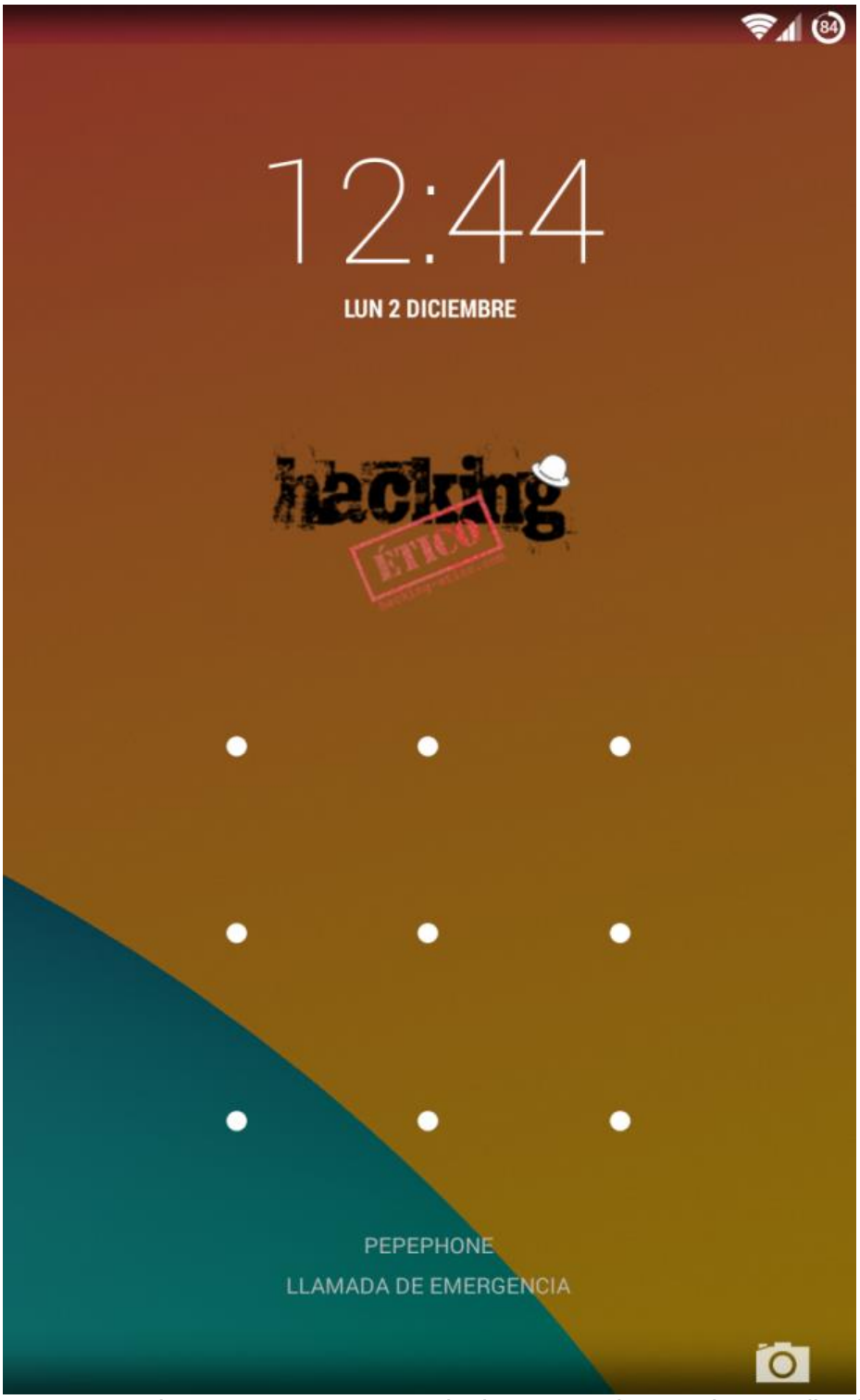
HACKEAR PATRON ANDROID

El uso intensivo de los smartphone hace que puedas encontrar diferentes modelos, marcas y/o sistemas operativos. Como bien sabéis uno de los más extendidos sino el que más es Android.
El buque insignia de Google en smartphones tanto gamas altas como en las más bajas, posee ciertas medidas de seguridad para los dispositivos. Al igual que posee bugs que pueden alterar el funcionamiento de tu terminal.
Una de las medidas de seguridad que ofrece Android, además de colocar un PIN, password, o simplemente desbloquear el terminal deslizando el dedo (seguridad por llamarlo de alguna manera) es la del **patrón de desbloqueo.** Por ello hoy vamos a demostrar (aunque necesitamos una serie de circunstancias) como averiguar un patrón de desbloqueo.



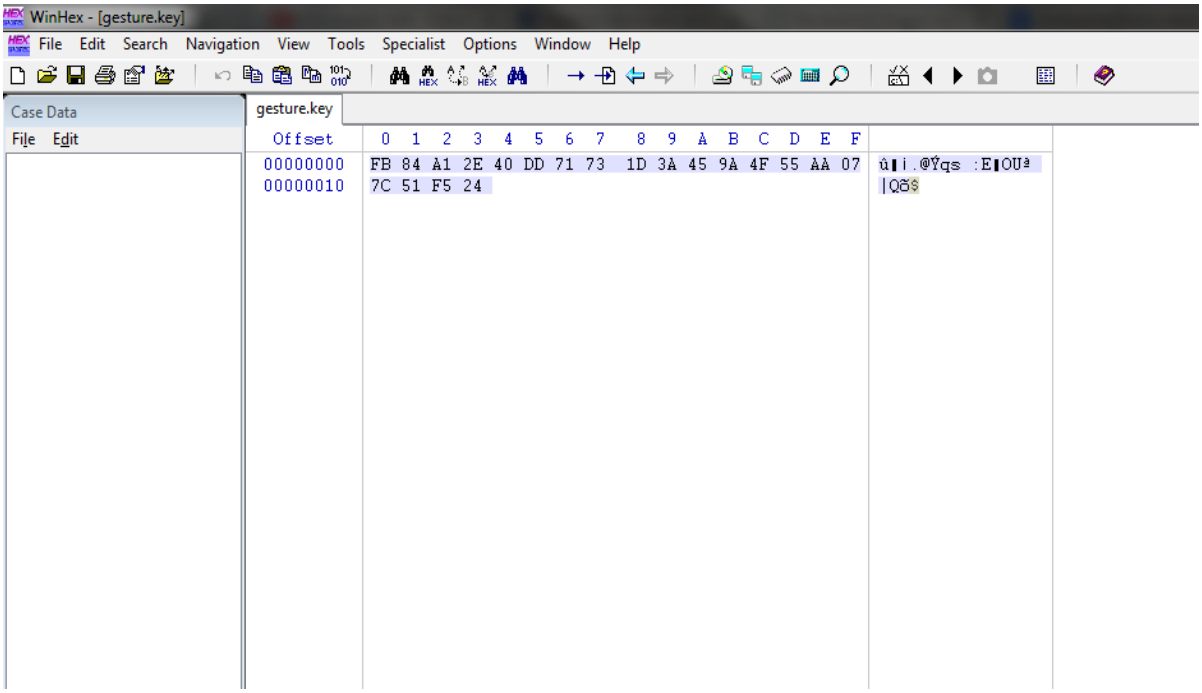
Lo primero que necesitamos es nuestro terminal. Las pruebas se han realizado con un Nexus 4 con Android KitKat 4.4. Decir que también se necesita el dispositivo rooteado.

Necesitamos algún tipo de explorador que pueda acceder a carpetas del sistema, en nuestro caso, hemos usado **Root Explorer**. Debemos acceder a la ruta */data/system* . Una vez accedido a esa ruta debemos buscar el fichero *gesture.key* el cual debemos copiar a cualquier ruta que tengamos acceso desde nuestro ordenador. Nosotros los

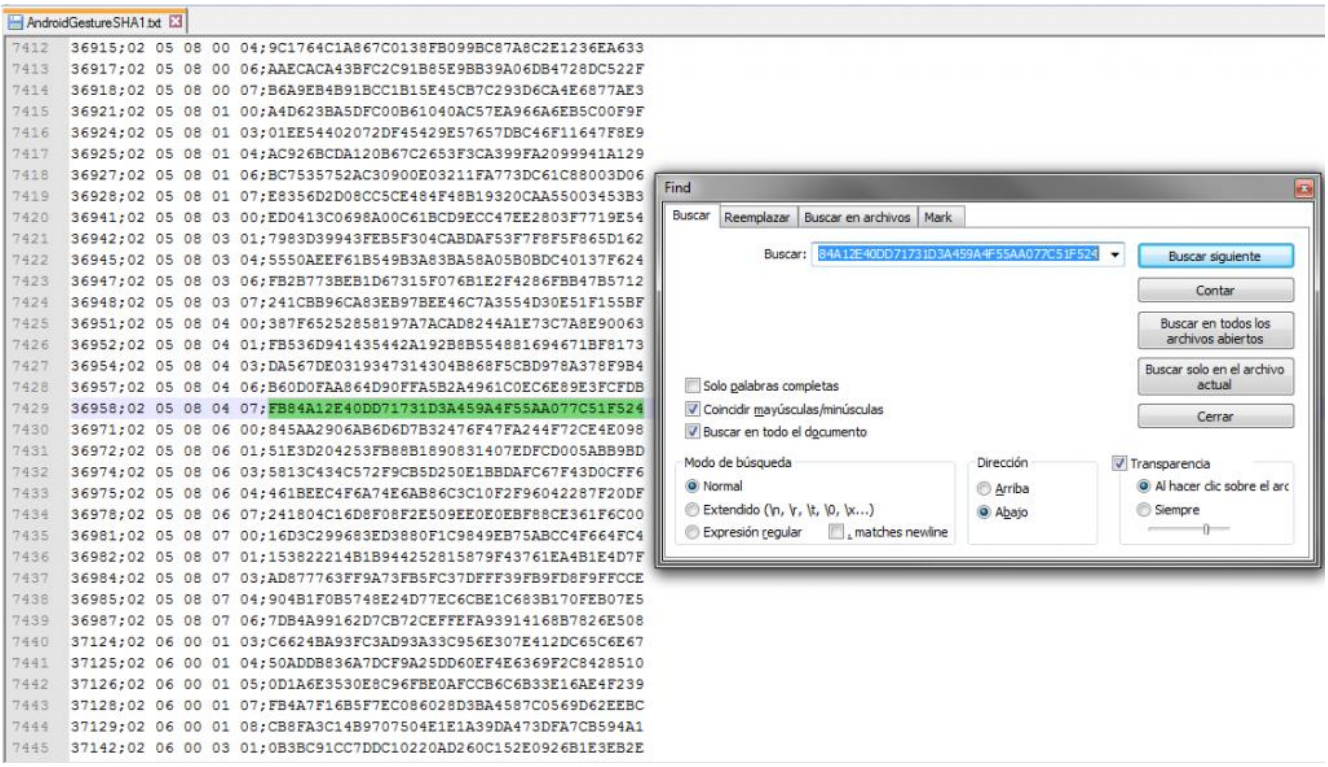
hemos subido a la nube (Cuenta BOX, aunque podemos traspasarlo conectándolo al portátil).
Una vez realizada la subida, procedemos a descargarlo en nuestro equipo. Ahora procederemos a descargar un par de instrumentos que necesitamos para analizar el archivo.

- WinHex (o similar) – Descargar
- Diccionario de Hashes – Descargar

WinHex lo usaremos para analizar los valores Hexadecimales de *gestures.key* ya que los necesitaremos para consultarlos en el diccionario de hashes SHA-1. Abrimos el programa WinHex, arrastramos el fichero *gestures.key* hasta el programa, y veremos unos valores similares a estos o al menos con la misma construcción.

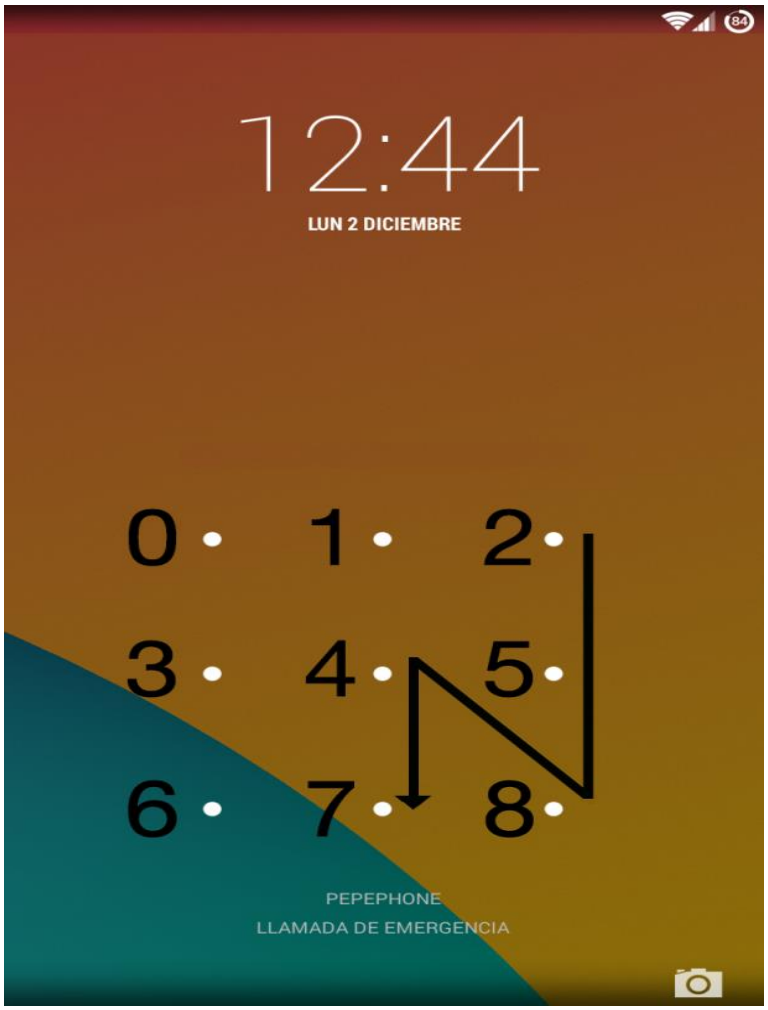


Debemos fijarnos en los valores marcados, concretamente *FB84A12E40DD71731D3A459A4F55AA077C51F524* estos valores diferirán dependiendo del patrón que poseamos. Ahora procedemos a copiar estos valores con la combinación de teclas **Ctrl + Shift + C .**
Ahora, cuando hayamos descargado y descomprimido el Diccionario de Hashes, recomendamos abrir con el programa **Notepad++** para evitar bloqueos en el editor de texto de Windows. Veremos una pantalla con miles de números hexadecimales. Procedemos a buscar la secuencia que hemos copiado anteriormente. Lo vemos en la siguiente captura.



Vemos como nos marca la secuencia en verde. Si nos fijamos en los números que le preceden 0205080407 podemos extraer el patrón. Por tanto y obviando el cero a la izquierda, nuestro patrón sería el *25847.*

¿Cómo interpreto esta numeración? Muy sencillo, aquí os dejamos la equivalencia de los números respecto a la posición de los puntos del patrón.



Si lo probamos en nuestro dispositivo veremos que realmente se cumple siempre. Nosotros hemos modificado el patrón varias veces para testear que esto es real. Y en todas nos ha dado la secuencia correcta.
Esta forma de averiguar el patrón puede ser aprovechada por malware en tu teléfono aunque si no lo tienes rooteado no deberías estar expuesto a esto pero no tener rooteado el teléfono limita muchas funciones de tu smartphone.