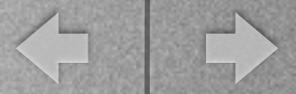




Análisis Forense de Dispositivos iOS

Jaime Andrés Restrepo





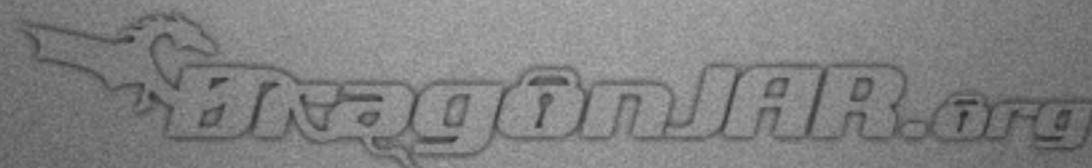
Agenda de la Charla





Agenda de la Charla

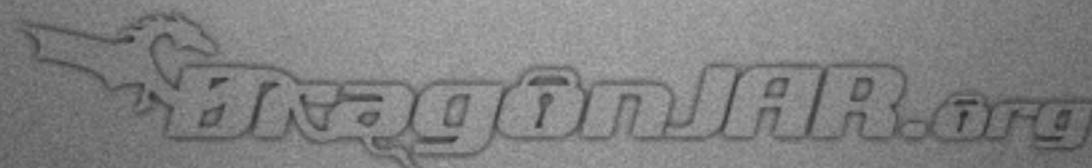
- Introducción





Agenda de la Charla

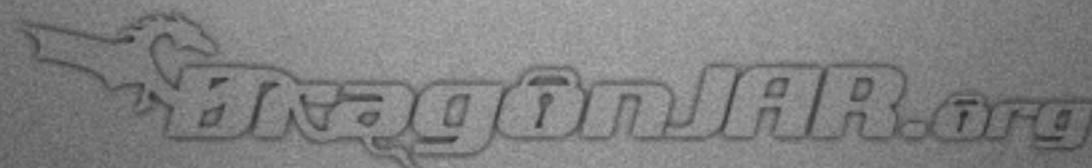
- Introducción
- ¿Como vamos a trabajar?





Agenda de la Charla

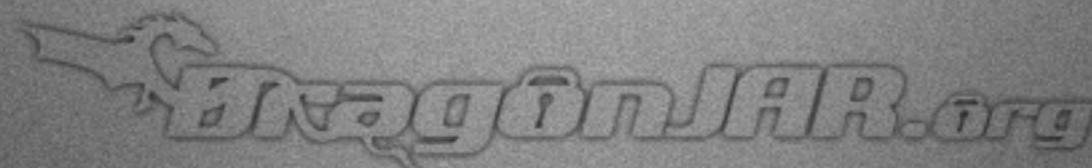
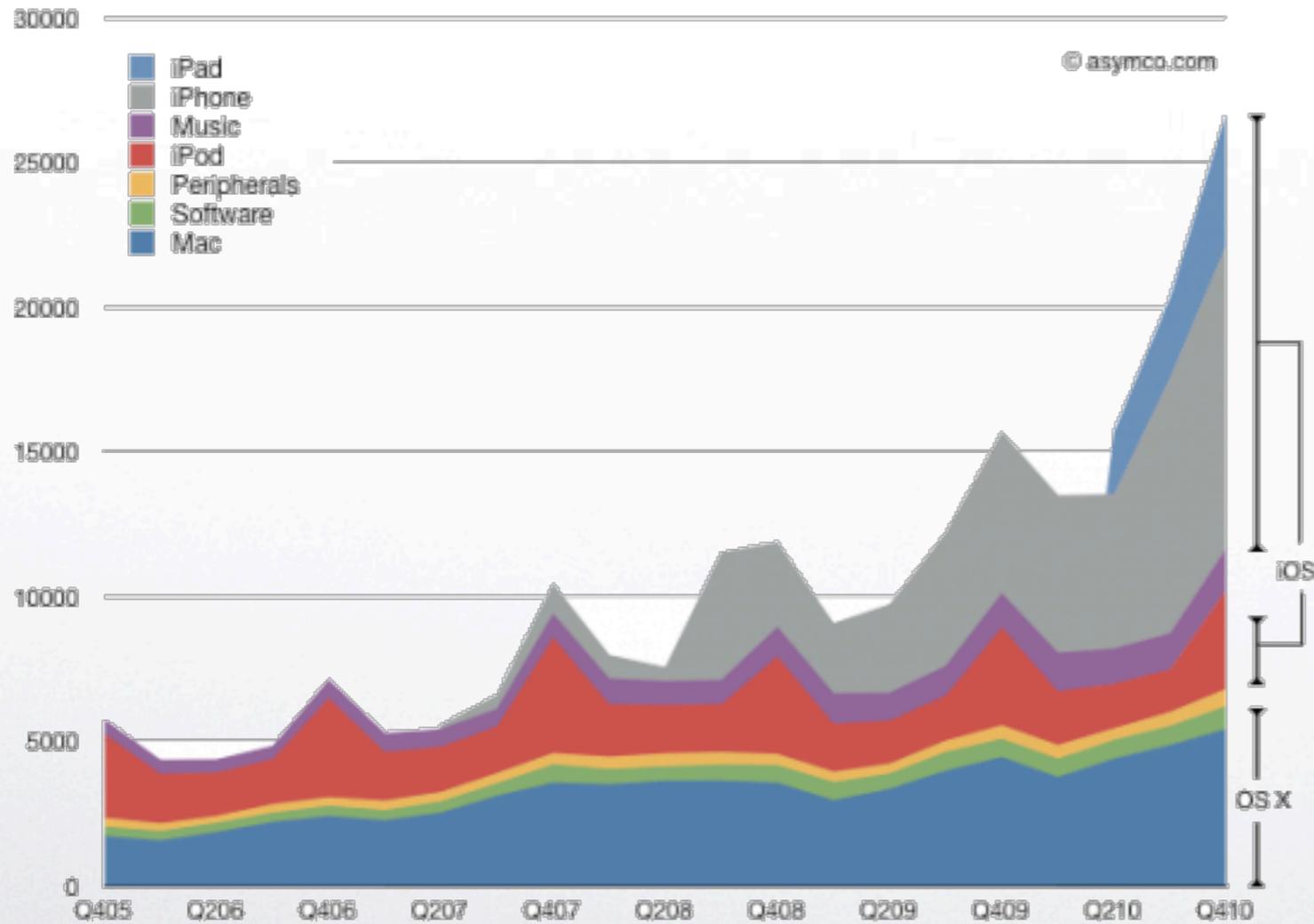
- Introducción
- ¿Como vamos a trabajar?
- **Manos a la Obra!!**





Introducción

Quarterly Sales by Product (\$ million)





 DragonJAR.org

The logo features a stylized dragon head on the left, followed by the text "DragonJAR.org" in a bold, outlined, sans-serif font.



¿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.





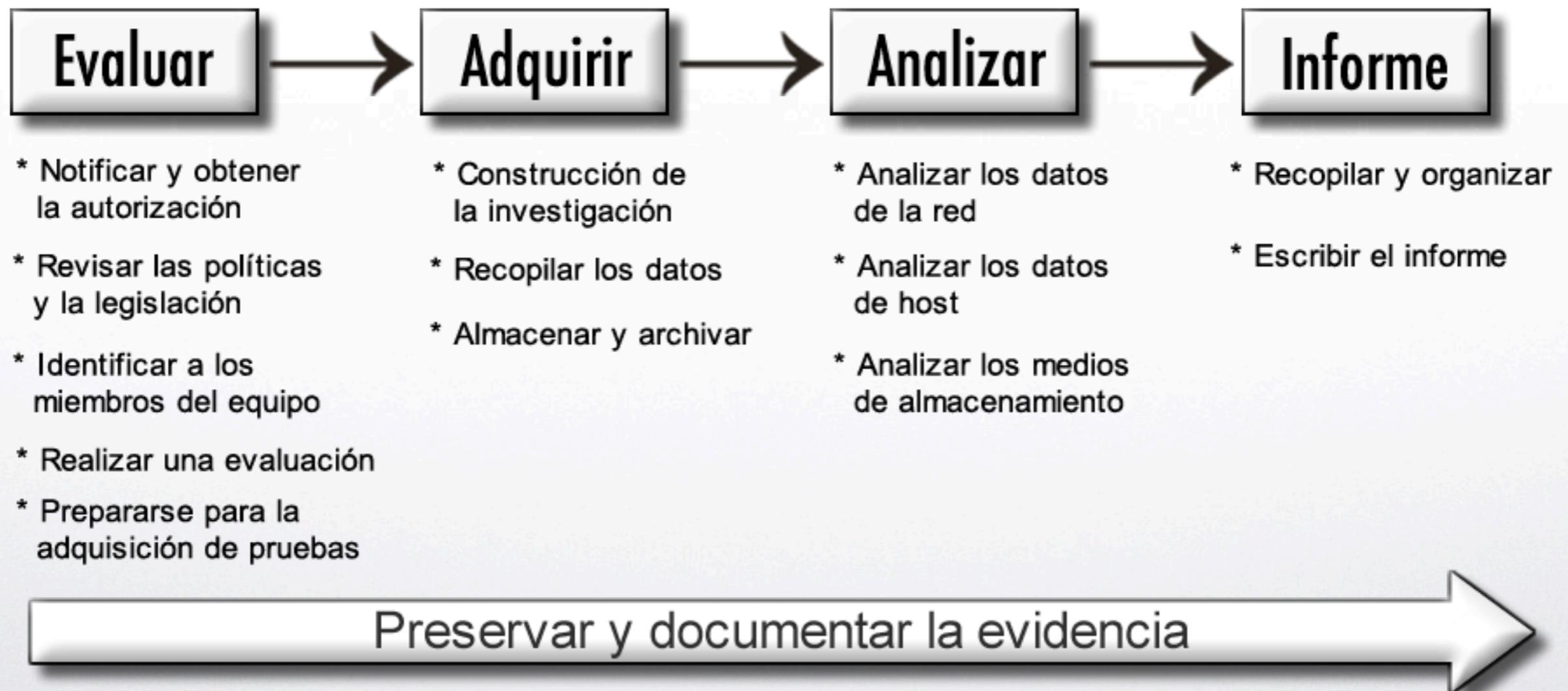
¿Cómo vamos a trabajar?

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



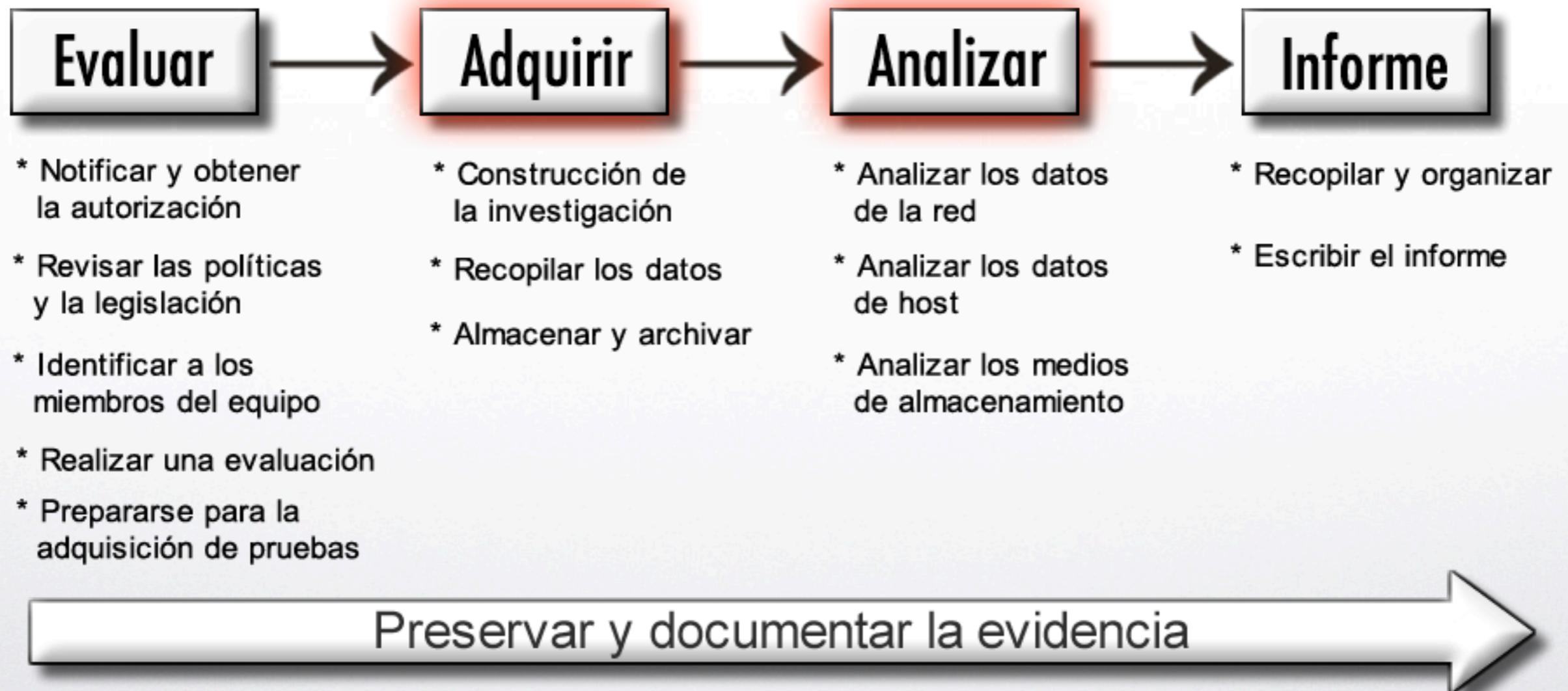


Etapas de un análisis forense





Etapas de un análisis forense





Etapa de evaluación

goo.gl/fskC2





Etapa de evaluación

- Notificar y obtener autorizaciones

goo.gl/fskC2



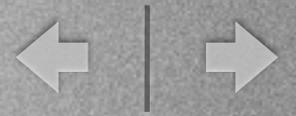


Etapa de evaluación

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

goo.gl/fskC2



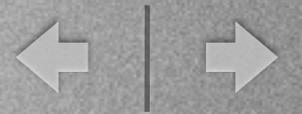


Etapa de evaluación

- 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

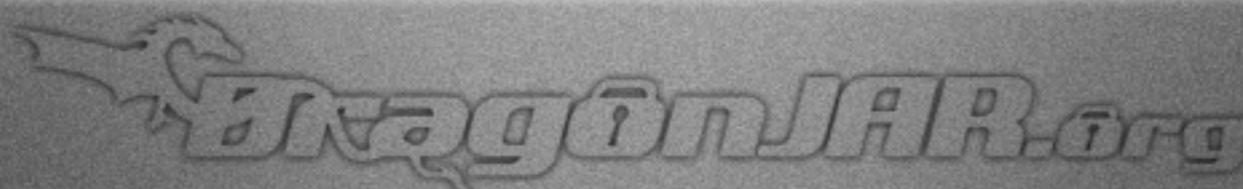
goo.gl/NmZAR

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



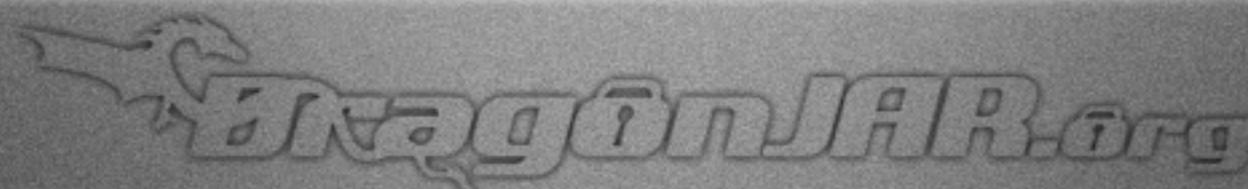


Tareas previas a la adquisición





Tareas previas a la adquisición





Tareas previas a la adquisición





Tareas previas a la adquisición



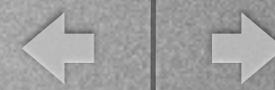


Tareas previas a la adquisición





 **DragonJAR.org**

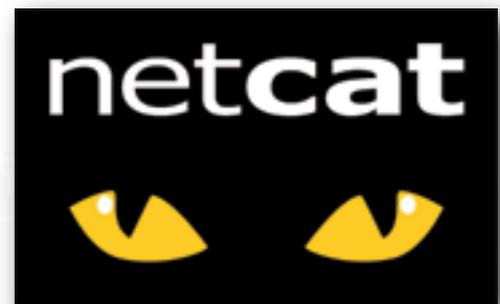


 **DragonJAR.org**



Adquisición con las uñas

Método

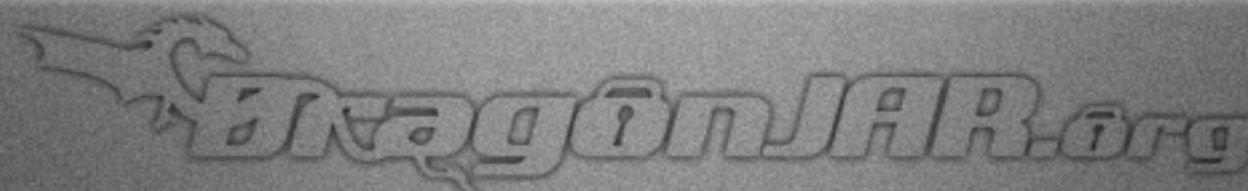


```
ios — ssh — 106x22
Hackintosh:iOS DragonJAR$ ssh root@192.168.0.12
root@192.168.0.12's password:
iPhone:~ root# dd if=/dev/disk0s2 bs=4096 | nc 192.168.0.10 9000
[]
```

dd if=/dev/disk0s2 bs=4096 | nc TU-IP PUERTO

```
ios — dd — 106x7
Hackintosh:iOS DragonJAR$ nc -l 9000 | dd of=imageniOS.img
```

nc -l 9000 | dd of=NOMBREIMAGEN.img

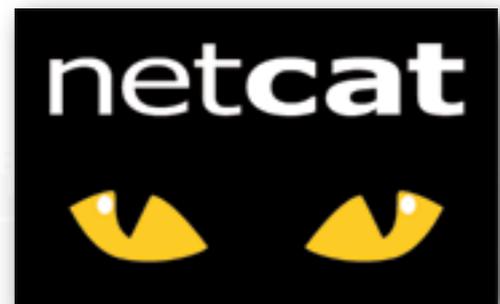




Adquisición con las uñas

- Que el dispositivo iOS tenga Jailbreak.

Método



```
ios — ssh — 106x22
Hackintosh:iOS DragonJAR$ ssh root@192.168.0.12
root@192.168.0.12's password:
iPhone:~ root# dd if=/dev/disk0s2 bs=4096 | nc 192.168.0.10 9000
[]
```

dd if=/dev/disk0s2 bs=4096 | nc TU-IP PUERTO

```
ios — dd — 106x7
Hackintosh:iOS DragonJAR$ nc -l 9000 | dd of=imageniOS.img
```

nc -l 9000 | dd of=NOMBREIMAGEN.img

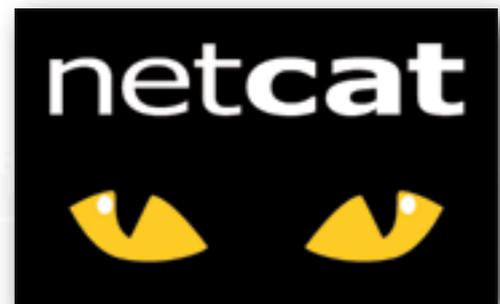




Adquisición con las uñas

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

Método



```
ios — ssh — 106x22
Hackintosh:iOS DragonJAR$ ssh root@192.168.0.12
root@192.168.0.12's password:
iPhone:~ root# dd if=/dev/disk0s2 bs=4096 | nc 192.168.0.10 9000
[]
```

dd if=/dev/disk0s2 bs=4096 | nc TU-IP PUERTO

```
ios — dd — 106x7
Hackintosh:iOS DragonJAR$ nc -l 9000 | dd of=imageniOS.img
```

nc -l 9000 | dd of=NOMBREIMAGEN.img

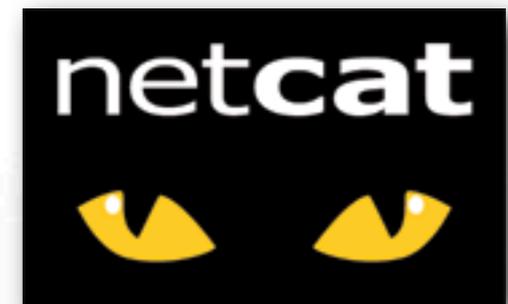




Adquisición con las uñas

- 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

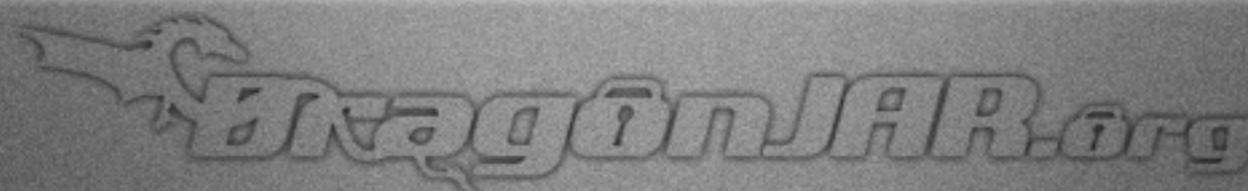


```
ios — ssh — 106x22
Hackintosh:iOS DragonJAR$ ssh root@192.168.0.12
root@192.168.0.12's password:
iPhone:~ root# dd if=/dev/disk0s2 bs=4096 | nc 192.168.0.10 9000
[]
```

dd if=/dev/disk0s2 bs=4096 | nc TU-IP PUERTO

```
ios — dd — 106x7
Hackintosh:iOS DragonJAR$ nc -l 9000 | dd of=imageniOS.img
```

nc -l 9000 | dd of=NOMBREIMAGEN.img





Adquisición con las uñas

Método



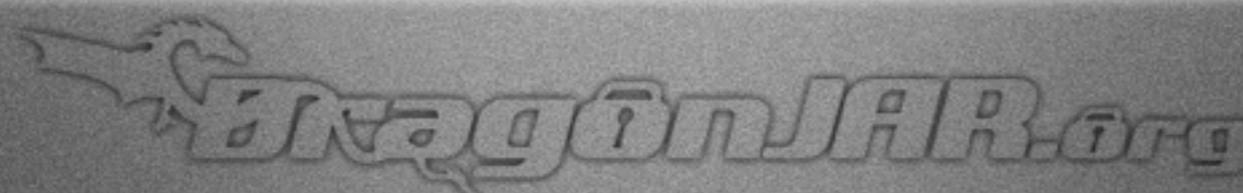
iPhone (E:)

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Carpetas

Dirección E:\

Nombre	Tamaño	Tipo	Fecha de modificación
.fsevents		Carpeta de archivos	16/09/2011 15:09
Applications		Carpeta de archivos	15/04/2011 1:12
bin		Carpeta de archivos	10/09/2011 0:24
boot		Carpeta de archivos	28/10/2006 14:07
cores		Carpeta de archivos	07/02/2011 3:58
dev		Carpeta de archivos	15/09/2011 1:32
Developer		Carpeta de archivos	18/03/2011 21:55
etc		Carpeta de archivos	15/04/2011 1:12
lib		Carpeta de archivos	28/10/2006 14:07
Library		Carpeta de archivos	15/04/2011 6:07
mnt		Carpeta de archivos	28/10/2006 14:07
private		Carpeta de archivos	16/09/2011 4:09
sbin		Carpeta de archivos	30/03/2011 9:47
System		Carpeta de archivos	26/03/2011 14:46
tmp		Carpeta de archivos	15/04/2011 1:12
User		Carpeta de archivos	15/09/2011 1:32
usr		Carpeta de archivos	15/04/2011 1:13
var		Carpeta de archivos	15/04/2011 1:12

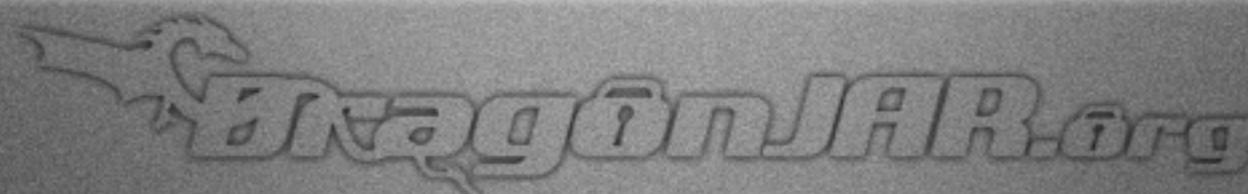
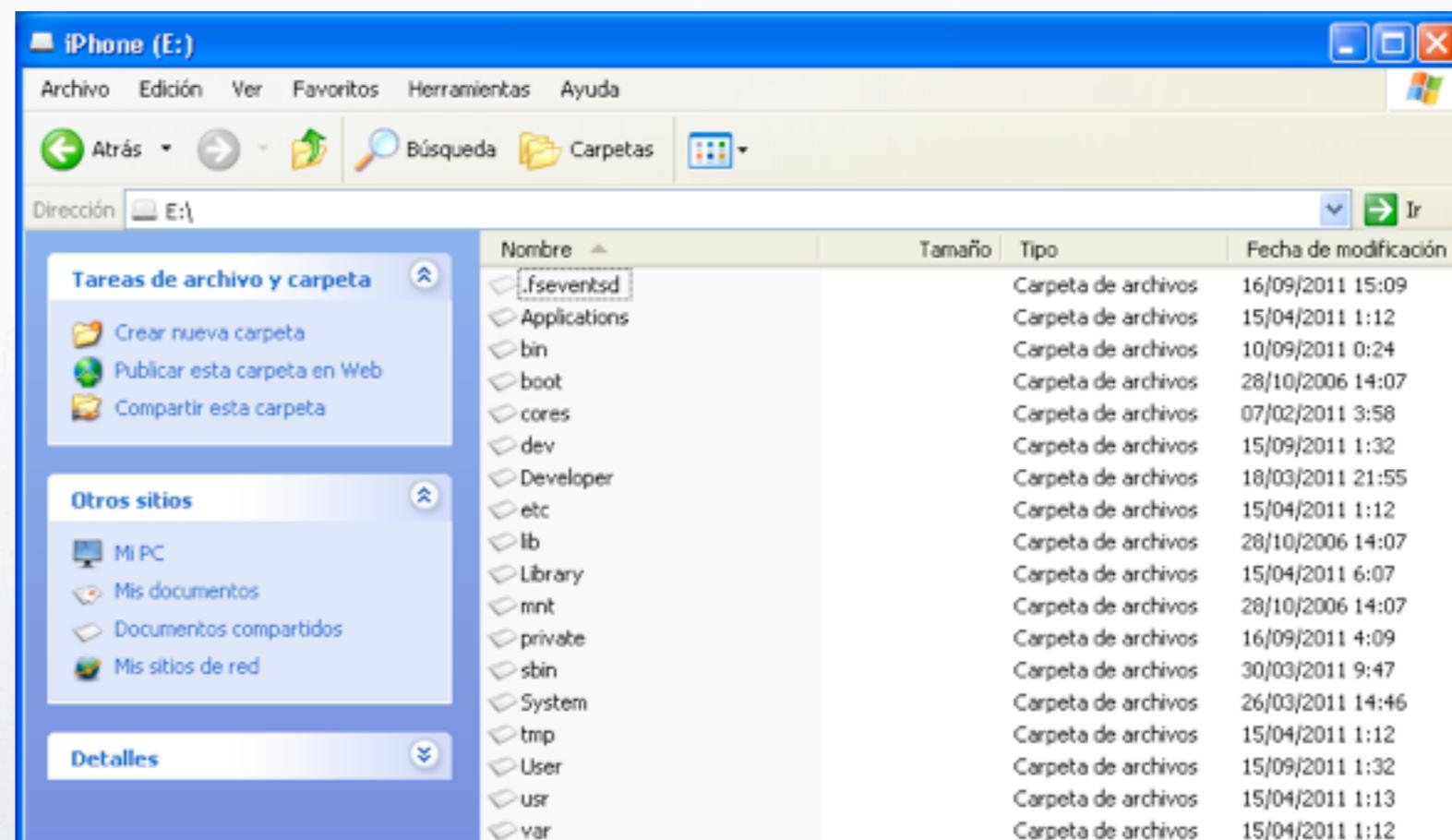




Adquisición con las uñas

- Obtener el PhoneDisk

Método



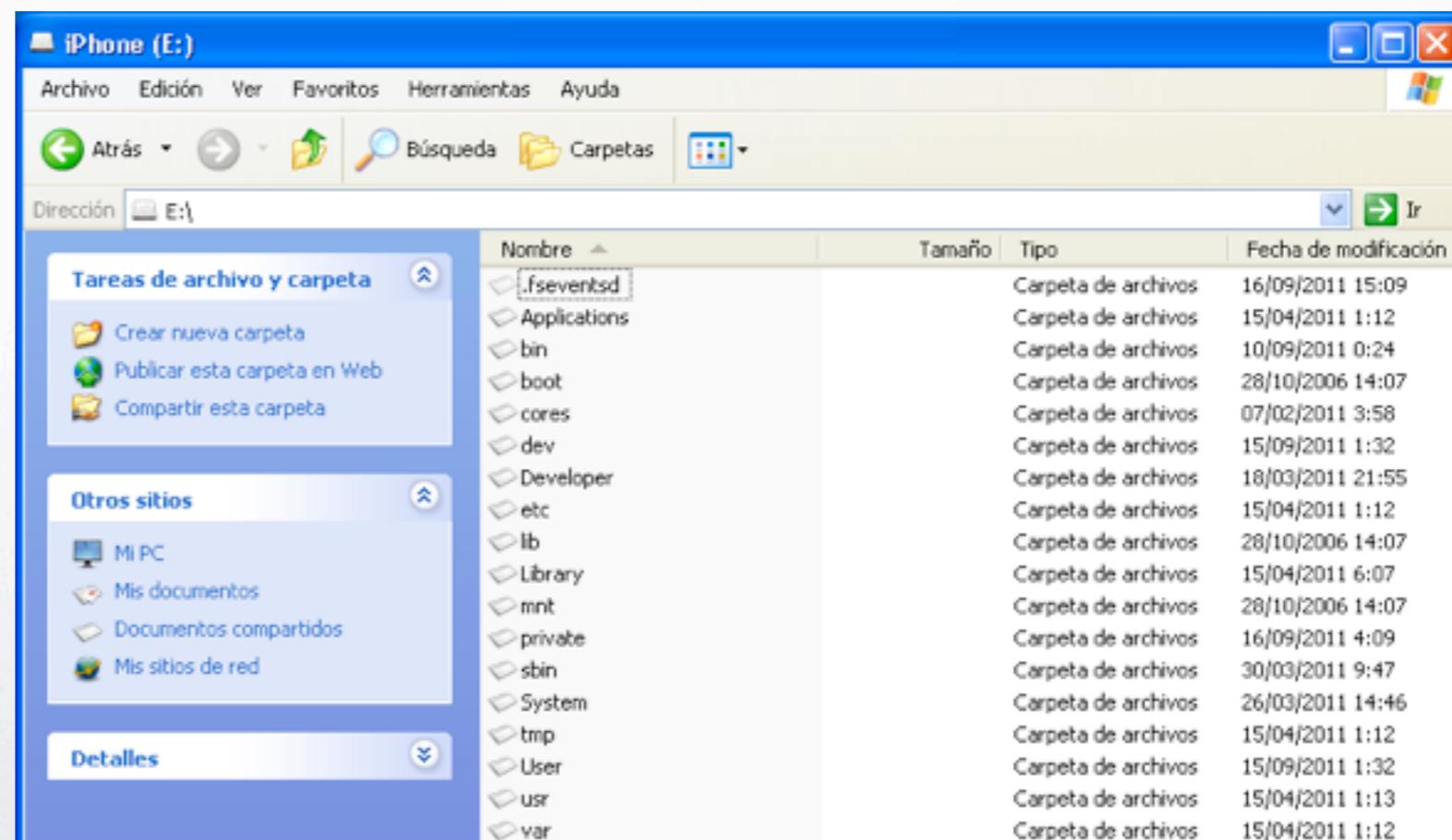


Adquisición con las uñas

Método



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



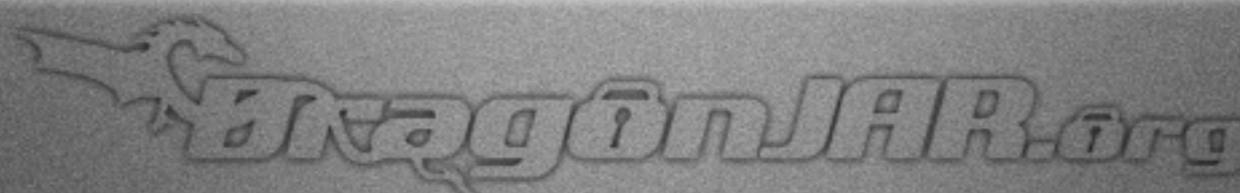
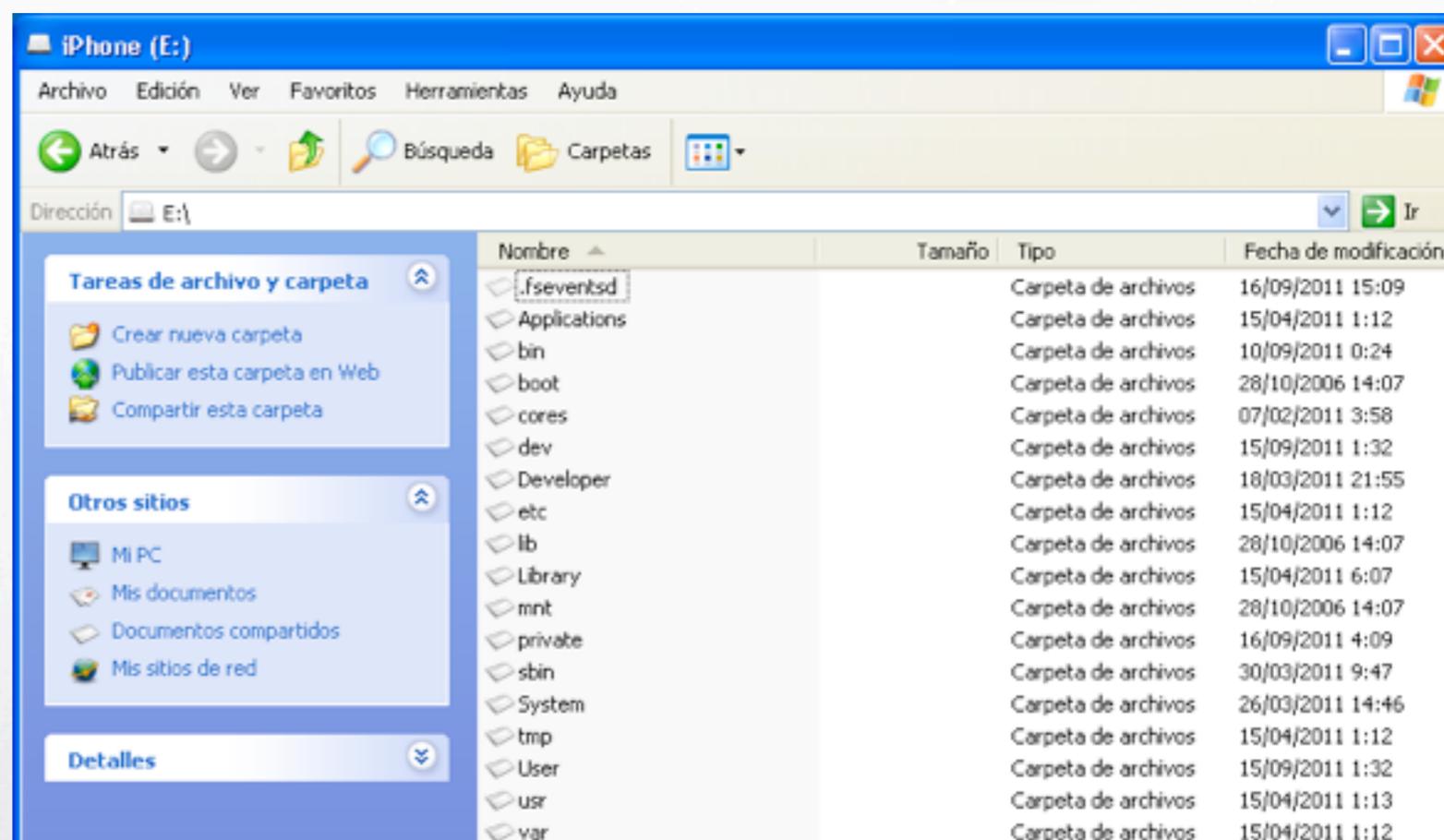


Adquisición con las uñas

Método



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



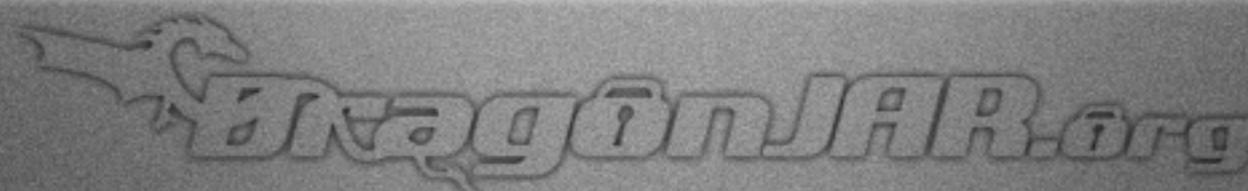
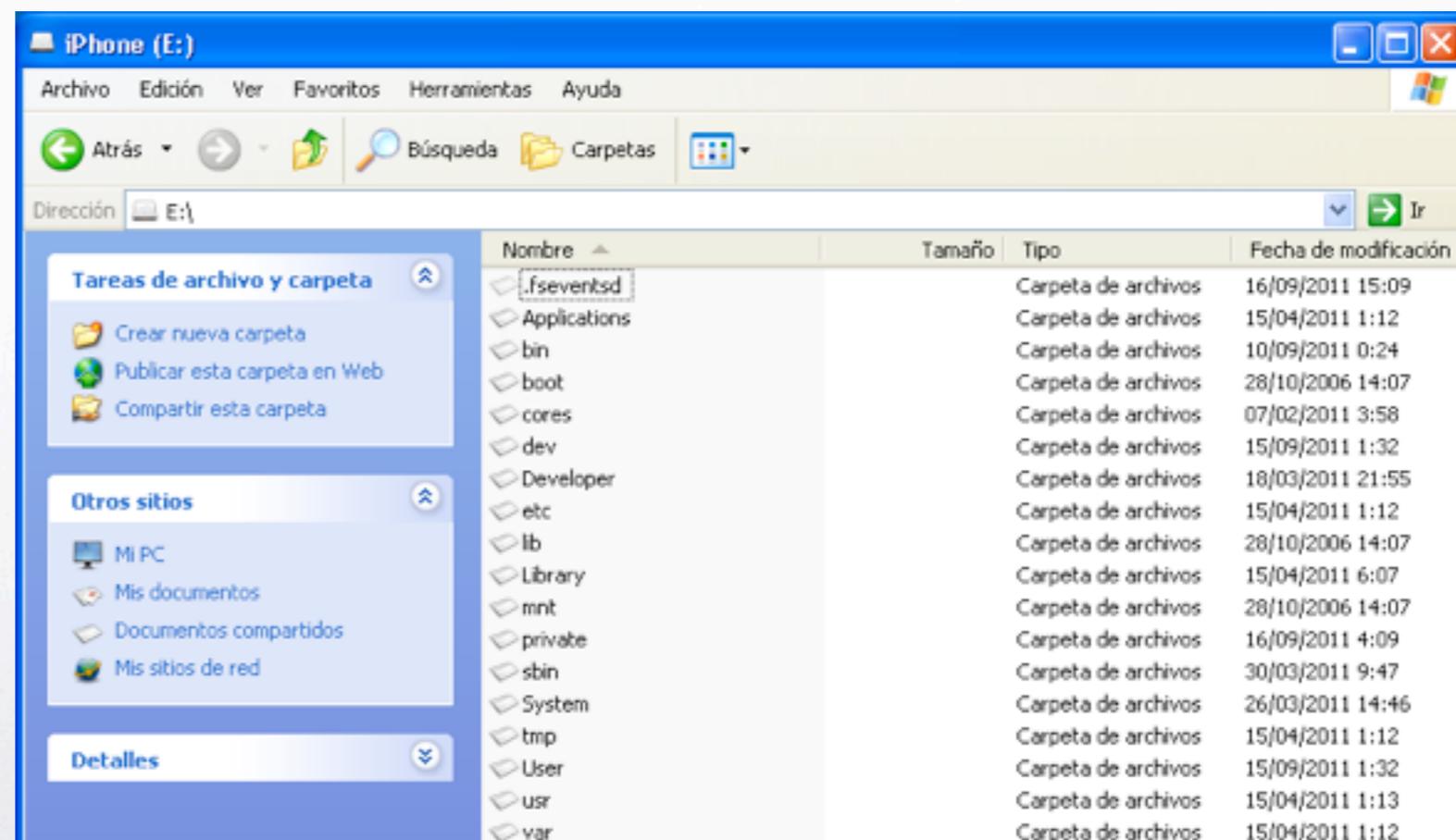


Adquisición con las uñas

Método



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



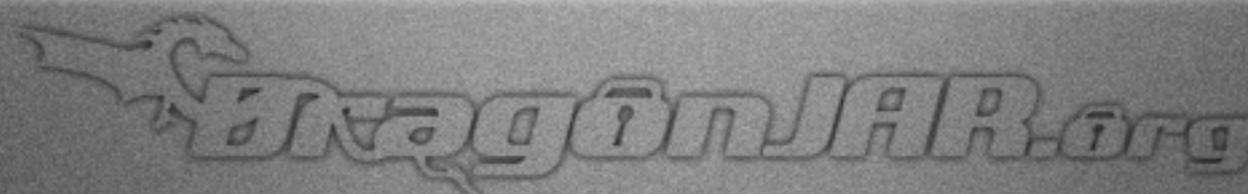
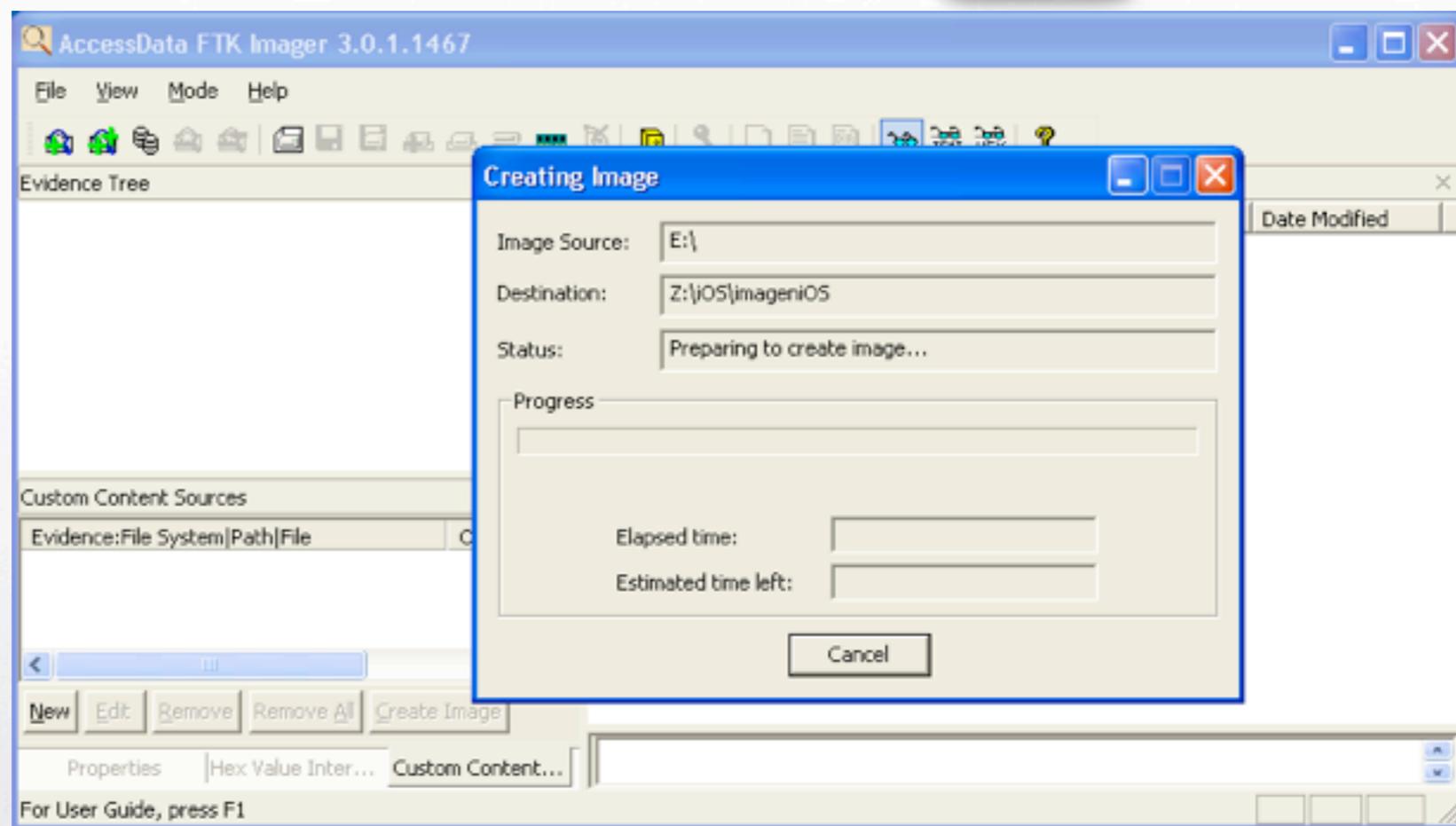


Adquisición con las uñas

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

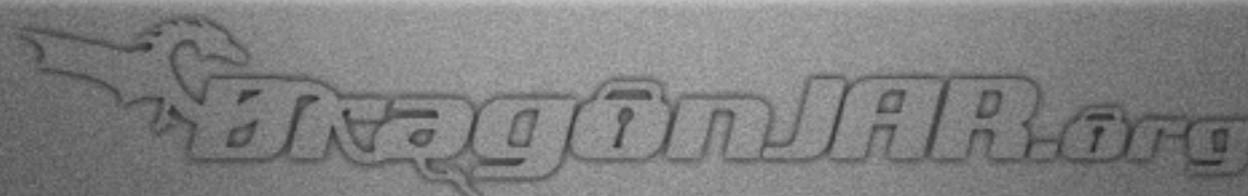
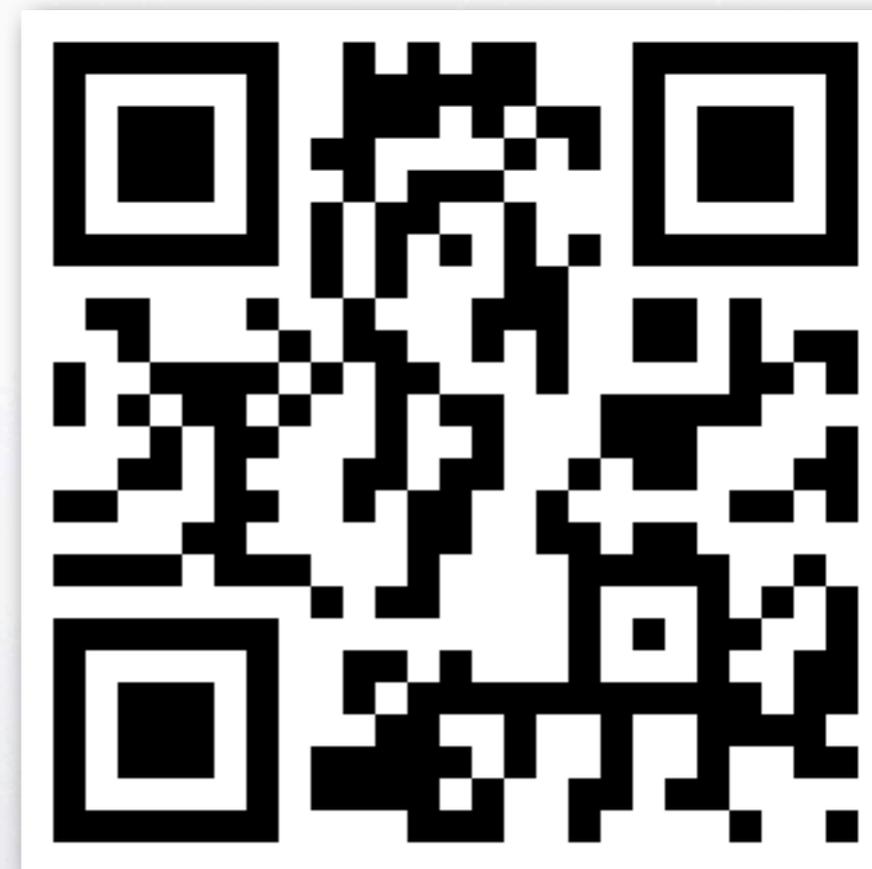
Tener \$3,999USD





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

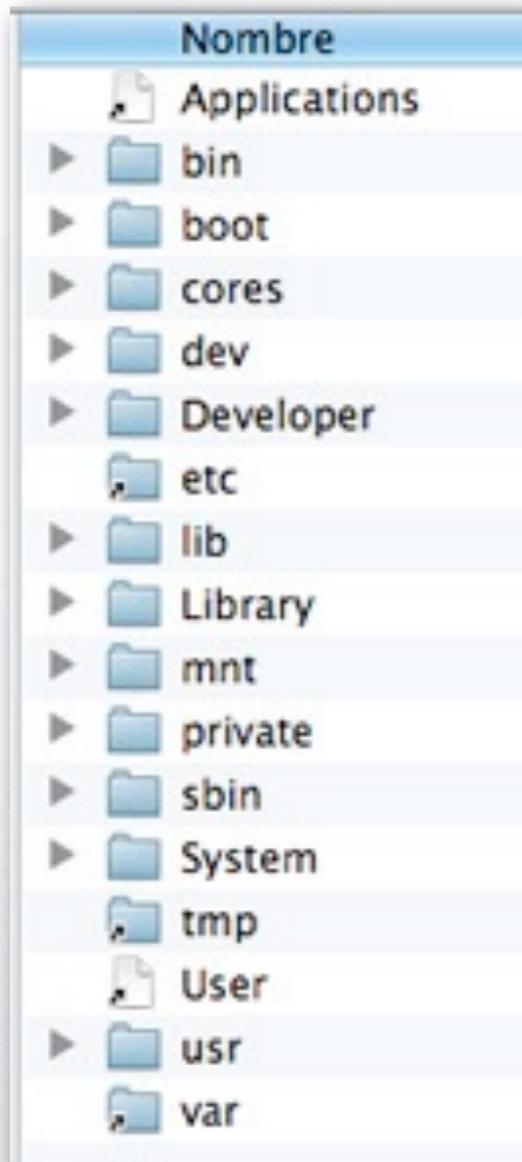
- Analizar los datos de la red
- Analizar los datos del dispositivo
- Analizar los medios de almacenamiento

goo.gl/Y2pgU





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

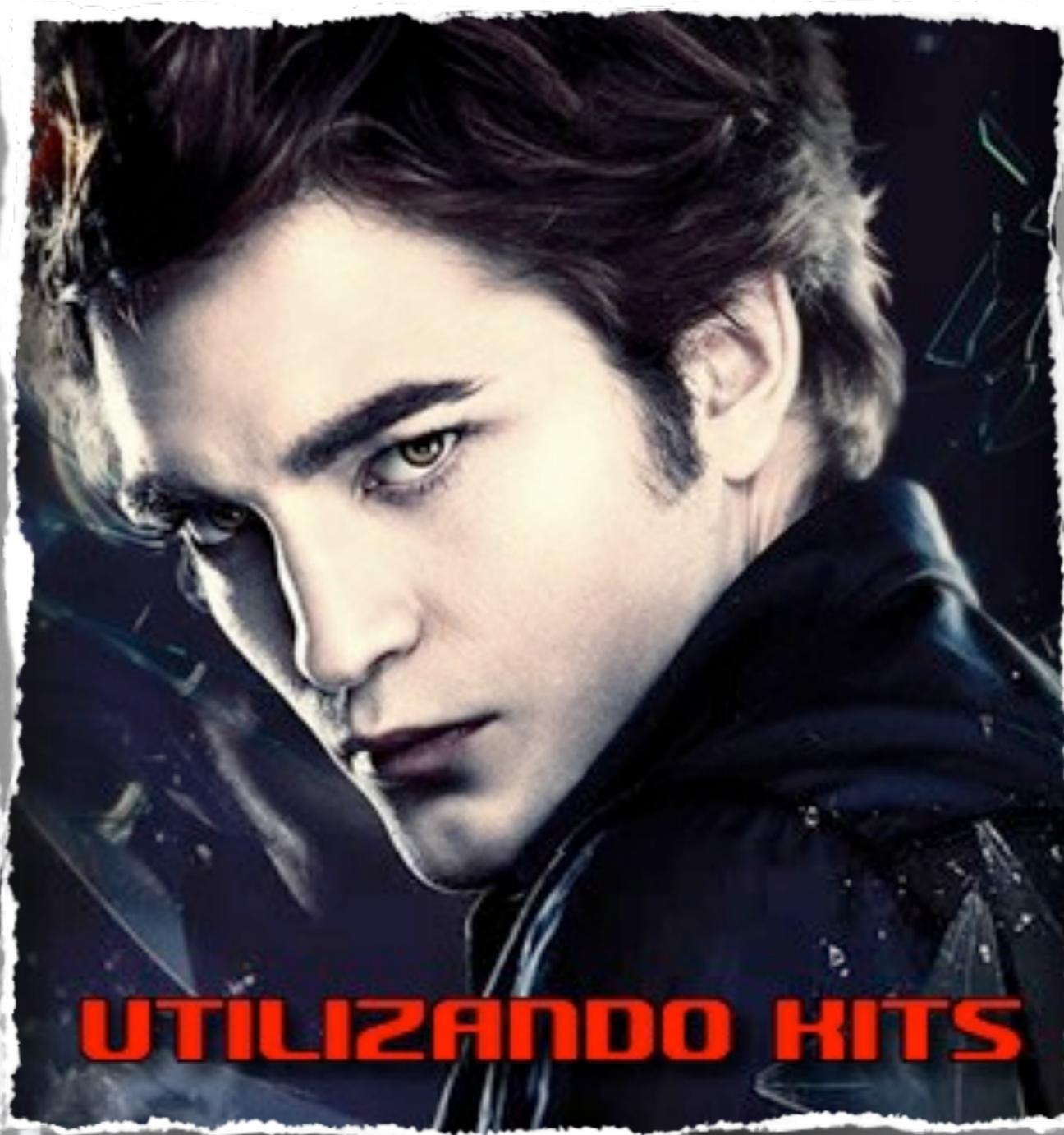
tmp: Es un enlace simbólico a -> private/var/tmp/

usr: Contiene los datos de zona horaria y ejecutables del sistema

var: Es un enlace simbólico a -> private/var/









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 recuperación de archivos



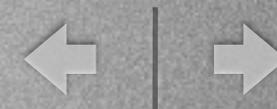


Análisis con las uñas - Herramientas



- 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 recuperación 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 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: últimas 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



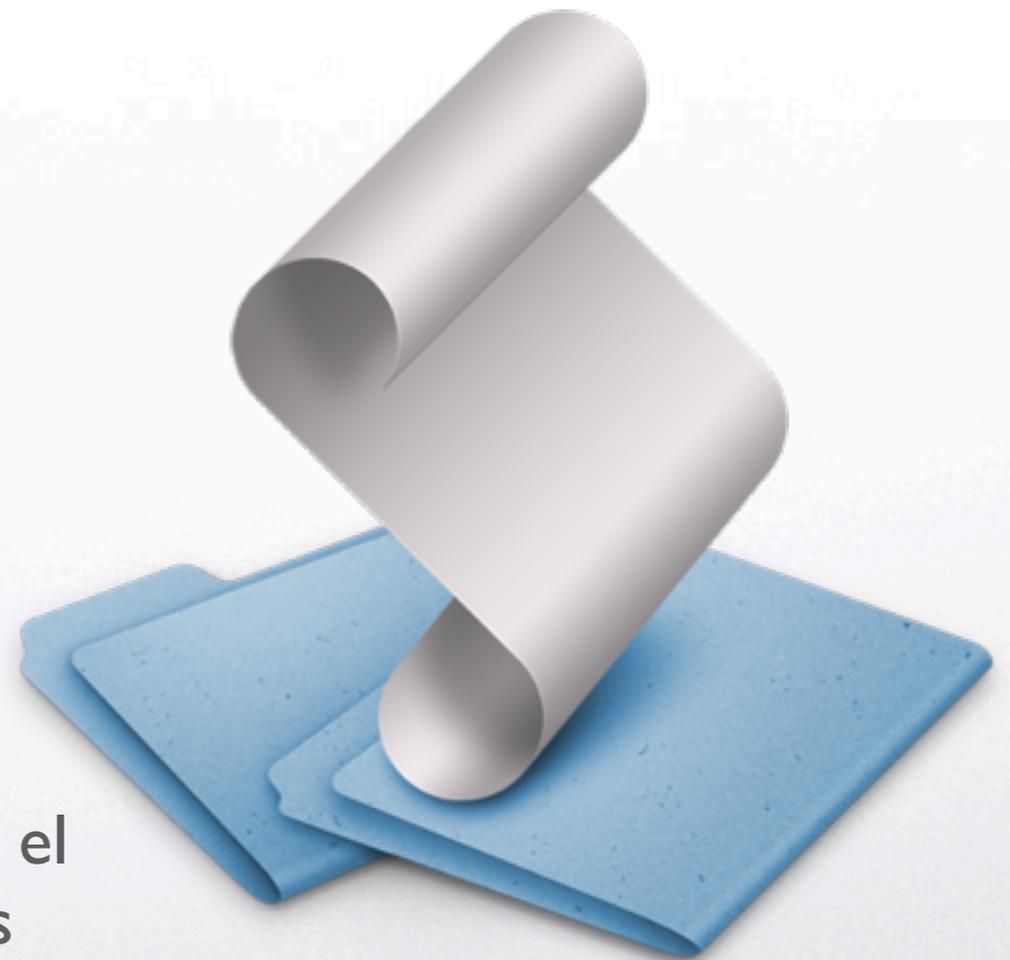


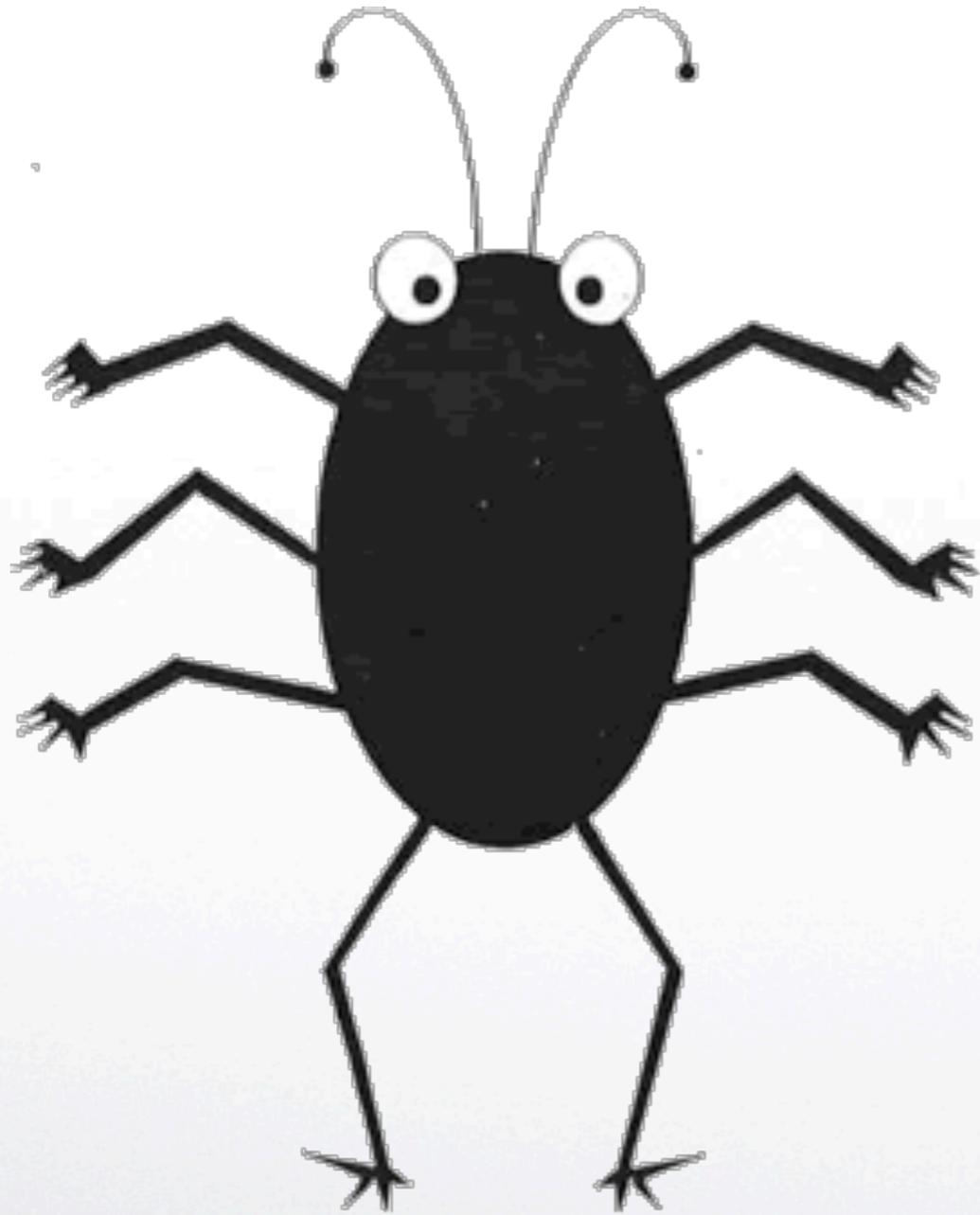
Análisis con las uñas - Logs

/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 línea de tiempo.

/var/wireless/Library/Logs logs sobre las conexiones inalámbricas (3G, Bluetooth, 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





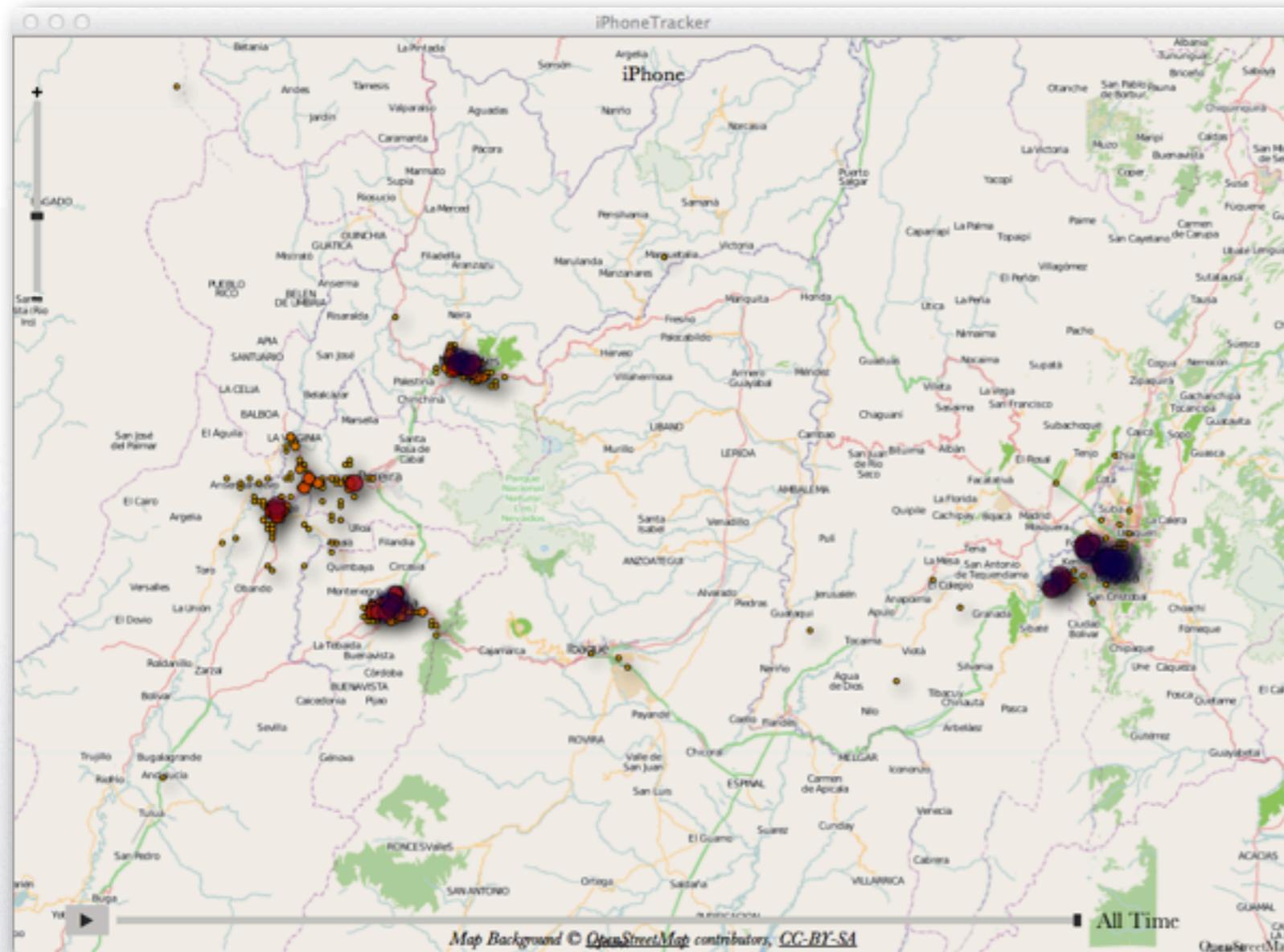
BUG



FUNCIONALIDAD



consolidate.db



**/private/var/root/
Library/Caches/
locationd/
consolidate.db**
archivo que contiene las
ultimas ubicaciones
donde estuvo nuestro
dispositivo

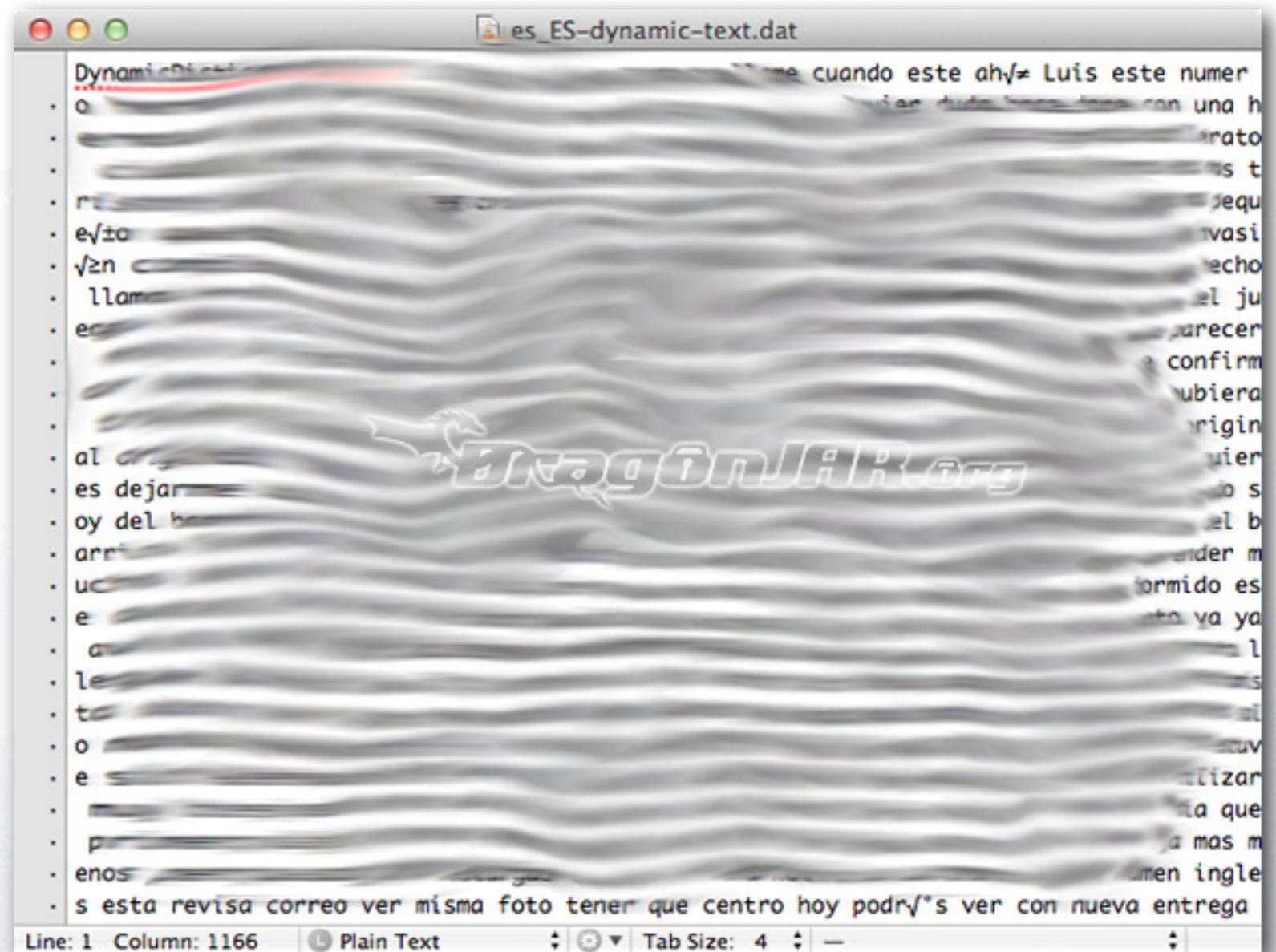




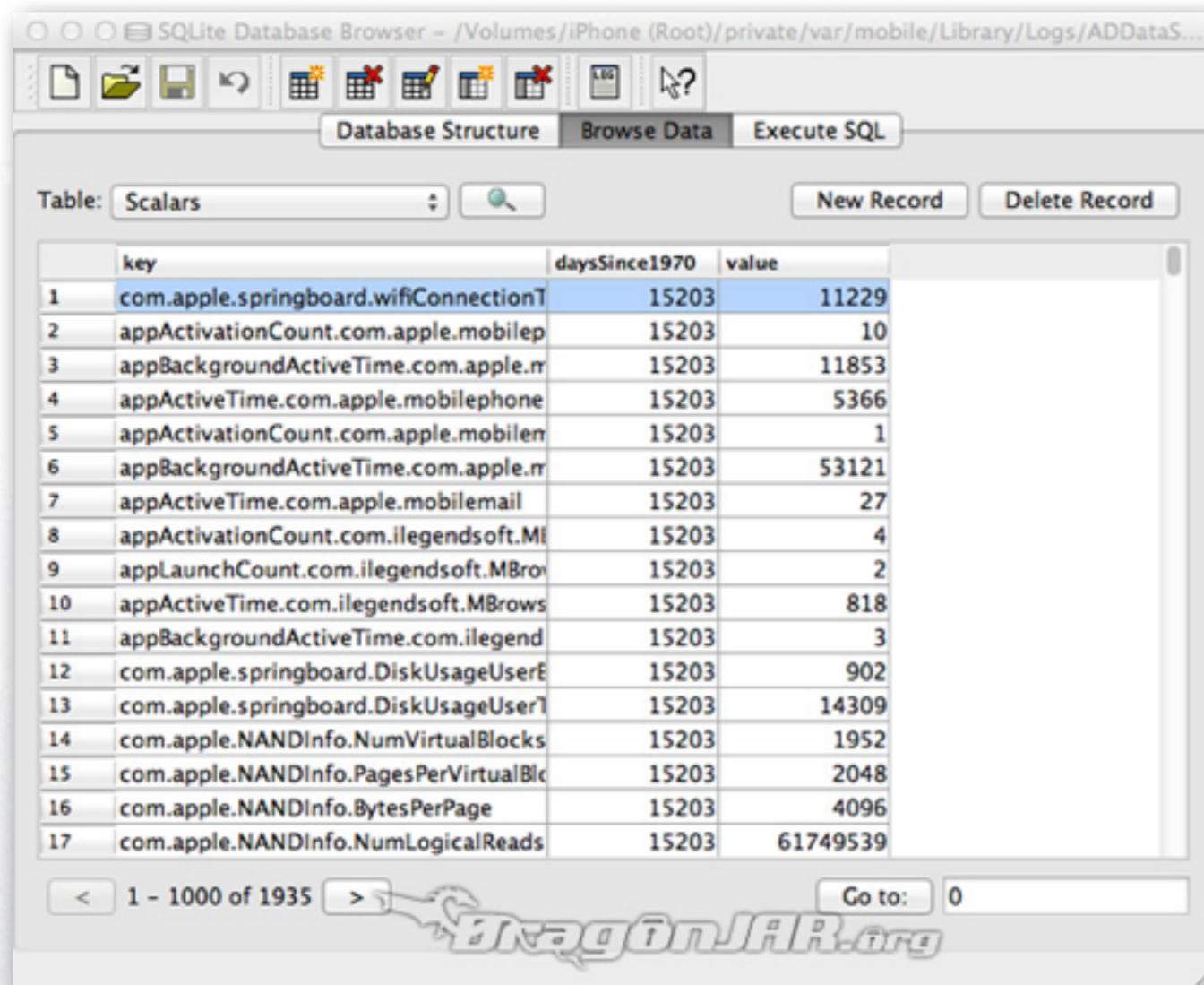
dynamic-text.dat o iKeylogger

**/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



SQLite Database Browser - /Volumes/iPhone (Root)/private/var/mobile/Library/Logs/ADDataS...

Database Structure Browse Data Execute SQL

Table: Scalars

	key	daysSince1970	value
1	com.apple.springboard.wifiConnectionT	15203	11229
2	appActivationCount.com.apple.mobilep	15203	10
3	appBackgroundActiveTime.com.apple.r	15203	11853
4	appActiveTime.com.apple.mobilephone	15203	5366
5	appActivationCount.com.apple.mobilen	15203	1
6	appBackgroundActiveTime.com.apple.r	15203	53121
7	appActiveTime.com.apple.mobileemail	15203	27
8	appActivationCount.com.ilegendsoft.MI	15203	4
9	appLaunchCount.com.ilegendsoft.MBro	15203	2
10	appActiveTime.com.ilegendsoft.MBrows	15203	818
11	appBackgroundActiveTime.com.ilegend	15203	3
12	com.apple.springboard.DiskUsageUserE	15203	902
13	com.apple.springboard.DiskUsageUserT	15203	14309
14	com.apple.NANDInfo.NumVirtualBlocks	15203	1952
15	com.apple.NANDInfo.PagesPerVirtualBlc	15203	2048
16	com.apple.NANDInfo.BytesPerPage	15203	4096
17	com.apple.NANDInfo.NumLogicalReads	15203	61749539

< 1 - 1000 of 1935 > Go to: 0

DragonJAR.org

**/private/var/mobile/
Library/Logs/
ADDataStore.sqlitedb**
historial de las aplicaciones
abiertas y el tiempo que fué
utilizada



Análisis con Software Comercial

Oxygen Forensic Suite 2011 (Trial)

Main View Tools Service Help

All devices > 1 > Forense en iOS (iPhone 4) - 04/09/2011 22:06:03 [012424000217453] Filtering criteria ...

Connect new device Load backup file Save to archive Remove Export Print Reset Filters Help

You can start Oxygen Forensic Suite 2011 Trial version 30 times only until 04/10/2011. Attempts remaining: 23. [Order a full version right now!](#)

Sections Search data View mode Actions

Devices and Ca...
All devices
1
For...

Common sections

- Messages**
Messages section allows to view SMS, MMS, E-mail, Beamed and other messages types and their attachments in default and custom folders.
- Event Log**
Event Log section stores data about all calls, SMS messages sent and received, GPRS and WIFI sessions of the device owner.
- Calendar**
Calendar section allows to analyze meetings, anniversaries, reminders and other types of events.
- Notes**
Notes section enables users to examine notes of any length.
- File Browser**
File Browser section presents the entire mobile device file system, including photos, videos, voice records, documents, geo files and other important information.

Extras

- Timeline**
Timeline section summarizes all phone events in a chronological order.
- Web Connections and Location Services**
Web Connections and Location Services section allows to inspect all web connections in one list and shows hot spots on the map.
- Applications**
Applications section presents the whole list of pre-installed or custom applications.
- Web Browsers Cache Analyzer**
Web Browsers Cache Analyzer displays a list of Internet sites visited and files downloaded by the device owner.
- Dictionaries**
Dictionaries section allows to identify words entered by the phone owner while making notes, writing messages, etc.

Trial version: 3.5.0.502 Forense en iOS (iPhone 4) Case: 1, Forense en iOS (iPhone 4) [012424000217453]



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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> All functionality of Analyst version Android Rooting Add-On 12 months of free updates 	\$ 2998 (€ 2498)

The screenshot shows the Oxygen Forensic Suite 2011 interface. At the top, there's a date and time filter: 04/09/2011 22:06:03 [012424000217453]. Below this are action buttons: Save to archive, Remove, Export, Print, Reset Filters, and Help. A warning message states: 'version 30 times only until 04/10/2011. Attempts remaining: 23.' and a link to 'Order a full version right now!'. The interface is divided into sections: 'Extras' on the right lists features like Timeline, Web Connections and Location Services, Applications, Web Browsers Cache Analyzer, and Dictionaries. The main area shows a list of analysis options, including 'view SMS, MMS, E-mail, Beamed and other attachments in default and custom folders.', 'Data about all calls, SMS messages sent and sessions of the device owner.', 'analyze meetings, anniversaries, reminders and...', and 'to examine notes of any length.' The bottom status bar shows 'Case: 1, Forense en iOS (iPhone 4) [012424000217453]'.



Análisis con Software Comercial

Prueba1.lantern

New Case Acquire Report Export Inspect Search

Case 1
Evidence 1

Info
Contacts
Calls
SMS/MMS
Notes
Calendar
Internet
Skype
Voicememos
Facebook
Locations
Wifi
Camera
Media
Usage
Documents
Timeline

	Time	To/From	Number	Duration	
	09/07/2011 10:46:28 GMT-05:00	Papá	(313) 700-0769	00:01:07	
X	09/07/2011 10:43:33 GMT-05:00	Luis Alberto Nieto	(320) 560-4880	00:00:00	
	09/07/2011 10:40:22 GMT-05:00	Juan Carlos Restrepo	(314) 768-1328	00:02:31	
!	09/07/2011 10:35:14 GMT-05:00		(318) 827-3342	00:00:00	
!	09/07/2011 10:34:44 GMT-05:00		(318) 827-3342	00:00:00	
X	09/07/2011 10:23:55 GMT-05:00	Juan Carlos Restrepo	(314) 768-1328	00:00:00	
	09/07/2011 10:23:30 GMT-05:00	Juan Carlos Restrepo	(314) 768-1328	00:00:03	
!	09/07/2011 09:19:14 GMT-05:00	Juan Carlos Restrepo	(314) 768-1328	00:00:00	
	09/06/2011 19:00:39 GMT-05:00	Papimon	(316) 297-8625	00:09:35	
X	09/06/2011 18:02:25 GMT-05:00	Papimon	(316) 297-8625	00:00:00	
X	09/06/2011 17:23:40 GMT-05:00	Papimon	(316) 297-8625	00:00:00	
X	09/06/2011 17:17:27 GMT-05:00	Papimon	(316) 297-8625	00:00:00	
X	09/06/2011 17:14:50 GMT-05:00	Papimon	(316) 297-8625	00:00:00	
X	09/06/2011 17:14:22 GMT-05:00	Papimon	(316) 297-8625	00:00:00	
X	09/06/2011 17:14:10 GMT-05:00	Papimon	(316) 297-8625	00:00:00	
	09/06/2011 17:05:39 GMT-05:00	Jhon Cesar Arango	(314) 872-6570	00:00:46	
!	09/06/2011 16:38:05 GMT-05:00		(316) 375-7914	00:00:00	
	09/05/2011 18:34:00 GMT-05:00	Amor	(317) 437-3592	00:00:11	
	09/05/2011 17:43:55 GMT-05:00	Amor	(317) 437-3592	00:11:04	
X	09/05/2011 17:22:11 GMT-05:00	Amor	(317) 437-3592	00:00:00	
	09/05/2011 17:19:47 GMT-05:00	Amor	(317) 437-3592	00:01:49	
!	09/05/2011 16:48:26 GMT-05:00		(311) 514-3095	00:02:41	
!	09/05/2011 16:32:06 GMT-05:00	Agialejandro	(314) 777-5814	00:10:24	
	09/05/2011 15:58:46 GMT-05:00	Luis Alberto Nieto	(320) 560-4880	00:06:49	
	09/05/2011 15:53:51 GMT-05:00		(311) 514-3095	00:00:38	
!	09/05/2011 15:38:46 GMT-05:00		(311) 514-3095	00:00:00	
!	09/05/2011 15:38:04 GMT-05:00		(311) 514-3095	00:00:00	
!	09/05/2011 12:11:47 GMT-05:00		(311) 514-3095	00:00:00	



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

Prueba1.lantern

New Case Acquire Report Export Inspect Search

Case 1
Evidence 1

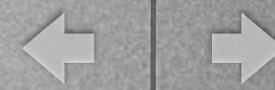
Info	Time	To/From	Number	Duration
Contacts	09/07/2011 10:46:28 GMT-05:00	Papá	(313) 700-0769	00:01:07
Calls	X 09/07/2011 10:43:33 GMT-05:00	Luis Alberto Nieto	(320) 560-4880	00:00:00
SMS/MMS	09/07/2011 10:40:22 GMT-05:00	Juan Carlos Restrepo	(314) 768-1328	00:02:31
Notes	! 09/07/2011 10:35:14 GMT-05:00		(318) 827-3342	00:00:00
Calendar	! 09/07/2011 10:34:44 GMT-05:00		(318) 827-3342	00:00:00
Internet	X 09/07/2011 10:23:55 GMT-05:00	Juan Carlos Restrepo	(314) 768-1328	00:00:00
Skype	09/07/2011 10:23:30 GMT-05:00	Juan Carlos Restrepo	(314) 768-1328	00:00:03
Voicememos	! 09/07/2011 09:19:14 GMT-05:00	Juan Carlos Restrepo	(314) 768-1328	00:00:00
Facebook	09/06/2011 19:00:39 GMT-05:00	Papimon	(316) 297-8625	00:09:35
Locations	X 09/06/2011 18:02:25 GMT-05:00	Papimon	(316) 297-8625	00:00:00
Wifi	X 09/06/2011 17:23:40 GMT-05:00	Papimon	(316) 297-8625	00:00:00
Camera	X 09/06/2011 17:17:27 GMT-05:00	Papimon	(316) 297-8625	00:00:00
Media	X 09/06/2011 17:14:50 GMT-05:00	Papimon	(316) 297-8625	00:00:00
Usage	X 09/06/2011 17:14:22 GMT-05:00	Papimon	(316) 297-8625	00:00:00
Documents	X 09/06/2011 17:14:10 GMT-05:00	Papimon	(316) 297-8625	00:00:00
Timeline	09/06/2011 17:05:39 GMT-05:00	Jhon Cesar Arango	(314) 872-6570	00:00:46
	! 09/06/2011 16:38:05 GMT-05:00		(316) 375-7914	00:00:00
	09/05/2011 18:34:00 GMT-05:00	Amor	(317) 437-3592	00:00:11
	09/05/2011 17:43:55 GMT-05:00	Amor	(317) 437-3592	00:11:04
	X 09/05/2011 17:22:11 GMT-05:00	Amor	(317) 437-3592	00:00:00
	09/05/2011 17:19:47 GMT-05:00	Amor	(317) 437-3592	00:01:49
	! 09/05/2011 16:48:26 GMT-05:00		(311) 514-3095	00:02:41
	! 09/05/2011 16:32:06 GMT-05:00	Agialejandro	(314) 777-5814	00:10:24
	09/05/2011 15:58:46 GMT-05:00	Luis Alberto Nieto	(320) 560-4880	00:06:49
	09/05/2011 15:53:51 GMT-05:00		(311) 514-3095	00:00:38
	! 09/05/2011 15:38:46 GMT-05:00		(311) 514-3095	00:00:00
	! 09/05/2011 15:38:04 GMT-05:00		(311) 514-3095	00:00:00
	! 09/05/2011 12:11:47 GMT-05:00		(311) 514-3095	00:00:00



DragonJAR.org



 **DragonJAR.org**



DragonJAR.org

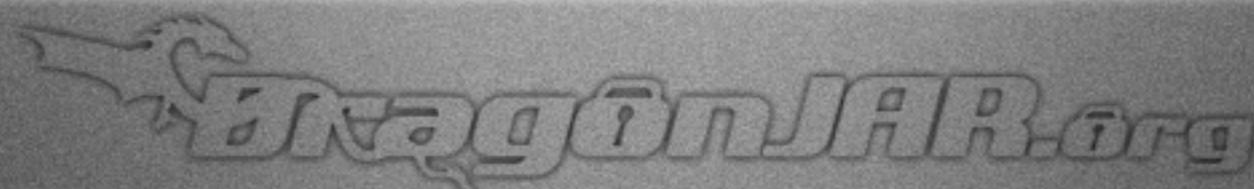


iSSH

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

```

config.dat
bplist00'      TStopX$objectsX$versionY$archiver-  TrootÄ Ø
  fghijklknvzùü†*φ•U$null"
  ZNS.objectsWNS.keysV$class° Ä ° Ä Ä Wconfigs"
  φ Ä Ä
  Ä fl (
. !"#%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJCECCNOPCPDECCDDXDPZD\CP^EEDCDCDThostXvnc_host
. YforceAnsiXrdp_port_ preferredOrientationYsendCtrlHWTunnels_ overrideTerminalType^scro
. llBackSizeXrdp_userZmacAddress\vnc_password[descriptionXencodingVuseKeyXvnc_portYuseDSA
. KeyWscModeZrdp_domain]remoteCommandXeightBit_ localLineEditingForceOffYisSectionXpass
. word[startOnOpen[connections_ keyboardOpacityVswapLFUloginTport[consoleType^connection
. Type\rdp_passwordXrdp_host]sharedSessionYsharedKey_ localEchoForceOff^useKeyFilename_
. lockOrientationÄ Ä Ä Ä Ä
  Ä »Ä Ä Ä Ä 6 Ä Ä Ä Ä
. "?Ä Ä Ä Ä Ä Ä Ä \ekoparty.orgPUDiego\ekoparty.org_ seteescapolatortuga"
  l †Ä "opquX$classesZ$classnameFirst^NSMutableArrayWNSArrayXNSObject^NSMutableArray"opwy
. †xt_ ConfigurationSetting_ ConfigurationSettingfl (
. !"#%&'()*+,-./0123456789:;<=>?@{BCDEFDÄCECCäâPCPDEäDDDäDP{D{CP^EEDCDCDÄ Ä Ä Ä Ä
  »Ä Ä Ä Ä 6Ä Ä Ä Ä "?Ä Ä Ä Ä Ä Ä Ä _ salsipuedes.com.coTroot_ salsipuedes.
. com.coWcerradoWderumbe"
  É †Ä "op†0fß@t_ NSMutableDictionary\NSDictionary_ NSMutableDictionary Ü†_ NSKeyed
. Archiver ( 2 5 : < T Z a l t { } Ä É Ö ç í î ó ô õ ö Ü , % / 7 N ] f q ~
. ä î ö é ≠ μ ¿ (E φ Ú , / 6 < A M \ i r Ä ä ü ≠ ø ; √ = Δ » Ä Ö æ - " ' ° Ÿ e > fl
. † , % Ä Ê Á È Í Ô • Ú Ù - - - - - " 8 = > @ E N Y ] l t } ä ë ï ' ~
. ! # % ' ) + - / 1 2 4 6 7 8 9 ; < A B D F H J K M N P Q f k Ä ä è ï ñ ò ù ° Σ f
. / fl
Line: 8 Column: 140 Plain Text Tab Size: 4
  
```





WordPress

SQLite Database Browser - /Volumes/Taller iOS EKO (Root)/private/var/mobile/Applications/2...

Database Structure | Browse Data | Execute SQL

Table: ZBLOG

New Record | Delete Record

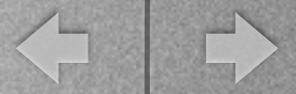
ZLASTPOSTSYN	ZPASSWORD	ZUSERNAME	ZXMLRPC	ZBLOGNAME	ZURL	ZAPIKE
1	nomostrarelpas	ekoparty	http://www.dr	La Comunidad	www.dragonjar.	

1 - 1 of 1

Go to: 0

**/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.

SQLite Database Browser - /Volumes/iPhone (Root)/private/var/mobile/Applications/D4309E4...

Database Structure Browse Data Execute SQL

Table: ZWAMESSAGE

SESSION	ZGROUPMEMBER	ZMESSAGEDATE	ZTOJID	ZFROMJID	ZTEXT	ZSTANZAID
1	1	332461893		573122030058	Entonces parce	1309153326-
2	2	555885.392574	57311	0		1312863061-
3	2	555938.805987		57311332443		1312810630-
4	2	525507.417977	57311	0	de hoy a	1312932672-
5	1	525805.432136	57312	8	anda	1312932672-
6	1	334626298		573122030058	ota	1312927514-
7	1	334626341		573122030058	a herma	1312927514-
8	1	526304.823273	5731	58	o aquí e	1312933453-
9	1	526543.639844		573122030058	pues y c	1312927514-
10	1	526581.686567	5731	58	ia	1312933453-
11	1	526587.912542	5731	58	amona	1312933453-
12	1	526607.383457		573122030058	ne imagi	1312927514-
13	1	526620.904516	5731	58	chita	1312933453-
14	1	526673.574679		573122030058		1312927514-

< 1 - 14 of 14 > Go to: 0

DragonJAR.org





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/lyjAl>

SQLite Database Browser - /Volumes/iPhone (Root)/private/var/mobile/Applications/D4309E4...

Database Structure Browse Data Execute SQL

Table: ZWAMESSAGE

ID	SESSION	ZGROUPMEMBER	ZMESSAGEDATE	ZTOJID	ZFROMJID	ZTEXT	ZSTANZAID
1	1		332461893		573122030058	Entonces parce	1309153326-
2	2		555885.392574	57311	0		1312863061-
3	2		555938.805987		57311332443		1312810630-
4	2		525507.417977	57311	0	de hoy a	1312932672-
5	1		525805.432136	57312	8	anda	1312932672-
6	1		334626298		573122030058	ota	1312927514-
7	1		334626341		573122030058	a herma	1312927514-
8	1		526304.823273	5731	58	o aquí e	1312933453-
9	1		526543.639844		573122030058	pues y c	1312927514-
10	1		526581.686567	5731	58	ia	1312933453-
11	1		526587.912542	5731	58	amona	1312933453-
12	1		526607.383457		573122030058	ne imagi	1312927514-
13	1		526620.904516	5731	58	chita	1312933453-
14	1		526673.574679		573122030058		1312927514-

1 - 14 of 14

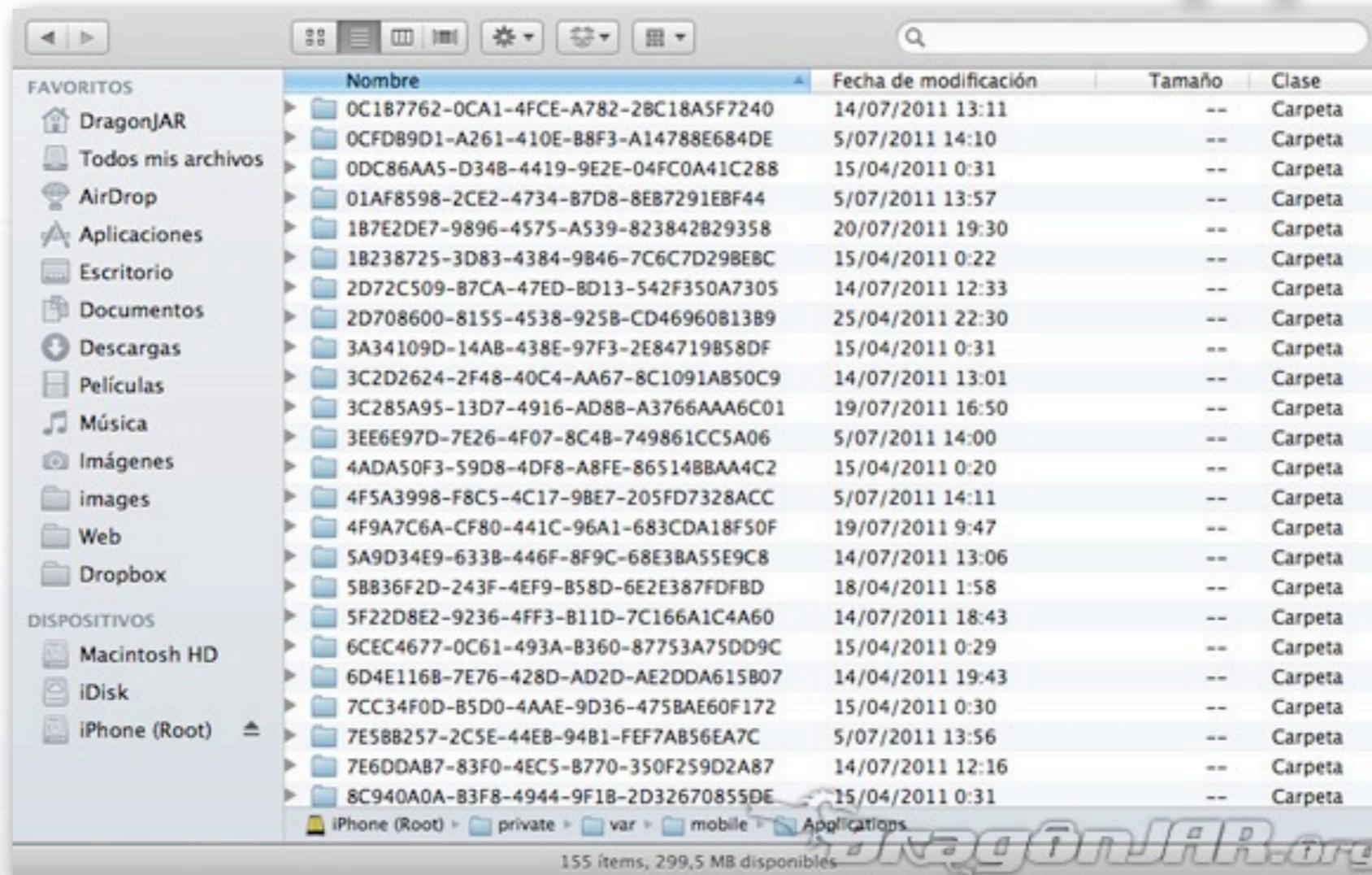
Go to: 0

DragonJAR.org





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





Dragón@DragónJAR.org

sigueme en  **twitter** @DragonJAR