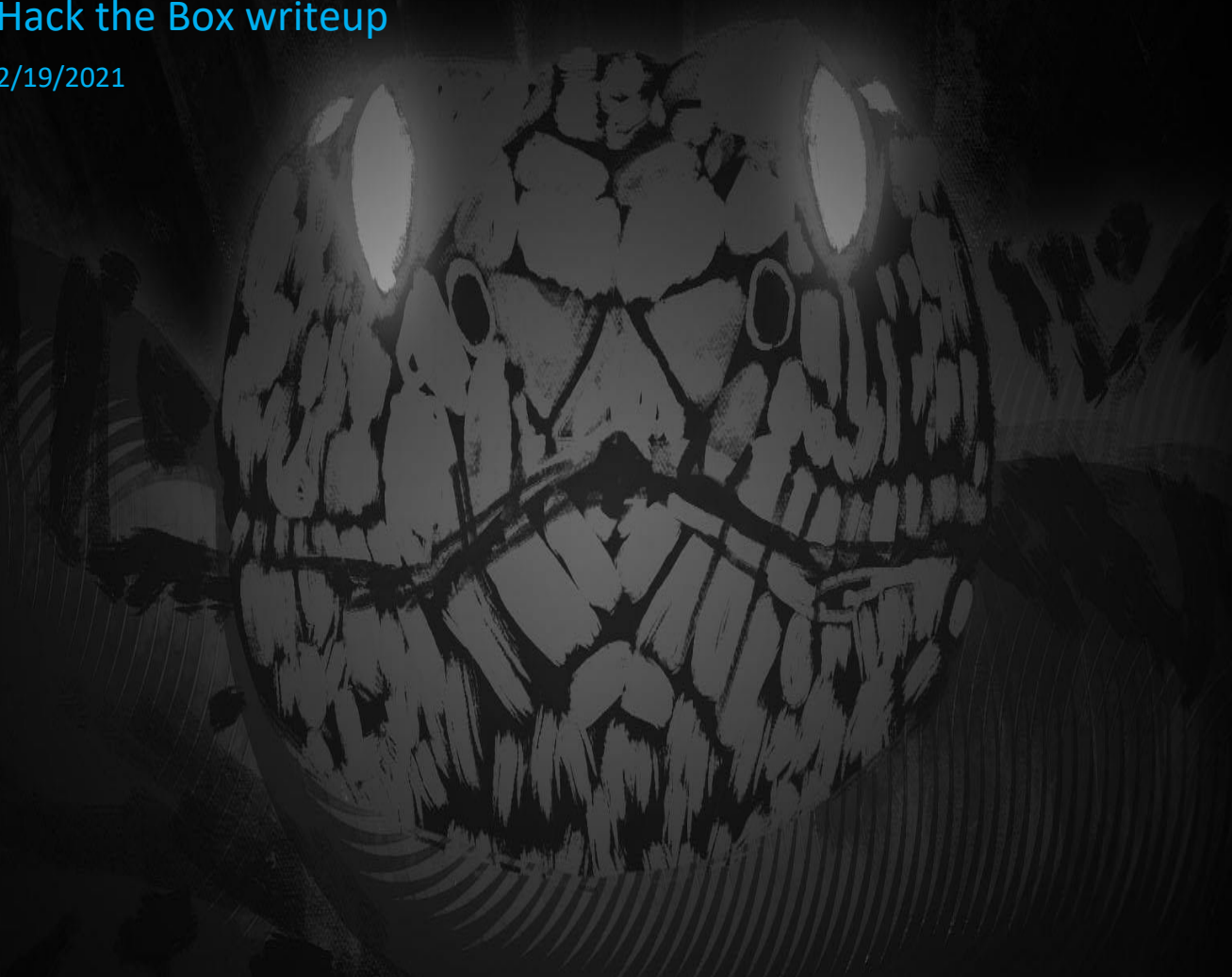


# LOGGER

Hack the Box writeup

2/19/2021



## Contents

Challenge.....	1
Process .....	1
Flag .....	9

# Challenge

🏆 **Logger** [by felamos] [40 solvers] 12 🍌 0 🗨️ Difficulty: 18/11/2020 ^

🔥 **First Blood:** HTB-Bot

A client reported that a PC might have been infected, as it's running slow. We've collected all the evidence from the suspect workstation, and found a suspicious trace of USB traffic. Can you identify the compromised data?

[Download](#) Zip Password: `hackthebox sha256: da9e222a1e6869cf96a9a84e4ef5c662e6819cb1426c60bd1ac0c0017c54464f`

## Process

This PC > WDBLue (D:) > HTB > Solved > logger > logger

Name	Date modified	Type	Size
keystrokes.pcapng	11/1/2020 2:30 PM	Wireshark capture file	27 KB

We start out with a pcap file that contains some USB info on it.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	host	1.16.0	USB	36	GET_DESCRIPTOR Request DEVICE
2	0.000000	1.16.0	host	USB	46	GET_DESCRIPTOR Response DEVICE
3	0.000000	host	1.16.0	USB	36	GET_DESCRIPTOR Request CONFIGURATION
4	0.000000	1.16.0	host	USB	87	GET_DESCRIPTOR Response CONFIGURATION
5	0.000000	host	1.16.0	USB	36	SET_CONFIGURATION Request
6	0.000000	1.16.0	host	USB	28	SET_CONFIGURATION Response

Scrolling through this, we don't see much change in the overview, but if we look at some of the data sending to the host, we see very slight changes in the HID Data Field

281 54.553733 1.13.1 host USB 33 URB\_INTERRUPT in

> Frame 283: 33 bytes on wire (264 bits), 33 bytes captured (264 bits) on interface wireshark\_extcap2640, id 0

> USB URB

HID Data: 0100ff5fff00

```
0000 1b 00 20 ea 9e d9 0e 98 ff ff 00 00 00 09 00 .....
```

285 54.569695 1.13.1 host USB 33 URB\_INTERRUPT in

> Frame 285: 33 bytes on wire (264 bits), 33 bytes captured (264 bits) on interface wireshark\_extcap2640, id 0

> USB URB

HID Data: 01000060ff00

```
0000 1b 00 20 ba e1 d2 0e 98 ff ff 00 00 00 09 00 .....
```

Unfortunately, it does not look like the data given is actually the keystrokes that are being sent, but the hex codes should be accurate.

I looked up a USB HID Code Table and came across this documentation:

[https://www.usb.org/sites/default/files/documents/hut1\\_12v2.pdf](https://www.usb.org/sites/default/files/documents/hut1_12v2.pdf)

Searching for keyboard information lead me to pg 53

9	GENERIC DEVICE CONTROLS PAGE (0X06).....	52
10	<b>KEYBOARD/KEYPAD PAGE (0X07).....</b>	<b>53</b>
11	LED PAGE (0X08).....	61
11.1	KEYBOARD INDICATORS .....	63
11.2	TELEPHONE INDICATORS .....	63

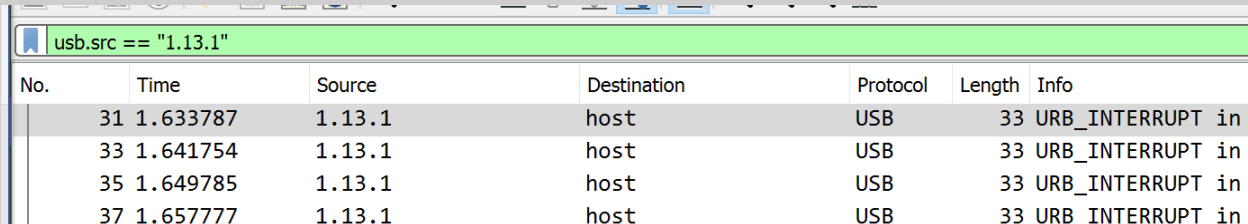
**Table 12: Keyboard/Keypad Page**

Usage ID (Dec)	Usage ID (Hex)	Usage Name	Ref: Typical AT-101 Position	PC- Mac UNI		Boot
				AT	X	
0	00	Reserved (no event indicated) <sup>9</sup>	N/A	√	√	√ 4/101/104
1	01	Keyboard ErrorRollOver <sup>9</sup>	N/A	√	√	√ 4/101/104
2	02	Keyboard POSTFail <sup>9</sup>	N/A	√	√	√ 4/101/104
3	03	Keyboard ErrorUndefined <sup>9</sup>	N/A	√	√	√ 4/101/104
4	04	Keyboard a and A <sup>4</sup>	31	√	√	√ 4/101/104
5	05	Keyboard b and B	50	√	√	√ 4/101/104
6	06	Keyboard c and C <sup>4</sup>	48	√	√	√ 4/101/104
7	07	Keyboard d and D	33	√	√	√ 4/101/104
8	08	Keyboard e and E	19	√	√	√ 4/101/104
9	09	Keyboard f and F	34	√	√	√ 4/101/104
10	0A	Keyboard g and G	35	√	√	√ 4/101/104
11	0B	Keyboard h and H	36	√	√	√ 4/101/104
12	0C	Keyboard i and I	24	√	√	√ 4/101/104
13	0D	Keyboard j and J	37	√	√	√ 4/101/104
14	0E	Keyboard k and K	38	√	√	√ 4/101/104
15	0F	Keyboard l and L	39	√	√	√ 4/101/104
16	10	Keyboard m and M <sup>4</sup>	52	√	√	√ 4/101/104
17	11	Keyboard n and N	51	√	√	√ 4/101/104
18	12	Keyboard o and O <sup>4</sup>	25	√	√	√ 4/101/104
19	13	Keyboard p and P <sup>4</sup>	26	√	√	√ 4/101/104
20	14	Keyboard q and Q <sup>4</sup>	17	√	√	√ 4/101/104

This looks perfect, now I just need to check and see if this data is actually what I think it is.

I filtered down the pcap to only show items from usb.src == "1.13.1"

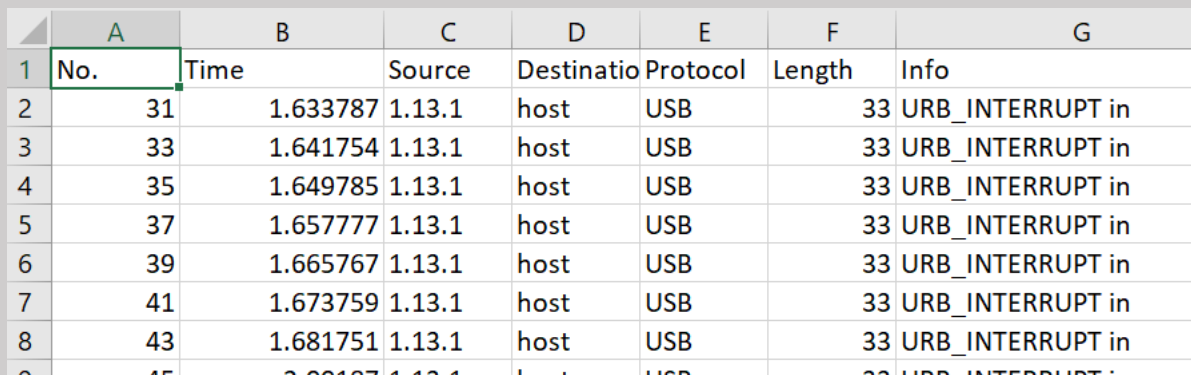
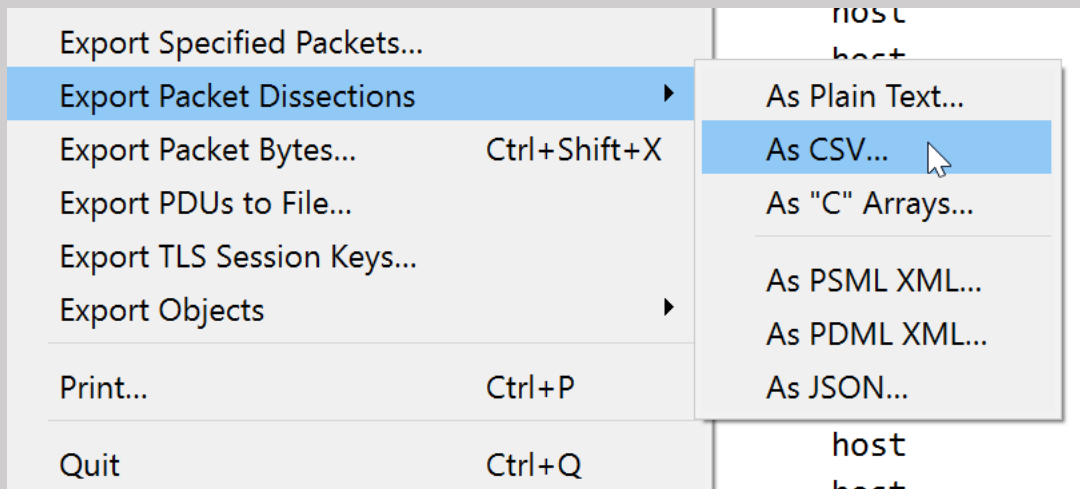
This way I reduce the noise I am getting.



The image shows a Wireshark packet list view with a filter 'usb.src == "1.13.1"'. The table below represents the data shown in the screenshot.

No.	Time	Source	Destination	Protocol	Length	Info
31	1.633787	1.13.1	host	USB	33	URB_INTERRUPT in
33	1.641754	1.13.1	host	USB	33	URB_INTERRUPT in
35	1.649785	1.13.1	host	USB	33	URB_INTERRUPT in
37	1.657777	1.13.1	host	USB	33	URB_INTERRUPT in

I then exported the list to a csv so I could quickly look through the data and parse it out as needed.



The image shows a CSV export of the filtered Wireshark data. The table below represents the data shown in the screenshot.

	A	B	C	D	E	F	G
1	No.	Time	Source	Destination	Protocol	Length	Info
2	31	1.633787	1.13.1	host	USB	33	URB_INTERRUPT in
3	33	1.641754	1.13.1	host	USB	33	URB_INTERRUPT in
4	35	1.649785	1.13.1	host	USB	33	URB_INTERRUPT in
5	37	1.657777	1.13.1	host	USB	33	URB_INTERRUPT in
6	39	1.665767	1.13.1	host	USB	33	URB_INTERRUPT in
7	41	1.673759	1.13.1	host	USB	33	URB_INTERRUPT in
8	43	1.681751	1.13.1	host	USB	33	URB_INTERRUPT in

Unfortunately, this does not have the data I need so I had to add a HID Data Column to wireshark

Wireshark · Preferences

- Appearance
  - Columns
  - Font and Colors
  - Layout
  - Capture
  - Expert
  - Filter Buttons
  - Name Resolution
  - Protocols
  - RSA Keys
  - Statistics
  - Advanced

Displayed	Title	Type	Fields	Field Occurrence
<input checked="" type="checkbox"/>	No.	Number		
<input checked="" type="checkbox"/>	Time	Time (format as specified)		
<input checked="" type="checkbox"/>	Source	Source address		
<input checked="" type="checkbox"/>	Destination	Destination address		
<input checked="" type="checkbox"/>	Protocol	Protocol		
<input checked="" type="checkbox"/>	Length	Packet length (bytes)		
<input checked="" type="checkbox"/>	HID Data	Custom	usbhid.data	0
<input checked="" type="checkbox"/>	Info	Information		

usb.src == "1.13.1"

No.	Time	Source	Destination	Protocol	Length	HID Data	Info
31	1.633787	1.13.1	host	USB	33	010001000000	URB_INTERRUPT in
33	1.641754	1.13.1	host	USB	33	010004000000	URB_INTERRUPT in
35	1.649785	1.13.1	host	USB	33	010006100000	URB_INTERRUPT in
37	1.657777	1.13.1	host	USB	33	010006100000	URB_INTERRUPT in
39	1.665767	1.13.1	host	USB	33	010003100000	URB_INTERRUPT in
41	1.673759	1.13.1	host	USB	33	010001000000	URB_INTERRUPT in

Now I should have what I need, so I exported it again

	A	B	C	D	E	F	G	H
1	No.	Time	Source	Destination	Protocol	Length	HID Data	Info
2	31	1.633787	1.13.1	host	USB	33	10001000000	URB_INTERRUPT in
3	33	1.641754	1.13.1	host	USB	33	10004000000	URB_INTERRUPT in
4	35	1.649785	1.13.1	host	USB	33	10006100000	URB_INTERRUPT in
5	37	1.657777	1.13.1	host	USB	33	10006100000	URB_INTERRUPT in
6	39	1.665767	1.13.1	host	USB	33	10003100000	URB_INTERRUPT in
7	41	1.673759	1.13.1	host	USB	33	10001000000	URB_INTERRUPT in
8	43	1.681751	1.13.1	host	USB	33	10001000000	URB_INTERRUPT in
9	45	2.00187	1.13.1	host	USB	33	10100000000	URB_INTERRUPT in
10	47	2.081778	1.13.1	host	USB	33	10000000000	URB_INTERRUPT in
11	217	54.24974	1.13.1	host	USB	33	0100ff0f0000	URB_INTERRUPT in
12	219	54.25771	1.13.1	host	USB	33	0100f2cfff00	URB_INTERRUPT in
13	221	54.26572	1.13.1	host	USB	33	0100dd7fff00	URB_INTERRUPT in
14	223	54.2737	1.13.1	host	USB	33	0100d14fff00	URB_INTERRUPT in
15	225	54.28172	1.13.1	host	USB	33	0100cc4fff00	URB_INTERRUPT in

Now I need to see what items are changing

0100d06fff00
0100d36fff00
0100d66fff00
0100d86fff00
0100dc8fff00
0100e18fff00
0100e77fff00
0100edafff00

The 5<sup>th</sup>, 6<sup>th</sup>, and 7<sup>th</sup> values seem to be changing, so one of them will hopefully be the data we want.

The 5<sup>th</sup> and 6<sup>th</sup> values don't seem to make a lot of sense so I tried the 6<sup>th</sup> and 7<sup>th</sup> and they didn't seem much better.

I did start at the top though, so it's possible this is a normal startup procedure.

I scrolled down a little bit towards the middle of the list and tried again.

Eventually I confirmed that I needed values 5 and 6. So I set out extracting those values with some regex. I also removed all 0 value entries.

```

1 "No.", "Time", "Source", "Destination", "Protocol", "Length", "HID Data", "Info"
2 "49", "5.977777", "1.16.1", "host", "USB", "35", "0000390000000000", "URB_INTERRUPT in"
3 "55", "8.033800", "1.16.1", "host", "USB", "35", "00000b0000000000", "URB_INTERRUPT in"
4 "59", "9.073763", "1.16.1", "host", "USB", "35", "0000170000000000", "URB_INTERRUPT in"
5 "63", "9.577804", "1.16.1", "host", "USB", "35", "0000050000000000", "URB_INTERRUPT in"
6 "67", "11.233790", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
7 "69", "11.561811", "1.16.1", "host", "USB", "35", "20002f0000000000", "URB_INTERRUPT in"
8 "71", "11.713787", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
9 "75", "13.489786", "1.16.1", "host", "USB", "35", "0000390000000000", "URB_INTERRUPT in"
10 "81", "13.913785", "1.16.1", "host", "USB", "35", "00000c0000000000", "URB_INTERRUPT in"
11 "85", "15.113768", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
12 "87", "15.561759", "1.16.1", "host", "USB", "35", "20002d0000000000", "URB_INTERRUPT in"
13 "89", "15.681893", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
14 "93", "16.865739", "1.16.1", "host", "USB", "35", "0000390000000000", "URB_INTERRUPT in"
15 "99", "20.129815", "1.16.1", "host", "USB", "35", "0000060000000000", "URB_INTERRUPT in"
16 "103", "21.673767", "1.16.1", "host", "USB", "35", "0000210000000000", "URB_INTERRUPT in"
17 "107", "22.657773", "1.16.1", "host", "USB", "35", "0000110000000000", "URB_INTERRUPT in"
18 "111", "23.977765", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
19 "113", "24.265914", "1.16.1", "host", "USB", "35", "20002d0000000000", "URB_INTERRUPT in"
20 "115", "24.457740", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
21 "119", "27.737754", "1.16.1", "host", "USB", "35", "0000220000000000", "URB_INTERRUPT in"
22 "123", "28.225733", "1.16.1", "host", "USB", "35", "0000200000000000", "URB_INTERRUPT in"
23 "127", "28.585776", "1.16.1", "host", "USB", "35", "0000200000000000", "URB_INTERRUPT in"
24 "131", "29.953785", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
25 "133", "30.361755", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
26 "135", "30.561776", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
27 "139", "31.161797", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
28 "145", "32.577771", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
29 "149", "35.097778", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
30 "155", "35.521746", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
31 "159", "39.577758", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
32 "163", "39.937846", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
33 "169", "40.649707", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
34 "173", "41.841734", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
35 "175", "42.217767", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
36 "177", "42.425785", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
37 "181", "44.489735", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
38 "187", "44.945736", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
39 "191", "46.481750", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
40 "195", "48.281744", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
41 "199", "49.345782", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
42 "203", "50.745835", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
43 "209", "51.105742", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
44 "211", "51.433727", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
45 "213", "51.665747", "1.16.1", "host", "USB", "35", "2000000000000000", "URB_INTERRUPT in"
46

```

Replace

Find Replace Find in Files Mark

Find what:

Replace with:

In selection

Backward direction

Match whole word only

Match case

Wrap around

Search Mode

Normal

Extended (\n, \r, \t, \0, \x...)

Regular expression  \_ matches newline

Transparency

On losing focus

Always

Find Next

Replace

Replace All

Replace All in All Opened Documents

Close

Replace All: 32 occurrences were replaced in entire file

```

1 HID Data
2 0000390000000000
3 00000b0000000000
4 0000170000000000
5 0000050000000000
6 2000000000000000
7 20002f0000000000
8 2000000000000000
9 0000390000000000
10 00000c0000000000
11 2000000000000000
12 20002d0000000000
13 2000000000000000
14 0000390000000000
15 0000060000000000
16 0000210000000000
17 0000110000000000
18 2000000000000000
19 20002d0000000000
20 2000000000000000
21 0000220000000000
22 0000200000000000
23 0000200000000000
24 2000000000000000
25 20002d0000000000
26 2000000000000000
27 0000390000000000
28 00001c0000000000
29 0000390000000000

```

```

1 HID Data
2 39
3 0b
4 17
5 05
6 2f
7 39
8 0c
9 2d
10 39
11 06
12 21
13 11
14 2d
15 22
16 20
17 20
18 2d
19 39
20 1c
21 39
22 12
23 18
24 39
25 15
26 2d
27 39
28 0e
29 20
30 1c
31 1f
32 39
33 30
34

```

Once I got my values carved out, I threw them into excel and made a vlookup against the table I had, this way I don't need to look everything up by hand

The document I was using does not allow me to copy text so I grabbed this table

[https://www.toomanyatoms.com/computer/usb\\_keyboard\\_codes.html](https://www.toomanyatoms.com/computer/usb_keyboard_codes.html)

	A	B	C	D	E
1	39	Keyboard Caps Lock11			
2	0b	Keyboard h and H			
3	17	Keyboard t and T			
4	5	Keyboard b and B			



	A	B
1	Usage ID (Hex)	Usage Name
2		0 Reserved (no event indicated)9
3		1 Keyboard ErrorRollOver9
4		2 Keyboard POSTFail9
5		3 Keyboard ErrorUndefined9
6		4 Keyboard a and A4
7		5 Keyboard b and B
8		6 Keyboard c and C4
9		7 Keyboard d and D
10		8 Keyboard e and E

All said and done, I got this

	A	B
1	39	Keyboard Caps Lock11
2	0b	Keyboard h and H
3	17	Keyboard t and T
4	5	Keyboard b and B
5	2f	Keyboard [ and {4
6	39	Keyboard Caps Lock11
7	0c	Keyboard i and I
8	2d	Keyboard - and (underscore)4
9	39	Keyboard Caps Lock11
10	6	Keyboard c and C4
11	21	Keyboard 4 and \$4
12	11	Keyboard n and N
13	2d	Keyboard - and (underscore)4
14	22	Keyboard 5 and %4
15	20	Keyboard 3 and #4
16	20	Keyboard 3 and #4
17	2d	Keyboard - and (underscore)4
18	39	Keyboard Caps Lock11
19	1c	Keyboard y and Y4
20	39	Keyboard Caps Lock11
21	12	Keyboard o and O4
22	18	Keyboard u and U
23	39	Keyboard Caps Lock11
24	15	Keyboard r and R
25	2d	Keyboard - and (underscore)4
26	39	Keyboard Caps Lock11
27	0e	Keyboard k and K
28	20	Keyboard 3 and #4
29	1c	Keyboard y and Y4
30	1f	Keyboard 2 and @4
31	39	Keyboard Caps Lock11
32	30	Keyboard ] and }4
33		

# Flag

HTB{i\_C4N\_533\_yOUr\_K3Y2}