**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)

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명 Human Interface Device인 블루투스 마우스의 네트워크 패킷 같다.

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



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.

텍스트, 소프트웨어, 번호, 컴퓨터 아이콘이(가) 표시된 사진

자동 생성된 설명

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.)

텍스트, 스크린샷, 디스플레이, 라인이(가) 표시된 사진

자동 생성된 설명

텍스트, 라인, 폰트, 그래프이(가) 표시된 사진

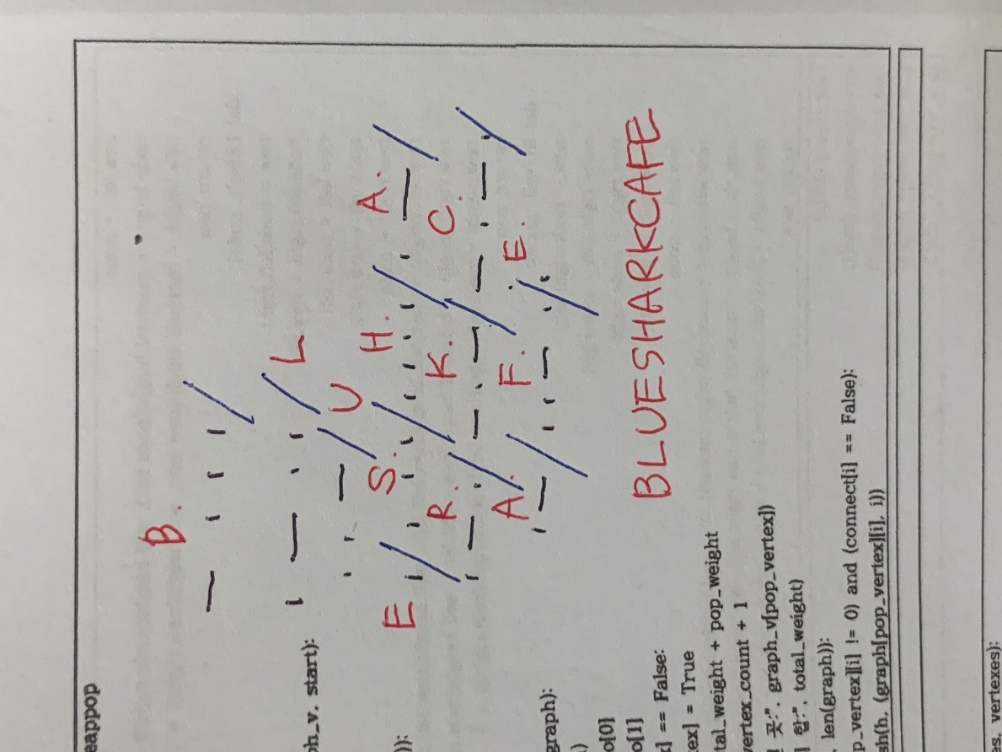
자동 생성된 설명 변경시킨 후, 상단의 메뉴 중 [전화-RTP(R)-RTP 스트림]으로 들어가면 상단과 같이 화면이 뜬다.

스트림 재생을 클릭한다.

텍스트, 스크린샷, 라인, 평행이(가) 표시된 사진

자동 생성된 설명

재생 버튼을 눌러 음성을 듣다보니 모스부호가 생각났다.



부호를 해석하면 **BLUESHARKCAFE** 라는 flag가 나온다.

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

텍스트, 폰트, 번호, 스크린샷이(가) 표시된 사진

자동 생성된 설명텍스트, 폰트, 스크린샷, 라인이(가) 표시된 사진

자동 생성된 설명

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.**