When sending commands to a camera through the Doodle Smart APP based on the MQTT protocol via a server, as shown in Figures 1 and 2, it is found that the device on the APP will temporarily go offline. At the same time, when capturing the communication packets between the device and the server, it is discovered that the device actively sends a FIN packet to terminate the current communication connection, as shown in Figures 3 and 4. This vulnerability leads to a denial of service for a period of time. The specific implementation involves triggering the execution of any control command to generate network traffic on the app side, then performing a man-in-the-middle attack between the APP and the server to decrypt the SSL/TLS packets, and reverse-engineering the original control commands based on the encryption algorithm. The control command ID and its corresponding value are then modified as shown in Figures 1 and 2. Subsequently, new packets are generated according to encryption and coding rules and sent to the server, which then forwards these packets to the device. Upon receiving these packets, the device exhibits abnormal behavior, resulting in the device going offline.

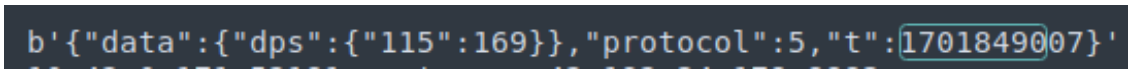

Figure 1: Plain text of the abnormal control command triggered by the APP - 1

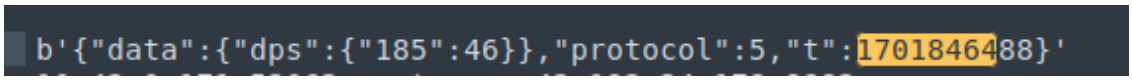

Figure 2 Plain text of the abnormal control command triggered by the APP - 2

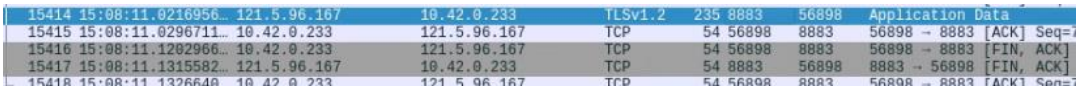

Figure 3 Communication packet between IoT device and server when anomaly is triggered - 1

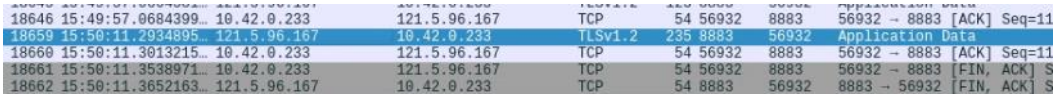

Figure 4 Communication packet between IoT device and server when anomaly is triggered - 2