

## 105 – BlueShark

### Team Information

Team Name: kimbabasaksaksak

Team Member: Jaeheon Kim, Donghyun Kim, Soyoung Yoo, Minhee Lee

Email Address: uaaoong@gmail.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
Version:	4.0.6		
URL:	<a href="https://www.wireshark.org/">https://www.wireshark.org/</a>		

## Step-by-step methodology:

**Q1.** What is the message from evidence1? (40 points)

- 2023.11.23 13:30 KST

evidence1.pcap 파일은 블루투스 마우스 패킷을 캡처한 파일이다. 블루투스 Low Energy(BLE) 프로토콜을 통해 전송된 마우스 입력 데이터를 나타내며, 마우스의 이동 정보가 담겨있다.

230	2.347999	Slave	Master	ATT	35 Rcvd Read Response, Handle: 0x0027 (Human Interface Device: Boot Mouse Input Report)
231	2.355000	Master	Slave	ATT	35 Sent Find Information Request, Handles: 0x0028..0x0028
232	2.355000	Slave	Master	LE LL	26 Empty PDU
233	2.362000	Master	Slave	LE LL	26 Empty PDU
234	2.363000	Slave	Master	ATT	36 Rcvd Find Information Response, Handle: 0x0028 (Human Interface Device: Boot Mouse Input Report)

Length: 9	0000	03 1c 00 02 52 08 06 0a 0d 00 22 6e 00 96 00 00	...R...n...
CRC: 0x6f17ef	0010	00 4b df e2 4b 06 09 05 00 04 00 0b 00 00 00 00	:K:K:...
Bluetooth L2CAP Protocol	0020	f6 e8 f7	...
Length: 5			
CID: Attribute Protocol (0x0004)			
Bluetooth Attribute Protocol			
Opcode: Read Response (0x0b)			
0... .. = Authentication Signature: False			
.. .. = Command: False			
..00 1011 = Method: Read Response (0x0b)			
[Handle: 0x0027 (Human Interface Device: Boot Mouse Input Report)]			
[Service UUID: Human Interface Device (0x1812)]			
[UUID: Boot Mouse Input Report (0x2a33)]			
0... .. = Button 8: False			
.. .. = Button 7: False			
.. .. = Button 6: False			
..0 .. = Button 5: False			
....0... = Button 4: False			
....0.. = Button Middle: False			
....0. = Button Right: False			
....0 = Button Left: False			
X Displacement: 0			
Y Displacement: 0			
Horizontal Scroll Wheel: 0			
[Request in Frame: 227]			

ATT 프로토콜 Device Information의 Manufacturer String, Model Number String 값을 통해 Logitech M720 Triathlon 블루투스 마우스 장비에서 발생한 패킷을 캡처한 것을 알 수 있다.

```

324 2.701001 Slave Master ATT 39 Rcvd Read Response, Handle: 0x000e (Device Information: Manufacturer Name String)
325 2.707000 Master Slave ATT 37 Sent Read By Type Request, GATT Include Declaration, Handles: 0x0008..0x000b
326 2.708000 Slave Master LE LL 26 Empty PDU
327 2.715000 Master Slave LE LL 26 Empty PDU
328 2.715000 Slave Master ATT 35 Rcvd Error Response - Attribute Not Found, Handle: 0x0008 (Generic Access Profile: Per
<
[ Frame 324: 39 bytes on wire (312 bits), 39 bytes captured (312 bits) on nRF Sniffer for Bluetooth LE ]
[ Bluetooth Low Energy Link Layer ]
[ Bluetooth L2CAP Protocol ]
[ Bluetooth Attribute Protocol ]
  [ Opcode: Read Response (0x0b) ]
    [ 0... .. = Authentication Signature: False ]
    [ .0... .. = Command: False ]
    [ ..00 1011 = Method: Read Response (0x0b) ]
  [ [Handle: 0x000e (Device Information: Manufacturer Name String)] ]
    [ [Service UUID: Device Information (0x180a)] ]
    [ [UUID: Manufacturer Name String (0x2a29)] ]
    [ Manufacturer String: Logitech ]
    [ Request in Frame: 321 ]

```

320	2.685001	Slave	Master	ATT	45 Rcvd Read Response, Handle: 0x0010 (Device Information: Model Number String)
321	2.692001	Master	Slave	ATT	33 Sent Read Request, Handle: 0x000e (Device Information: Manufacturer Name String)
322	2.693000	Slave	Master	LE LL	26 Empty PDU

<	Frame 320: 45 bytes on wire (360 bits), 45 bytes captured (360 bits)	0000	03 26 00 02 ac 08 06 0a 0d 16 1e 9b 00 96 00 00	.&.....
>	nRF Sniffer for Bluetooth LE	0010	00 4b df e2 4b 06 13 0f 00 04 00 0b 4d 37 32 30	.K..K...M720
>	Bluetooth Low Energy Link Layer	0020	20 54 72 69 61 74 68 6c 6f 6a 27 a7 69	Triathl on i
>	Bluetooth L2CAP Protocol			
>	Bluetooth Attribute Protocol			
>	Opcode: Read Response (0x0b)			
>	0... .... = Authentication Signature: False			
>	..0... .... = Command: False			
>	..00 1011 = Method: Read Response (0x0b)			
>	[Handle: 0x0010 (Device Information: Model Number String)]			
>	[Service UUID: Device Information (0x180a)]			
>	[UUID: Model Number String (0x2a24)]			
>	Model Number String: M720 Triathlon			
>	[Request in Frame: 317]			

파이썬으로 btatt(Bluetooth Attribute Protocol) 패킷을 필터링하고 마우스 이동 데이터를 추출하여 그래프로 표시하는 코드를 작성하였다.

```

Q1.py

import matplotlib.pyplot as plt
import pyshark

mousePositionX = 0
mousePositionY = 0

X = []
Y = []

f = pyshark.FileCapture('evidence1.pcap', display_filter="btatt")

for p in f:
    data = p['btatt'].get_field_value('value')
    if data == None:
        continue

    Bytes = data.split(":")
    if len(Bytes) == 7:
        horizontal = 2
        vertical = 3
    else:
        continue

    offsetX = int(Bytes[horizontal], 16)
    offsetY = int(Bytes[vertical], 16)

```

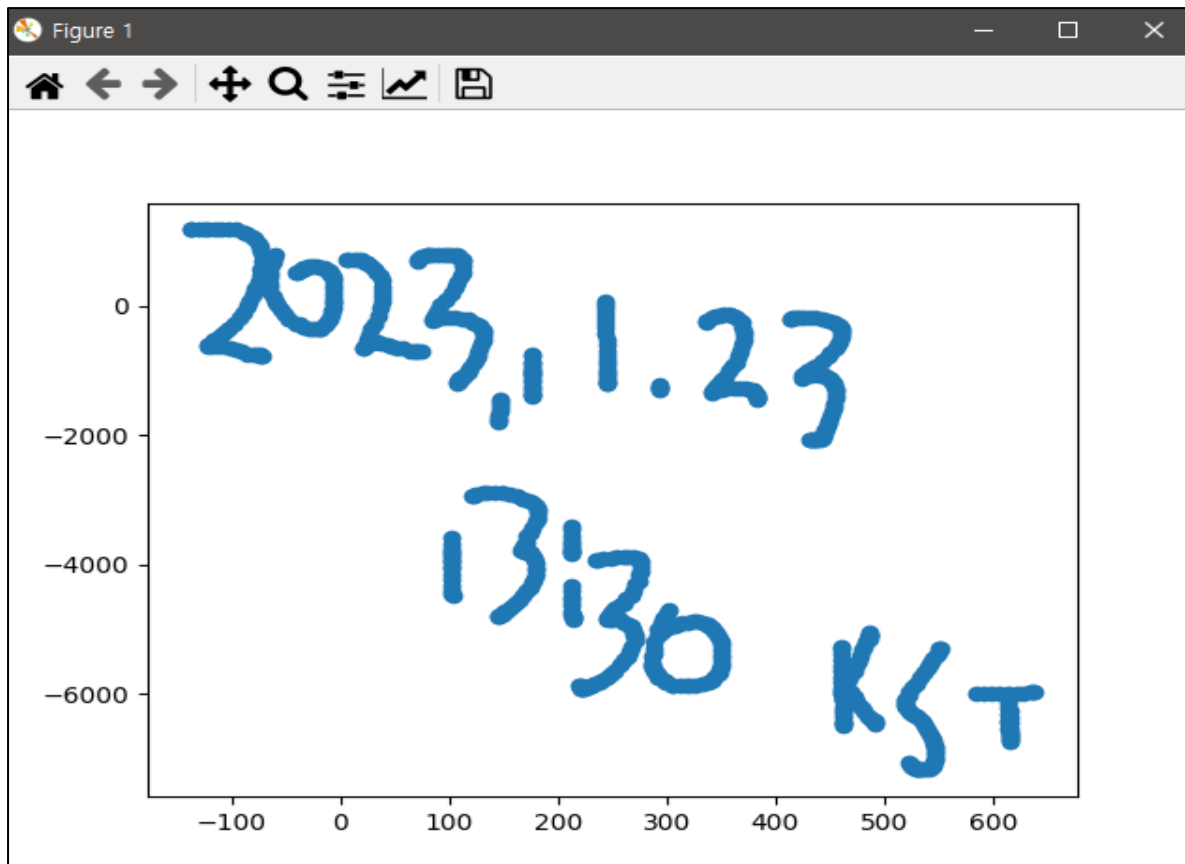
```
if offsetX > 127:
    offsetX -= 256
if offsetY > 127:
    offsetY -= 256

mousePositionX += offsetX
mousePositionY += offsetY

if Bytes[0] == "01":
    #print("[+] Left.")
    X.append(mousePositionX)
    Y.append(-mousePositionY)
elif Bytes[0] == "02":
    #print("[+] Right.")
    X.append(mousePositionX)
    Y.append(-mousePositionY)
else:
    print("[-] Known operate.")
    pass

fig = plt.figure()
ax1 = fig.add_subplot()
ax1.scatter(X, Y)
plt.show()
```

파이썬 코드 실행 결과는 아래와 같으며, "2023.11.23 13:30 KST" 메시지를 확인할 수 있다.



## Q2. What is the message from evidence2? (40 points)

- BLUESHARKCAFE

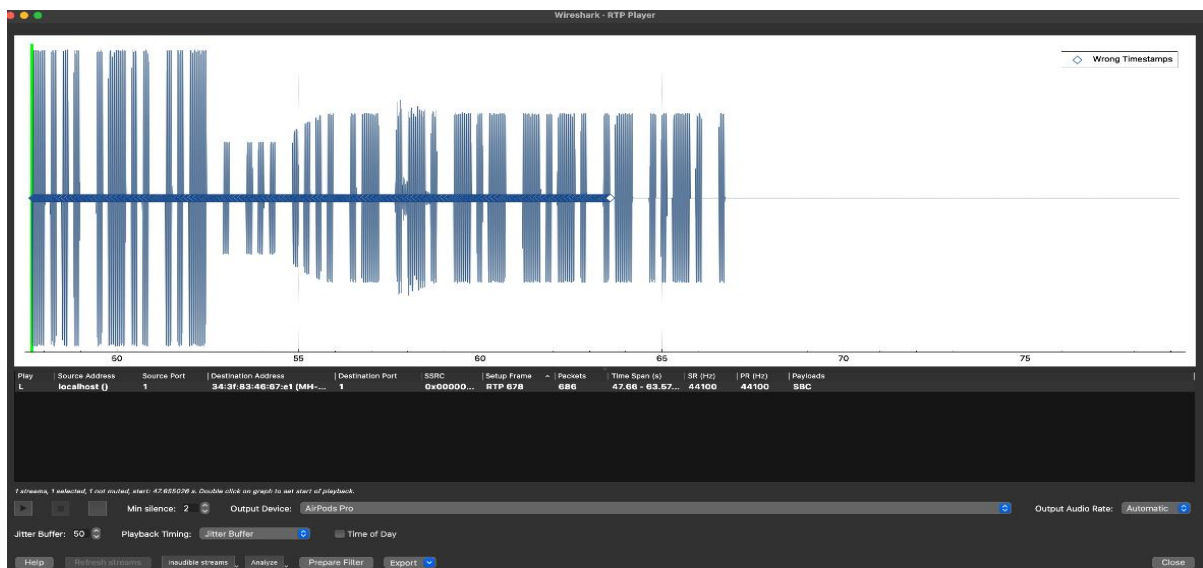
Evidence2.pcap 파일은 블루투스 오디오 패킷을 캡처한 파일이다. 패킷은 블루투스 A2DP(Advanced Audio Distribution Profile)를 통해 오디오 스트림을 전송한다. A2DP 프로파일을 통해 오디오 스트림 데이터를 RTP 프로토콜을 사용하여 전송하고 있으며, SBC 오디오 코덱을 사용하고 "MH-M28" 모델의 블루투스 오디오 모듈을 사용하는 것을 알 수 있다.

No.	Time	Source	Destination	Protocol	Length	Info
742	48.486615	localhost ()	34:3f:83:46:67:e1 (~ SBC	654	PT=SBC, SSRC=0x0, Seq=23309, Time=796399022	Frames=8
743	48.425705	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
744	48.426459	localhost ()	34:3f:83:46:67:e1 (~ SBC	654	PT=SBC, SSRC=0x0, Seq=23310, Time=796400046	Frames=8
745	48.449724	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
746	48.456194	localhost ()	34:3f:83:46:67:e1 (~ SBC	654	PT=SBC, SSRC=0x0, Seq=23311, Time=796401070	Frames=8
747	48.472713	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
748	48.476289	localhost ()	34:3f:83:46:67:e1 (~ SBC	654	PT=SBC, SSRC=0x0, Seq=23312, Time=796402094	Frames=8
749	48.496453	localhost ()	34:3f:83:46:67:e1 (~ SBC	654	PT=SBC, SSRC=0x0, Seq=23313, Time=796403118	Frames=8
750	48.499707	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
751	48.502698	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
752	48.526645	localhost ()	34:3f:83:46:67:e1 (~ SBC	654	PT=SBC, SSRC=0x0, Seq=23314, Time=796404142	Frames=8
753	48.546344	localhost ()	34:3f:83:46:67:e1 (~ SBC	654	PT=SBC, SSRC=0x0, Seq=23315, Time=796405166	Frames=8
754	48.546713	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets

0000	02 04 20 89 02 85 02 47	00 80 60 5a f9 2f 77 c5	.....G...Z./w...
0010	ae 00 00 00 00 00 00 00	21 3e c0 e2 00 00 00 00	.....l.....
0020	00 00 00 e5 7e df 5a d3	28 ee 2d 56 24 ee 16 a3	.....Z...(-V\$...
0030	3a 50 4b 50 1e d4 45 a8	cf c8 fa d5 63 48 89 69	..PKP..E...-ch-i...
0040	4d 22 86 b5 e5 a4 7e 5a	ff 08 5b ad 79 a2 b7 d6	M...U...-T...y...
0050	b5 00 c8 db 55 a4 8b 75	a8 d7 04 54 d4 07 91 01	.....j1-N...!>.....
0060	6a 31 b6 4e b5 9c bd 21	3e c0 e2 00 00 00 00 00	..W..Z..o...-y'V...
0070	00 00 57 17 17 5a d2 6f	a1 2d 79 27 9f 56 bf c3	..^y...M...o...j7...
0080	16 eb 5e 79 ed d5 ad 4d	e7 0a d5 6f fa fd 6a 3f	.....QZ...-UZ...
0090	e5 00 b5 01 f5 51 5a 8b	f0 08 ad 55 5a 06 16 b4	d..k^8W5...-k...
00a0	64 a8 6b 5e 38 57 35 af	f0 ad d2 d7 a2 d3 7d 6b	V...!>.....
00b0	56 ed ce b5 9c bd 21 3e	c0 e2 00 00 00 00 00 00	.....Z...-Z...-@{.....
00c0	00 5d b2 ba 5a 8e 7d c3	2d 40 7b 11 d6 a2 da 04	.....U;2%...-j...-k...
00d0	0b 55 3b 32 25 ad 0b 6a	12 d7 89 bd d9 6b fc 03	.....P...-Z...p-W/V...?
00e0	72 b5 e9 a7 dd 5a d6 90	f0 2d 57 dc 2f 56 a3 c4	.....Z...-H(yk?...
00f0	91 0b 50 20 f4 75 a8 ae	f9 1a d5 48 28 79 6b 3f	Z...!>.....
0100	5a 7e b5 9c bd 21 3e c0	e2 00 00 00 00 00 00 00	CtZ...>...z-w...+...
0110	e1 43 74 5a fe ed d8 a9	7a a5 77 16 b5 d9 1c 2b	V...-B...-j...-B...
0120	56 13 1c 15 a8 fa 94 42	d4 08 e5 29 6a 29 e8 42	..Pd..Z...-8...-v...
0130	b5 50 64 1c 5a ce f7 20	2d 38 05 9a d6 bf b7 7e	.....!>.....
0140	eb 5e b9 4d a5 ad 83 bf	52 d5 0b b6 fe 6a 40 e9	..^M...-R...-j@...
0150	16 b5 9c bd 21 3e c0 e2	00 00 00 00 00 00 00 02	.....SNZ...-S-G...-+...
0160	53 4e 5a 89 fe 92 ad 53	ae 47 16 b3 85 c7 2b 5d	.....UR...-kd1...-
0170	ee a7 95 af ec 55 52 d7	b1 c3 b1 6b 64 31 be b5	d...-Z...-D...-@...-c-K...
0180	64 b0 c2 5a 90 d6 44 2d	40 a1 94 16 a2 63 04 4b	T..A...-i...-v...-k...V...
0190	54 d1 41 d5 ac d3 69 d2	d7 76 e5 d5 6b fa c1 56	.....l>.....
01a0	b5 9c bd 21 3e c0 e2 00	00 00 00 00 00 00 ed 5d	.....l>.....

Wireshark에서 제공하는 RTP 스트림 재생 기능 RTP Player를 통해 음성 데이터를 재생할 수 있다.



The screenshot shows a web application with a light green header bar. On the left, the word "Recipe" is displayed. To its right are three icons: a floppy disk, a folder, and a trash can. Below the header, the left sidebar has a green background. It features the text "From Morse Code" in white, followed by a power icon and a pause icon. There are two input fields: "Letter delimiter" with the value "Space" and "Word delimiter" with the value "Line feed". The main area on the right has a light gray header labeled "Input". Below it is a large text input field containing the Morse code ".... .-.-. .-.. .- .-.-. -.-. -.-. -.-. -.-. |". At the bottom of the main area, there is a status bar showing "rec 50" and a hamburger menu icon next to the number "1". Below the status bar is a light gray header labeled "Output". The output area displays the text "BLUESHARKCAFE" in a yellow box.

### Q3. What is the message from evidence3? (20 points)

- contact the person in the black hat

Evidence3.pcap 파일은 블루투스 키보드 패킷을 캡처한 파일이다. 블루투스 키보드는 HID(Human Interface Device) 프로파일을 사용하여 데이터를 전송하며, GATT(Generic Attribute Profile)를 기반으로 하여 프로토콜 스택의 계층 구조를 따른다. 문제에서 주어진 패킷 파일을 살펴보면, 블루투스 키보드의 패킷 구조를 나타내고 있음을 확인 가능하다.

343	11.179932	fd:53:22:42:a8:5b (- localhost)	ATT	32 Rcvd Read By Type Response, Attribute List Length: 3, Report, Report Map, Boot Keyboard Input Report
344	11.180074	localhost ()	fd:53:22:42:a8:5b (- ATT	16 Sent Read By Type Request, GATT Characteristic Declaration, Handles: 0x0031..0xffff
345	11.211196	controller	host	8 Rcvd Number of Completed Packets
346	11.239980	fd:53:22:42:a8:5b (- localhost)	ATT	32 Rcvd Read By Type Response, Attribute List Length: 3, Boot Keyboard Output Report, HID Information, HID Control Point
347	11.240121	localhost ()	fd:53:22:42:a8:5b (- ATT	16 Sent Read By Type Request, GATT Characteristic Declaration, Handles: 0x0038..0xffff
348	11.271192	controller	host	8 Rcvd Number of Completed Packets
349	11.299649	fd:53:22:42:a8:5b (- localhost)	ATT	14 Rcvd Error Response - Attribute Not Found, Handle: 0x0038 (Human Interface Device: HID Control Point)
350	11.299833	localhost ()	fd:53:22:42:a8:5b (- ATT	14 Sent Find Information Request, Handles: 0x0039..0xffff
351	11.331190	controller	host	8 Rcvd Number of Completed Packets
352	11.359778	fd:53:22:42:a8:5b (- localhost)	ATT	14 Rcvd Error Response - Attribute Not Found, Handle: 0x0039 (Human Interface Device: HID Control Point: Unknown)
353	11.360803	localhost ()	fd:53:22:42:a8:5b (- ATT	12 Sent Read Request, Handle: 0x0036 (Human Interface Device: HID Information)
354	11.391195	controller	host	8 Rcvd Number of Completed Packets
355	11.419640	fd:53:22:42:a8:5b (- localhost)	ATT	14 Rcvd Read Response, Handle: 0x0036 (Human Interface Device: HID Information)
356	11.419828	localhost ()	fd:53:22:42:a8:5b (- ATT	12 Sent Read Request, Handle: 0x0034 (Human Interface Device: Boot Keyboard Output Report)
357	11.481197	controller	host	8 Rcvd Number of Completed Packets
358	11.509645	fd:53:22:42:a8:5b (- localhost)	ATT	11 Rcvd Read Response, Handle: 0x0034 (Human Interface Device: Boot Keyboard Output Report) - LEDs: NumLock, CapsLock, ScrollLock
359	11.509970	localhost ()	fd:53:22:42:a8:5b (- ATT	12 Sent Read Request, Handle: 0x0031 (Human Interface Device: Boot Keyboard Input Report)
360	11.540207	controller	host	13 Rcvd LE Meta (LE Connection Update Complete)
361	11.541189	controller	host	8 Rcvd Number of Completed Packets
362	11.554737	fd:53:22:42:a8:5b (- localhost)	ATT	18 Rcvd Read Response, Handle: 0x0031 (Human Interface Device: Boot Keyboard Input Report) - RIGHT ALT + RIGHT SHIFT + RIGHT CTRL + LEFT SHIFT

HCI Packet Type: ACL Data (0x02)	
Bluetooth HCI ACL Packet	
.... 0000 0001 0000	= Connection Handle: 0x010
..10 .... ....	= PB Flag: First Automatically Flushable Packet (2)
00.. .... ....	= BC Flag: Point-To-Point (0)
Data Total Length: 27	
Data	
[Connect in frame: 262]	
[Source BD_ADDR: fd:53:22:42:a8:5b (fd:53:22:42:a8:5b)]	
[Source Device Name: BT5.0Keyboard]	
[Source Role: Unknown (0)]	
[Destination BD_ADDR: 00:00:00:00:00:00 (00:00:00:00:00:00)]	
[Destination Device Name: ]	
[Destination Role: Unknown (0)]	

0000	02 10 20 1b 00 17 00 04 00 09 07 33 00 8e 34 00	.....3.4
0010	32 2a 15 02 02 36 00 4a 2a 37 00 04 38 00 4c 2a	2*6J*7:8L*

GATT는 ATT 프로토콜을 기반으로 동작하기 때문에 키보드의 입력 데이터는 ATT의 Attribute에 포함되어 GATT 프로파일을 통해 전송된다. 입력 데이터는 Value 값에서 확인 가능하며, 입력된 문자의 대소문자 여부를 판단하는 modifier byte\*가 "00"으로 입력된 문자는 모두 소문자인 것을 알 수 있다. (대문자의 경우 "20")

- <https://cdn.sparkfun.com/datasheets/Wireless/Bluetooth/RN-HID-User-Guide-v1.0r.pdf>



547 31.074325	fd:53:22:42:a8:5b (- localhost ())	ATT	20 Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)	
548 31.159792	fd:53:22:42:a8:5b (- localhost ())	ATT	20 Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)	
549 31.389754	fd:53:22:42:a8:5b (- localhost ())	ATT	20 Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)	
550 31.399753	fd:53:22:42:a8:5b (- localhost ())	ATT	20 Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)	
551 31.639751	fd:53:22:42:a8:5b (- localhost ())	ATT	20 Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)	
552 31.759796	fd:53:22:42:a8:5b (- localhost ())	ATT	20 Rcvd Handle Value Notification, Handle: 0x0018 (Human Interface Device: Report)	
Bluetooth HCI H4				0000 02 10 20 0f 00 0b 00 04 00 1b 18 00 00 06 00 ... ..
[Direction: Rcvd (0x01)]				0010 00 00 00 00
HCI Packet Type: ACL Data (0x02)				
Bluetooth HCI ACL Packet				
.... 0000 0001 0000 = Connection Handle: 0x010				
..10 .... = PB Flag: First Automatically Flushable Packet (2)				
00.... = BC Flag: Point-To-Point (0)				
Data Total Length: 15				
Data				
[Connect in frame: 262]				
[Source BD_ADDR: fd:53:22:42:a8:5b (fd:53:22:42:a8:5b)]				
[Source Device Name: BT5.0Keyboard]				
[Source Role: Unknown (0)]				
[Destination BD_ADDR: 00:00:00:00:00:00 (00:00:00:00:00:00)]				
[Destination Device Name: ]				
[Destination Role: Unknown (0)]				
[Current Mode: Unknown (-1)]				
Bluetooth L2CAP Protocol				
Length: 11				
CID: Attribute Protocol (0x0004)				
Bluetooth Attribute Protocol				
Opcode: Handle Value Notification (0x1b)				
0... = Authentication Signature: False				
.0... = Commands: False				
..01 1011 = Method: Handle Value Notification (0x1b)				
Handle: 0x0018 (Human Interface Device: Report)				
[Service UUID: Human Interface Device (0x1812)]				
[UUID: Report (0x2a4d)]				
Value: 0000060000000000				
[Export Info (Note/Undecoded): Undecoded]				
[Undecoded]				

HID Keyboard Usage Table([https://www.usb.org/sites/default/files/documents/hut1\\_12v2.pdf](https://www.usb.org/sites/default/files/documents/hut1_12v2.pdf)) 에서 hex 값에 따른 문자열 테이블을 찾은 후 파이썬으로 pcap 파일 내부 패킷을 파싱하여 문자열로 변환하는 코드를 작성하였다.

```
import binascii

urb = {
    '04': 'a',
    '05': 'b',
    '06': 'c',
    '07': 'd',
    '08': 'e',
    '09': 'f',
    '0a': 'g',
    '0b': 'h',
    '0c': 'i',
    '0d': 'j',
    '0e': 'k',
    '0f': 'l',
    '10': 'm',
    '11': 'n',
    '12': 'o',
    '13': 'p',
}
```

'14': 'q',  
'15': 'r',  
'16': 's',  
'17': 't',  
'18': 'u',  
'19': 'v',  
'1a': 'w',  
'1b': 'x',  
'1c': 'y',  
'1d': 'z',  
'1e': '1',  
'1f': '2',  
'20': '3',  
'21': '4',  
'22': '5',  
'23': '6',  
'24': '7',  
'25': '8',  
'26': '9',  
'27': '0',  
'28': 'Wn',  
'29': '[ESC]',  
'2a': '[BACKSPACE]',  
'2b': '[TAB]',  
'2c': ' ',  
'2d': '\_',  
'2e': '=',  
'2f': '{',  
'30': '}',  
'31': '[CAPSLOCK]',  
'32': '[F1]',  
'33': '[F2]',  
'34': '[F3]',  
'35': '[F4]',  
'36': '[F5]',  
'37': '[F6]',  
'38': '[F7]',  
'39': '[F8]',  
'3a': '[F9]',

```

'3b': '[F10]',
'3c': '[F11]',
'3d': '[F12]',
'4c': '[DELETE]',
'4f': '[RIGHT]',
'50': '[LEFT]',
'51': '[DOWN]',
'52': '[UP]'
}

def find_hex_values(pcap_file):
    pattern = '02 10 20 0F 00 0B 00 04 00 1B 18 00 00 00'
    hex_values = []

    with open(pcap_file, 'rb') as file:
        pcap_data = file.read()

    pattern_bytes = bytes.fromhex(pattern)

    indices = [i for i in range(len(pcap_data)) if pcap_data[i:i+len(pattern_bytes)] ==
pattern_bytes]

    for index in indices:
        hex_byte = pcap_data[index + len(pattern_bytes):index + len(pattern_bytes) + 1]
        hex_value = hex_byte.hex().lower()

        if hex_value == '00':
            continue

        if hex_value in urb:
            hex_values.append(urb[hex_value])

    return hex_values

pcap_file = 'evidence3.pcap'
result = find_hex_values(pcap_file)
print(''.join(result))

```

파이썬 코드 실행 결과는 아래와 같으며, "contact the person in the black hat" 메시지를 확인할 수 있다.

```
D:\Users\mini\Desktop\DFC2023\105 - BlueShark\Evidence>python Q3.py evidence3.pcap
contact the person in the black hat
```