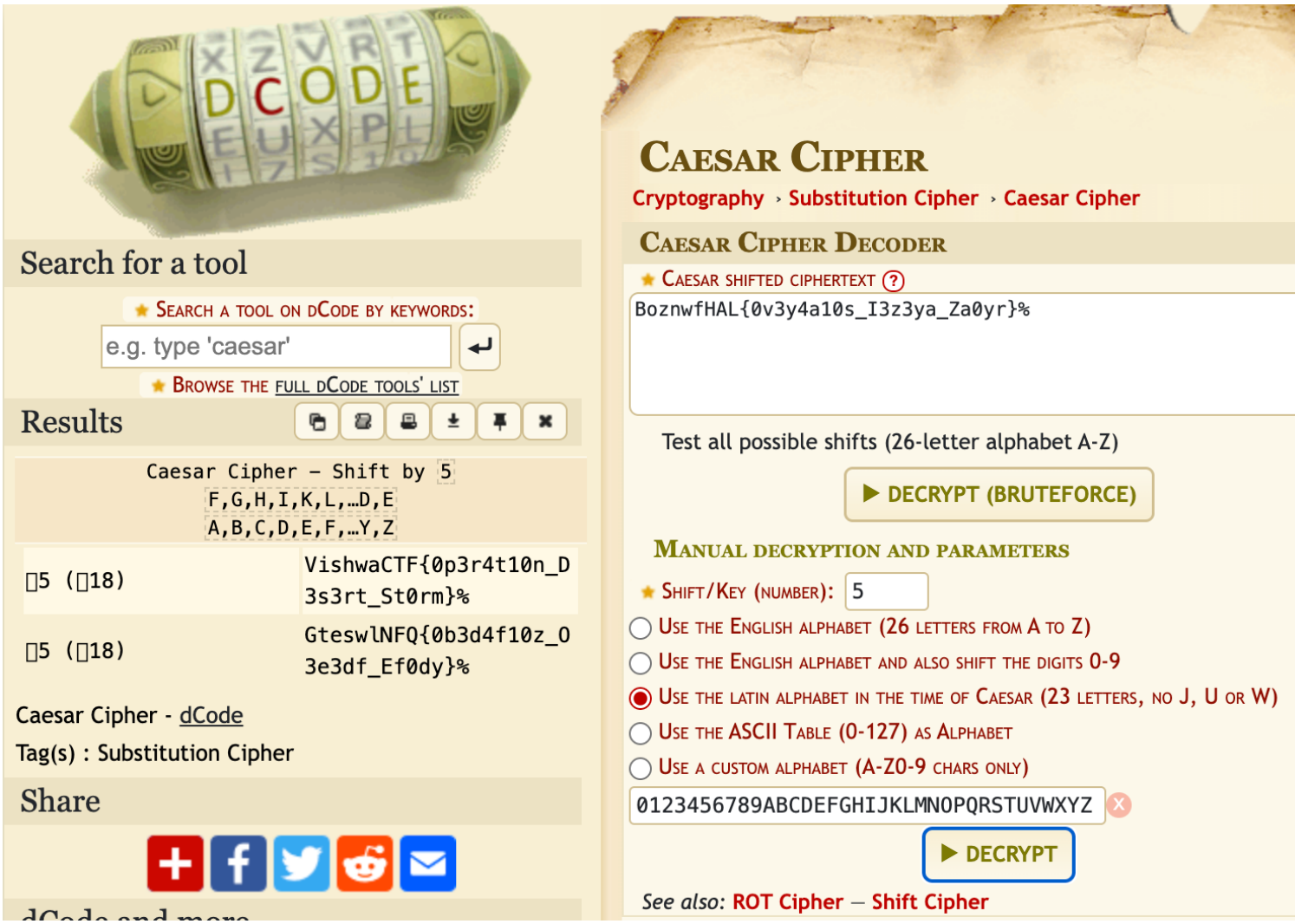
Step 4)

As the description suggests we need to use caser cipher to solve further but the configuration we need to set it as is given within the pcap file itself if we observe carefully at the last few packages we see that they are coming from a USB device with address 2 and which indicates that these indeed are mouse clicks so by counting the Number of Packets where the starting bits are **01** which means that the right mouse button was pressed .

If we count the number of such packets it turns out to be 5 so we need to set our cipher up for 5 shifts.



Here we can See that this is a packet with address as 2 and HID data as 01 which means this is indeed a Mouse Click.



Flag: VishwaCTF{0p3r4t10n_D3s3rt_St0rm}