Android Anti Anti-Emulator

written by Mert SARICA | 1 January 2017

2014 yılında, T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na bağlı Haberleşme Genel Müdürlüğü tarafından yayımlanan Kurumsal SOME Kurulum ve Yönetim Rehberi'nin yönetici özetinde de belirtildiği üzere, Kurumsal Siber Olaylara Müdahale Ekipleri (SOME), siber olayları bertaraf etmede, oluşması muhtemel zararları önlemede veya azaltmada hayati önemi olan yapılardır.

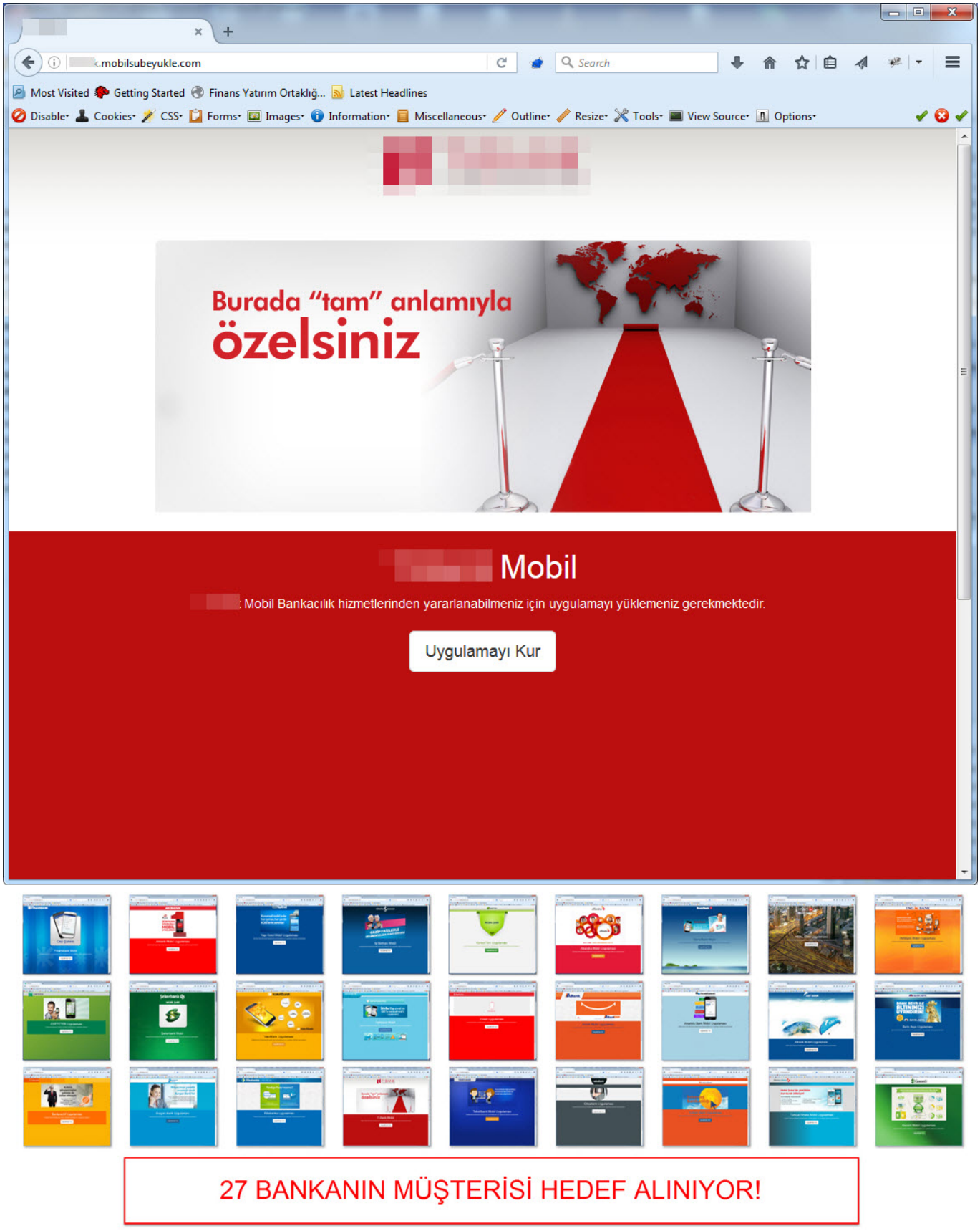
SIEM mühendislerinin, sızma testi uzmanlarının yanı sıra, zararlı yazılım analizi bilgi ve becerisine sahip güvenlik uzmanlarına da sahip olan SOMElerin, kurumların savunmasını güçlendirme ve müşterilerini koruma adına, bu uzmanlıklardan yoksun olan SOMElere kıyasla bir adım daha önde olduklarını söyleyebiliriz. (Tek kişilik dev SOME ekipleri yok sayılmıştır.)

Kritik altyapı sektörlerinden biri olan finans sektöründe yer alan bankaların ve kurumsal SOMElerinin, mobil olsun veya olmasın bankacılık zararlı yazılımlarını yakından takip etmeleri oldukça önemlidir. Kimi zaman bir banka, bankacılık zararlı yazılımlarının gelişimini izleyerek, ileride ne tür bir tehdit ile karşı karşıya kalabileceğini öngörebilir ve hazırlığını yapabilir.

Mobil bankacılık zararlı yazılımlarının dışında, yeni nesil oltalama (phishing) saldırılarının da mobil zararlı yazılım ile gerçekleştiriliyor olması, mobil zararlı yazılım analizi bilgi ve becerisine sahip olan güvenlik uzmanlarına olan ihtiyacı da ortaya koymaktadır.

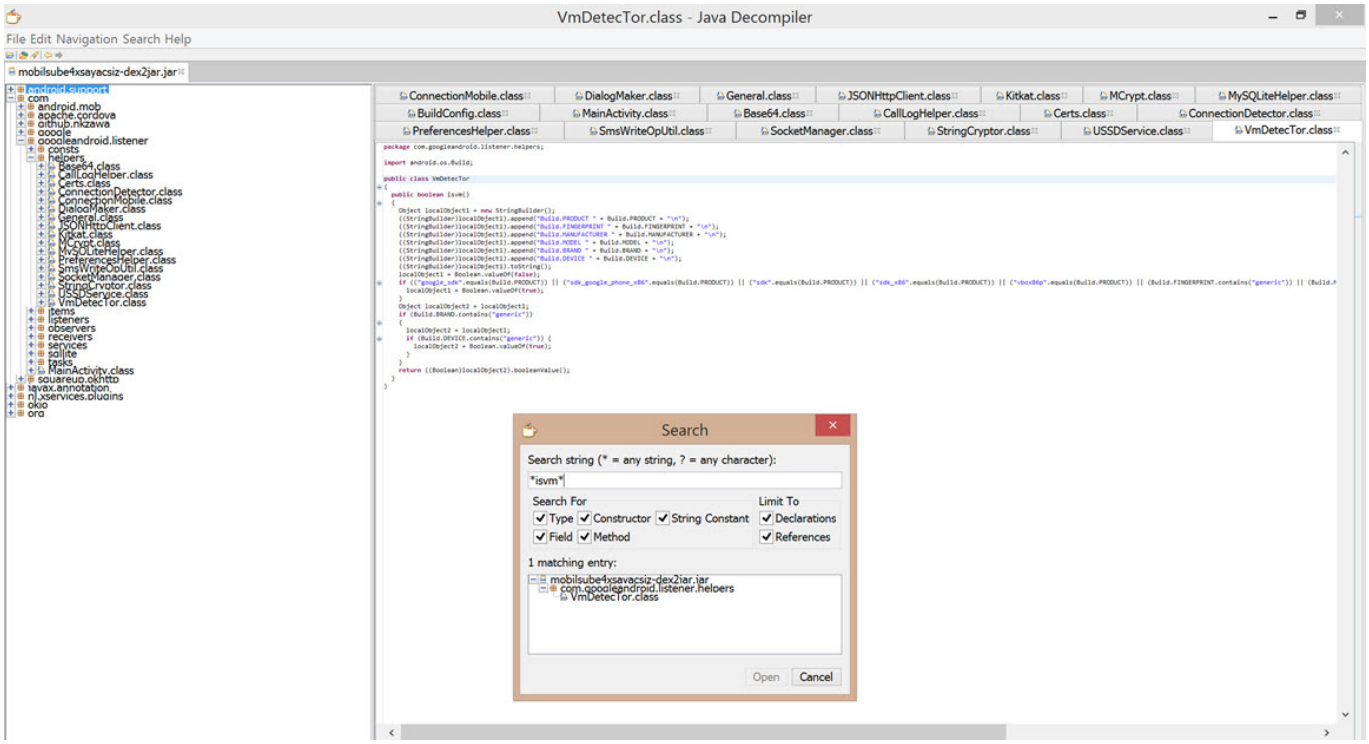
2015 yılı ortalarında bankalar, müşterilerini hedef alan ve Bakır EMRE'nin de detaylı bir şekilde analiz etmiş olduğu Android zararlı yazılımı ile karşı karşıya kaldılar.

2016 yılının ortasına geldiğimizde ise bu Android zararlı yazılımını geliştirenlerin, zararlı yazılıma TOR üzerinden haberleşme özelliği de eklediklerini gördük. Bununla da kalmayarak Türkiye'de faaliyet gösteren 51 tane bankadan (2015 yılı rakamları) 27 tanesine ait sahte sayfaları da (banka.mobilsubeyukle.com) web sayfalarında oluşturduklarına tanık olduk.

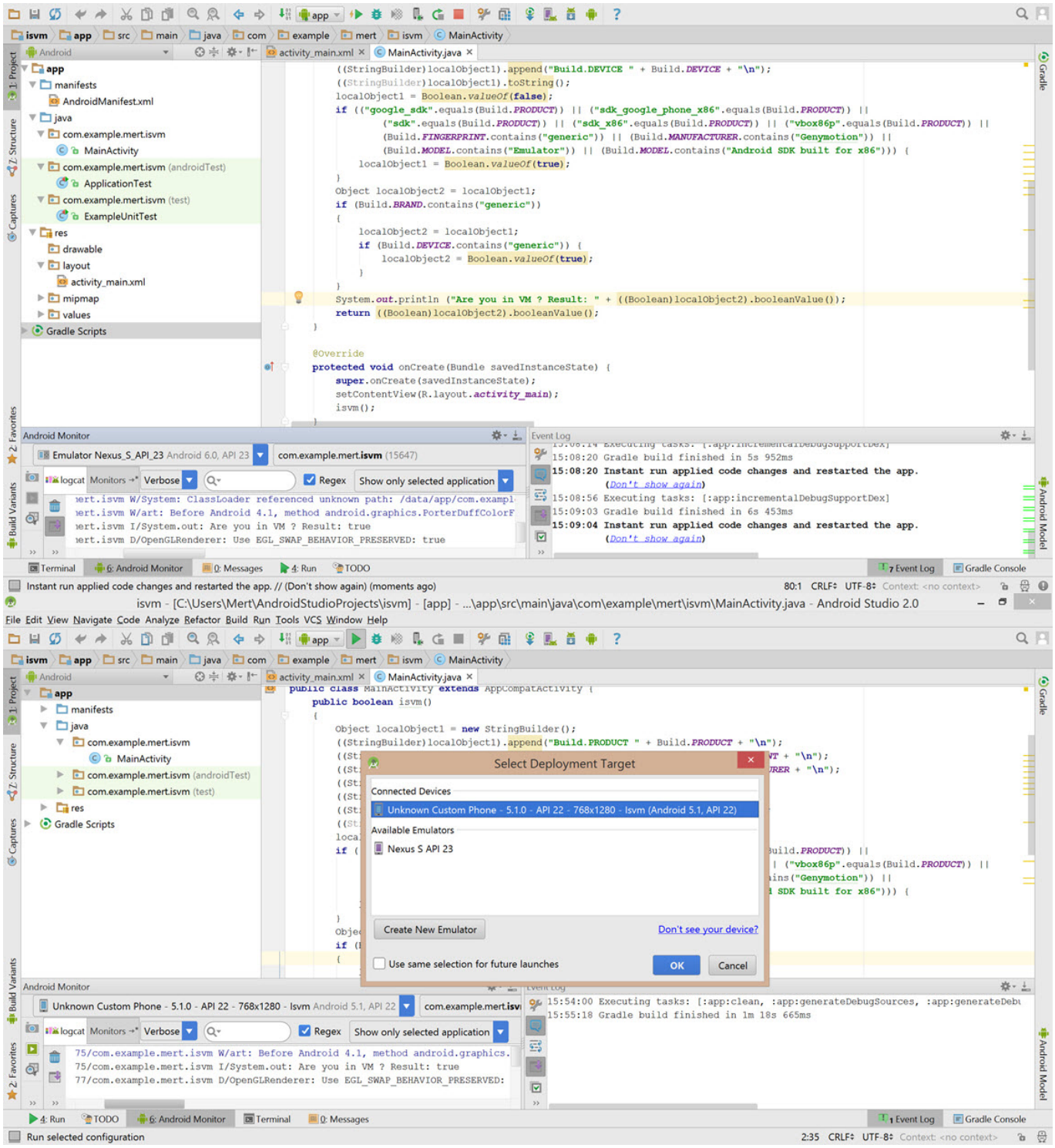


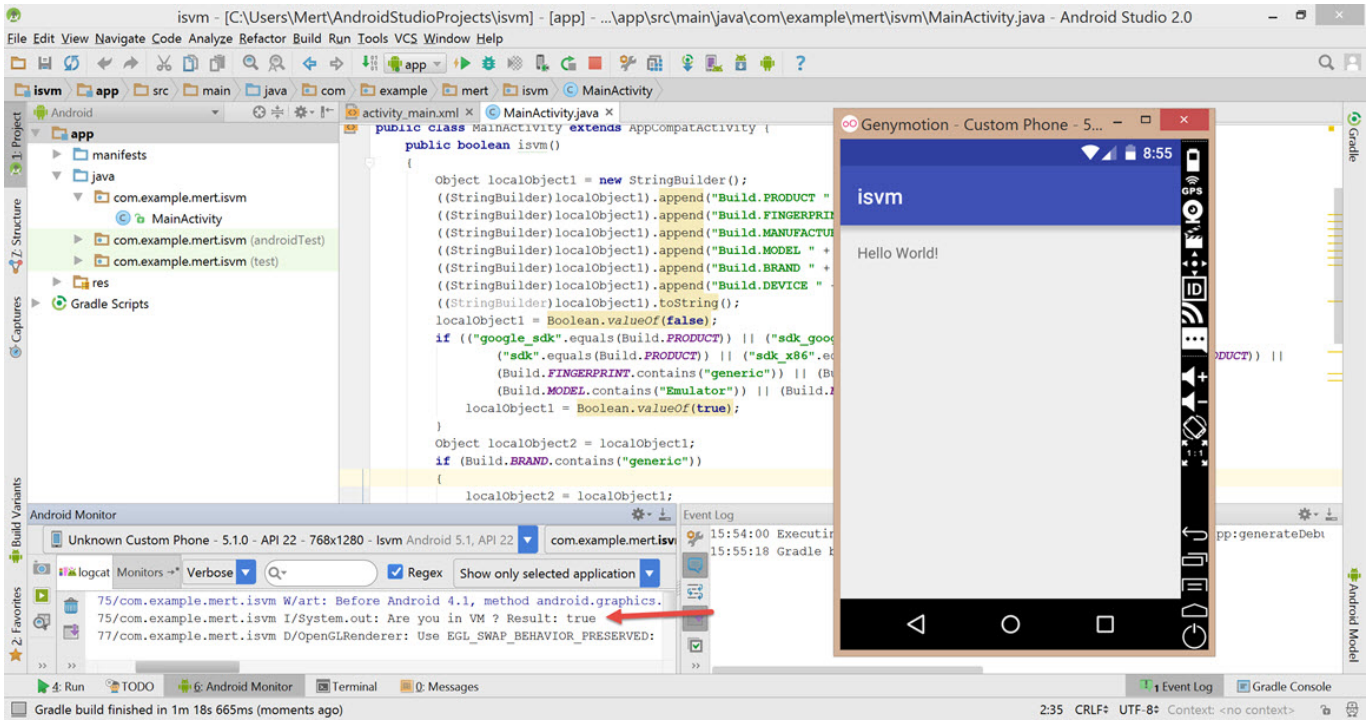
Zararlı yazılımı analiz ederken, Türkçe fonksiyon isimlerinin yanı sıra, isvm isimli başka bir fonksiyon adı dikkatimi çekti. Fonksiyonun başka herhangi bir fonksiyon tarafından çağrılmamış olması da (xref), bana ilerleyen sürümlerde bu fonksiyon ile karşılaşacağımız mesajını verdi. Fonksiyona baktığımda bunun güvenlik uzmanları tarafından zararlı yazılımı analizinde de

kullanılan Android Emulator, Genymotion öykünücülerini (emulator), tespit etmeye yönelik olduğunu gördüm. Hayata geçtiğinde bunu en kolay ne şekilde atlatabilirim diye üzerinde çalışmaya başladım.

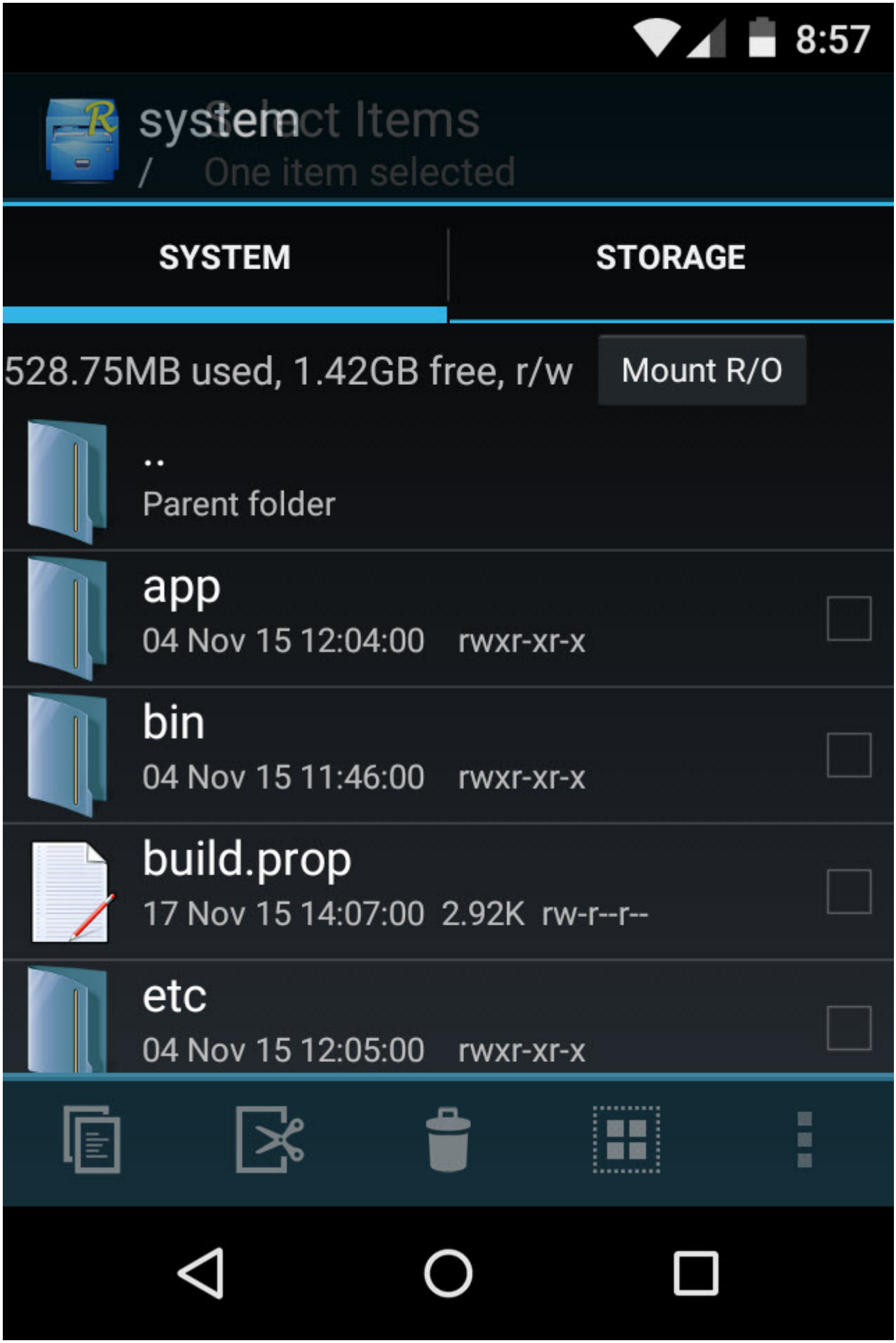


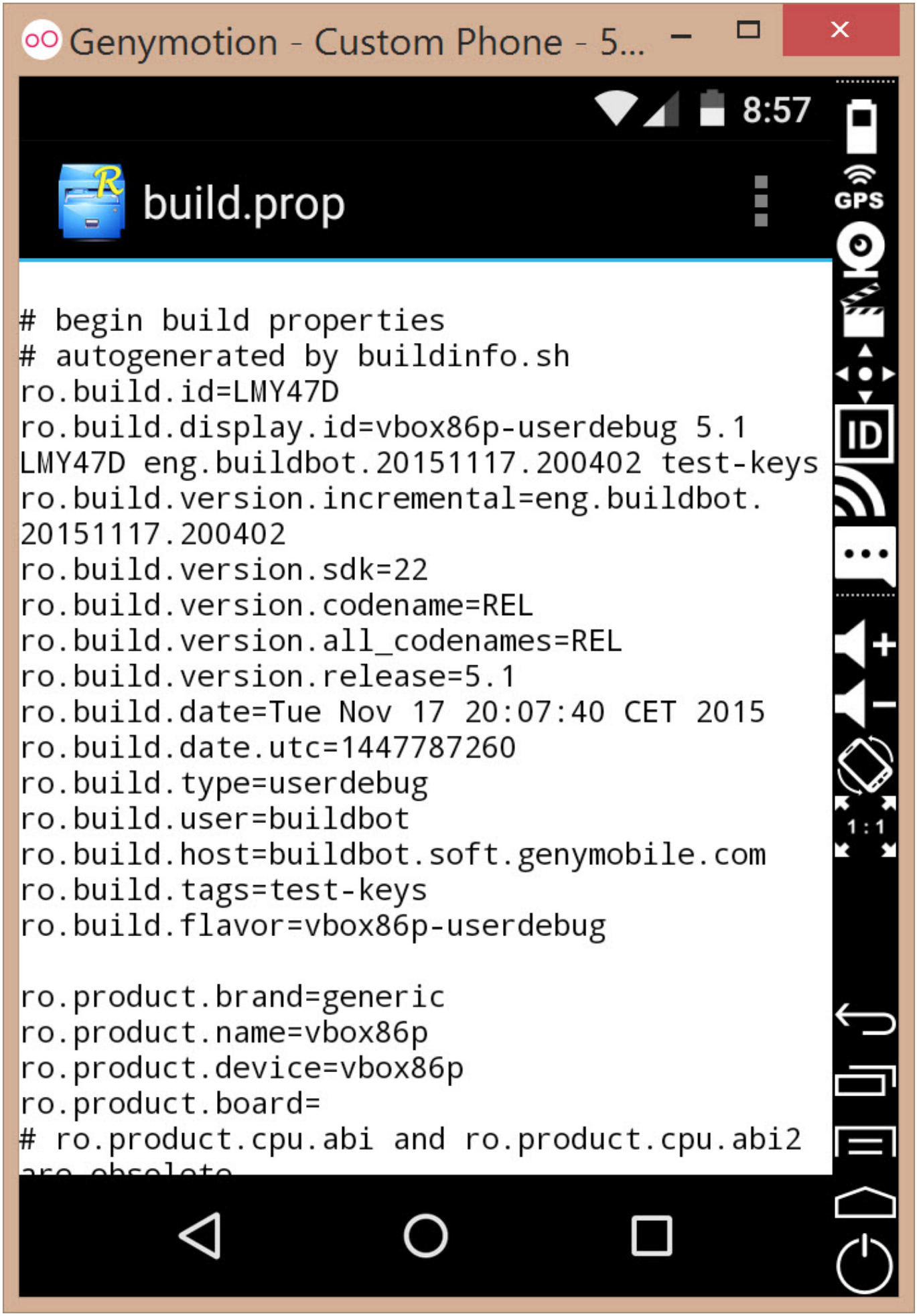
İlk olarak Google tarafından Android uygulaması geliştirmek amacıyla ücretsiz olarak dağıtılan Android Studio sürümünü kurup, jD-GUI (Java Decompiler) ile elde ettiğim isvm fonksiyonunu, tespit sonucunu çıktı olarak da gösterecek şekilde (Are you in in VM ? Result:) değiştirdikten sonra öykünücü içinde çalıştıracak bir kod hazırladım.

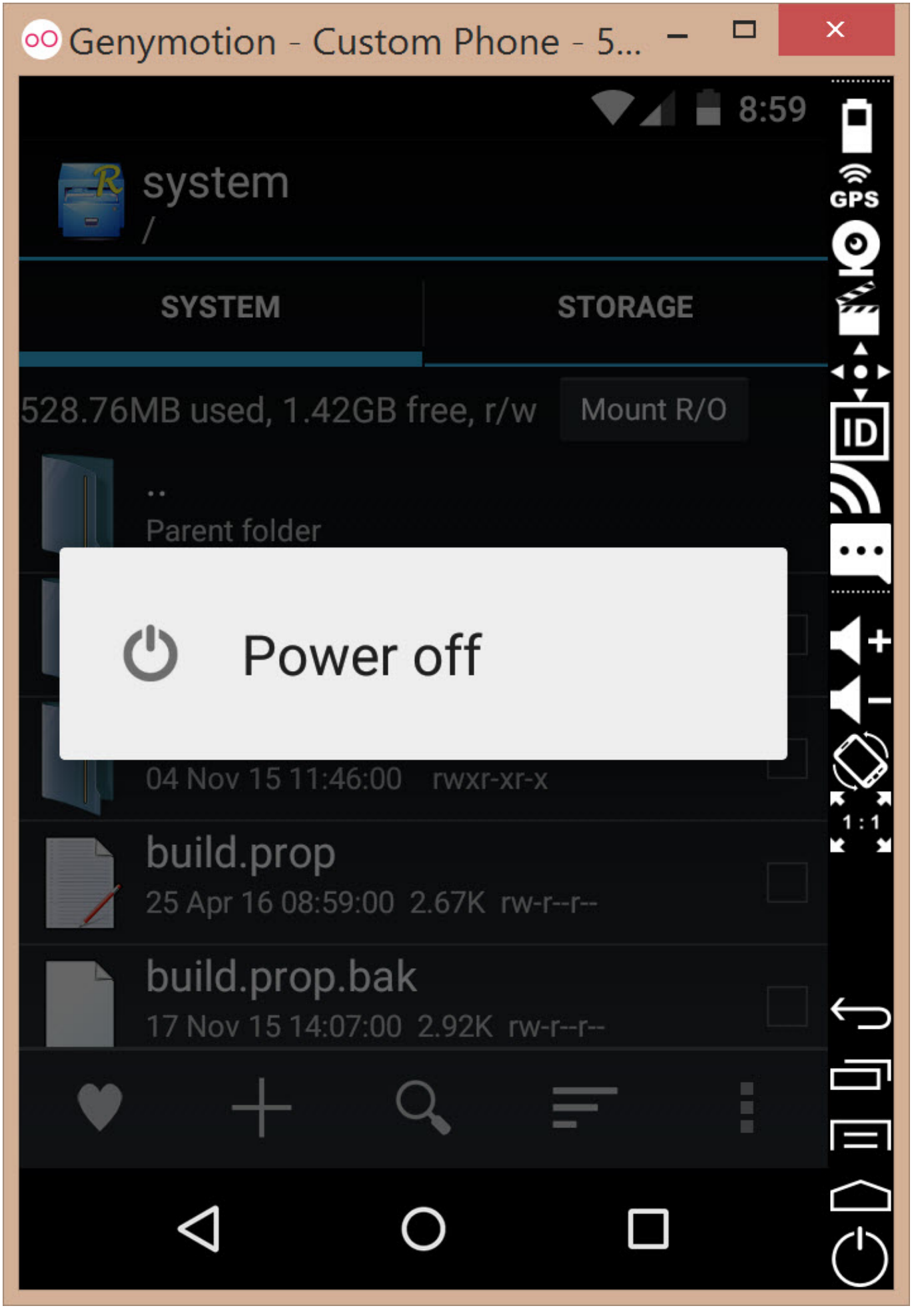

isvm - [C:\Users\Mert\AndroidStudioProjects\isvm] - [app] - ...\app\src\main\java\com\example\mert\isvm\MainActivity.java - Android Studio 2.0
File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help
Select Deployment Target
Connected Devices
Unknown Custom Phone - 5.1.0 - API 22 - 768x1280 - Isvm (Android 5.1, API 22)
Available Emulators
Nexus S API 23
Create New Emulator
Don't see your device?
Use same selection for future launches
OK
Cancel
Android Monitor
Event Log
Run selected configuration

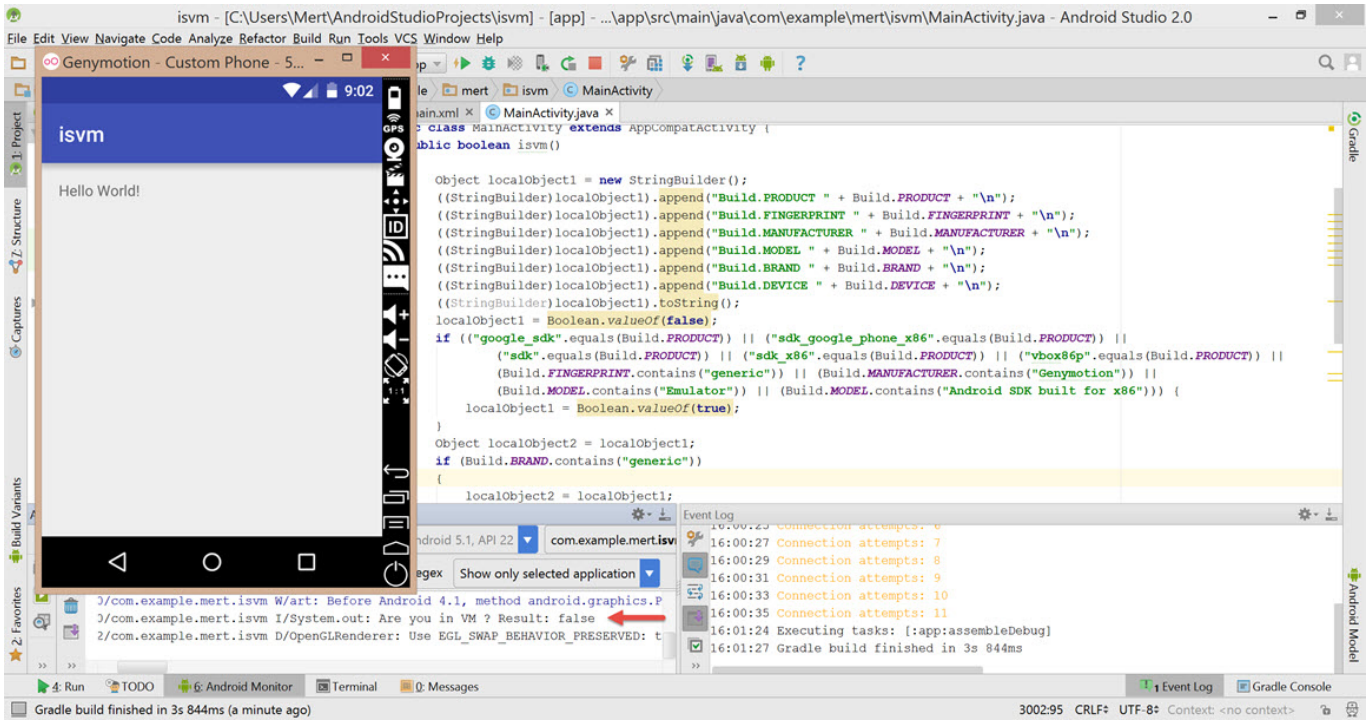


İlgili kod, öykünücüleri Build.PRODUCT, Build.FINGERPRINT, Build.MANUFACTURE, Build.MODEL, Build.BRAND, Build.DEVICE değerlerine göre tespit ettiği için (Are you in in VM ? Result: true) bunları GenyMotion üzerinde çalışan Custom Phone – 5.1.0 – API 22 imajında nasıl değiştirebileceğimi araştırmaya başladım. Çok geçmeden /system/build.prop dosyasında cihaz üreticisine dair bu değerlerin yer aldığını buldum. Genymotion öykünücüsünde yer alan imajlar root yetkisi ile çalıştığı için Root Explorer uygulamasını kurduktan sonra /system/build.prop dosyasında yer alan ve tespit için kullanılan değerleri teker teker silmeye başladım. Ardından dosyayı kayıt, edip öykünücüyü yeniden başlatıp öykünücü kontrolünü gerçekleştiren isvm kodunu/uygulamasını tekrar çalıştırdığımda bu defa öykünücü tespitini IDA ile uğraşmadan sistem üzerinde ufak bir değişiklikle atlatabilmiş (Are you in in VM ? Result: false) oldum :)


8:57
system
Select Items
/ One item selected
SYSTEM
STORAGE
528.75MB used, 1.42GB free, r/w
Mount R/O
..
Parent folder
app
04 Nov 15 12:04:00 rwxr-xr-x
bin
04 Nov 15 11:46:00 rwxr-xr-x
build.prop
17 Nov 15 14:07:00 2.92K rw-r--r--
etc
04 Nov 15 12:05:00 rwxr-xr-x


Genymotion - Custom Phone - 5...
8:57
build.prop
# begin build properties
# autogenerated by buildinfo.sh
ro.build.id=LMY47D
ro.build.display.id=vbox86p-userdebug 5.1
LMY47D eng.buildbot.20151117.200402 test-keys
ro.build.version.incremental=eng.buildbot.
20151117.200402
ro.build.version.sdk=22
ro.build.version.codename=REL
ro.build.version.all_codenames=REL
ro.build.version.release=5.1
ro.build.date=Tue Nov 17 20:07:40 CET 2015
ro.build.date.utc=1447787260
ro.build.type=userdebug
ro.build.user=buildbot
ro.build.host=buildbot.soft.genymobile.com
ro.build.tags=test-keys
ro.build.flavor=vbox86p-userdebug
ro.product.brand=generic
ro.product.name=vbox86p
ro.product.device=vbox86p
ro.product.board=
ro.product.cpu.abi and ro.product.cpu.abi2
GPS
1:1


Genymotion - Custom Phone - 5...
8:59
system
/
SYSTEM
STORAGE
528.76MB used, 1.42GB free, r/w
Mount R/O
..
Parent folder
Power off
04 Nov 15 11:46:00 rwxr-xr-x
build.prop
25 Apr 16 08:59:00 2.67K rw-r--r--
build.prop.bak
17 Nov 15 14:07:00 2.92K rw-r--r--
GPS
ID
1:1



Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.