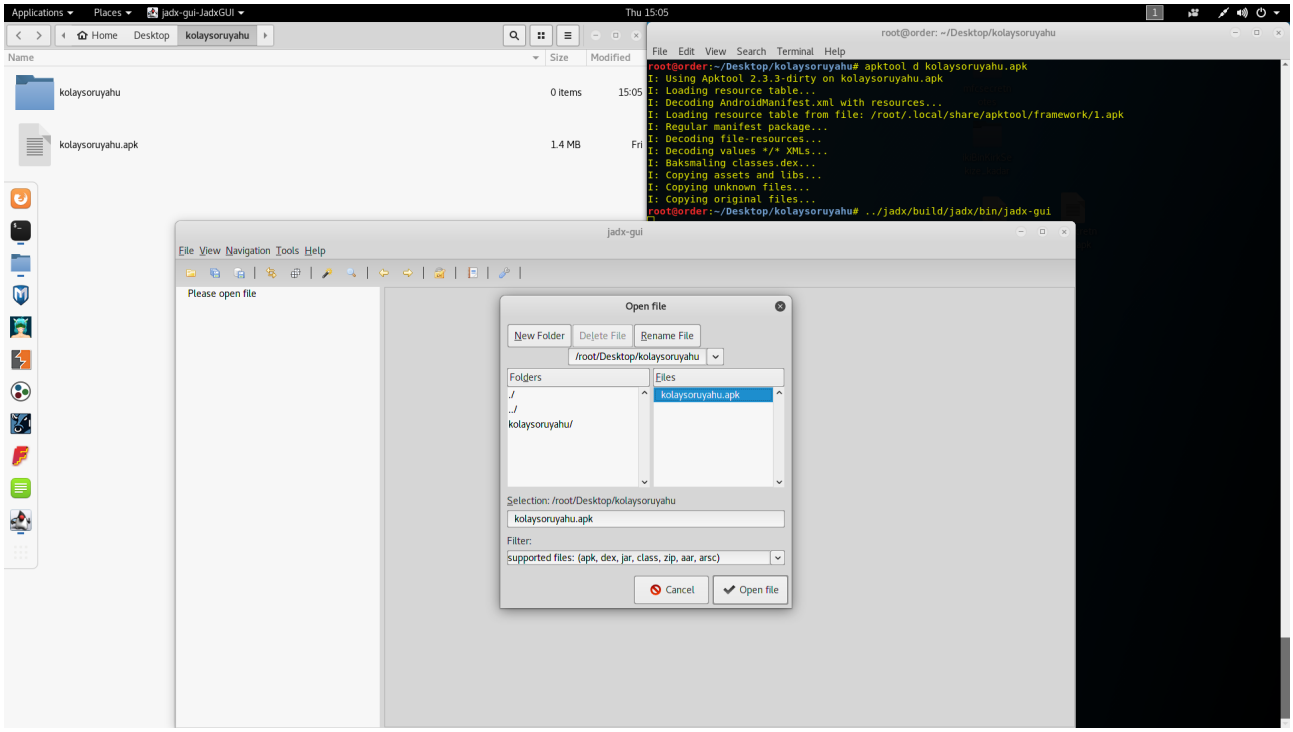
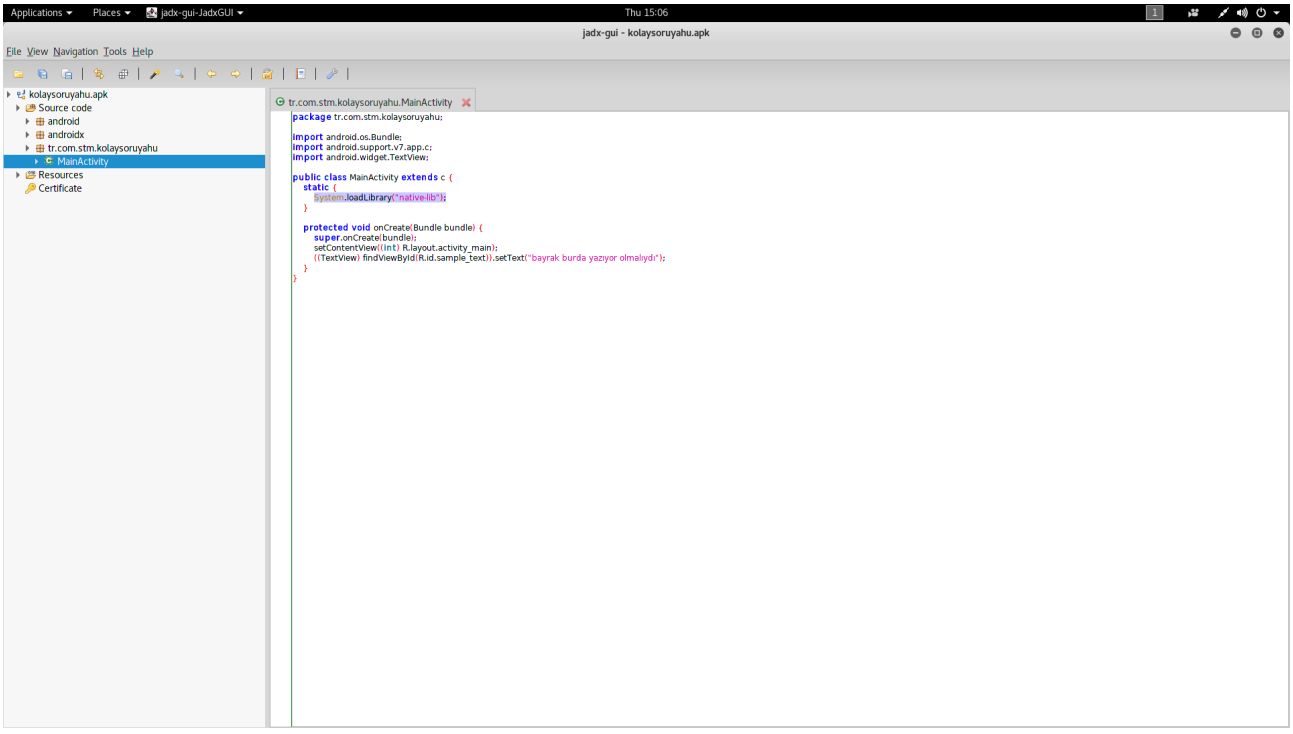
STM CTF MOBILE WRITEUP

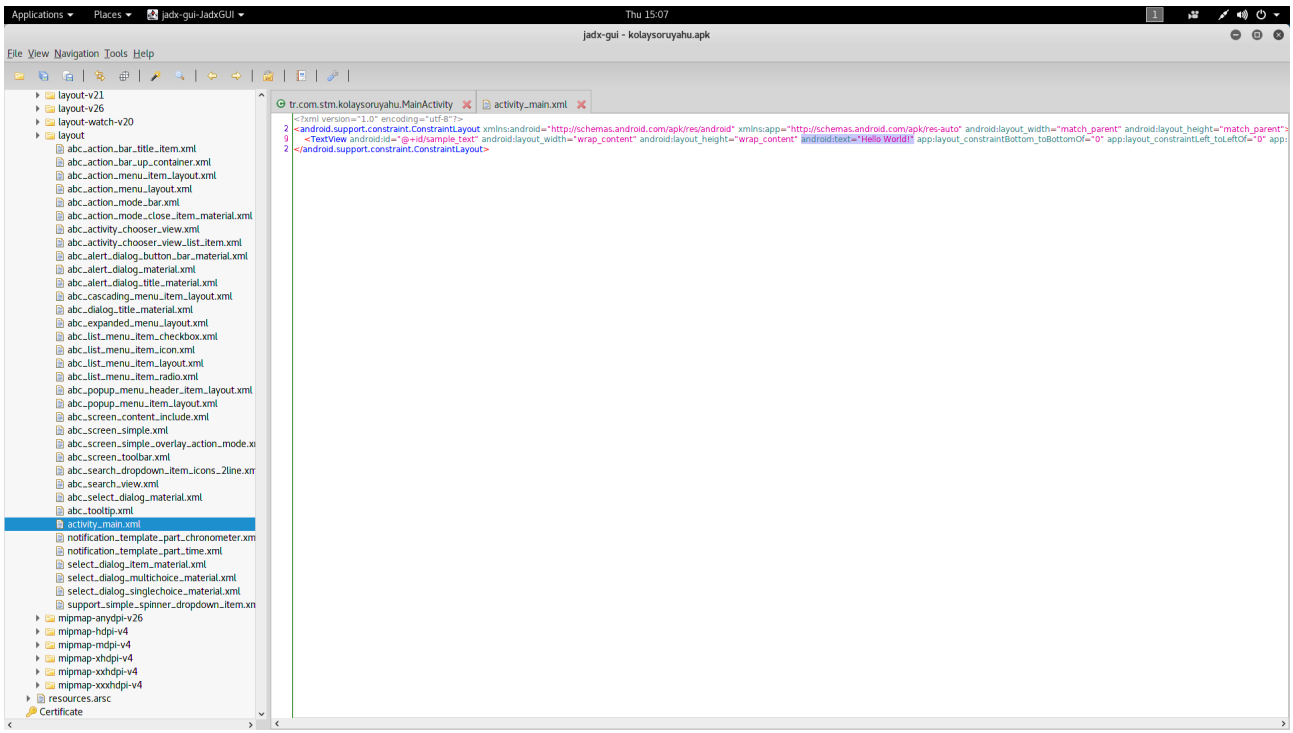
Soru 1

Apk'yı "**Apktool d kolaysoruyahu.apk**" komutu ile çıkardım.

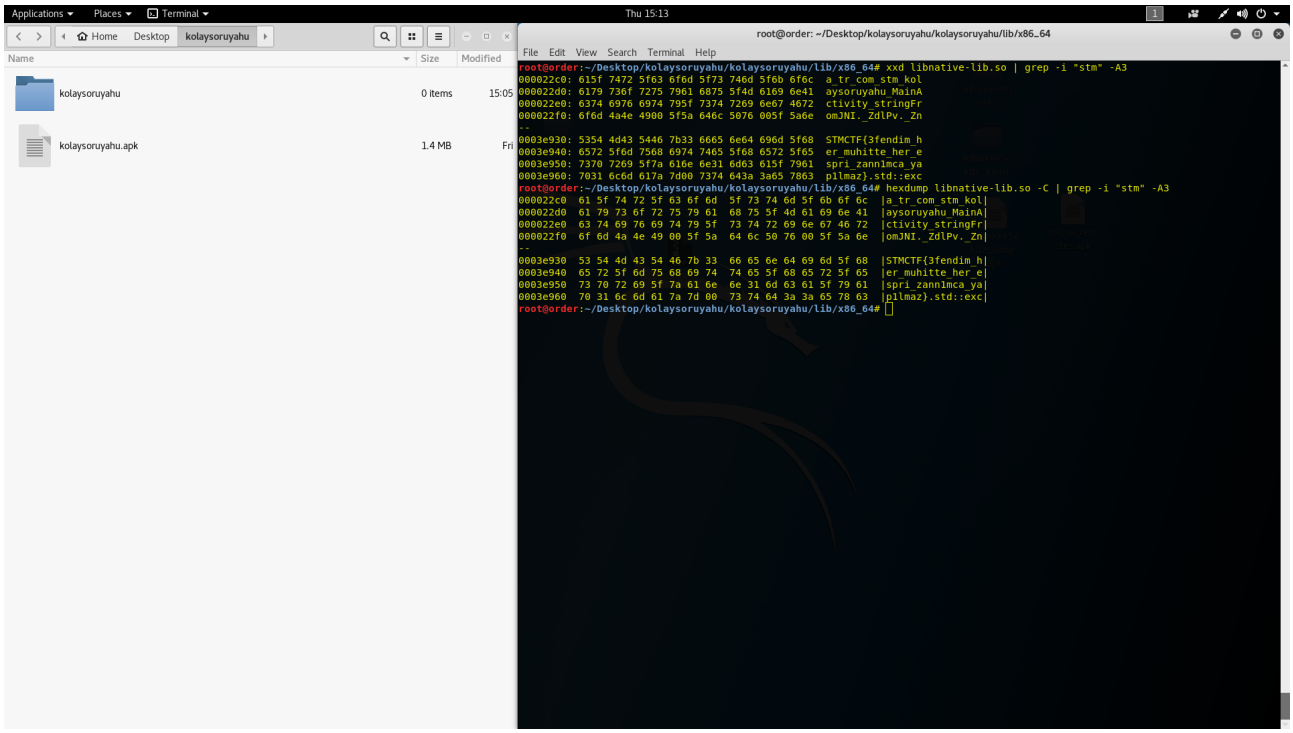


Çıkardığım Apk'yı Jadx-gui programı ile açtım ve içinde bulunan decompile edilmiş koda göz gezdirirken bayrak burda yazıyor olmalıydı yazısına denk geldim. Aklıma öncelikle layouta bakmak geldi. Layout'da flagi göreyemeyince ve görünürde native library olduğu için sıra native library'ye bakmaya geldi.



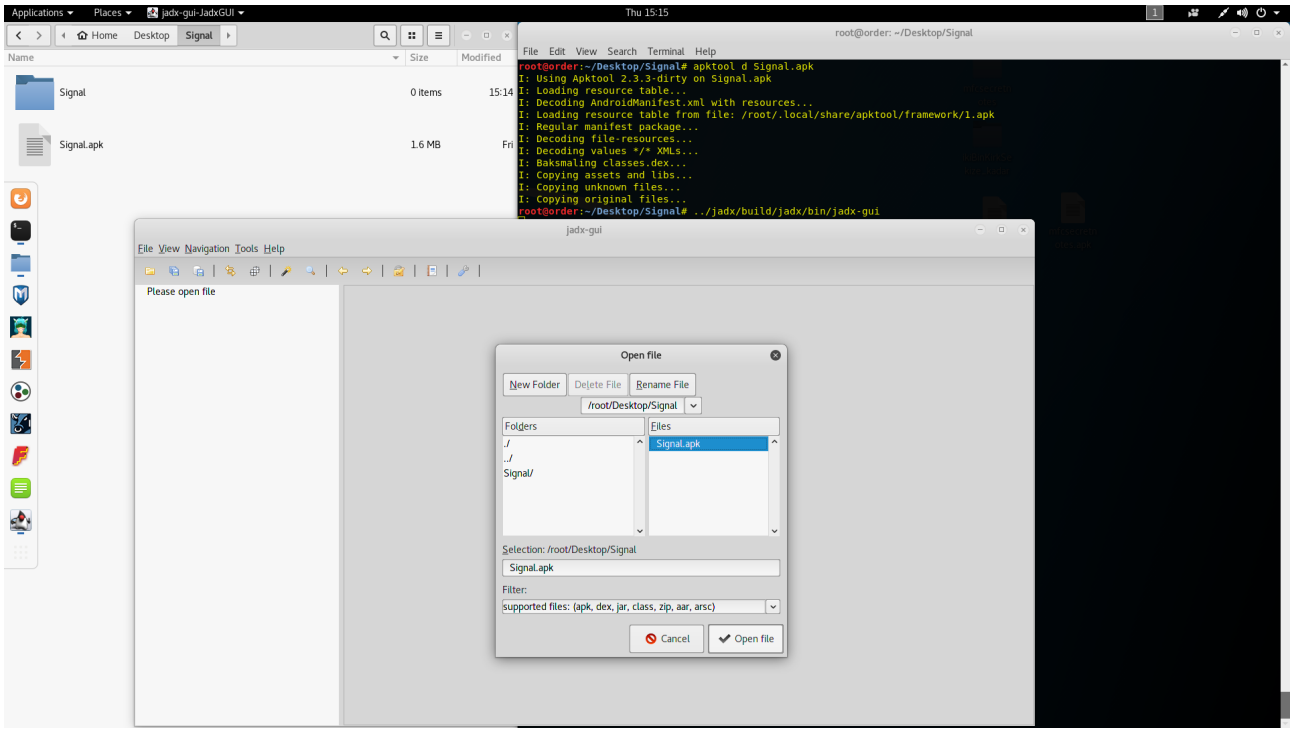


2 farklı komut ile sorunun cevabını aşağıdaki şekilde bulduk.

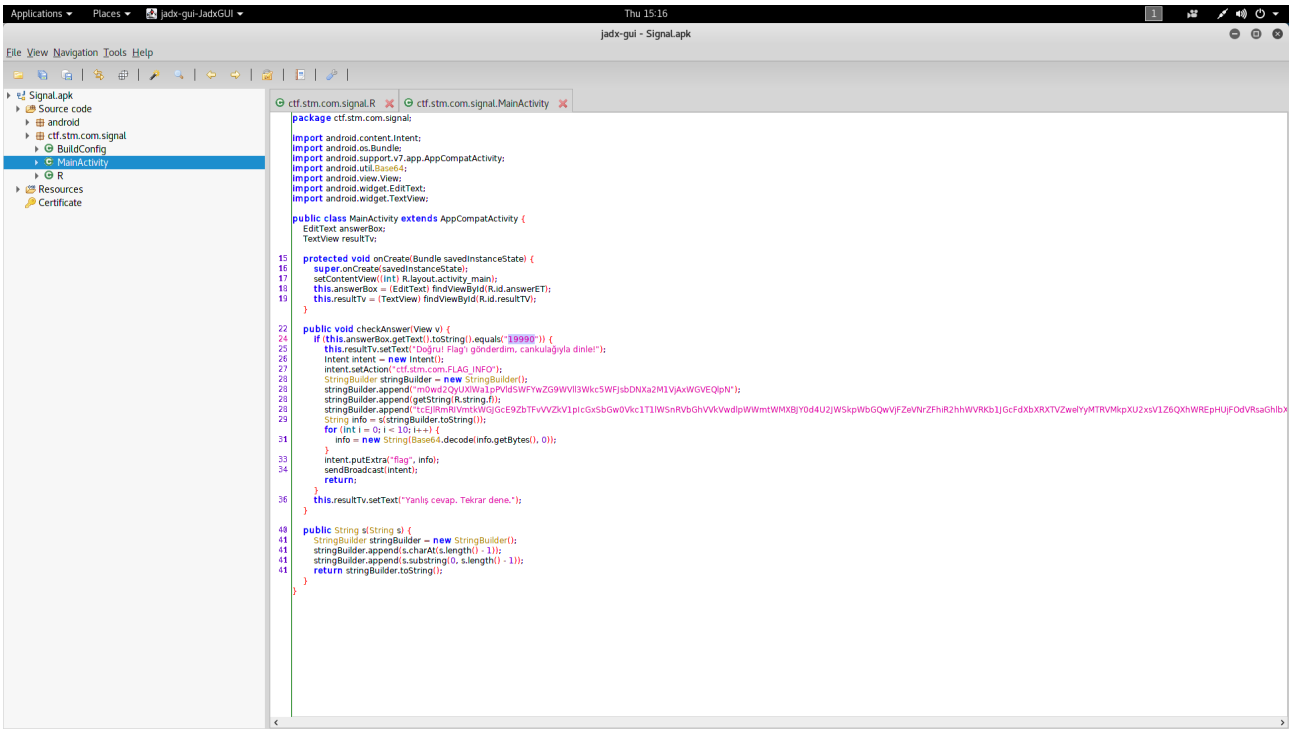


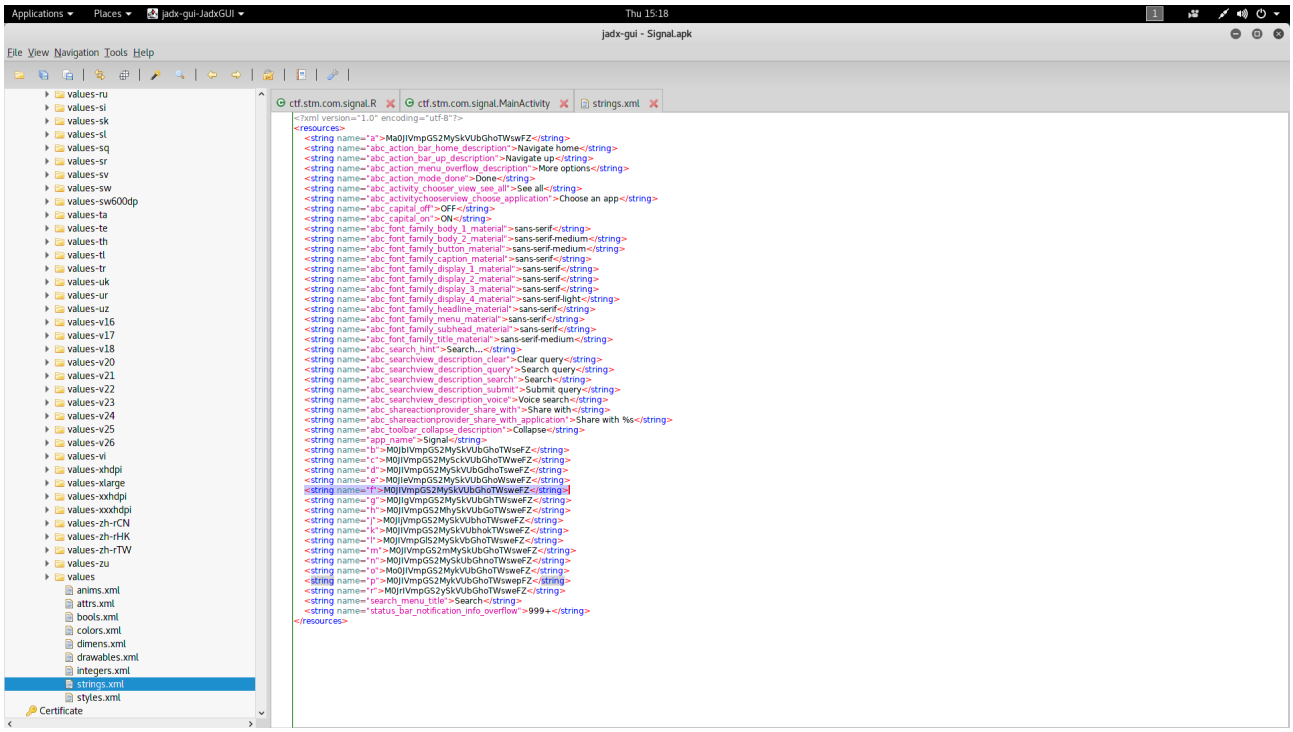
Soru 2

Aynı ıvır zıvır gene devam apk açıldı jadx veya jdgui ile decompile edildi.



Apk'nın içini açtığımda ilk gördüğüm String builder ile yapılmış bir kaç işlem.





Öncelikle bu soruyu çok farklı şekillerde çözebilirsiniz.

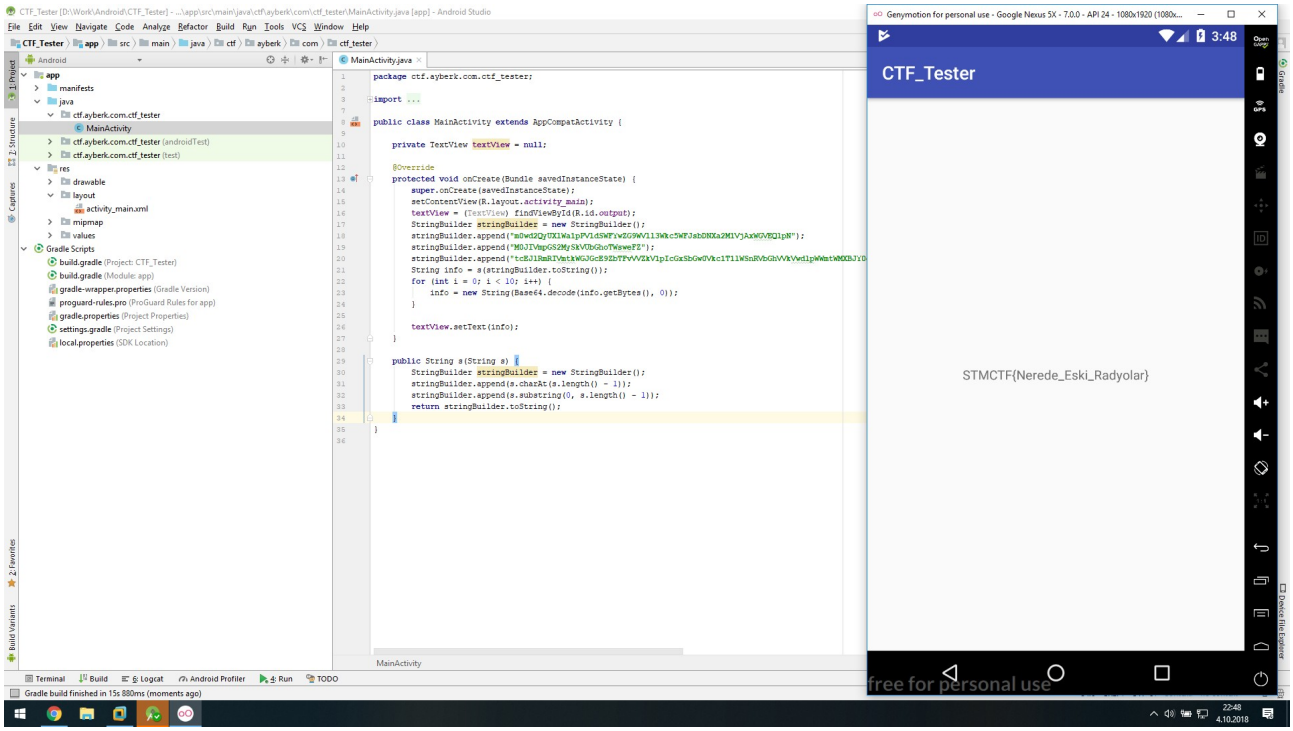
1- Aynı kodu hazır bulunan projenizde çalıştırıp sonuca ulaşabilirsiniz

2- Kodu yeteneğe göre göz veya kalem ile 3 5 dk'de çözebilirsiniz.

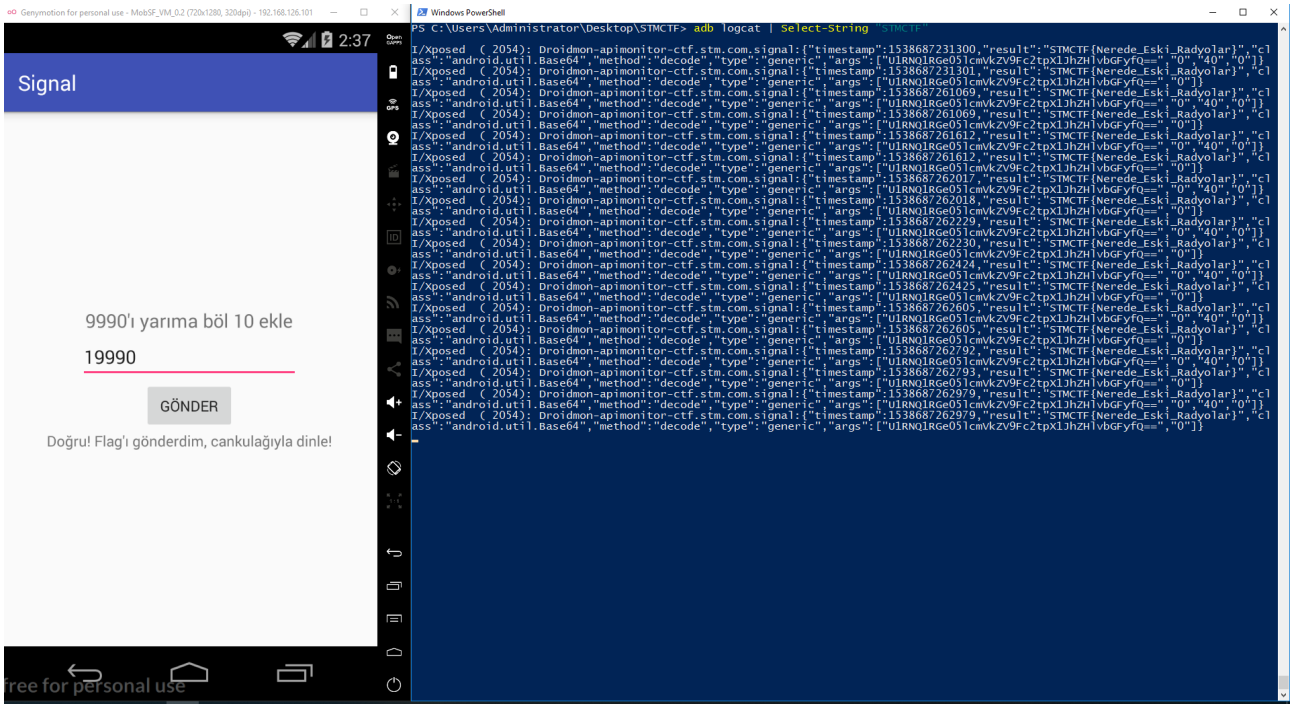
3- Sorunun adı dinlemeli olduğu için logları dinleyebilirsiniz.

Ben burada 2 yönteminde sslerini paylaşayım hangisi kolayına gelirse :)

Öncelikle elimde her zaman hazır olan ve 1 adet textview içeren(textview'ı output olarak kullanıyorum istersen log kullan keyif meselesi) android uygulaması. Decompile edilmiş kodu aynen kopyala yapıştır çalıştır sonucu gelsin.

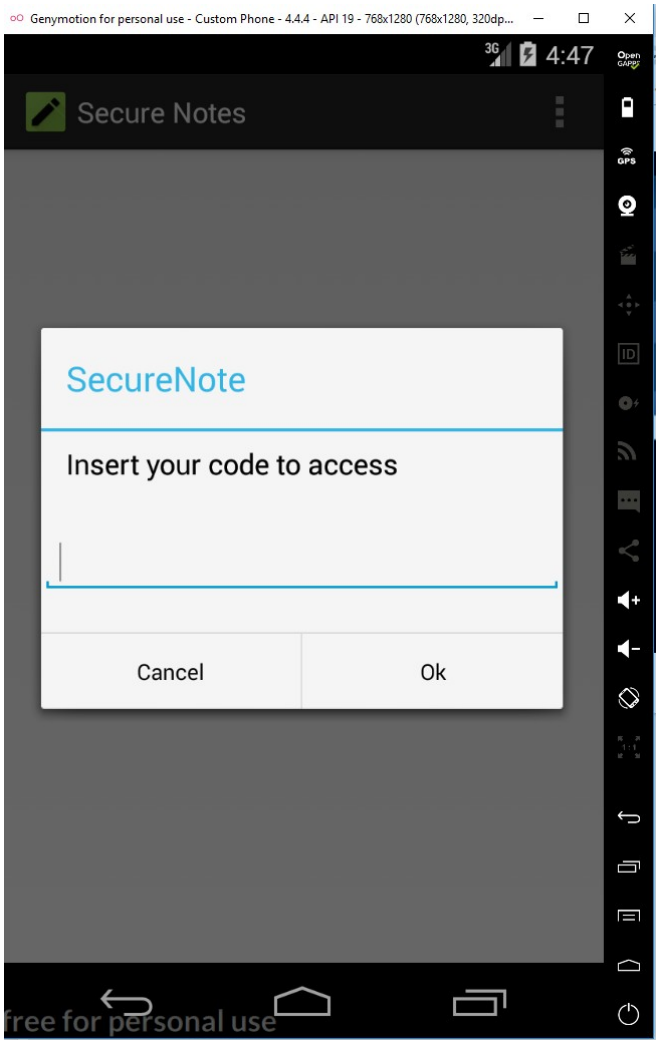


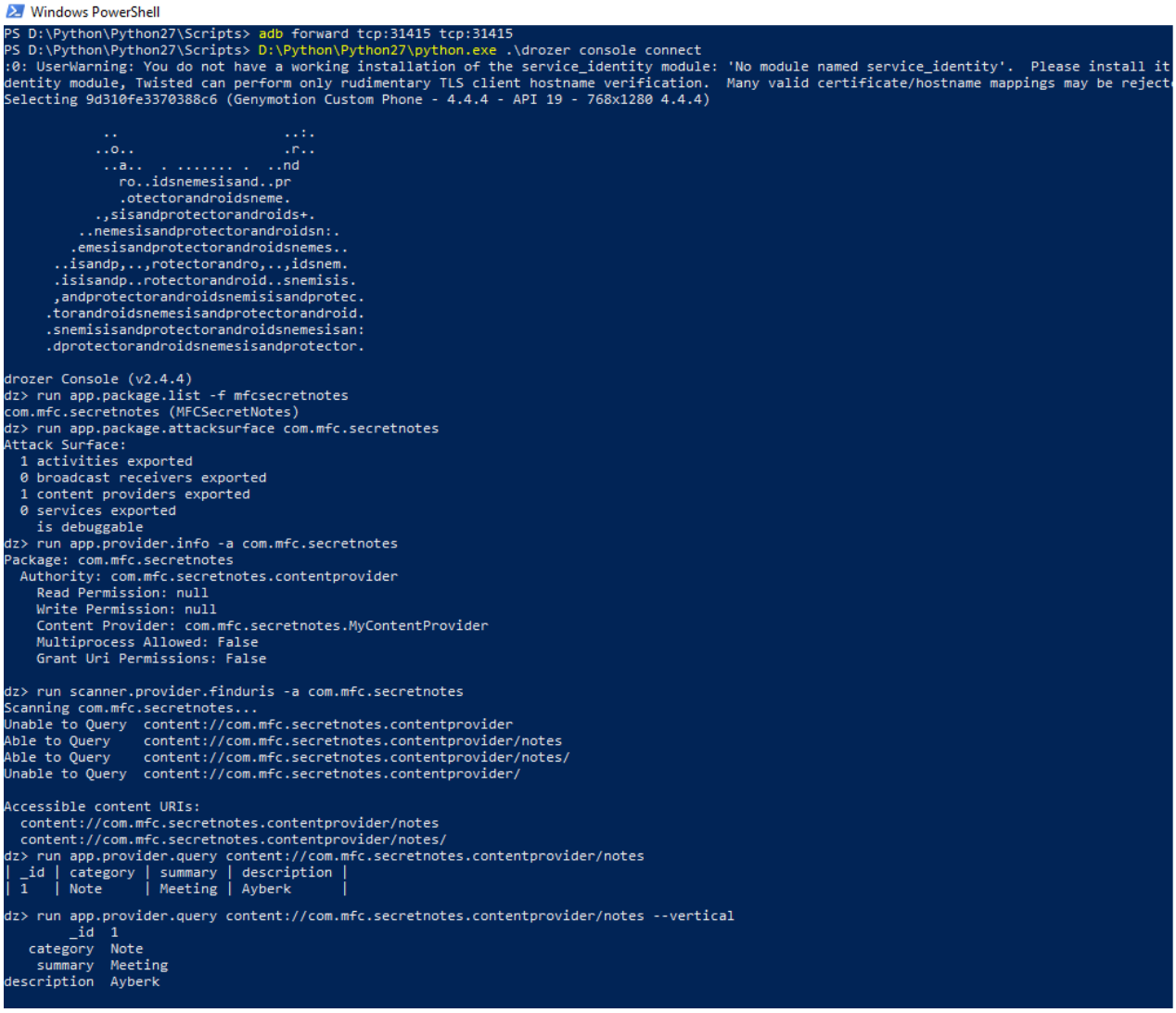
Burada ise logları dinliyorum arkadaş zaten hazır olarak gönderiyor :(

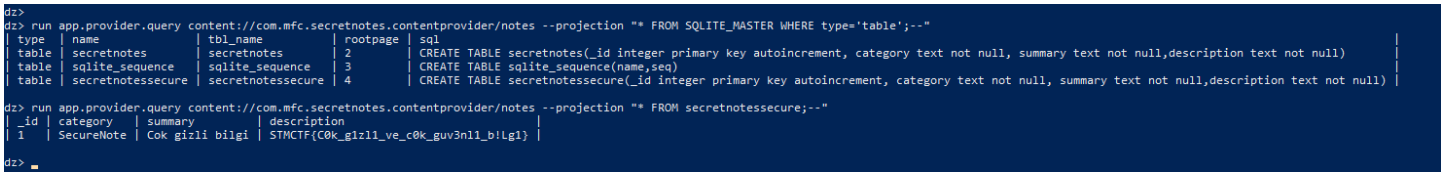


Soru 3

Arkadaşlar bu soruda klasik provider problemlerinden bir tanesini içermekte drozer adlı programı kullanarak ortalama 3-5 dk içinde çözebilirsiniz.
Uygulamayı yükledim apk'yı açtım oraları atlıyorum. Manifeste baktığımda export edilmiş provider olduğunu gördüm. Bu sebep ile aşağıdaki tool'u kullanıp flagi elde ettim.







Şimdilik bu kadar, buraya kadar dayanıp okudu isen saygılar :)
Ayberk