Report:

IMO decryption:

First of all, we do some background study about the safety and security issue of IMO. One reference: “ <https://www.quora.com/Is-it-safe-to-use-IMO-for-video-call> “. The answer is somehow in our favor as in the policy pages of IMO (“ <https://www.imo.im/policies/terms_of_service>” ), there is no mention of any types of encryption process where as Viber directly tells us about their encryption process which is nearly impossible to break. So, we can make an assumption that the encryption process may be easier (may be a little bit) than Viber.

Then, we take some capture by Wireshark while using IMO. We try to find out any TSL packets like “Client Hello or Server Hello”. But fortunately, we don’t get any of them. So, we may say that, IMO doesn’t use the encryption method that Facebook or Viber use.

Then, we try to find any other TLS packet present there. We have found some SSL data and all of them are named “Continuation Data”. We are trying to find out their significance. Continuation data is somewhat like without the header of a tcp packet and maybe they have not that much significance.

Then, we have made an analysis with the packets of that particular capture where we have entered to IMO app and make a call. Entering to IMO and making the call was done at 13.104 second (55 no packet) and the first packet with the receiver’s ip address we have found at 14.4033 second (80 no packet). So, we are assuming that within these packet range (55-79) we have the signaling packet where the receiver’s information is provided. So, next we are working with analyzing these particular packets deeply to find any significant information.