



TAREA 02


**REALIZACIÓN DE
ANÁLISIS FORENSES EN
DISPOSITIVOS MÓVILES**

ANÁLISIS FORENSE INFORMÁTICO

ALBA MOREJÓN GARCÍA

2024/2025

CETI - Ciberseguridad en Entornos de las Tecnologías de la Información



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.

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 movil 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)

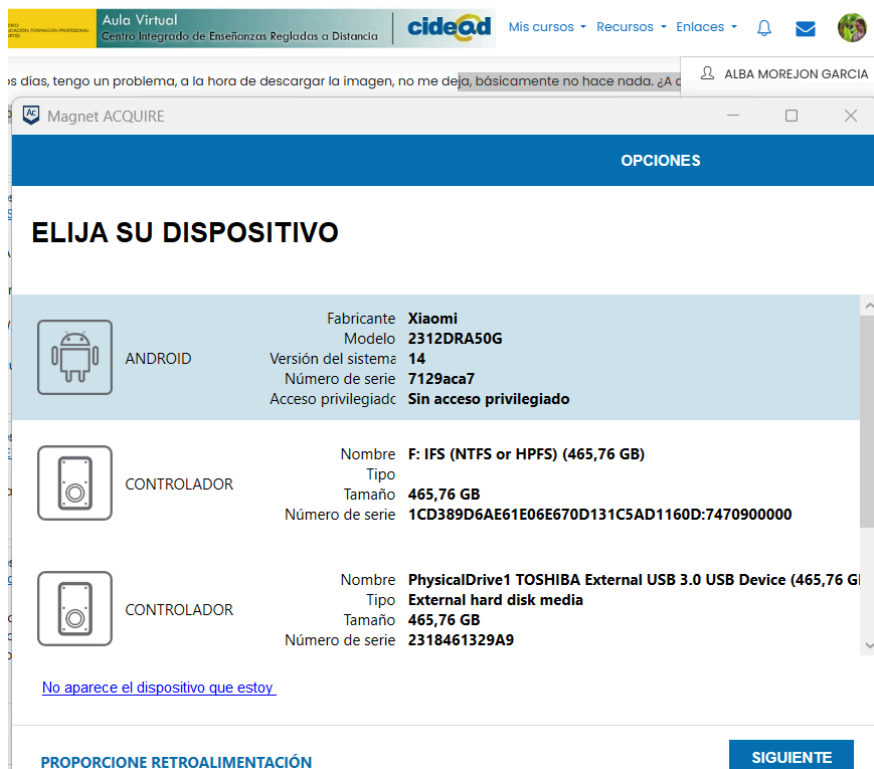
En mi caso, no he podido conseguir un dispositivo móvil con sistema IOS para poder realizar este apartado.

Para hacer una copia directamente del dispositivo se puede hacer desde la configuración del móvil:

Ajustes > Sobre el teléfono > Hacer copia de seguridad y restaurar > Local: Dispositivo móvil. Y se genera una carpeta en el dispositivo donde contiene la información: Almacenamiento interno > MIUI > backup > AllBackup.

También se podría utilizar la aplicación de Magnet Acquire facilitada en el enunciado:

Se descarga e instala la aplicación:



Seleccionamos nuestro dispositivo y la ubicación dónde queramos que se guarde la copia.

Aula Virtual

Centro Integrado de Enseñanzas Regladas a Distancia

cidead


Mis cursos ▾ Recursos ▾ Enlaces ▾

ALBA MOREJON GARCIA

Magnet ACQUIRE

OPCIONES

RESUMEN



ANDROID

Puede que las imágenes no se hayan completado exitosamente.

Tiempo

0 horas 2 minutos

Tamaño de la

0 B

Xiaomi

2312DRA50G

14

7129aca7

Sin acceso privi...

C:\Users\moreg\Desktop\CETI\Android Image - 2025-01-19 02-24-31

ABRIR CARPETA

Inicializando...	Completar
Preparando para imágenes...	Completar
Retirando datos en vivo desde el dispositivo...	Completar
Comprobando si se estableció una contraseña de copia de seguridad de escritorio...	Completar
Desinstalando agente anterior...	No aplica
Instalando agente...	Completar
Confirmar que el dispositivo está desbloqueado...	Completar

PROPORCIONE RETROALIMENTACIÓN

ATRÁS

SALIR

Una vez terminada, se creará una carpeta con los datos copiados del dispositivo.

ual

grado de Enseñanzas Regladas a Distancia

cidead

Mis cursos ▾ Recursos ▾ Enlaces ▾

ALBA MOREJON GARCIA

CETI

Escritorio > CETI >

Busca

Nuevo ▾

OneDrive - Persor

Escritorio

Descargas

Documentos

Nombre	Fecha de modificación
AFI02	18/01/2025 21:14
Android Image - 2025-01-19 02-24-31	19/01/2025 2:27
Ejecutables	23/12/2024 1:07
prueba	21/12/2024 17:59

Apartado 2: Procesado y Preguntas

Utilizaremos el siguiente software para procesar las evidencias: <https://github.com/abrignoni/iLEAPP>

Tienes una guía del software aquí [Guía software de procesamiento 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.

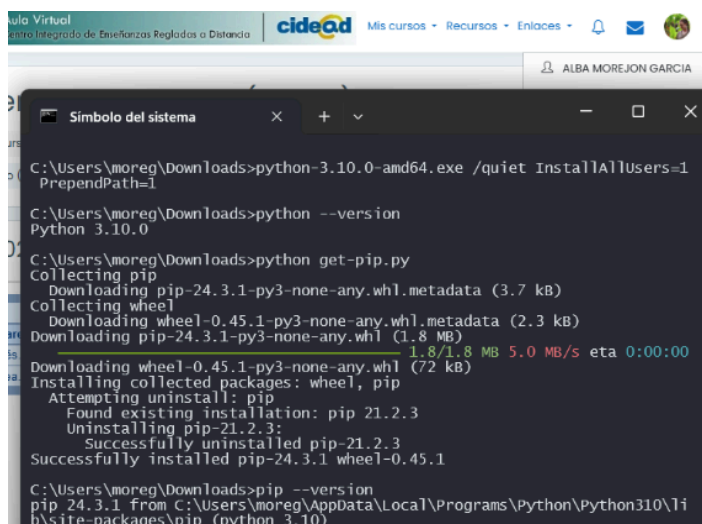
PROCESADO

Utilizaremos un equipo con sistema operativo Windows 11 para este apartado.

Lo primero que haremos será descargar una versión de python que sea compatible con el proceso que vamos a realizar, en este caso descargamos python 3.10 de la siguiente página:

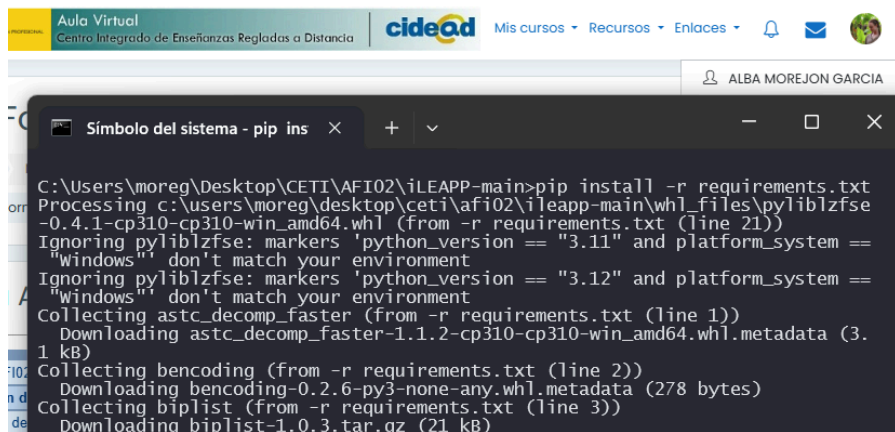
<https://www.python.org/downloads/release/python-3100/> y después instalaremos pip que es una herramienta de gestión de los paquetes relacionados con python.

Utilizaremos los comandos “python-3.10.0-amd64.exe /quiet InstallAllUsers=1 PrependPath=1” y “python get-pip.py” situándonos en la carpeta donde descargamos el ejecutable de python.



```
Símbolo del sistema
C:\Users\moreg\Downloads>python-3.10.0-amd64.exe /quiet InstallAllUsers=1
PrependPath=1
C:\Users\moreg\Downloads>python --version
Python 3.10.0
C:\Users\moreg\Downloads>python get-pip.py
Collecting pip
  Downloading pip-24.3.1-py3-none-any.whl.metadata (3.7 kB)
Collecting wheel
  Downloading wheel-0.45.1-py3-none-any.whl.metadata (2.3 kB)
  Downloading pip-24.3.1-py3-none-any.whl (1.8 MB)
    1.8/1.8 MB 5.0 MB/s eta 0:00:00
  Downloading wheel-0.45.1-py3-none-any.whl (72 kB)
Installing collected packages: wheel, pip
  Attempting uninstall: pip
    Found existing installation: pip 21.2.3
    Uninstalling pip-21.2.3:
      Successfully uninstalled pip-21.2.3
  Successfully installed pip-24.3.1 wheel-0.45.1
C:\Users\moreg\Downloads>pip --version
pip 24.3.1 from C:\Users\moreg\AppData\Local\Programs\Python\Python310\lib\
site-packages\pip (python 3.10)
```

Descargamos el software iLEAPP <https://github.com/abrignoni/iLEAPP> e instalamos las dependencias que necesita desde el archivo requirements.txt. Utilizando el comando “pip install -r requirements.txt”

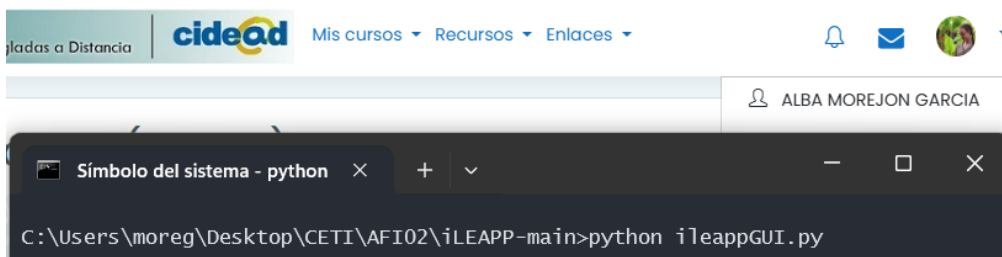


```
Símbolo del sistema - pip ins
C:\Users\moreg\Desktop\CETI\AFI02\iLEAPP-main>pip install -r requirements.txt
Processing c:\users\moreg\desktop\ceti\afi02\ileapp-main\whl_files\pyliblzfse
-0.4.1-cp310-cp310-win_amd64.whl (from -r requirements.txt (line 21))
Ignoring pyliblzfse: markers 'python_version == "3.11" and platform_system ==
"Windows"' don't match your environment
Ignoring pyliblzfse: markers 'python_version == "3.12" and platform_system ==
"Windows"' don't match your environment
Collecting astc_decomp_faster (from -r requirements.txt (line 1))
  Downloading astc_decomp_faster-1.1.2-cp310-cp310-win_amd64.whl.metadata (3.
1 kB)
Collecting bencoding (from -r requirements.txt (line 2))
  Downloading bencoding-0.2.6-py3-none-any.whl.metadata (278 bytes)
Collecting biplist (from -r requirements.txt (line 3))
  Downloading biplist-1.0.3.tar.gz (21 kB)
```

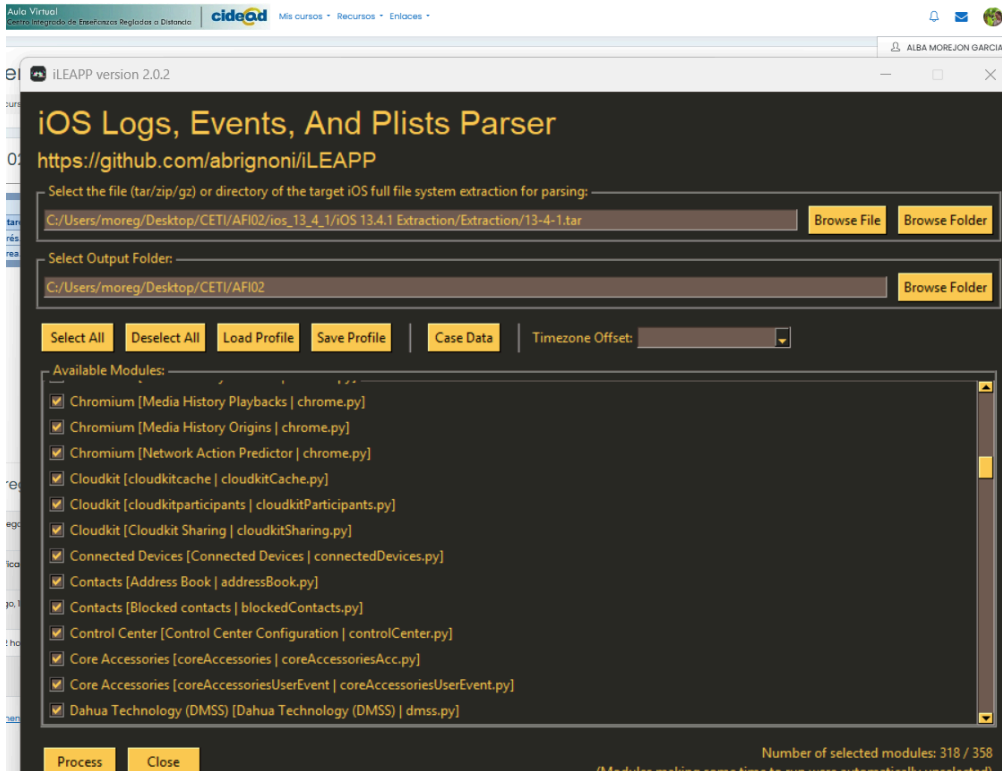
Ahora descargamos la imagen del teléfono móvil ios facilitada en el ejercicio

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

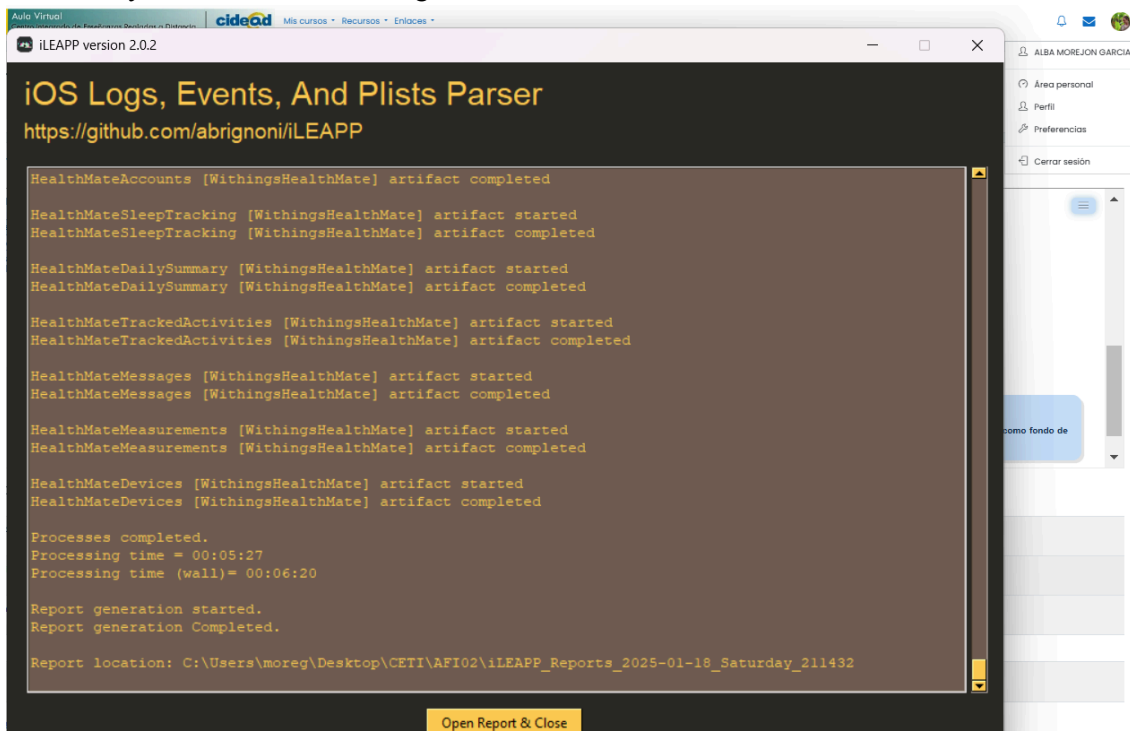
Nos situamos en la carpeta en la que se encuentra el software y ejecutamos la herramienta iLEAPP con la interfaz gráfica “python ileappGUI.py”.



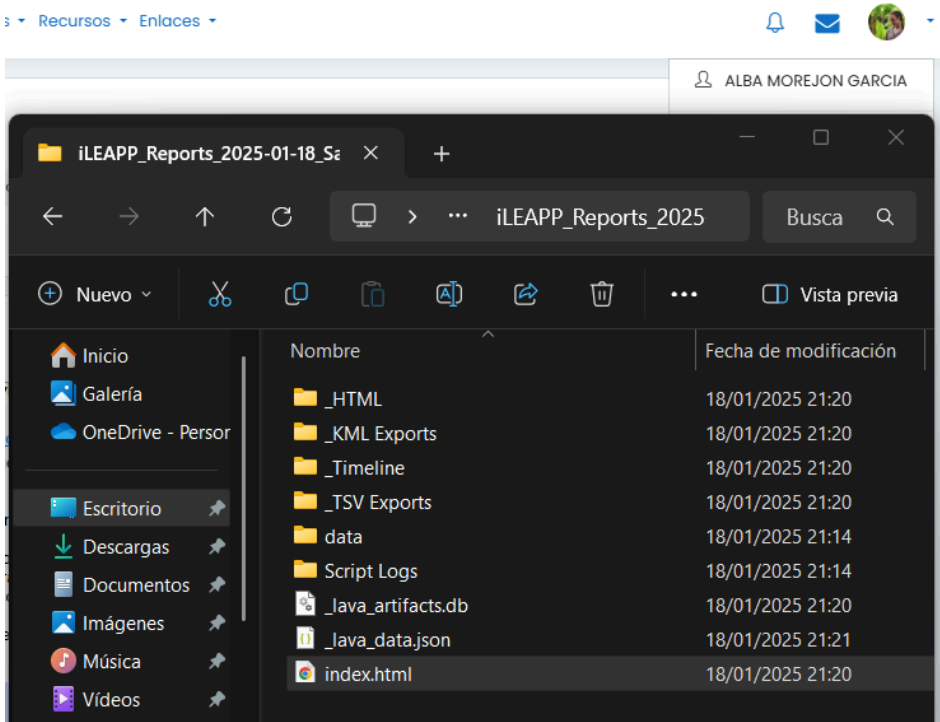
Se abrirá la siguiente ventana y tendremos que seleccionar la carpeta donde se encuentre la información de la del teléfono en nuestro equipo y donde queremos que nos guarde el documento que se cree.



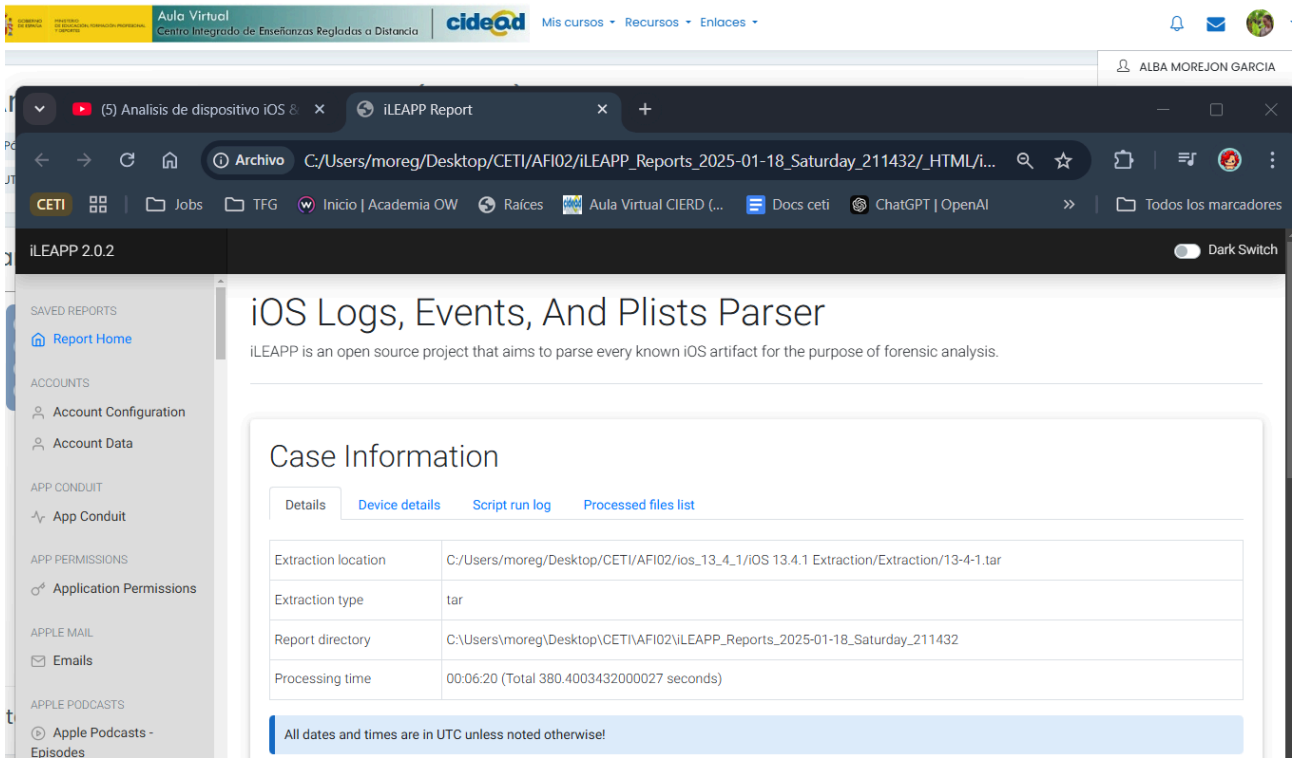
Cuando haya finalizado saldrá lo siguiente.



En la carpeta que hubiésemos seleccionado para que se guardase la información extraída, nos creará una carpeta llamada iLEAPP_Reports y ejecutamos el archivo index.html que contiene con un navegador.



Se abrirá esta web mostrando toda la información sobre el teléfono.



PREGUNTAS

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

Cuando conectamos el dispositivo IOS (ya sea un iPhone, iPad...) a un ordenador aparece un mensaje en pantalla que dice: “¿Confiar en este ordenador/dispositivo?”, este mensaje solicita al usuario que indique si desea confiar en el ordenador. Da dos opciones “Confiar” o “No confiar”, si elige confiar el ordenador, este podrá acceder a la información que contiene el dispositivo móvil como fotos, contactos y otros datos, si decide no confiar, se bloquea el acceso a todos esos datos y el ordenador no podrá acceder.

Un ejemplo:



- **¿Qué tipo de extracción es?**

La copia de seguridad realizada se considera una extracción lógica. Este tipo de extracción copia los datos accesibles del dispositivo, como los contactos, mensajes, fotos, notas... pero no incluye información como los datos del sistema o los datos eliminados, tampoco se accede directamente al almacenamiento del dispositivo.

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

Los riesgos relacionados con una copia de seguridad es que incluye la posibilidad de que personas no autorizadas puedan acceder a los datos si la copia no está protegida con una contraseña. Además, si el ordenador en el que se hace esa copia de seguridad estuviera infectado con algún tipo de malware, los datos estarían comprometidos.

Durante la extracción lógica se pueden modificar los datos en el dispositivo, no llevar a cabo un procedimiento adecuado o cualquier error durante el proceso de la copia de seguridad podría resultar en la pérdida o alteración de los datos. Es crucial utilizar herramientas especializadas para realizar este tipo de copias y saber que durante la extracción lógica que el dispositivo puede generar nuevos registros de actividad, usar herramientas no certificadas también podría producir daños en los datos...

En la imagen facilitada no se produce ningún tipo de cambio cuando se hace la copia, ya que este proceso es de solo lectura, los datos se copian sin modificar el contenido. Pero, podemos identificar en el apartado de “Sysdiagnose - Shutdown Log Processes” que existen algunos eventos que realiza el teléfono, se muestra en pantalla el mensaje de que el dispositivo ha sido conectado al ordenador y si queremos dar permisos.

Simplemente por haber conectado el teléfono deja este rastro en los logs (y esto se podría interpretar como una modificación).

Timestamp	Entry Number	PID	Path	Source File
2020-03-21 22:57:26+00:00	1	283	/System/Library/PrivateFrameworks/EmailDaemon.framework/mailid/D99E22EE-C0EF-32D3-9ECC-9FA4214B47EC	VC:/Users/morej.../01-18_Saturday.../Private/var/
2020-03-21 22:57:26+00:00	2	267	/System/Library/Frameworks/Accounts.framework/accountsd/A8843ABC-C657-3BF4-A60D-23DAF85876E3	VC:/Users/morej.../01-18_Saturday.../Private/var/
2020-03-21 22:57:26+00:00	3	249	/usr/libexec/corelvd/27E3596C-8086-3F87-9C18-6485DEB851C6	VC:/Users/morej.../01-18_Saturday.../Private/var/
2020-03-21 22:57:26+00:00	4	193	/usr/libexec/swcd/45AA79C0-E7BC-9ECB-AFF0-BD9A164E12DD	VC:/Users/morej.../01-18_Saturday.../Private/var/
2020-03-21 22:57:26+00:00	5	188	/usr/libexec/duetexperts/B765CECF-9329-3FA2-AA51-9CF426204C97	VC:/Users/morej...

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

Existen dos tipos de extracciones una lógica, como la que hemos realizado en esta práctica, en la que se copian los datos accesibles del dispositivo y una lógica en la que se realiza una copia de la imagen completa del almacenamiento del dispositivo, en la que se incluyen los datos del sistema operativo y los archivos eliminados. Este tipo de extracción requiere el acceso físico al dispositivo y herramientas especializadas.

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

En caso de que tenga sincronizado el dispositivo con iCloud, se podría acceder a la página web para hacer una copia de seguridad de los datos guardados, utilizando las credenciales del usuario (fotos, contactos...). En caso de usar un equipo que ya haya sido establecido como de confianza para el teléfono, no haría falta desbloquear el móvil para confiar nuevamente, conectando el dispositivo al ordenador, se accedería a los datos.

- **¿Eres capaz de identificar el número de móvil?**

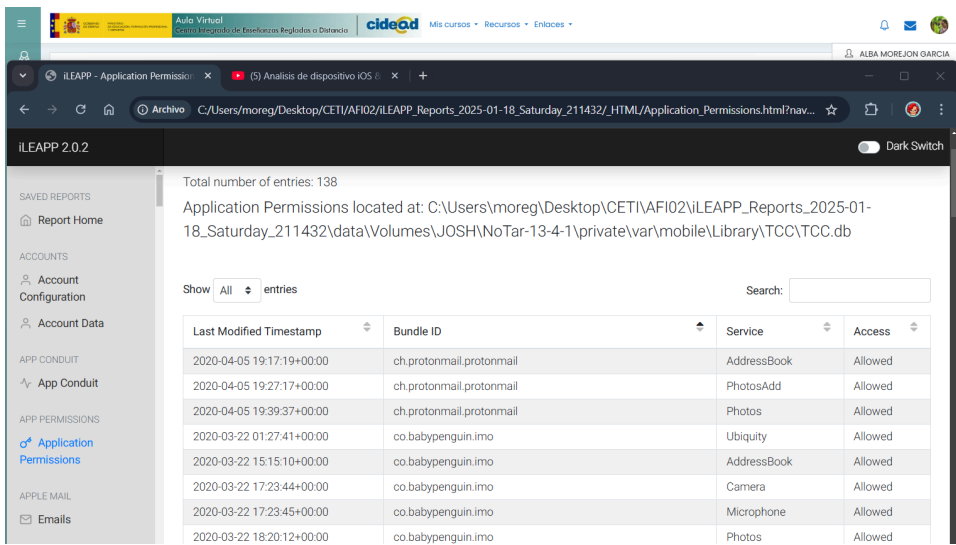
En el reporte que creó la aplicación de iLEAPP, en el apartado “Device details” nos especifica la información sobre el dispositivo. En este caso el número de teléfono es: +19195794674, donde el +1 indica el prefijo internacional para Estados Unidos, 919 el código del área y el resto es la identificación única del número

The screenshot shows the iLEAPP 2.0.2 application window. The browser address bar shows the file path: C:/Users/moreg/Desktop/CETI/AFI02/iLEAPP_Reports_20... The application has a sidebar on the left with the following sections: SAVED REPORTS (Report Home), ACCOUNTS (Account Configuration, Account Data), APP CONDUIT (App Conduit), APP PERMISSIONS (Application Permissions), APPLE MAIL (Emails), APPLE PODCASTS (Apple Podcasts - Episodes, Apple Podcasts - Shows), APPLE WALLET (Cards, PK Pass - Apple Cash), and BLUETOOTH (Bluetooth Other LE, Bluetooth Paired LE). The main content area is titled 'iLEAPP 2.0.2' and has a 'Dark Switch' toggle. It contains four tabs: Details, Device details (selected), Script run log, and Processed files list. The 'Device details' tab displays the following information:

- Find My iPhone: Enabled
- Find My iPhone Add Time: 2020-03-21 21:48:00.790952
- com.apple.MobileSMS.plist - Keep Messages for Days (iOS <=16): 0
- com.apple.mobileSMS.plist - Keep Messages for Days (iOS <=16): Forever
- Obliterated Timestamp: 2020-03-21 21:38:44+00:00
- com.apple.mobileslideshow.plist-downloadAndKeepOriginals: False
- com.apple.purplebuddy.plist-SetupState: SetupUsingiTunes
- Device Information ---
- iOS version: 13.4.1 (Source: lastBuild)
- 13.4.1 (Source: systemVersionPlist)
- ProductBuildVersion: 17E262 (Source: lastBuild)
- 17E262 (Source: systemVersionPlist)
- Product Name: iPhone OS (Source: lastBuild)
- iPhone OS (Source: systemVersionPlist)
- Reported Phone Number: 19195794674 (Source: deviceDatam)
- IMEIs: [{"second": "355800076093966", "first": "1:kOne"}] (Source: deviceDatam)
- Device Name: This Is's iPhone (Source: deviceName)
- Model: N69AP (Source: preferencesPlist)
- Local Host Name: This-Is's-iPhone (Source: preferencesPlist)
- Device/Computer Name: This Is's iPhone (Source: preferencesPlist)
- Host Name: This-Is's-iPhone (Source: preferencesPlist)
- Serial Number: DX3T126VH2XV (Source: serialNumber)
- Last Bootstrap Date: 2020-04-15 00:59:55.731066+00:00 (Source: timezoneInfo)
- Cellular ---
- Last Known ICCID: 8901260971148676693 (Source: cellWireless)
- Reported Phone Number: 19195794674 (Source: cellWireless)
- IMEI: 355800076093966 (Source: cellWireless)
- MEID: 355800076093966 (Source: cellWireless)
- Last Good IMSI: 310260974867669 (Source: imeiImei)
- Self Registration Update IMSI: 310260974867669 (Source: imeiImei)
- Self Registration Update IMEI: 355800076093966 (Source: imeiImei)
- Phone Number: 19195794674 (Source: imeiImei)
- SIM Cards: Slot 1 -> ICCID: 8901260971148676693 | MSISDN: +19195794674 | Last Update: 2020-04-16 15:53:09+00:00 (Source: subscriberInfo)

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

En el apartado de “Applications Permissions” muestra la base de datos TCC.db que nos indica qué aplicaciones tienen permisos concedidos a qué recursos. En la siguiente captura se puede corroborar que los permisos han sido concedidos “Allowed” en caso de que algún permiso hubiese sido denegado, saldría catalogado como “Not Allowed”. En algunos casos se registran en las notificaciones si el usuario consiente los permisos, pero en este caso no he podido localizar dónde está registrada esa información.



Application Permissions located at: C:\Users\moreg\Desktop\CET\AFI02\LEAPP_Reports_2025-01-18_Saturday_211432\data\Volumes\JOSH\NoTar-13-4-1\private\var\mobile\Library\TCC\TCC.db

Show entries

Last Modified Timestamp	Bundle ID	Service	Access
2020-04-05 19:17:19+00:00	ch.protonmail.protonmail	AddressBook	Allowed
2020-04-05 19:27:17+00:00	ch.protonmail.protonmail	PhotosAdd	Allowed
2020-04-05 19:39:37+00:00	ch.protonmail.protonmail	Photos	Allowed
2020-03-22 01:27:41+00:00	co.babypenguin.imo	Ubiquity	Allowed
2020-03-22 15:15:10+00:00	co.babypenguin.imo	AddressBook	Allowed
2020-03-22 17:23:44+00:00	co.babypenguin.imo	Camera	Allowed
2020-03-22 17:23:45+00:00	co.babypenguin.imo	Microphone	Allowed
2020-03-22 18:20:12+00:00	co.babypenguin.imo	Photos	Allowed

A continuación se muestra una tabla con los permisos otorgados a cada aplicación:

CLIENT	CAMERA	MICROPHONE	LOCATION	CONTACT	LOCATION	PHOTOS	SIRI	LIVERPOOL	ADDRESSBOOK
ch.protonmail.protonmail	0	0	0	0	0	1	0	0	1
co.babypenguin.imo	1	1	0	0	1	1	0	0	1
com.apple.accessibilityUIServer	0	0	0	0	0	0	0	1	0
com.apple.DocumentsApp	0	0	0	0	1	0	0	0	0
com.apple.iCloudNotification	0	0	0	0	0	0	0	1	0
com.apple.MailCompositionService	0	0	0	0	1	0	0	0	0
com.apple.Maps	0	0	0	0	0	0	0	1	0
com.apple.MobileBackup.framework	0	0	0	0	0	0	0	1	0
com.apple.PassKitCore	0	0	0	0	1	0	0	0	0
com.apple.Passbook	0	0	0	0	1	0	0	0	0
com.apple.mobilemail	0	0	0	0	1	0	0	0	0
com.apple.mobilenotes	0	0	0	0	0	0	0	1	0
com.apple.mobilesafari	0	0	0	0	1	0	0	1	0
com.apple.news	0	0	0	0	0	0	0	1	0
com.apple.newsdaemon	0	0	0	0	0	0	0	1	0
com.apple.stocks	0	0	0	0	0	0	0	1	0
com.apple.purplebuddy	0	0	0	0	1	0	0	0	0
com.apple.VoiceShortcuts	0	0	0	0	0	0	0	1	0
com.belkin.plugin	0	0	0	0	1	0	0	0	0
com.adhoclabs.burner	0	0	0	0	0	0	0	0	1
com.burbn.instagram	1	1	0	0	0	1	0	0	0
com.burbn.threads	1	1	0	0	0	0	0	0	0
com.coverme.covermeAdhoc	1	1	0	0	0	1	0	0	1
com.facebook.Messenger	1	1	0	0	0	1	0	0	0
com.hammerandchisel.discord	0	1	0	0	0	1	0	0	0
com.herzick.houseparty	1	1	0	0	0	0	0	0	1
com.keepsafe.KeepSafe	0	0	0	0	1	1	0	0	0
com.kik.chat	0	0	0	0	0	1	0	0	1
com.mentionmobile.cyberdust	1	0	0	0	0	1	0	0	1
com.mewe	1	1	0	0	1	1	0	0	0
com.mywicks.wicks	1	1	0	0	1	1	0	0	0
com.reddit.Reddit	0	0	0	0	0	1	0	0	0
com.silentscircle.SilentPhone	0	1	0	0	0	1	1	0	1
com.skout.SKOUT	1	1	0	0	0	1	0	0	0
com.skype.skype	1	1	0	0	0	1	0	0	1
com.tinginteractive.usms	1	1	0	0	0	1	0	0	0
com.toyopagroup.picaboo	1	1	0	0	0	1	0	0	0
com.viber	1	1	0	0	1	1	1	0	1
com.wearezeta.zclient.ios	1	1	0	0	1	1	0	0	0
com.zhilioapp.musically	1	1	0	0	0	1	0	0	0
de.tutao.tutanota	0	0	0	0	1	1	0	0	0
imgurmobile	0	0	0	0	1	1	0	0	0
jp.naver.line	1	1	0	0	1	1	0	0	1
net.kortina.labs.Venmo	0	0	0	0	0	0	1	0	1
net.whatsapp.WhatsApp	1	1	0	0	1	1	0	0	1
org.whispersystems.signal	1	1	0	0	1	1	0	0	1
ph.telegra.Telegraph	1	1	0	0	1	1	1	0	1
us.zoom.videomeetings	1	1	0	0	1	1	1	0	0