



Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)



Análisis Forense Informático

UD02. Consideraciones entorno móvil.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

	Pag
1. Caso práctico	2
2. Extracción de la evidencia	2
3. Procesado y preguntas	3
4. Anexo	6
5. Webgrafía	13

1.- Descripción de la tarea.

Caso práctico

María está trabajando en el laboratorio cuando recibe la tarea de analizar un dispositivo móvil.

Por una parte, es un escenario nuevo para ella por lo que está viendo de qué manera extraer la información. Sabe que es un teléfono móvil Iphone y por tanto es un sistema cerrado que sin los consiguientes accesos será complicado de analizar.

Necesita saber si la actividad del dueño del dispositivo durante las últimas semanas.

¿Qué te pedimos que hagas?

✓ Apartado 1: Extracción de la evidencia

Vamos a trabajar sobre la base de un móvil Iphone, para ello puedes usar tu teléfono o el de algún amigo. Si no tienes estas facilidades puedes disponer de una imagen de teléfono móvil en el siguiente enlace:

http://downloads.digitalcorpora.org/corpora/mobile/ios_13_4_1/ios_13_4_1.zip

El objetivo de la actividad es entender qué aparte de cómo se realiza una extracción y procesado, qué problemas nos podemos encontrar con el análisis forense de dispositivos móviles en especial de dispositivos basados en iOS.

Necesitas poder extraer la evidencia, para ello tienes dos alternativas:

➤ Realizar un backup mediante el software de Itunes de Apple.

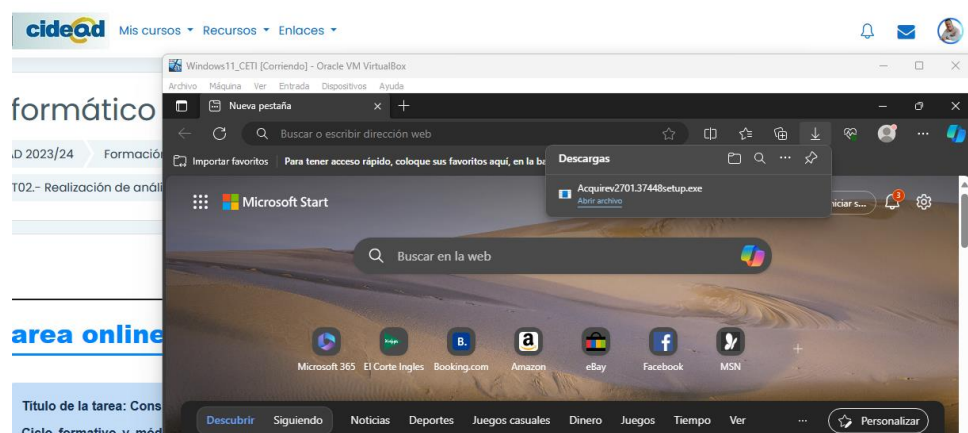
- Tienes una guía aquí: [Guía Itunes de Apple](#).

➤ Extraer las evidencias mediante software forense específico.

- Tienes el software disponible aquí

<https://www.magnetforensics.com/resources/magnet-acquire>

- Tienes una guía aquí [Guía de software forense](#) (está basado en Android, pero el proceso para Iphone es el mismo)



Podemos ver la instalación de **Magnet Acquire** en Windows 11 en el anexo final.

✓ Apartado 2: Procesado y Preguntas

- Utilizaremos el siguiente software para procesar las evidencias:

- <https://github.com/abrignoni/iLEAPP>

Podemos revisar todo el proceso de instalación y pruebas de **iLEAPP** en el anexo final.

- Tienes una guía del software aquí [Guía software de procesado de evidencias](#)
- Te recomendamos que hagas estas dos partes y luego intentes responder a las preguntas. Algunas de las preguntas pueden requerir que investigues determinadas características del sistema iOS.

- ¿Qué sucede cuando conectamos el dispositivo móvil al ordenador?

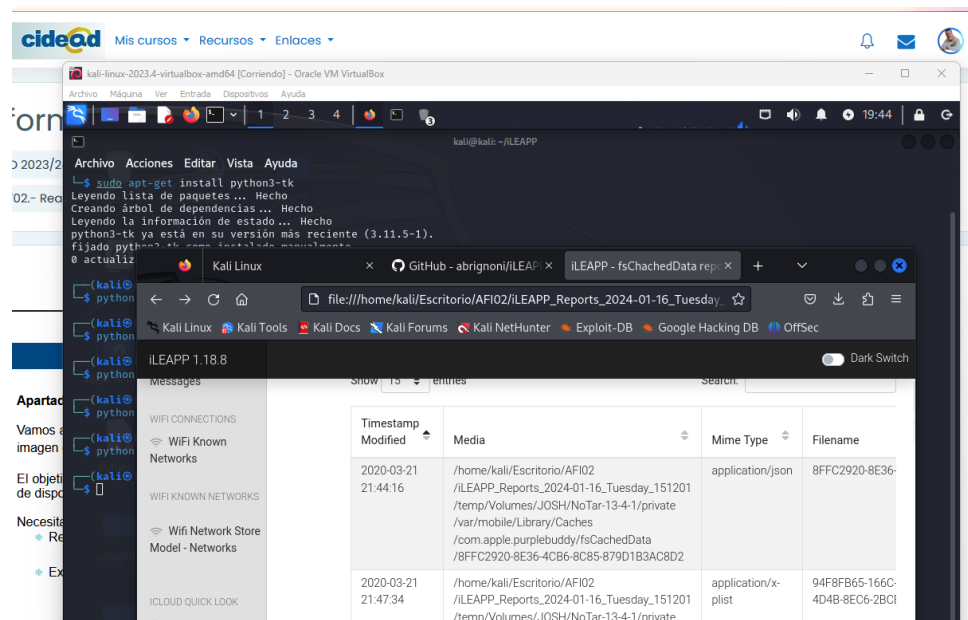
Al haber utilizado la imagen proporcionada, no podemos comprobar este paso, tampoco con la utilización de dos dispositivos distintos Android con **Magnet** pero visto el proceso de conexión con el dispositivo (ver anexo) en caso de ser un dispositivo desconocido, tendremos que agregarlo como tal y habilitar el ordenador como equipo de confianza.

- ¿Qué tipo de extracción es?

Extracción de tipo lógica.

- ¿Qué riesgo tenemos? ¿Qué cambios se han producido al hacer este tipo de extracción?

Se pueden escribir datos en el dispositivo (cosa que hemos hecho), alterando la integridad de estos.



The screenshot shows a Kali Linux virtual machine environment. In the foreground, a web browser displays the iLEAPP web interface. The interface has a sidebar with navigation options like 'Mis cursos', 'Recursos', and 'Enlaces'. The main content area shows a table of extracted data. The terminal in the background shows the installation of python3-tk using the command `sudo apt-get install python3-tk`.

Timestamp Modified	Media	Mime Type	Filename
2020-03-21 21:44:16	/home/kali/Escritorio/AFI02/iLEAPP_Reports_2024-01-16_Tuesday_151201/temp/Volumes/JOSH/NoTar-13-4-1/private/var/mobile/Library/Caches/com.apple.purplebuddy/fsCachedData/8FFC2920-8E36-4CB6-8CB5-879D1B3AC8D2	application/json	8FFC2920-8E36-
2020-03-21 21:47:34	/home/kali/Escritorio/AFI02/iLEAPP_Reports_2024-01-16_Tuesday_151201/temp/Volumes/JOSH/NoTar-13-4-1/private	application/x-plist	94F8FB65-166C-4D4B-8EC6-2BCI

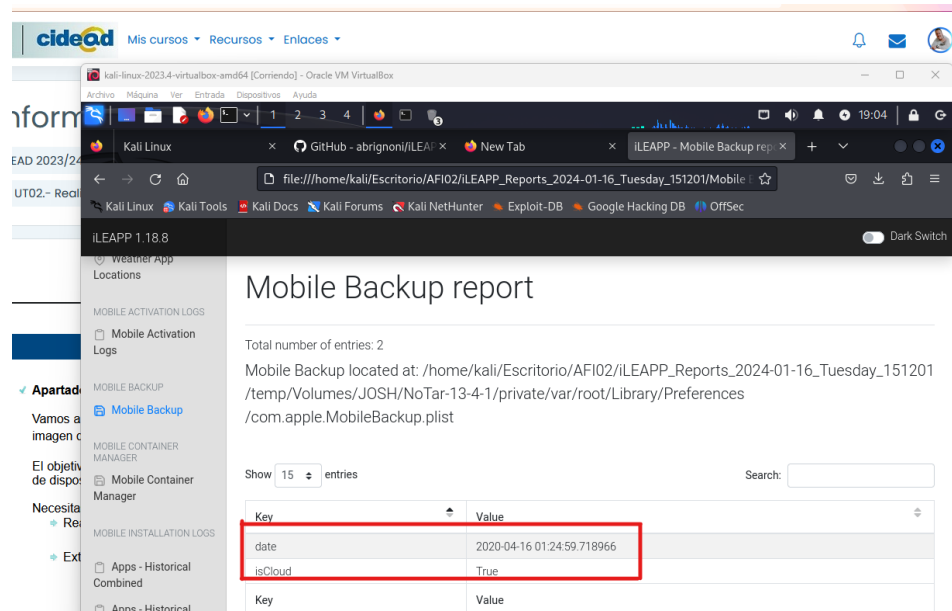
- ¿Qué diferencias tenemos entre este tipo de extracción y una física?

En la física, exponemos la integridad de las posibles pruebas al tener que manipularlo directamente. Es además muy completa y compleja, al trabajar sobre el chip.

- ¿Qué alternativas tenemos si no conocemos el código de desbloqueo, pero tenemos o podemos conseguir el usuario y contraseña de la cuenta de apple?

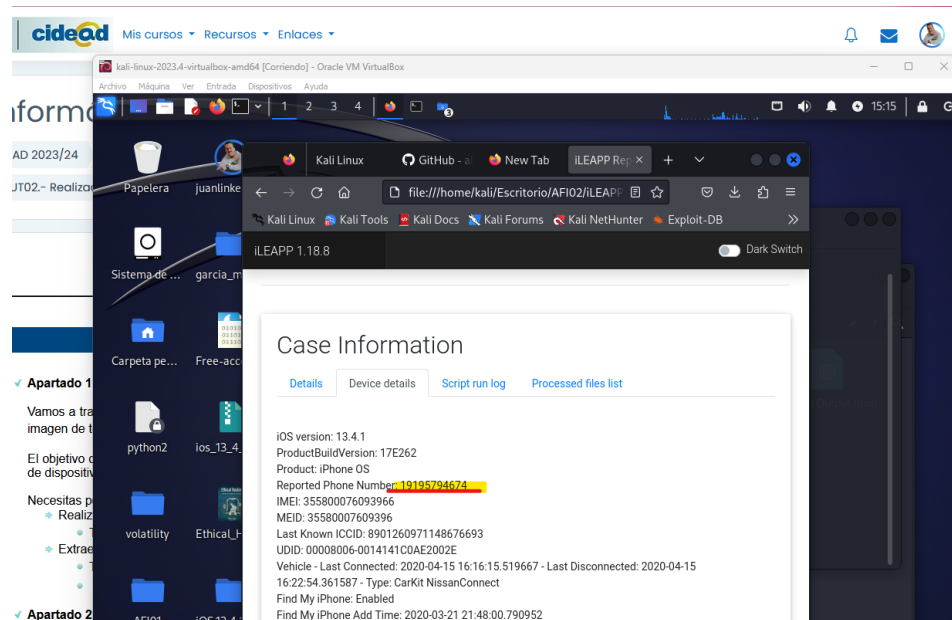
Hay disponible un backup alojado en la nube que podríamos utilizar para un análisis con un software como **Cellebrite**.

También, el disponer de estos datos, nos puede facilitar acceso a información desde documentos, email, ...



- ¿Eres capaz de identificar el número de móvil?

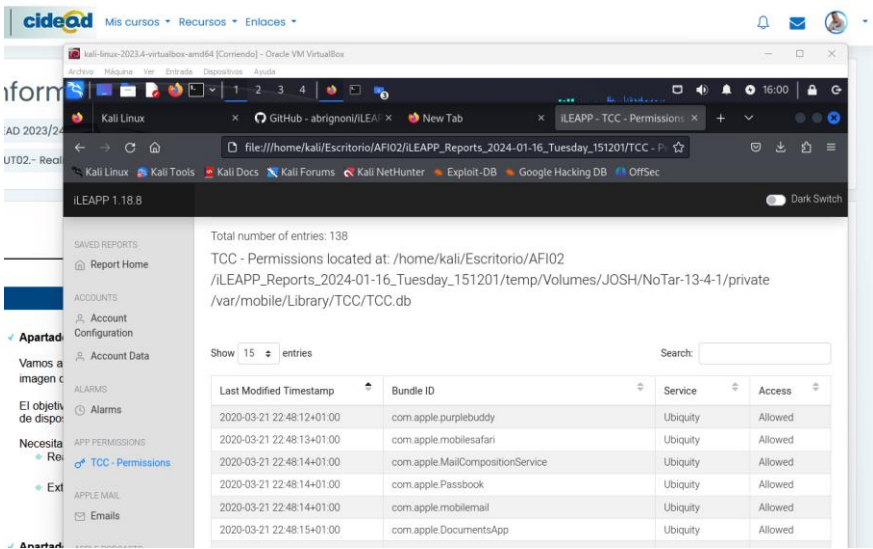
Podemos verlo en la misma vista de propiedades: **19195794674**



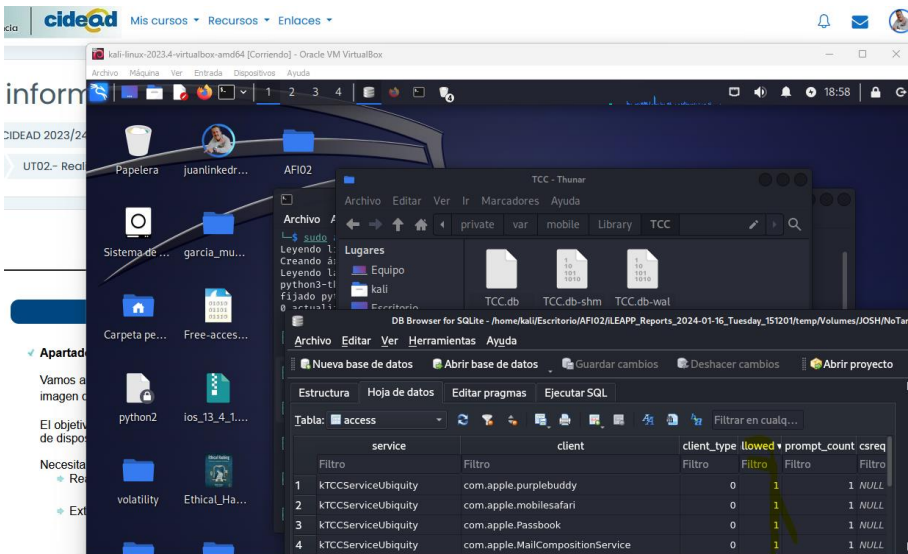
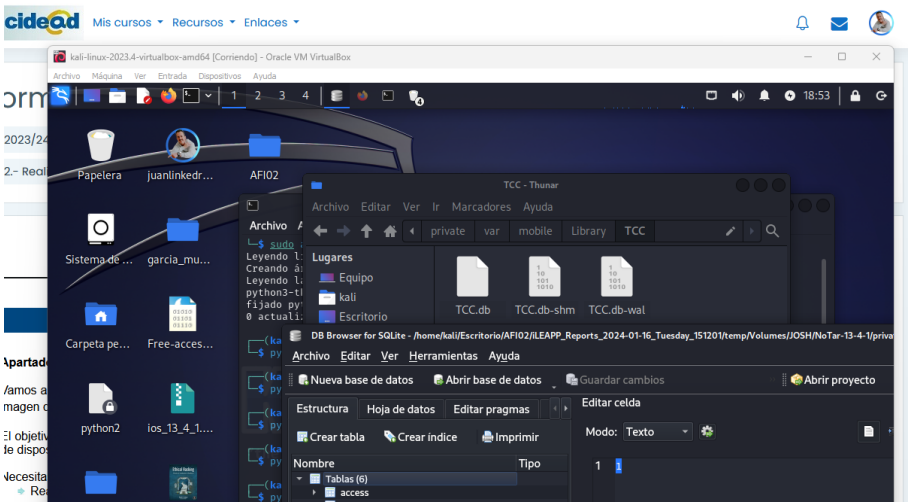
- ¿Eres capaz de identificar que apps tienen concedidos permisos a qué recursos?
¿El usuario ha sido consciente de forma explícita de este consentimiento?

En el menú lateral tenemos la opción **TCC-Permissions** report.

Podemos observar las apps y permisos.



También observando la ruta de consulta para esta tabla, podemos acceder a **TCC.db** y observar los valores, para ver si se ha concedido el permiso solicitado o no. En el caso de iOS, por seguridad “obliga” a aceptar (se presume ser consciente)

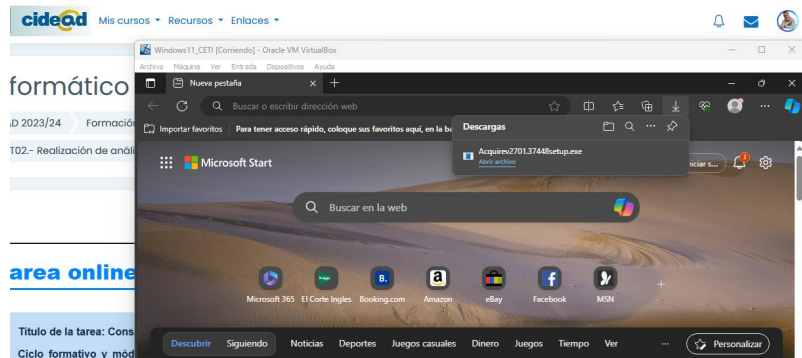


Anexo.

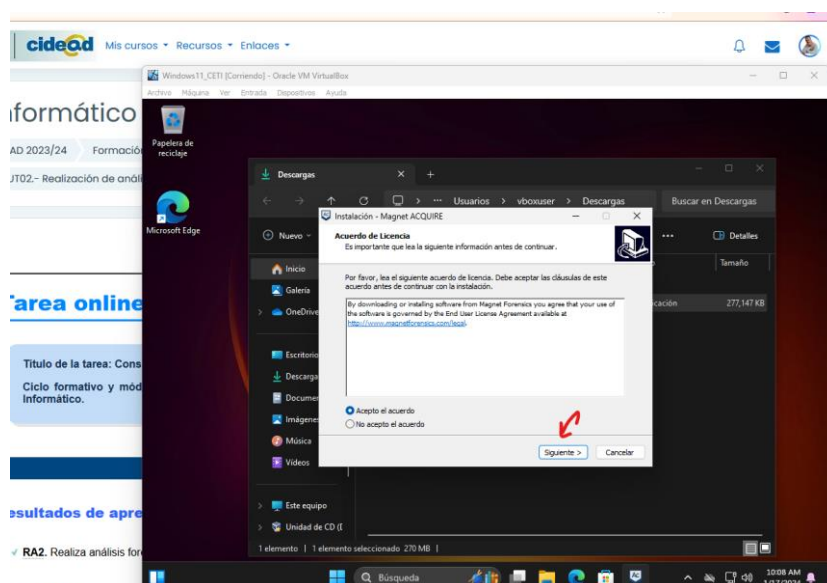
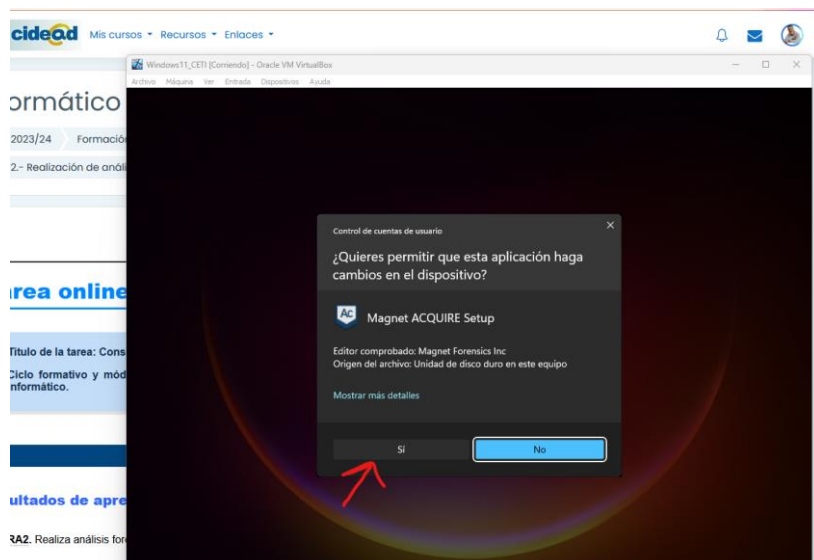
Instalación Magnet Acquire.

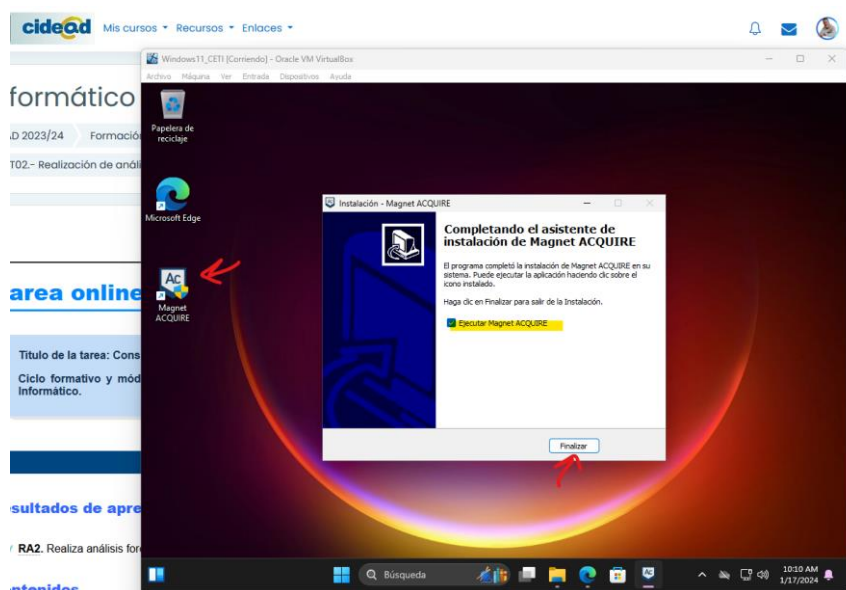
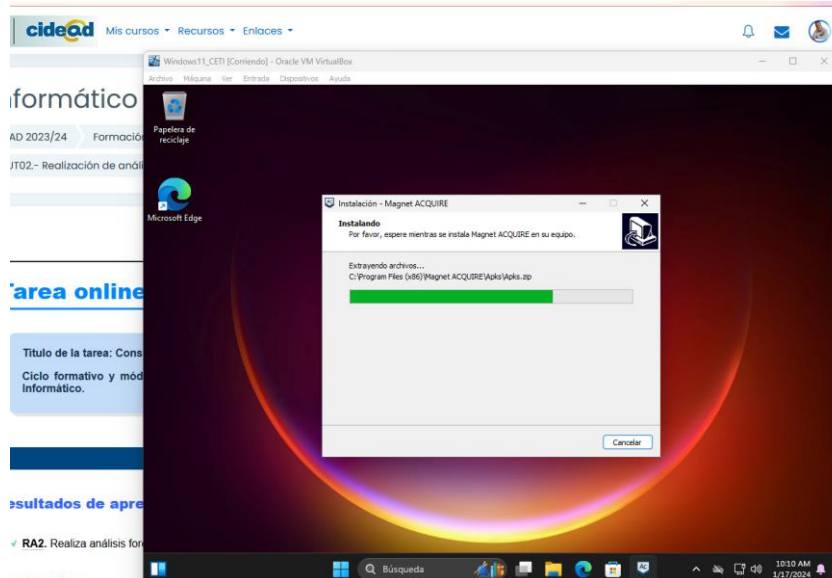
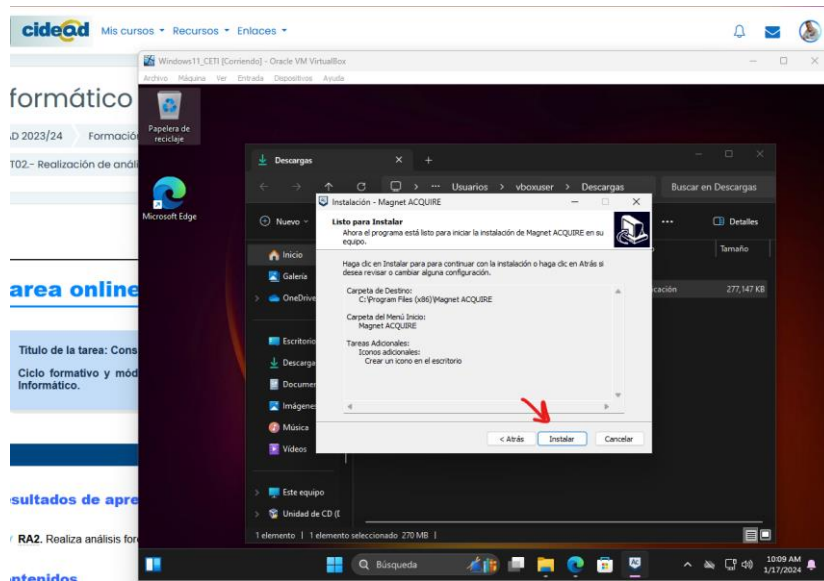
Abro una máquina en VirtualBox con Windows 11, creada para este curso.

Procedo desde el navegador a la descarga de **Magnet Acquire**



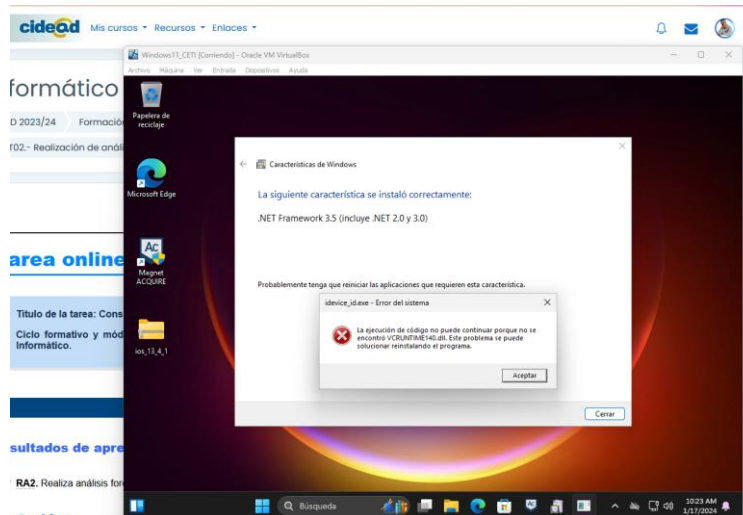
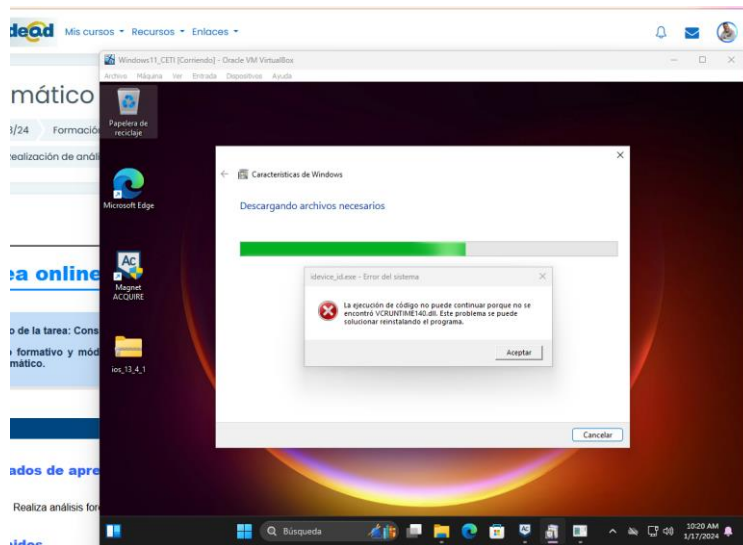
Tras la descarga automática, empezamos la instalación como cualquier otro programa en Windows.



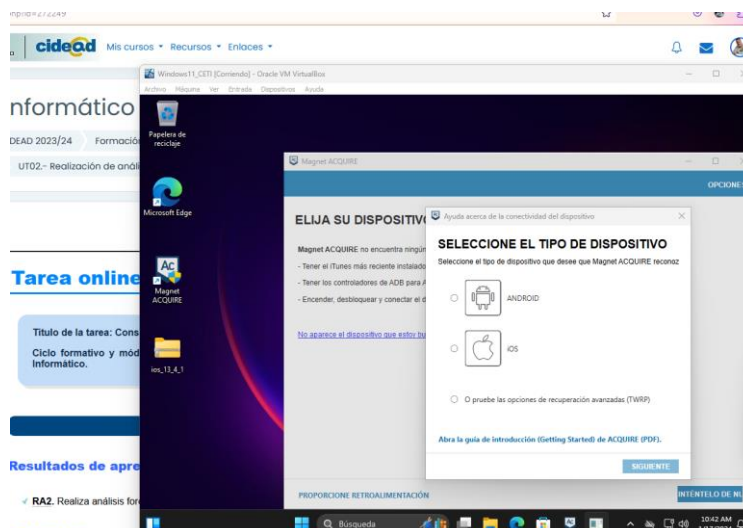


Al iniciarse y ser una instalación nueva de Windows, podemos encontrarnos con que nos falten librerías como alguna de C++ necesarias.

Autorizamos la instalación, aprovecho para ir descargando la imagen de iOS y esperamos que los dos procesos terminen:



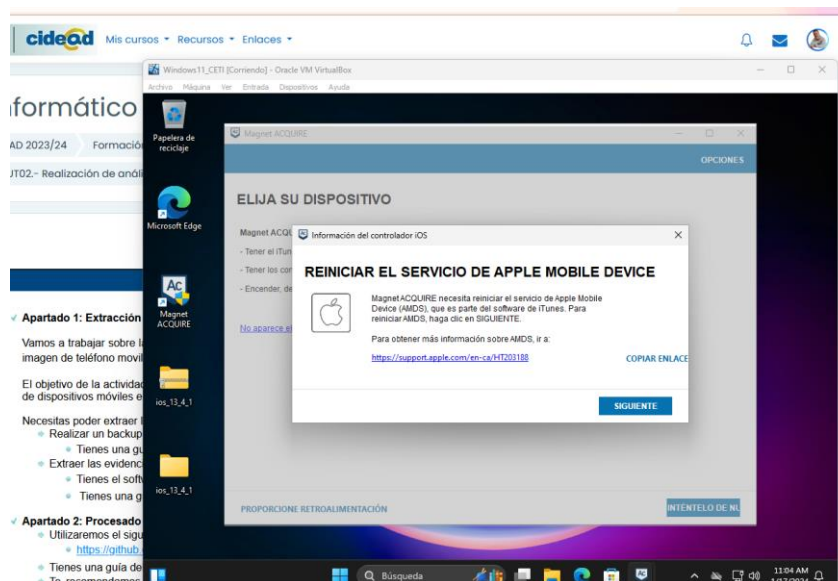
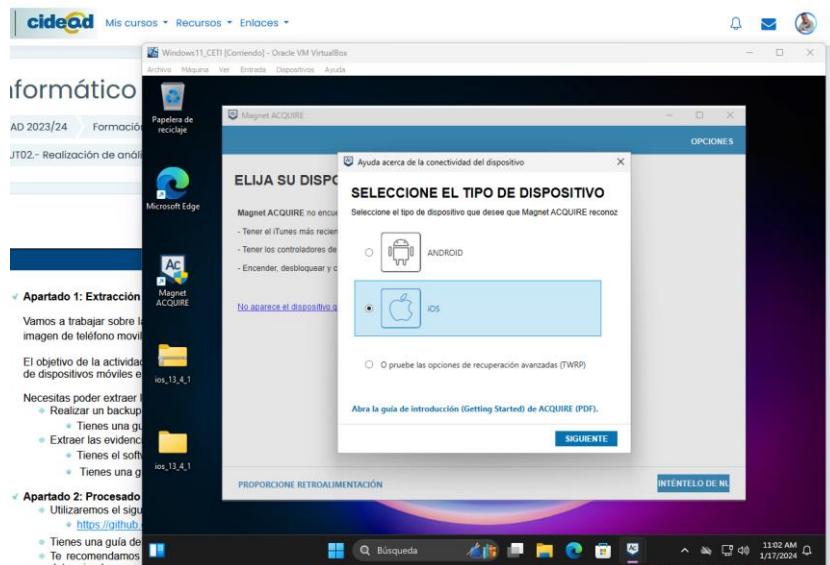
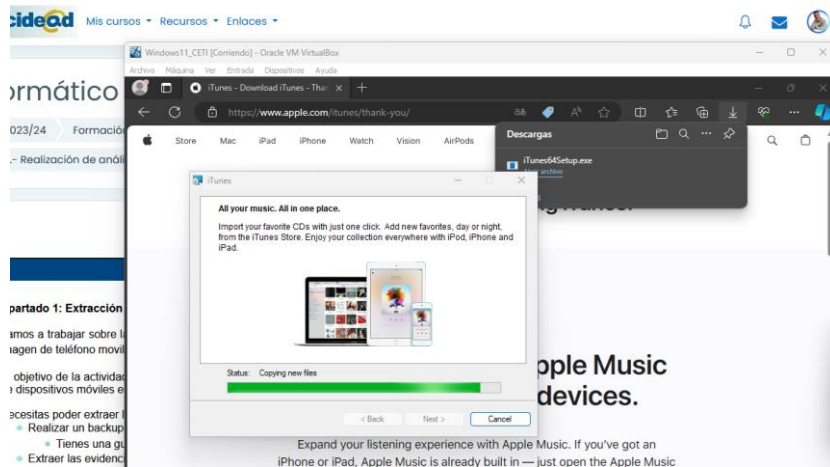
Reiniciamos la máquina y volvemos a abrir el programa para ir haciendo pruebas.



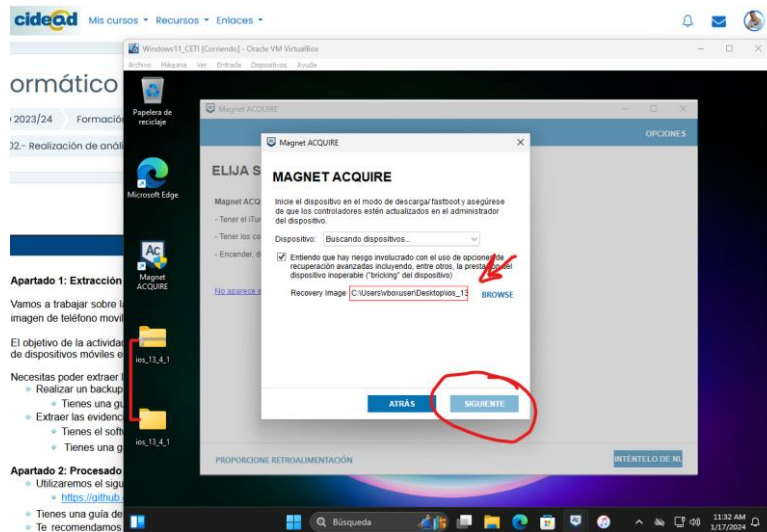
Si no encuentra dispositivos, podemos intentarlo desde el enlace que nos abre este menú.

Para iOS necesitamos que instale iTunes y para Android, los drivers ADB.

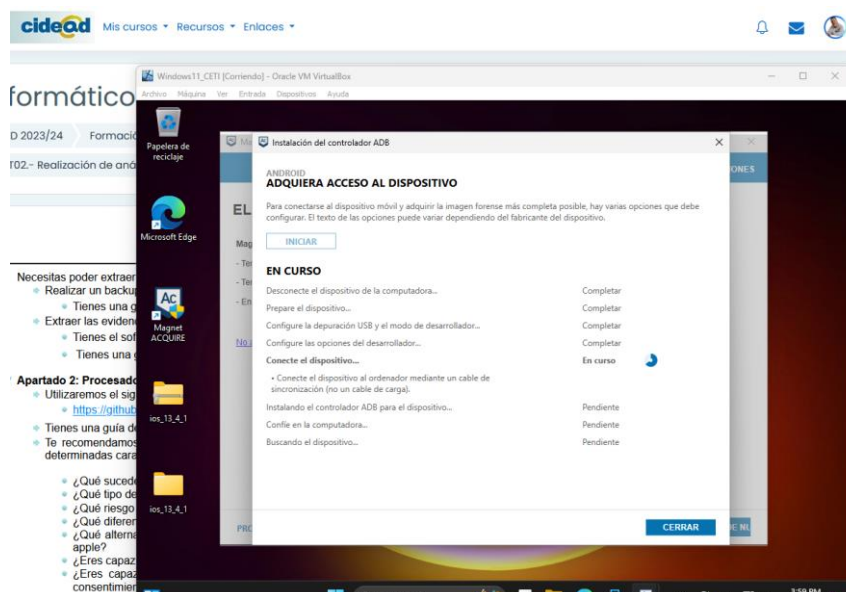
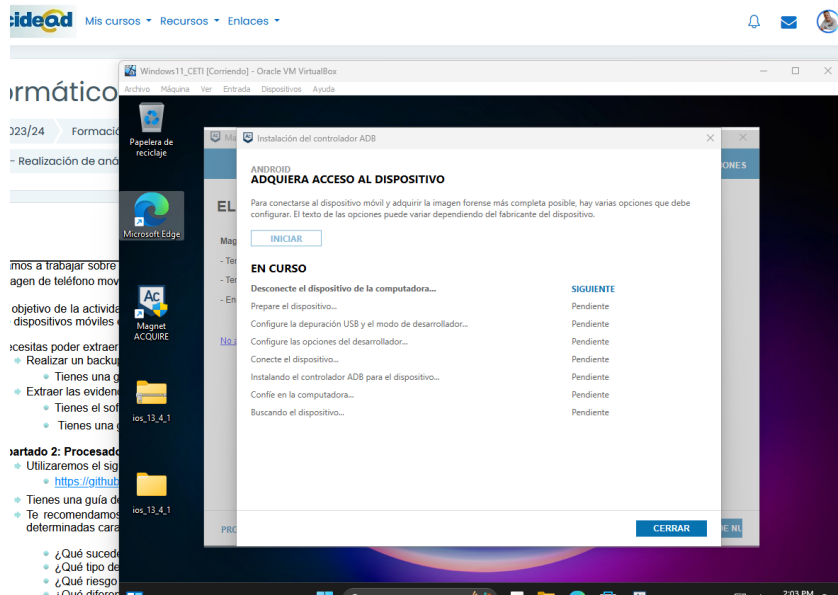
Autorizamos la instalación del primero.

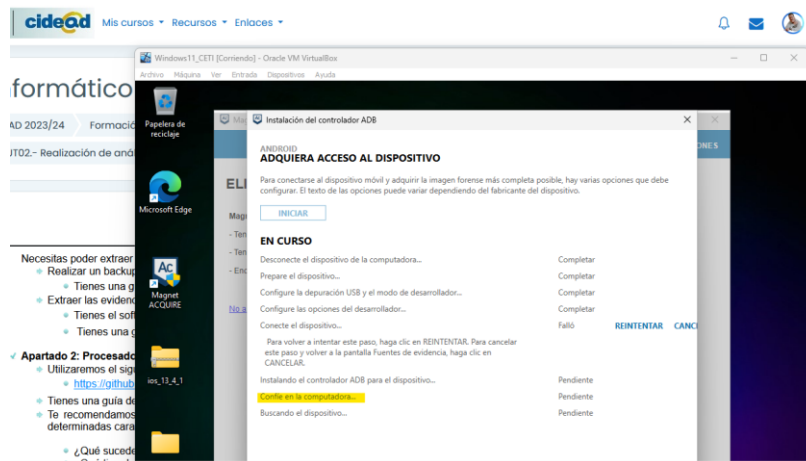


Podemos intentar también acceder desde algún backup, aunque el de iOS facilitado no nos sirva.



Hacemos una prueba con un dispositivo Android no conectado antes.

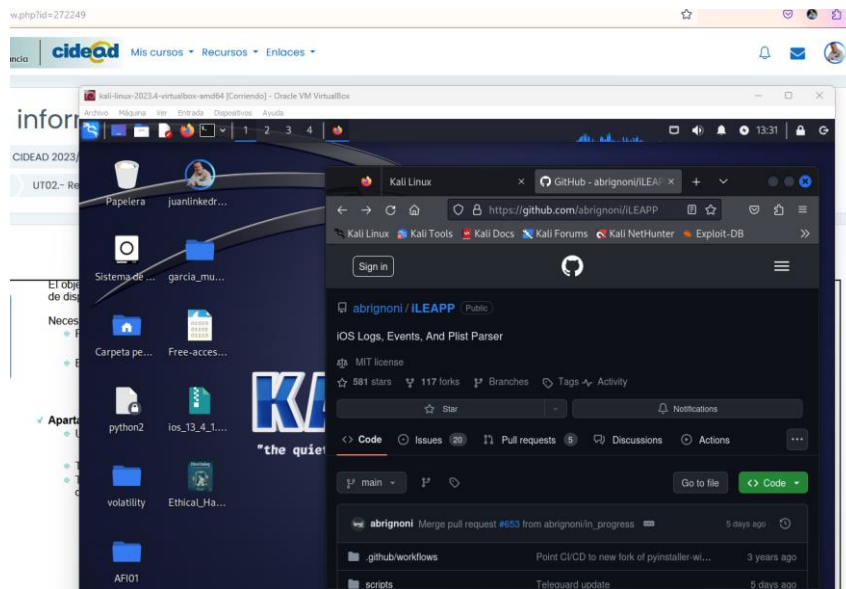




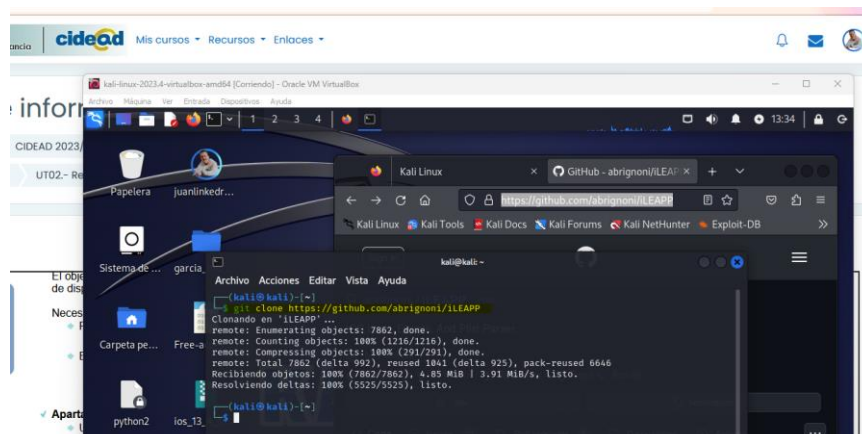
A pesar de intentarlo con dos dispositivos distintos e incluso instalar los drivers de forma directa, no he podido pasar de esta parte, aunque se presume que debemos de añadir los permisos para confiar en el equipo.

Instalación y prueba de iLEAPP.

Accedemos desde nuestra máquina al repositorio del proyecto iLEAPP

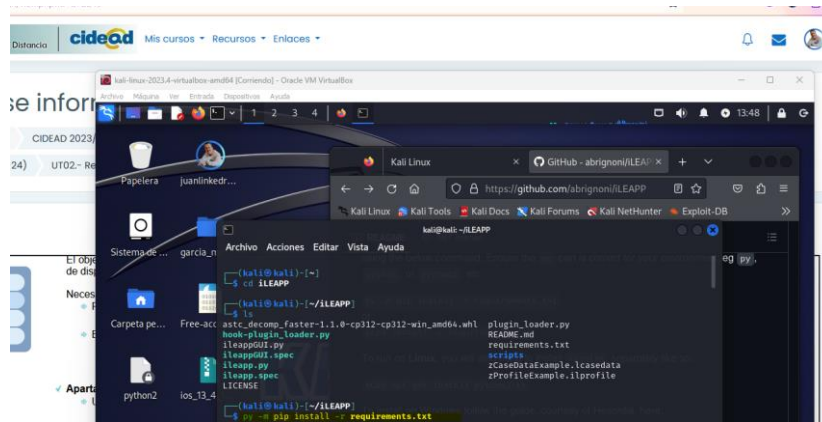


`git clone https://github.com/abrignoni/iLEAPP`



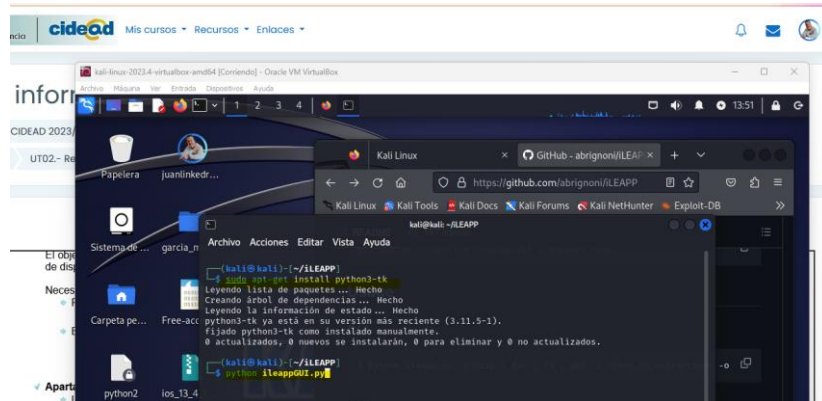
Reviso el directorio para comprobar el clonado y poder seguir los pasos que indican:

```
cd iLEAPP
ls
py -m pip install -r requirements.txt
```



Necesitamos tinker:

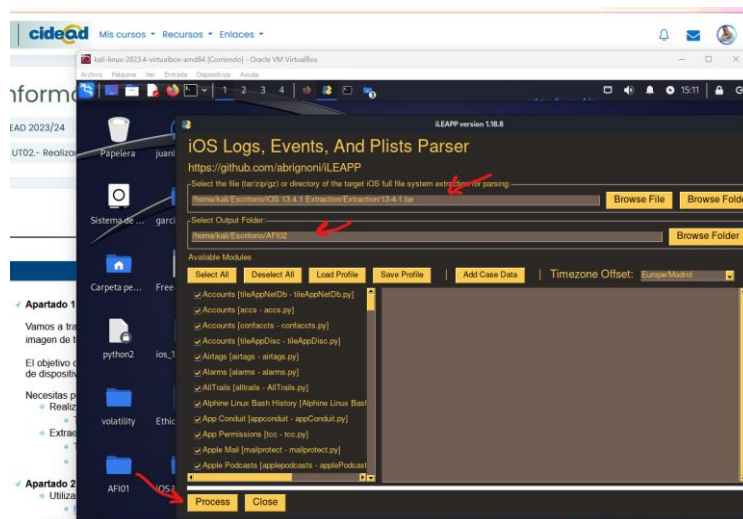
```
sudo apt-get install python3-tk
```



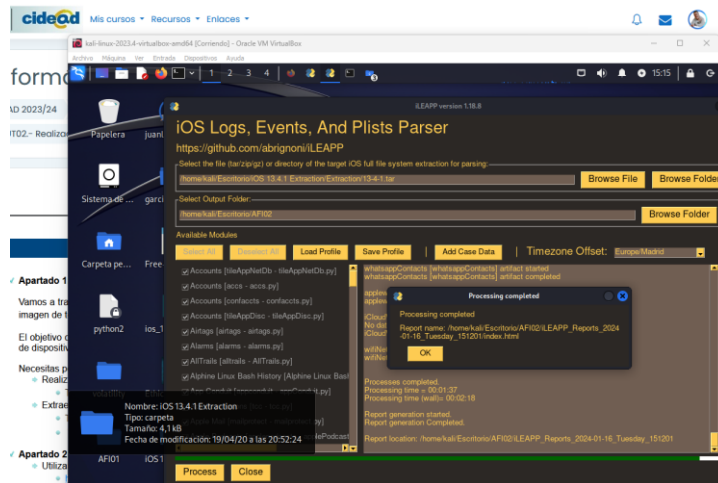
Abro la interfaz gráfica:

```
python ileappGUI.py
```

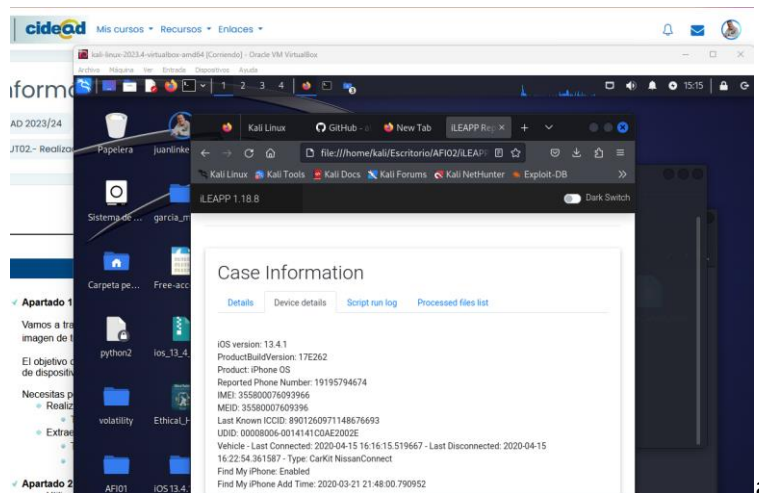
Seleccionamos el archivo .tar descomprimido, el directorio donde queremos guardar los datos extraídos y dejamos que trabaje unos minutos.



Nos avisa de la finalización del proceso:



Al cerrar ese diálogo, nos abre en el navegador una vista con la información volcada para el análisis.



Webgrafía.

<https://www.magnetforensics.com/dl/acquire>

<https://www.magnetforensics.com/resources/magnet-acquire>

<https://github.com/abrignoni/iLEAPP>

<https://www.youtube.com/watch?v=ZTxIJjNp77g>

<https://www.xataka.com/basics/como-conectar-controlar-tu-android-ordenador-adb>

<https://blog.elhacker.net/2022/01/instalar-adb-y-usar-los-comandos-basicos.html>