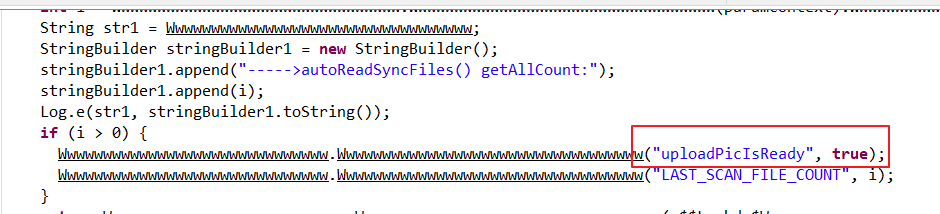
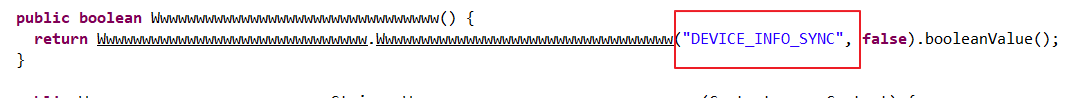
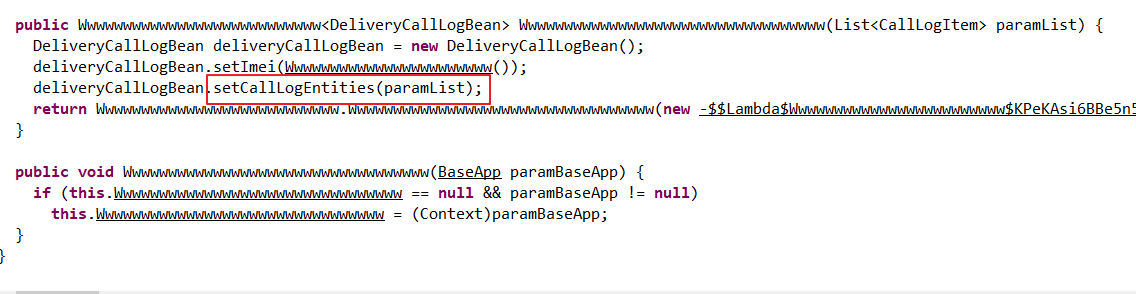


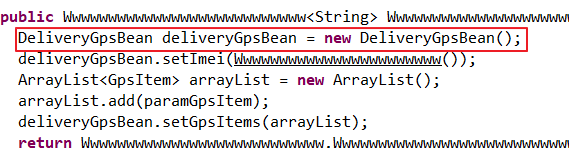
* spyss/com.spyss.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwwww.Wwwwwwwwwwwwwwwwwwwwwwww 분석



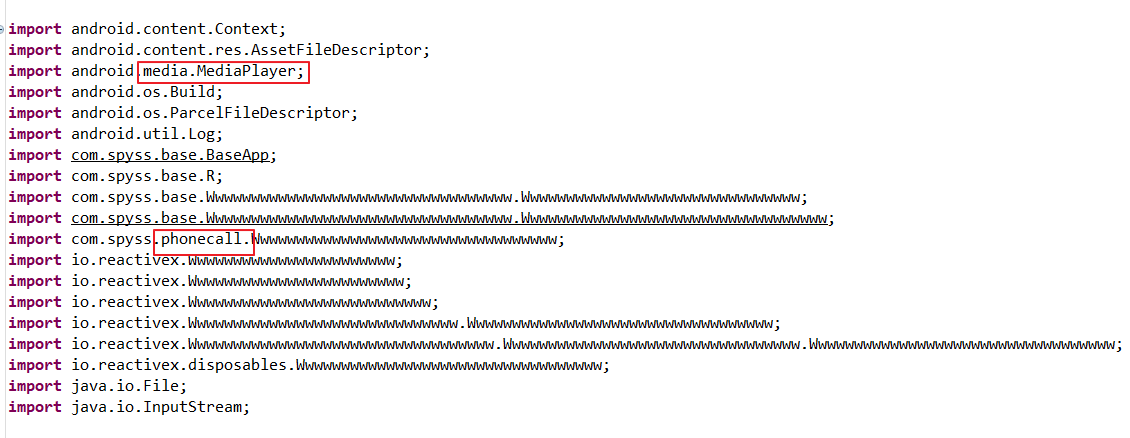




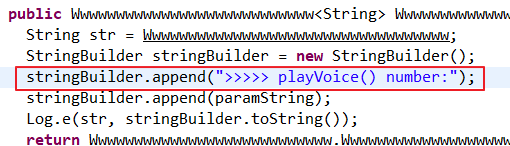




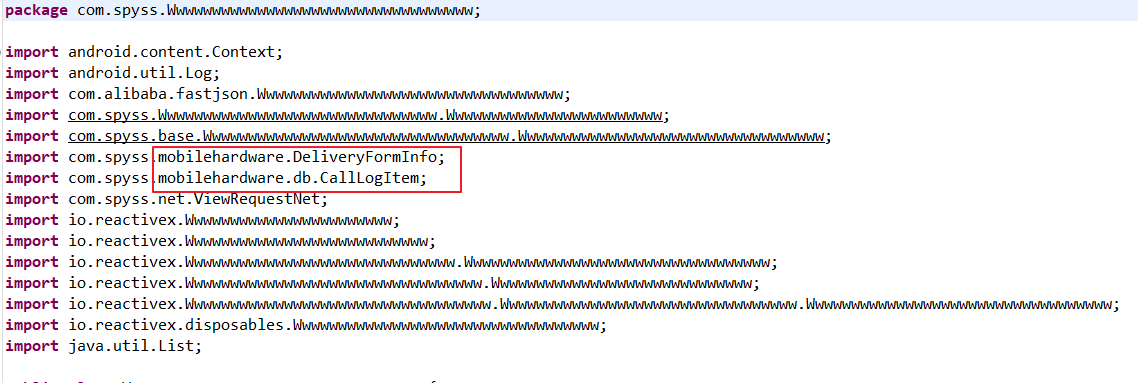
* com.spyss.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwwww.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww 분석

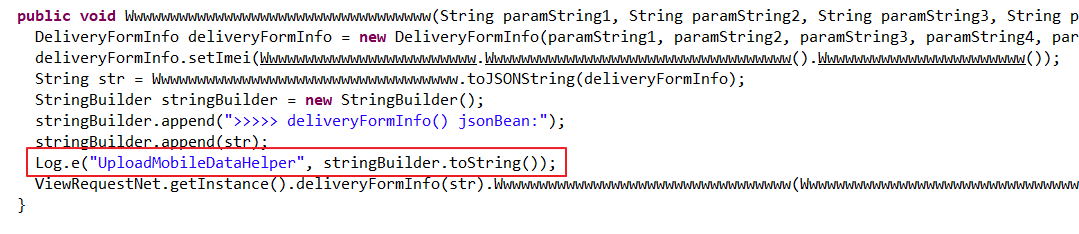






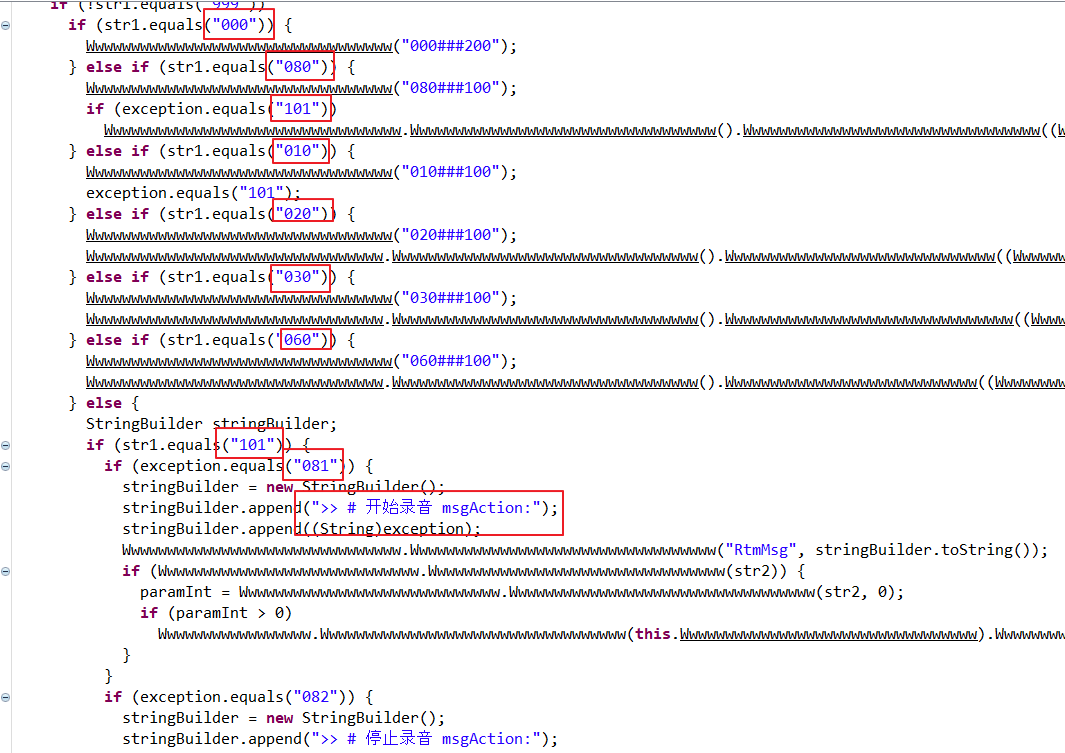
* com.spyss.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww 분석



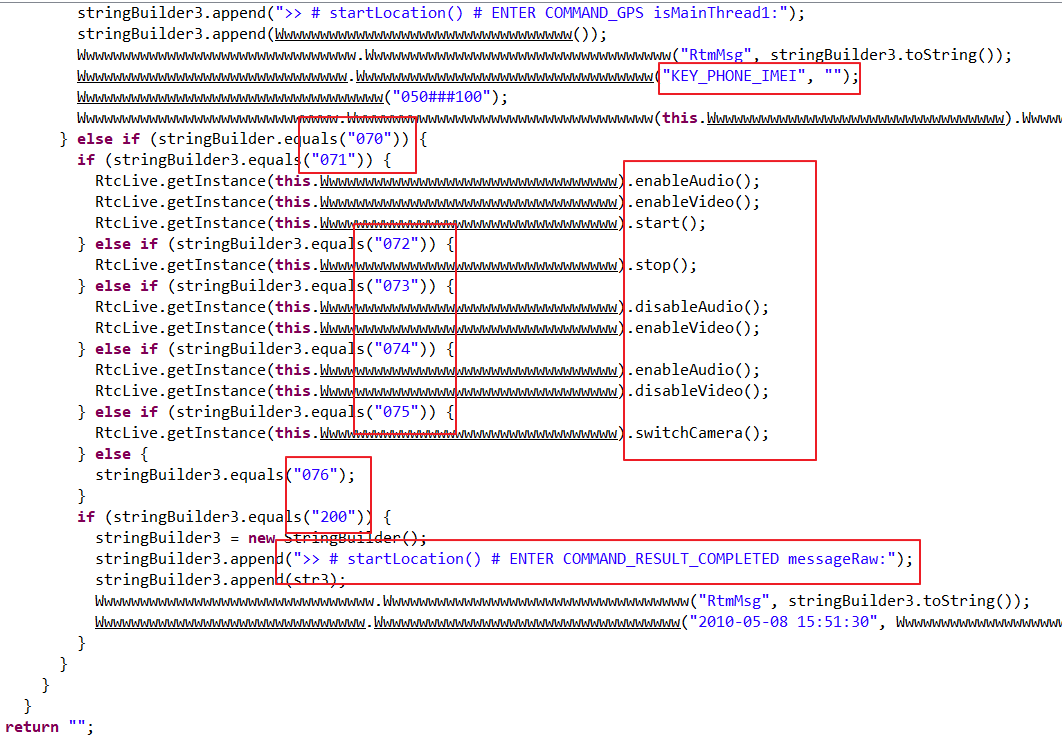


* com.spyss.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww 분석

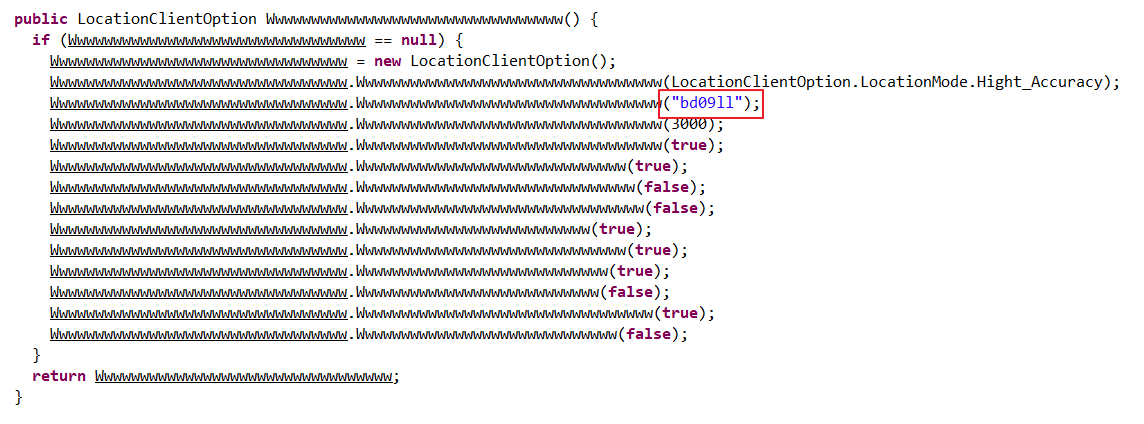








* com.spyss.baidus.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwww 분석

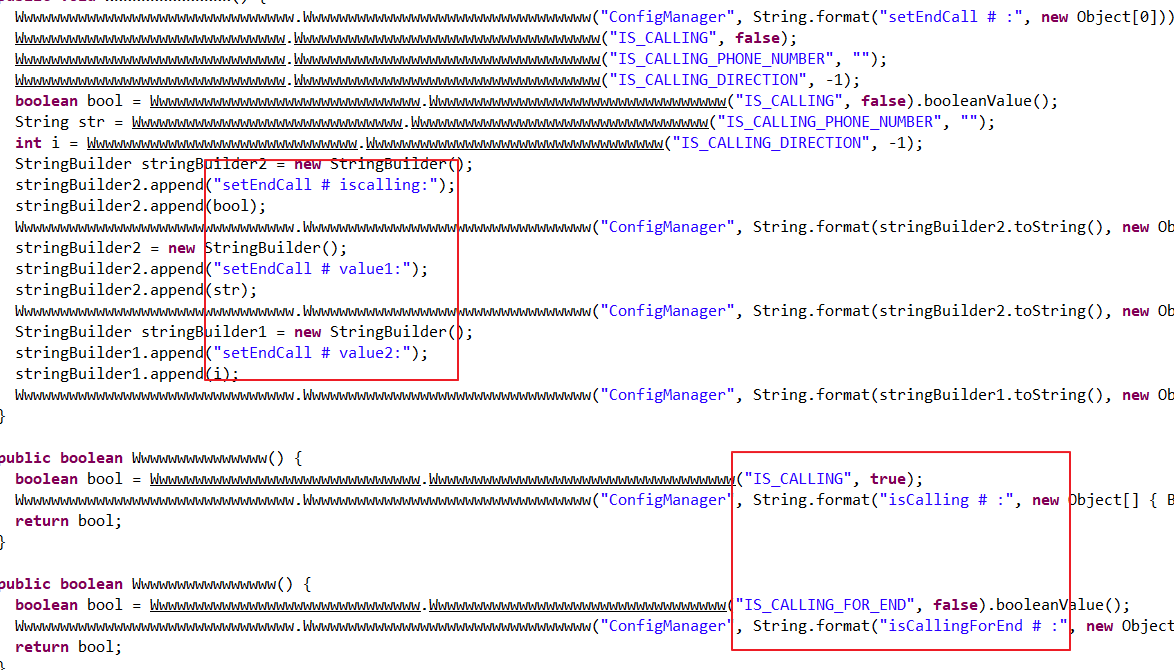




* com.spyss.base.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww 분석

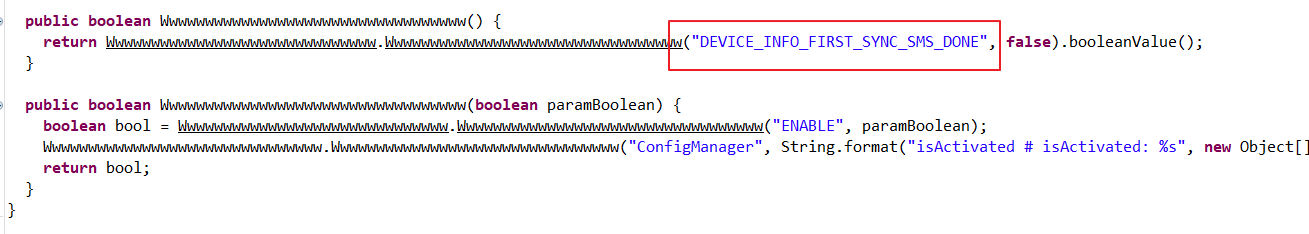




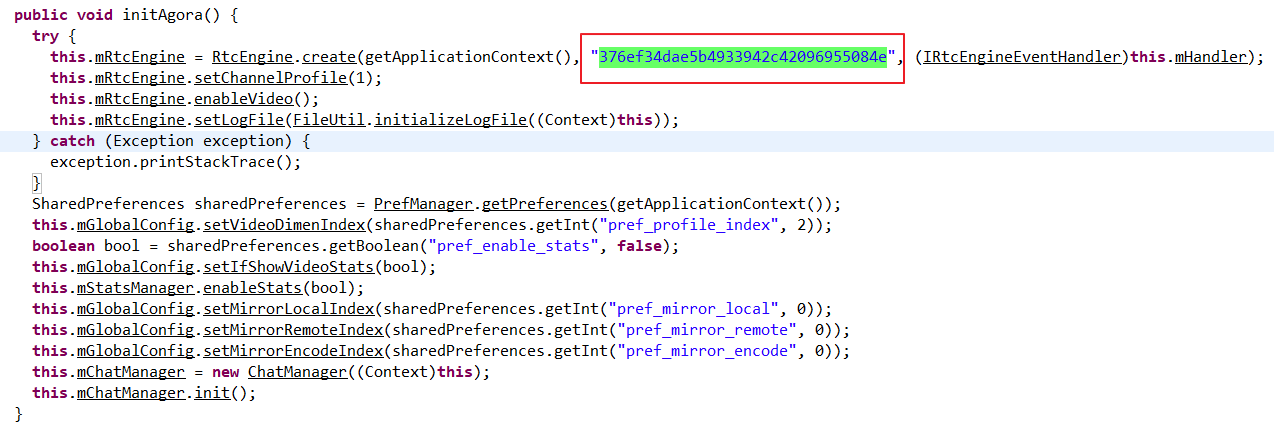






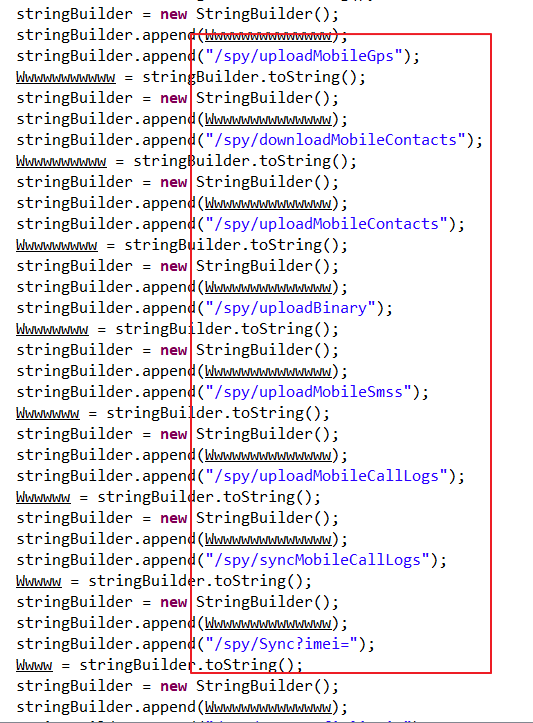


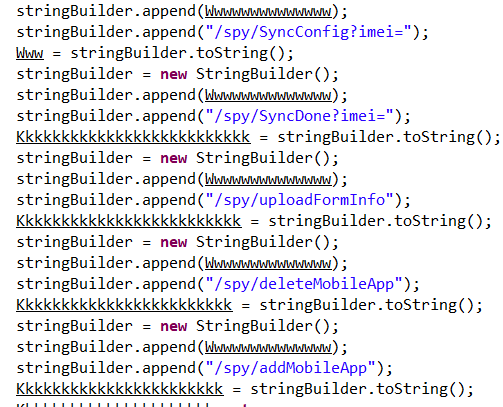
* com.spyss.base.BaseApp 분석



* com.spyss.base.Wwwwwwwwwwwwwwwwwwwwwwwwwwwww 분석



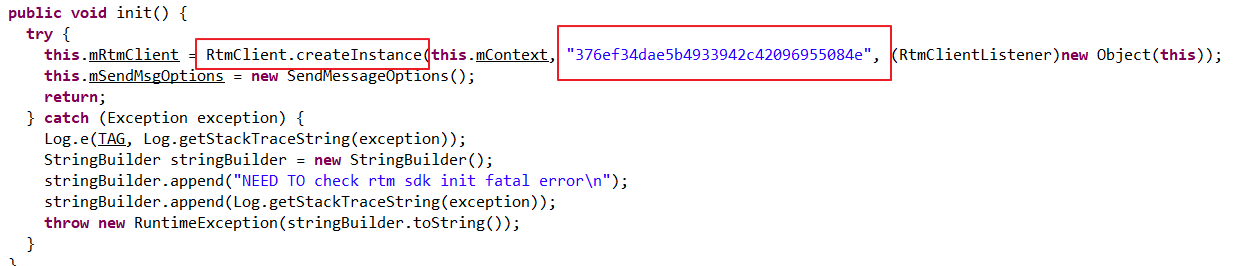




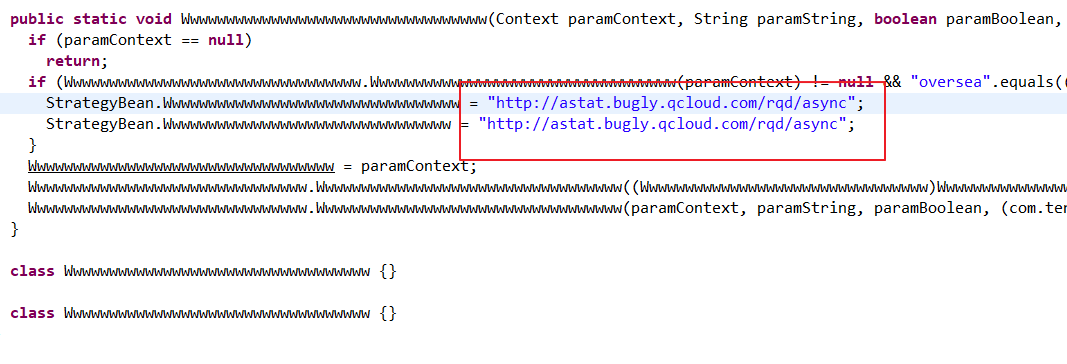




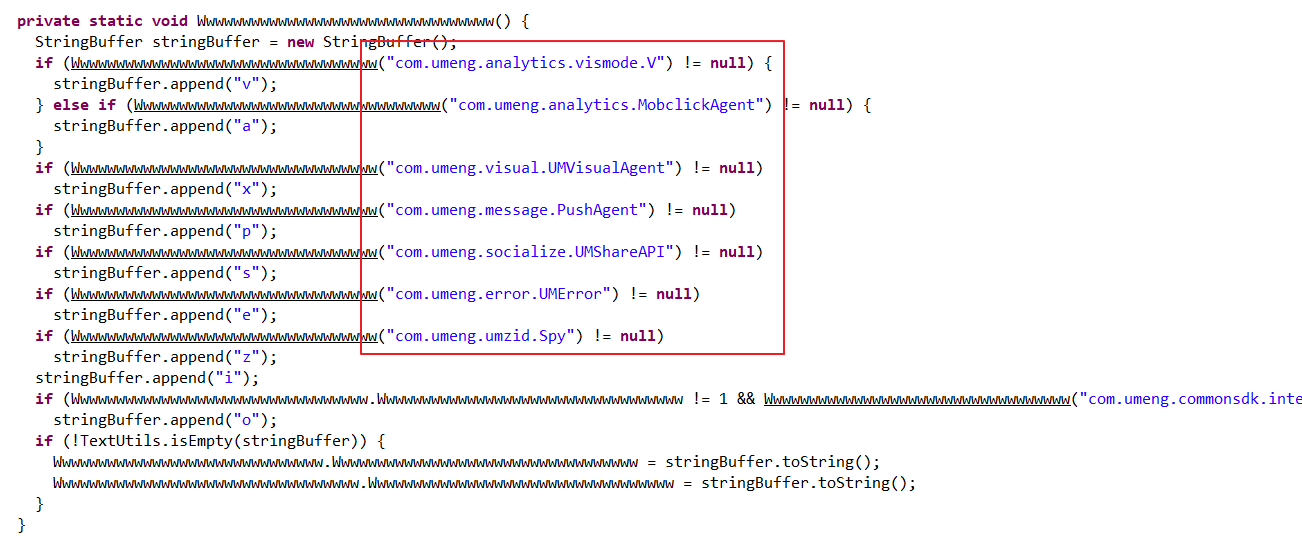
* com.spyss.openlive.rtmtutorial.ChatManager 분석



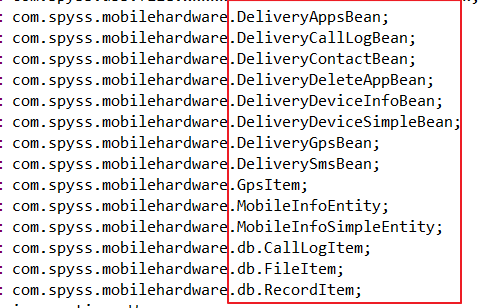
* com.tencent.bugly.crashreport.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww 분석

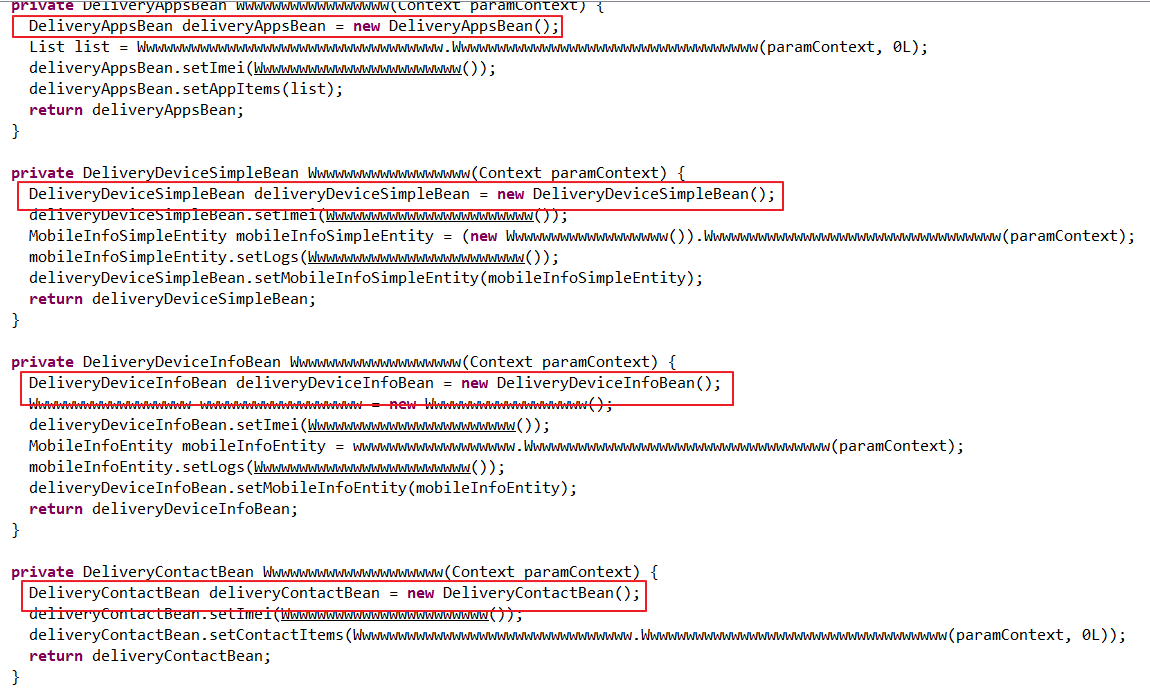


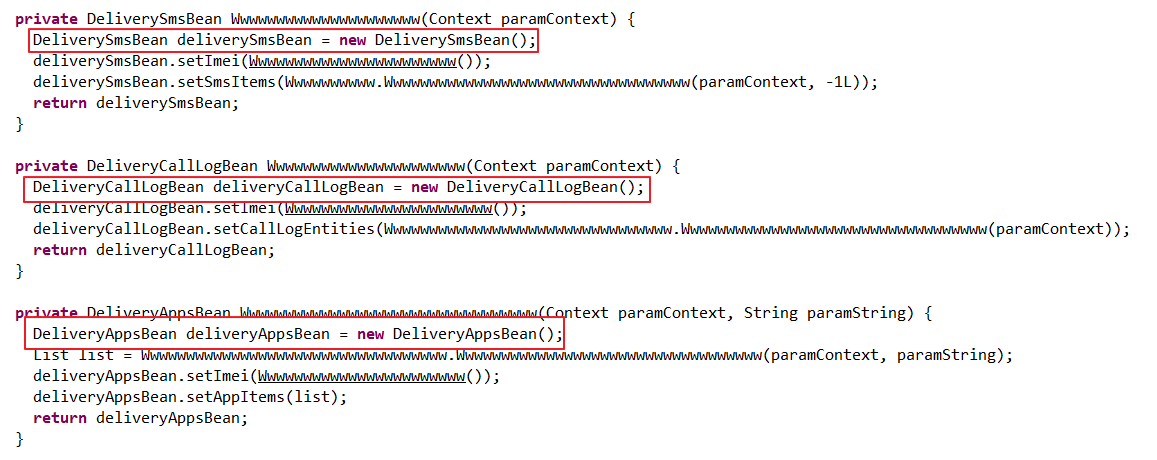
* com.umeng.commonsdk.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww 분석



* com.spyss.Wwwwwwwwwwwwwwwwwwwwwwwwwwwwwww.Wwwwwwwwwwwwwwwwwwwwwwww 분석







* **분석 결론 :** 
  + SMS(문자), CONTACTS(연락처)에 접근합니다.
  + uploadPicIsReady에서 사진을 업로드 함을 알 수 있습니다.
  + setCallLogEntities에서 전화한 사람들의 연락처를 알 수 있습니다.
  + GPS를 통해 삼각측량 위치를 알 수 있습니다. (본인의 기기 위치)
  + COTACT를 통해 연락처의 정보를 알 수 있습니다.
  + 사진 업로드 기능
  + 디바이스 정보 획득
  + 통화 기록 획득
  + 금융권 또는 기관의 전화번호로 통화 시 녹음되어 상대방에게 전달(금융정보, 개인정보 획득) 및 보이스피싱 기능
  + 원격에서 상대방이 녹음 제어 가능
  + 원격에서 상대방이 비디오 촬영 제어 가능 (카메라 방향 전환 가능)
  + 전화 도청 기능
  + 앱 삭제 기능
  + 앱 추가 기능
  + 연락처 추가 기능

**P.S. 해커가 업로드에 이용하는 의심 서버:**

* RtmClient.createInstance(this.mContext,"376ef34dae5b4933942c42096955084e", (RtmClientListener)new Object(this));