DISCLAIMER

L’app che andremo ad analizzare in questo intervento è stata scritta da me e la chiave che viene utilizzata è la mia

Questo talk è solo a scopo didattico

Di Cosa Parliamo Oggi?

μh
muhack.org

Cos’è il Reverse engineering

Il **reverse engineering** è un processo atto ad analizzare un sistema, software o dispositivo, anche senza accesso al suo codice sorgente, per comprenderne il funzionamento, la logica interna e le strutture.

Si parte **dall'output**, o dal comportamento osservabile, e si lavora a ritroso per ricostruire come è stato realizzato.

muhack.org

Statico vs Dinamico

Statico

Analisi che viene condotta senza eseguire il codice.

Vengono utilizzati una serie di tools e strumenti per analizzare il programma al fine di ricavarne lo scopo e le funzionalità.

Dinamico

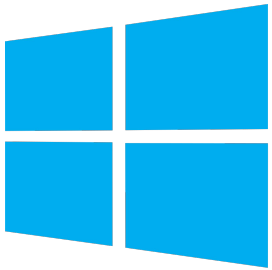
Analisi che viene condotta eseguendo il programma e osservandone il comportamento monitorando ad esempio il flusso di esecuzione, le interazioni con server e servizi o l'uso della memoria.

Reverse engineers Statico su un App Android

Abbiamo spiegato cosa vuol dire reversare staticamente un programma, ma su android come funziona?

Prima di tutto dobbiamo avere un *eseguibile* da studiare.

Se ad esempio su windows abbiamo i *.exe* e su linux abbiamo *.elf,* su android abbiamo gli **apk**



Cos’è un APK?

Un APK **(Android Application Package)** è il formato con cui vengono distribuite e installate le applicazioni Android.

Si può pensare come un "pacchetto" che contiene tutto ciò di cui un’app ha bisogno per funzionare: codice compilato, risorse grafiche, file di configurazione e altro.

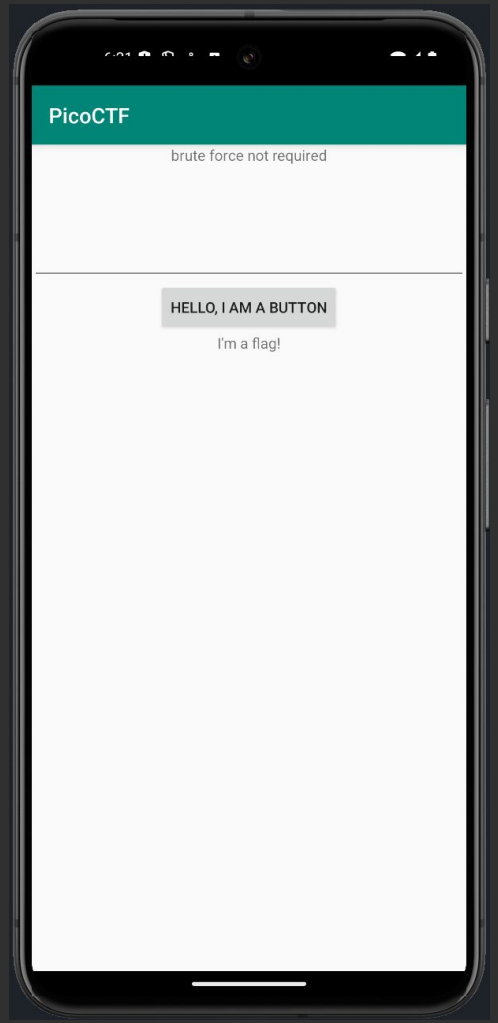
Quando scarichi un’app, il tuo dispositivo Android "scarta" l'APK e lo installa.

muhack.org

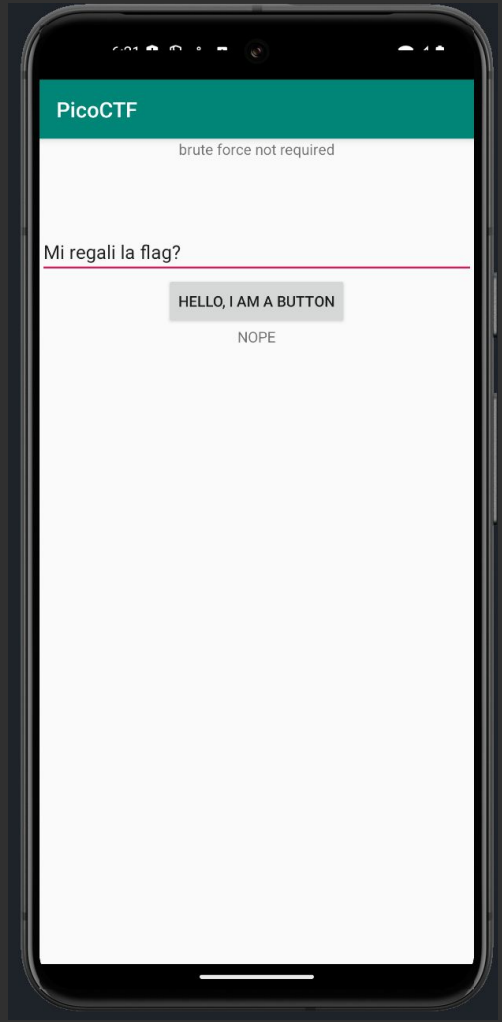
Strumenti

Tutto bellissimo, ma quindi?

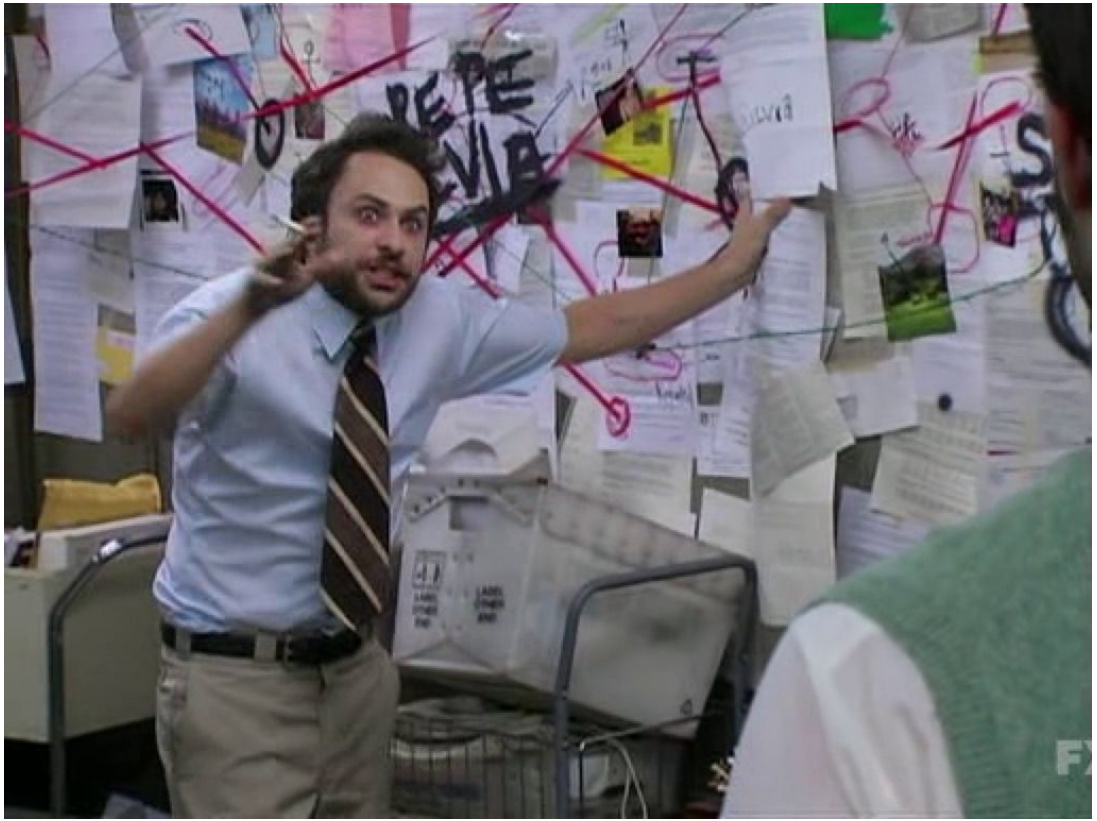
PicoCTF 2019



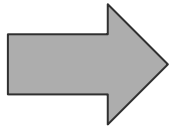
PicoCTF 2019

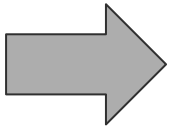


Okay qual è il piano?

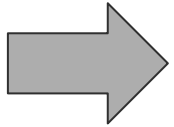


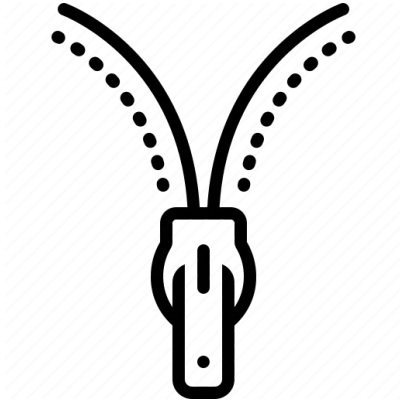
Partiamo dall’APK

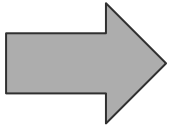




Partiamo dall’APK





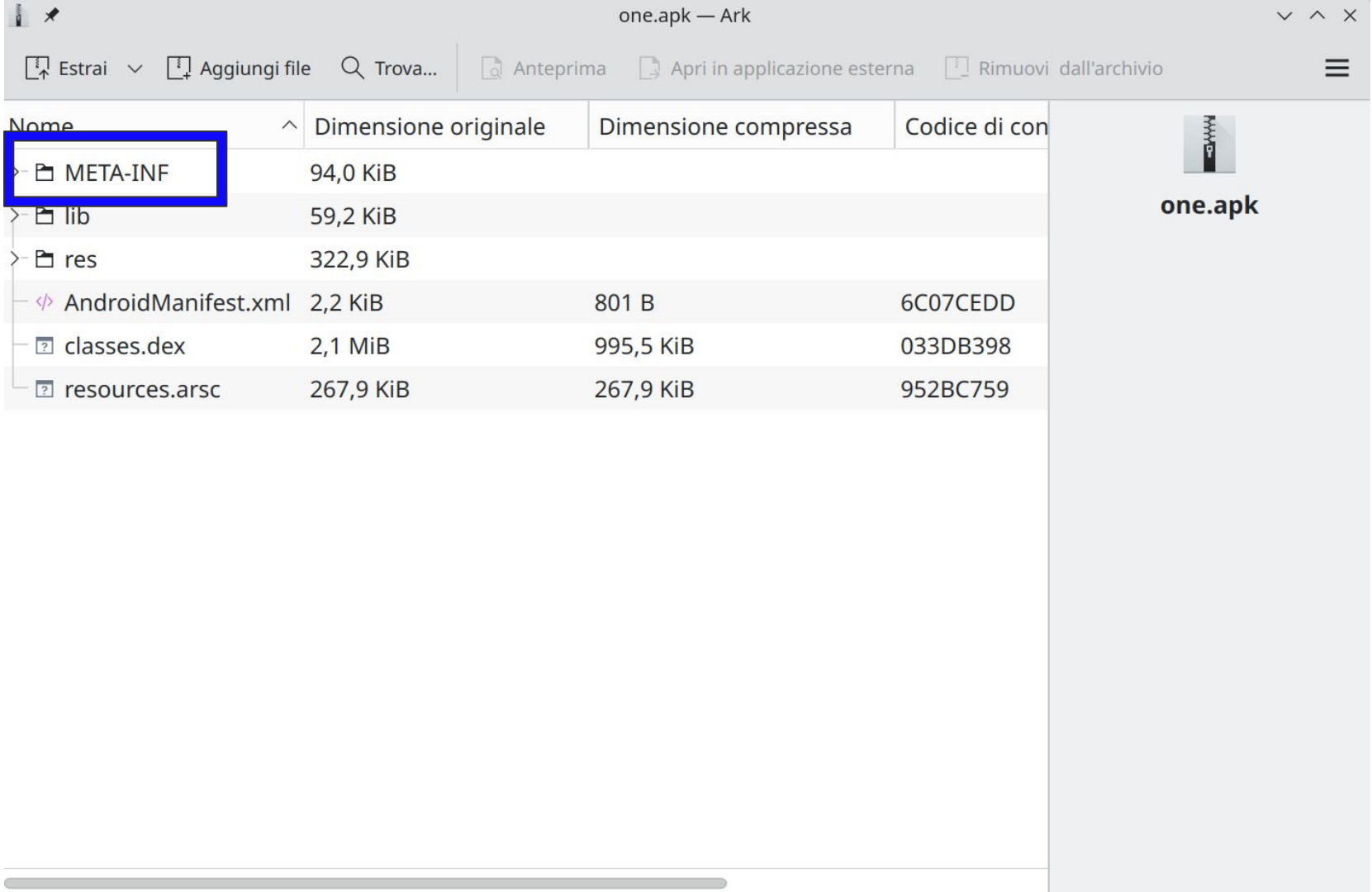


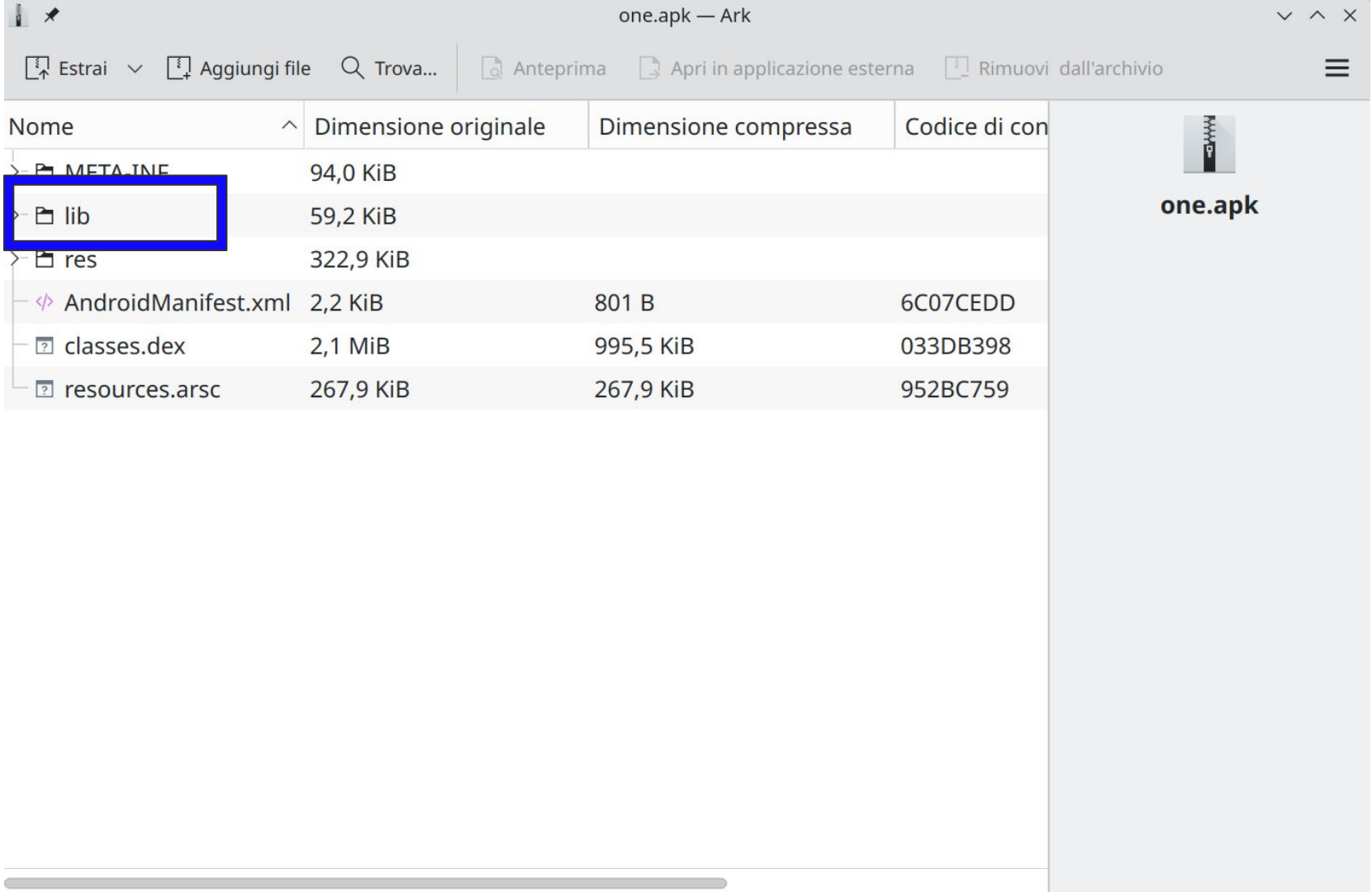
one.apk — Ark

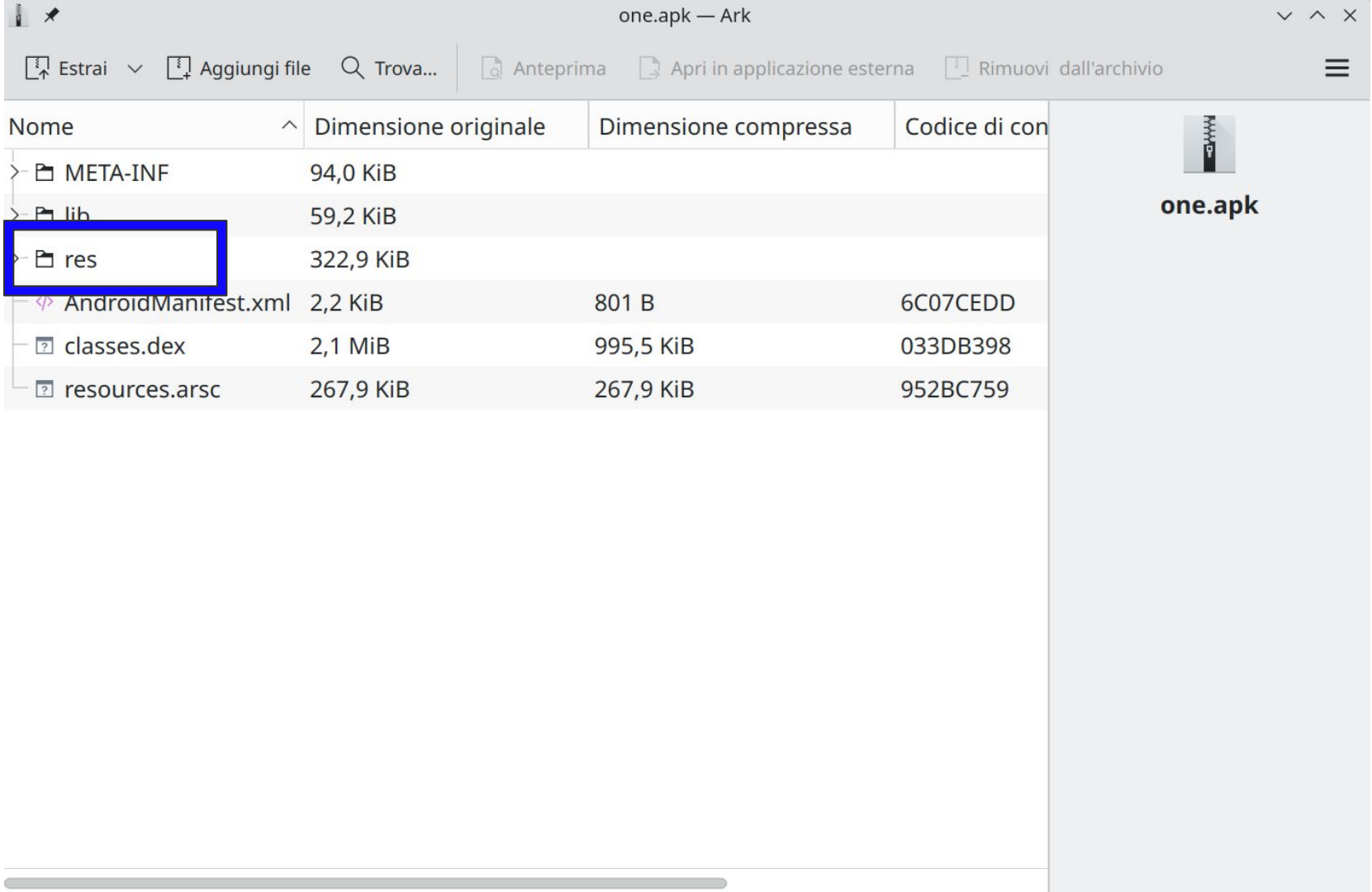
Estrai | Aggiungi file | Trova... | Anteprima | Apri in applicazione esterna | Rimuovi dall'archivio

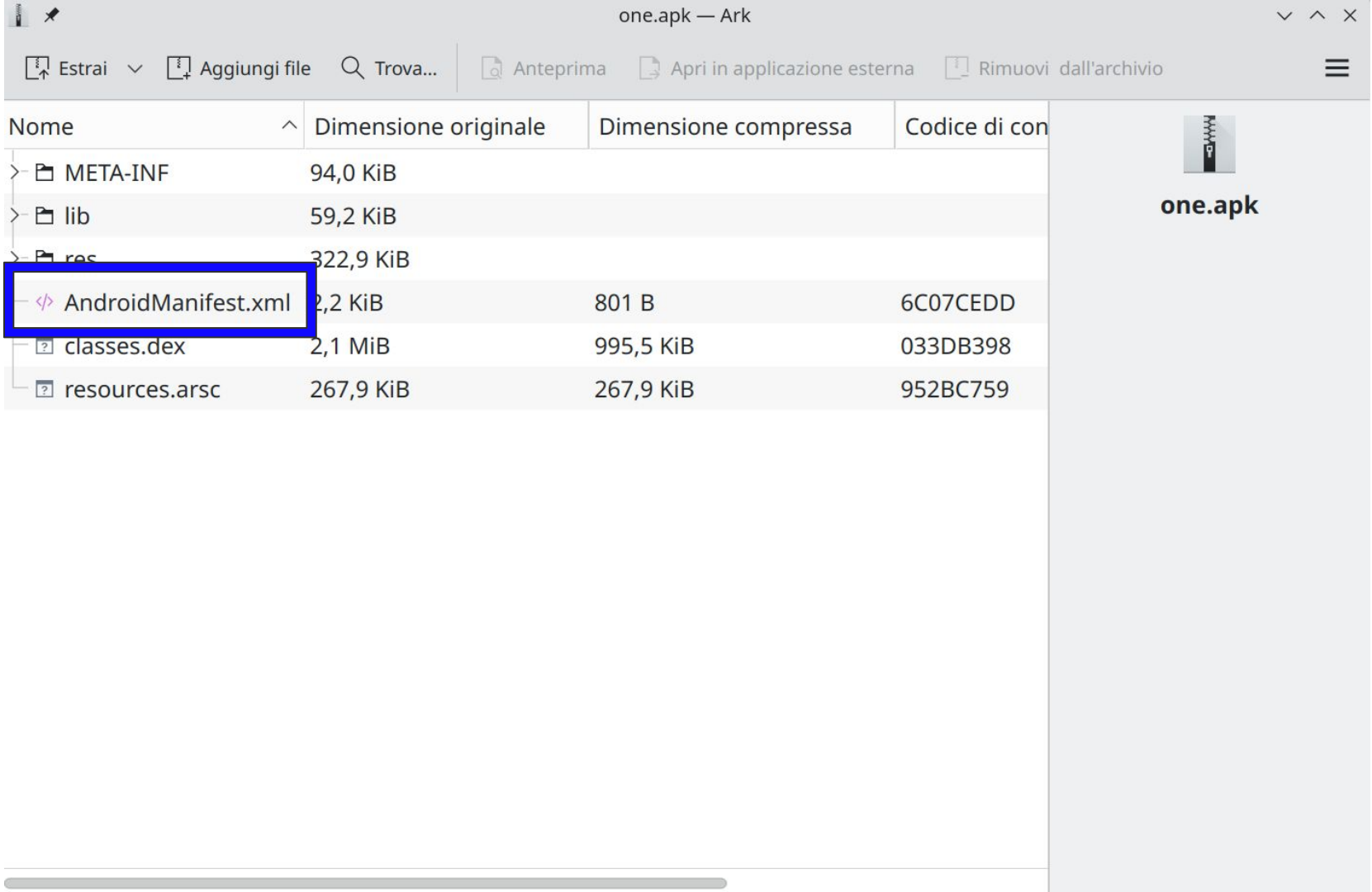
Nome	Dimensione originale	Dimensione compressa	Codice di con
META-INF	94,0 KiB		
lib	59,2 KiB		
res	322,9 KiB		
AndroidManifest.xml	2,2 KiB	801 B	6C07CEDD
classes.dex	2,1 MiB	995,5 KiB	033DB398
resources.arsc	267,9 KiB	267,9 KiB	952BC759

one.apk


one.apk — Ark
Estrai
Aggiungi file
Trova...
Anteprima
Apri in applicazione esterna
Rimuovi dall'archivio
Nome
Dimensione originale
Dimensione compressa
Codice di con
META-INF
94,0 KiB
lib
59,2 KiB
res
322,9 KiB
AndroidManifest.xml
2,2 KiB
801 B
6C07CEDD
classes.dex
2,1 MiB
995,5 KiB
033DB398
resources.arsc
267,9 KiB
267,9 KiB
952BC759
one.apk


one.apk — Ark
Estrai
Aggiungi file
Trova...
Anteprima
Apri in applicazione esterna
Rimuovi dall'archivio
Nome
Dimensione originale
Dimensione compressa
Codice di con
META-INF
94,0 KiB
lib
59,2 KiB
res
322,9 KiB
AndroidManifest.xml
2,2 KiB
801 B
6C07CEDD
classes.dex
2,1 MiB
995,5 KiB
033DB398
resources.arsc
267,9 KiB
267,9 KiB
952BC759
one.apk


one.apk — Ark
Estrai
Aggiungi file
Trova...
Anteprima
Apri in applicazione esterna
Rimuovi dall'archivio
Nome
Dimensione originale
Dimensione compressa
Codice di con
META-INF
94,0 KiB
lib
59,2 KiB
res
322,9 KiB
AndroidManifest.xml
2,2 KiB
801 B
6C07CEDD
classes.dex
2,1 MiB
995,5 KiB
033DB398
resources.arsc
267,9 KiB
267,9 KiB
952BC759
one.apk

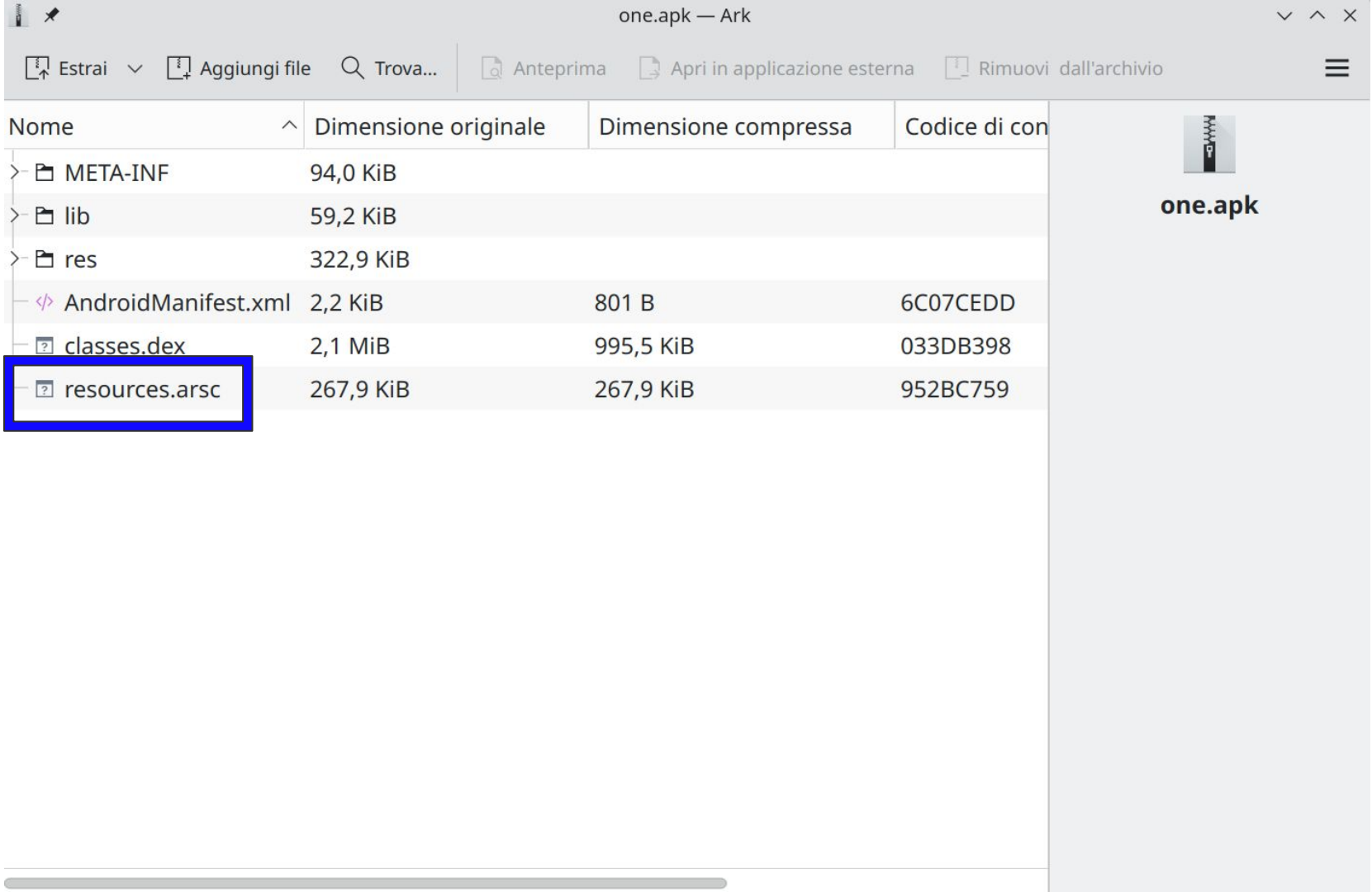

one.apk — Ark
Estrai
Aggiungi file
Trova...
Anteprima
Apri in applicazione esterna
Rimuovi dall'archivio
Nome
Dimensione originale
Dimensione compressa
Codice di con
META-INF
94,0 KiB
lib
59,2 KiB
res
322,9 KiB
AndroidManifest.xml
2,2 KiB
801 B
6C07CEDD
classes.dex
2,1 MiB
995,5 KiB
033DB398
resources.arsc
267,9 KiB
267,9 KiB
952BC759
one.apk

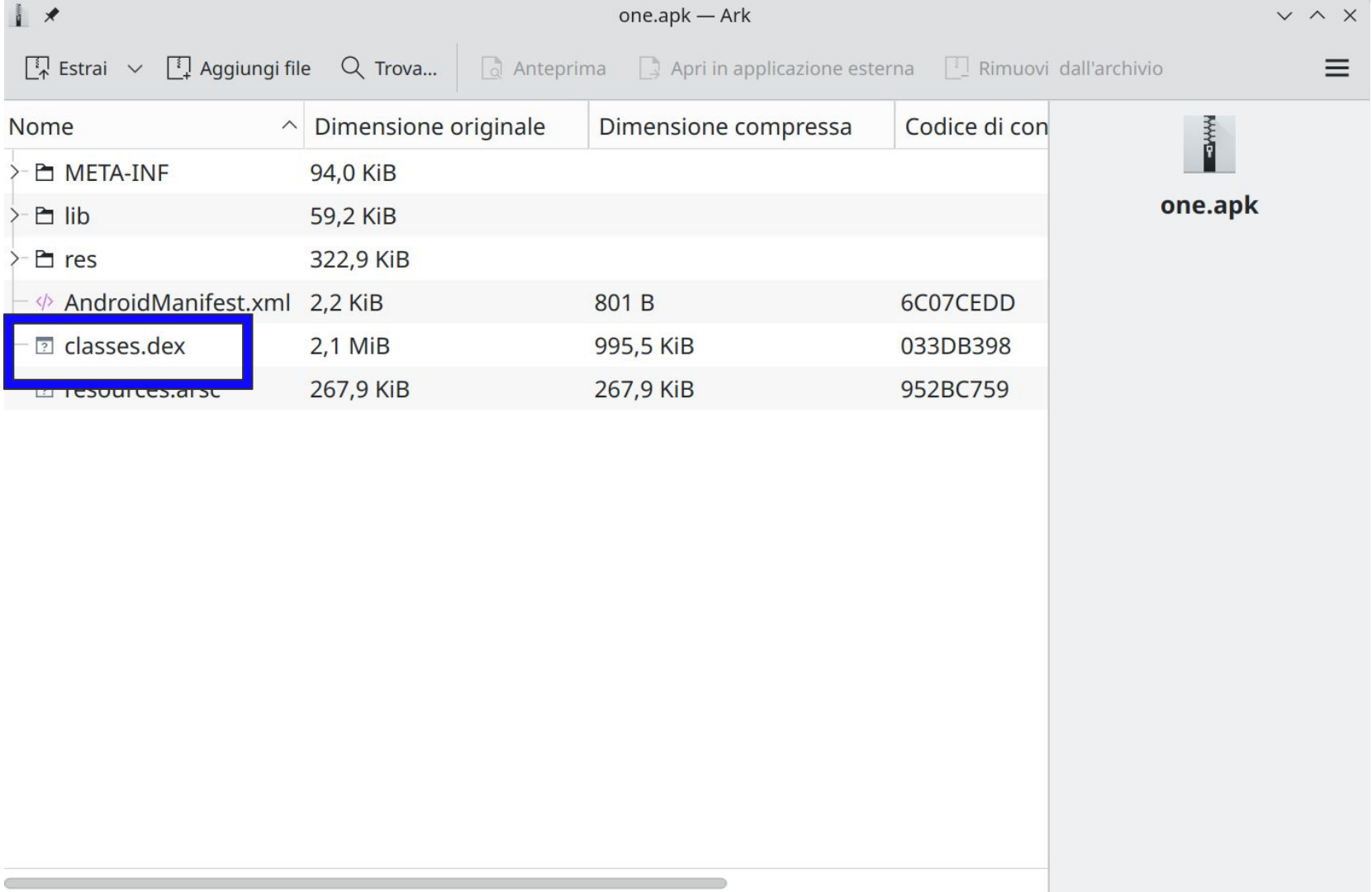
one.apk — Ark

Estrai | Aggiungi file | Trova... | Anteprima | Apri in applicazione esterna | Rimuovi dall'archivio

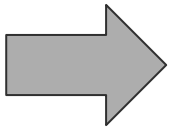
Nome	Dimensione originale	Dimensione compressa	Codice di con
META-INF	94,0 KiB		
lib	59,2 KiB		
res	322,9 KiB		
AndroidManifest.xml	2,2 KiB	801 B	6C07CEDD
classes.dex	2,1 MiB	995,5 KiB	033DB398
resources.arsc	267,9 KiB	267,9 KiB	952BC759

one.apk

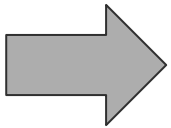

one.apk — Ark
Estrai
Aggiungi file
Trova...
Anteprima
Apri in applicazione esterna
Rimuovi dall'archivio
Nome
Dimensione originale
Dimensione compressa
Codice di con
META-INF 94,0 KiB
lib 59,2 KiB
res 322,9 KiB
AndroidManifest.xml 2,2 KiB 801 B 6C07CEDD
classes.dex 2,1 MiB 995,5 KiB 033DB398
resources.arsc 267,9 KiB 267,9 KiB 952BC759
one.apk

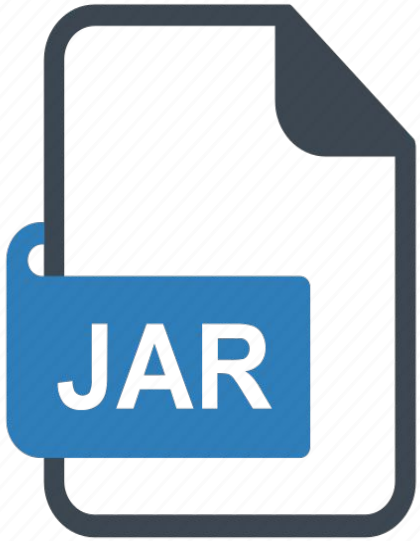

one.apk — Ark
Estrai
Aggiungi file
Trova...
Anteprima
Apri in applicazione esterna
Rimuovi dall'archivio
Nome
Dimensione originale
Dimensione compressa
Codice di con
META-INF
94,0 KiB
lib
59,2 KiB
res
322,9 KiB
AndroidManifest.xml
2,2 KiB
801 B
6C07CEDD
classes.dex
2,1 MiB
995,5 KiB
033DB398
267,9 KiB
267,9 KiB
952BC759
one.apk

Convertire un Dex?

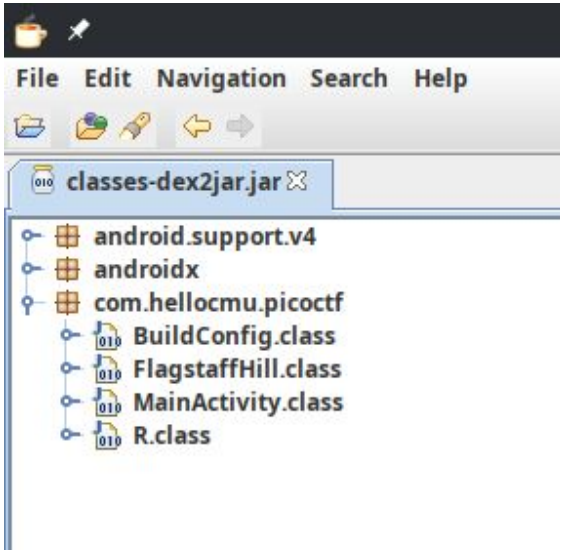


Convertire un Dex?

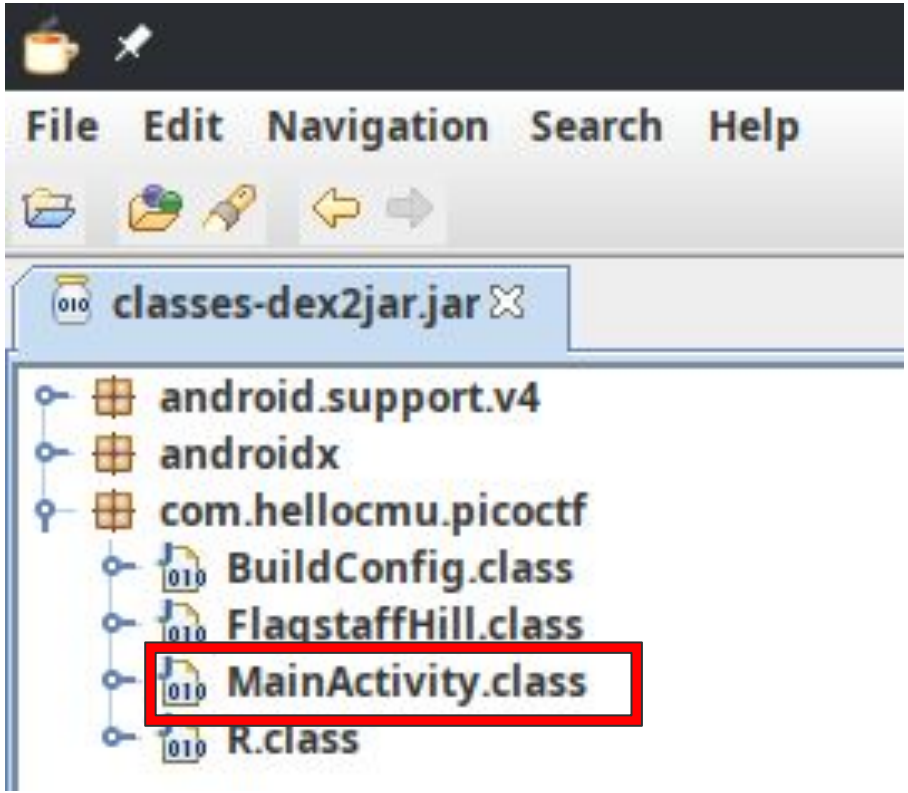




Come apriamo un jar?



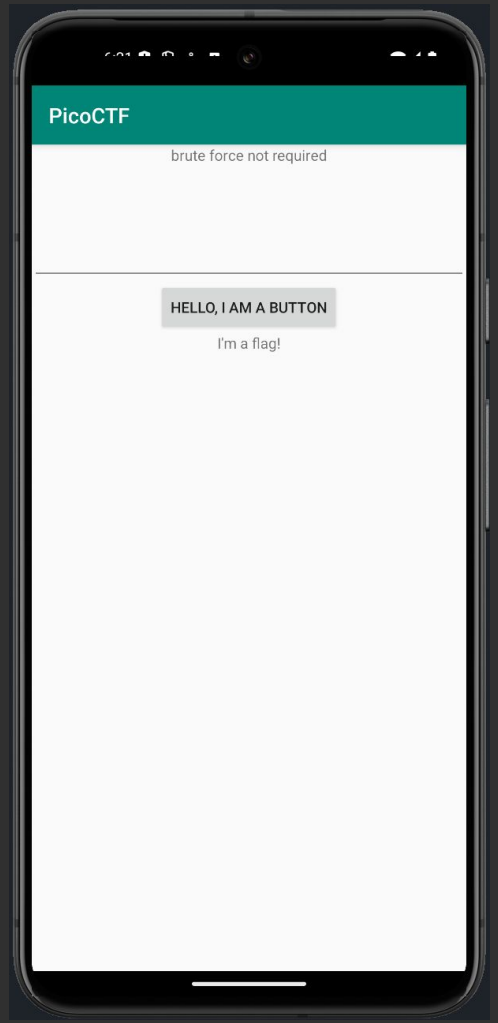
JD-GUI



MainActivity.class - Java Decompiler

MainActivity.class

```
package com.hellocmu.picoctf;

import android.content.Context;
import android.os.Bundle;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.TextView;
import androidx.appcompat.app.AppCompatActivity;

public class MainActivity extends AppCompatActivity {
  Button button;

  Context ctx;

  TextView text_bottom;

  EditText text_input;

  TextView text_top;

  public void buttonClick(View paramView) {
    String str = this.text_input.getText().toString();
    this.text_bottom.setText(FlagstaffHill.getFlag(str, this.ctx));
  }

  protected void onCreate(Bundle paramBundle) {
    super.onCreate(paramBundle);
    setContentView(2131296284);
    this.text_top = (TextView)findViewById(2131165322);
    this.text_bottom = (TextView)findViewById(2131165320);
    this.text_input = (EditText)findViewById(2131165321);
    this.ctx = getApplicationContext();
    System.loadLibrary("hellojni");
    this.text_top.setText(2131427372);
  }
}
```

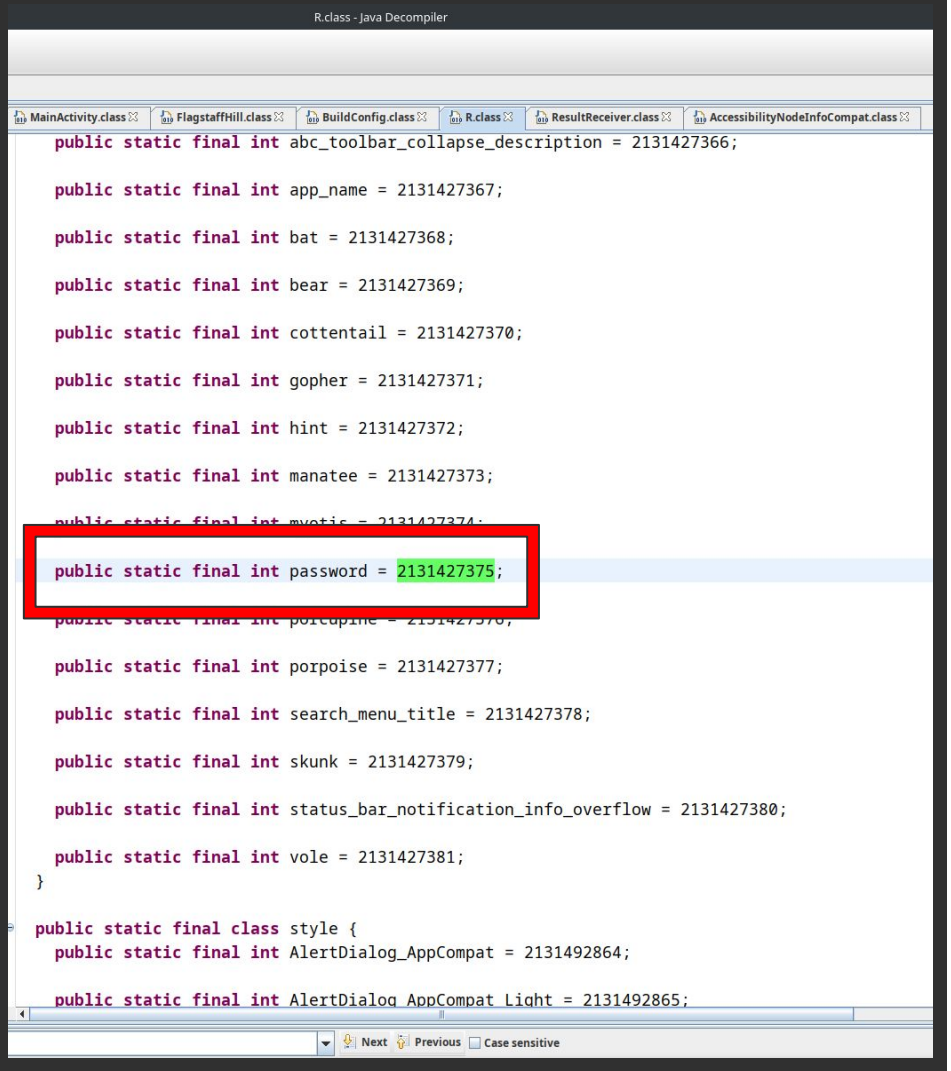


FlagstaffHill.class - Java Decompiler

MainActivity.class | FlagstaffHill.class

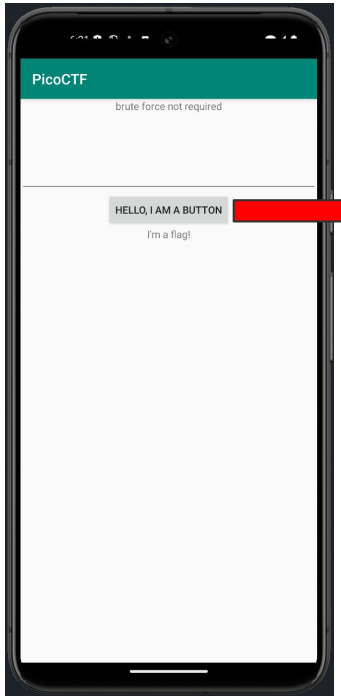
```
package com.hellocmu.picoctf;

import android.content.Context;

public class FlagstaffHill {
  public static native String fenugreek(String paramString);

  public static String getFlag(String paramString, Context paramContext) {
    return paramString.equals(paramContext.getString(2131427375)) ? fenugreek(paramString) : "NOPE";
  }
}
```

```
(paramContext.getString(2131427375))
```



Ci siamo quasi…

Riassumendo in breve:



ButtonClick() Testo GetFlag()

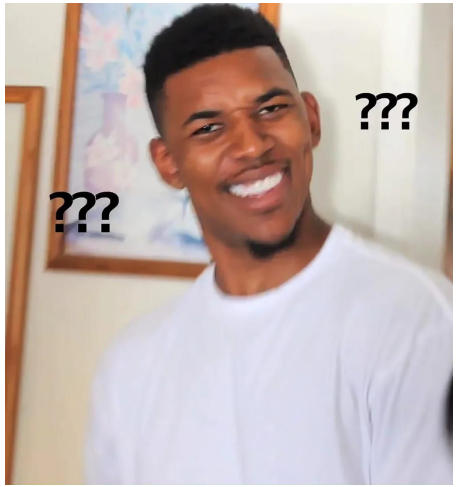
"Nope"

FLAG

Password

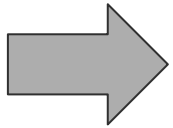
Estrai Aggiungi file Trova...

Nome	Dimensione or
META-INF	94,0 KiB
lib	59,2 KiB
res	322,9 KiB
AndroidManifest.xml	2,2 KiB
classes.dex	2,1 MiB
resources.arsc	267,9 KiB



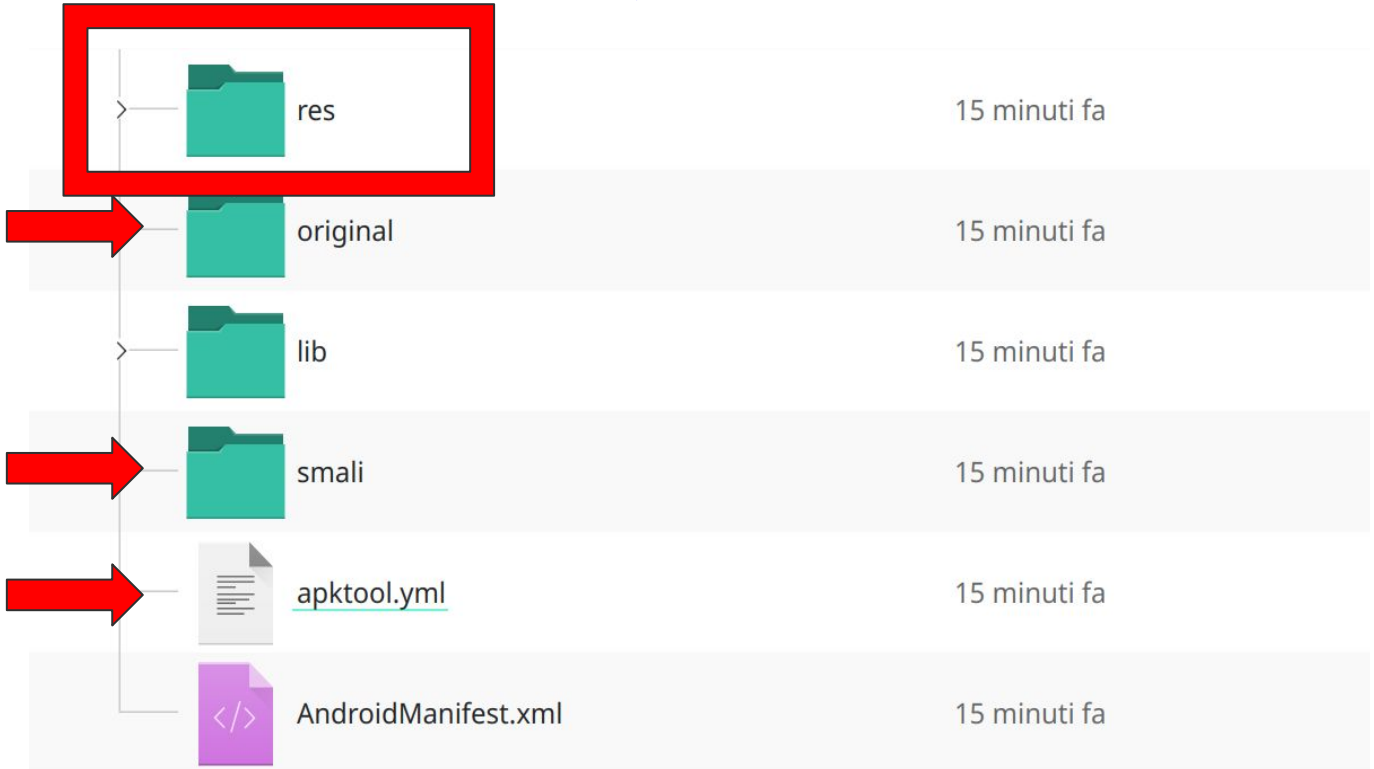
Nome	Modificato
mipmap-xxxhdpi-v4	13/12/01 alle 21:45
mipmap-xxhdpi-v4	13/12/01 alle 21:45
mipmap-xhdpi-v4	13/12/01 alle 21:45
mipmap-mdpi-v4	13/12/01 alle 21:45
mipmap-hdpi-v4	13/12/01 alle 21:45
mipmap-anydpi-v26	13/12/01 alle 21:45
layout-watch-v20	13/12/01 alle 21:45
layout-v26	13/12/01 alle 21:45
layout-v22	13/12/01 alle 21:45
layout-v21	13/12/01 alle 21:45
layout-v17	13/12/01 alle 21:45
layout-v16	13/12/01 alle 21:45
layout	13/12/01 alle 21:45
drawable-xxxhdpi-v4	13/12/01 alle 21:45
drawable-xxhdpi-v4	13/12/01 alle 21:45
drawable-xhdpi-v4	13/12/01 alle 21:45
drawable-watch-v20	13/12/01 alle 21:45
drawable-v24	13/12/01 alle 21:45
drawable-v23	13/12/01 alle 21:45
drawable-v21	13/12/01 alle 21:45
drawable-mdpi-v4	13/12/01 alle 21:45
drawable-ldrtl-xxxhdpi-v17	13/12/01 alle 21:45
drawable-ldrtl-xxhdpi-v17	13/12/01 alle 21:45
drawable-ldrtl-xhdpi-v17	13/12/01 alle 21:45
drawable-ldrtl-mdpi-v17	13/12/01 alle 21:45
drawable-ldrtl-hdpi-v17	13/12/01 alle 21:45
drawable-ldpi-v4	13/12/01 alle 21:45
drawable-hdpi-v4	13/12/01 alle 21:45
drawable-anydpi-v21	13/12/01 alle 21:45
drawable	13/12/01 alle 21:45
color-v23	13/12/01 alle 21:45
color-v21	13/12/01 alle 21:45
color	13/12/01 alle 21:45
anim	13/12/01 alle 21:45

Torniamo all’APK

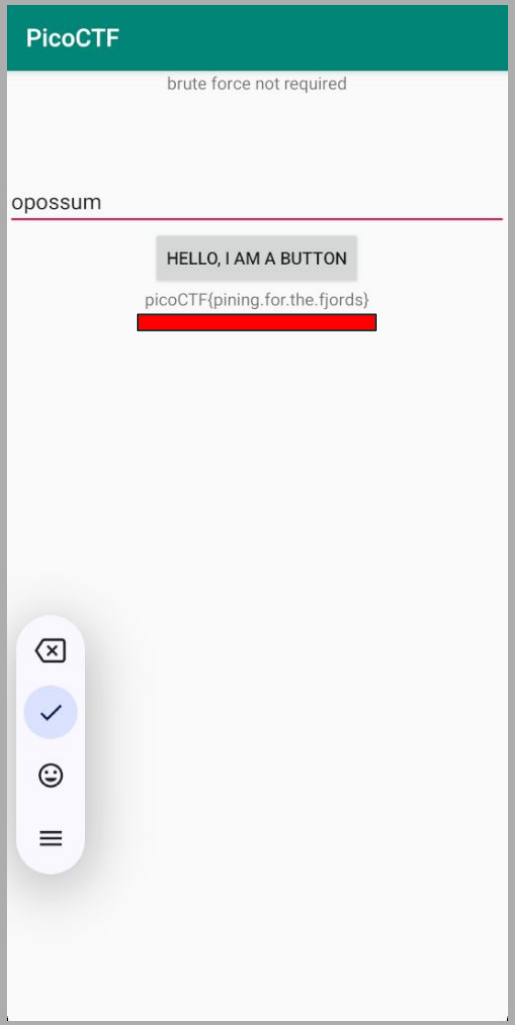


Torniamo all’APK

Qualcosa di nuovo?



strings.xml - one - Visual Studio Code
File Modifica Selezione Visualizza Vai Esegui Terminale Guida
CERCA
password
Sostituisci
20 risultati in 9 file - Apri nell'editor
public.xml res/values 1
...public type="string" name="password" id="0x7f0b002f" />
strings.xml res/values 1
<string name="password">opossum</string>
AppCompatTextHelper.smali smali/androidx/appcompat/widget 1
..., v9, Landroid/text/method/PasswordTransformationMethod;
AccessibilityNodeInfoCompat.smali smali/androidx/core/view/accessibility 7
.method public isPassword()Z
...AccessibilityNodeInfo;->isPassword()Z
.method public setPassword(Z)V
.param p1, "password" # Z
...AccessibilityNodeInfo;->setPassword(Z)V
const-string v2, "; password: "
...AccessibilityNodeInfoCompat;->isPassword()Z
AccessibilityRecordCompat.smali smali/androidx/core/view/accessibility 5
.method public isPassword()Z
...accessibility/AccessibilityRecord;->isPassword()Z
.method public setPassword(Z)V
.param p1, "isPassword" # Z
.../AccessibilityRecord;->setPassword(Z)V
TextViewCompat.smali smali/androidx/core/widget 1
..., v0, Landroid/text/method/PasswordTransformationMethod;
ExploreByTouchHelper.smali smali/androidx/customview/widget 2
...AccessibilityNodeInfoCompat;->isPassword()Z
...accessibility/AccessibilityEvent;->setPassword(Z)V
FlagstaffHill.smali smali/com/hellocmu/picoctf 1
.local v0, "password":Ljava/lang/String;
R$string.smali smali/com/hellocmu/picoctf 1
...field public static final password:I = 0x7f0b002f
strings.xml
res > values > strings.xml > resources > string
<resources>
<string name="abc_menu_shift_shortcut_label">Shift+</string>
<string name="abc_menu_space_shortcut_label">space</string>
<string name="abc_menu_sym_shortcut_label">Sym+</string>
<string name="abc_prepend_shortcut_label">Menu+</string>
<string name="abc_search_hint">Search…</string>
<string name="abc_searchview_description_clear">Clear query</string>
<string name="abc_searchview_description_query">Search query</string>
<string name="abc_searchview_description_search">Search</string>
<string name="abc_searchview_description_submit">Submit query</string>
<string name="abc_searchview_description_voice">Voice search</string>
<string name="abc_shareactionprovider_share_with">Share with</string>
<string name="abc_shareactionprovider_share_with_application">Share with %s</string>
<string name="abc_toolbar_collapse_description">Collapse</string>
<string name="app_name">PicoCTF</string>
<string name="bat">mink</string>
<string name="bear">margay</string>
<string name="cottentail">shrew</string>
<string name="gopher">armadillo</string>
<string name="hint">brute force not required</string>
<string name="manatee">caribou</string>
<string name="password">opossum</string>
<string name="porpoise">mouflon</string>
<string name="search_menu_title">Search</string>
<string name="skunk">elk</string>
<string name="status_bar_notification_info_overflow">999+</string>
<string name="vole">beaver</string>
</resources>
muhack.org
Duo
Ri 50, col 27 (8 selezionate)
Spazi: 4
UTF-8
LF
XML



strings.xml - one - Visual Studio Code

ngs.xml

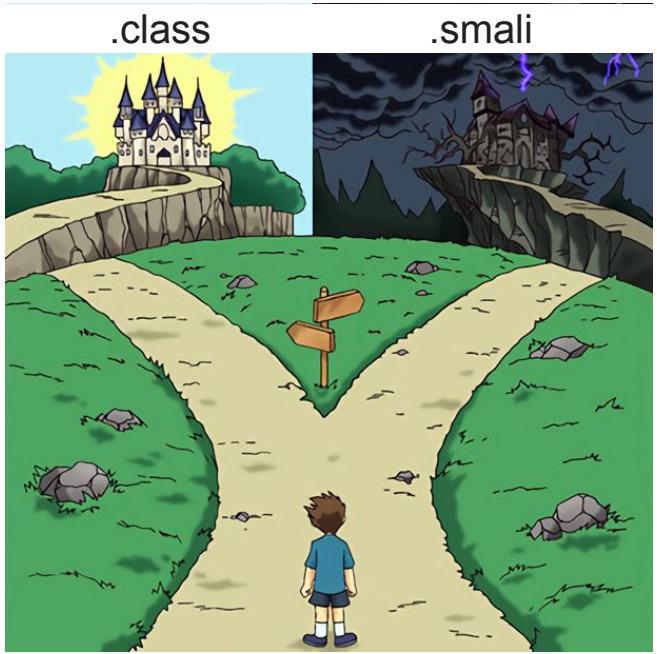
values > strings.xml > resources > string

```
<resources>
    <string name="abc_menu_shift_shortcut_label">Shift+</string>
    <string name="abc_menu_space_shortcut_label">space</string>
    <string name="abc_menu_sym_shortcut_label">Sym+</string>
    <string name="abc_prepend_shortcut_label">Menu+</string>
    <string name="abc_search_hint">Search…</string>
    <string name="abc_searchview_description_clear">Clear query</string>
    <string name="abc_searchview_description_query">Search query</string>
    <string name="abc_searchview_description_search">Search</string>
    <string name="abc_searchview_description_submit">Submit query</string>
    <string name="abc_searchview_description_voice">Voice search</string>
    <string name="abc_shareactionprovider_share_with">Share with</string>
    <string name="abc_shareactionprovider_share_with_application">Share with %s</string>
    <string name="abc_toolbar_collapse_description">Collapse</string>
    <string name="app_name">PicoCTF</string>
    <string name="bat">mink</string>
    <string name="bear">margay</string>
    <string name="cottentail">shrew</string>
    <string name="gopher">armadillo</string>
    <string name="hint">brute force not required</string>
    <string name="manatee">caribou</string>
    <string name="password">opossum</string>
    <string name="porpoise">mouflon</string>
    <string name="search_menu_title">Search</string>
    <string name="skunk">elk</string>
    <string name="status_bar_notification_info_overflow">999+</string>
    <string name="vole">beaver</string>
</resources>
```

muhack.org

Duo Ri 50, col 27 (8 selezionate) Spazi: 4 UTF-8 LF XML

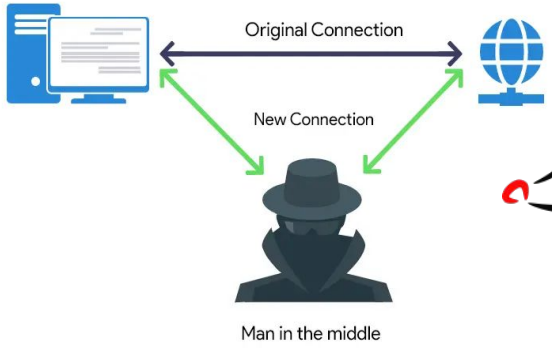
Prima di andare oltre



Reverse Dinamico su Android

Il **reverse engineering dinamico** su Android consiste nell'**analisi di un'applicazione durante la sua esecuzione**.

Si utilizza per **monitorare** chiamate a metodi, **intercettare e modificare** il traffico di rete attraverso un **proxy** e **aggirare protezioni** come il pinning SSL.



Strumentopoli Pt.2

Il mio Setup

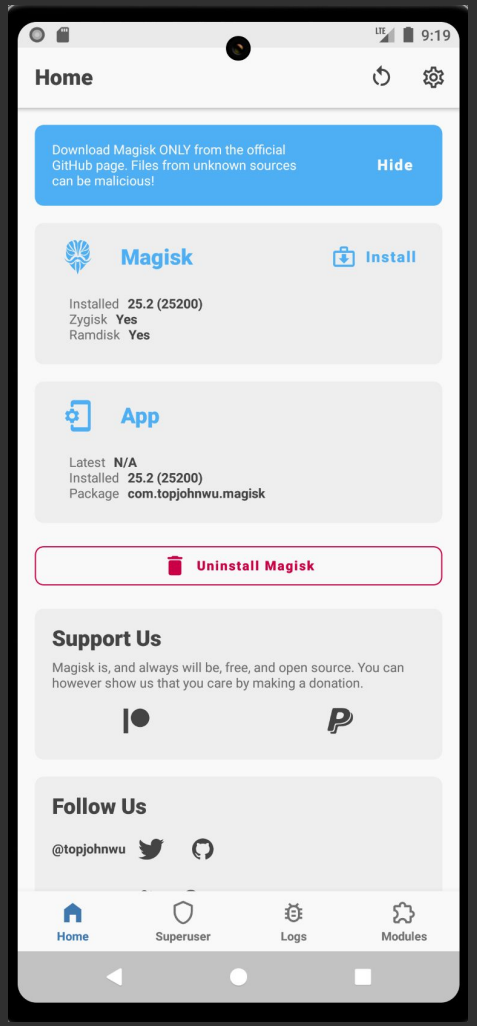
Emulatore Pixel 7a

-> API 26

-> Android 8 x86 Oreo

Per i permessi di root:

https://github.com/newbit1/rootAVD

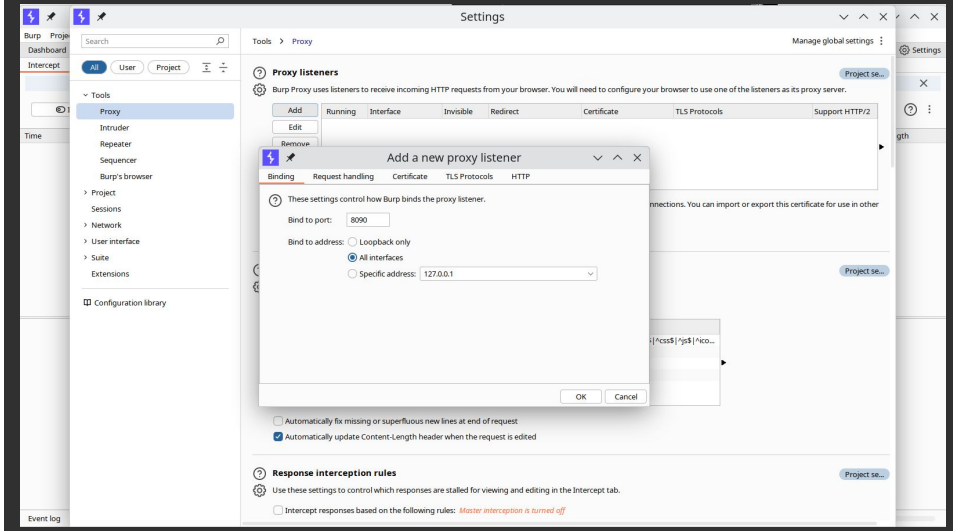


Proxy Setup

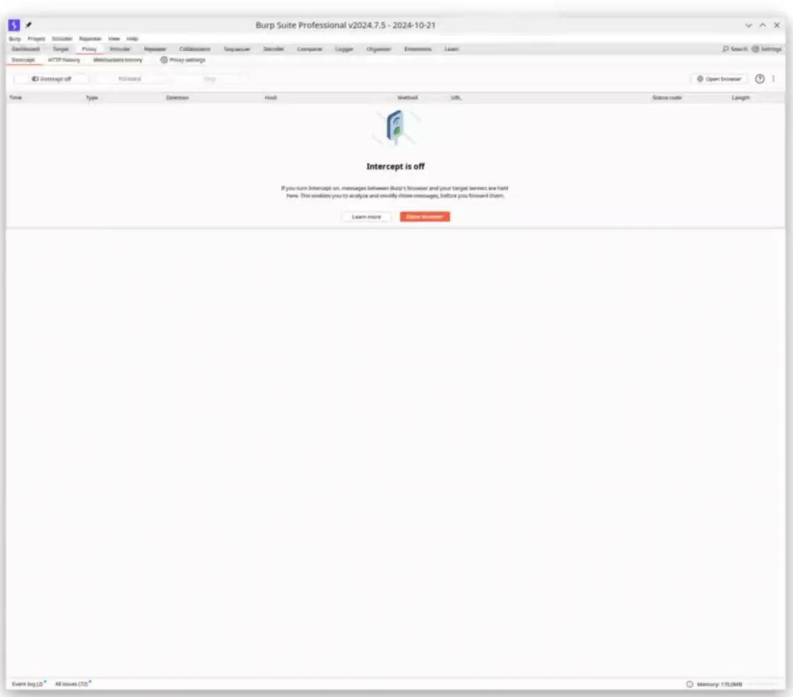
Configurare il proxy con Burp e installare i certificati sull'emulatore può essere abbastanza tedioso

Quindi vi lascio un po' di doc che può aiutare se volete provare:

-> https://portswigger.net/burp/documentation/desktop/mobile/config-android-device
-> https://www.youtube.com/watch?v=qQicUW0svB8



Se siete stati bravi



muhack.org

muhack.org

Quindi?

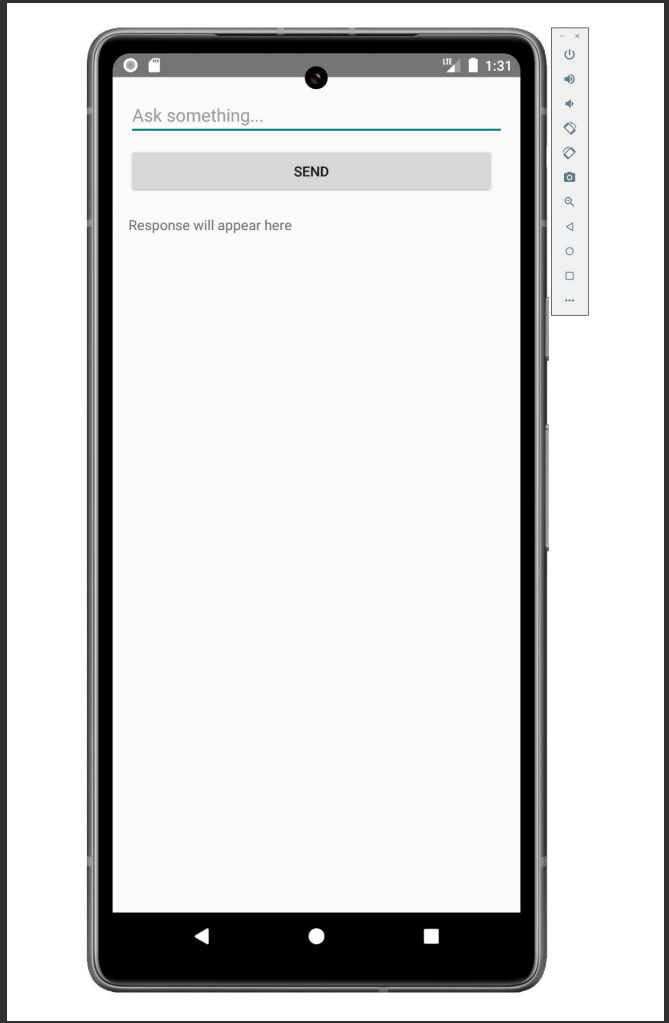
Proxy per la versione Base

Proxy per la versione *pro*, Why doesn't work?

Bypass del pinning SSL

La nostra app di test

Versione Base



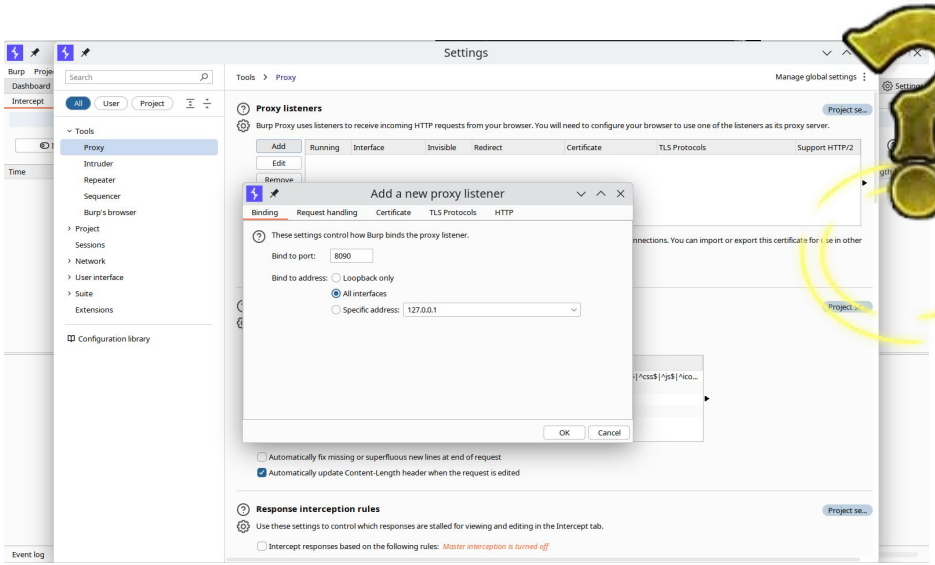
Come funziona

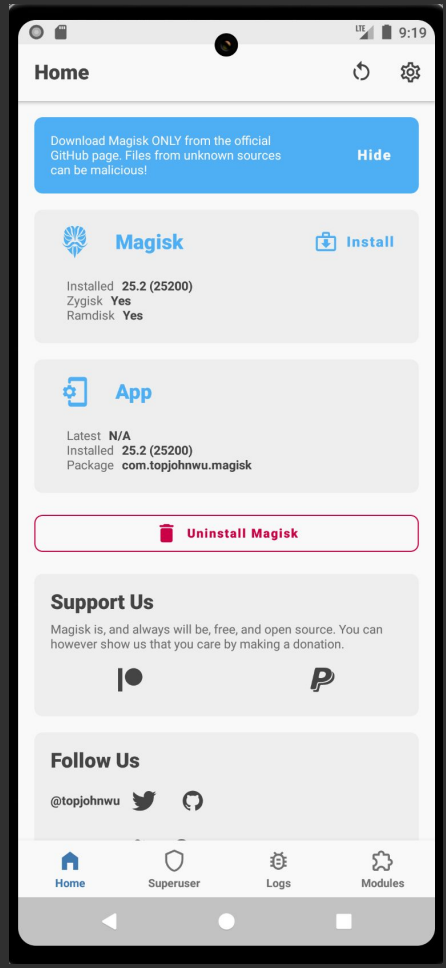
Proxy

Se tutto il setup iniziale con Burp è andato a buon fine il risultato finale è questo:

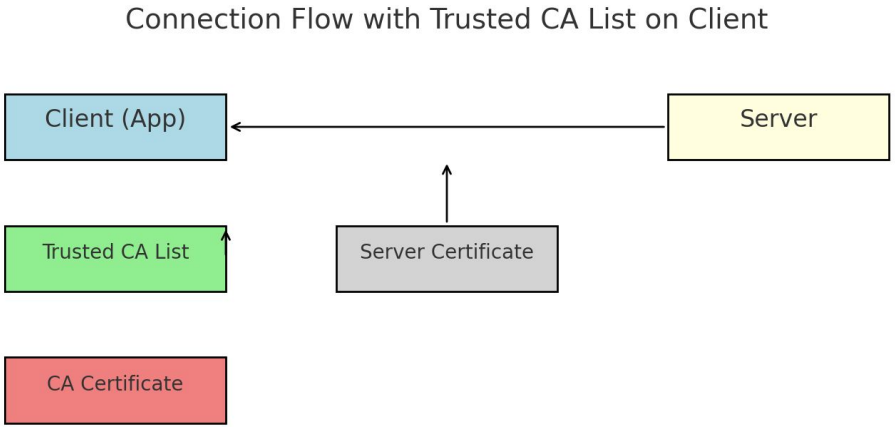
But First

Torniamo indietro

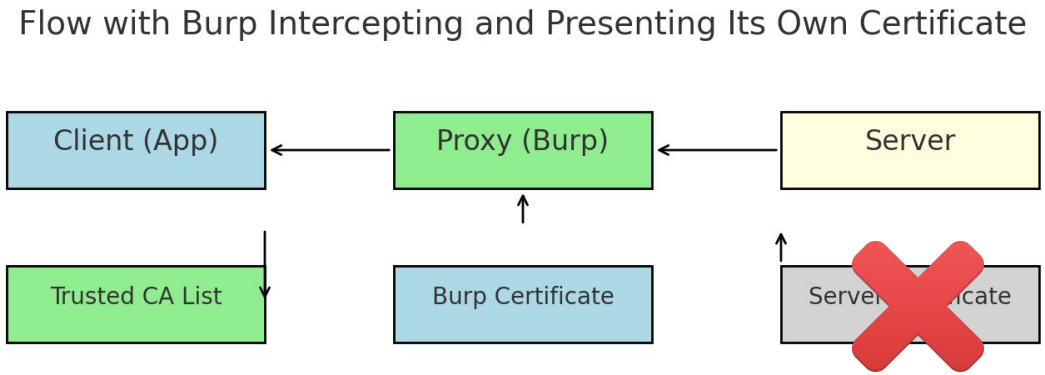


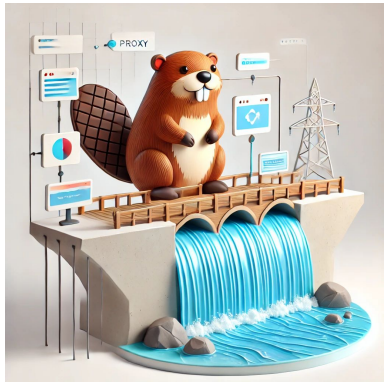


Https e Certificati



Proxy e Burp

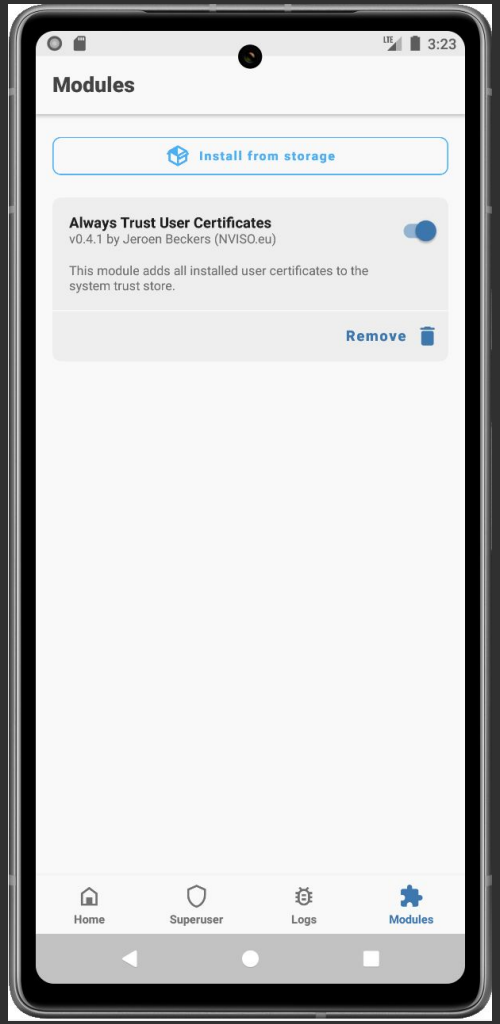




muhack.org

Certificato e permessi di root

Android per motivi di sicurezza non ci permette di installare **certificati** che sono in una **partizione di sola lettura,** quindi se vogliamo installare il nostro certificato abbiamo bisogno dei **permessi di root**



Ma torniamo al nostro esempio

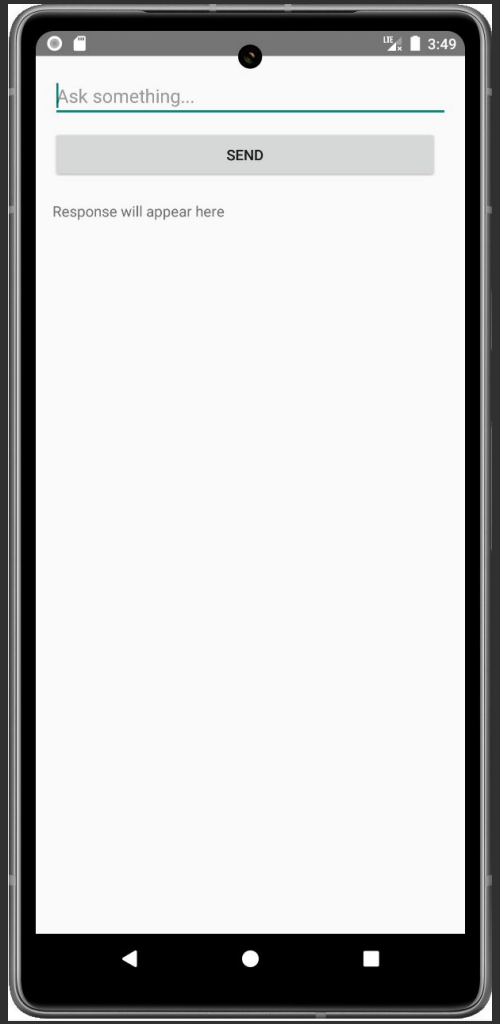
Proxy per la versione Base

Proxy per la versione *pro*, Why doesn't work?

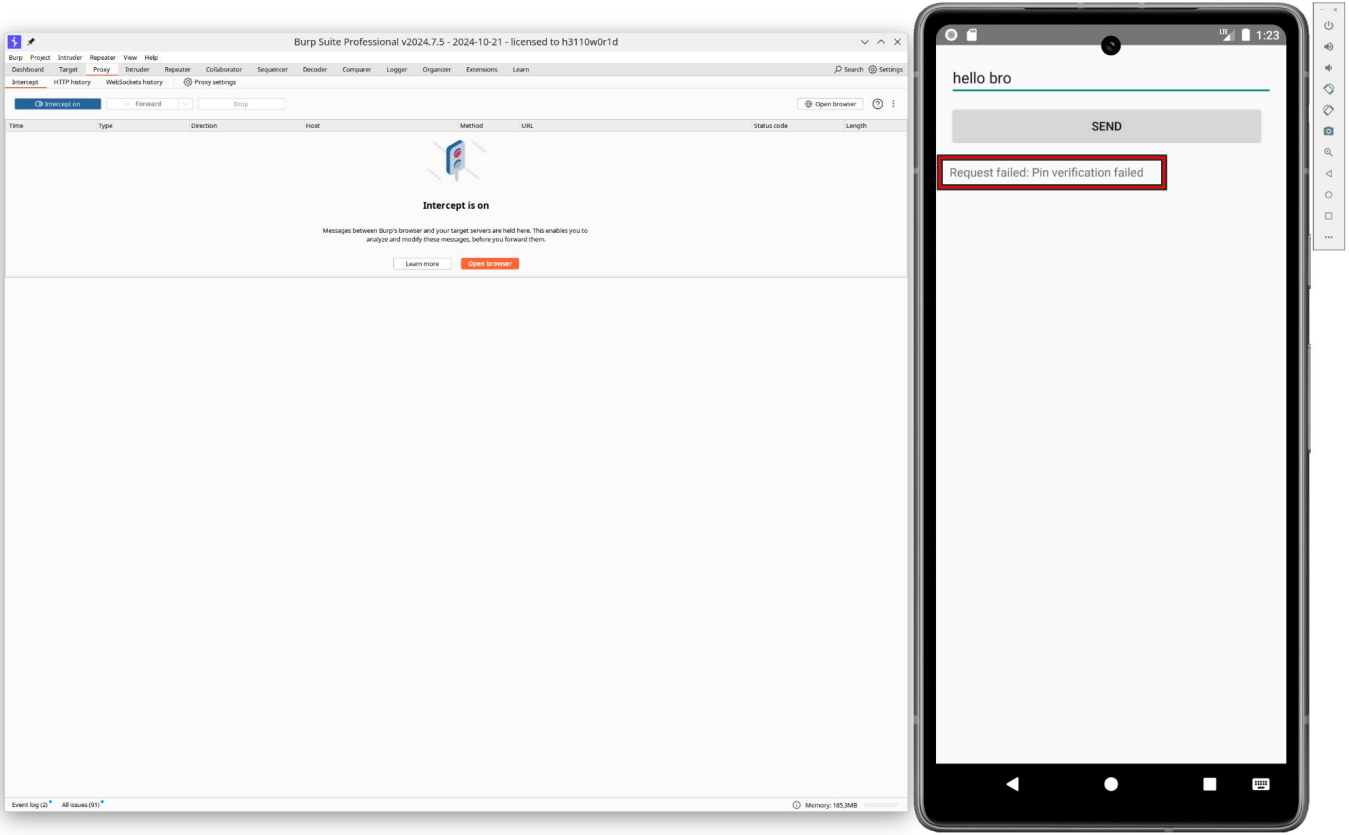
Bypass del pinning SSL

La nostra app di test

Versione PRO



O quasi…


Burp Suite Professional v2024.7.5 - 2024-10-21 - licensed to h3110w0r1d
Intercept is on
Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.
Learn more
Open browser
hello bro
SEND
Request failed: Pin verification failed
1:23

Pinning SSL

Proxy per la versione *pro*, Why doesn't work?

Request fail: Pin verification failed

Il **pinning SSL** è una tecnica di sicurezza utilizzata per rafforzare la verifica dei certificati durante le connessioni HTTPS.

L'applicazione "pinna" uno specifico certificato o chiave pubblica, **limitando le connessioni solo ai server che presentano il certificato esatto o una chiave specifica.**

muhack.org

Quindi cosa facciamo?

Quindi usiamo uno strumentopolo!

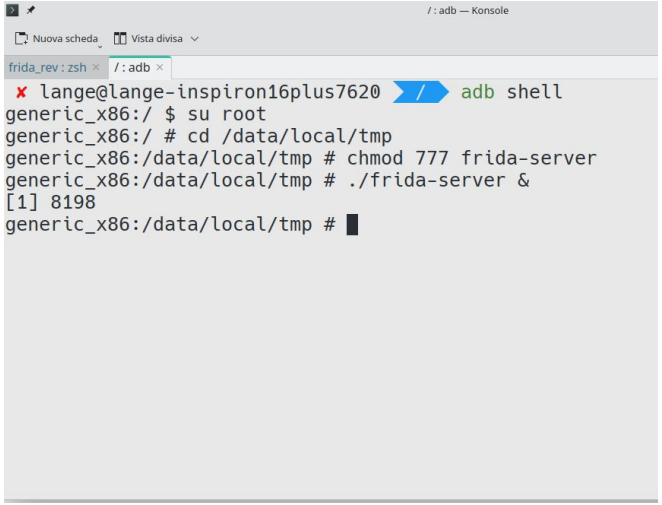
Frida è uno degli strumenti più potenti per il reverse engineering dinamico.

Con Frida, si può **iniettare codice** nell'app in esecuzione e modificare il comportamento del pinning SSL in tempo reale.

muhack.org

How to use Frida?

1. Scarichiamo frida-server
2. Scarichiamo il codice da iniettare*
3. Installiamo frida-server sul telefono e lo avviamo con i giusti permessi

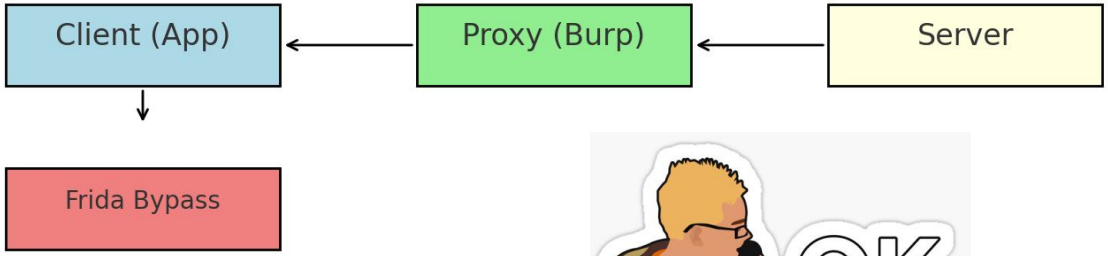


* https://codeshare.frida.re/@pcipolloni/universal-android-ssl-pinning-bypass-with-frida/

Il piano

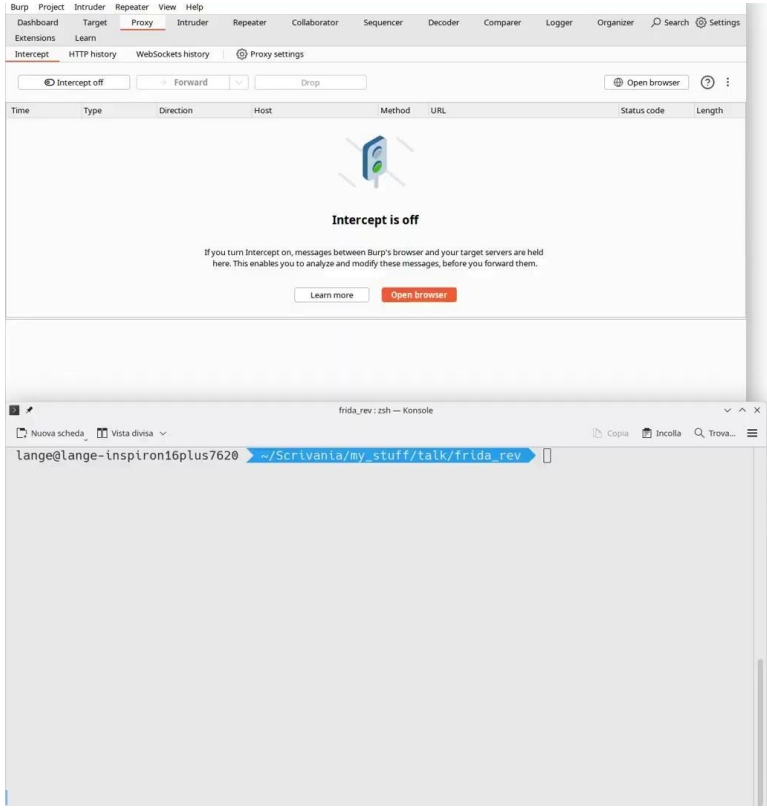
Bypass del pinning SSL

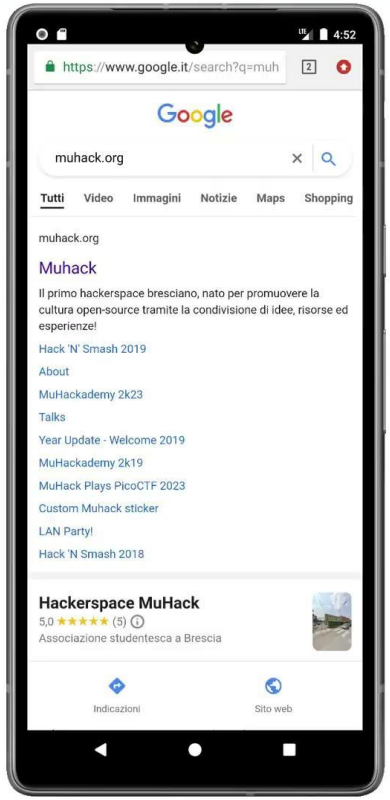
MitM Attack with Frida Bypassing SSL Pinning and Burp Intercepting



muhack.org

Proviamo!


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Search Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Intercept off Forward Drop Open browser
Time Type Direction Host Method URL Status code Length
Intercept is off
If you turn Intercept on, messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.
Learn more Open browser
frida_rev : zsh — Konsole
Nuova scheda Vista divisa Copia Incolla Trova...
lange@lange-inspiron16plus7620 ~/Scrivania/my_stuff/talk/frida_rev


4:52
https://www.google.it/search?q=muh
Google
muhack.org
Tutti Video Immagini Notizie Maps Shopping
muhack.org
Muhack
Il primo hackerspace bresciano, nato per promuovere la cultura open-source tramite la condivisione di idee, risorse ed esperienze!
Hack 'N' Smash 2019
About
MuHackademy 2k23
Talks
Year Update - Welcome 2019
MuHackademy 2k19
MuHack Plays PicoCTF 2023
Custom Muhack sticker
LAN Party!
Hack 'N Smash 2018
Hackerspace MuHack
5,0 (5)
Associazione studentesca a Brescia
Indicazioni
Sito web

Domande?

Grazie per l’attenzione!