Análisis IOS

CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

MODULO ANALISIS FORENSE

ALUMNO: XINWEI WU

Resumen Ejecutivo

Este informe detalla el proceso de extracción, análisis y evaluación de evidencia digital en un dispositivo iOS. Se documentan herramientas empleadas, riesgos asociados y hallazgos clave, destacando las diferencias entre extracciones lógicas y físicas, con recomendaciones prácticas para optimizar los procesos forenses.

Hallazgos principales:

- Identificación del número de móvil y permisos de aplicaciones.
- Configuraciones clave como "Find My iPhone" activado y respaldos sincronizados en la nube.

Riesgos detectados:

- Posibilidad de sobrescritura de datos y alteración de metadatos.

Introducción

Este informe documenta el proceso de extracción, análisis y respuesta a preguntas clave sobre un dispositivo iOS, usando herramientas forenses y métodos disponibles. Se examinan los riesgos y desafíos específicos asociados al análisis forense en dispositivos móviles basados en iOS.

El trabajo se divide en dos partes principales:

1. Extracción de la evidencia.
2. Procesado de la evidencia y respuestas a preguntas relacionadas.

1. Características y información del Dispositivo

Durante el análisis, se recopilaron las siguientes características del dispositivo iOS a partir de los datos extraídos:

1.1 Información General

- **Versión de iOS:** 13.4.1 (Build 17E262).
- **Nombre del dispositivo:** This Is's iPhone.
- **Modelo:** N69AP.
- **Número de serie:** DX3T126VH2XV.
- **IMEI:** 355800076093966.
- **MEID:** 35580007609396.
- **Última fecha de configuración inicial:** 2020-04-15 00:59:55 UTC.
- **Última zona horaria configurada:** America/New_York.

1.2 Red y Conectividad

- **Dirección MAC Wi-Fi:** a0:d7:95:79:dd:a1.
- **Adaptadores Ethernet:**
    - en1: a2:d7:95:79:dd:a3.
    - en2: a2:d7:95:79:dd:5c.
- **Último número de teléfono reportado:** +1 (919) 579-4674.
- **Último IMSI conocido:** 310260974867669.
- **Última SIM registrada:**
    - ICCID: 8901260971148676693.
    - MSISDN: +1 (919) 579-4674.

1.3 Ajustes del Dispositivo

- **Find My iPhone:** Activado desde el 2020-03-21 21:48:00 UTC.
- **Mensajes almacenados:** Configuración para guardar mensajes "para siempre".
- **Servicios de localización:** Activados.
- **Respaldo en la nube:** Activado.

1.4 Historial de Vehículo Conectado

- **Tipo de conexión:** CarKit NissanConnect.
- **Última conexión:** 2020-04-15 16:16:15 UTC.
- **Última desconexión:** 2020-04-15 16:22:54 UTC.

1.5 Información Publicitaria

- **Identificador publicitario de Apple:** 0D99ABE9-B1D0-41C1-8C45-2681A498AD97.

1.6 Respaldo del Sistema

- **Último respaldo en iTunes:**
    - Fecha: 2020-04-16 15:48:50 UTC.
    - Zona horaria: EDT.
- **Último respaldo en la nube:**
    - Fecha: 2020-04-16 01:25:30 UTC.
    - Zona horaria: EDT.

2. Objetivo del Análisis

El objetivo principal de este análisis es entender los procesos de extracción y procesamiento de evidencias digitales en un dispositivo iOS. En particular:

1. Examinar las características del dispositivo y recopilar información relevante para una investigación forense.
2. Evaluar los riesgos y los cambios que pueden surgir al realizar extracciones de datos en dispositivos iOS.
3. Responder preguntas clave sobre la evidencia extraída, identificando la relación entre las configuraciones del sistema y el comportamiento del dispositivo.

3. Metodología

Se realizaron dos métodos de extracción, detallados a continuación:

- **Método 1:** Backup lógico con iTunes para obtener datos accesibles al usuario, como mensajes, fotos y contactos.
- **Método 2:** Uso de Magnet Acquire para realizar una extracción avanzada y obtener configuraciones del sistema, datos sincronizados y registros adicionales.

Ambos métodos fueron evaluados en términos de limitaciones y riesgos:

- **Ventajas:** El respaldo lógico es rápido y accesible, mientras que Magnet Acquire permite un análisis más profundo de datos sincronizados.
- **Limitaciones:** Ambos métodos están restringidos por el cifrado de iOS, y requieren configuraciones específicas para evitar alteraciones de la evidencia.

3.1 Revisión de la Información Extraída

- Validación de los datos utilizando múltiples fuentes (e.g., backups de iCloud y datos locales).
- Comparación de los resultados obtenidos con las preguntas planteadas en el informe.

4. Extracción de la Evidencia

4.1 Métodos de Extracción Utilizados

Se realizaron pruebas de extracción con las siguientes herramientas:

1. Backup mediante iTunes:
    - Herramienta nativa de Apple utilizada para realizar una copia lógica de los datos del dispositivo.
    - Proceso detallado en la Guía de iTunes de Apple.
2. Extracción forense con Magnet Acquire:
    - Software diseñado para capturar datos de dispositivos móviles de manera más avanzada.
    - Proceso descrito en la Guía de software forense.

4.2 Resultados de la Extracción

Ambos métodos permitieron obtener un conjunto de datos inicial para el análisis, incluyendo:

- Mensajes, contactos, registros de llamadas y fotografías (extracción lógica).
- Metadatos adicionales (en el caso de Magnet Acquire).

4.3 Riesgos y Cambios Detectados Durante la Extracción

- Riesgos:
    - Posibilidad de sobrescritura de datos al generar un nuevo backup.
    - Alteración de metadatos debido a la conexión del dispositivo.
    - Sincronización automática con iCloud si no se desactiva previamente.
- Cambios Observados:
    - Registro de conexión en los logs del dispositivo.
    - Creación de archivos temporales.

5. Procesado de la Evidencia

5.1. Herramienta Utilizada: iLEAPP

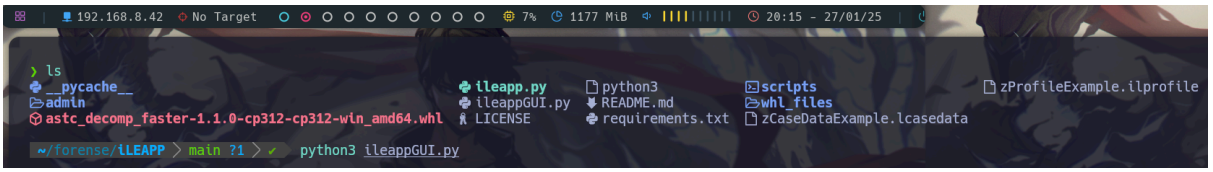
El procesado de la evidencia se realizó usando iLEAPP, una herramienta de análisis forense específica para dispositivos iOS.

- Repositorio de iLEAPP.
- Guía de uso de iLEAPP.

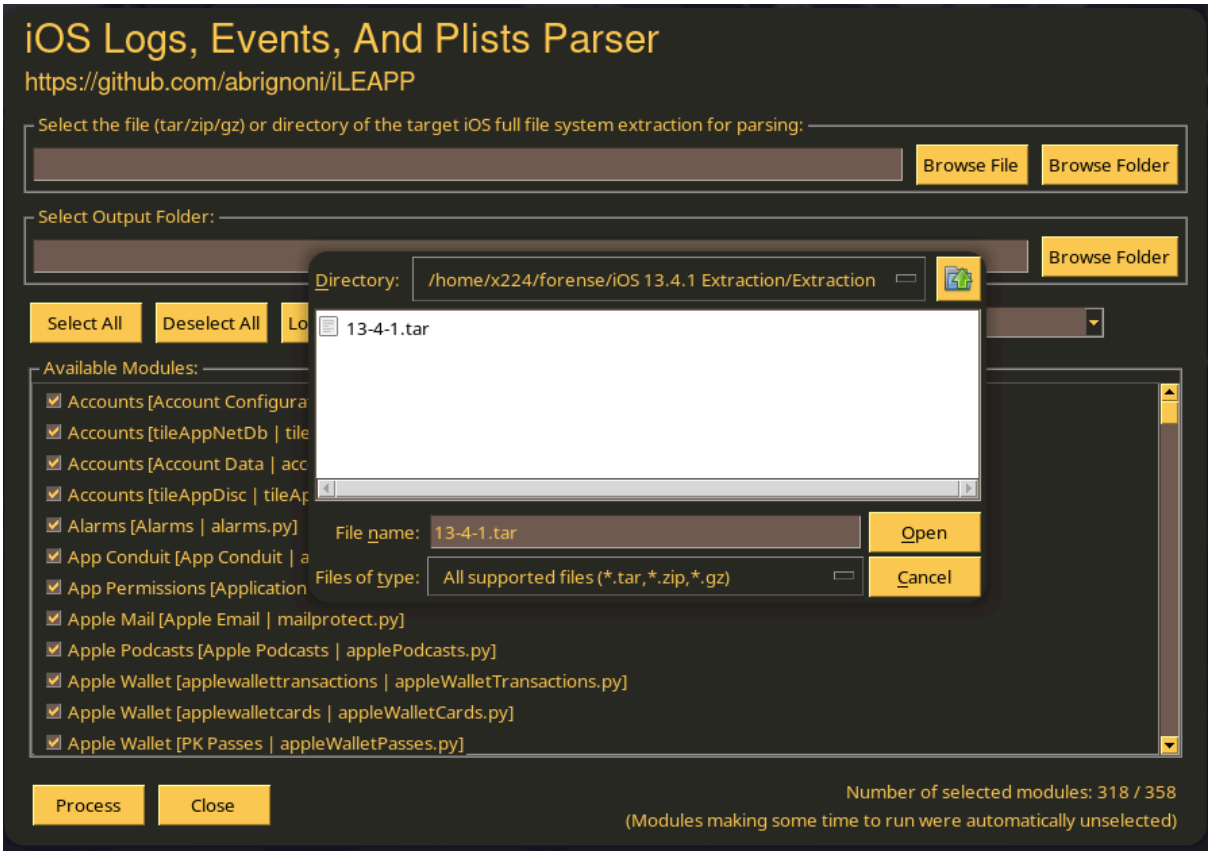
5.2. Uso de la herramienta.

1º - Ejecutamos la herramienta
Iniciamos la herramienta desde la consola con el siguiente comando:

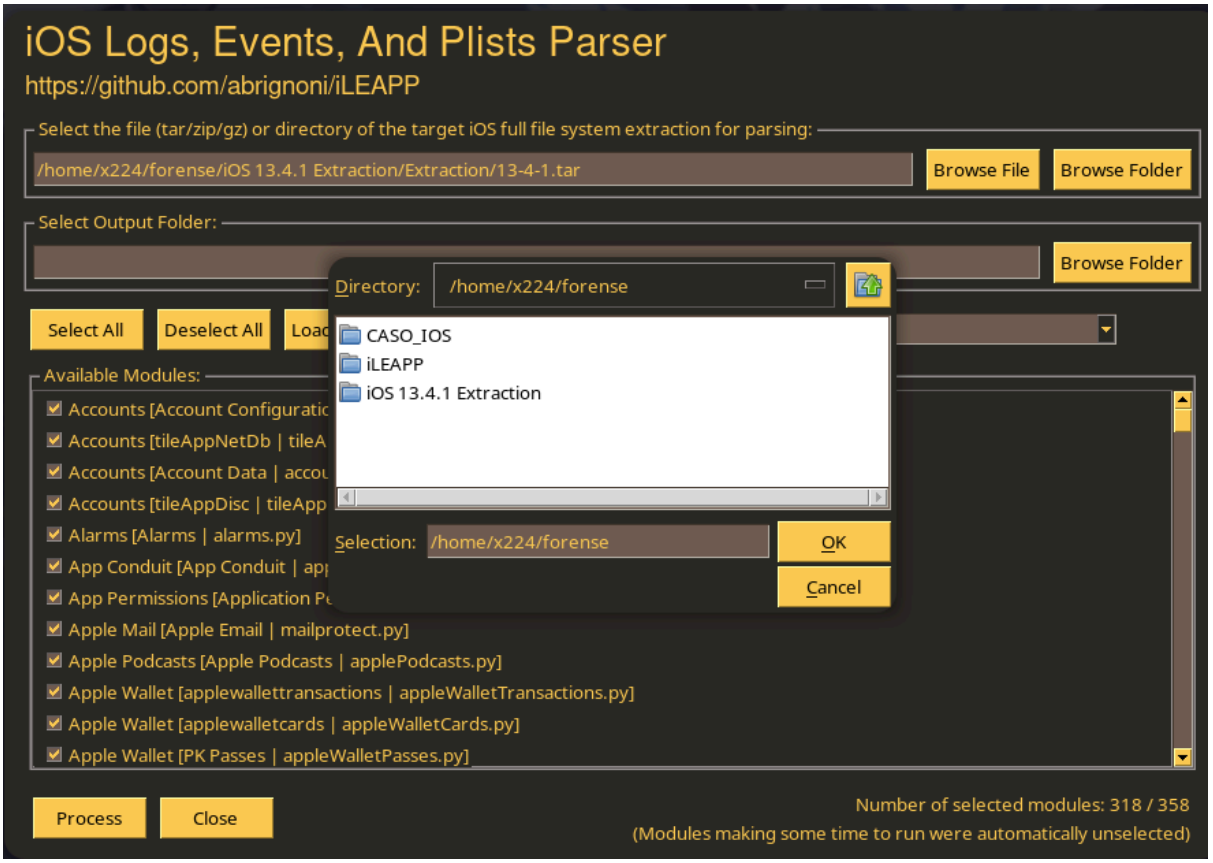
Python3 ileappGUI.py



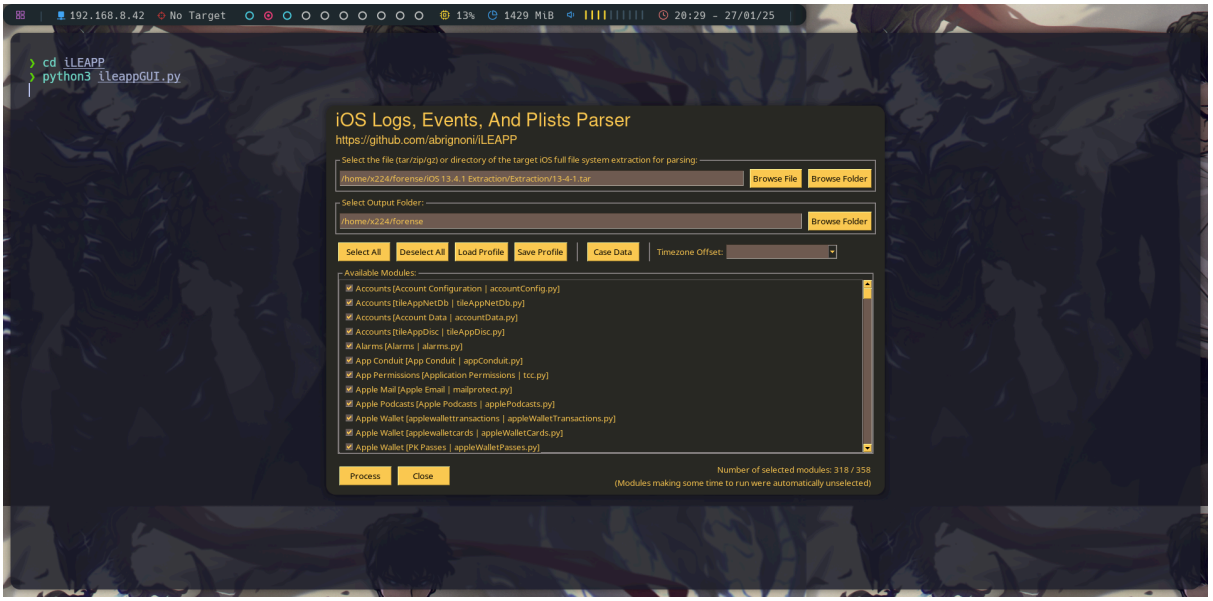
2º-Seleccionar el volcado
Localizamos el archivo de volcado de datos. En este caso, se trata de `13-4.1.tar`.



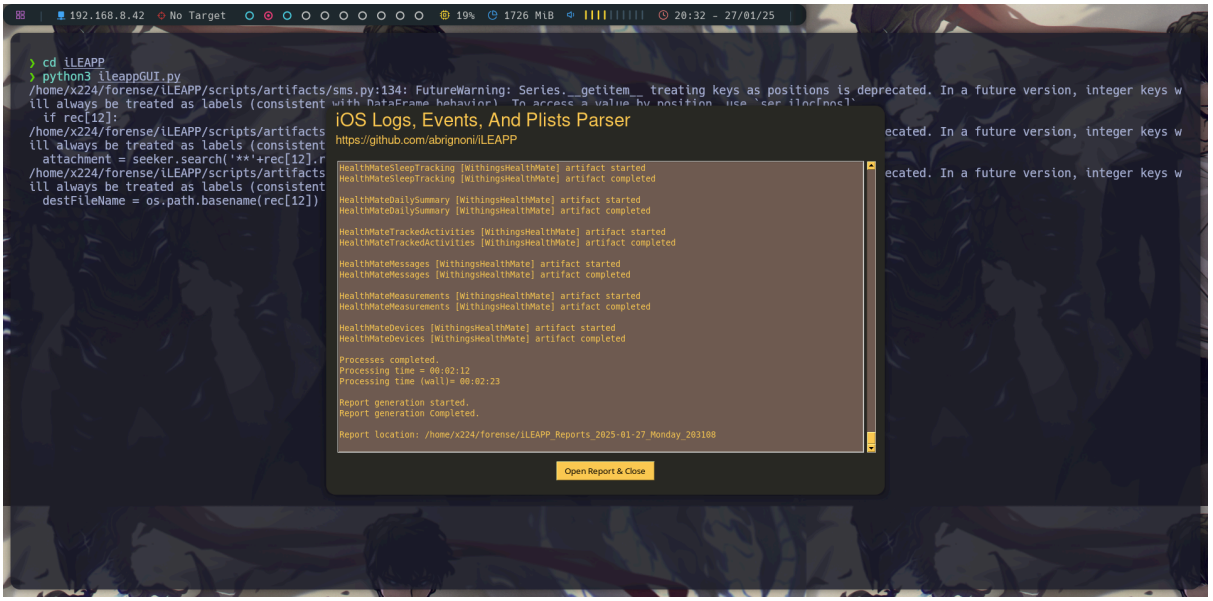
3º Elegimos nuestra carpeta de salida.
Seleccionamos el directorio de destino donde se guardarán los resultados procesados. En este análisis, se utilizó la carpeta `CASO_IOS`.



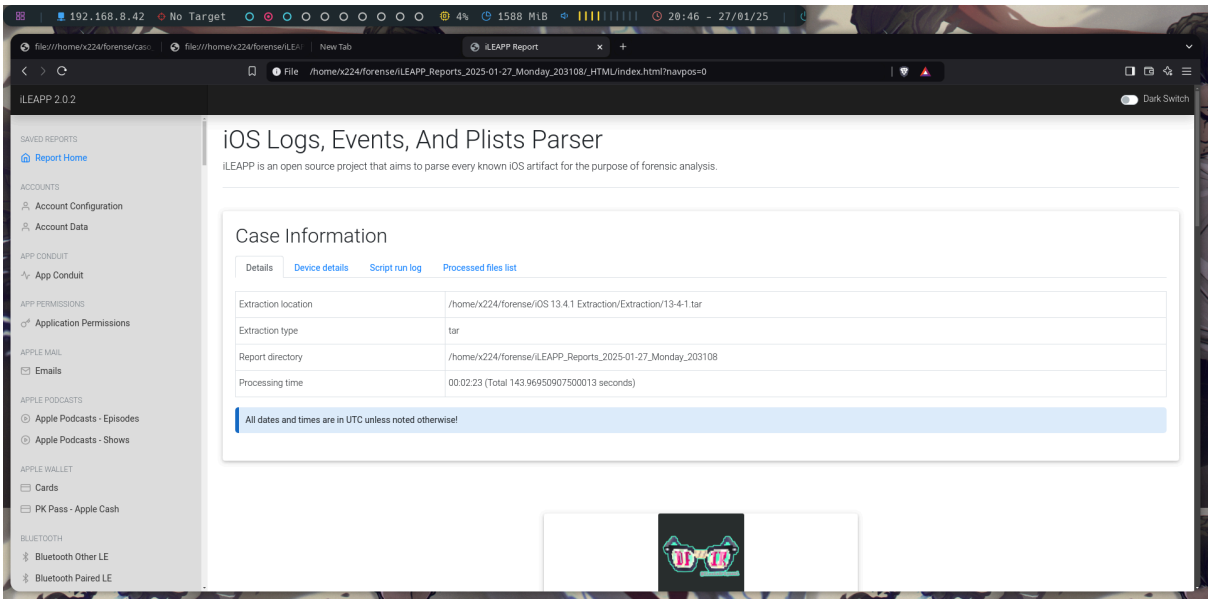
4º Procesar la evidencia:
Hacemos clic en el botón **“Process”** para iniciar el procesamiento del volcado.



5º Abrir los resultados:



Una vez finalizado el procesamiento, accedemos a la carpeta de salida para analizar los datos extraídos.



5.3 Resultados del Procesado

El análisis permitió identificar:

1. Número de móvil: Localizado en registros del dispositivo y cuentas configuradas.
2. Permisos de aplicaciones: Identificados a través de los registros extraídos, mostrando qué apps tienen acceso a recursos como contactos, ubicación y micrófono.

6. Identificación y Custodia de la Evidencia

Para garantizar la autenticidad e integridad de los datos forenses, se realizaron las siguientes acciones al manejar el volcado del dispositivo:

6.1. Identificación del Volcado de Datos

- Nombre del archivo: 13-4-1.tar
- Tamaño: 16 GB
- Fecha y hora de creación: Sat Apr 18 22:20:50 2020

6.2. Cálculo de Hashes

Se calcularon los hashes MD5 y SHA-256 para verificar la integridad del archivo y garantizar que no ha sido modificado durante el análisis:

- MD5: c2a733e6db7af9be6bd0437fd7c765f8
- SHA-256: 991727d92145a08623e998c008cc2a05f086be722ee2945815d0eb46a78f04fb

6.3. Custodia de la Evidencia.

El archivo 13-4-1.tar fue almacenado en un entorno seguro y accesible únicamente por el analista designado para el caso.

- Ubicación del almacenamiento: Carpeta “CASO_IOS” en un disco cifrado.
- Procedimientos aplicados: Se aseguró que los accesos al archivo fueran limitados y rastreables mediante registros de acceso.

Para reforzar la custodia de la evidencia, se generaron logs detallados de acceso al archivo y se almacenaron copias redundantes en diferentes ubicaciones seguras, siguiendo los principios de la "regla 3-2-1" de respaldo forense (3 copias de la evidencia, en 2 medios distintos, y 1 copia fuera del sitio principal).

7. Respuesta a Preguntas

7.1. ¿Qué sucede cuando conectamos el dispositivo móvil al ordenador?

Al conectar el dispositivo al ordenador, el sistema operativo del ordenador intenta identificar el dispositivo como medio externo. En el caso de iPhones:

- iOS solicita autorización para establecer confianza entre el dispositivo y el ordenador.
- Si se autoriza, iTunes o herramientas forenses detectarán el dispositivo y podrán acceder a los datos permitidos.
- Dependiendo de la configuración, se pueden acceder a backups previos o generar nuevos.

7.2. ¿Qué tipo de extracción es?

El tipo de extracción depende del método utilizado:

- Backup con iTunes: Es una extracción lógica, ya que se obtienen datos accesibles para el usuario, como contactos, mensajes, fotos, etc.
- Software forense especializado: Puede realizar extracciones lógicas o avanzadas, dependiendo de las capacidades de la herramienta y las configuraciones del dispositivo.

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

- Riesgos:
  - Generar un nuevo backup puede sobrescribir datos existentes en el dispositivo.
  - Alteración de metadatos al conectar o acceder a ciertos archivos.
  - Si el dispositivo no está en modo avión, puede recibir nuevas notificaciones o datos que alteren la evidencia.
- Cambios:
  - Se registran logs de conexión en el dispositivo.
  - Pueden generarse archivos temporales o sincronización automática de datos con iCloud.

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

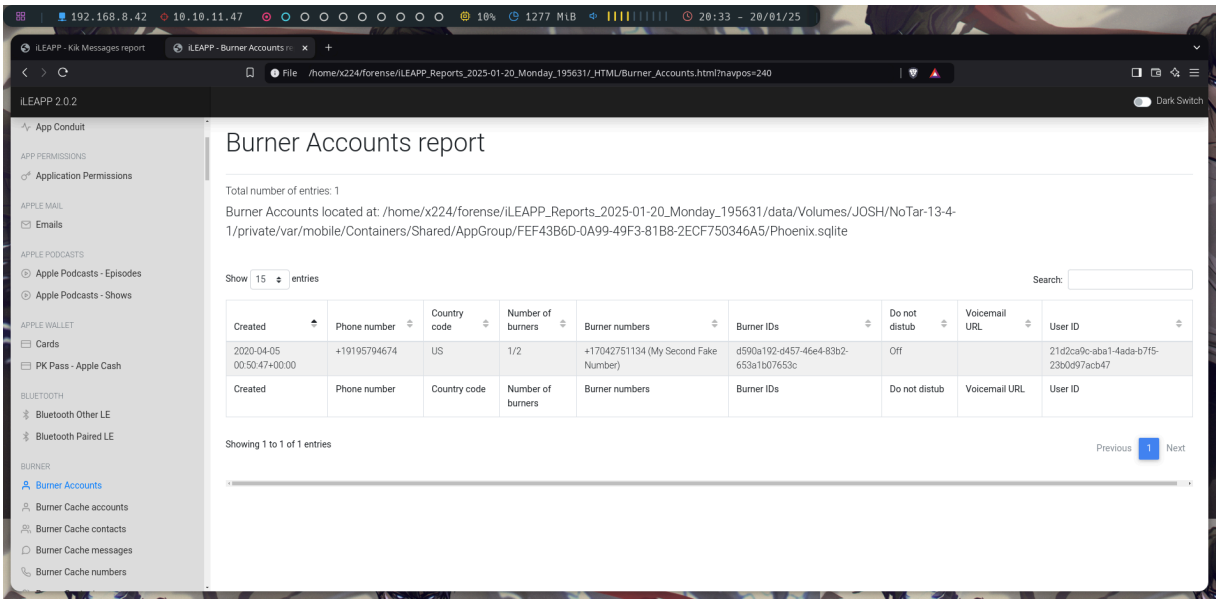
Extracción Lógica	Extracción Física
Datos accesibles al usuario.	Incluye datos eliminados.
No requiere acceso completo.	Requiere técnicas avanzadas (e.g., jailbreaking).
Menos invasiva.	Acceso completo al sistema de archivo

7.5. ¿Qué alternativas tenemos si no conocemos el código de desbloqueo pero tenemos o podemos conseguir el usuario y contraseña de la cuenta de Apple?

- Usar las credenciales de iCloud para acceder a backups almacenados en la nube.
- Restaurar el dispositivo desde iCloud a un entorno controlado, generando un backup lógico.
- Utilizar herramientas especializadas que aprovechen las credenciales para extraer datos sincronizados con iCloud, como Magnet Acquire o Elcomsoft iOS Forensic Toolkit.

7.6. ¿Eres capaz de identificar el número de móvil?

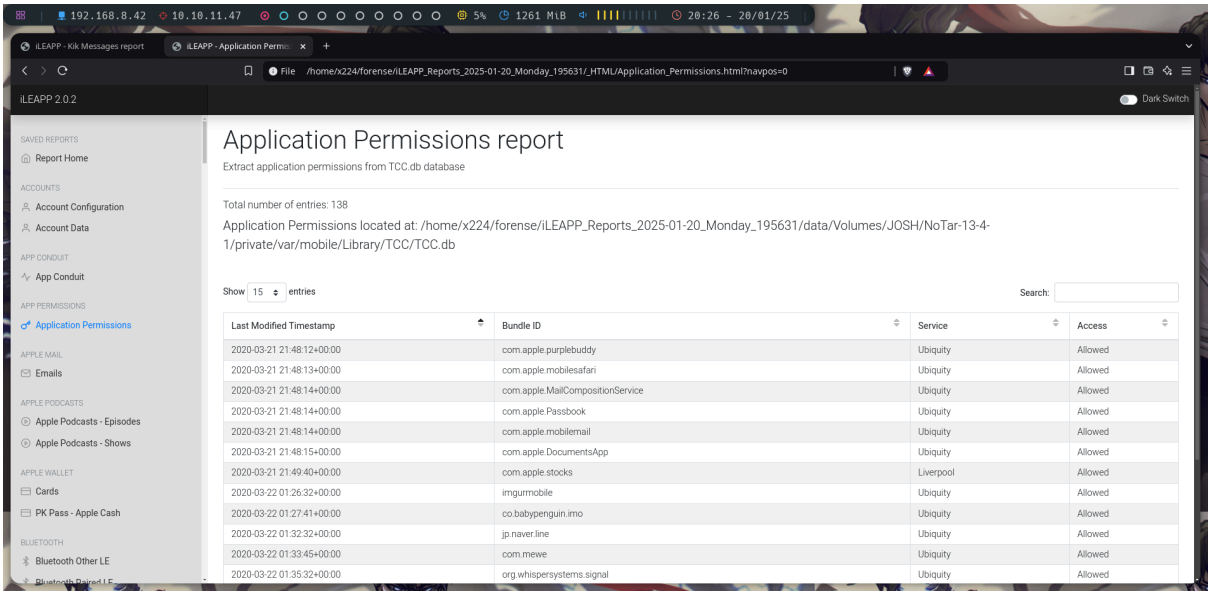
Sí, el número de móvil se puede identificar en el apartado Burner Accounts, el numero original y el número desechable.



7.7. ¿Eres capaz de identificar qué apps tienen concedidos permisos a qué recursos?

Sí, es posible identificar qué aplicaciones tienen permisos para acceder a recursos específicos como contactos, ubicación o micrófono. Esto se hace analizando los registros extraídos del dispositivo y generados por herramientas como iLEAPP.

Nota adicional: Aunque iOS solicita confirmación explícita para conceder permisos, es común que los usuarios acepten sin leer las implicaciones. Esto resalta la importancia de concienciar sobre la privacidad digital.



¿El usuario ha sido consciente de forma explícita de este consentimiento?

iOS solicita permisos explícitos para cada recurso en el momento en que la app lo requiere. Sin embargo, muchos usuarios no comprenden completamente el alcance del acceso que conceden.

8. Conclusión y recomendaciones

El análisis forense de dispositivos iOS requiere un enfoque meticuloso y adaptado a las limitaciones técnicas y legales de este tipo de dispositivos. Los métodos aplicados en este informe han demostrado ser efectivos para recopilar y procesar evidencia, aunque se debe considerar lo siguiente:

1. **Priorización de extracciones físicas:** En investigaciones críticas, las extracciones físicas permiten recuperar datos eliminados y obtener acceso completo al sistema de archivos.
2. **Evitación de alteraciones de datos:** Configurar el dispositivo en modo avión y desactivar sincronizaciones automáticas antes de realizar la extracción.
3. **Educación del usuario:** Capacitar a usuarios y empresas sobre los permisos que otorgan a aplicaciones y cómo impactan en su privacidad y seguridad.
4. **Uso de herramientas actualizadas:** Garantizar que las herramientas forenses utilizadas sean compatibles con la última versión del sistema operativo iOS.

9. Firmas y Certificación

Certificación del Análisis

Este informe certifica que el análisis forense digital aquí descrito fue realizado siguiendo las mejores prácticas de la disciplina, utilizando herramientas reconocidas en el ámbito forense y bajo un entorno controlado.

Las evidencias fueron manejadas conforme a los estándares legales y técnicos, asegurando la cadena de custodia y la integridad de los datos obtenidos.

Investigador:

- **Nombre**: Xinwei
- **Apellidos**: Wu
- **DNI/NIE**: U8766008F
- **Teléfono**: 600 000 000
- **Correo electrónico**: xinwei.wu@forense.digital.es
- **Fecha de elaboración del informe**: 28 de enero de 2025

Firma: Xinwei Wu

(Firma del investigador o equipo forense)

Xinwei Wu

10. BIBLIOGRAFÍA

1. Apple Inc. (2020). *Guía de iTunes para copia de seguridad y restauración*. Recuperado de https://support.apple.com.
2. Magnet Forensics. (2020). *Guía del usuario de Magnet Acquire*. Recuperado de https://www.magnetforensics.com.
3. Mislan, R., Casey, E., & Kessler, G. (2010). *Mobile device forensics: Current research and future trends*. *Digital Investigation, 7*(3-4), S14-S23.
4. NIST. (2014). *Guidelines on Mobile Device Forensics*. Special Publication 800-101 Revision 1. Recuperado de https://www.nist.gov.
5. iLEAPP Repository. (2025). *iLEAPP Forensics Tool Documentation*. Recuperado de https://github.com/abrignoni/iLEAPP.

11. ANEXOS

Las imágenes adjuntadas en el informe se encuentran en el archivo comprimido ANEXOS.ZIP. Este archivo contiene una serie de capturas de pantalla y evidencias visuales que respaldan los hallazgos descritos en el informe.