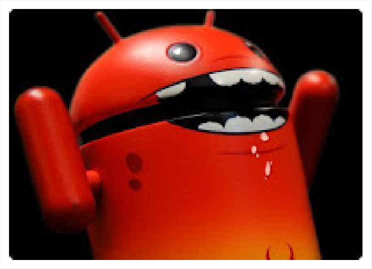
Cybersecurity Blog

Everything about threat intelligence, blue team, red team, pentesting, security audit, security review, testing and assessment.

Monday, October 31, 2016

Blocking Adwares on Android - Protect against malwares and privacy



According to Mcafee, "A company from India has released an advertising software developer kit (SDK) called SilverPush that uses your phone's microphone to listen for near-ultrasonic sounds placed in TV, radio and Web advertisements. Once SilverPush detects the signal, it collects data from your device and sends information about your device back to the advertiser. While this is not a piece of malware, it is a huge concern from a privacy perspective. It collects personal information from your device, including, but not limited to:

- IMEI number (a unique number that identifies your phone)
- Operating system version
- Location
- Potentially the identity of the owner
- The user's television, radio and Web behavior

SilverPush is not a standalone app, but is embedded as part of another application and typically runs without the user's consent. If an application on your mobile device is detected as containing SilverPush, the best solution is to remove that application from your device."

I searched various mobile threats. Well zero days we can not protect and detect in advance obviously. So I tried to block all advertisements and here is the takeout.

We will require to install AdAway application. Unfortunately this application requires rooted device because it is directly interacting **/etc/hosts** file.

Translate Language

Search

Search

Subscribe via email

Email address... Submit

Blog Archive

- ► 2020 (2)
- ► 2019 (6)
- ► 2018 (4)
- ► 2017 (5)
- ▼ 2016 (11)
  - ► November 13 (1)
  - ▼ October 30 (1)
    - Blocking Adwares on Android - Protect against malw...
  - ► October 23 (1)
  - ► October 9 (1)
  - ► September 11 (1)
  - ► September 4 (1)
  - ► July 17 (1)

You must have got the idea what I am talking about. Yes we are going to add all advertisement websites names within our **/etc/hosts** files so that it will not be able to connect. Here is how.

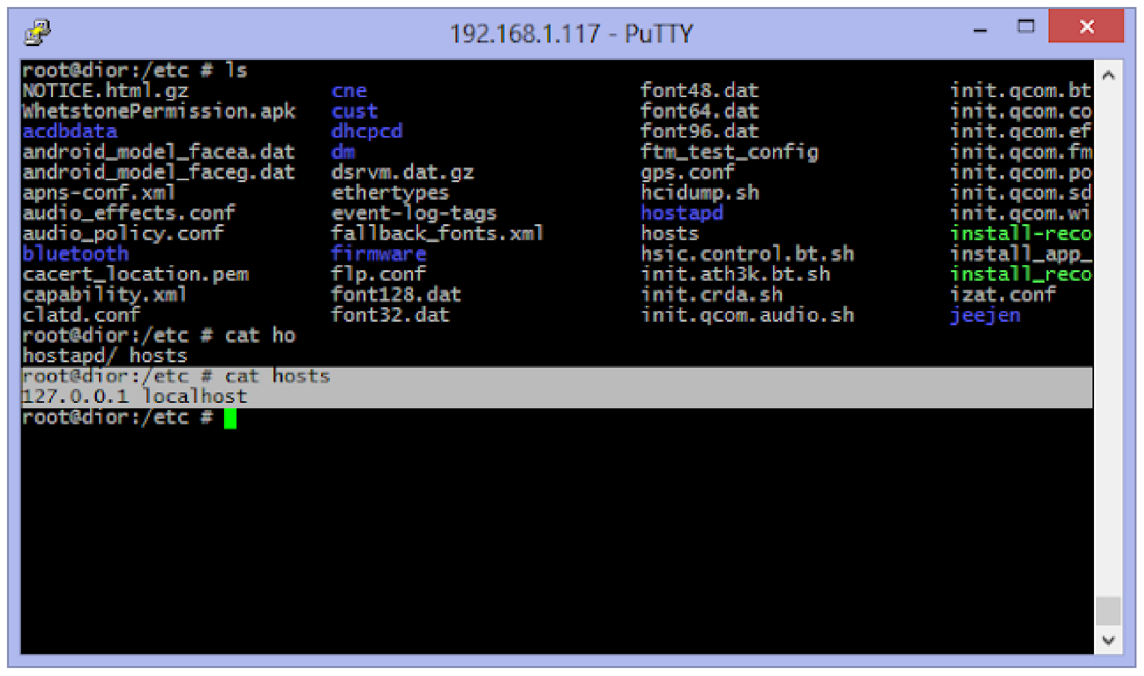
What is /etc/hosts and what does it do?
The hosts file is one of several system facilities that assists in addressing network nodes in a computer network. It is a common part of an operating system's Internet Protocol (IP) implementation, and serves the function of translating human-friendly hostnames into numeric protocol addresses, called IP addresses, that identify and locate a host in an IP network. In some operating systems, the hosts file's content is used preferentially to other methods, such as the Domain Name System (DNS), but many systems implement name service switches (e.g., nsswitch.conf for Linux and Unix) to provide customization. Unlike the DNS, the hosts file is under the direct control of the local computer's administrator.

It means that the system will not do a DNS lookup for mydomain, it will be automatically redirected to the IP address you specified in your hosts file.

Target: Add all adblocker websites to your /etc/hosts files.
How and where to get all list: Adaway Application.

Scenario 1: Without advertisement blocking protection.

Currently your phone's default /etc/hosts file would look like below screenshot.



192.168.1.117 - PuTTY

```
root@dior:/etc # ls
NOTICE.html.gz            cne                       font48.dat                init.qcom.bt
WhetstonePermission.apk   cust                      font64.dat                init.qcom.co
acdbdata                  dhcpcd                    font96.dat                init.qcom.ef
android_model_facea.dat   dm                        ftm_test_config           init.qcom.fm
android_model_faceg.dat   dsrvm.dat.gz              gps.conf                  init.qcom.po
apns-conf.xml             ethertypes                hcidump.sh                init.qcom.sd
audio_effects.conf        event-log-tags            hostapd                   init.qcom.wi
audio_policy.conf         fallback_fonts.xml        hosts                     install-reco
bluetooth                 firmware                  hsic.control.bt.sh        install_app_
cacert_location.pem       flp.conf                  init.ath3k.bt.sh          install_reco
capability.xml            font128.dat               init.crda.sh              izat.conf
clatd.conf                font32.dat                init.qcom.audio.sh        jeejen
root@dior:/etc # cat ho
hostapd/ hosts
root@dior:/etc # cat hosts
127.0.0.1 localhost
root@dior:/etc #
```

▶ May 1 (1)
▶ April 10 (1)
▶ April 3 (2)

▶ 2015 (4)
▶ 2014 (22)
▶ 2013 (58)

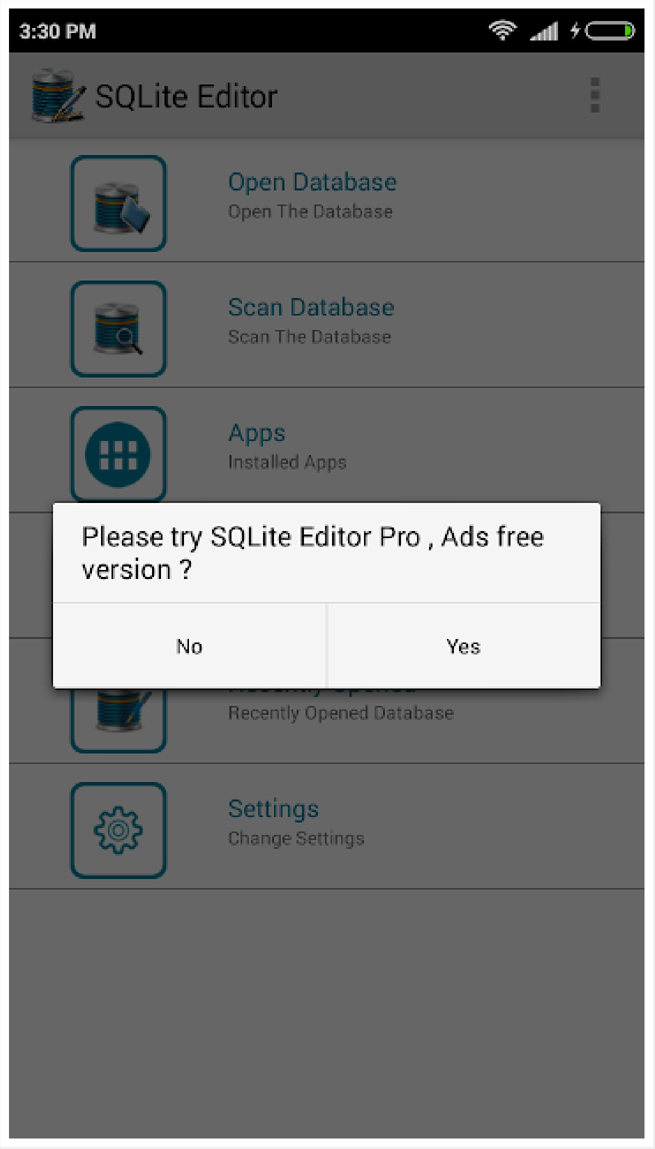
On most systems the default entry in the hosts file is:

```
127.0.0.1    localhost
```

127.0.0.1 is always the address of the computer you're on. For example, if you run a web server on your pc, you can access it from the web browser via the http://localhost:port instead of typing the whole IP address http://127.0.0.1:port.

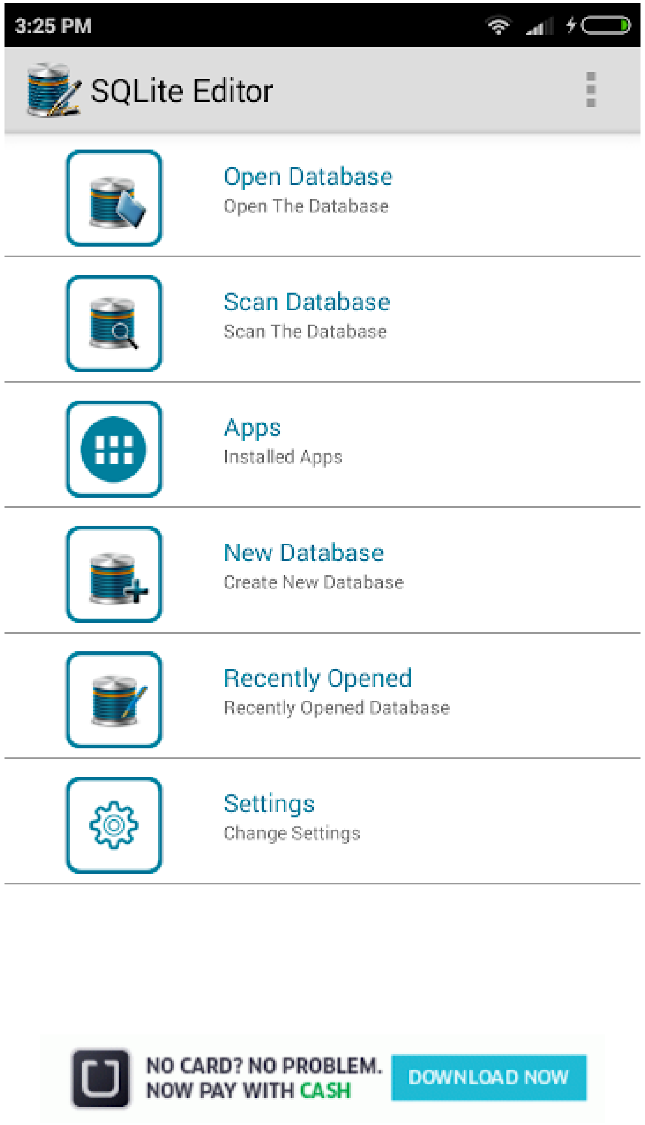
So I can assume that any application, browser which will connect to any 3rd party advertisement company will be connected and work in silent mode without user's consent. What add companies takes user data, we are unaware.

For the demo purpose I am going to use 'SQLite editor' application. This application provides GUI access of each application's database. It is famous among pentester. Now this application comes in two versions. If we purchase it we will get add free version as this free version from playstore will contain advertisements within the application.



Please try SQLite Editor Pro , Ads free version ?

Now lets just use this application in normal way. You will observe that it will provide many adds while we use it.



3:25 PM

SQLite Editor

Open Database
Open The Database

Scan Database
Scan The Database

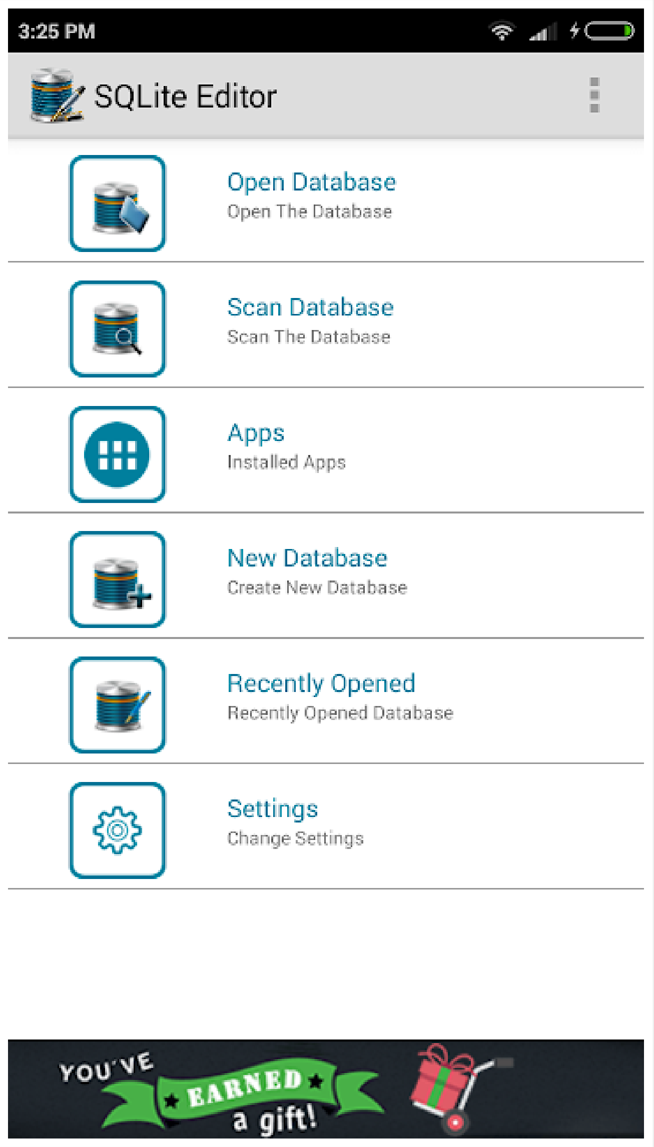
Apps
Installed Apps

New Database
Create New Database

Recently Opened
Recently Opened Database

Settings
Change Settings

Uber Add



3:25 PM

SQLite Editor

Open Database
Open The Database

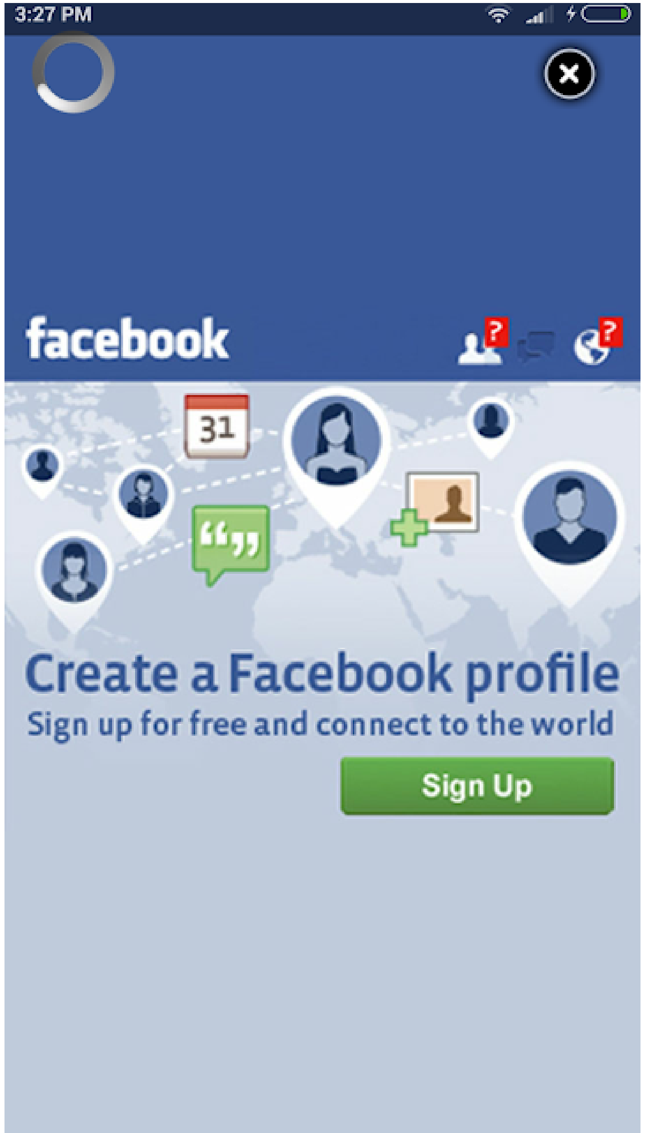
Scan Database
Scan The Database

Apps
Installed Apps

New Database
Create New Database

Recently Opened
Recently Opened Database

Settings
Change Settings


3:27 PM
facebook
Create a Facebook profile
Sign up for free and connect to the world
Sign Up

Facebook add

"Now I am not sure why Facebook brand will give their add in small security related application lying on playstore which has nearly 10000+ users only. It can be phishy.."

Scenario 2: How to block contents using hosts file.

For the demo purpose I am adding facebook domain to my host file and giving ip 127.0.0.1. That means I am telling my mobile to not to look for DNS in order to resolve the IP from the domain name as I am telling that facebook's IP is 127.0.0.1. Now application and browser on my mobile device will try to connect to 127.0.0.1 thus by landing nowhere on the internet and this is how we will block facebook through host file.

Before moving foward, let me inform you that you can not simply edit host file as it has only read-only permission.

Once we root the phone yes we have root access, but we can not edit content. For that we need to remount /system to be read/write access using following command.

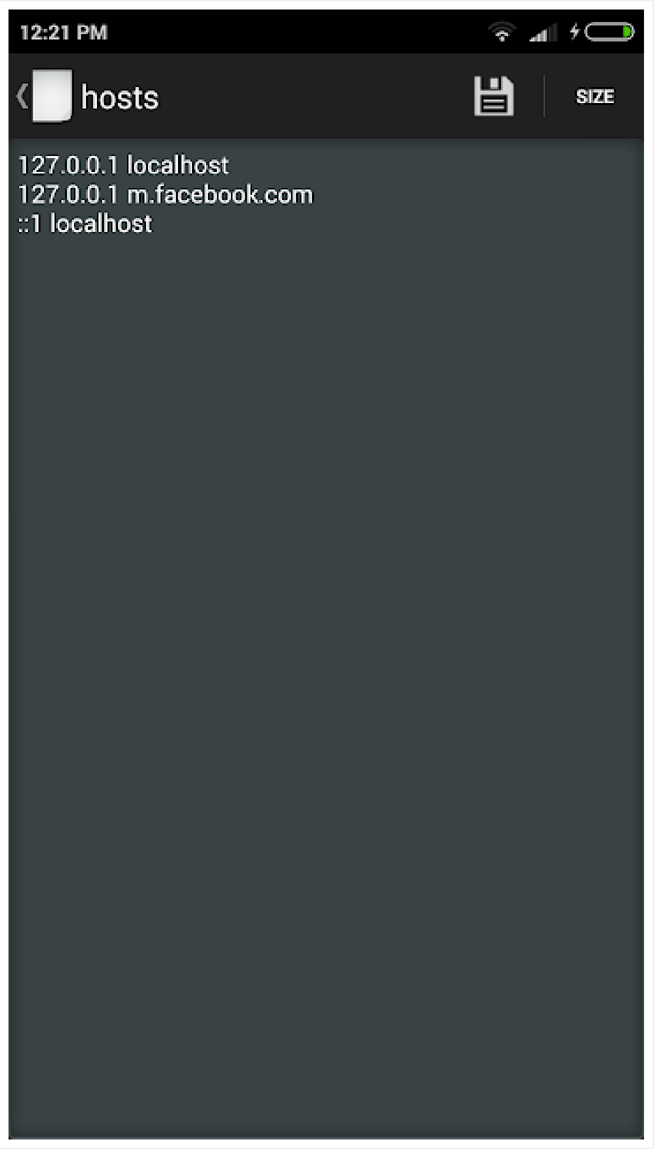
$ adb shell

$ su

$ mount -o rw,remount -t yaffs2 /dev/block/mtdblock3 /system

In case if you do not want to fall into this huddle, you can simply use "Root Browser" application to do this. Using root browser, you can navigate to whole system and edit files.

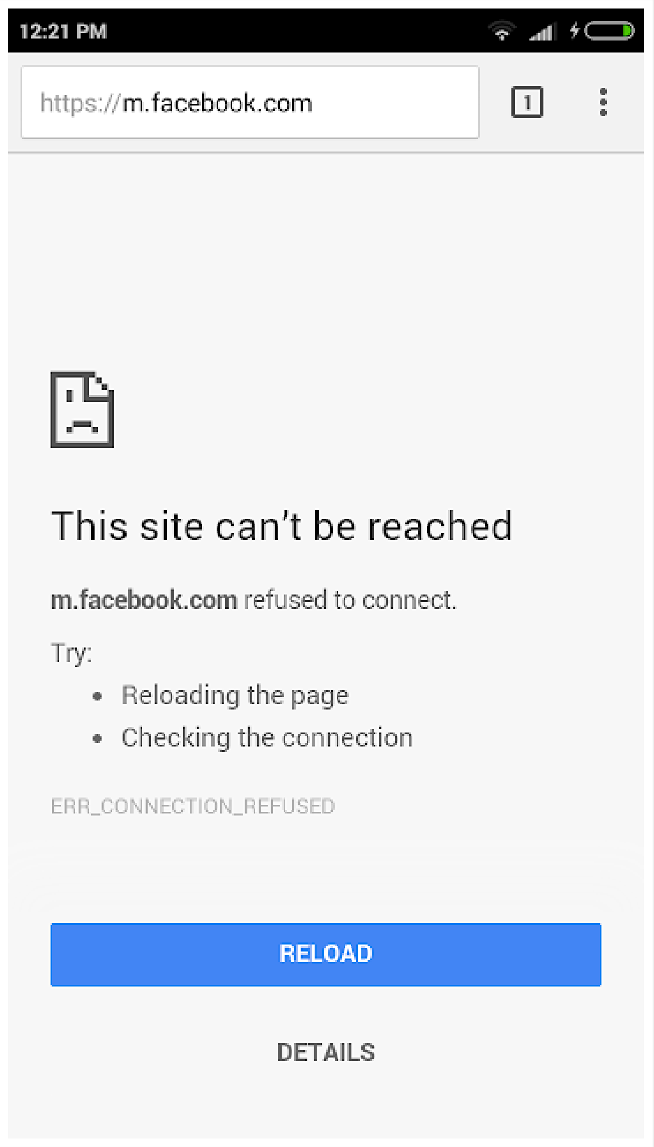
Now I am going to add facebook domain to hosts file as mentioned below.



```
127.0.0.1 localhost
127.0.0.1 m.facebook.com
::1 localhost
```

After adding content click on save.

Now try to access m.facebook.com domain through chrome browser on your mobile phone.



12:21 PM

https://m.facebook.com

This site can’t be reached

m.facebook.com refused to connect.

Try:

- Reloading the page
- Checking the connection

ERR_CONNECTION_REFUSED

Bingo!! We blocked.

Question: How to gather all add block websites and insert into hosts file.

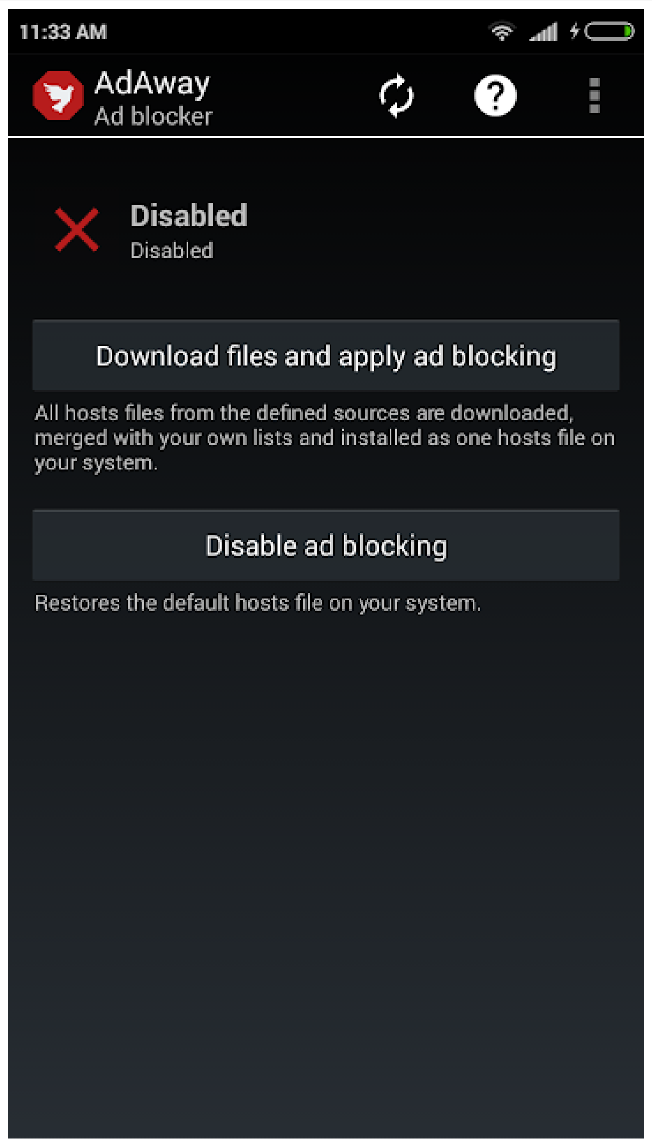
Adaway in action

AdAway is an open source ad blocker for Android using the hosts file. It needs Android >= 2.1 and ROOT access.

It has all those advertisement domains categorized nicely for us at https://github.com/AdAway/adaway.github.io/blob/master/hosts.txt

Install adaway. It is not available on playstore. Find and install.

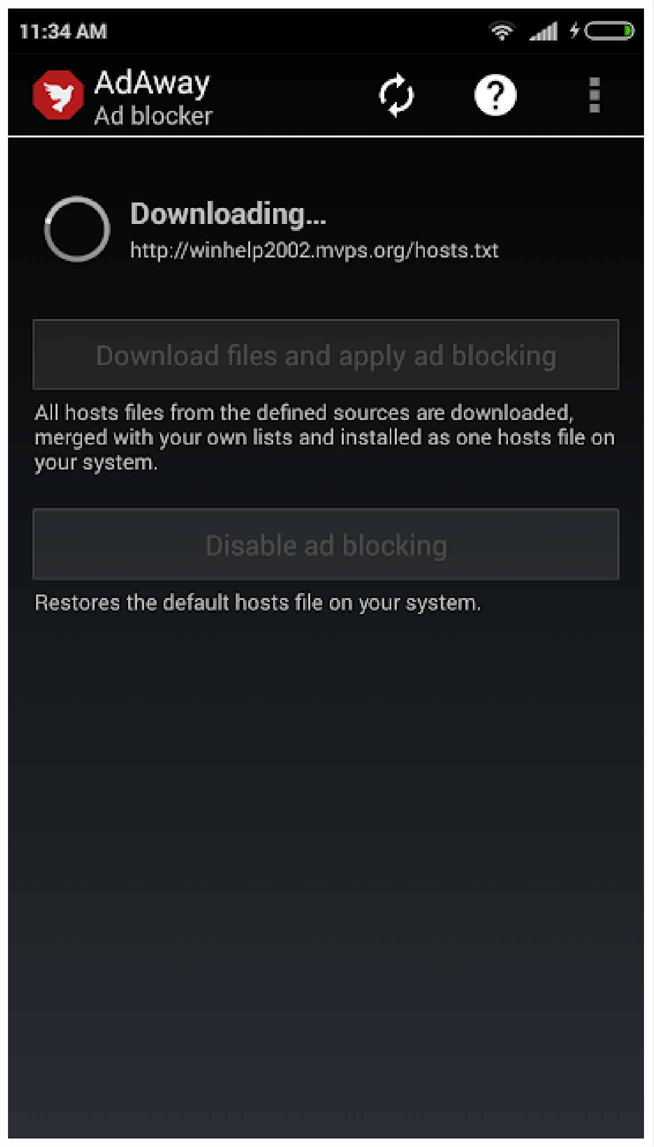
Post installation you will see below screen.



All hosts files from the defined sources are downloaded, merged with your own lists and installed as one hosts file on your system.

Restores the default hosts file on your system.

Click on "Download files and apply ad blocking".

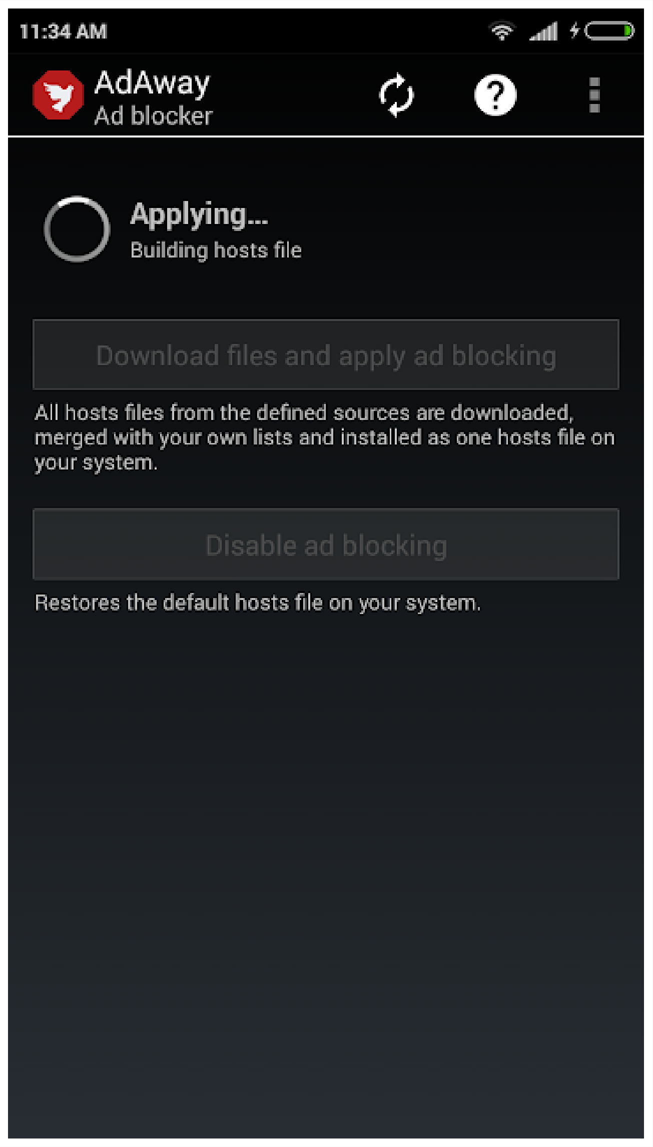


Downloading...

http://winhelp2002.mvps.org/hosts.txt

All hosts files from the defined sources are downloaded, merged with your own lists and installed as one hosts file on your system.

Restores the default hosts file on your system.



Applying...

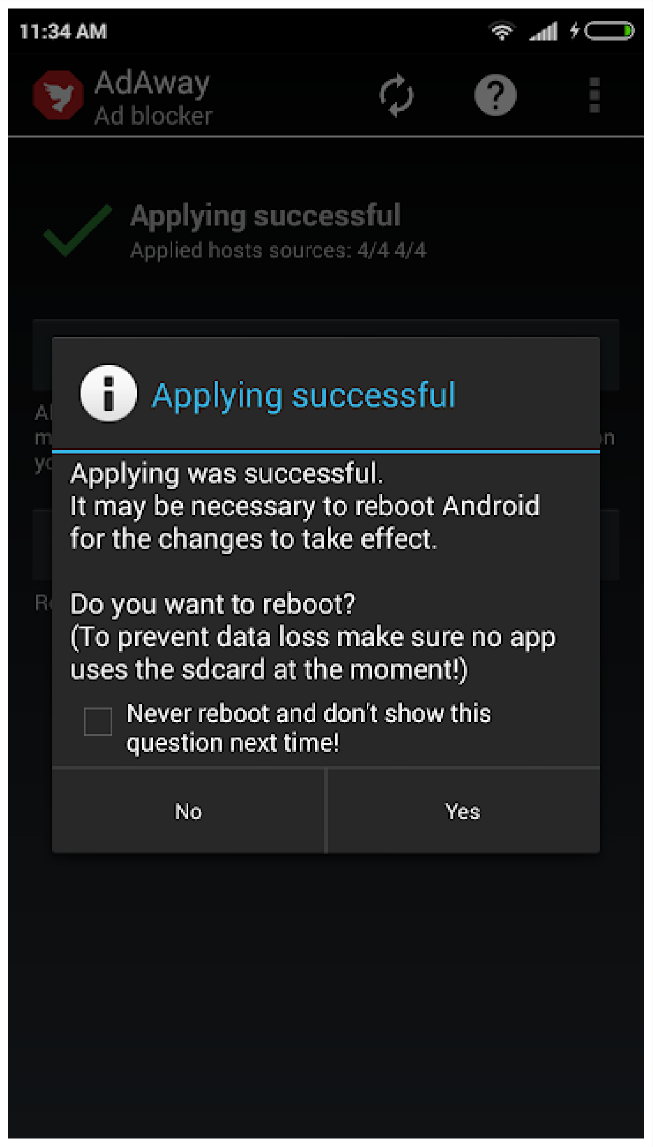
Building hosts file

Download files and apply ad blocking

All hosts files from the defined sources are downloaded, merged with your own lists and installed as one hosts file on your system.

Disable ad blocking

Restores the default hosts file on your system.



Applying successful

Applied hosts sources: 4/4 4/4

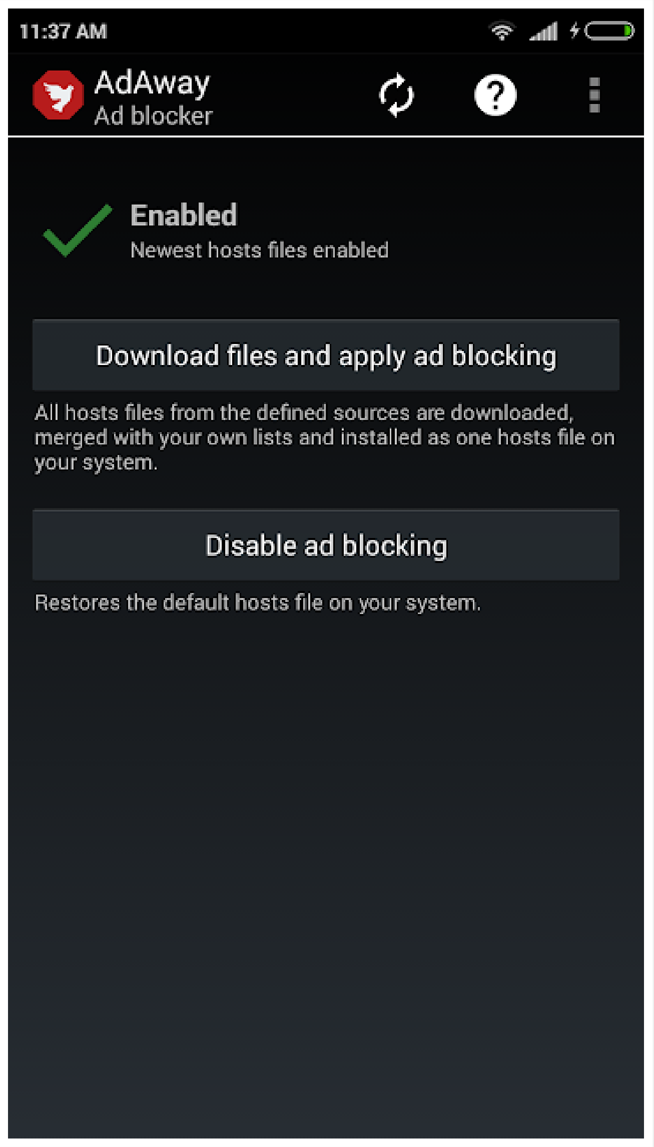
Applying successful

Applying was successful.
It may be necessary to reboot Android for the changes to take effect.

Do you want to reboot?
(To prevent data loss make sure no app uses the sdcard at the moment!)

□ Never reboot and don't show this question next time!

In my case, rebooting was not required. You can check if changes have been affected or not. Depending upon that you can reboot.



11:37 AM

AdAway
Ad blocker

✓ **Enabled**
Newest hosts files enabled

Download files and apply ad blocking

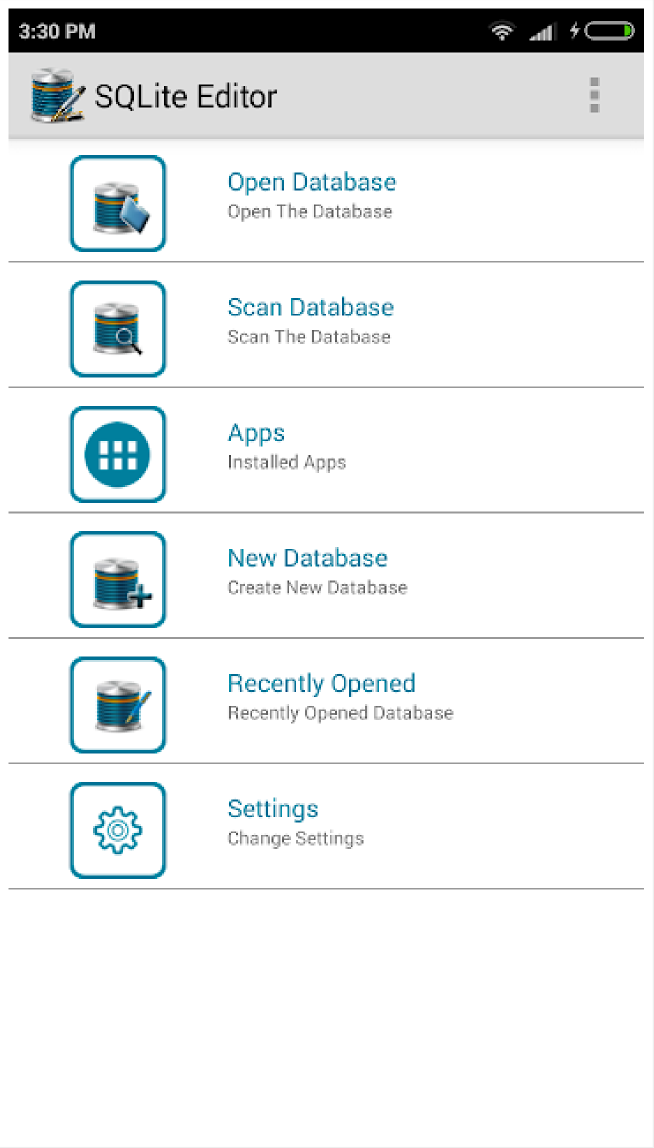
All hosts files from the defined sources are downloaded, merged with your own lists and installed as one hosts file on your system.

Disable ad blocking

Restores the default hosts file on your system.

Post reboot, it will be enabled.

Now let us check our SQLite editor application. It will look like below screenshot. Add free :)



Open Database
Open The Database

Scan Database
Scan The Database

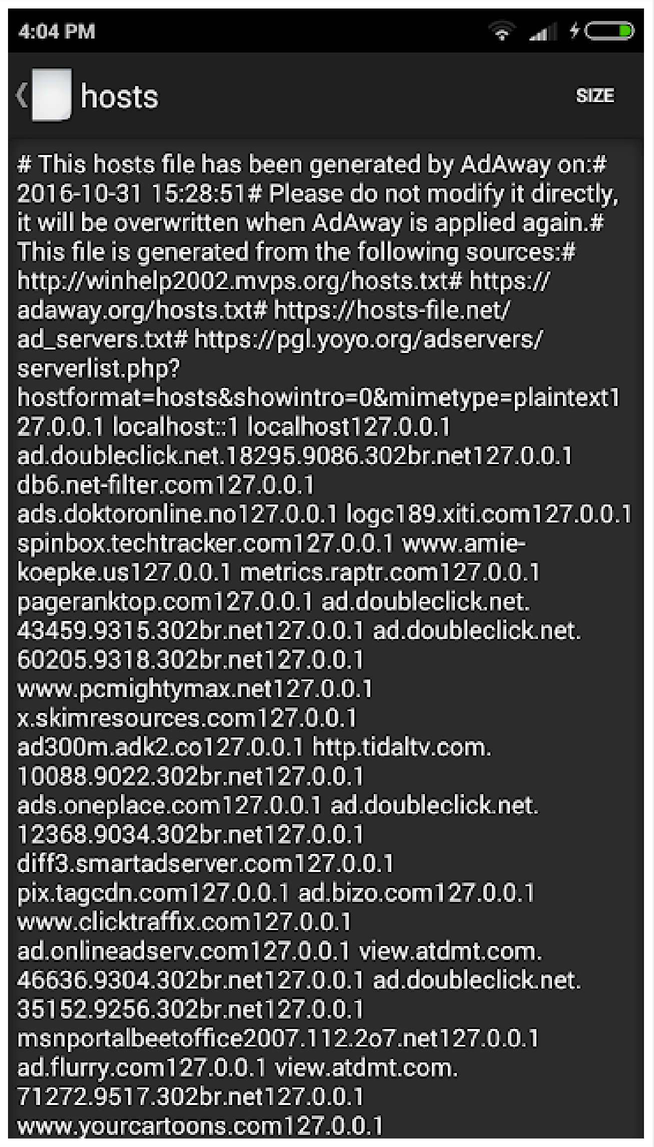
Apps
Installed Apps

New Database
Create New Database

Recently Opened
Recently Opened Database

Settings
Change Settings

Now let us check our hosts file. It will look as below.



```
# This hosts file has been generated by AdAway on:#
2016-10-31 15:28:51# Please do not modify it directly,
it will be overwritten when AdAway is applied again.#
This file is generated from the following sources:#
http://winhelp2002.mvps.org/hosts.txt# https://
adaway.org/hosts.txt# https://hosts-file.net/
ad_servers.txt# https://pgl.yoyo.org/adservers/
serverlist.php?
hostformat=hosts&showintro=0&mimetype=plaintext1
27.0.0.1 localhost::1 localhost127.0.0.1
ad.doubleclick.net.18295.9086.302br.net127.0.0.1
db6.net-filter.com127.0.0.1
ads.doktoronline.no127.0.0.1 logc189.xiti.com127.0.0.1
spinbox.techtracker.com127.0.0.1 www.amie-
koepke.us127.0.0.1 metrics.raptr.com127.0.0.1
pageranktop.com127.0.0.1 ad.doubleclick.net.
43459.9315.302br.net127.0.0.1 ad.doubleclick.net.
60205.9318.302br.net127.0.0.1
www.pcmightymax.net127.0.0.1
x.skimresources.com127.0.0.1
ad300m.adk2.co127.0.0.1 http.tidaltv.com.
10088.9022.302br.net127.0.0.1
ads.oneplace.com127.0.0.1 ad.doubleclick.net.
12368.9034.302br.net127.0.0.1
diff3.smartadserver.com127.0.0.1
pix.tagcdn.com127.0.0.1 ad.bizo.com127.0.0.1
www.clicktraffix.com127.0.0.1
ad.onlineadserv.com127.0.0.1 view.atdmt.com.
46636.9304.302br.net127.0.0.1 ad.doubleclick.net.
35152.9256.302br.net127.0.0.1
msnportalbeetoffice2007.112.2o7.net127.0.0.1
ad.flurry.com127.0.0.1 view.atdmt.com.
71272.9517.302br.net127.0.0.1
www.yourcartoons.com127.0.0.1
```

It has added so many domains within hosts file which are listed on

https://raw.githubusercontent.com/AdAway/adaway.github.io/master/hosts.txt

So now our majority of applications are add free. It will help us to protect our privacy as well as blocking mobile mawlares at certain levels. Rooted phone users must do it as rooting phone itself pauses many risks.

Reference:

1. *www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf*
2. *https://adaway.org/*
3. *http://askubuntu.com/questions/183176/what-is-the-use-of-etc-hosts*
4. *https://play.google.com/store/apps/details?id=com.ksk.sqliteeditor&hl=en*
5. *http://android-tricks.blogspot.in/2009/01/mount-filesystem-read-write.html*

Posted by Frogy at 10/31/2016

Labels: adaway tutorial, adware, android malware, android security, how to use adaway, malware, spyware, virus

1 comment:

Anonymous said...

This reminds of Google Pixel-2 latest feature, Which has inbuilt listener that recognizes near by music being played.

October 23, 2017 at 11:30 AM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)