

IPHONE  
LOCKED,  
UNLOCKED

Nelson Murilo  
<nelson@pangeia.com.br>



# Agenda

Motivações

Definições

Ferramentas

Limitações

Demo



# Apresentação

Interesting ports on 172.16.0.2:

Not shown: 1714 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

MAC Address: 00:23:12:XX:XX:XX (**Unknown**)

```
$ grep 00-23-12 /usr/local/etc/oui.txt
```

```
00-23-12 (hex)
```

```
Apple, Inc
```

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

# Motivações

- Análise forense em iphone
- Existem 3 tipos atualmente:
  - Desbloqueados por hardware (chip)
  - Desbloqueados por software (jailbroken)
  - **Bloqueados (non-jailbroken)**

# Motivações

Claro e Vivo confirmam: Lançamento iPhone dia 26/09/2008.

Sexta-feira, 26 de Setembro de 2008

**PRETA GIL QUER UM IPHONE "G3"**



**Faustão anuncia iPod 3G da Claro**

Postado em 14 out 2008 por Antino Silva

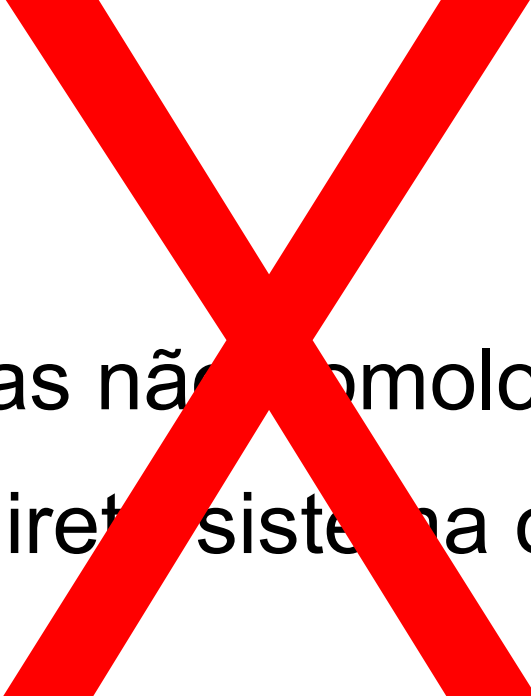


# Iphone jailbroken

- Funções adicionais
  - MMS
  - Modem
  - Programas não homologados pela Apple
  - Acesso direto ao sistema operacional
  - SSH
  - etc.



# Iphone Bloqueado

- Funções adicionais
    - MMS
    - Modem
    - Programas não homologados
    - Acesso direto ao sistema operacional
    - SSH
    - etc.
- 



# Iphone Bloqueado

- (Quase) todo acesso é feito pelo Itunes
- Acesso limitado
  - Áreas de armazenamendo de fotos





# Protocolo

Toda a comunicação entre um computador e o iPhone é feita via uma interface chamada Apple File Communication Protocol (AFC) via porta USB

Usado para sincronismo e instalação de atualizações de firmware

Acesso somente à segunda partição (media folder)



# Protocolo

## Protocolos via USB

`dfu` - Dev Firmware Update/Recovery

`iboot` - Usado para recovery

`Layered communications` - Comunicação multiplexada usada em operação normais (sincronia)

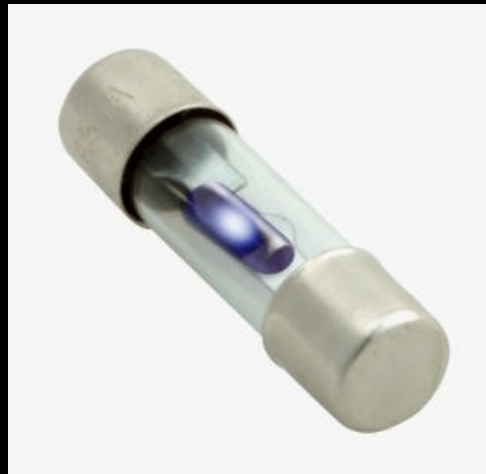
# Filesystems

## Block Devices

---

disk0	iPhone flash memory (4, 8 or 16GB)
disk0s1	OS partition. Stores / root file system.
disk0s2	User space. Stores Music, Photos, Videos, Podcasts, Ringtones and Apps. Mounted as /private/var.

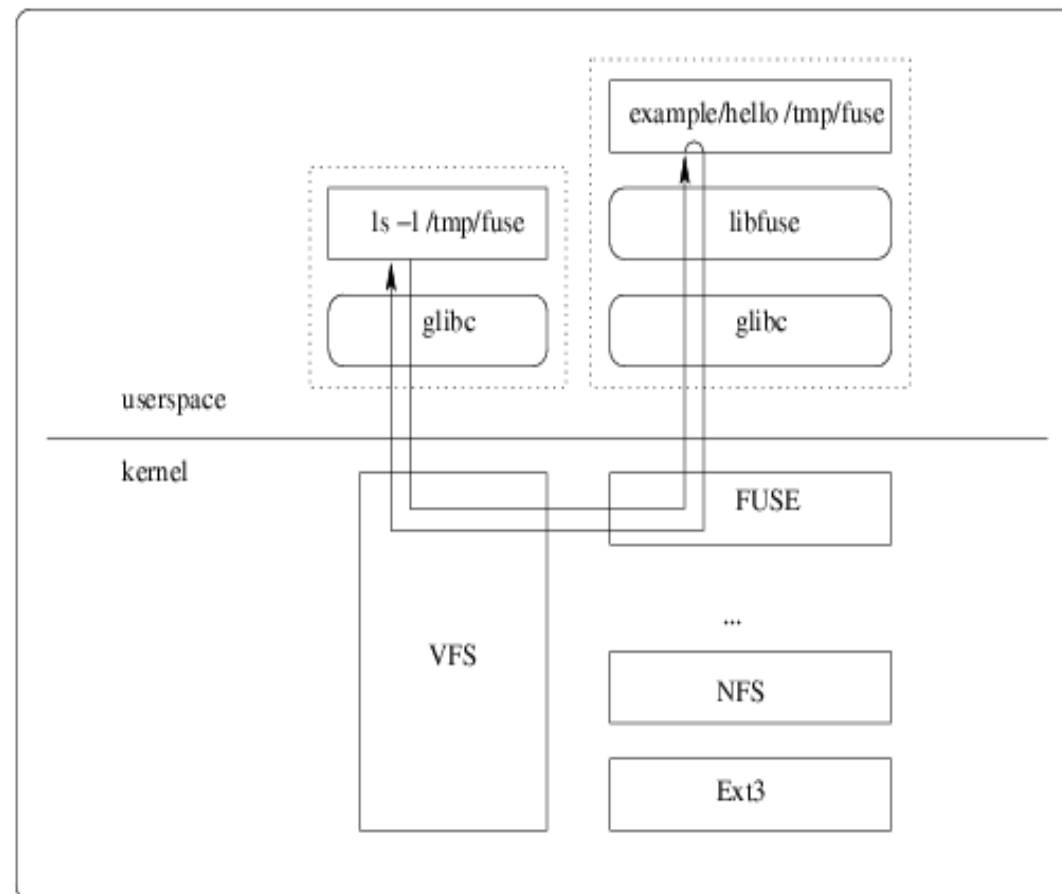
# Fuse filesystem



# Filesystems

## How does it work?

The following figure shows the path of a filesystem call (e.g. `stat`) in the above *hello world* example:



# Filesystems

```
# modprobe fuse
```

```
# lsmod | grep fuse
```

```
fuse                43836    2
```

```
#
```



# Filesystems

Main Page - iFuse - Iceweasel

[View](#) [History](#) [Bookmarks](#) [Tools](#) [Help](#)

 [http://matt.colyer.name/projects/iphone-linux/index.php?title=Main\\_Page](http://matt.colyer.name/projects/iphone-linux/index.php?title=Main_Page) 

[Main Page](#)

[Protocol Documentation](#)

[Create an iTunes Trace](#)

[Code](#)

[Recent Changes](#)

## iFuse and libiphone

**iFuse** allows you to mount an iPhone or iPod Touch under Linux using the USB cable. You can view and edit the files similar to a normal USB disk drive. iFuse does not require "jailbreaking" or voiding your warranty and works *without* needing extra software installed on the phone (such as `ssh`).

### What is it?

**libiphone** is a software library that talks the native Apple USB protocols that the iPhone uses. Unlike other projects, `libiphone` does not depend on using any existing `.dll` or `.so` libraries from Apple.

**iFuse** is a **FUSE filesystem** driver which **uses `libiphone` to connect to devices without jailbreak**. iFuse is using the native Apple "AFC" protocol, over the normal USB cable in order to access the iPhone's (or iPod Touch's) media files under Linux.

**e**

an iPhone or iPod Touch under Linux using the USB cable. You can view and edit the files similar to what you can do on a Mac. This tool does not require "jailbreaking" or voiding your warranty and works *without* needing extra software installed on the device.

A library that talks the native Apple USB protocols that the iPhone uses. Unlike other projects, `libiphon` does not use any existing `.dll` or `.so` libraries from Apple.

A driver which uses `libiphone` to connect to devices without jailbreak. `iFuse` is using the native Apple USB protocols to connect to the iPhone via a USB cable in order to access the iPhone's (or iPod Touch's) media files under Linux.



# Filesystems

```
# mkdir ~/iphone
# ~/fnt/libiphone/src/ifuse -s ~/iphone
# mount
[...]
lt-ifuse on ~/iphone type fuse.lt-ifuse
(rw,nosuid,nodev)

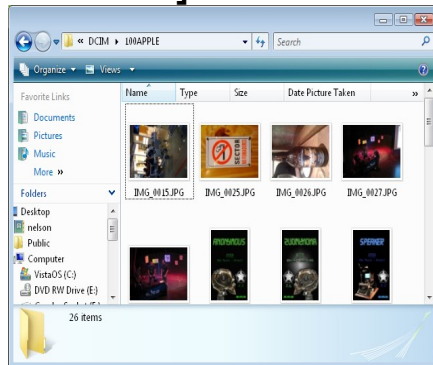
# ls -AFC ~/iphone
ApplicationArchives/
DCIM/
iTunes_Control/
Purchases/
com.apple.itunes.lock_sync
Downloads/
Photos/
```

# Diretórios

**DCIM**

**100APPLE**

[ Fotos e imagens salvas ]



**999APPLE**

[ ScreenShots ]



**.MISC**

[ Temporários ]



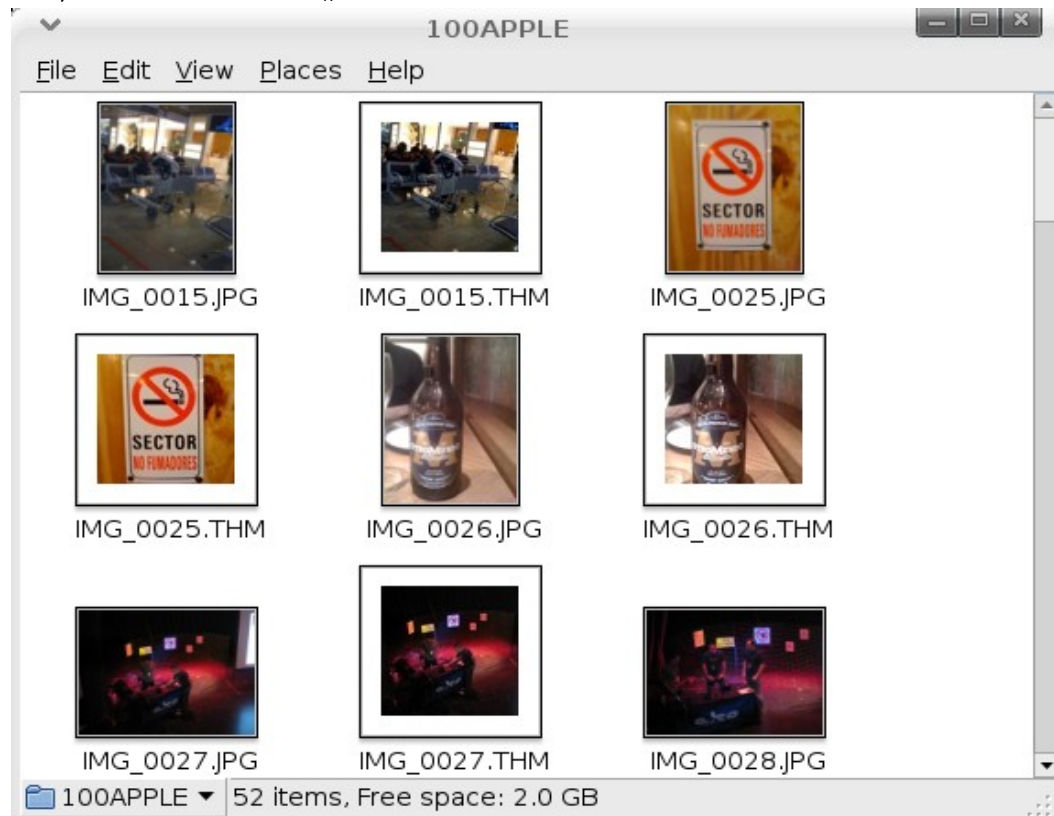
# Iphorensics

```
:~/iphone/DCIM/100APPLE# ls
```

```
IMG_0027.THM  IMG_0035.JPG  IMG_0039.THM  IMG_0048.JPG
```

```
IMG_0052.THM  IMG_0028.JPG  IMG_0035.THM  IMG_0044.JPG
```

```
:~/iphone/DCIM/100APPLE# nautilus .
```

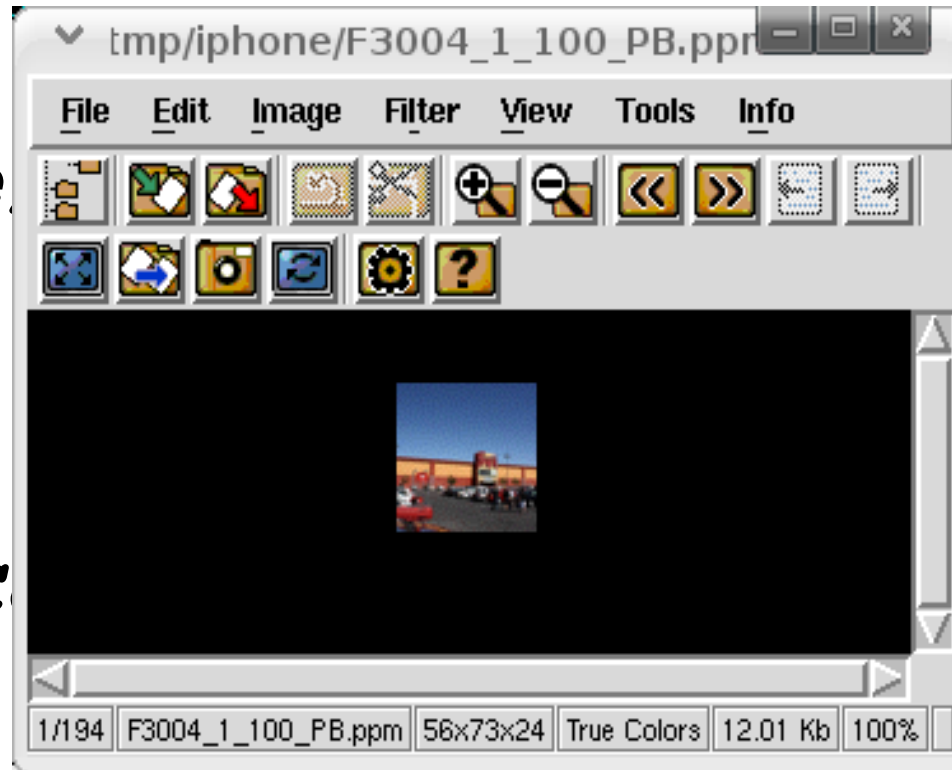


# Iphorensics

```
$ ls ~/iphone  
F3004_1.itmb  
F3009_1.itmb
```

```
$ wine iThmbC mb
```

```
$ xnvview *.ppm
```



# Iphorensics

File Edit View History Bookmarks Tools Help

http://www.apple.com/iphone/features/photos.html

Store Mac iPod + iTunes iPhone Downloads Support Search

## iPhone 3G


Features App Store iTunes Gallery Tech Specs Find a Store Buy iPhone 3G

- Home Screen
- Phone
- Mail
- Safari
- iPod
- SMS
- Maps with GPS
- iTunes
- App Store
- Calendar
- YouTube
- Photos + Camera**
- Stocks, Weather, Notes
- Calculator

### Photos + Camera

With a built-in camera and an advanced photo application, iPhone is the most photo-friendly phone ever. It takes snapshots, automatically syncs photos with your PC or Mac, displays albums with the flick of a finger, and posts pictures directly to a MobileMe Gallery.

**See Photos in action.**  
[Watch the demo](#)



**Snap photos.**

Done

# Iphorensics

The image is a screenshot of a web browser window displaying the Apple website's 'iPhone 3G' features page, specifically focusing on GPS. The browser's address bar shows the URL <http://www.apple.com/iphone/features/gps.html>. The page header includes navigation links for 'Store', 'Mac', 'iPod + iTunes', 'iPhone', 'Downloads', and 'Support', along with a search bar. The main content area features a vertical list of iPhone applications on the left, including Home Screen, Phone, Mail, Safari, iPod, SMS, Maps with GPS, iTunes, App Store, Calendar, YouTube, Photos + Camera, Stocks, Weather, Notes, and Calculator. The central focus is a large image of an iPhone 3G. The phone's screen displays a Google Maps interface with a search for 'Pizza' and a location marker for 'John's Pizzeria'. To the right of the phone is a screenshot of the iPhone's 'Settings' application, specifically the 'General' settings page. The 'Location Services' option is highlighted and turned 'ON'. Other settings visible include 'About', 'Usage' (9m), 'Network', 'Bluetooth' (Off), 'Auto-Lock' (1 Minute), 'Passcode Lock' (Off), and 'Restrictions' (Off). The text 'GPS and beyond.' is positioned below the phone image. The browser's status bar at the bottom left shows the word 'Done'.

Apple - iPhone - Features - GPS - Iceweasel

File Edit View History Bookmarks Tools Help

<http://www.apple.com/iphone/features/gps.html>

Store Mac iPod + iTunes iPhone Downloads Support Search

## iPhone 3G

Features App Store iTunes Gallery Tech Specs Find a Store Buy iPhone 3G

- Home Screen
- Phone
- Mail
- Safari
- iPod
- SMS
- Maps with GPS
- iTunes
- App Store
- Calendar
- YouTube
- Photos + Camera
- Stocks, Weather, Notes
- Calculator

**GPS and beyond.**

Settings General

- About
- Usage 9m
- Network
- Bluetooth Off
- Location Services **ON**
- Auto-Lock 1 Minute
- Passcode Lock Off
- Restrictions Off

Done

# Iphorensics

```
# exif IMG_0056.JPG
```

```
EXIF tags in 'IMG_0056.JPG' ('Motorola' byte order):
```

```
-----+-----  
Tag                |Value  
-----+-----  
Manufacturer       |Apple  
Model              |iPhone  
Orientation        |right - top  
Date and Time      |2008:11:14 16:17:12  
Compression        |JPEG compression  
Date and Time (origi|2008:11:14 16:17:12  
Date and Time (digit|2008:11:14 16:17:12  
[...]  
North or South Latit|S  
Latitude          |12.00, 59.13, 0.00  
East or West Longitu|W  
Longitude         |38.00, 27.07, 0.00
```

```
-----+-----  
EXIF data contains a thumbnail (9764 bytes).
```

# Iphorensics

```
North or South Latit|S
Latitude             |12.00, 59.13, 0.00
East or West Longitu|W
Longitude            |38.00, 27.07, 0.00
```

***\$ bc -l***

bc 1.06.94

Copyright 1991-1994, 1997, 1998, 2000, 2004, 2006 Free  
Software Foundation, Inc.

This is free software with ABSOLUTELY NO WARRANTY.

For details type `warranty'.

**12+59.13/60**

**12.98550000000000000000**

**38+27.07/60**

**38.451166666666666666**



# Iphorensics

-12.9855,-38.45117 - Google Maps - Iceweasel

File Edit View History Bookmarks Tools Help

http://maps.google.com/

Google Maps

Search Maps [Show search options](#)

Get Directions My Maps

**-12° 59' 7.80", -38° 27' 4.21"**

Explore this area

Photos

More photos, videos, and user-created maps

**-12.985500, -38.451170**  
-12° 59' 7.80", -38° 27' 4.21"  
Get directions: [To here](#) - [From here](#)  
[Search nearby](#) - [Save to My Maps](#)

Av. Tancredo Neves  
Av. Prof. Manoel Ribeiro  
Av. Paulo VI  
Praça Flávio Eduardo Pereira de Souza  
Lagoa dos Prades  
Praça Aquarius  
Área Verde

©2008 Google - Map data ©2008 MapLink/Tele Atlas - [Terms of Use](#)

# Iphorensics

## **# exif IMG\_0027.JPG**

EXIF tags in 'IMG\_0027.JPG' ('Motorola' byte order):

Tag	Value
Orientation	top - left
x-Resolution	72.00
y-Resolution	72.00
Compression	JPEG compression
Orientation	top - left
x-Resolution	72.00
y-Resolution	72.00
PixelXDimension	1024
PixelYDimension	768

EXIF data contains a thumbnail (6293 bytes).

hagnarok:~/iphone/DCIM/100APPLE#

# Futuro





View



- Summary
- Info
- Ringtones
- Music
- Photos
- Podcasts
- Video
- Applications

## iPhone



**Name:** nmor

**Capacity:** 14,64 GB

**Software Version:** 2.1

**Serial Number**

## Version

Your iPhone software is up to date. iTunes will automatically check for an update again on 17/11/2008.

Check for Update

If you are experiencing problems with your iPhone, you can restore its original settings by clicking Restore.

Restore

## Options

Automatically sync when this iPhone is connected

Sync only checked songs and videos

Manually manage music and videos

# Futuro

- Engenharia reversa da rotina de update (backup e instalação)



Engenharia reversa da aplicação que instala aplicações (AppStore)

# Futuro

```
~/iphone/iTunes_Control/iTunes# file *
Extras.itdb: SQLite 3.x database
IC-Info.sidb: TTComp archive data
IC-Info.sidv: raw G3 data, byte-padded
iTunesApplicationIDs: data
iTunesControl: empty
iTunesDB: data
iTunesMovies: data
iTunesPlaylists: data
iTunesPodcasts: data
iTunesPrefs: data
iTunesRingtones: data
PhotosFolderAlbums: data
PhotosFolderName: data
PhotosFolderPrefs: data
PlayCounts.plist: Apple binary property list
Rentals.plist: XML document text
Ringtones.plist: XML document text
```

# Protocolo

## Melhor voodoo

`dfu` - Dev Firmware Update/Recovery

`iboot` - Usado para recovery

# Q & A

