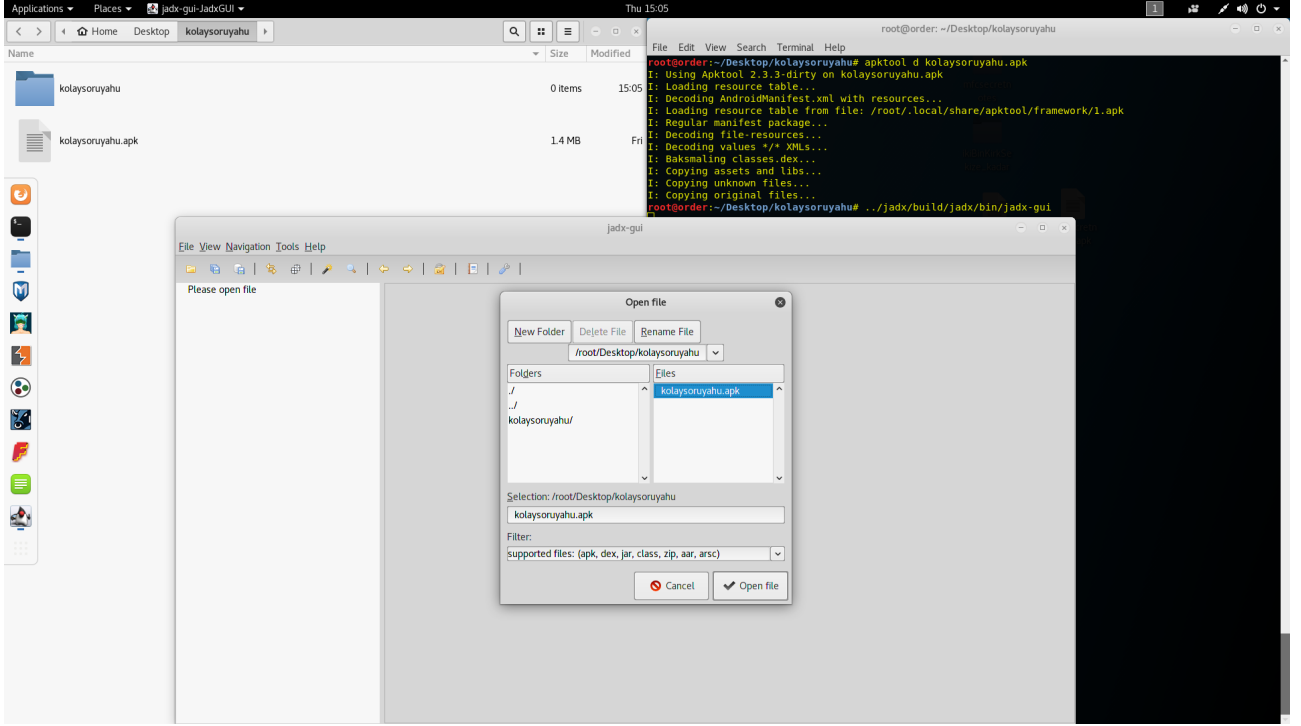


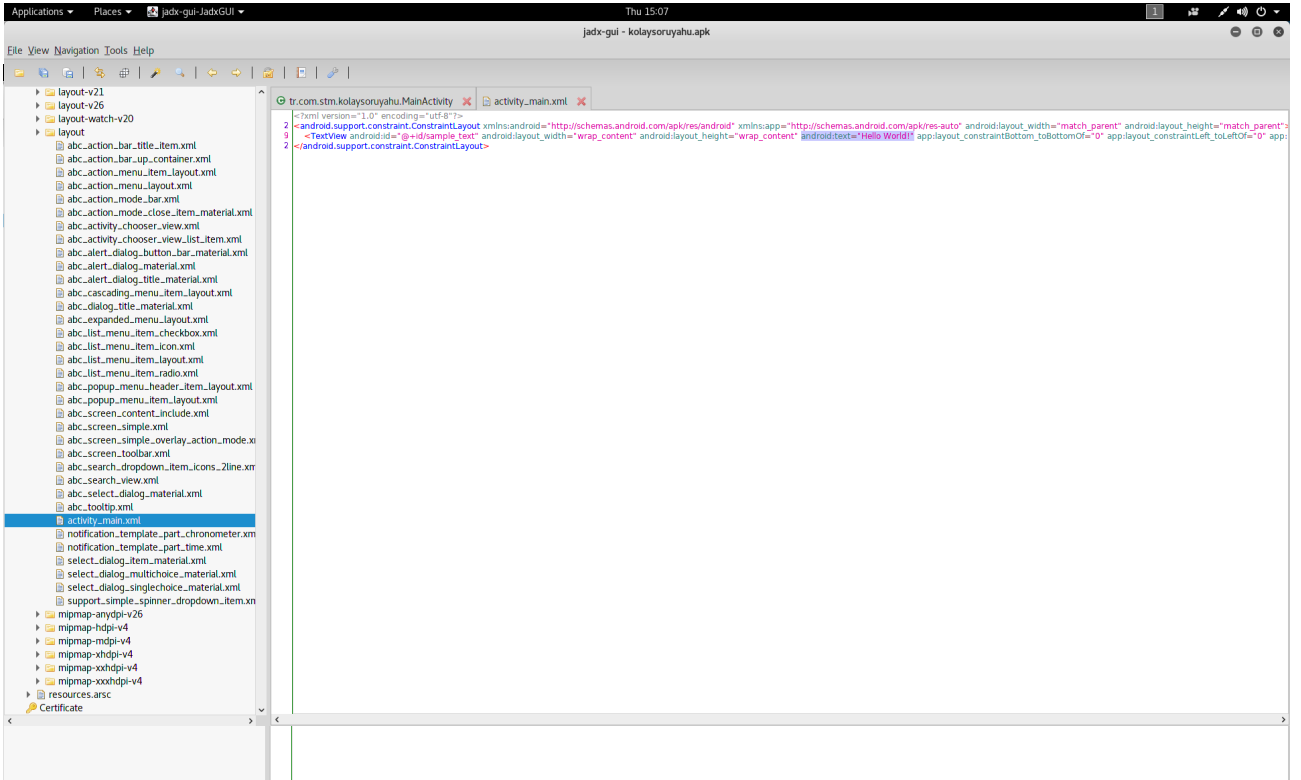
# STM CTF MOBILE WRITEUP

## Soru 1

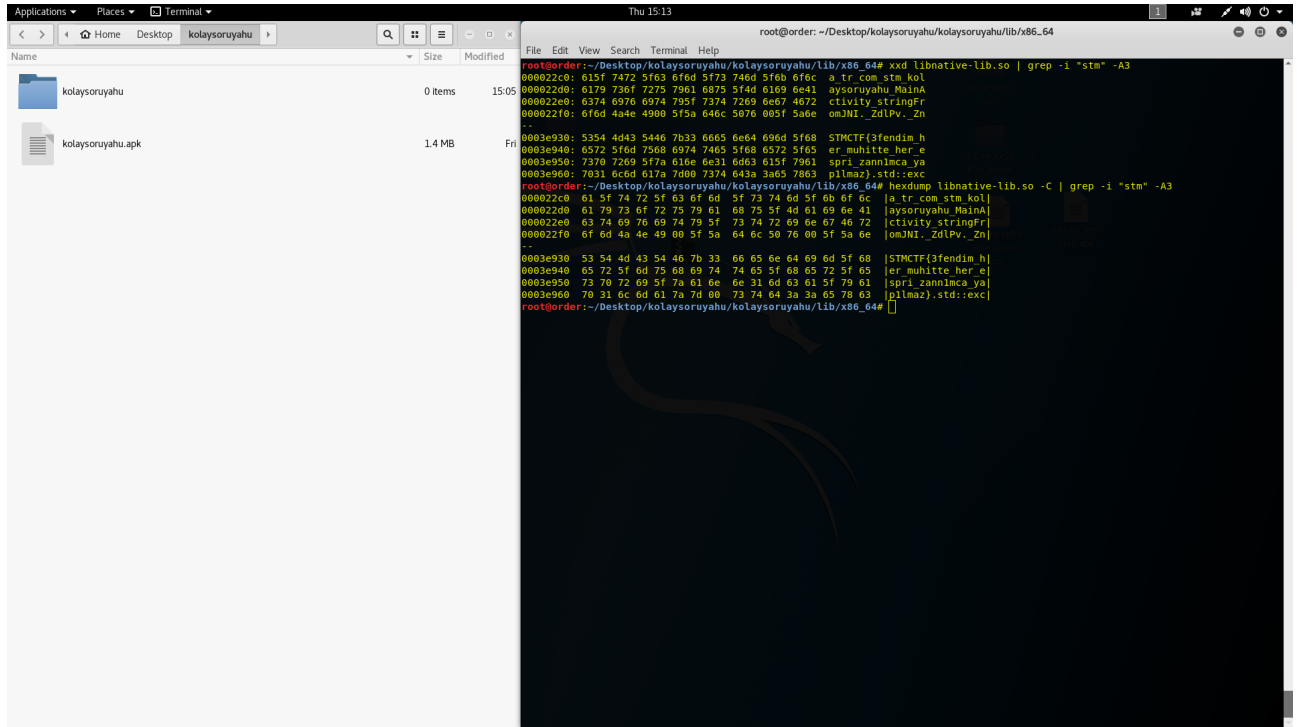
Apk'yı “**Apktool d kolaysoruyahu.apk**” komutu ile çıkardım.



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.

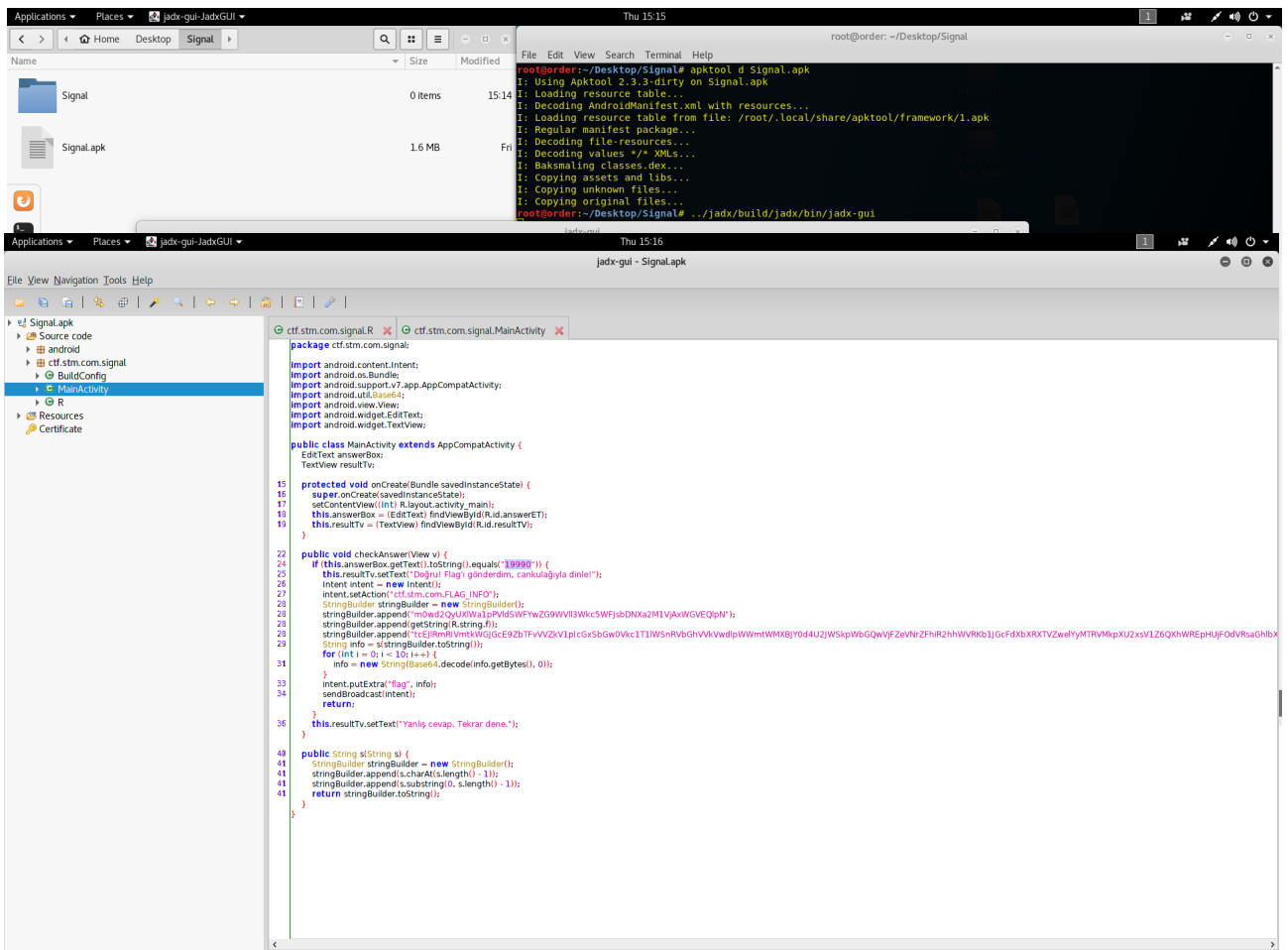


2 farklı komut ile sorunun cevabını aşağıdaki şekilde bulduk.

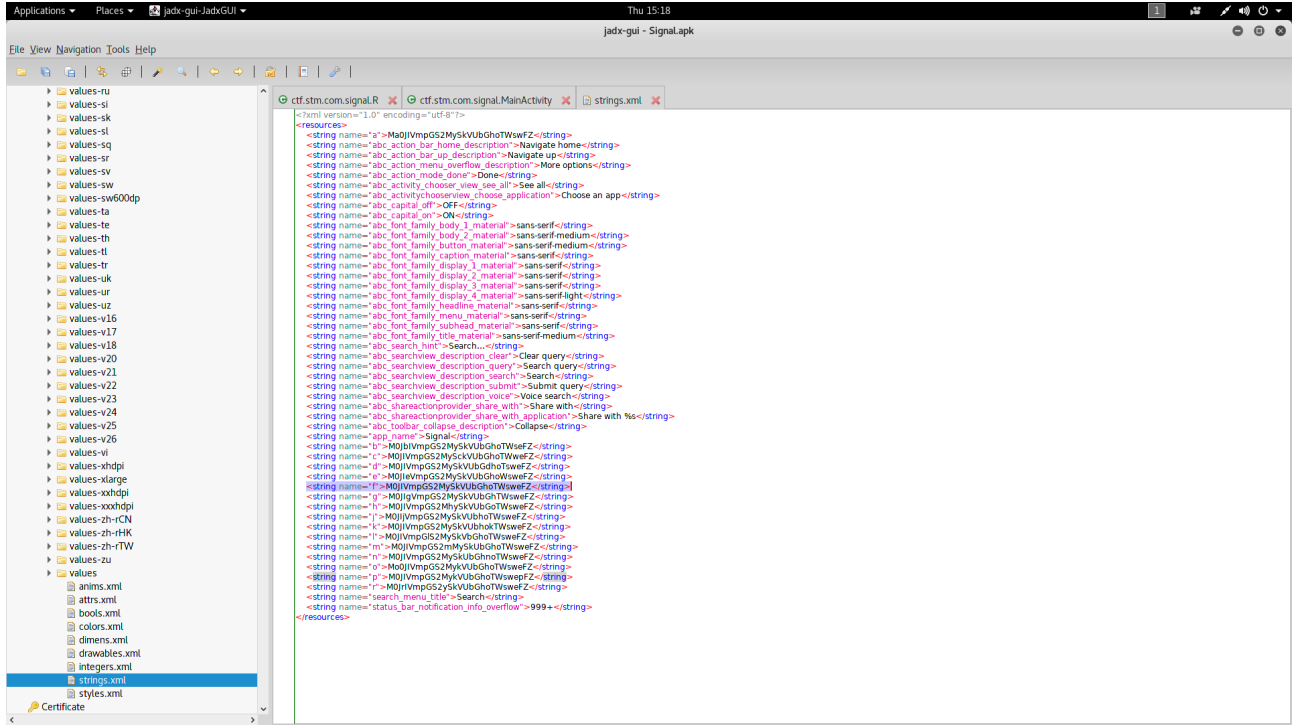


## Soru 2

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.

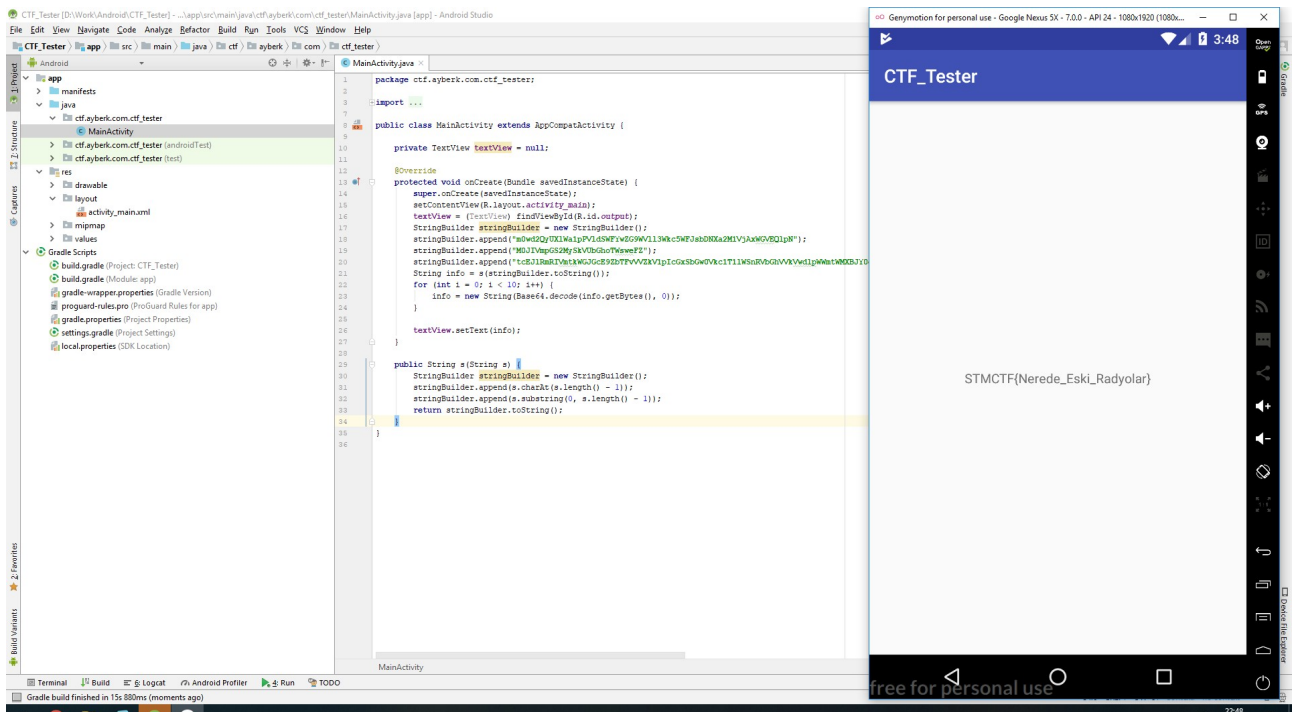


**Öncelikle bu soruyu çok farklı şekillerde çözebilirsiniz.**

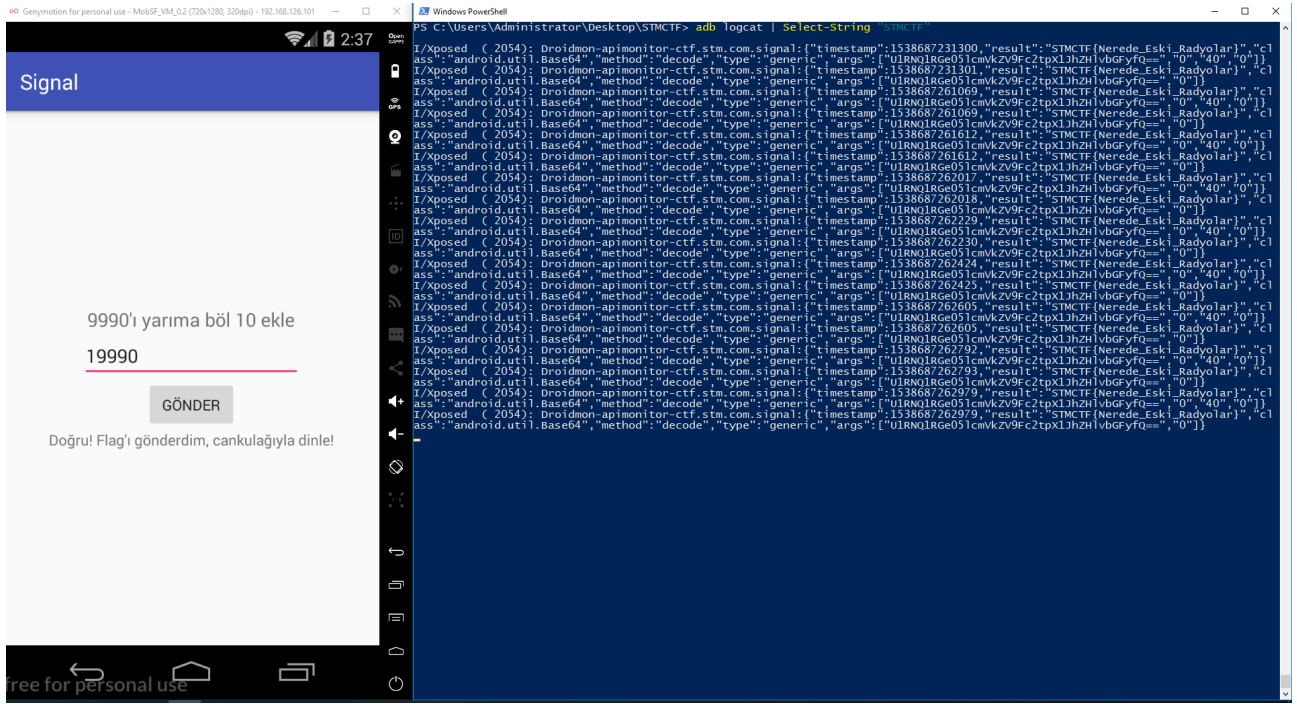
- 1- Aynı kodu hazır bulunan projenizde çalıştırıp sonuca ulaşabilirsiniz
- 2- Kodu yeteneğe göre göz veya kalem ile 3 5 dk'de çözebilirsiniz.
- 3- Sorunun adı dinlemeli olduğu için logları dinleyebilirsiniz.
- 4- Smail değiştirip yeniden paketleyebilirsiniz.

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. metod en çok uğraştıran metod, smali koduna log.d() ekleyip repack edip Apk'yı logları dinlemek.(Bu senaryoda bu gereksiz bir yöntem ama gene de yazalım.)

Sıra ile kullandıklarım

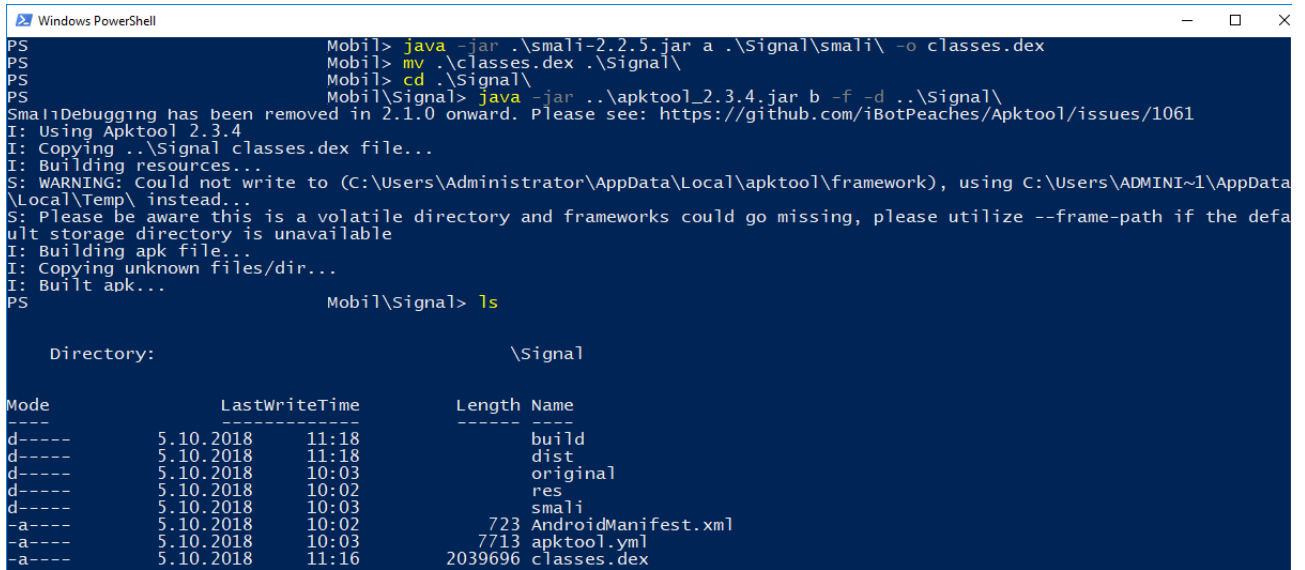
Apktool debug için

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\u0015f 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/CompatActivity;->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.

```

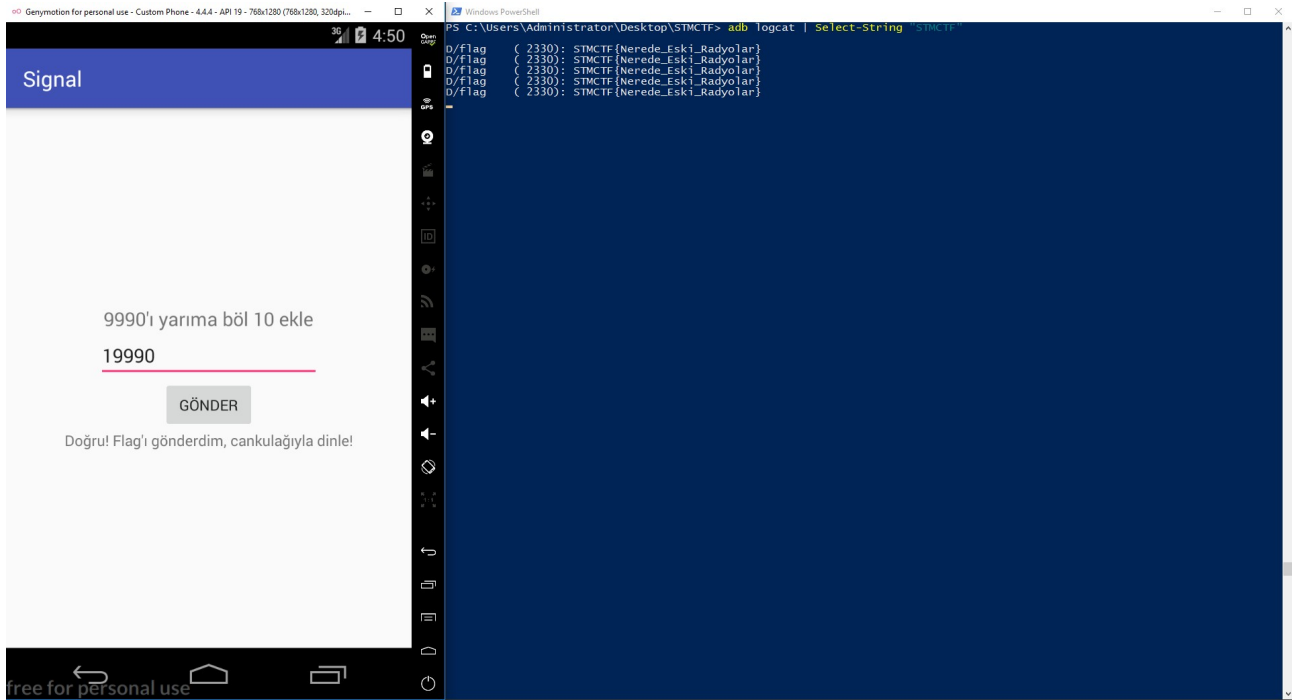
root@order: ~
File Edit View Search Terminal Help
root@order:~# keytool -genkey -v -keystore keyfile -alias pass -keyalg RSA -keysize 2048 -validity 25000
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: 1
What is the name of your organizational unit?
[Unknown]: 2
What is the name of your organization?
[Unknown]: 3
What is the name of your City or Locality?
[Unknown]: 4
What is the name of your State or Province?
[Unknown]: 5
What is the two-letter country code for this unit?
[Unknown]: 6
Is CN=1, OU=2, O=3, L=4, ST=5, C=6 correct?
[no]: yes
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 25,000 days
for: CN=1, OU=2, O=3, L=4, ST=5, C=6
[Storing keyfile]
root@order:~#

```

```

Applications Places Terminal Fri 04:42
root@order: ~
File Edit View Search Terminal Help
root@order:~# jarsigner -verbose -sigalg MD5withRSA -digestalg SHA1 -keystore keyfile ~/Desktop/Signal_ayberk.apk pass
Enter Passphrase for keystore:
updating: META-INF/PASS.SF
updating: META-INF/PASS.RSA
signing: AndroidManifest.xml
signing: classes.dex
signing: res/anim/abc_fade_in.xml
signing: res/anim/abc_fade_out.xml
signing: res/anim/abc_grow_fade_in_from_bottom.xml
signing: res/anim/abc_popup_enter.xml
signing: res/anim/abc_popup_exit.xml
signing: res/anim/abc_shrink_fade_out_from_bottom.xml
signing: res/anim/abc_slide_in_bottom.xml
signing: res/anim/abc_slide_in_top.xml
signing: res/anim/abc_slide_out_bottom.xml
signing: res/anim/abc_slide_out_top.xml
signing: res/anim/abc_tooltip_enter.xml
signing: res/anim/abc_tooltip_exit.xml
signing: res/color/abc_background_cache_hint_selector_material_dark.xml
signing: res/color/abc_background_cache_hint_selector_material_light.xml
signing: res/color/abc_btn_colored_borderless_text_material.xml
signing: res/color/abc_btn_colored_text_material.xml
signing: res/color/abc_hint_foreground_material_dark.xml
signing: res/color/abc_hint_foreground_material_light.xml
signing: res/color/abc_primary_text_disable_only_material_dark.xml
signing: res/color/abc_primary_text_disable_only_material_light.xml
signing: res/color/abc_primary_text_material_dark.xml
signing: res/color/abc_primary_text_material_light.xml
signing: res/color/abc_search_url_text.xml
signing: res/color/abc_secondary_text_material_dark.xml
signing: res/color/abc_secondary_text_material_light.xml
signing: res/color/abc_tint_btn_checkable.xml
signing: res/color/abc_tint_default.xml
signing: res/color/abc_tint_edittext.xml
signing: res/color/abc_tint_seek_thumb.xml
signing: res/color/abc_tint_spinner.xml
signing: res/color/abc_tint_switch_track.xml
signing: res/color/switch_thumb_material_dark.xml
signing: res/color/switch_thumb_material_light.xml
signing: res/color-v21/abc_btn_colored_borderless_text_material.xml
signing: res/color-v23/abc_btn_colored_borderless_text_material.xml
signing: res/color-v23/abc_btn_colored_text_material.xml
signing: res/color-v23/abc_color_highlight_material.xml
signing: res/color-v23/abc_tint_btn_checkable.xml
signing: res/color-v23/abc_tint_default.xml
signing: res/color-v23/abc_tint_edittext.xml
signing: res/color-v23/abc_tint_seek_thumb.xml
signing: res/color-v23/abc_tint_spinner.xml
signing: res/color-v23/abc_tint_switch_track.xml
signing: res/drawable/abc_btn_borderless_material.xml
signing: res/drawable/abc_btn_check_material.xml
signing: res/drawable/abc_btn_colored_material.xml
signing: res/drawable/abc_btn_default_mtrl_shape.xml
signing: res/drawable/abc_btn_radio_material.xml
signing: res/drawable/abc_cab_background_internal_bg.xml

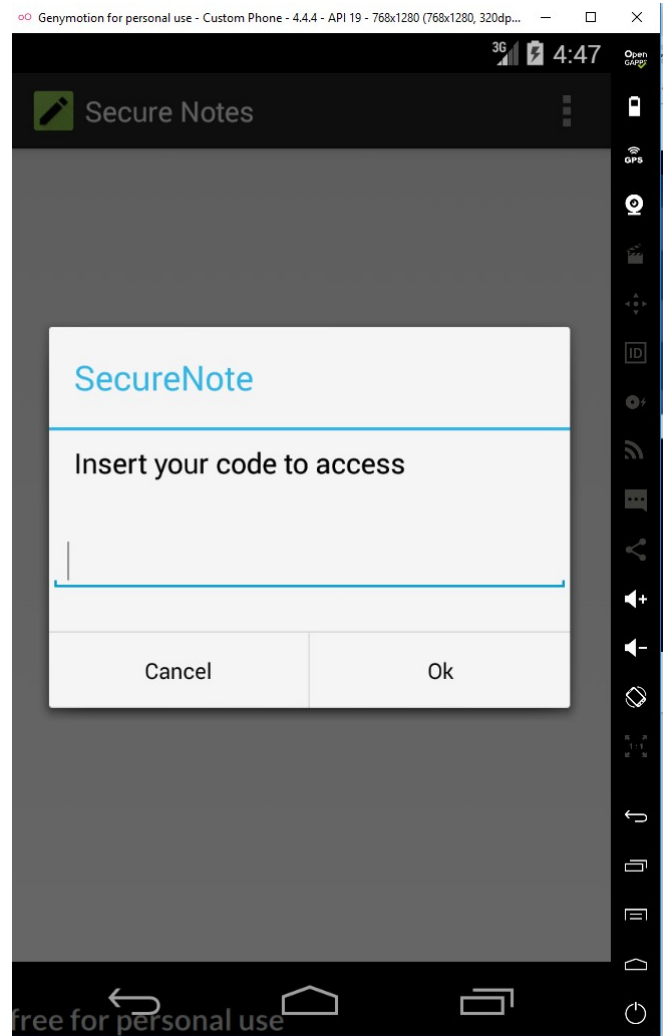
```



### 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
identity 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..       .f..
..a.. . . . . . . .nd
   ro..idsnemesisand..pr
   .otectorandroidsneme.
   .,sisandprotectorandroids+.
   ..nemesisandprotectorandroidsn:.
   .emesisandprotectorandroidsnemes..
   ..isandp,..rotectorandro,..idsnem.
   .isisandp..rotectorandroid..snemis.
   ,andprotectorandroidsnemisandprot.
   .torandroidsnemisandprotectorandroid.
   .snemisandprotectorandroidsnemis.
   .dprotectorandroidsnemisandprotector.

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_g1zli_ve_c0k_guv3nli_b1lg1} |

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 oralarından 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. If 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);
    }
}

```

MainActivity.class - Java Decompiler

File Edit Navigation Search Help



ikiBinKirkSekize\_kadar-dex2jar.jar

- android.support
- com.uberspot.a2048
- de.cketti.library.changelog
- stm.tufan.ikiBinKirkSekize\_kadar
  - Detector.class
  - MainActivity.class
  - MainActivity

MainActivity.class

```

}

@SuppressLint("SetJavaScriptEnabled", "NewApi", "ShowToast", "MissingPermission")
protected void onCreate(Bundle paramBundle)
{
    super.onCreate(paramBundle);
    requestWindowFeature(1);
    if (Build.VERSION.SDK_INT >= 11) {
        getWindow().setFlags(16777216, 16777216);
    }
    applyFullScreen(isFullScreen());
    int i = 0;
    try
    {
        j = Settings.System.getInt(getContentResolver(), "accelerometer_rotation");
        if (j == 1) {
            i = 1;
        } else {
            i = 0;
        }
    }
    catch (Settings.SettingNotFoundException localSettingNotFoundException)
    {
        Log.d("2048_MainActivity", "Settings could not be loaded");
    }
    int j = getResources().getConfiguration().screenLayout & 0xF;
    if (((j == 3) || (j == 4)) && (i != 0)) {
        setRequestedOrientation(4);
    }
    setContentView(2130968576);
    this.mWebView = ((WebView)findViewById(2130903040));
    Object localObject = this.mWebView.getSettings();
    ((WebSettings)localObject).setJavaScriptEnabled(true);
    ((WebSettings)localObject).setDomStorageEnabled(true);
    ((WebSettings)localObject).setDatabaseEnabled(true);
    ((WebSettings)localObject).setRenderPriority(WebSettings.RenderPriority.HIGH);
    StringBuilder localStringBuilder = new StringBuilder();
    localStringBuilder.append(getFilesDir().getParentFile().getPath());
    localStringBuilder.append("/databases");
    ((WebSettings)localObject).setDatabasePath(localStringBuilder.toString());
    isEmulator();
    if (paramBundle != null)
    {
        this.mWebView.restoreState(paramBundle);
    }
    else
    {
        paramBundle = this.mWebView;
        localObject = new StringBuilder();
        ((StringBuilder)localObject).append("file:///android_asset/2048/index.html?lang=");
        ((StringBuilder)localObject).append(Locale.getDefault().getLanguage());
        paramBundle.loadUrl(((StringBuilder)localObject).toString());
    }
    Toast.makeText(getApplication(), 2131099667, 0).show();
    this.mWebView.setOnTouchListener(new View.OnTouchListener()
    {
        public boolean onTouch(View paramAnonymousView, MotionEvent paramAnonymousMotionEvent)
        {

```

Find: Emulator

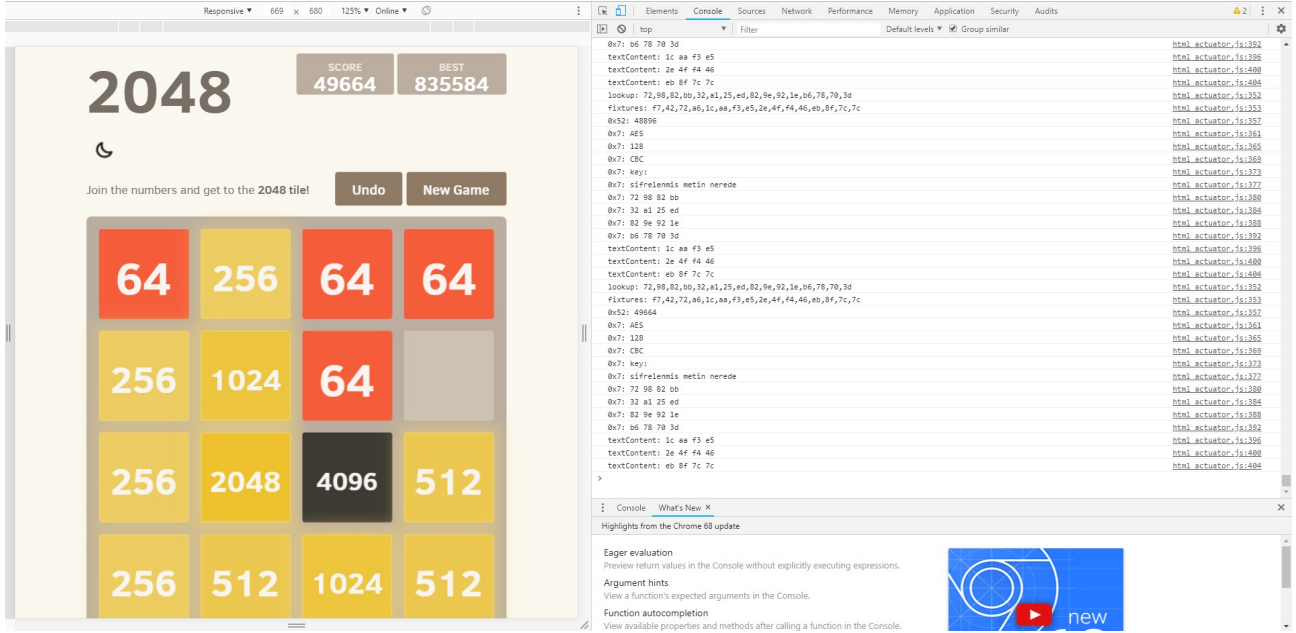


value'yu 1024 yaparak kendime  
hep 1024'lük kutulardan  
gönderttim. Score verisini  
değiştirerek ise ileri skorlardan  
başladım bu sayede ne oluyor ne  
bitiyor anlamaya çalıştım.

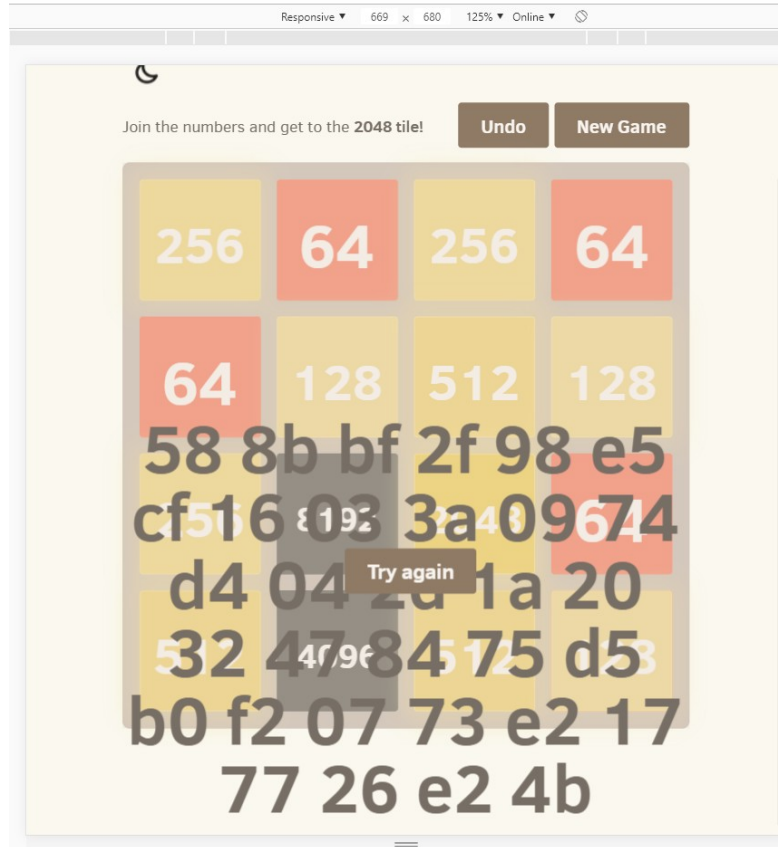
```
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
application.js bind_polyfill.js classlist_polyfill.js game_manager.js grid.js html_actuator.js
87     this.over      = previousState.over;
88     this.won       = previousState.won;
89     this.keepPlaying = previousState.keepPlaying;
90   } else {
91     this.grid      = new Grid(this.size);
92     this.score     = 0;
93     this.over      = false;
94     this.won       = false;
95     this.keepPlaying = false;
96
97     // Add the initial tiles
98     this.addStartTiles();
99   }
100
101   // Update the actuator
102   this.actuate();
103 };
104
105 // Set up the initial tiles to start the game with
106 GameManager.prototype.addStartTiles = function () {
107   for (var i = 0; i < this.startTiles; i++) {
108     this.addRandomTile();
109   }
110 };
111
112 // Adds a tile in a random position
113 GameManager.prototype.addRandomTile = function () {
114   if (this.grid.cellsAvailable()) {
115     var value = 1024;
116     var tile = new Tile(this.grid.randomAvailableCell(), value);
117
118     this.grid.insertTile(tile);
119   }
120 };
121
122 // Sends the updated grid to the actuator
123 GameManager.prototype.actuate = function () {
124   if (this.storageManager.getBestScore() < this.score) {
125     this.storageManager.setBestScore(this.score);
126   }
127
128   // Clear the state when the game is over (game over only, not win)
129   if (this.over) {
130     this.storageManager.clearGameState();
131   } else {
132     this.storageManager.setGameState(this.serialize());
133     this.storageManager.pushGameState(this.serialize());
134   }
135
136   this.actuator.actuate(this.grid, {
137     score:      this.score,
138     over:       this.over,
139     won:        this.won,
140     bestScore:  this.storageManager.getBestScore(),
141     terminated: this.isGameTerminated(),
142     keepPlaying: this.keepPlaying
143   });
144
145   ...

```

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 cıphar



```

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 lap1 = first - this[b("0x52")];
this[b("0x52")] = first;
this[b("0x14")][b("0x7")] = this[b("0x52")];
if (lap1 > 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	S T M C T F { H e r _ s 3 y i N _ 1 _ I l k 1 _ V @ r d i R } .
00000010	5f 31 5f 49 6c 6b 31 5f 56 40 72 64 69 52 7d 00	

[\[Download as a binary file\] \[?\]](#) Inactive

STMCTF{Her\_s3yiN\_1\_I1k1\_V@rdiR}

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