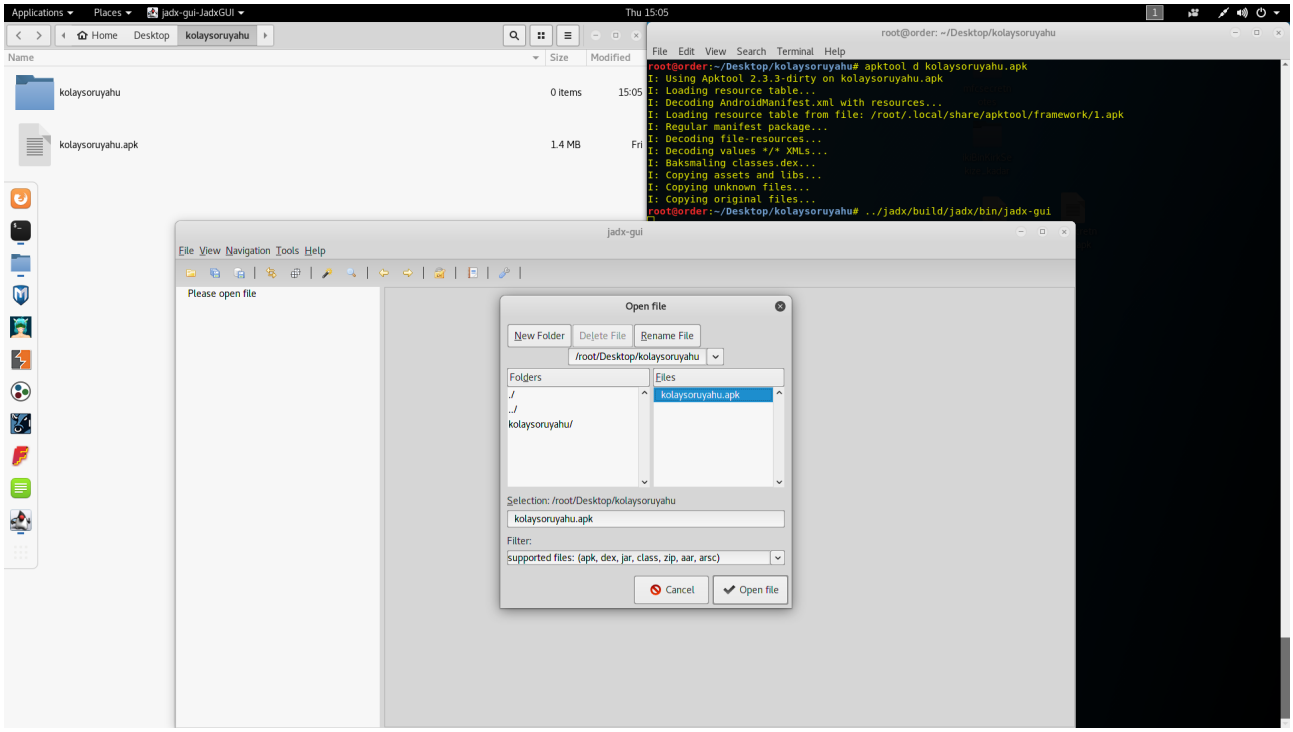
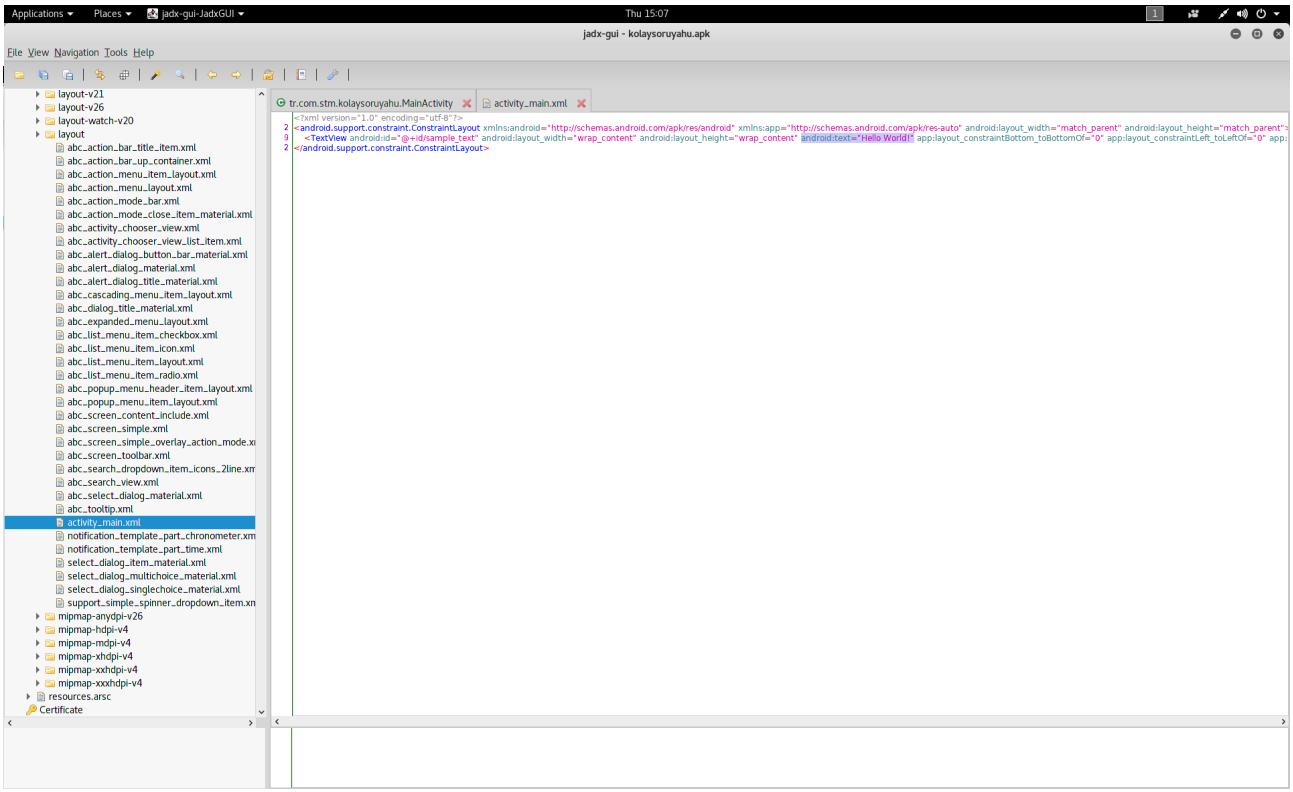
STM CTF MOBILE WRITEUP

Soru 1

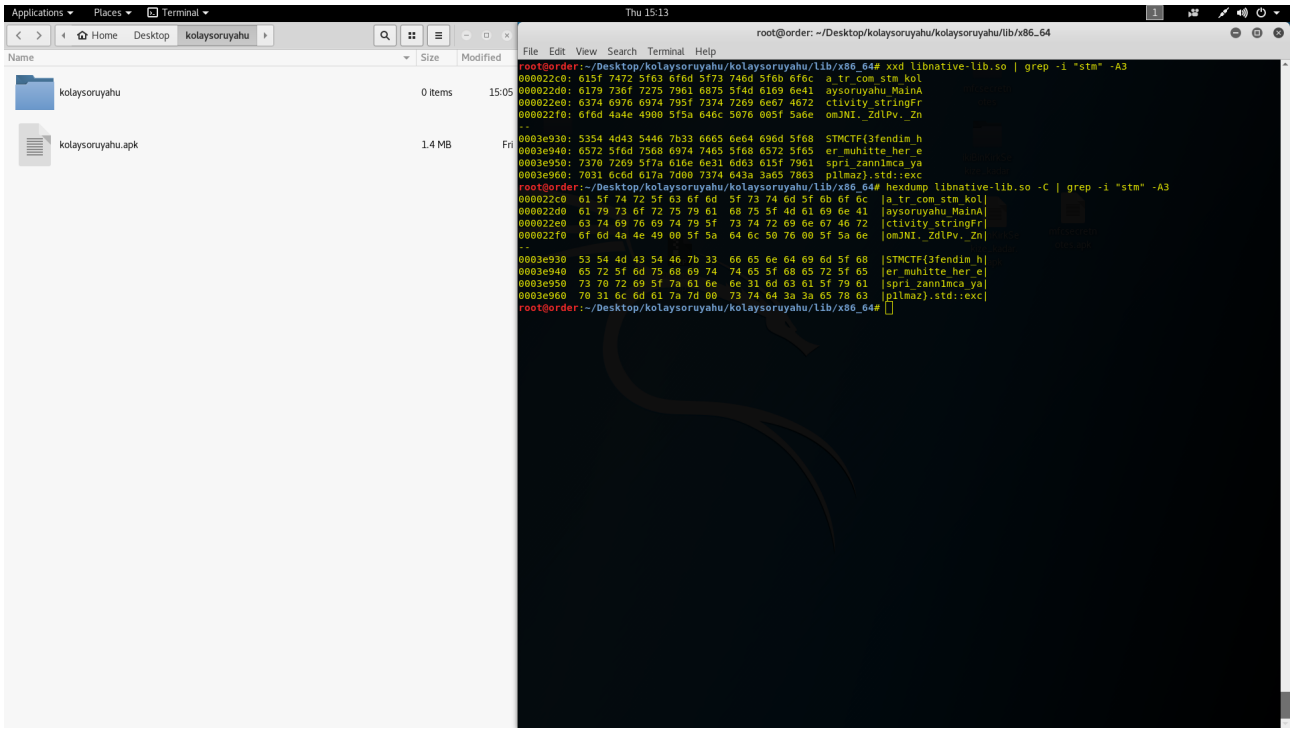
Apk'yı "Apktool d kolaysoruyahu.apk" komutu ile çıkardım.



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.

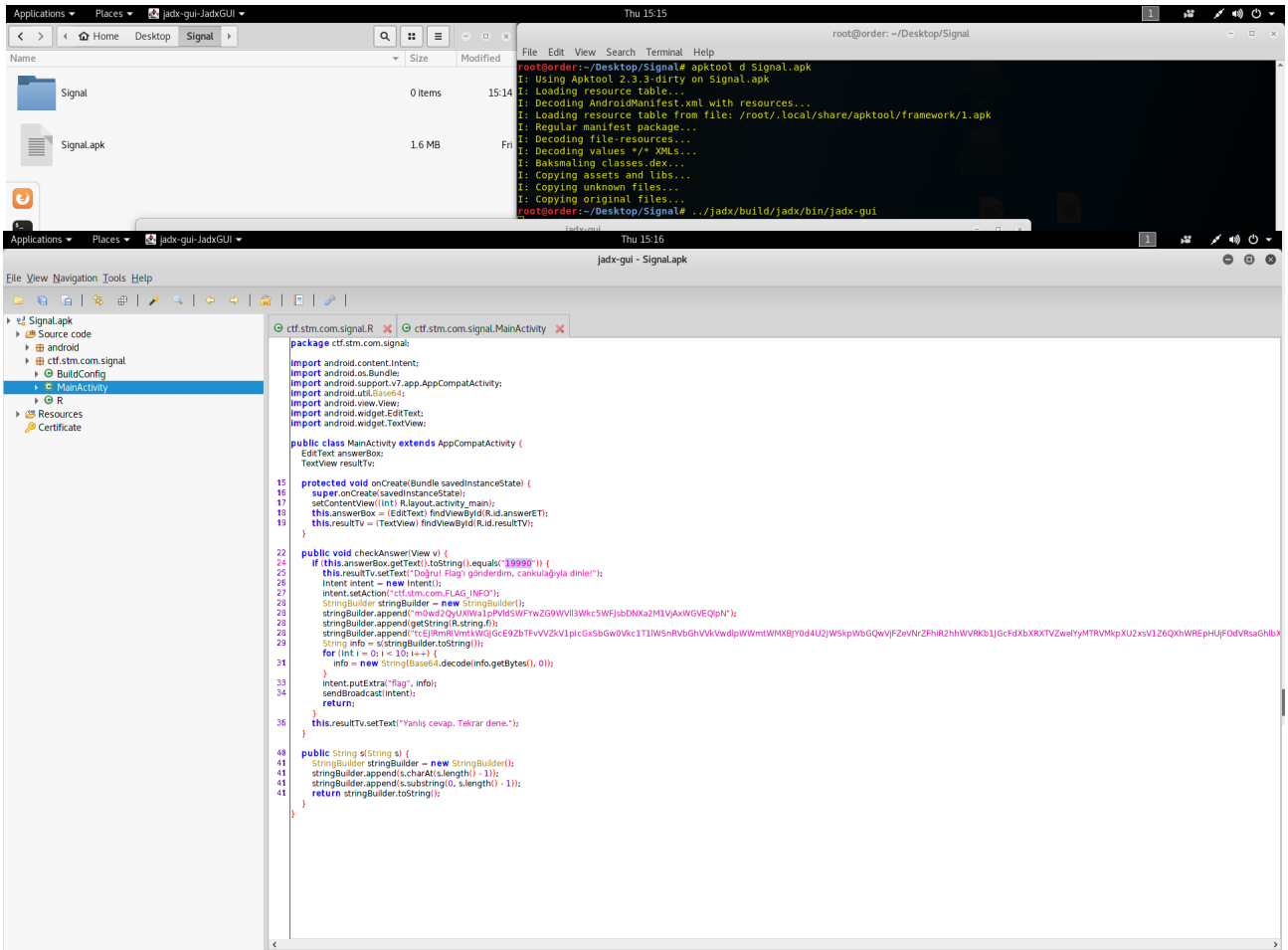


2 farklı komut ile sorunun cevabını aşağıdaki şekilde bulduk.

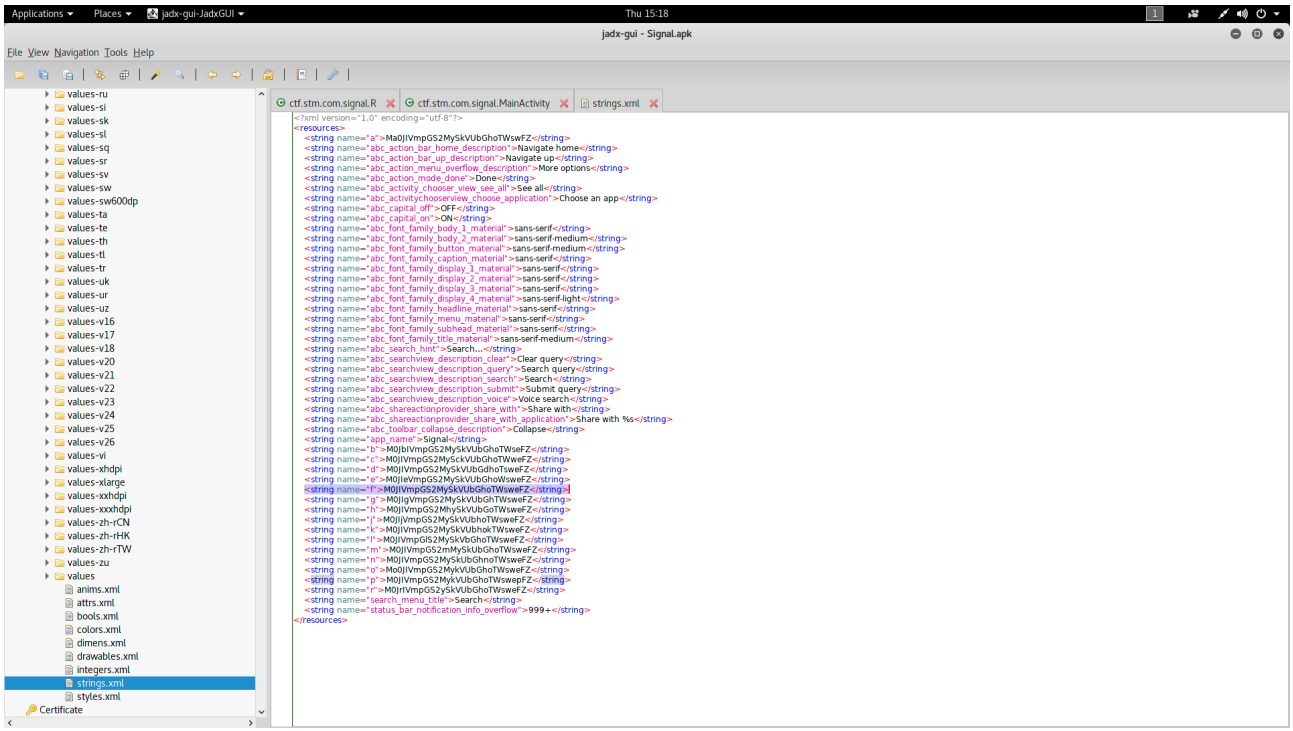


Soru 2

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



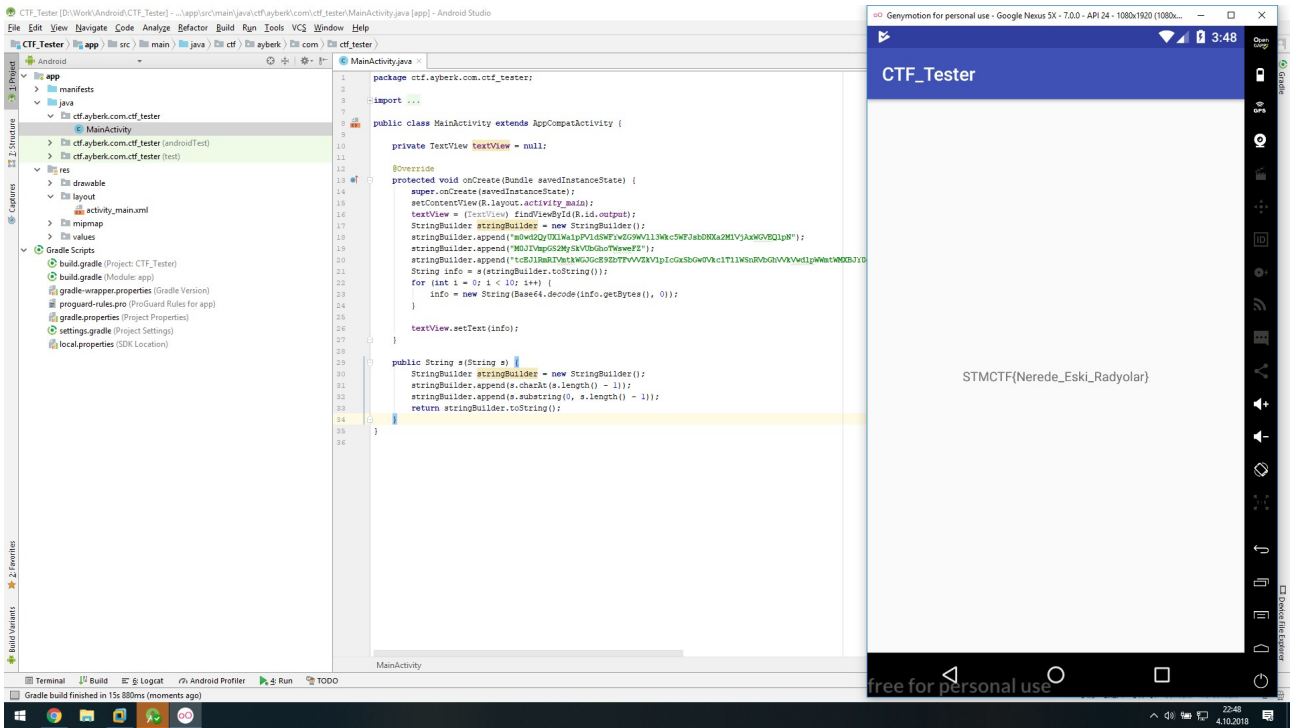
Apk'nın içini açtığımda ilk gördüğüm String builder ile yapılmış bir kaç işlem.



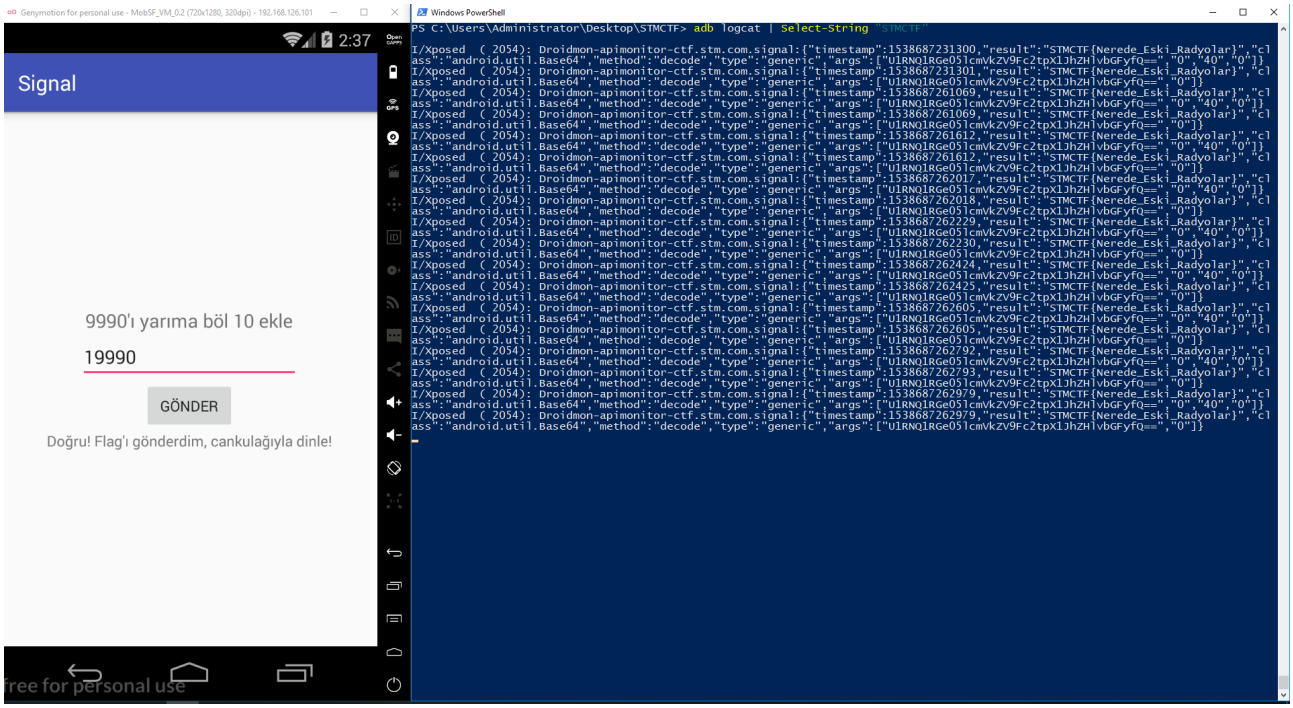
Öncelikle bu soruyu çok farklı şekillerde çözebilirsiniz.
1- Aynı kodu hazır bulunan projenizde çalıştırıp sonuca ulaşabilirsiniz
2- Kodu yeteneğe göre göz veya kalem ile 3 5 dk'de çözebilirsiniz.
3- Sorunun adı dinlemeli olduğu için logları dinleyebilirsiniz.
4- Smali değiştirip yeniden paketleyebilirsiniz.

Ben burada 2 yönteminde sslerini paylaşayım hangisi kolayına gelirse :)

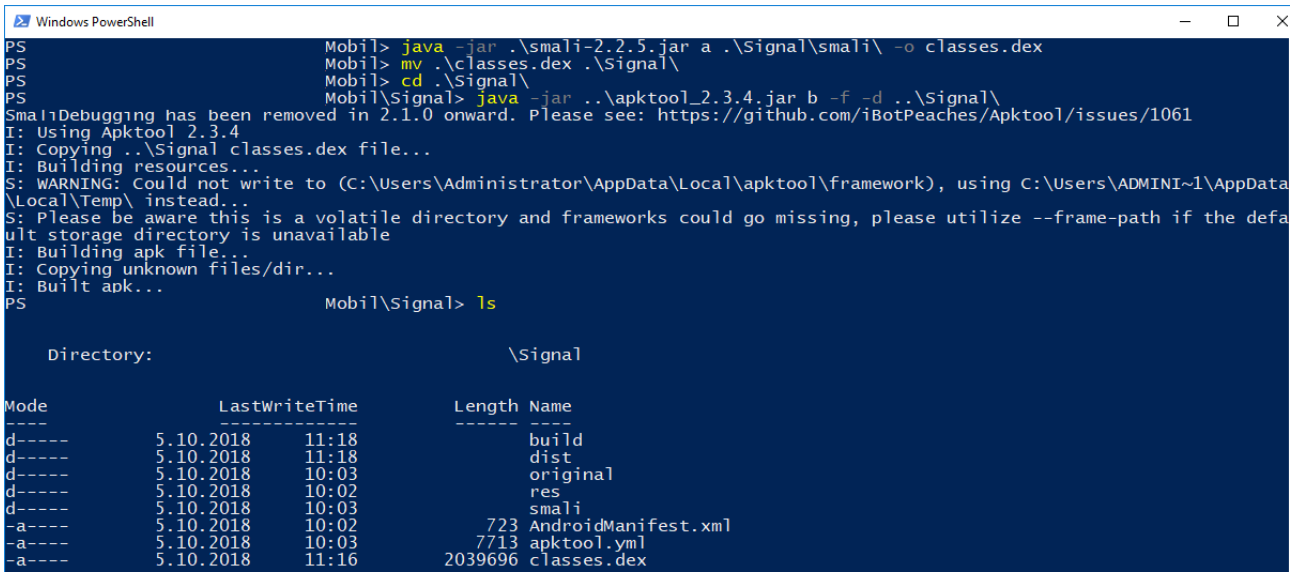
Öncelikle elimde her zaman hazır olan ve 1 adet textview içeren(textview'ı output olarak kullanıyorum istersen log kullan keyif meselesi) android uygulaması. Decompile edilmiş kodu aynen kopyala yapıştır çalıştır sonucu gelsin.



Burada ise logları dinliyorum arkadaş zaten hazır olarak gönderiyor :(

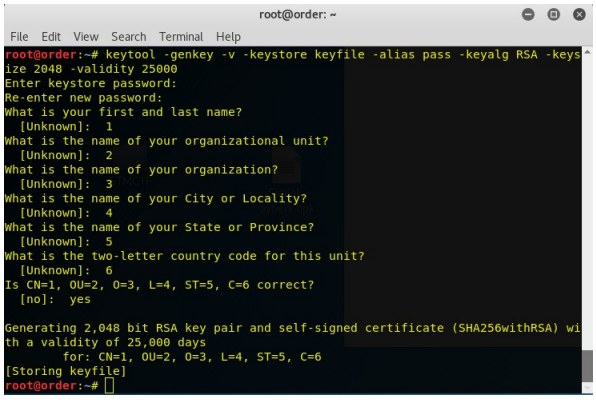


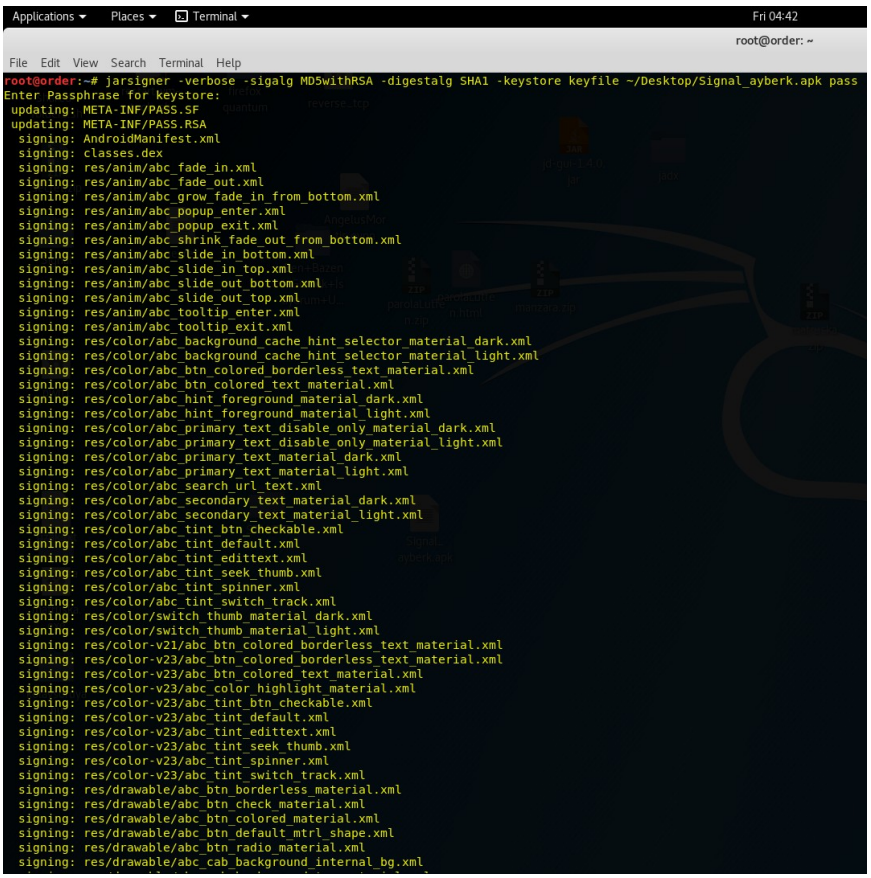
4. metot en çok uğraştıran metot, smali koduna log.d() ekleyip repack edip Apk'yı logları dinlemek.(Bu senaryoda bu gereksiz bir yöntem ama gene de yazalım.)
Sıra ile kullandıklarım
Apktool debug için
Smali dex repack için
Apktool build için
keytool key üretmek için
jarsigner ise apk'yı imzalamak için.

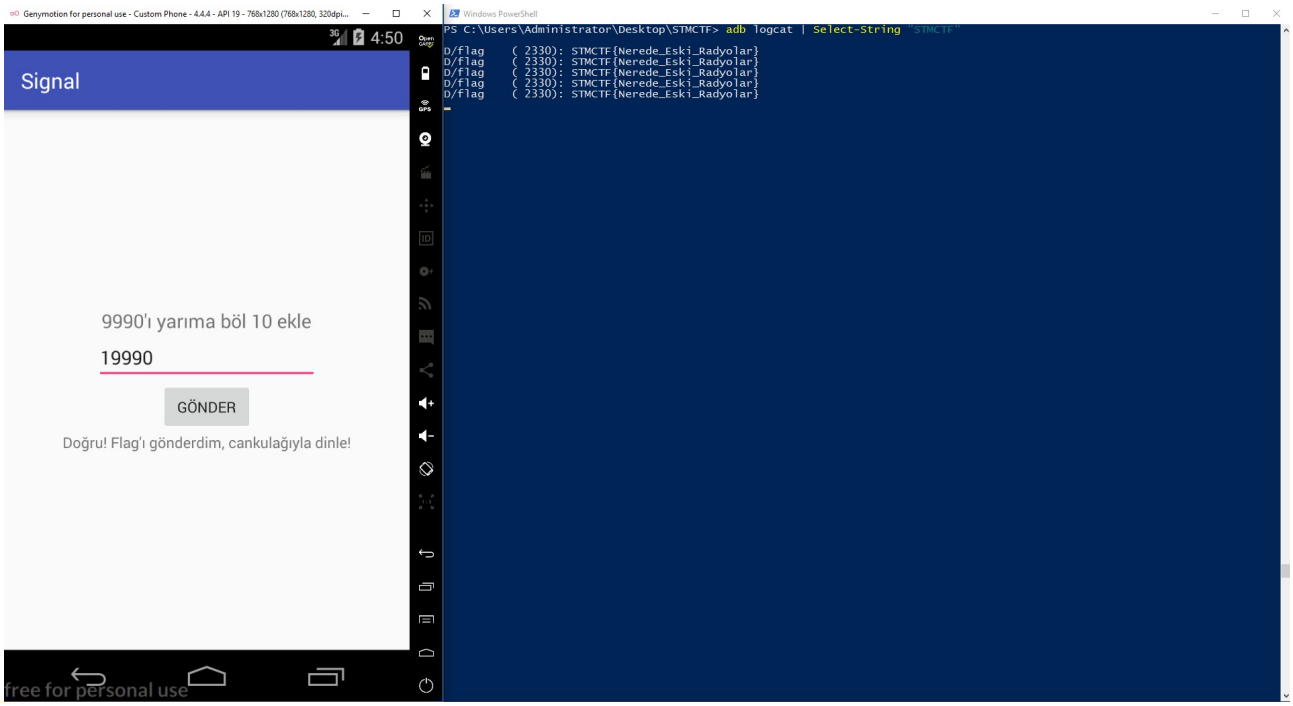


```
    goto :goto_0

    .line 33
    .end local v2    # "i":I
    :cond_0
    const-string v2, "flag"

    invoke-virtual {v4}, Ljava/lang/String;->toString()Ljava/lang/String;
    move-result-object v3
    invoke-static {v2, v3}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I

    invoke-virtual {v1, v2, v4}, Landroid/content/Intent;->putExtra(Ljava/lang/String;Ljava/lang/String;)Landroid/content/Intent;




    .line 34
    invoke-virtual {p0, v1}, Lctf/stm/com/signal/MainActivity;->sendBroadcast(Landroid/content/Intent;)V

    .line 35
    .end local v1    # "intent":Landroid/content/Intent;
    .end local v4    # "info":Ljava/lang/String;
    goto :goto_1

    .line 36
    :cond_1
    iget-object v1, p0, Lctf/stm/com/signal/MainActivity;->resultTv:Landroid/widget/TextView;

    const-string v2, "Yanl\u0131\u015f cevap. Tekrar dene."

    invoke-virtual {v1, v2}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V

    .line 38
    :goto_1
    return-void
.end method

.method protected onCreate(Landroid/os/Bundle;)V
    .locals 1
    .param p1, "savedInstanceState"    # Landroid/os/Bundle;

    .line 16
    invoke-super {p0, p1}, Landroid/support/v7/app/AppCompatActivity;->onCreate(Landroid/os/Bundle;)V

    .line 17
    const v0, 0x7f09001b

    invoke-virtual {p0, v0}, Lctf/stm/com/signal/MainActivity;->setContentView(I)V
```

Smali kodunda işaretli yere debug smalisi ekliyorum ve yeniden paketleyip yüklüyorum.

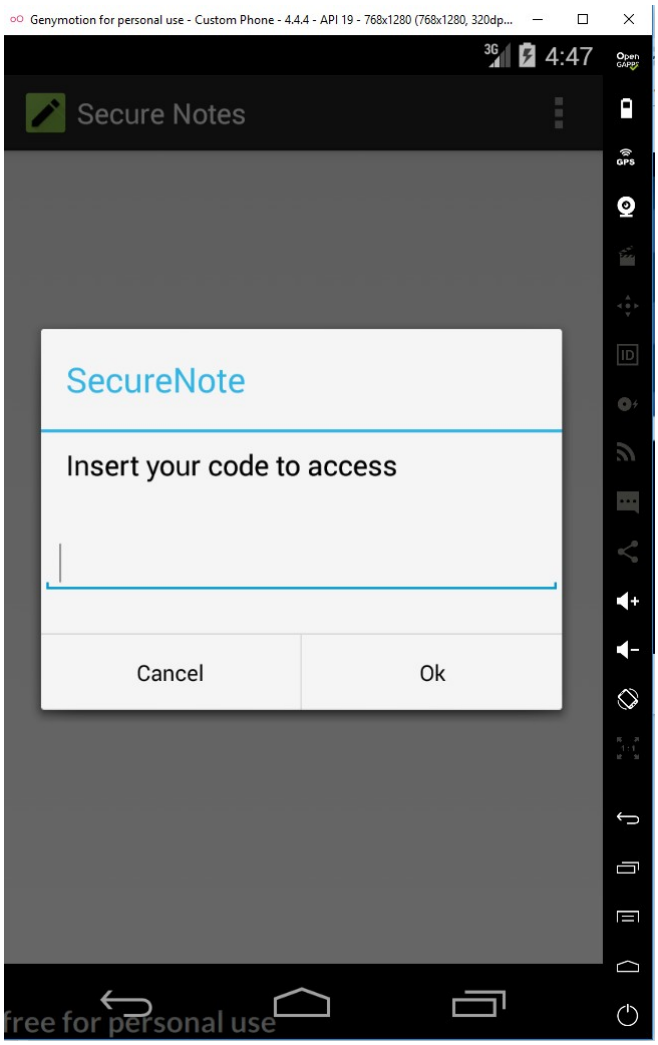






Soru 3

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.



Windows PowerShell

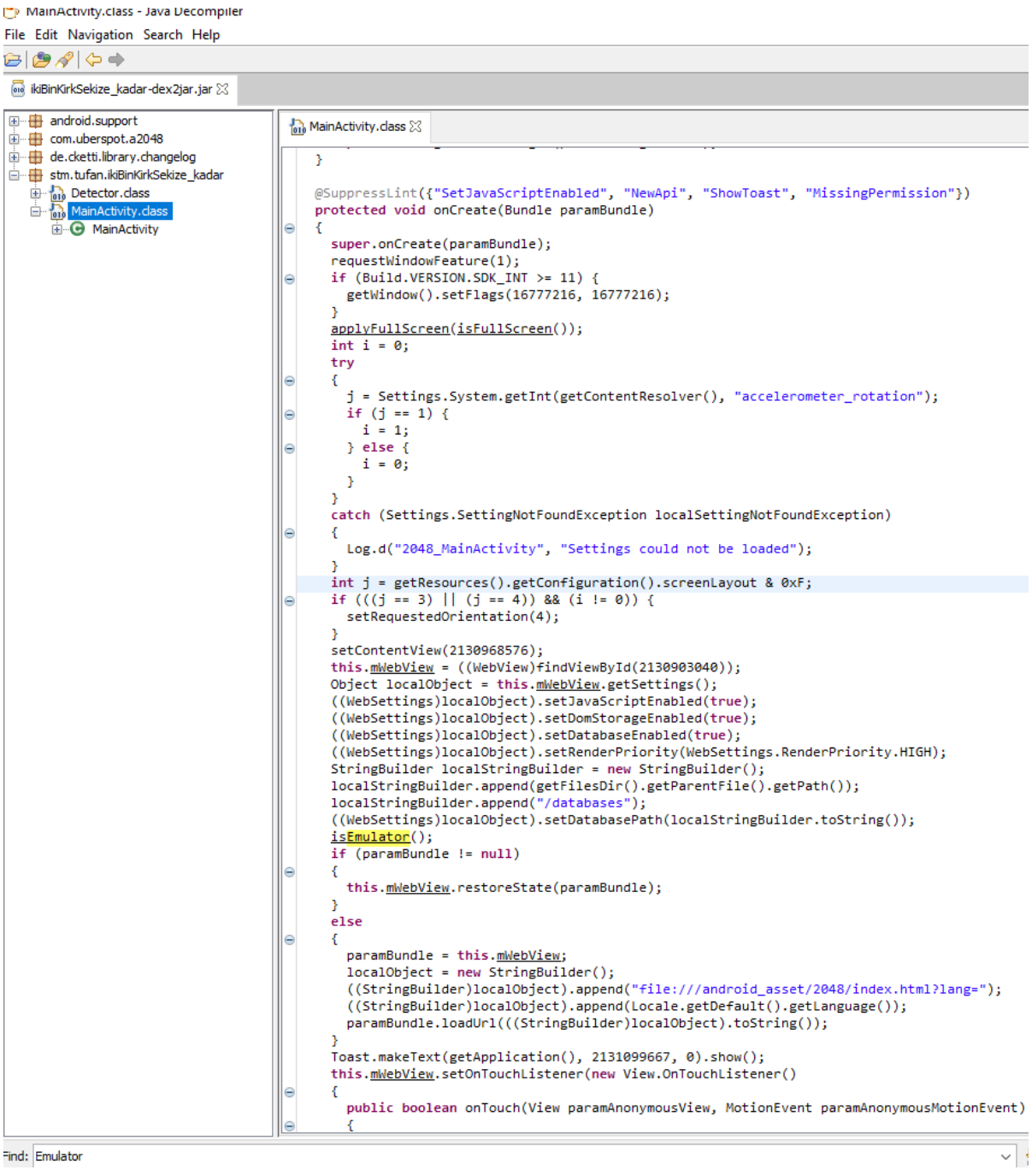
```
PS D:\Python\Python27\Scripts> adb forward tcp:31415 tcp:31415
PS D:\Python\Python27\Scripts> D:\Python\Python27\python.exe .\drozer console connect
:0: UserWarning: You do not have a working installation of the service_identity module: 'No module named service_identity'.  Please install it
dentity module, Twisted can perform only rudimentary TLS client hostname verification.  Many valid certificate/hostname mappings may be reject
Selecting 9d310fe3370388c6 (Genymotion Custom Phone - 4.4.4 - API 19 - 768x1280 4.4.4)

            ..                    ..:.
           ..o..                  .r..
            ..a..  . ....... .  ..nd
              ro..idsnemesisand..pr
              .otectorandroidsneme.
           .,sisandprotectorandroids+.
         ..nemesisandprotectorandroidsn:.
        .emesisandprotectorandroidsnemes..
      ..isandp,..,rotectorandro,..,idsnem.
      .isisandp..rotectorandroid..snemisis.
      ,andprotectorandroidsnemisisandprotec.
     .torandroidsnemesisandprotectorandroid.
     .snemisisandprotectorandroidsnemesisan:
     .dprotectorandroidsnemesisandprotector.

drozer Console (v2.4.4)
dz> run app.package.list -f mfcsecretnotes
com.mfc.secretnotes (MFCSecretNotes)
dz> run app.package.attacksurface com.mfc.secretnotes
Attack Surface:
  1 activities exported
  0 broadcast receivers exported
  1 content providers exported
  0 services exported
    is debuggable
dz> run app.provider.info -a com.mfc.secretnotes
Package: com.mfc.secretnotes
  Authority: com.mfc.secretnotes.contentprovider
    Read Permission: null
    Write Permission: null
    Content Provider: com.mfc.secretnotes.MyContentProvider
    Multiprocess Allowed: False
    Grant Uri Permissions: False

dz> run scanner.provider.finduris -a com.mfc.secretnotes
Scanning com.mfc.secretnotes...
Unable to Query  content://com.mfc.secretnotes.contentprovider
Able to Query    content://com.mfc.secretnotes.contentprovider/notes
Able to Query    content://com.mfc.secretnotes.contentprovider/notes/
Unable to Query  content://com.mfc.secretnotes.contentprovider/

Accessible content URIs:
  content://com.mfc.secretnotes.contentprovider/notes
  content://com.mfc.secretnotes.contentprovider/notes/
dz> run app.provider.query content://com.mfc.secretnotes.contentprovider/notes
| _id | category | summary | description |
| 1   | Note     | Meeting | Ayberk      |

dz> run app.provider.query content://com.mfc.secretnotes.contentprovider/notes --vertical
        _id  1
   category  Note
    summary  Meeting
description  Ayberk
```

```
dz>
dz> run app.provider.query content://com.mfc.secretnotes.contentprovider/notes --projection "* FROM SQLITE_MASTER WHERE type='table';--"
| type  | name              | tbl_name          | rootpage | sql                                                                                                                   |
| table | secretnotes       | secretnotes       | 2        | CREATE TABLE secretnotes(_id integer primary key autoincrement, category text not null, summary text not null,description text not null)       |
| table | sqlite_sequence   | sqlite_sequence   | 3        | CREATE TABLE sqlite_sequence(name,seq)                                                                                |
| table | secretnotessecure | secretnotessecure | 4        | CREATE TABLE secretnotessecure(_id integer primary key autoincrement, category text not null, summary text not null,description text not null) |

dz> run app.provider.query content://com.mfc.secretnotes.contentprovider/notes --projection "* FROM secretnotessecure;--"
| _id | category   | summary         | description                          |
| 1   | SecureNote | Cok gizli bilgi | STMCTF{C0k_g1zl1_ve_c0k_guv3nl1_b!Lg1} |

dz>
```

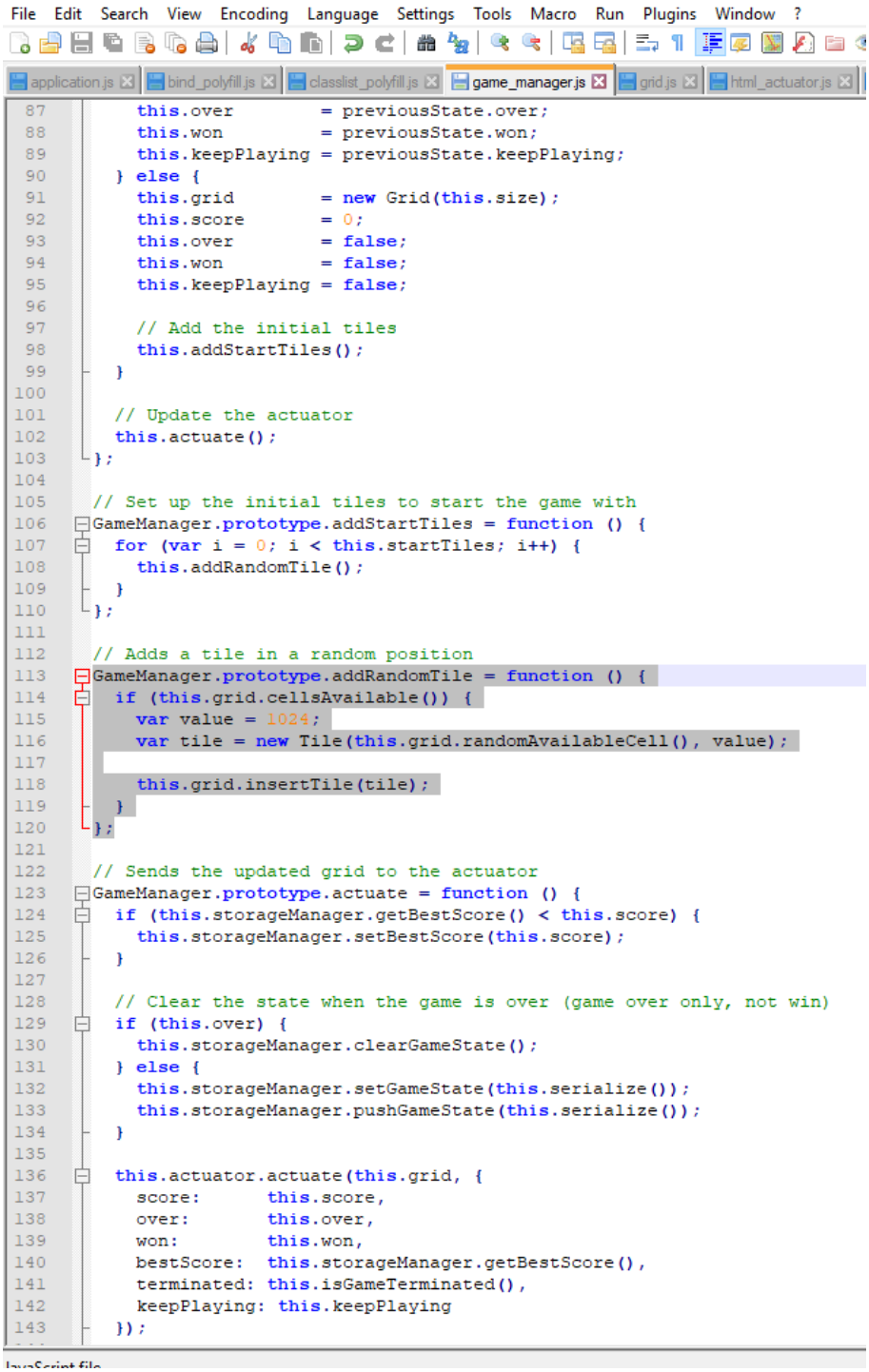
Soru 4

Bu soruda öncelikle yaptığım işlemlerden bahsedeyim. Apk dosyasını emulatore gönderdim yüklendi fakat açılmadı bende Emu koruması olduğunu o an anladım. Daha sonra Apk'nın içini apktool ile açtım ve içinden çıkan paketi jadx ve jdgui ile decompile edip içine baktım. Main class'ında emulator koruması olduğunu gördüm. Bir gaz ile emu korumasının call edildiği smaliyi sildim tekrar paketledim fakat o ana kadar mevzunun hala emu ile alakalı olduğunu varsayıyordum. Boşa paketlemelerle uğraştığım için oralardan bahsetmeyeceğim. Paketlenen dosyayı emuda açtığımda 2048 oyunun olduğunu ve bu oyunu web (js) olarak çalıştırdığını ve bu paketlerin assets dosyası içinde olduğunu gördüm. Javascript dosyası çok karışık ve if else doluydu tekrar paketleyip telefonda denemek yerine verileri pcye çekip chrome'da test ettim. Olay bir anda mobil ctf'den çıkıp javascript reverse'e döndü :) Arrayler hazır içinde hazır halde bulunuyordu fakat ben onların direkt olarak key veya v ector olabileceğini hesaba katmadım o yüzden bir dizi javascript Logu attım kodun içine. İf else'deki işlemlerin neler yaptığını görmek amacı ile hepsini print ettirdim. En sonunda mevzuyu anlayınca AES toolu kullanarak cevaba ulaştım.

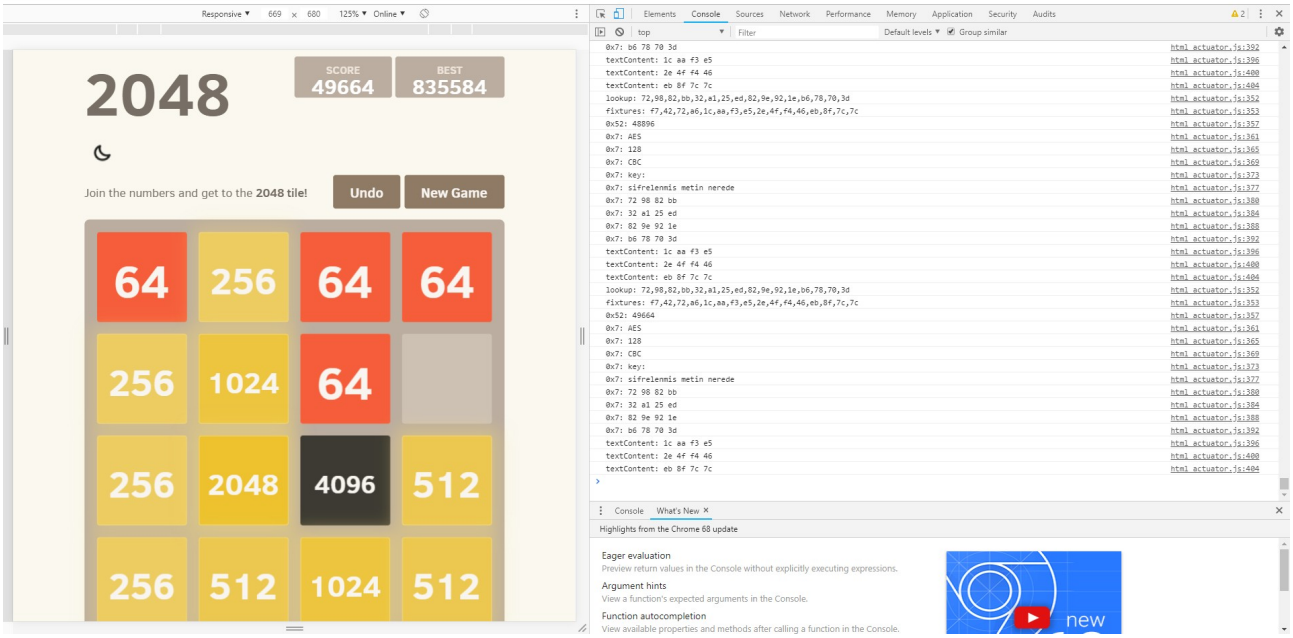
```
private void isEmulator()
{
  if (new Detector(this).isEmulator())
  {
    finish();
    System.exit(0);
  }
}
```



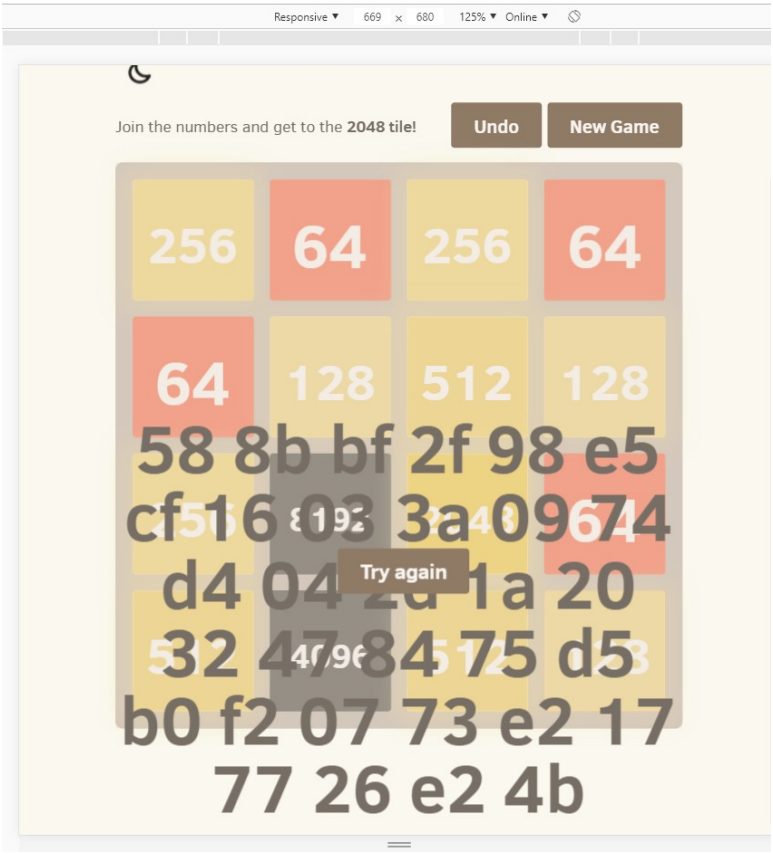
value'yu 1024 yaparak kendime hep 1024'lük kutulardan gönderttim. Score verisini değiştirerek ise ileri skorlardan başladım bu sayede ne oluyor ne bitiyor anlamaya çalıştım.



Koda koyduğum Loglar ile outputları inceledim ve AES 128 CBC olduğunu anladım. AES 128 CBC için 3 input gerekiyor. 1. input oyunda yenildiğinizde geliyor diğer 2 si ise if'leri doğru olarak sağladığınızda geliyor. Tabi biz bu ifleri bypass ettik.



Yenildiğinizde geldiğinden söz ettiğimiz o cipher



```
var lookup = ["72", "98", "82", "bb", "32", "a1", "25", "ed", "82", "9e", "92", "1e", "b6", "78", "70", "3d"];
/** @type {!Array} */
var fixtures = ["f7", "42", "72", "a6", "1c", "aa", "f3", "e5", "2e", "4f", "f4", "46", "eb", "8f", "7c", "7c"];
/** @type {!Array} */
//fixtures = [];
/** @type {string} */
var th_field = "";
/** @type {number} */
var lapl = first - this[b("0x52")];
this[b("0x52")] = first;
this[b("0x14")][b("0x7")] = this[b("0x52")];
if (lapl > 0) {
  var target = document[b("0x26")](b("0x27"));
  ////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

  console.log("lookup: " + lookup.toString());
  console.log("fixtures: " + fixtures.toString());

  //SCORE
  target[b("0x2f")][b("0x30")](b("0x53"));
  console.log("0x52: " + this[b("0x52")].toString());

  //AES
  target["textContent"] = "AES";
  console.log("0x7: " + target["textContent"].toString());

  //128
  target[b("0x7")] = b("0xa");
  console.log("0x7: " + target[b("0x7")].toString());

  //CBC
  target[b("0x7")] = b("0x54");
  console.log("0x7: " + target[b("0x7")].toString());

  //KEY
  target[b("0x7")] = b("0x55");
  console.log("0x7: " + target[b("0x7")].toString());

  //SIFRELENMİS METİN NEREDE
  target[b("0x7")] = b("0x5f");
  console.log("0x7: " + target[b("0x7")].toString());

  target[b("0x7")] = lookup[0] + " " + lookup[1] + " " + lookup[2] + " " + lookup[3];
  console.log("0x7: " + target[b("0x7")].toString());


  target["textContent"] = lookup[4] + " " + lookup[5] + " " + lookup[6] + " " + lookup[7];
  console.log("0x7: " + target["textContent"].toString());


  target[b("0x7")] = lookup[8] + " " + lookup[9] + " " + lookup[10] + " " + lookup[11];
  console.log("0x7: " + target[b("0x7")].toString());


  target[b("0x7")] = lookup[12] + " " + lookup[13] + " " + lookup[14] + " " + lookup[15];
  console.log("0x7: " + target[b("0x7")].toString());


  target[b("0x7")] = fixtures[4] + " " + fixtures[5] + " " + fixtures[6] + " " + fixtures[7];
  console.log("textContent: " + target["textContent"].toString());


  target[b("0x7")] = fixtures[8] + " " + fixtures[9] + " " + fixtures[10] + " " + fixtures[11];
  console.log("textContent: " + target["textContent"].toString());
```

Input type: Text

Input text: (hex)

```
58 8b bf 2f 98 e5 cf 16 03 3a 09 74 d4 04 2d 1a 20 32 47 84 75 d5 b0 f2 07 73 e2 17
77 26 e2 4b
```

Plaintext Hex Autodetect: ON | OFF

Function: AES

Mode: CBC (cipher block chaining)

Key: (hex)

```
72 98 82 bb 32 a1 25 ed 82 9e 92 1e b6 78 70 3d
```

Plaintext Hex

Init. vector:

```
f7 42 72 a6 1c aa f3 e5 2e 4f f4 46 eb 8f 7c 7c
```

> Encrypt! > Decrypt!

Initialization vector:

f74272a61caaf3e52e4ff446eb8f7c7c (256 bits)

Decrypted text:

```
00000000  53 54 4d 43 54 46 7b 48 65 72 5f 73 33 79 69 4e  STMCTF{Her_s3yiN
00000010  5f 31 5f 49 6c 6b 31 5f 56 40 72 64 69 52 7d 00  _1_Ilk1_V@rdiR}.
```

[Download as a binary file] [?] Inactive

STMCTF{Her_s3yiN_1_I1k1_V@rdiR}

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