Análisis Forense de Dispositivos iOS

Jaime Andrés Restrepo

Agenda de la Charla

Agenda de la Charla

- Introducción

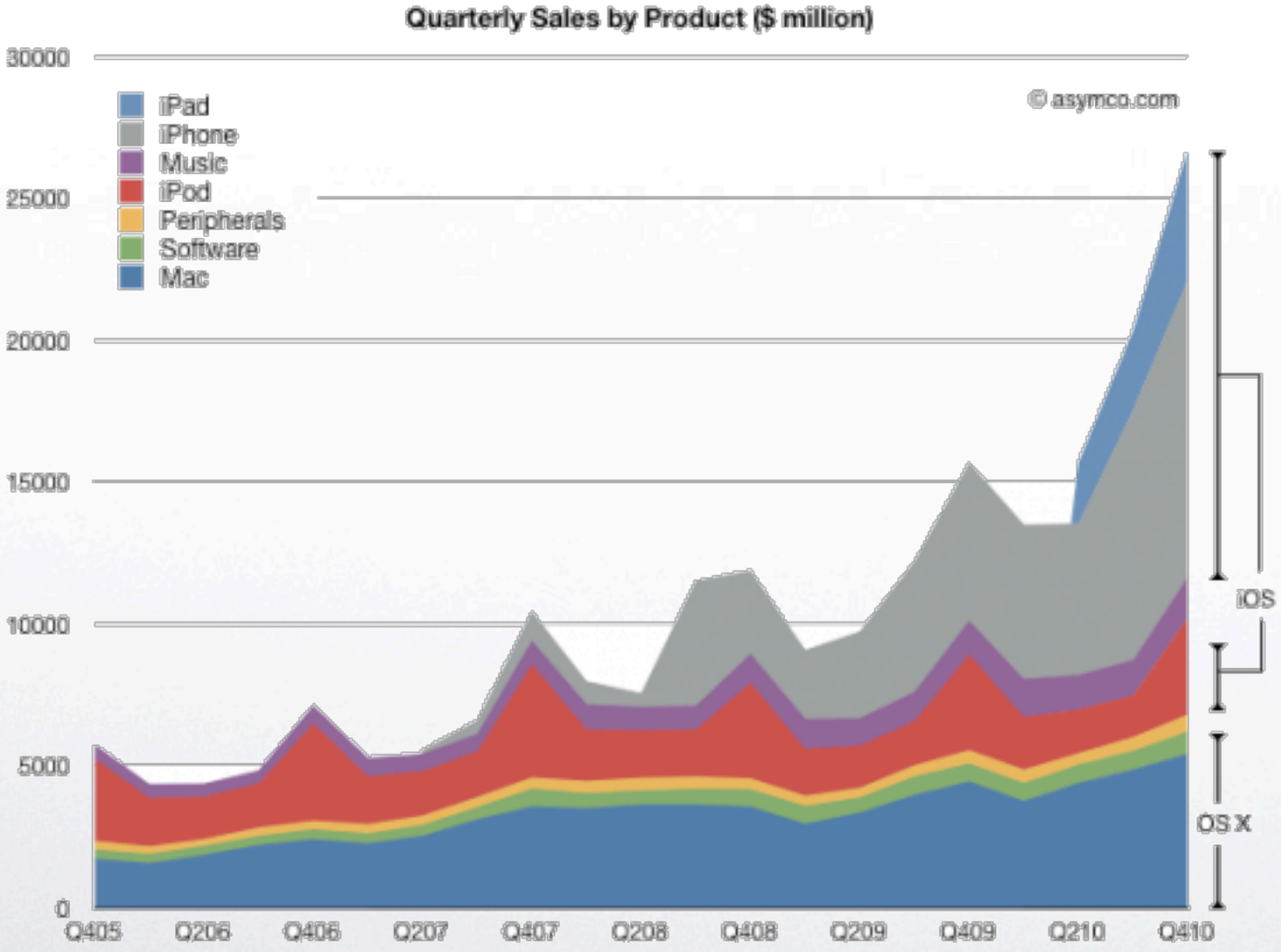
Agenda de la Charla

- Introducción
- ¿Como vamos a trabajar?

Agenda de la Charla

- Introducción
- ¿Como vamos a trabajar?
- **Manos a la Obra!!**

Introducción



¿Cómo vamos a trabajar?

¿Cómo vamos a trabajar?

- No dejarlos iniciados.

¿Cómo vamos a trabajar?

- No dejarlos iniciados.
- Utilizaremos códigos QR y acortadores de direcciones.

¿Cómo vamos a trabajar?

- No dejarlos iniciados.
- Utilizaremos códigos QR y acortadores de direcciones.
- Dejaremos la teoría para la casa y veremos los temas practicos

Etapas de un análisis forense

Evaluar → **Adquirir** → **Analizar** → **Informe**

* Notificar y obtener la autorización
* Revisar las políticas y la legislación
* Identificar a los miembros del equipo
* Realizar una evaluación
* Prepararse para la adquisición de pruebas

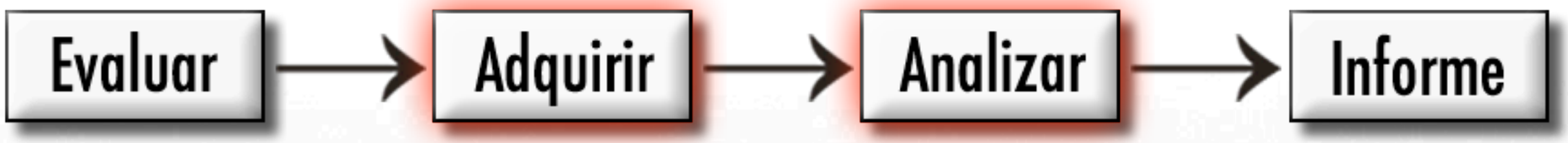
* Construcción de la investigación
* Recopilar los datos
* Almacenar y archivar

* Analizar los datos de la red
* Analizar los datos de host
* Analizar los medios de almacenamiento

* Recopilar y organizar
* Escribir el informe

Preservar y documentar la evidencia

Etapas de un análisis forense



* Notificar y obtener la autorización
* Revisar las políticas y la legislación
* Identificar a los miembros del equipo
* Realizar una evaluación
* Prepararse para la adquisición de pruebas

* Construcción de la investigación
* Recopilar los datos
* Almacenar y archivar

* Analizar los datos de la red
* Analizar los datos de host
* Analizar los medios de almacenamiento

* Recopilar y organizar
* Escribir el informe

Preservar y documentar la evidencia

Etapa de evaluación

goo.gl/fskC2

Etapa de evaluación

- Notificar y obtener autorizaciones

goo.gl/fskC2

Etapa de evaluación

- Notificar y obtener autorizaciones
- Revisar legislación y políticas de cada país

goo.gl/fskC2

Etapa de evaluación

- Notificar y obtener autorizaciones
- Revisar legislación y políticas de cada país
- Identificar los miembros del equipo

goo.gl/fskC2

Etapa de evaluación

- Notificar y obtener autorizaciones
- Revisar legislación y políticas de cada país
- Identificar los miembros del equipo
- Realizar una evaluación previa

goo.gl/fskC2

Etapa de evaluación

- Notificar y obtener autorizaciones
- Revisar legislación y políticas de cada país
- Identificar los miembros del equipo
- Realizar una evaluación previa
- Prepararse para la adquisición de pruebas

goo.gl/fskC2

Etapa de adquisición

goo.gl/NmZAR

Etapa de adquisición

goo.gl/NmZAR

- Construcción de la investigación

Etapa de adquisición

goo.gl/NmZAR

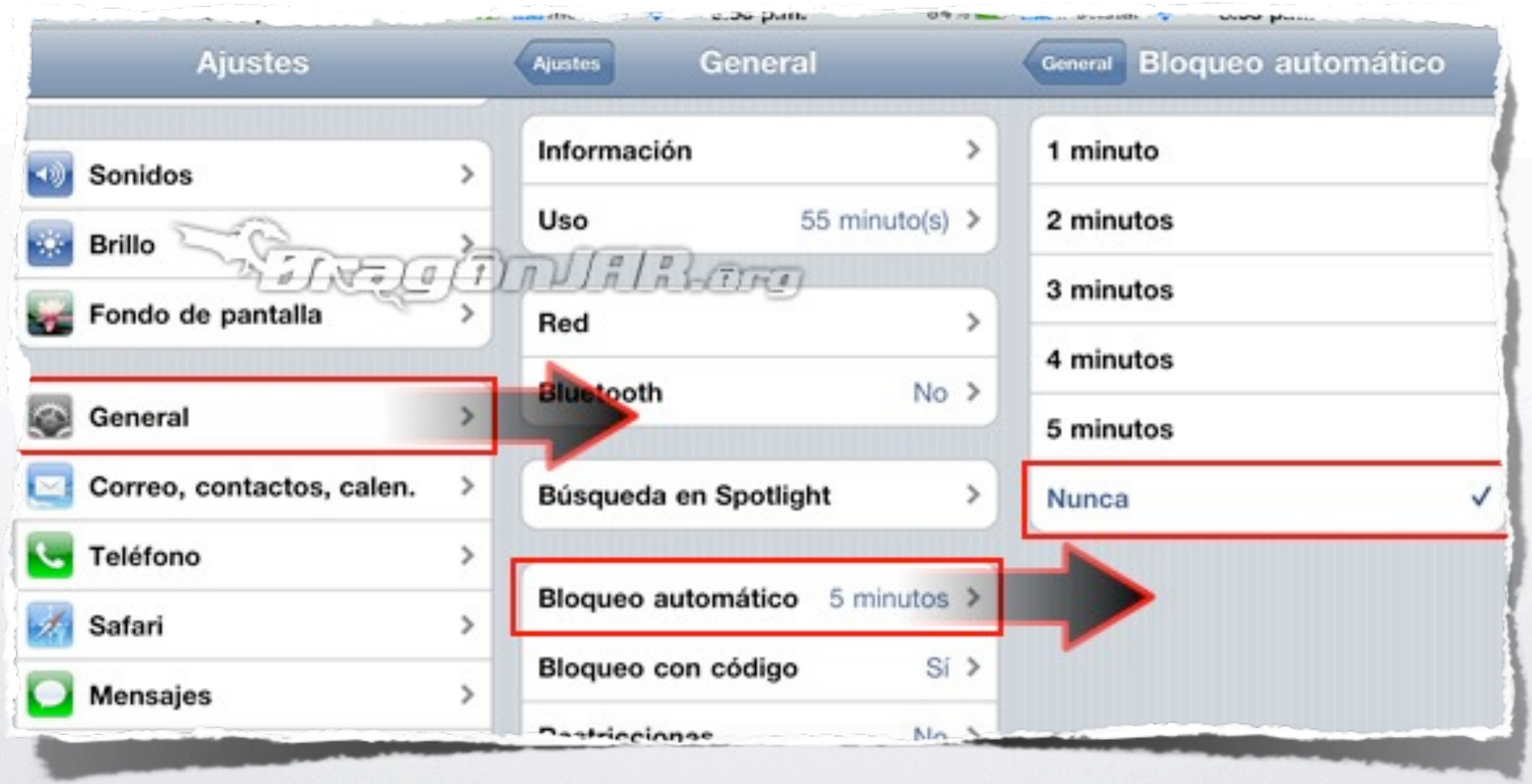
- Construcción de la investigación
- Recopilar los datos

Etapa de adquisición

goo.gl/NmZAR

- Construcción de la investigación
- Recopilar los datos
- Almacenar y archivar

Tareas previas a la adquisición



Tareas previas a la adquisición

Tareas previas a la adquisición

Tareas previas a la adquisición

Tareas previas a la adquisición


Lifemax

Adquisición con las uñas

Método

Adquisición con las uñas

- Que el dispositivo iOS tenga Jailbreak.

Método

Adquisición con las uñas

- Que el dispositivo iOS tenga Jailbreak.
- Servidor SSH y netcat o que permita instalarlos.

Método

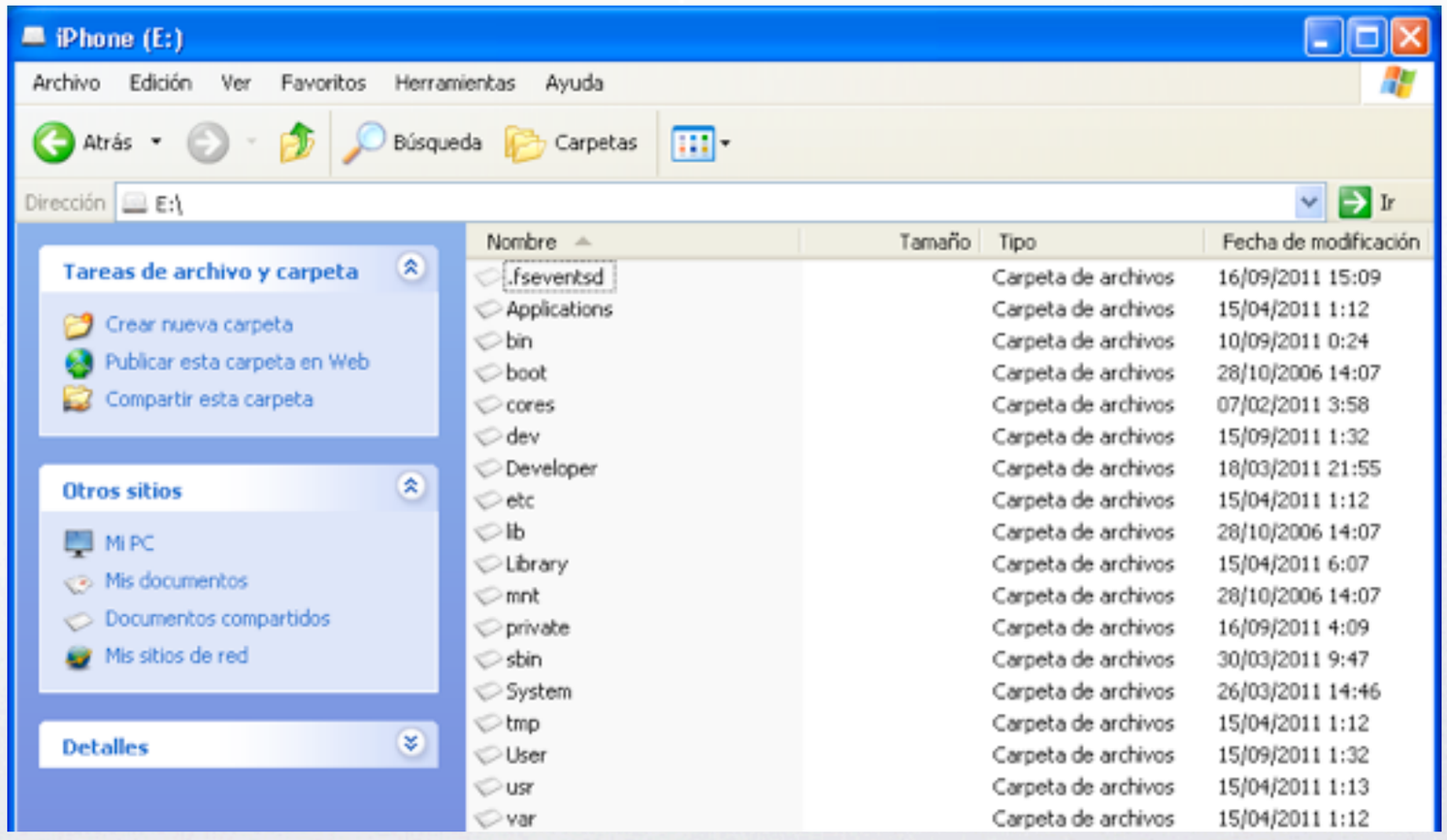
Adquisición con las uñas

- Que el dispositivo iOS tenga Jailbreak.
- Servidor SSH y netcat o que permita instalarlos.
- Servidor SSH con clave por defecto “alpine” o una clave débil.

Método

Adquisición con las uñas

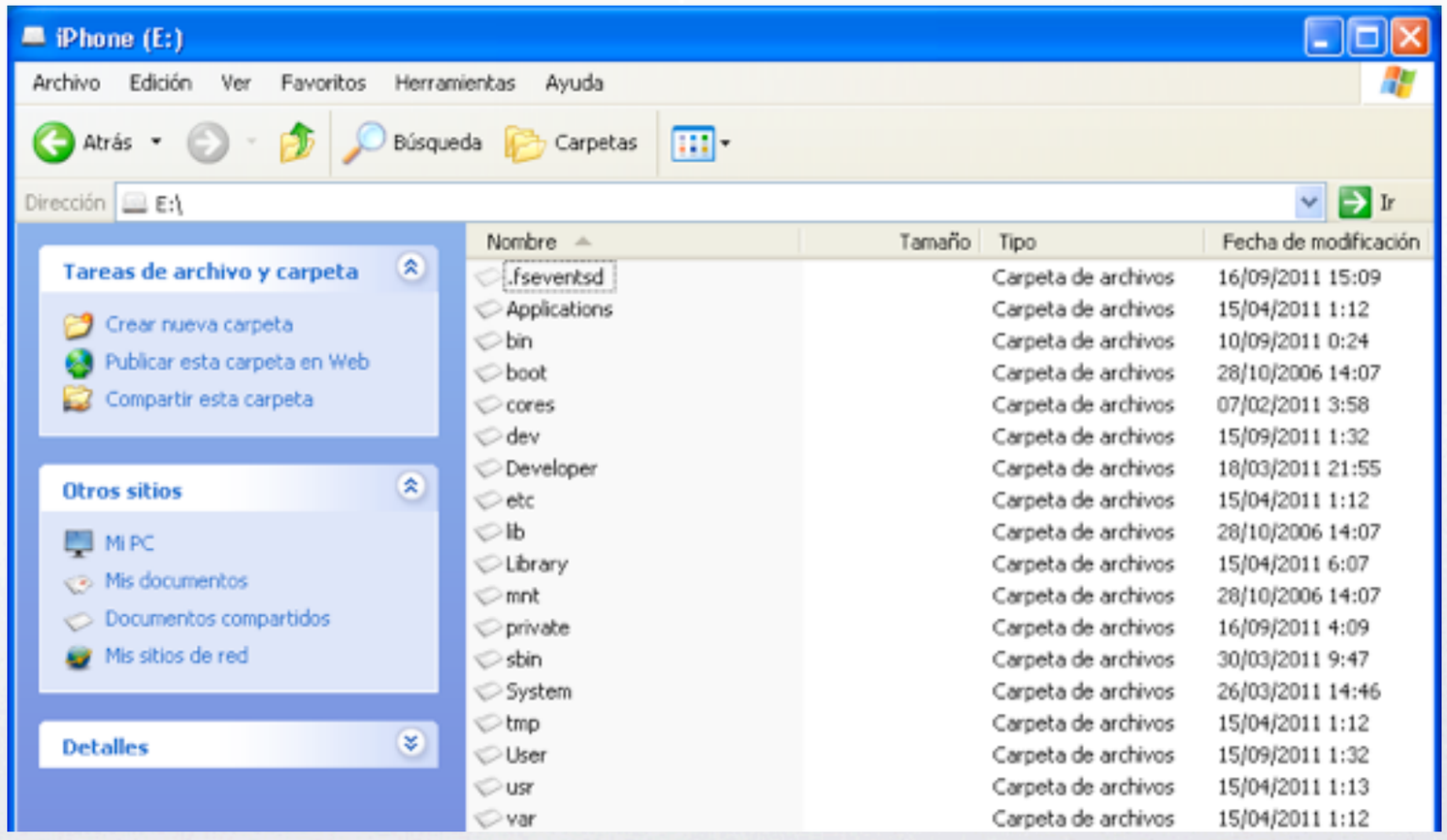
Método



Adquisición con las uñas

Método 

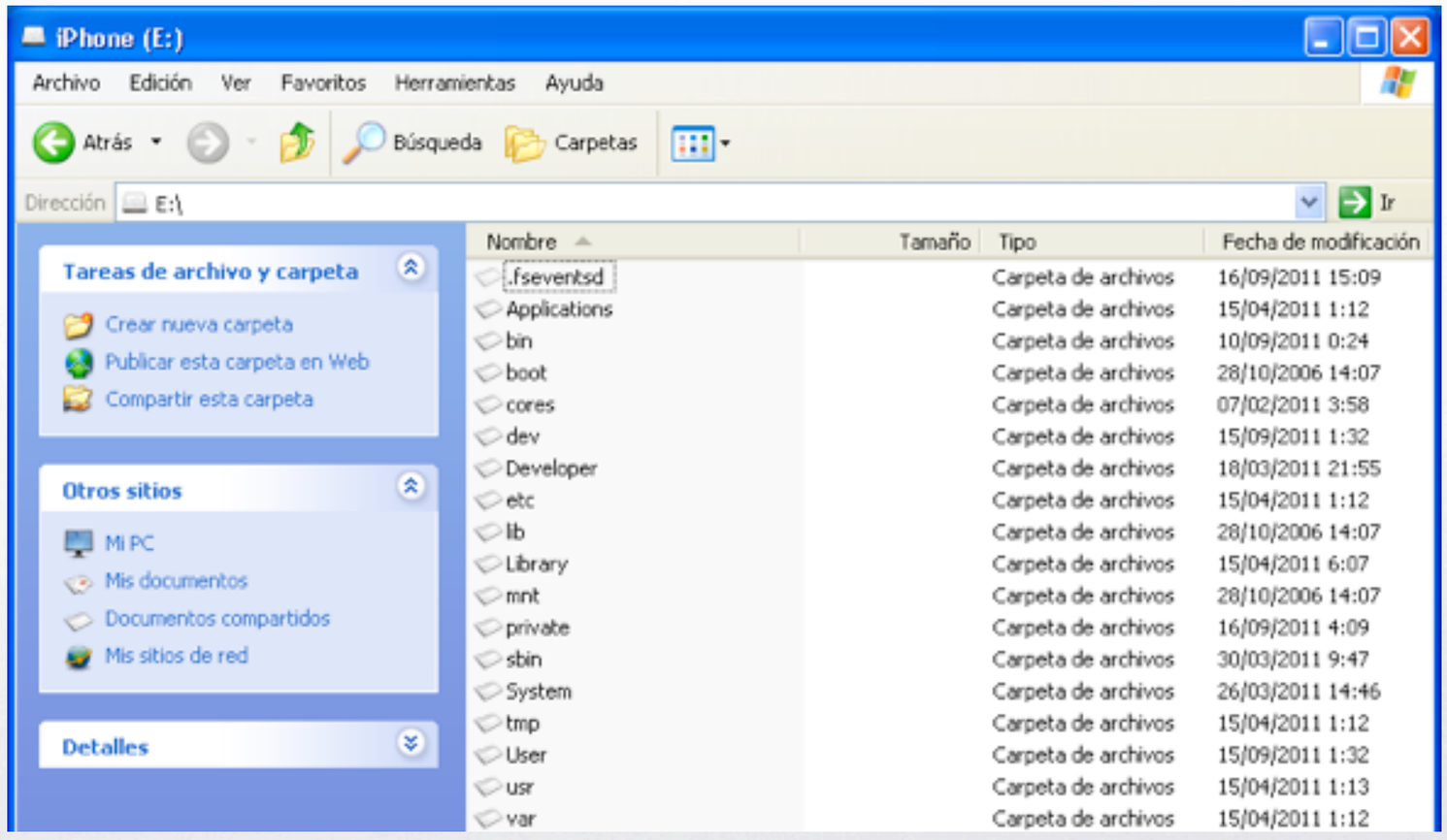
- Obtener el PhoneDisk



Adquisición con las uñas

Método

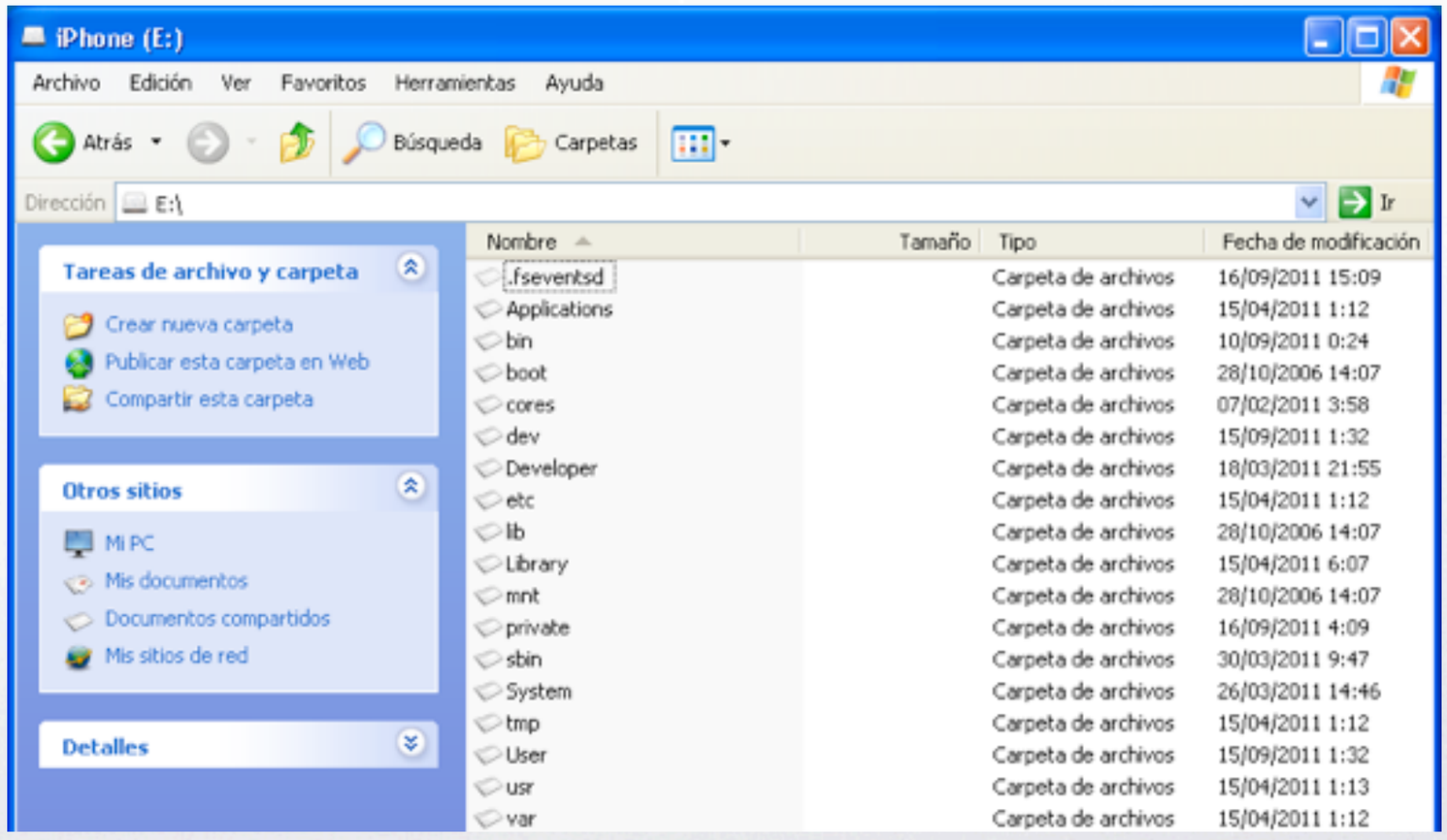
- Obtener el PhoneDisk
- Que el dispositivo iOS tenga Jailbreak.



Adquisición con las uñas

Método

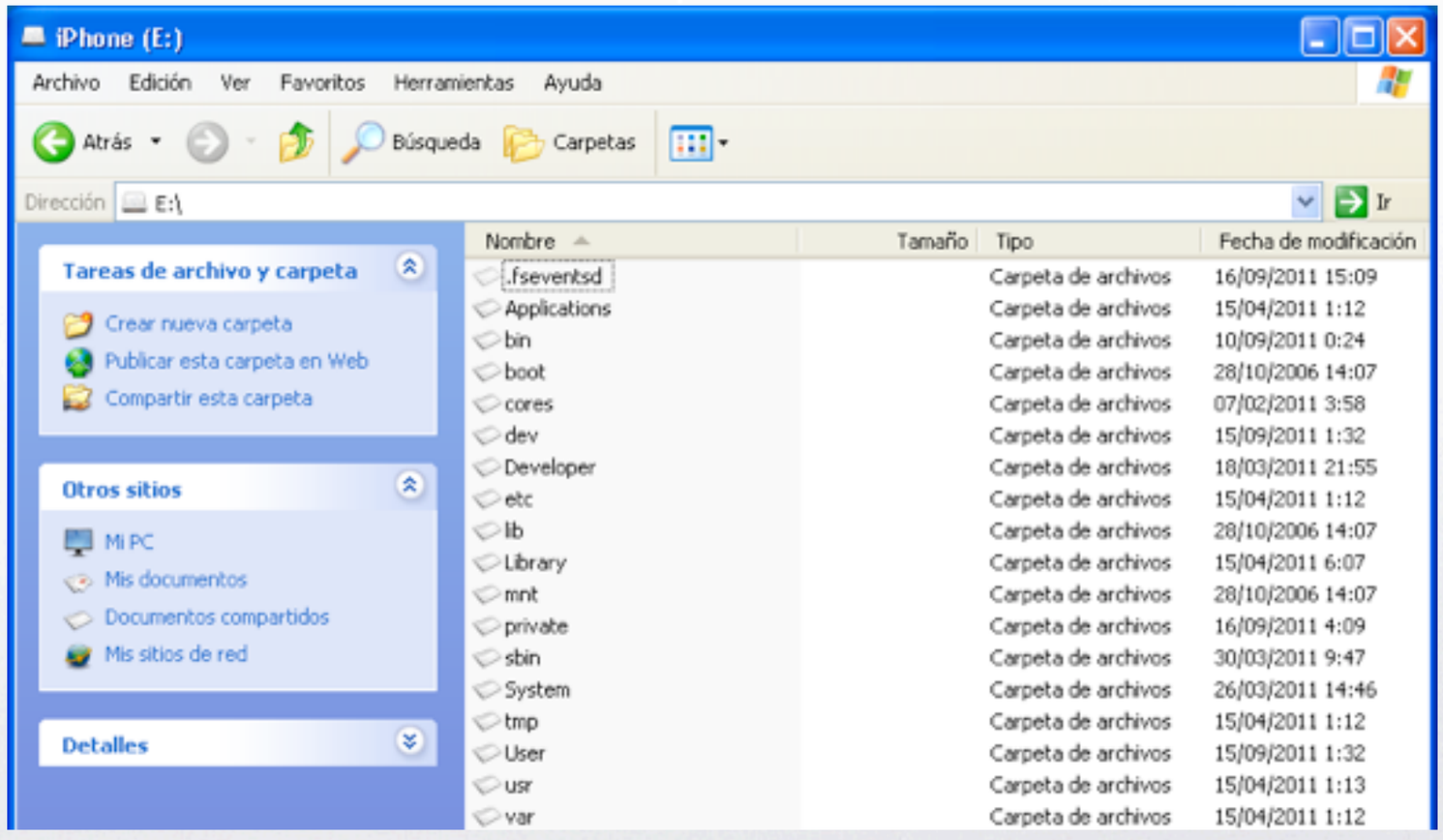
- Obtener el PhoneDisk
- Que el dispositivo iOS tenga Jailbreak.
- Que tenga instalado el componente afc2add.



Adquisición con las uñas

Método

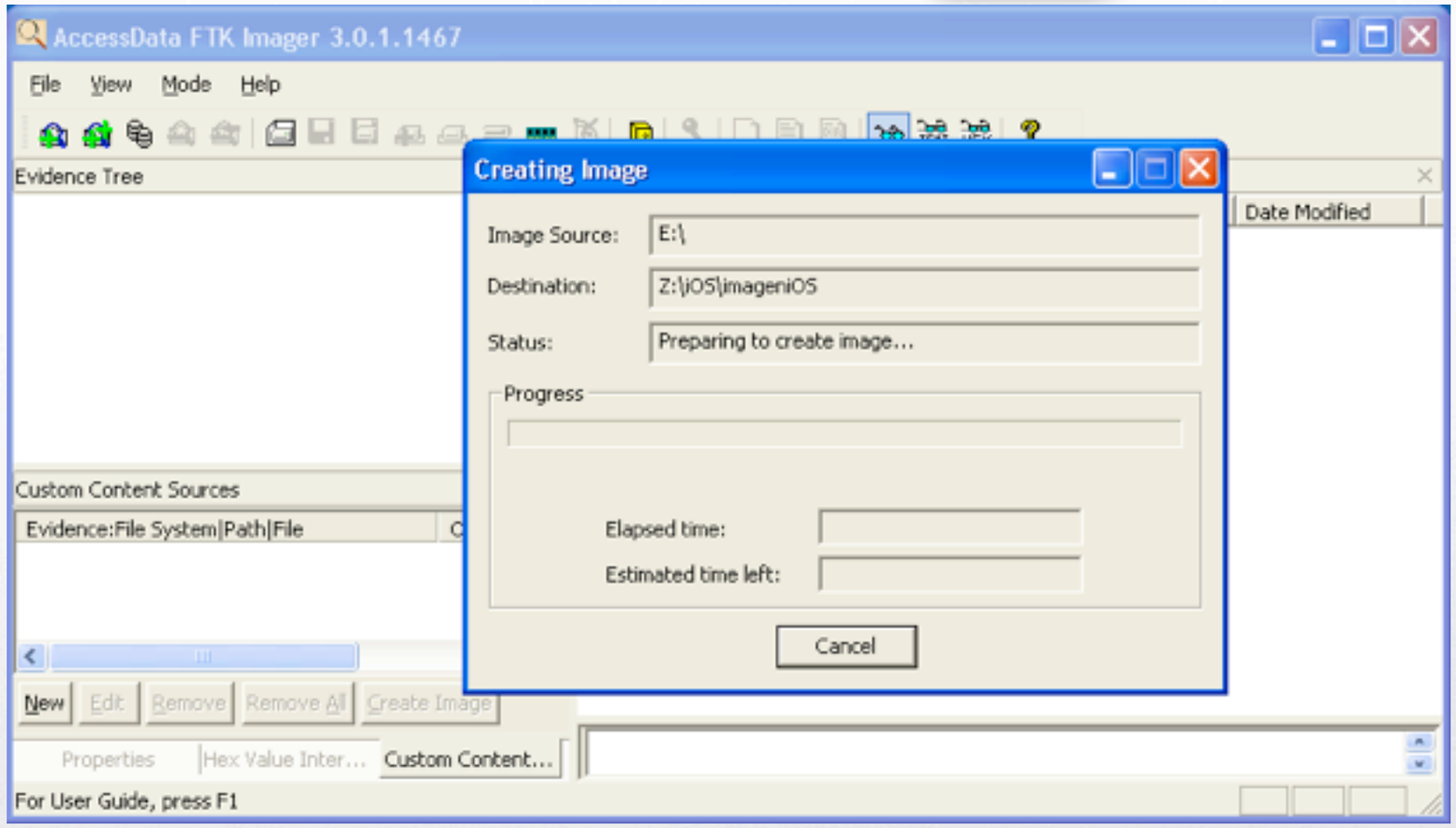
- Obtener el PhoneDisk
- Que el dispositivo iOS tenga Jailbreak.
- Que tenga instalado el componente afc2add.
- Usar cualquier herramienta forense para adquirir la imagen.



Adquisición con las uñas

Método

- Obtener el PhoneDisk
- Que el dispositivo iOS tenga Jailbreak.
- Que tenga instalado el componente afc2add.
- Usar cualquier herramienta forense para adquirir la imagen.



Adquisición con Kits

Cellebrite UFED

Adquisición con Kits

Cellebrite UFED

Tener $3,999USD

Etapa de análisis

goo.gl/Y2pgU

Etapa de análisis

- Analizar los datos de la red

goo.gl/Y2pgU

Etapa de análisis

- Analizar los datos de la red
- Analizar los datos del dispositivo

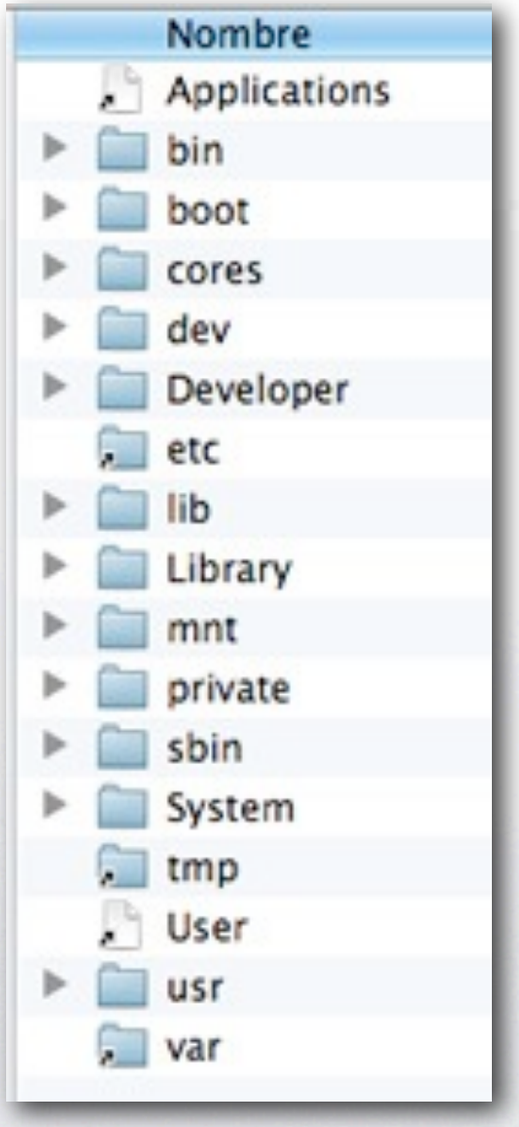
goo.gl/Y2pgU

Etapa de análisis

goo.gl/Y2pgU

- Analizar los datos de la red
- Analizar los datos del dispositivo
- Analizar los medios de almacenamiento

Estructura de un sistema iOS



Applications: Es un enlace simbólico a -> /var/stash/Applications.pwn
Developer: Esta vacío
Library: Como en cualquier sistema Mac OS X, plugins, configuraciones, etc..
System: Contiene las preferencias del sistema y del dispositivo
User: Es un enlace simbólico a -> /var/mobile
bin: Contiene los ejecutables del sistema
boot: Esta vacío
cores: Esta vacío
dev: Esta vacío
etc: Es un enlace simbólico a -> private/etc/
lib: Esta vacío
mnt: Esta vacío
private: Contiene los directories etc y var (fstab, passwd y muchos mas)
sbin: Contiene los ejecutables del sistema
tmp: Es un enlace simbólico a -> private/var/tmp/
usr: Contiene los datos de zona horaria y ejecutables del sistema
var: Es un enlace simbólico a -> private/var/


DragonJAR.org
CON LAS UÑAS


CON LAS UÑAS


UTILIZANDO KITS

Análisis con las uñas - Herramientas

Análisis con las uñas - Herramientas

- Imagen de iOS adquirida

Análisis con las uñas - Herramientas

- Imagen de iOS adquirida
- Cliente SQLite (puede ser SQLitebrowser SQLiteman SQLite Manager) o cualquier otro

Análisis con las uñas - Herramientas

- Imagen de iOS adquirida
- Cliente SQLite (puede ser SQLitebrowser SQLiteman SQLite Manager) o cualquier otro
- Lector de archivos .plist (XCode, plistviewer, plist editor)

Análisis con las uñas - Herramientas

- Imagen de iOS adquirida
- Cliente SQLite (puede ser SQLitebrowser SQLiteman SQLite Manager) o cualquier otro
- Lector de archivos .plist (XCode, plistviewer, plist editor)
- plutil.pl para parsear un .plist si nos lo encontramos binario

Análisis con las uñas - Herramientas

- Imagen de iOS adquirida
- Cliente SQLite (puede ser SQLitebrowser SQLiteman SQLite Manager) o cualquier otro
- Lector de archivos .plist (XCode, plistviewer, plist editor)
- plutil.pl para parsear un .plist si nos lo encontramos binario
- Software para recuperado de archivos

Análisis con las uñas - Herramientas

- Imagen de iOS adquirida
- Cliente SQLite (puede ser SQLitebrowser SQLiteman SQLite Manager) o cualquier otro
- Lector de archivos .plist (XCode, plistviewer, plist editor)
- plutil.pl para parsear un .plist si nos lo encontramos binario
- Software para recuperado de archivos
- Editor hexadecimal

Análisis con las uñas - Contactos

/private/var/mobile/Library/AddressBook una de las carpetas mas importantes, ya que en ella se encuentran los archivos AddressBookImages.sqlitedb donde están almacenadas las imágenes asociadas a los contactos y AddressBook.sqlitedb que hacen referencia a nuestra libreta de contactos

Análisis con las uñas - Llamadas

/private/var/wireless/Library/CallHistory/ en esta carpeta encontraremos el archivo **call_history.db** donde esta el listado de las ultimas 100 llamadas realizadas desde el dispositivo.

Análisis con las uñas - Mails

/private/var/mobile/Library/Mail encontraremos mucha información sobre los correos recibidos desde el dispositivo, las cuentas de correo, los tiempos de actualización, archivos adjuntos y mensajes de correo electrónico.

Análisis con las uñas - Media

/private/var/mobile/Media/DCIM/100APPLE y **/private/var/mobile/Media/PhotoData** fotos y vídeos grabados con el dispositivo iOS, recuerda que por defecto las fotos tomadas con un dispositivo iOS incluye la posición GPS del lugar donde fue tomada en sus meta-datos, por lo que puede ser de mucha utilidad.

Análisis con las uñas - SMS's

/private/var/mobile/Library/SMS la siguiente base de datos que nos llama la atención, es la de los mensajes SMS, en ella podremos encontrar el archivo **sms.db** y la carpeta **Drafts** con los borradores que estén guardados en el dispositivo iOS.

Análisis con las uñas - Notas

/private/var/mobile/Library/Notes la información ingresada en la aplicación notas incorporada en todas las versiones del sistema iOS de Apple

Análisis con las uñas - Calendario

/private/var/mobile/Library/Calendar aquí encontraremos el **Calendar.sqlitedb** que contiene toda la información sobre los calendarios del dispositivos, alarmas y fechas lo que nos puede ser muy útil en nuestra investigación forense

Análisis con las uñas - Internet

/private/var/mobile/Library/Safari encontramos los favoritos del safari **Bookmarks.db**, el historial **History.plist** y los buscadores usados **SearchEngines.plist** ademas del archivo **SuspendState.plist** que almacena las "pestañas" o paginas suspendidas de Safari

/private/var/mobile/Library/Preferences/com.apple.mobilesafari.plist ultimas búsquedas en safari

Análisis con las uñas - Spotlight

/private/var/mobile/Library/Spotlight aquí encontraremos un listado con las aplicaciones abiertas por medio del buscador spotlight **db.sqlitedb** y los mensajes que están indexados por este buscador **SMSSearchdb.sqlitedb**

Análisis con las uñas - Mapas

/private/var/mobile/Library/Maps encontraremos los archivos **History.plist** y **Directions.plist** con la información que tengamos almacenada en la aplicación mapas, del dispositivo iOS

Análisis con las uñas - Voz

/private/var/mobile/Media/Recordings encontraremos las notas de voz y una base de datos **Recordings.db** con con toda su información y las etiquetas personalizadas de la nota (si la tiene) **CustomLabels.plist**

/private/var/mobile/Library/Voicemail aquí encontraras los correos de voz que se encuentren en el dispositivo

Análisis con las uñas - Preferencias

/private/var/mobile/Library/Preferences

com.apple.Maps.plist: ultimas búsquedas en el programa de mapas
com.apple.mobiletimer.plist y com.apple.mobilecal.alarmengine.plist: información sobre las alarmas puestas en el reloj
com.apple.mobilephone.speeddial.plist: números de llamada rápida
com.apple.youtube.plist: últimos vídeos buscados en la aplicación de youtube
com.apple.preferences.datetime.plist zona horaria del dispositivo
com.apple.springboard.plist lista de aplicaciones estándar y añadidas por el usuario
com.apple.stocks.plist el stock de acciones listadas en la aplicación bolsa
com.apple.weather.plist listado de ciudades añadidas a la aplicación de clima

Análisis con las uñas - SpringBoard

/private/var/mobile/Library/SpringBoard aquí encontraremos las aplicaciones instaladas **applicationstate.plist** la organización de estas aplicaciones dentro del equipo **IconState.plist** y una miniatura del fondo utilizado **LockBackgroundThumbnail.jpg**

Análisis con las uñas - Passwords

/private/etc/master.passwd y **/private/etc/passwd** utilizando john the ripper o cualquier otra herramienta para crackear passwords, podremos obtener las claves del sistema

En la carpeta **/private/var/Keychains/** encontraremos los archivos TrustStore.sqlite3, **keychain-2.db**, ocspcache.sqlite3 donde encontraremos en texto plano algunas de las contraseñas usadas por las aplicaciones instaladas

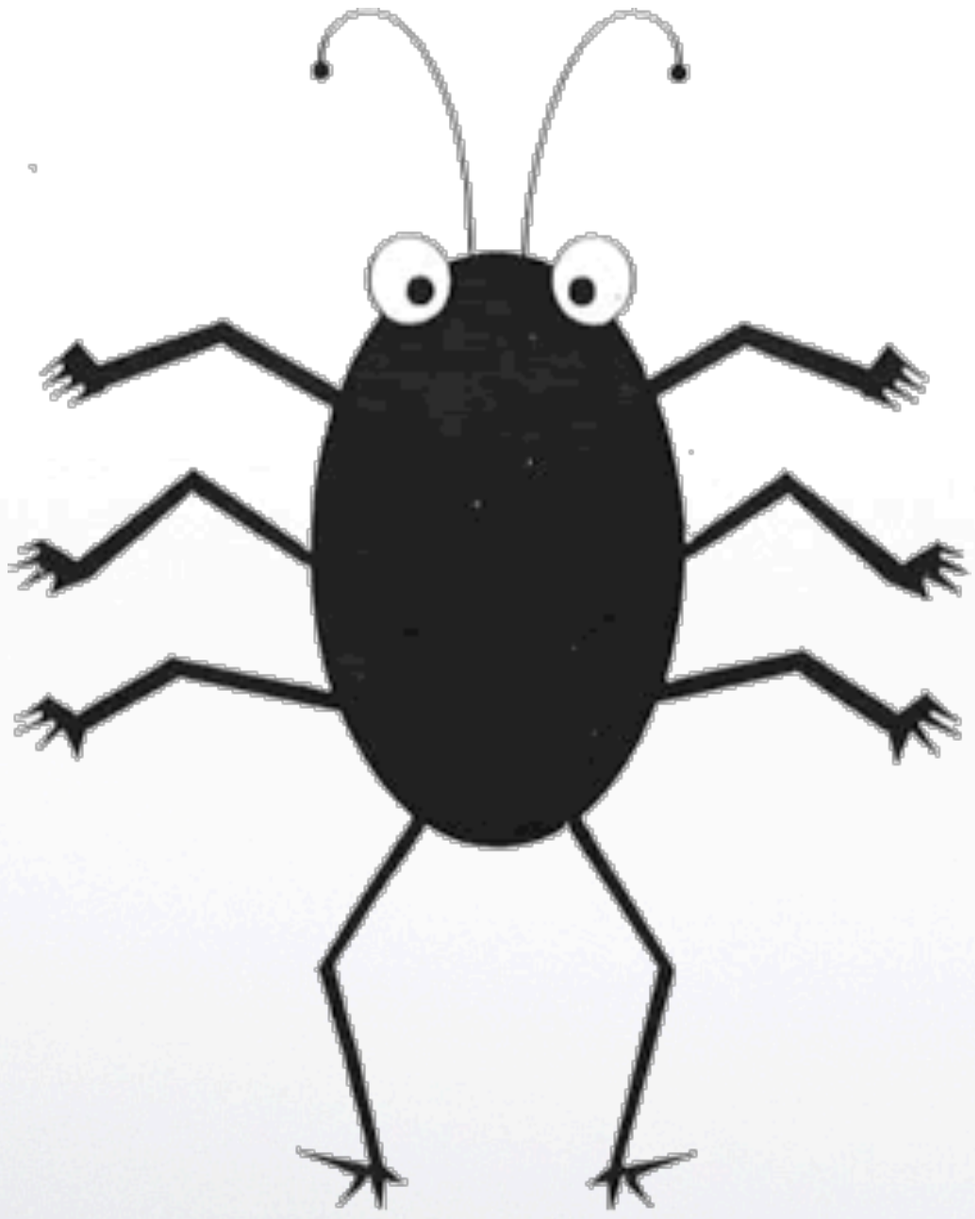
/private/var/root/Library/Lockdown/ en esta carpeta encontraras los certificados públicos y privados del dispositivo

Análisis con las uñas - Logs

/private/var/logs/ y **/private/var/log/**en estas carpetas encontraremos una gran cantidad de logs del sistema iOS que nos pueden ayudar en la elaboración de nuestra linea de tiempo.

/var/wireless/Library/Logs logs sobre las conexiones inalámbricas (3G, Bluetooht, WiFi) del dispositivo

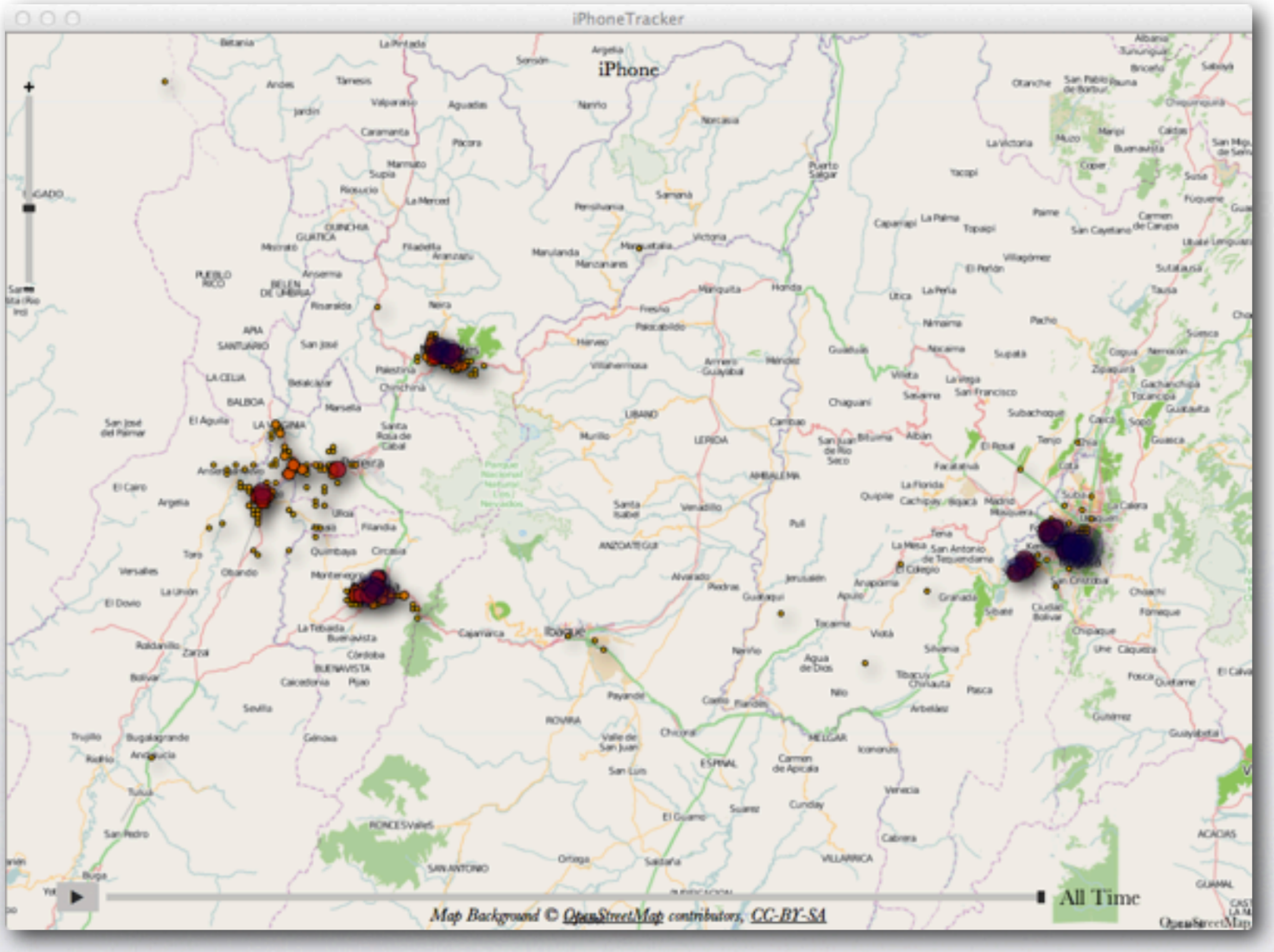
/private/var/mobile/Library/Logs Esta carpeta de logs es bastante interesante, por que nos muestra los errores de las aplicaciones instaladas en el equipo, podremos sacar buena información de todos estos archivos



BUG

FUNCIONALIDAD

consolidate.db



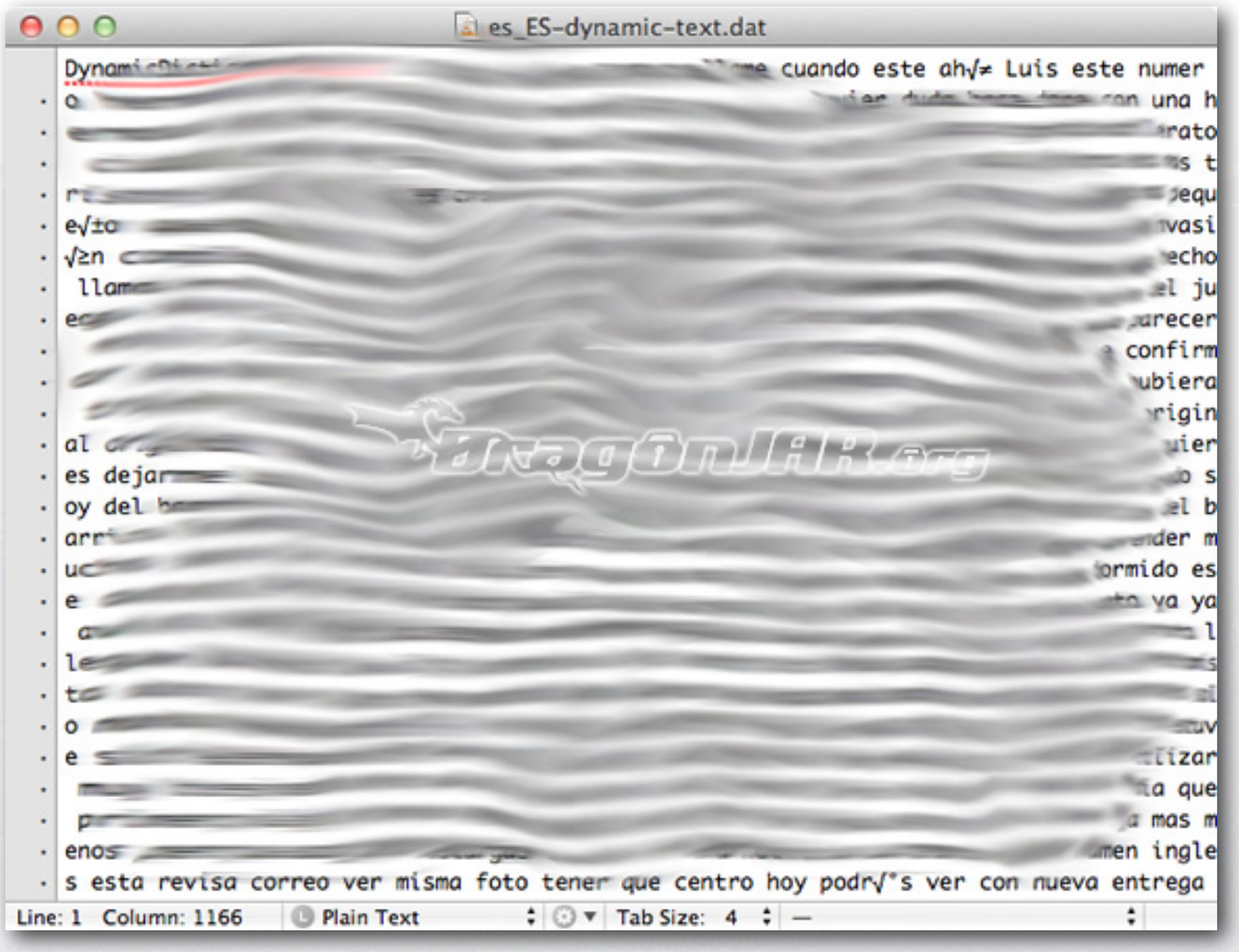
/private/var/root/Library/Caches/locationd/consolidate.db

archivo que contiene las ultimas ubicaciones donde estuvo nuestro dispositivo

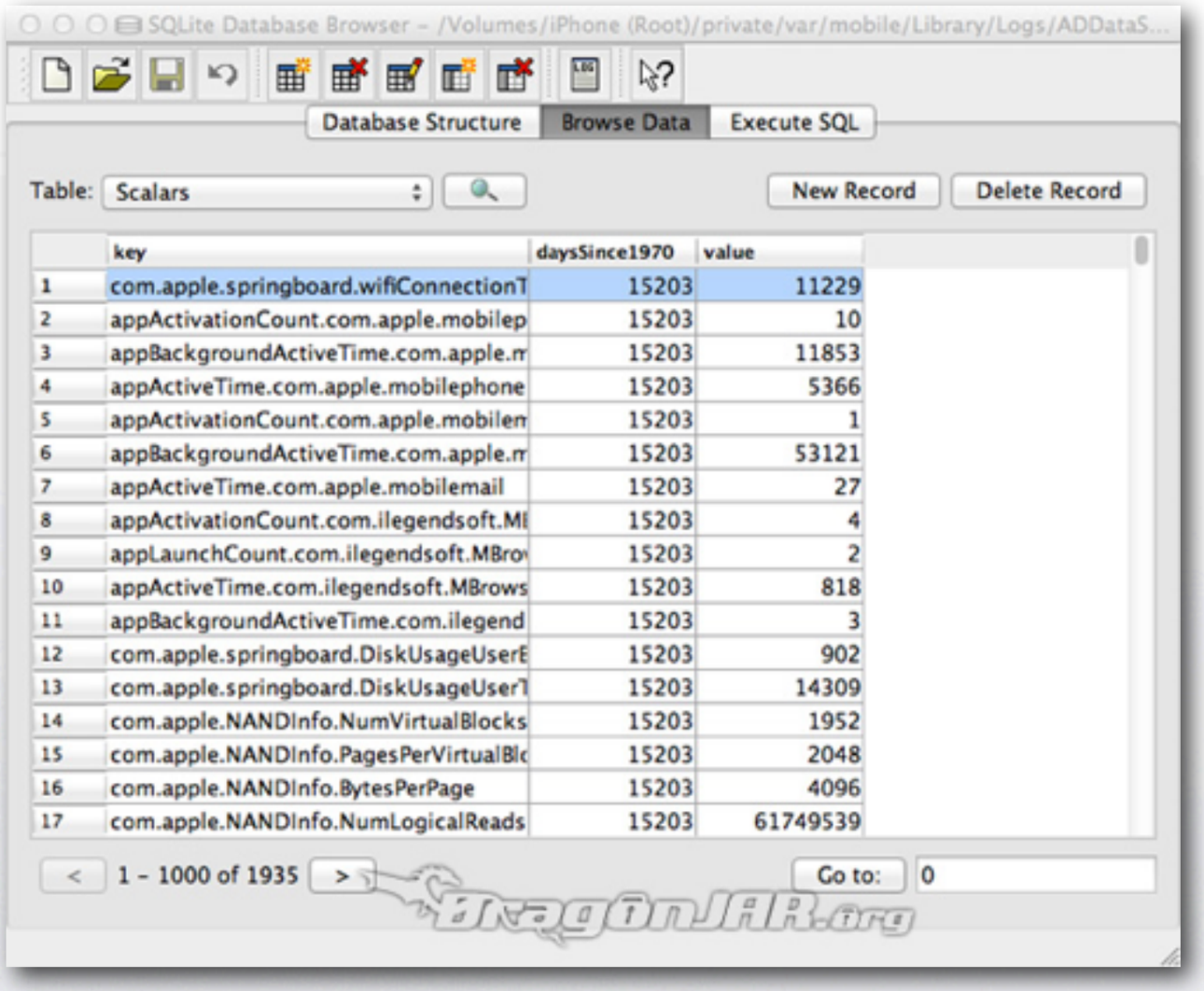
dynamic-text.dat o iKeylogger

/private/var/mobile/Library/Keyboard/(idioma)-dynamic-text.dat

Diccionario personalizado que almacena las palabras que escribimos en el dispositivo iOS añadir al diccionario las palabras que mas usas



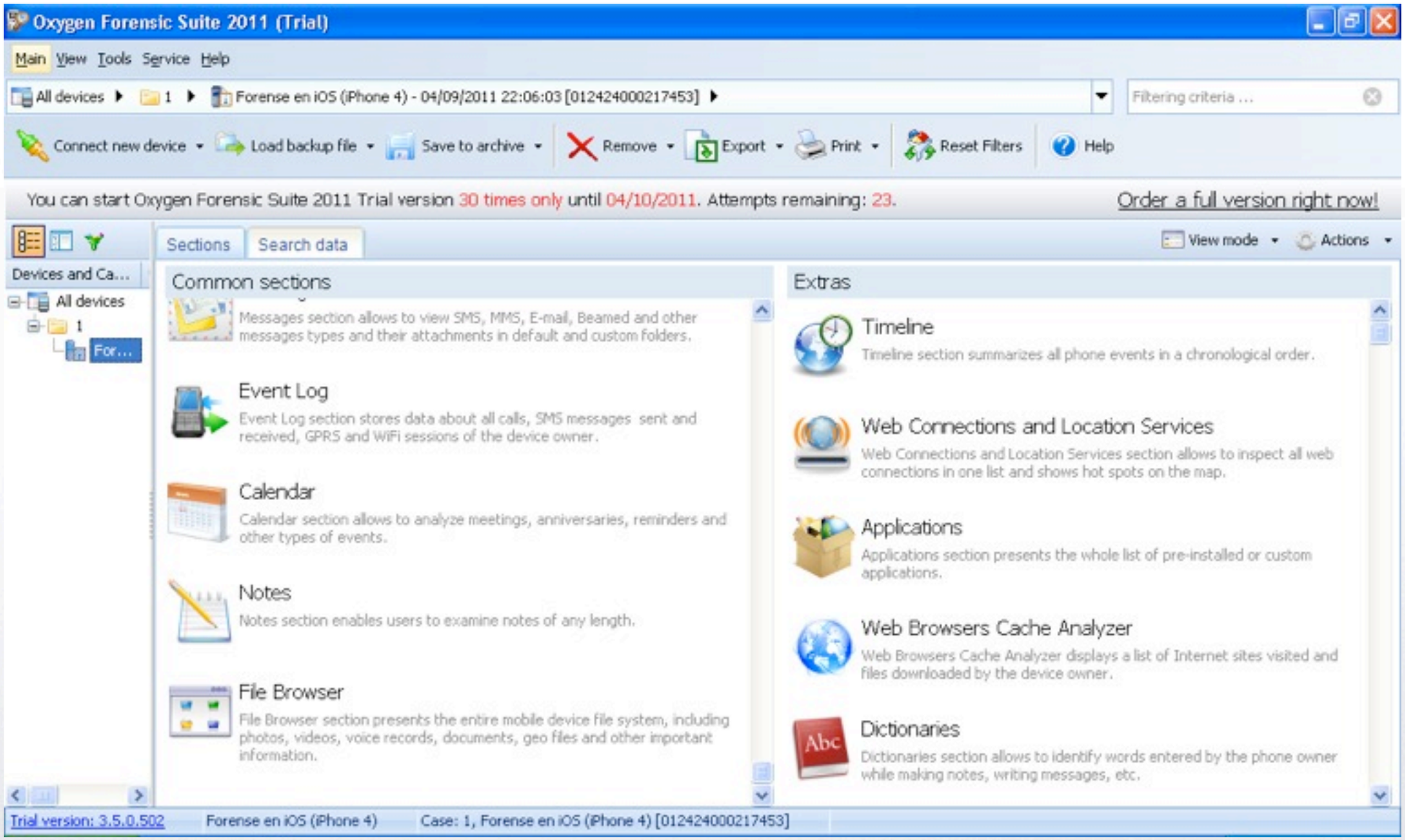
ADDataStore.sqlitedb



/private/var/mobile/Library/Logs/ADDataStore.sqlitedb

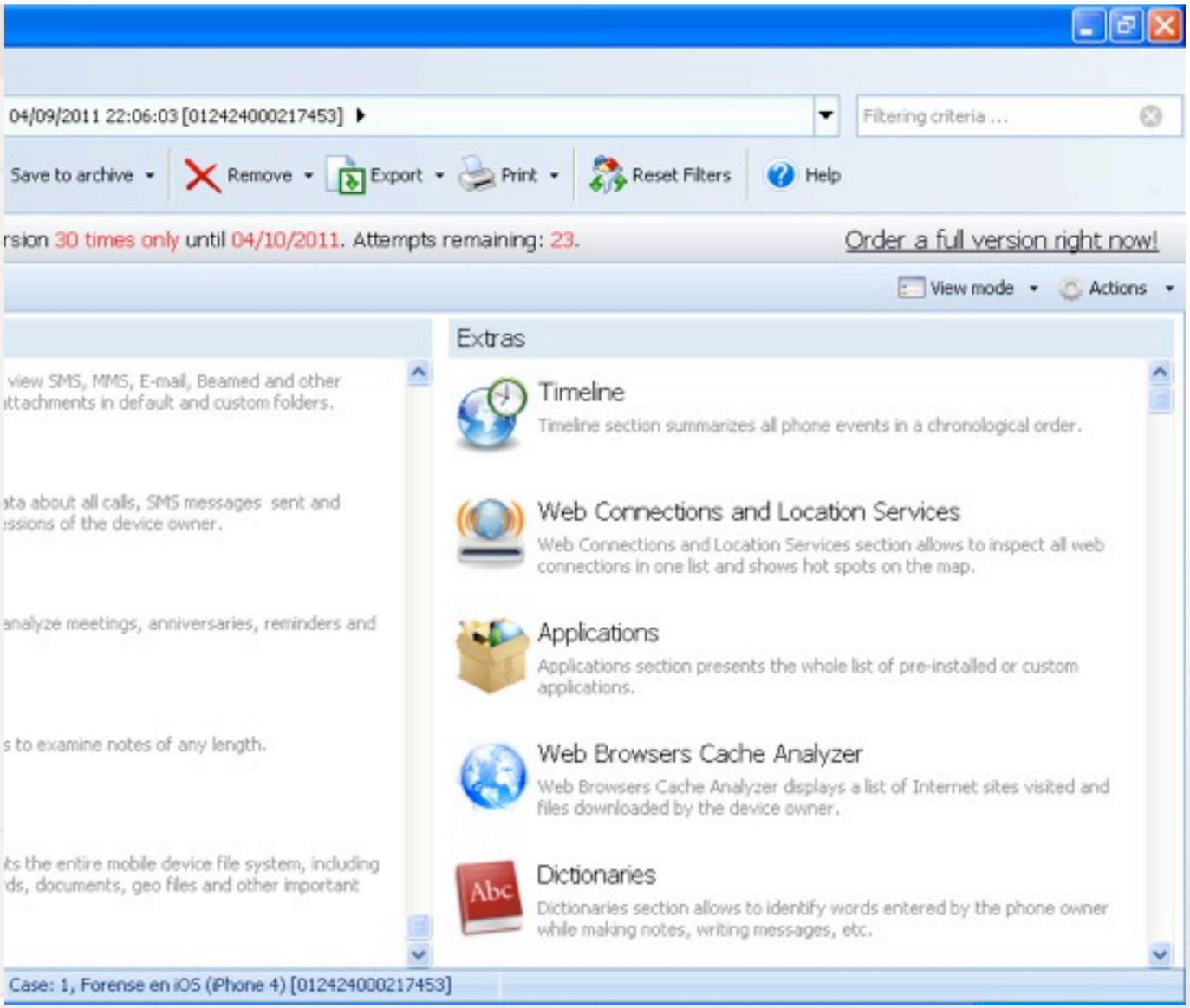
historial de las aplicaciones abiertas y el tiempo que fué utilizada

Análisis con Software Comercial

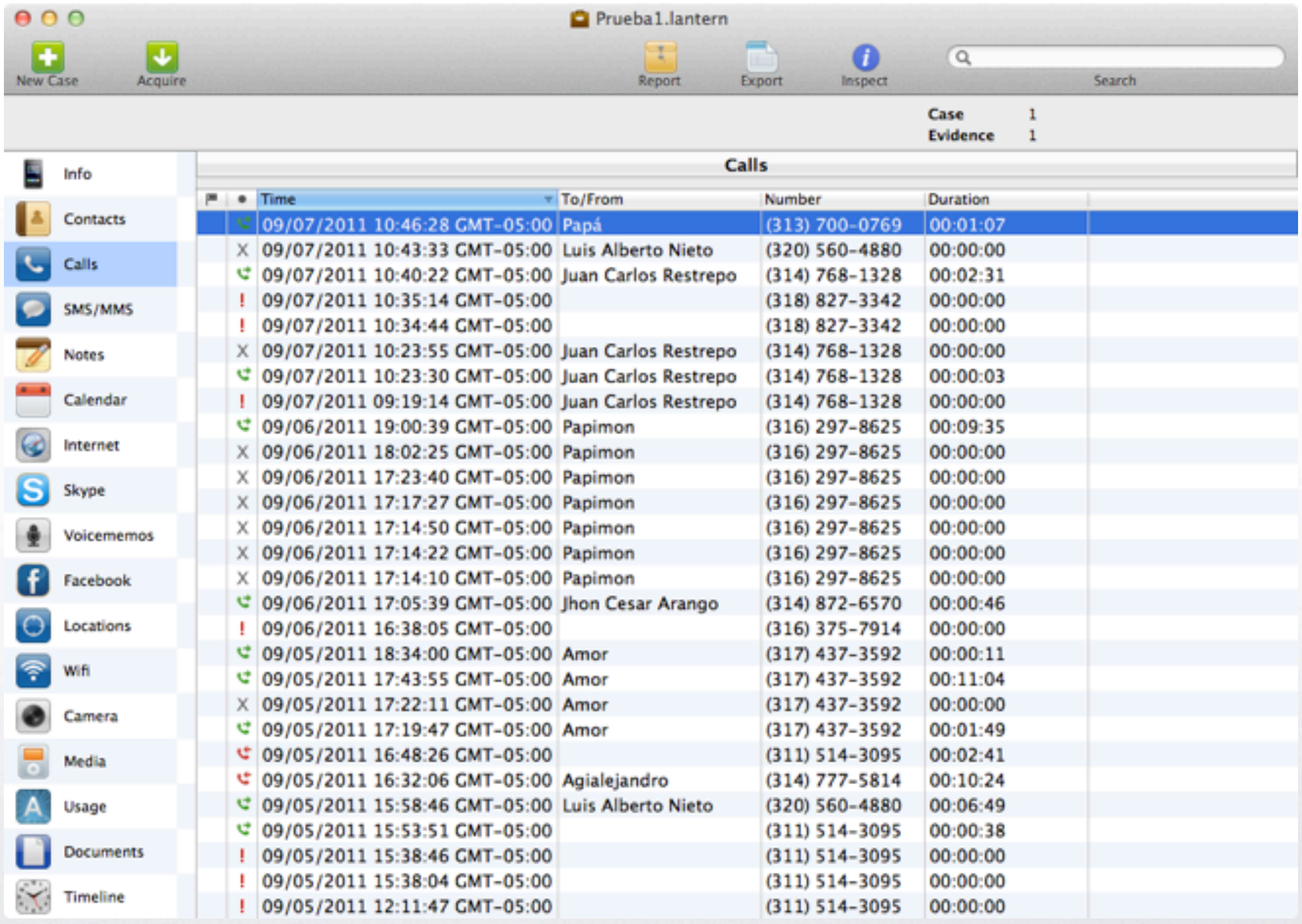


Análisis con Software Comercial

License [1] [Compare]	Price [2]
Oxygen Forensics for iPhone License includes 12 months of updates and iPhone password-protected backup reader add-on.	$ 599 (€ 399)
Oxygen Forensic Suite 2011 License includes 12 months of updates.	$ 799 (€ 499)
Oxygen Forensic Suite 2011 PRO License includes: • All functionality of **Standard** version • Geo event positioning Add-On • Web browsers cache analyzer Add-On • iPhone password-protected backup reader Add-On • Skype analyzer • Web Connections and Location Services • Dictionaries • DMG Backup Reader • 12 months of free updates	$ 1499 (€ 899)
Oxygen Forensic Suite 2011 Analyst License includes: • All functionality of **PRO** version • SQLite database viewer with deleted data • Plist viewer • Timeline Add-On • Blackberry IPD Backup Reader and Viewer • Applications • Google Mail • Google Maps • Yahoo! Messenger • Nokia PM Viewer • Global search through multiple devices • 12 months of free updates	$ 1999 (€ 1499)
Oxygen Forensic Suite 2011 Analyst With Android Rooting Add-On License includes: • All functionality of **Analyst** version • Android Rooting Add-On • 12 months of free updates	$ 2998 (€ 2498)



Análisis con Software Comercial



Análisis con Software Comercial

Lantern 2.0.4

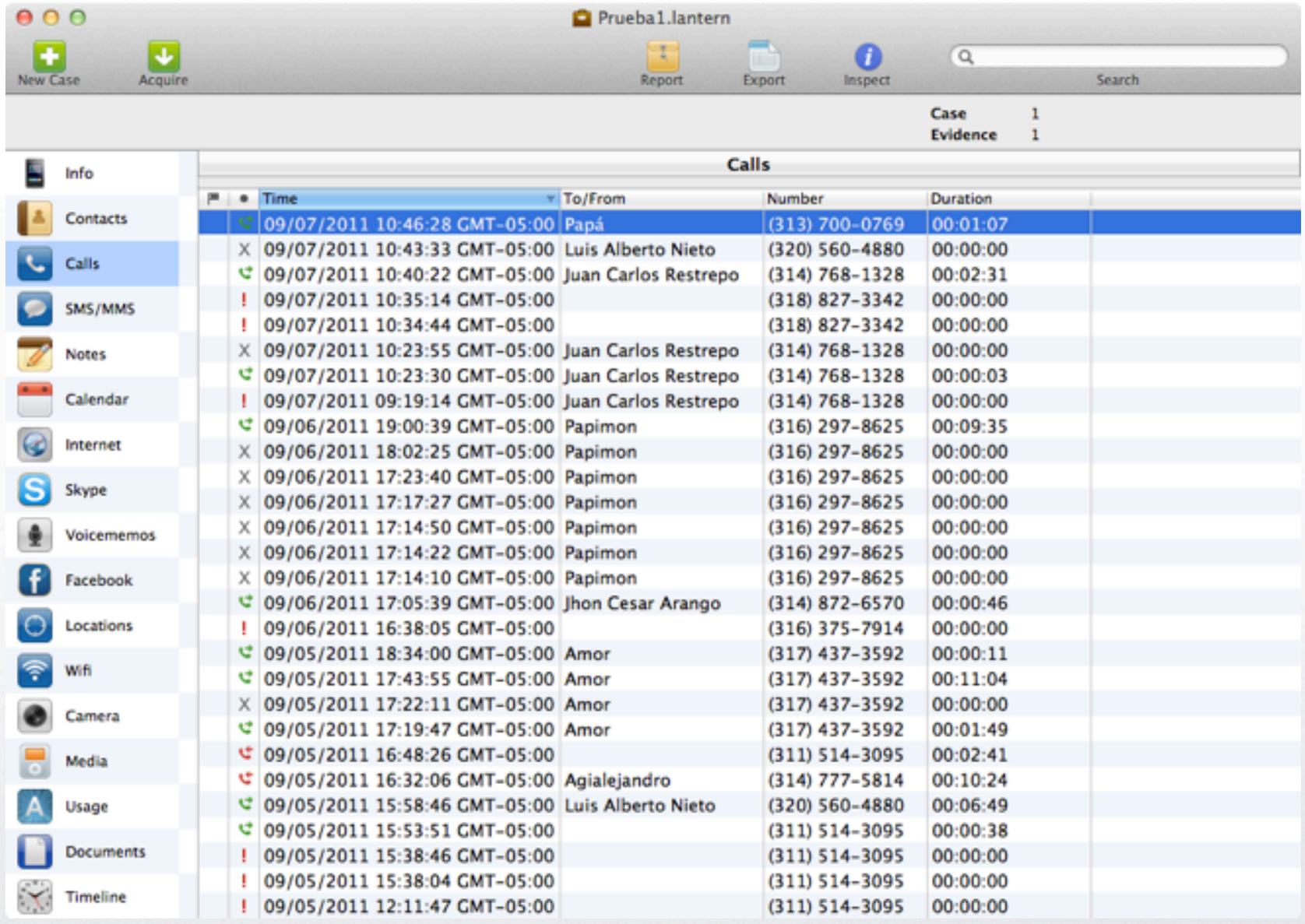
$699,00

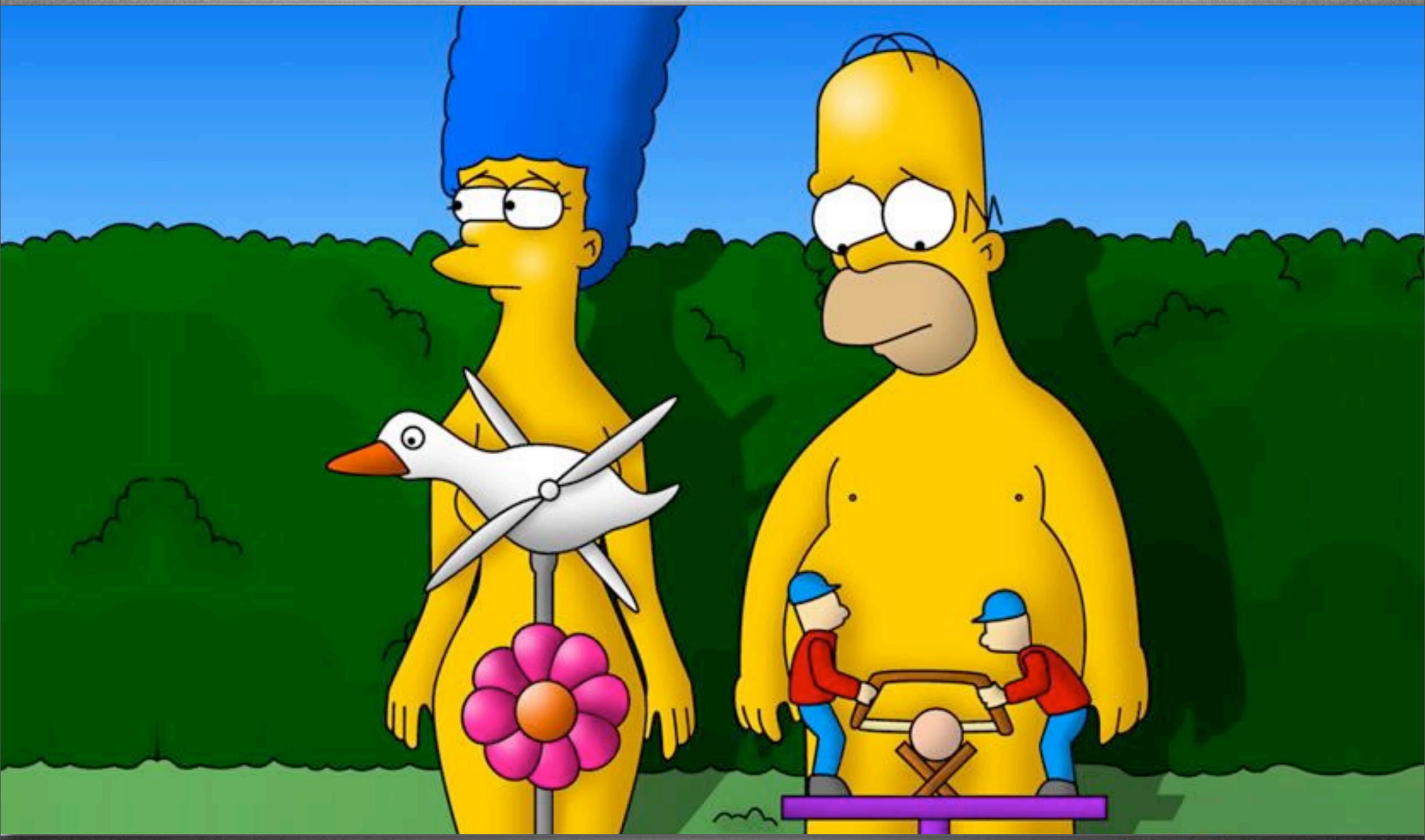
Lantern 2.0 Upgrade

$200,00

Apple Mac Mini and Lantern 2

$1.498,00

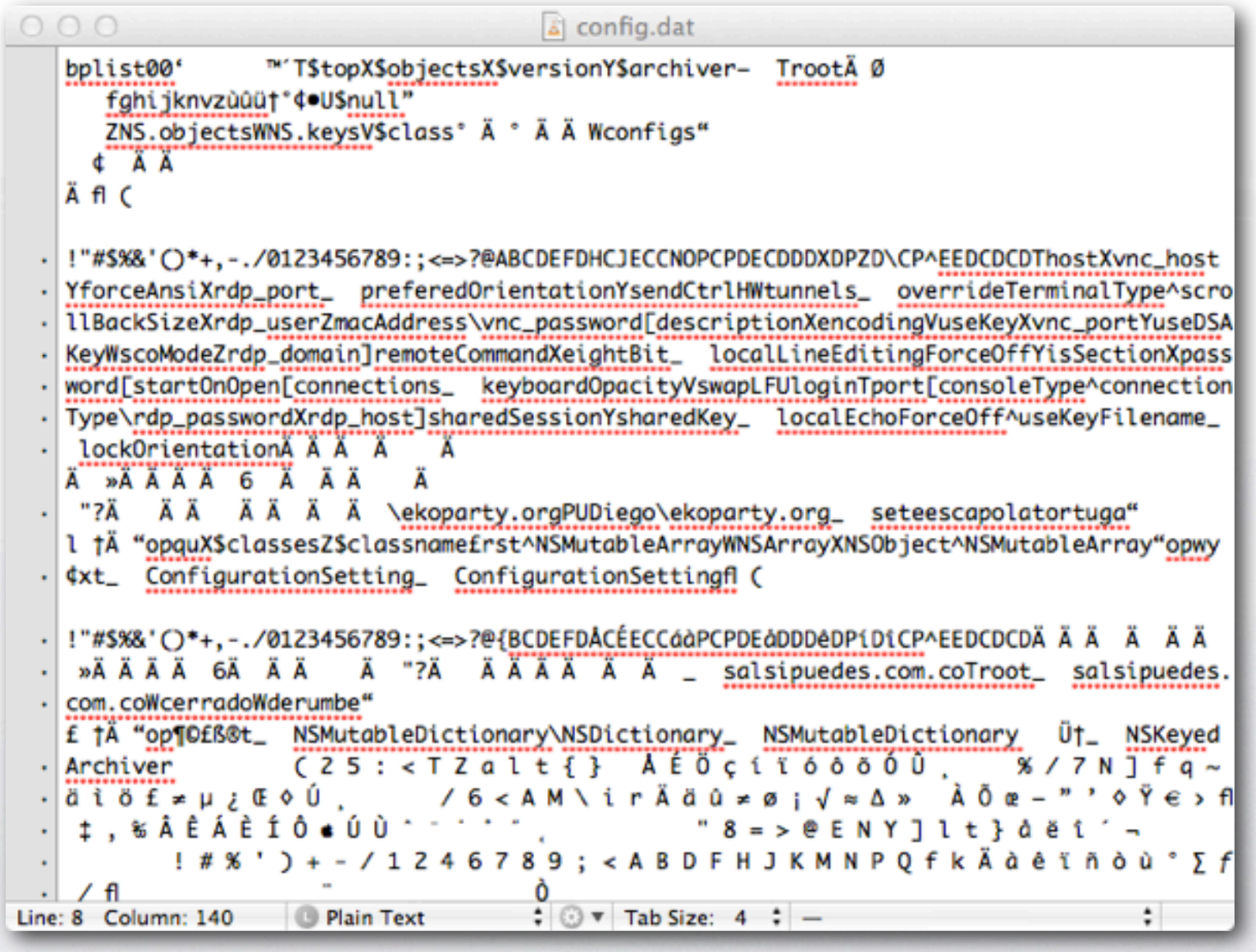




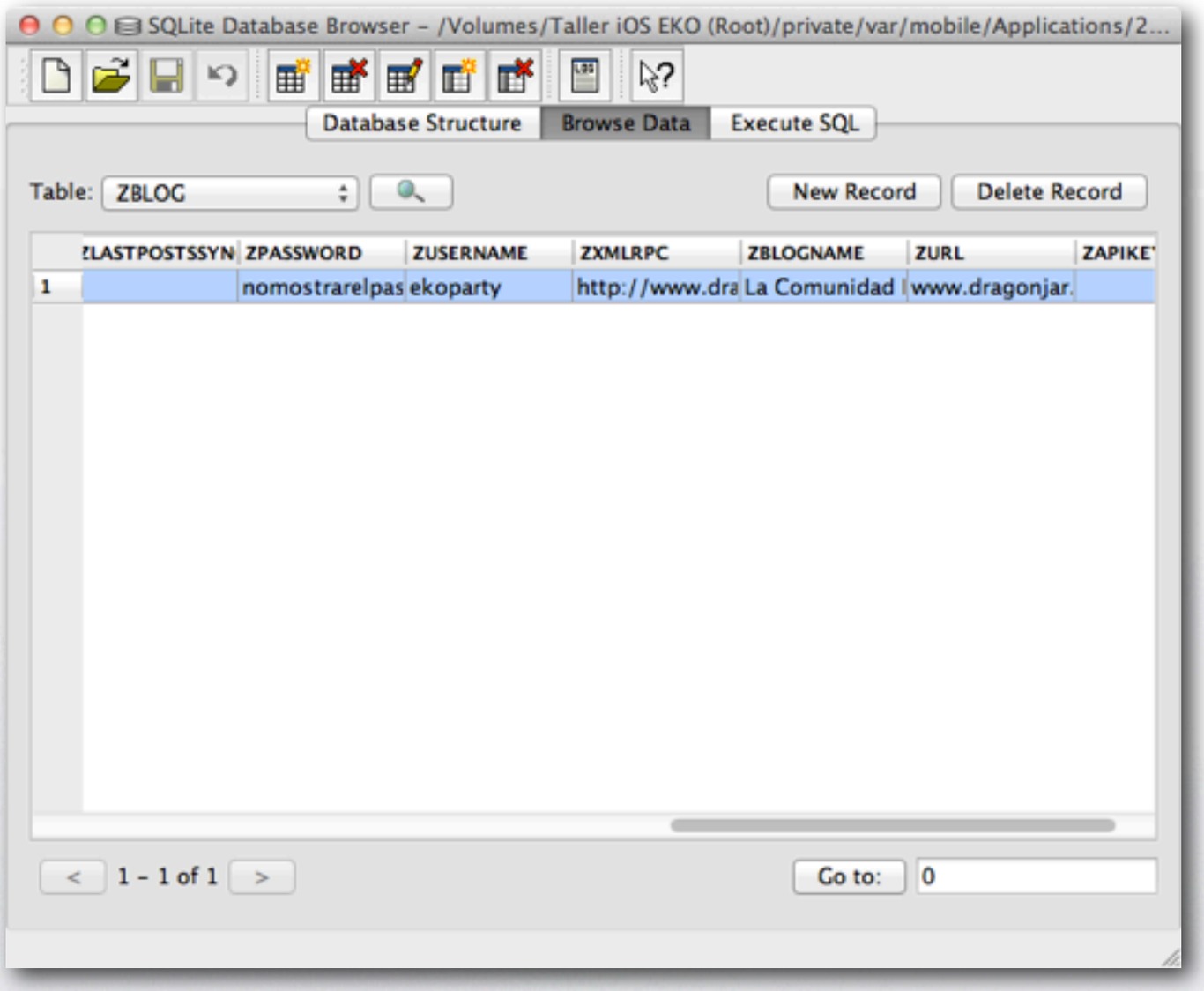

Lifemax

iSSH

/private/var/
mobile/
Applications/
CAMBIA/Library/
Preferences/
config.dat el cliente SSH mas popular de los sistemas iOS no cifra la informacion



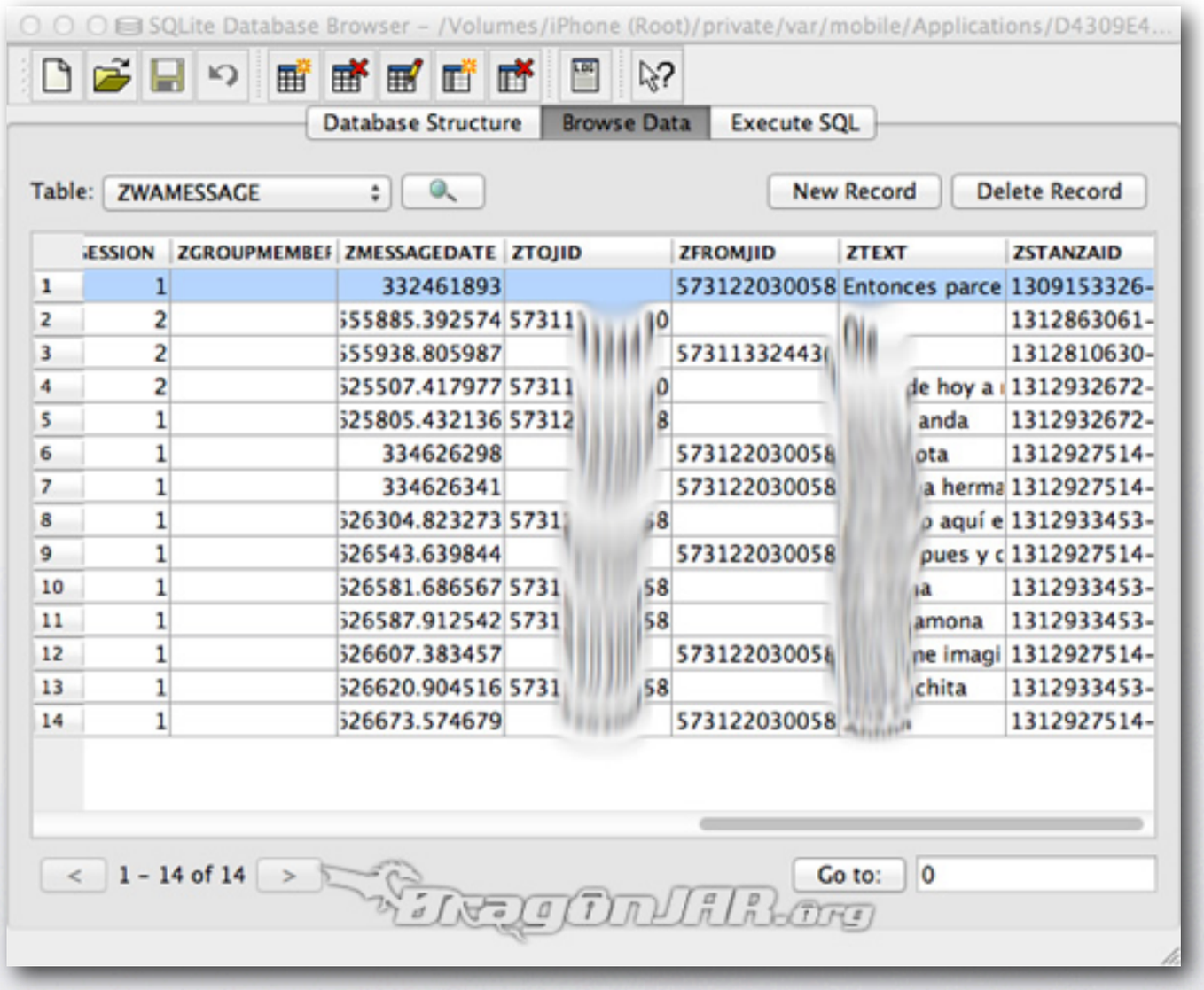
WordPress



/private/var/mobile/Applications/CAMBIA/Documents/WordPress.sqlite ademas de mostrar nuestros datos sin cifrar almacena todos los post, comentarios y borradores de nuestro blog.

WhatsApp

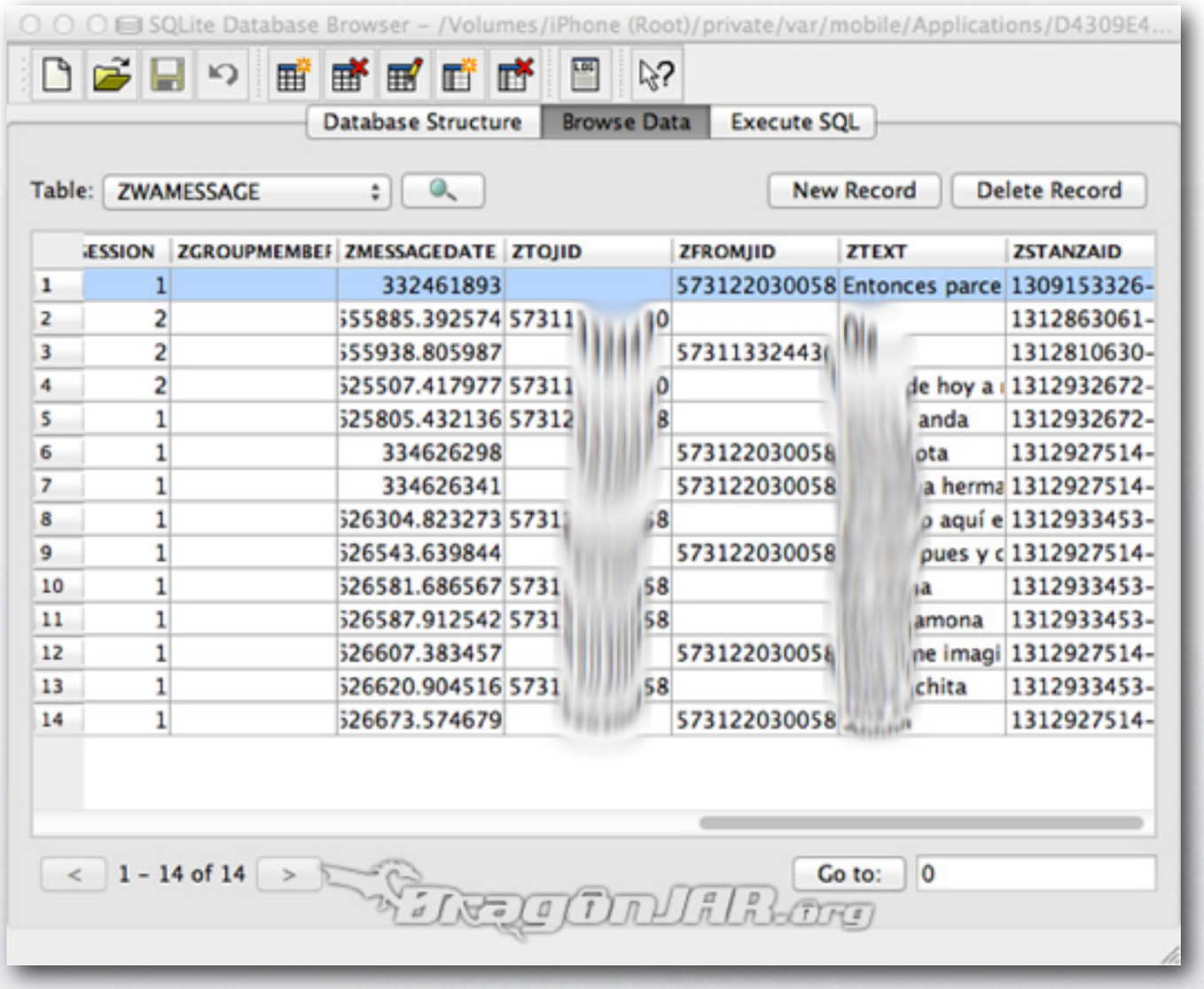
/private/var/mobile/Applications/CAMBIA/Documents/ChatStorage.sqlite ademas de enviar nuestros datos sin cifrar por la red, almacena todos los mensajes enviados desde la aplicación.



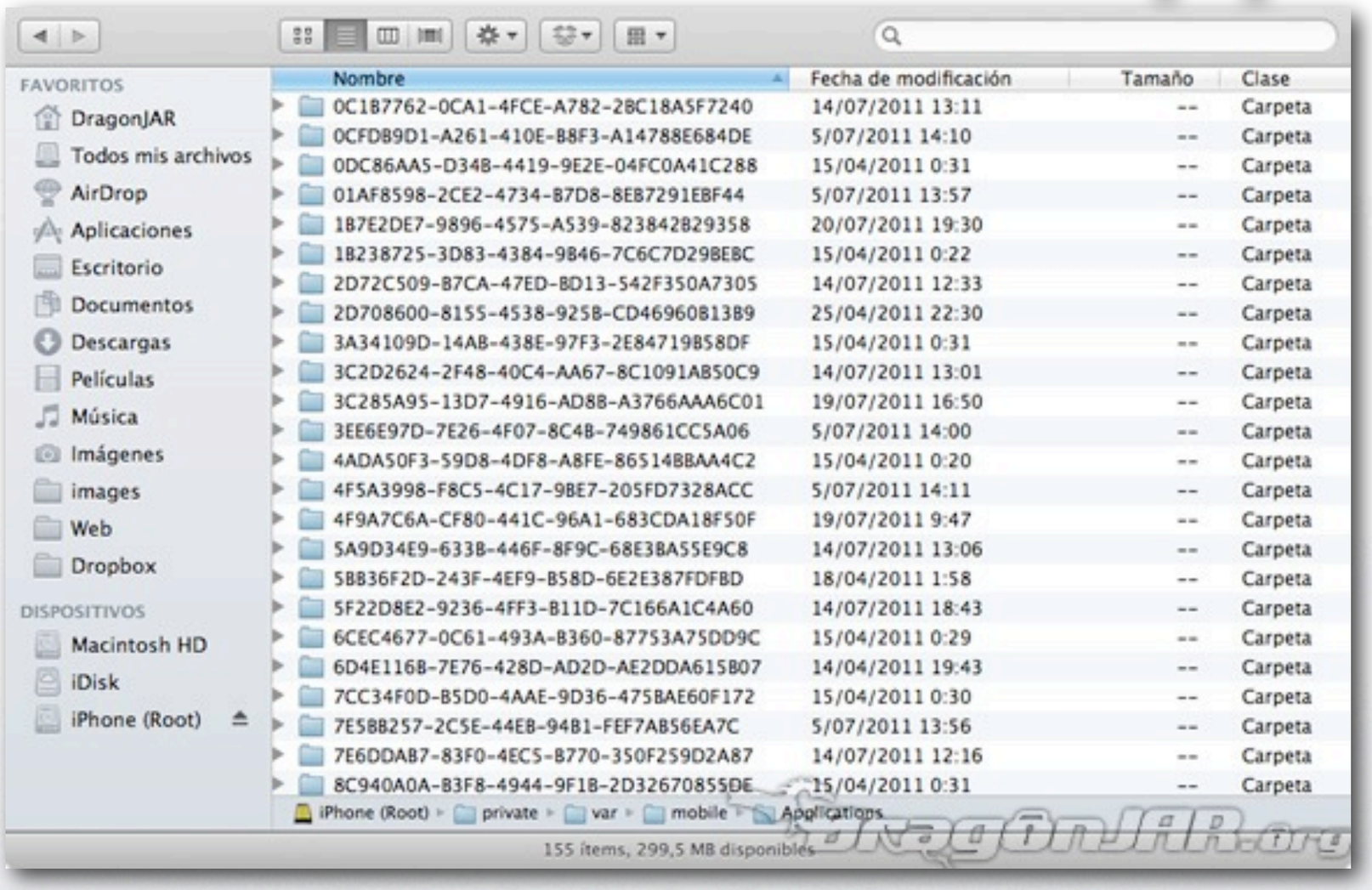
WhatsApp

/private/var/mobile/Applications/CAMBIA/Documents/ChatStorage.sqlite ademas de enviar nuestros datos sin cifrar por la red, almacena todos los mensajes enviados desde la aplicación.

http://goo.gl/lyjAI



Muchísimas mas App's...



/private/var/mobile/Applications

Etapa de informes

goo.gl/lt5AI

- Recopilar y organizar la información
- Escribir los informes
- Ganamos un iPad

DragonJAR.org

sigueme en twitter @DragonJAR