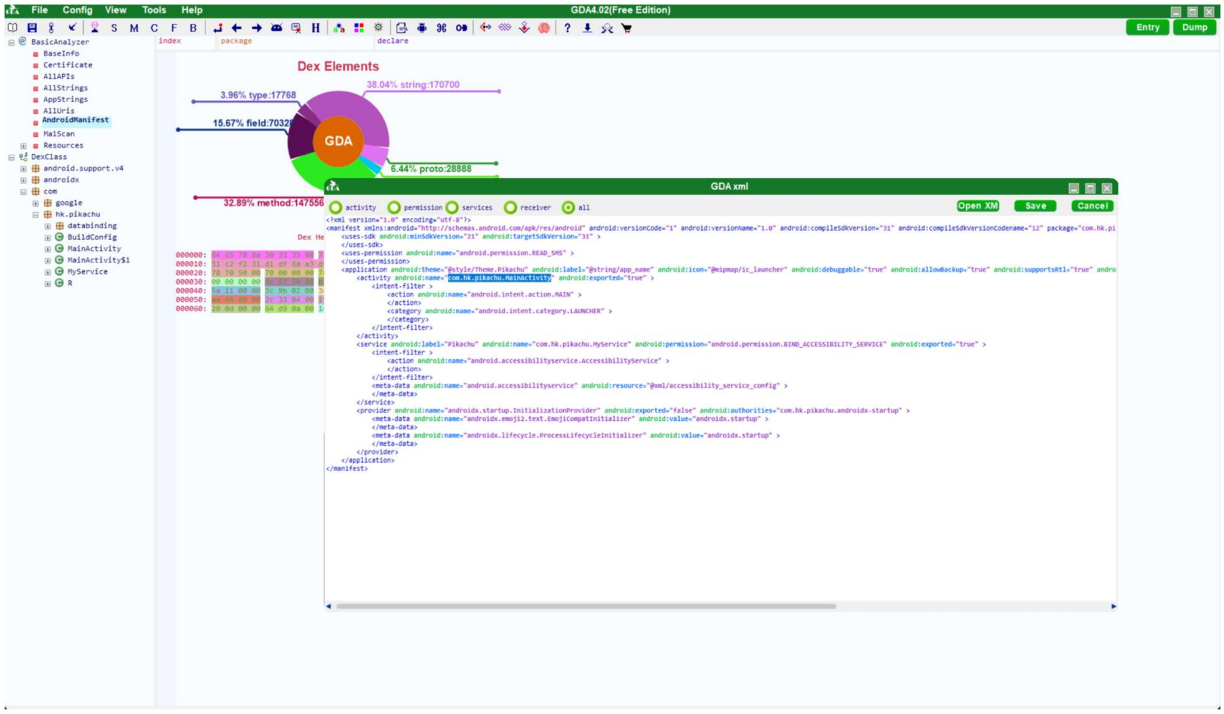
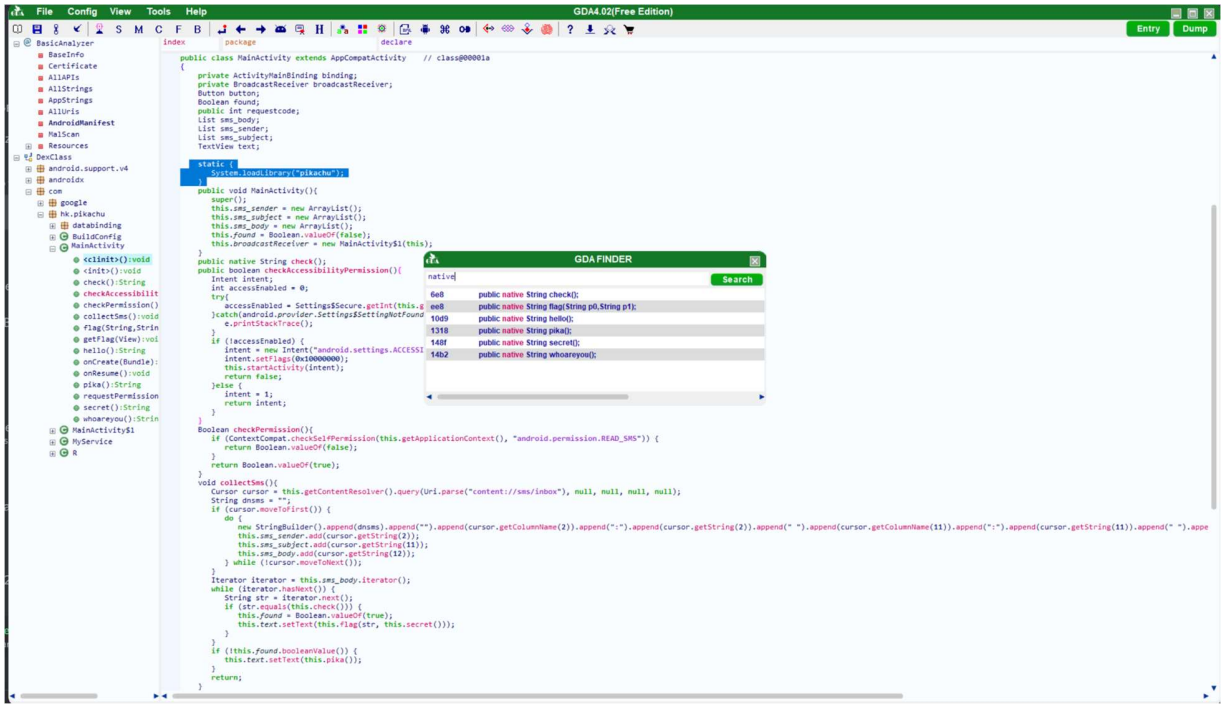
Pikachu

Verilen Pikachu.apk dosyasını GDA-android-reversing-Tool ile açıp inceledik, *AndroidManifest.xml*'den uygulamanın *com.hk.pikachu.MainActivity* aktivitesini çalıştırdığını gördük.



AndroidManifest.xml

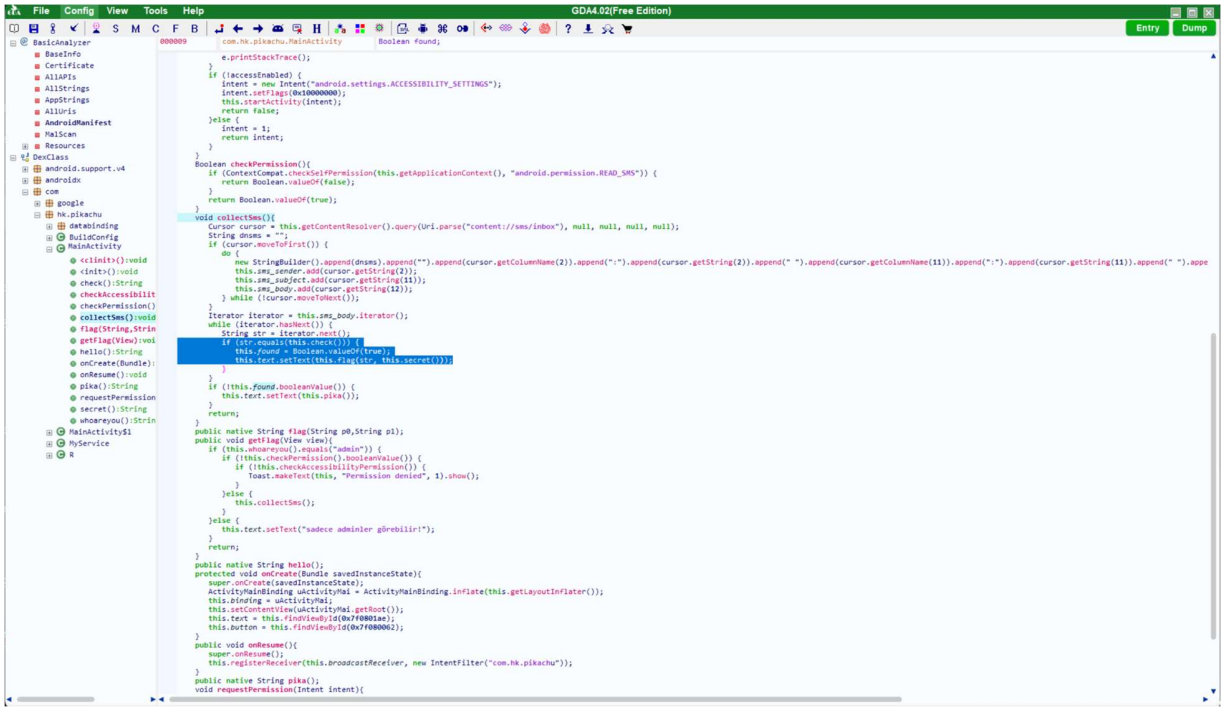
com.hk.pikachu.MainActivity classının *pikachu* isimli paylaşılan objeyi yüklediğini ve bu objeden *check, flag, hello, pika, secret* ve *whoareyou* olmak üzere 6 adet native metot tanımlandığını gördük.



pikachu paylaşılan objesi

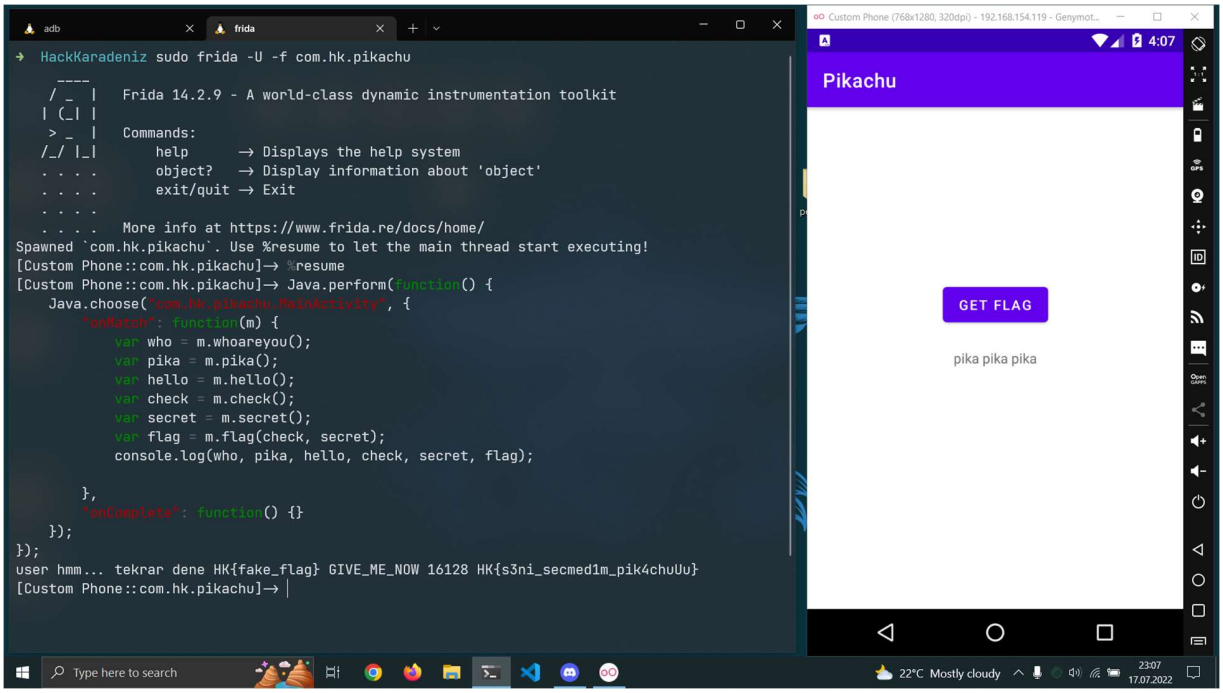
Bu aşamada apk dosyasını ayıklayıp, içerisinden *lib/* klasörü altındaki *libpikachu.so* dosyalarını inceleme yoluna gidebilirdik ancak bunun yerine, aktif uygulama üzerinden Frida kullanarak kodu direk çağırmanın daha kolay olacağına kanaat getirdik.

Tanımlanan bu native metotların uygulamada nasıl çağrıldığını görmek için kodu inceledik. *collectSms* metodunun gelen kutusundaki kısa mesajları okuyup *check* metodu ile karşılaştırdığını eğer bulursa, *secret* metodunun döndürdüğü değer ile birlikte *flag* metodunu çağırdığını ve sonucunu da ekrana yazdırdığını gördük.



collectSms metodunun flag metodunu çağırması

Uygulamayı Genymotion emulatorüne yükledik ve Frida ile açtık. *Java.choose* metodu ile aktif *com.hk.pikachu.MainActivity* instance'larını aradık, bulduğumuz instance'lar üzerinde native metodları çağırarak çıktılarına baktık, son olarak da *flag* metodunu *check* ve *secret* metodlarının çıktıları ile çağırarak bayrağı elde ettik.



Frida bayrak