105 – BlueShark

Team Information

Team Name _____

Team Member _____

_____

_____

Email Address _____

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:		Publisher:	
Version:			

URL:	

Step-by-step methodology:

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

메모 포함[오전1]: evidence1에서의 메시지는 무엇입니까?

```
26 Empty PDU
35 Rcvd Read Response, Handle: 0x0027 (Human Interface Device: Boot Mouse Input Report)
35 Sent Find Information Request, Handles: 0x0028..0x0028
```

Human Interface Device인 블루투스 마우스의 네트워크 패킷 같다.

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

메모 포함[오전2]: evidence2의 메세지는 무엇입니까?

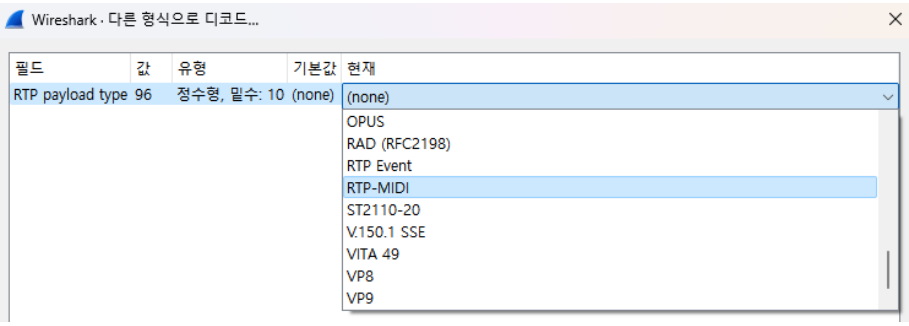
```
Extended Inquiry Response Data
  Device Name: MH-M28
```

MH-M28을 구글링해본 결과, 무선 오디오 모듈이라는 것을 알 수 있었다.

Wireshark 내에서 오디오 관련 기능을 찾아보았고 RTP를 알게 되었다.

RTP는 실시간 전송 프로토콜이다. 네트워크를 통해 오디오와 비디오를 전달하기 위한 패킷 포맷이라고 한다.

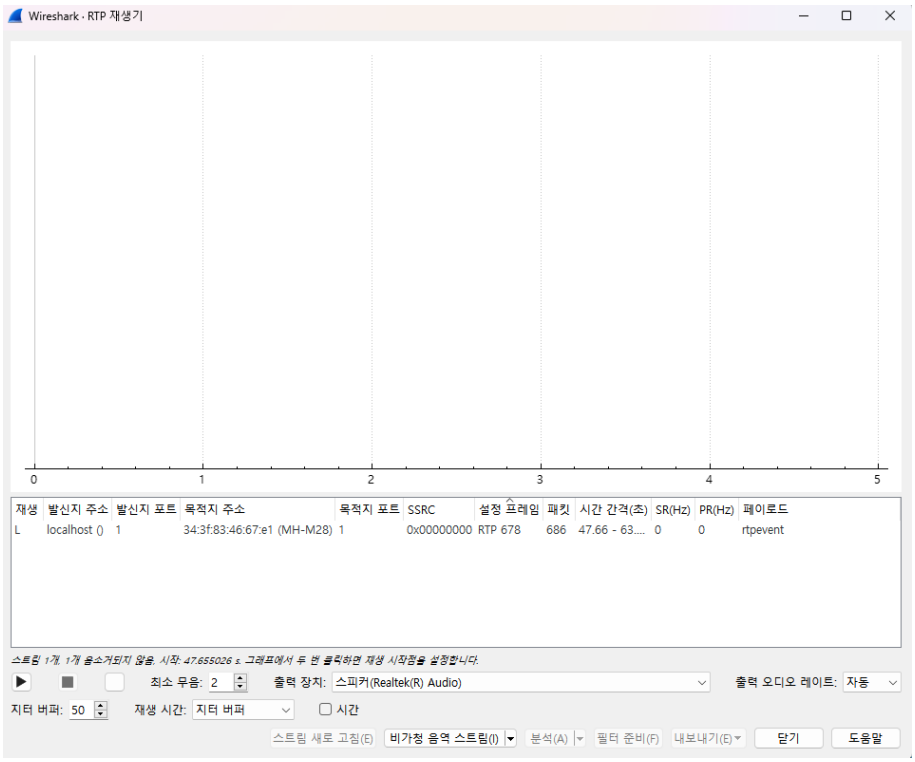
제공받은 pcap 파일 중 프로토콜은 6개가 있었고, 그 중 Device Name이 제공되었던 SBC 프로토콜을 우선적으로 분석하였다.



Protocol 순서대로 정렬을 한 후, SBC에서 가장 첫 번째 패킷의 [우클릭-다른 형식으로 디코드]로

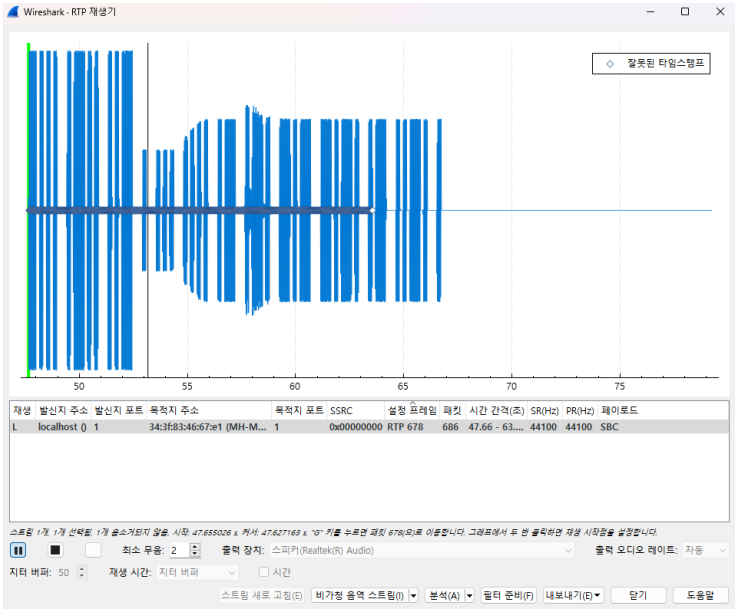
들어가 '현재'칸을 (none)이 아닌 RTP-MIDI로 설정해준다.

(RTP Event도 진행해보았으나 MIDI에서만 오디오를 들을 수 있었다.)

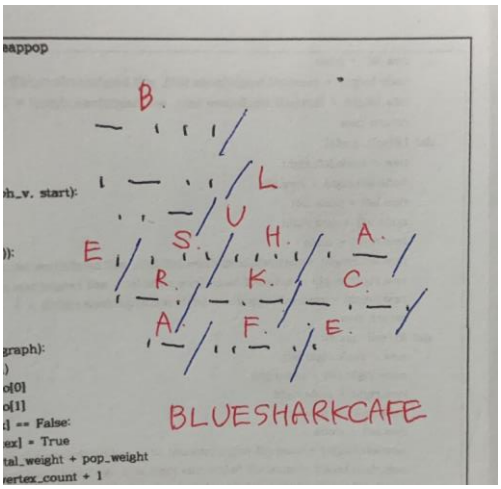


변경시킨 후, 상단의 메뉴 중 [전화-RTP(R)-RTP 스트림]으로 들어가면 상단과 같이 화면이 뜬다.

스트림 재생을 클릭한다.



재생 버튼을 눌러 음성을 듣다보니 모스부호가 생각났다.



부호를 해석하면 **BLUESHARKCAFE** 라는 flag가 나온다.

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

메모 포함[오전3]: evidence3의 메세지는 무엇입니까?

Custom	Source	Destination	Protocol	Length	Info
04:41:35.350843	controller	host	HCI_EVT	7	Rcvd Command Complete (LE Set Scan Enable)
04:41:35.396739	host	controller	HCI_CMD	29	Sent LE Create Connection
04:41:35.399887	controller	host	HCI_EVT	7	Rcvd Command Status (LE Create Connection)
04:41:35.482876	controller	host	HCI_EVT	22	Rcvd LE Meta (LE Connection Complete)
04:41:35.482902	host	controller	HCI_CMD	6	Sent LE Read Channel Map
04:41:35.486853	controller	host	HCI_EVT	14	Rcvd Command Complete (LE Read Channel Map)
04:41:35.487923	localhost ()	fd:53:22:42:a8:5b (BT5.0Keyboard)	ATT	12	Sent Exchange MTU Request, Client Rx MTU: 527
04:41:35.499862	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets

```
[Destination BD_ADDR: fd:53:22:42:a8:5b (fd:53:22:42:a8:5b)]
[Destination Device Name: BT5.0Keyboard]
[Destination Role: Unknown (0)]
```

BT5.0keyboard라는 Desitination과 Destination Device Name을 보고 블루투스 키보드의 네트워크 패킷이라는 것을 알 수 있다.

The deadline for this problem is August 31.

Please do not post your write-up before the deadline for fair competition!

*** Delete this box when submitting your answer.**