

105 – BlueShark

Team Information

Team Name : ForensicGPT

Team Member : Eungchang Lee, Donghyun HA, Hyunwoo Shin, Jinhyeok Son

Email Address : forensicgpt@googlegroups.com

Instructions

Description Analyze the following evidence to identify the message

Target	Hash (MD5)
evidence.zip	B4345B48C5FCE8205762A856DB98D03C

Questions

- 1) What is the message from evidence1? (40 points)
- 2) What is the message from evidence2? (40 points)
- 3) What is the message from evidence3? (20 points)

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

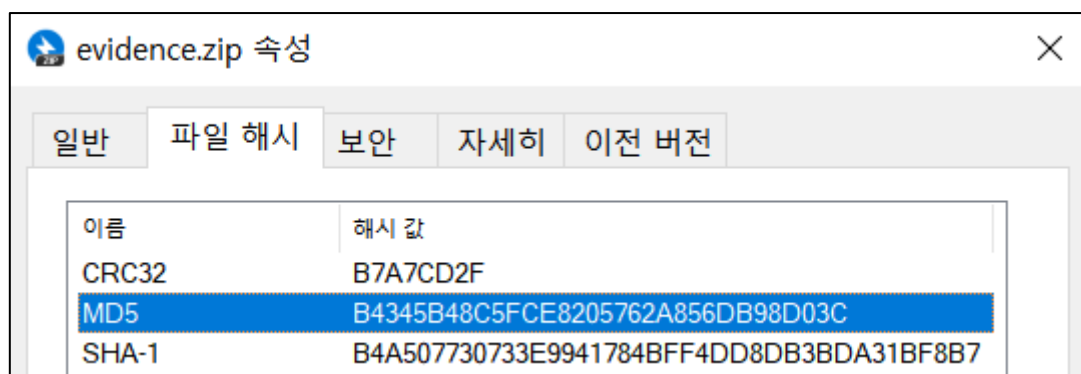
Name:	Wireshark	Publisher:	Wireshark Foundation
Version:	3.6.6		
URL:	https://www.wireshark.org		

Name:	TShark	Publisher:	Wireshark Foundation
Version:	3.2.3		
URL:	https://www.wireshark.org		

Name:	HashTab	Publisher:	Implbits Software
Version:	6.0.0		
URL:	https://implbits.com		

Name:	Visual Studio code	Publisher:	Microsoft
Version:	1.79.2		
URL:	https://code.visualstudio.com/download		

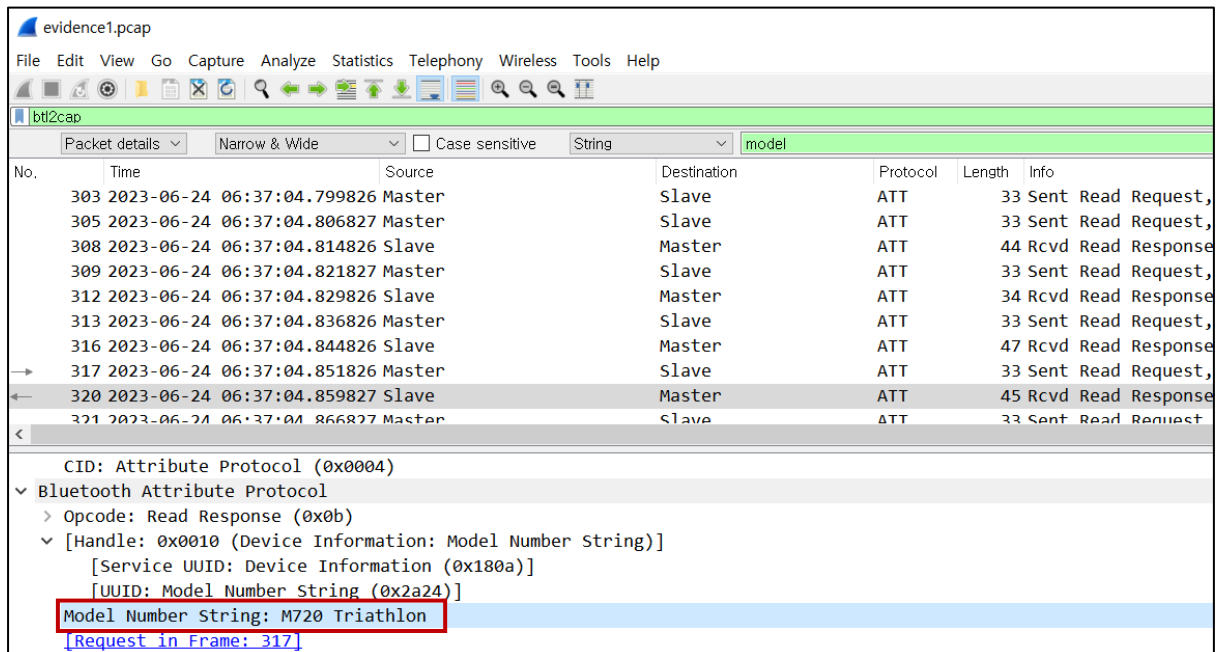
Step-by-step methodology:



[그림 1] evidence.zip 파일 해시 값 확인

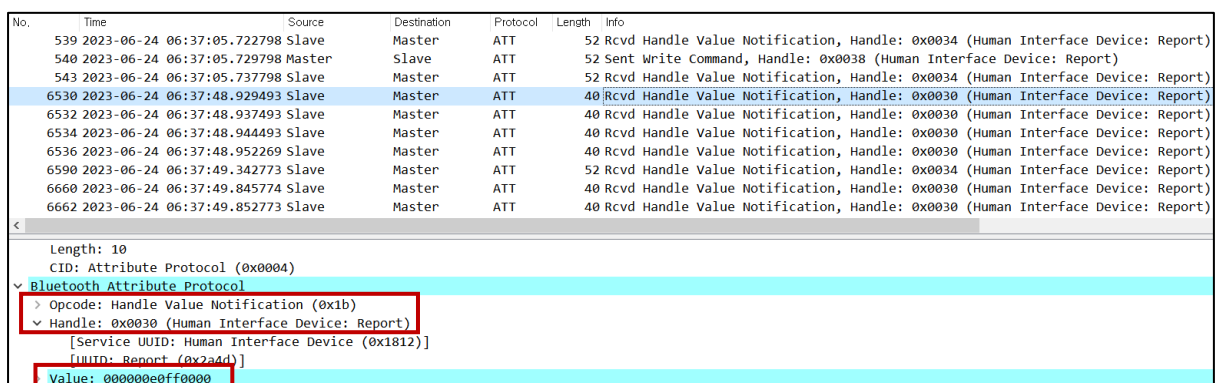
분석에 앞서 파일에 대한 해시 값을 산출하여, md5 해시 값이 일치함을 확인하였습니다.

1) What is the message from evidence1? (40 points)



[그림 2] BLE packet 상 주고받은 메시지와 관련 의심 모델

wireshark 도구를 통해 evidence1.pcap 파일 내 주고받은 패킷 중 Bluetooth low energy 기술을 사용하는 장치에 관해 살펴보았습니다. btl2cap 필터링을 통해 BLE 프로토콜 스택에 존재하는 ATT 프로토콜로 주고받은 패킷 중에서 model 관련 정보를 확인할 수 있었습니다. 이후, M720 Triathlon 모델이 마우스 장치라는 것을 확인하였고, HID(Human Interface Device)로써 Master와 Slave간에 메시지를 주고받았을 것이라고 판단하였습니다.



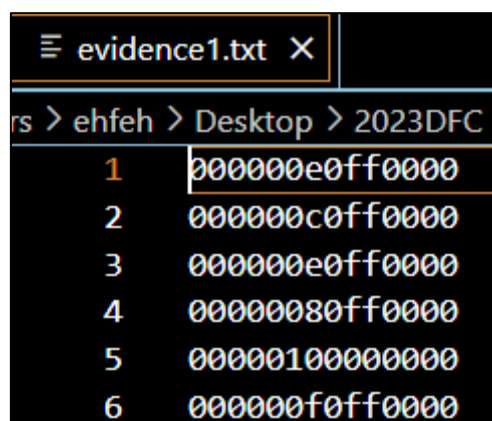
[그림 3] Handle : 0x0030(Human Interface Device)에서 발견되는 Value

그 후, Rcvd Handle Value Notification, Handle : 0x0030(Human Interface Device: Report) 정보를 가진 패킷에서 균등한 7바이트 Value를 가지는 것을 확인하였습니다.

또한, 해당 패킷의 Bluetooth Attribute Protocol 데이터의 opcode 에서는 0x1b값을 가지며, Value에서는 첫번째 바이트, 세번째 바이트, 네번째 바이트에서 값이 변화하는 것을 확인하였습니다.

따라서, handle은 0x0030 값과 Opcode는 0x1b 값을 가지는 패킷에 대해 다음의 명령어를 수행하여 Value 값을 추출하였습니다.

- 명령어 : **tshark -r evidence1.pcap -Y "btatt.handle == 0x0030 && btatt.opcode == 0x1b" -T fields -e btatt.value > evidence1.txt**



1	000000e0ff0000
2	000000c0ff0000
3	000000e0ff0000
4	00000080ff0000
5	00000100000000
6	000000f0ff0000

[그림 4] 추출된 Value값 확인

다음의 7 바이트 Value 값에서 첫번째 바이트는 0x00, 0x01 이라는 특징을 가지고 있었으며, 세번째 바이트와 네번째 바이트는 0x00 ~ 0xff 범위의 값을 가지고 있었습니다. 또한, 해당 데이터의 첫번째 바이트 값인 00과 01의 값이 각각 붙어 있는 것을 통해 클릭이 아닌 mouse down event로 판단하였습니다.

```

import struct
import matplotlib.pyplot as plt
import numpy as np

Ask EasyCode | Explain | Refactor
def parse_hid_data(data):
    buttons, tmp, movement_x, movement_y = struct.unpack("4b", data[:4])
    mouse_down = buttons == 0x01
    move = buttons == 0x00
    return mouse_down, move, movement_x, movement_y

Ask EasyCode | Explain | Refactor
def extract_mouse_movements(txt_file):
    with open(txt_file, "r") as f:
        lines = f.readlines()

    coords = []
    clicks = []
    x, y = 0, 1920
    for line in lines:
        data = bytes.fromhex(line.strip())
        if len(data) >= 4:
            mouse_down, move, movement_x, movement_y = parse_hid_data(data)
            if mouse_down:
                x += movement_x
                y -= movement_y
                clicks.append((x, y))
            elif move:
                x += movement_x
                y -= movement_y
                coords.append((x, y))

    return coords, clicks

```

[그림 5] mouse HID data 시각화 코드 구현 - 1

```

def visualize_movements(coords, clicks):
    # Plot the coordinates
    coords = np.array(coords)
    fig, ax = plt.subplots()
    #ax.plot(coords[:, 0], coords[:, 1], marker=".", markersize=4, linestyle="-")

    # Mark left clicks
    clicks = np.array(clicks)
    ax.scatter(clicks[:, 0], clicks[:, 1], color='red', label="Left Click")

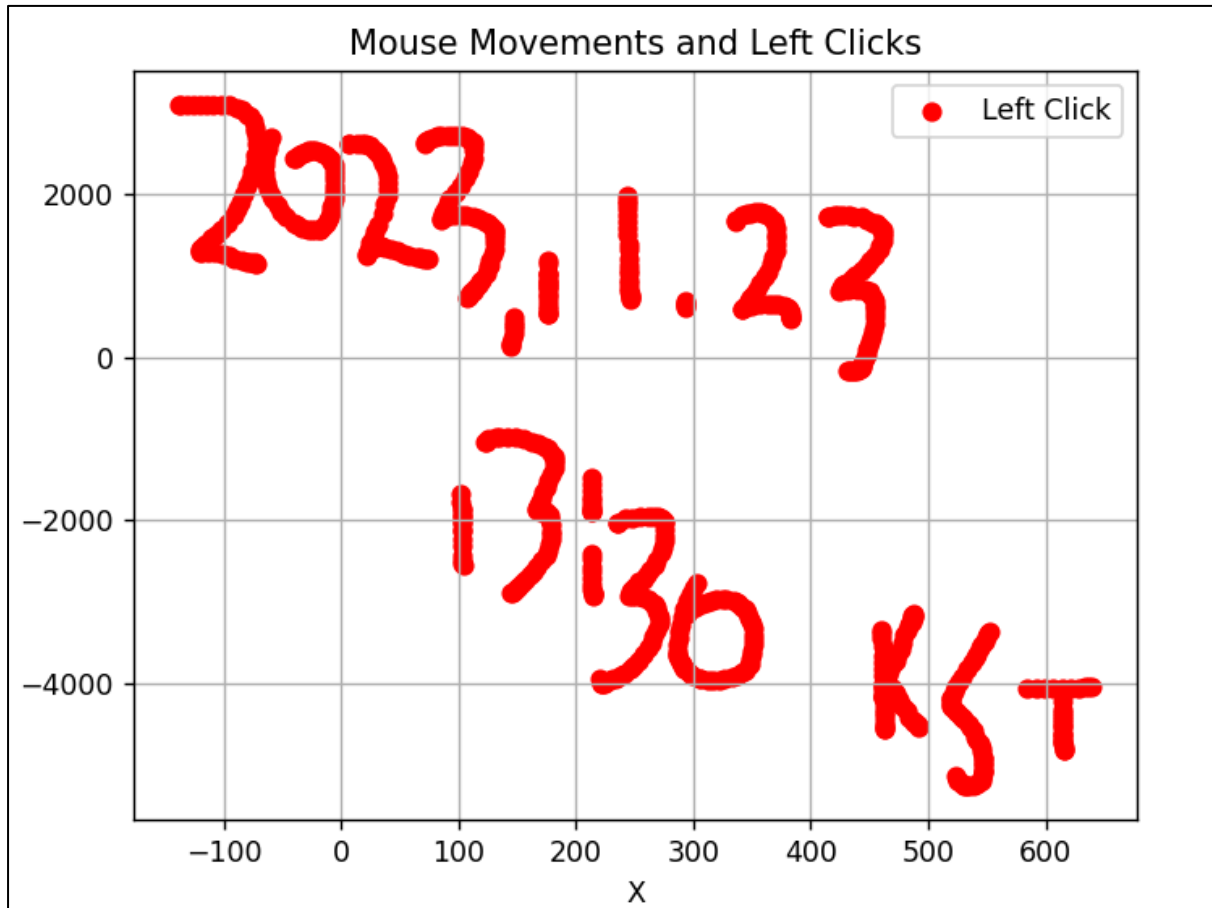
    plt.xlabel("X")
    plt.ylabel("Y")
    plt.title("Mouse Movements and Left Clicks")
    plt.grid()
    plt.legend()
    plt.show()

if __name__ == "__main__":
    txt_file = "evidence1.txt" # Update with your txt file path
    coords, clicks = extract_mouse_movements(txt_file)
    visualize_movements(coords, clicks)

```

[그림 6] mouse HID data 시각화 코드 구현 - 2

분석을 토대로 python code를 작성하여 mouse HID data를 시각화하였습니다.



[그림 7] 시각화 결과

코드를 통해 추출한 Value값을 시각화 한 결과 **2023.11.23 13:30 KST**라는 메시지를 확인할 수 있었습니다.

2) What is the message from evidence2? (40 points)

56	2023-06-28 08:34:35.145264	controller	host	HCI_EVT	258 Rcvd Extended Inquiry Result
57	2023-06-28 08:34:35.148883	controller	host	HCI_EVT	46 Rcvd LE Meta (LE Advertising Report)
58	2023-06-28 08:34:35.151906	controller	host	HCI_EVT	33 Rcvd LE Meta (LE Advertising Report)
59	2023-06-28 08:34:35.152882	controller	host	HCI_EVT	15 Rcvd LE Meta (LE Advertising Report)
60	2023-06-28 08:34:35.191913	controller	host	HCI_EVT	32 Rcvd LE Meta (LE Advertising Report)
61	2023-06-28 08:34:35.192878	controller	host	HCI_EVT	15 Rcvd LE Meta (LE Advertising Report)

Device Name: MH-M28
Length: 7
Type: Device Name (0x09)
Device Name: MH-M28
Manufacturer Specific

[그림 8] Device Name 확인

wireshark를 통해 evidence2.pcap 파일에서 확인한 Device Name은 MH-M28이었습니다. 이를 통해, 해당 장치가 블루투스 오디오 리시버 모듈임을 확인하였습니다. 따라서, 메시지와 관련된 부분은 음성일 것이라 판단하였습니다.

No.	Time	Source	Destination	Protocol	Length	Info
658	2023-06-28 08:34:46.572271	localhost ()	34:3f:83:46:67:e1 (MH-M28)	AVRCP	65	Sent Vendor dependent: Stable - GetElementAttributes
673	2023-06-28 08:35:21.654803	localhost ()	34:3f:83:46:67:e1 (MH-M28)	AVDTP	12	Sent Command - Start - ACP SEID [2 - Audio Sink]
675	2023-06-28 08:35:21.735798	34:3f:83:46:67:e1_	localhost ()	AVDTP	11	Rcvd ResponseAccept - Start
678	2023-06-28 08:35:21.765203	localhost ()	34:3f:83:46:67:e1 (MH-M28)	SBC	654	PT=SBC, SSRC=0x0, Seq=23277, Time=796366254 Frames=8
680	2023-06-28 08:35:21.796452	localhost ()	34:3f:83:46:67:e1 (MH-M28)	SBC	654	PT=SBC, SSRC=0x0, Seq=23278, Time=796367278 Frames=8
682	2023-06-28 08:35:21.816555	localhost ()	34:3f:83:46:67:e1 (MH-M28)	SBC	654	PT=SBC, SSRC=0x0, Seq=23279, Time=796368302 Frames=8
684	2023-06-28 08:35:21.846802	localhost ()	34:3f:83:46:67:e1 (MH-M28)	SBC	654	PT=SBC, SSRC=0x0, Seq=23280, Time=796369326 Frames=8
686	2023-06-28 08:35:21.866763	localhost ()	34:3f:83:46:67:e1 (MH-M28)	SBC	654	PT=SBC, SSRC=0x0, Seq=23281, Time=796370350 Frames=8
688	2023-06-28 08:35:21.886810	localhost ()	34:3f:83:46:67:e1 (MH-M28)	SBC	654	PT=SBC, SSRC=0x0, Seq=23282, Time=796371374 Frames=8
690	2023-06-28 08:35:21.916497	localhost ()	34:3f:83:46:67:e1 (MH-M28)	SBC	654	PT=SBC, SSRC=0x0, Seq=23283, Time=796372398 Frames=8

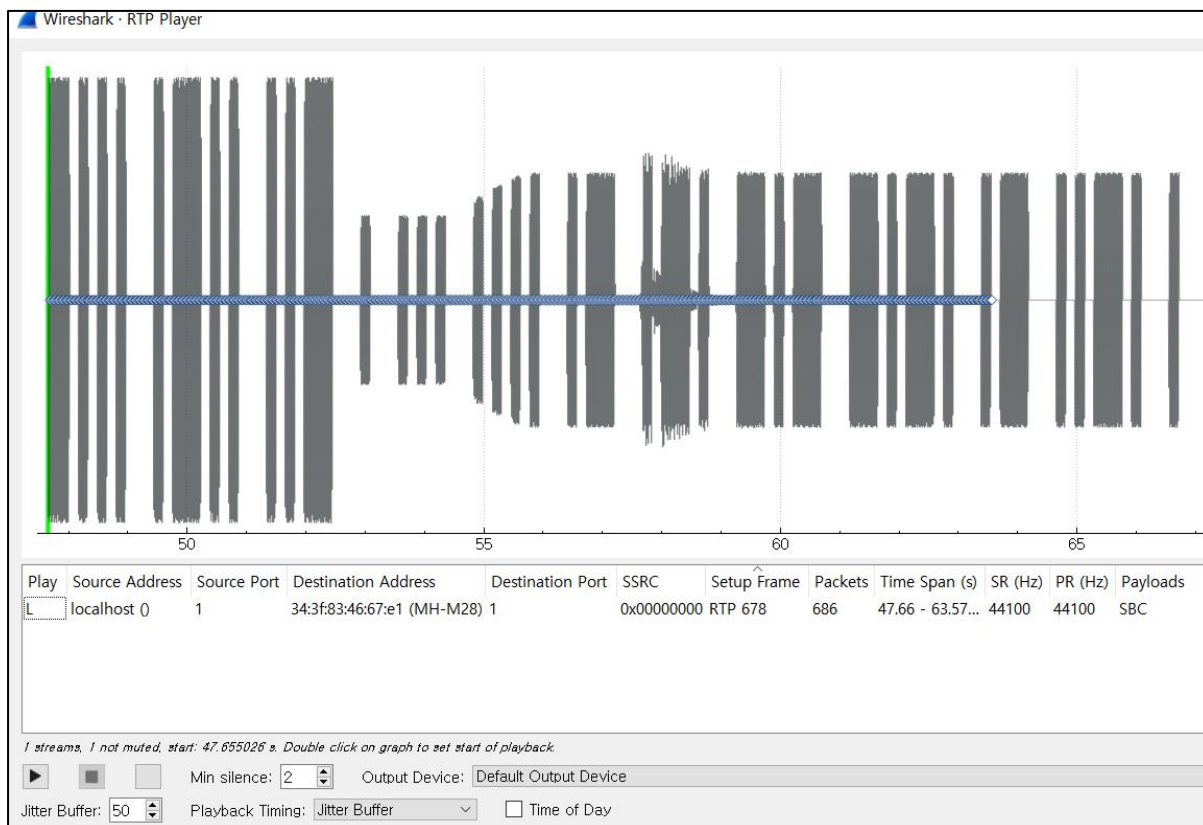
[그림 9] SBC codec packet 확인

음성 메시지가 있을 것이라고 판단되는 SBC Codec 프레임이 들어있는 패킷을 확인하였습니다.

Wireshark · Decode As...				
Field	Value	Type	Default	Current
UDP port	56905	Integer, base 10 (none)		QUIC
BT L2CAP CID 0x0044		Integer, base 16 (none)		RTP
BT L2CAP CID 0x0047		Integer, base 16 (none)		(none)

[그림 10] [Decode As] - [Current] RTP 세팅

해당 SBC 패킷에서 우클릭 후 [Decode As]를 누르고 Current에 RTP를 추가해주었습니다.



[그림 11] RTP Player에서 발견된 모스 부호 음성

그 후, Wireshark 상에서 [Telephony] -> [RTP] -> [RTP Streams] 기능을 누르고 [RTP Streams]에서 [Play Streams]를 누르게 되면 evidence2.pcap 파일 상에 존재하는 SBC 패킷들에 대한 음성을 들을 수 있는 것을 확인하였습니다. 해당 음성은 모스 부호로 판단되었고, 들리는 부분과 위 그림 상에서 보이는 긴 폭과 짧은 폭에 대해 - 과 . 으로 해석한 부분을 종합하여 evidence2.pcap 파일에서 확인된 메시지는 **BLUESHARKCAFE** 임을 확인하였습니다.

3) What is the message from evidence3? (20 points)

btl2cap				
No.	Time	Source	Destination	Protocol
274	2023-06-28 04:41:35.618728	fd:53:22:42:a8:5b...	localhost ()	SMP
276	2023-06-28 04:41:35.648284	fd:53:22:42:a8:5b...	localhost ()	ATT
278	2023-06-28 04:41:35.649511	localhost ()	fd:53:22:42:a8:5b (BT5.0Keyb...	ATT
280	2023-06-28 04:41:35.675031	localhost ()	fd:53:22:42:a8:5b (BT5.0Keyb...	SMP
282	2023-06-28 04:41:35.738810	fd:53:22:42:a8:5b...	localhost ()	ATT
283	2023-06-28 04:41:35.739058	localhost ()	fd:53:22:42:a8:5b (BT5.0Keyb...	ATT
286	2023-06-28 04:41:35.798471	fd:53:22:42:a8:5b...	localhost ()	ATT
287	2023-06-28 04:41:35.798669	localhost ()	fd:53:22:42:a8:5b (BT5.0Keyb...	ATT
289	2023-06-28 04:41:35.858275	fd:53:22:42:a8:5b...	localhost ()	ATT
290	2023-06-28 04:41:35.858445	localhost ()	fd:53:22:42:a8:5b (BT5.0Keyb...	ATT

[Connect in frame: 262]

[Source BD_ADDR: 00:00:00_00:00:00 (00:00:00:00:00:00)]

[Source Device Name:]

[Source Role: Unknown (0)]

[Destination BD_ADDR: fd:53:22:42:a8:5b (fd:53:22:42:a8:5b)]

[Destination Device Name: BT5.0Keyboard]

[그림 12] Keyboard device 확인

evidence3.pcap에서 btl2cap 필터링을 통해 식별된 장치는 BT5.0keyboard로 keyboard 장치였습니다.

No.	Time	Source	Destination	Protocol	Length	Info
547	2023-06-28 04:42:02.727985	fd:53:22:42:a8:5b...	localhost ()	ATT	20	Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)
548	2023-06-28 04:42:02.813452	fd:53:22:42:a8:5b...	localhost ()	ATT	20	Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)
549	2023-06-28 04:42:02.963414	fd:53:22:42:a8:5b...	localhost ()	ATT	20	Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)
550	2023-06-28 04:42:03.053413	fd:53:22:42:a8:5b...	localhost ()	ATT	20	Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)
551	2023-06-28 04:42:03.293411	fd:53:22:42:a8:5b...	localhost ()	ATT	20	Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)
552	2023-06-28 04:42:03.413456	fd:53:22:42:a8:5b...	localhost ()	ATT	20	Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)
553	2023-06-28 04:42:04.223433	fd:53:22:42:a8:5b...	localhost ()	ATT	20	Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)
554	2023-06-28 04:42:04.403451	fd:53:22:42:a8:5b...	localhost ()	ATT	20	Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)
555	2023-06-28 04:42:04.643452	fd:53:22:42:a8:5b...	localhost ()	ATT	20	Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)
556	2023-06-28 04:42:04.763410	fd:53:22:42:a8:5b...	localhost ()	ATT	20	Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)

[Destination Device Name:]

[Destination Role: Unknown (0)]

[Current Mode: Unknown (-1)]

> Bluetooth L2CAP Protocol

> Bluetooth Attribute Protocol

> Opcode: Handle Value Notification (0x1b)

> Handle: 0x0018 (Human Interface Device: Report)

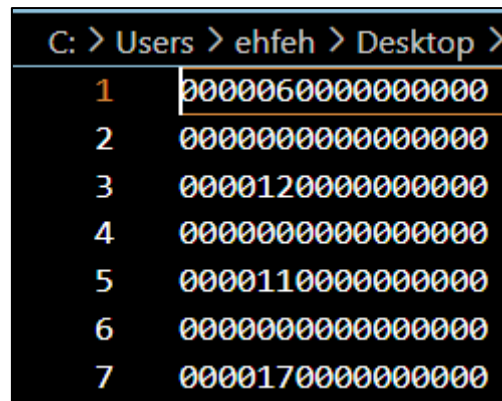
> Value: 0000000000000000

[그림 13] Bluetooth Attribute Protocol 정보 확인

또한, evidence1.pcap과 비슷하게 Rcvd에서 Handle Value Notification을 나타내는 opcode 0x1b를 가지고, Handle은 0x0018(Human Interface Device: Report)를 가지는 패킷 등에서 균일한 8바이트 Value를 식별할 수 있었습니다.

해당 Value를 가진 패킷들 역시 tshark를 통해 Value 부분만 다음과 같은 명령어로 출력하였습니다.

- 명령어 : `tshark -r evidence3.pcap -Y "btatt.handle == 0x0018 && btatt.opcode == 0x1b" -T fields -e btatt.value > evidence3.txt`



C: > Users > ehfeh > Desktop >	
1	0000060000000000
2	0000000000000000
3	0000120000000000
4	0000000000000000
5	0000110000000000
6	0000000000000000
7	0000170000000000

[그림 14] 추출된 Value값 확인

해당 참고 문헌¹에서 기록된 Keyboard Page에서 hex 값에 대응되는 keyboard 입력을 매핑하였습니다. 첫번째 바이트가 00이며, 추출된 Value값에서 발견된 shift나 caps lock에 매핑 되는 hex값이 존재하지 않았기 때문에, 매핑한 결과 evidence3.pcap에서 식별된 메시지는 **contact the person in the black hat**임을 확인하였습니다.

¹ https://www.usb.org/sites/default/files/documents/hut1_12v2.pdf