**Adquisición de un sistema Android**



Daniel Escaño Hernández CET Ciberseguridad

# 

# 

# **1. Índice:**

[**1. Índice:**](#_oe0sczh5n4lv) **1**

[**2. Importación Maquina Android**](#_frvif2kdaiya) **2**

[**2.1 Creación y configuración de la máquina:**](#_5d38uxjyswtl) **2**

[**3. Adquisición Máquina Android**](#_v5oi9ih92ax6) **4**

[**3.1 Escenario 1: Uso de ADB, dd y netcat a estación de trabajo**](#_13hjj32400su) **4**

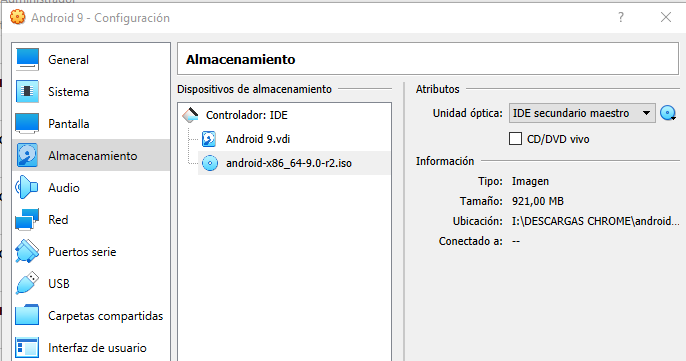
[**3.2 Escenario 2: Uso de ADB, dd y netcat a servidor**](#_5feqm9p11ucc) **5**

[**3.3 Comprobación**](#_z222ppkb02f7) **6**

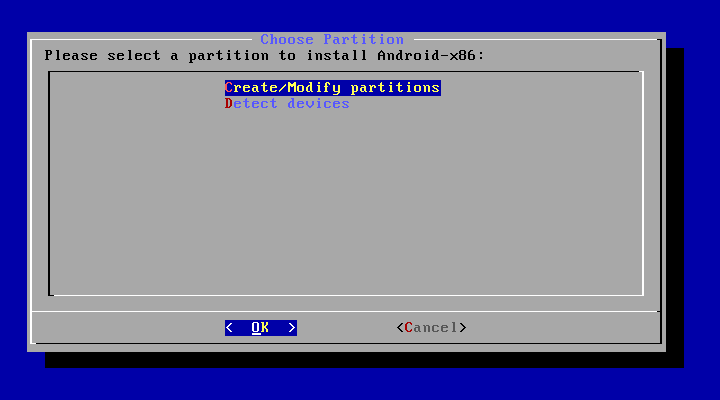
[**4. Webgrafía**](#_4kkf8zpjfmjy) **6**

# **2. Importación Maquina Android**

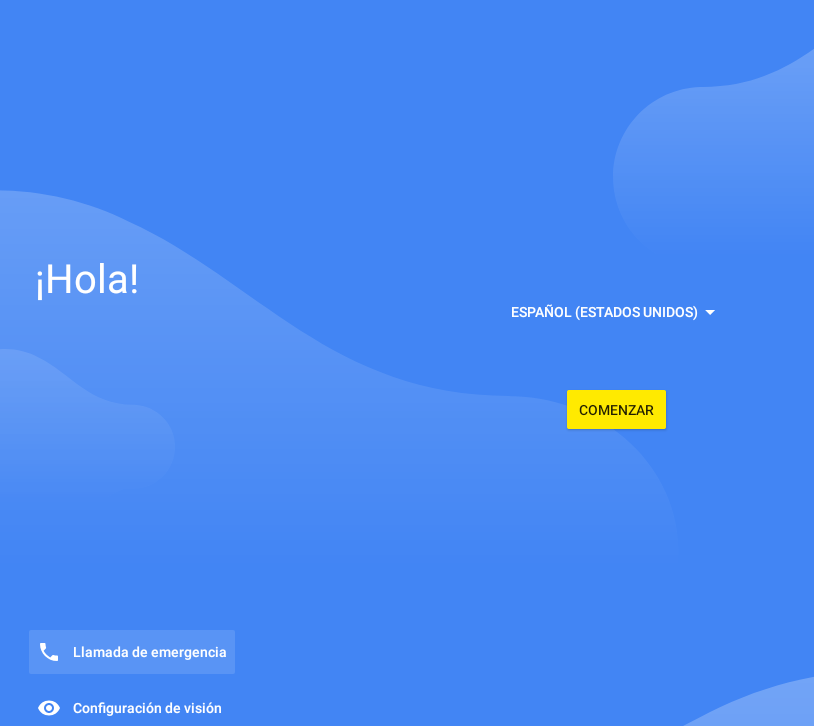
### **2.1 Creación y configuración de la máquina:**

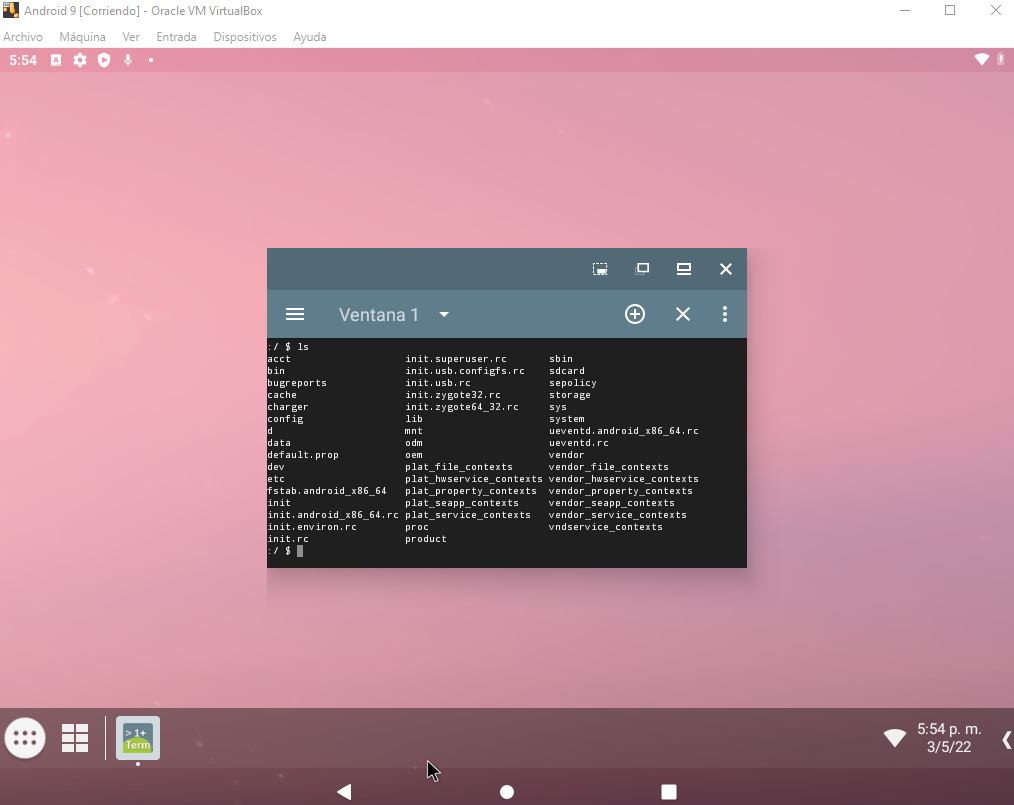








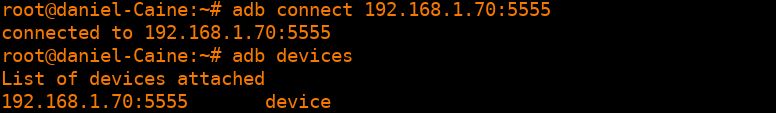




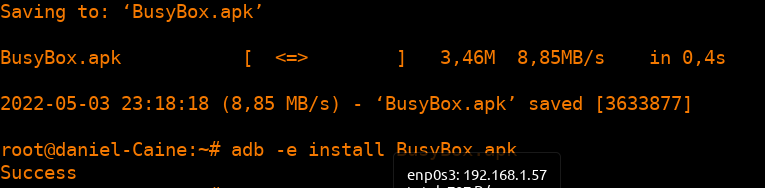
# **3. Adquisición Máquina Android**

### **3.1 Escenario 1: Uso de ADB, dd y netcat a estación de trabajo**

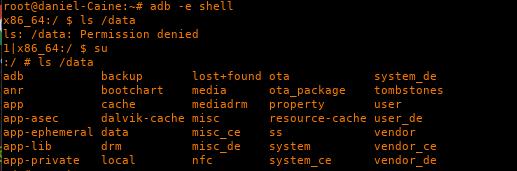
Nos conectamos mediante ADB utilizando el siguiente comando dirigido a la dirección IP de nuestra máquina Android.



Descargamos la aplicación BusyBox, una vez hecho, la instalamos en el sistema Android a través de ADB.



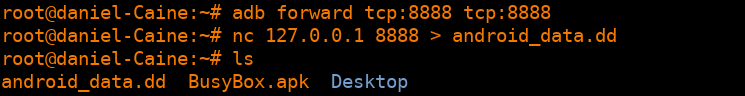
Accedemos a una shell mediante ADB:



Y comenzamos la adquisición de los archivos en los que estamos interesados, en este caso, el directorio /data, ubicado en /dev/block/sda1.

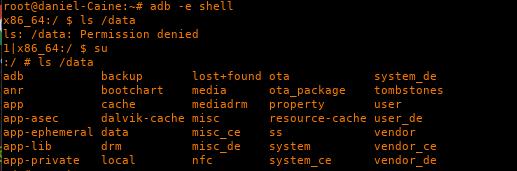


En nuestra estación de trabajo recolectamos esta información y la inyectamos en el software Autopsy.



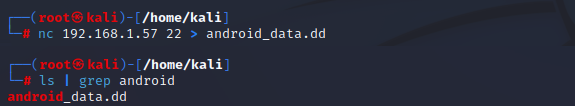
### **3.2 Escenario 2: Uso de ADB, dd y netcat a servidor**

Lo único que modificaremos en este escenario sería la opción de una vez extraída la imagen, enviarla al servidor correspondiente, en este caso una máquina kali, haciendo uso del comando netcat.

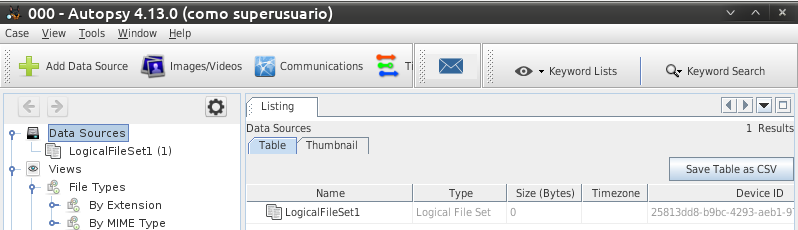








### **3.3 Comprobación**



# **4. Webgrafía**

https://www.android-x86.org/download.html

<https://stackoverflow.com/questions/9702447/using-busybox-version-of-netcat-for-listening-tcp-port>

<https://www.youtube.com/watch?time_continue=9&v=LbObAY6pMrI&feature=emb_title>

<https://www.android-x86.org/documentation/virtualbox.html>