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

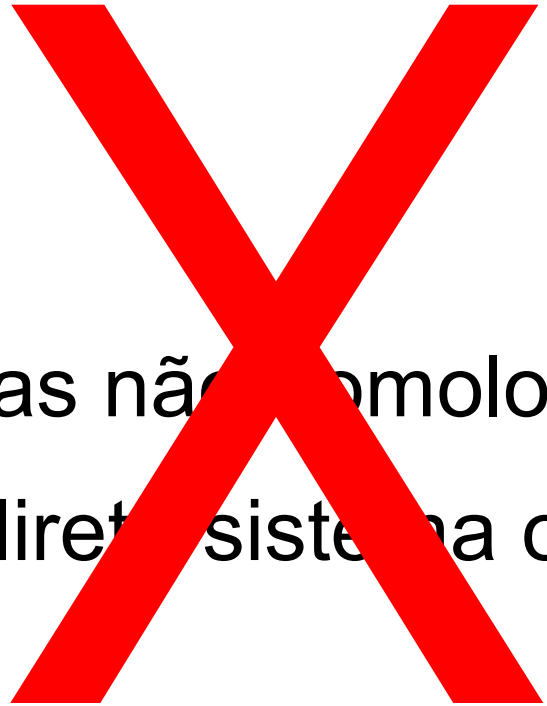
Postado em 14 out 2008 por Antino Silva

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

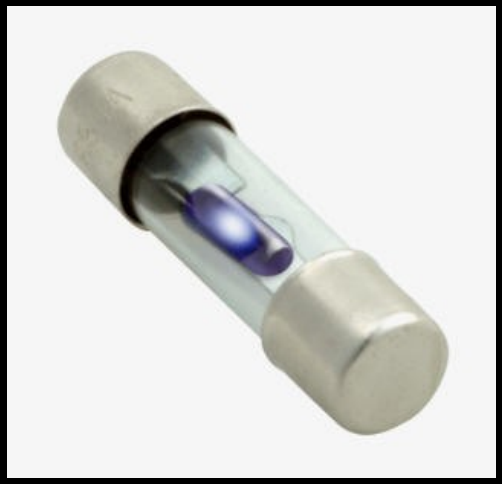
Layered communications - Comunicação mutiplexada usada em operação normais (sincronia)

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.

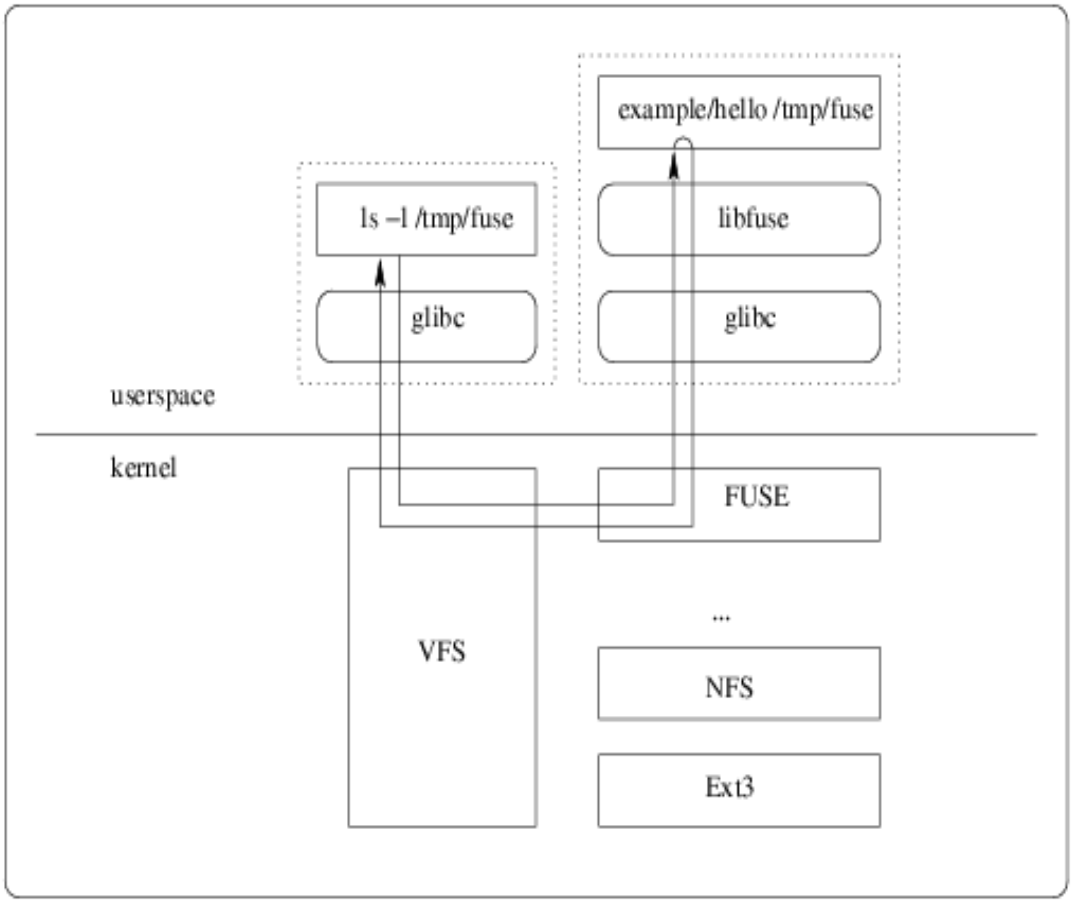
Fuse filesystem



Filesystems

How does it work?

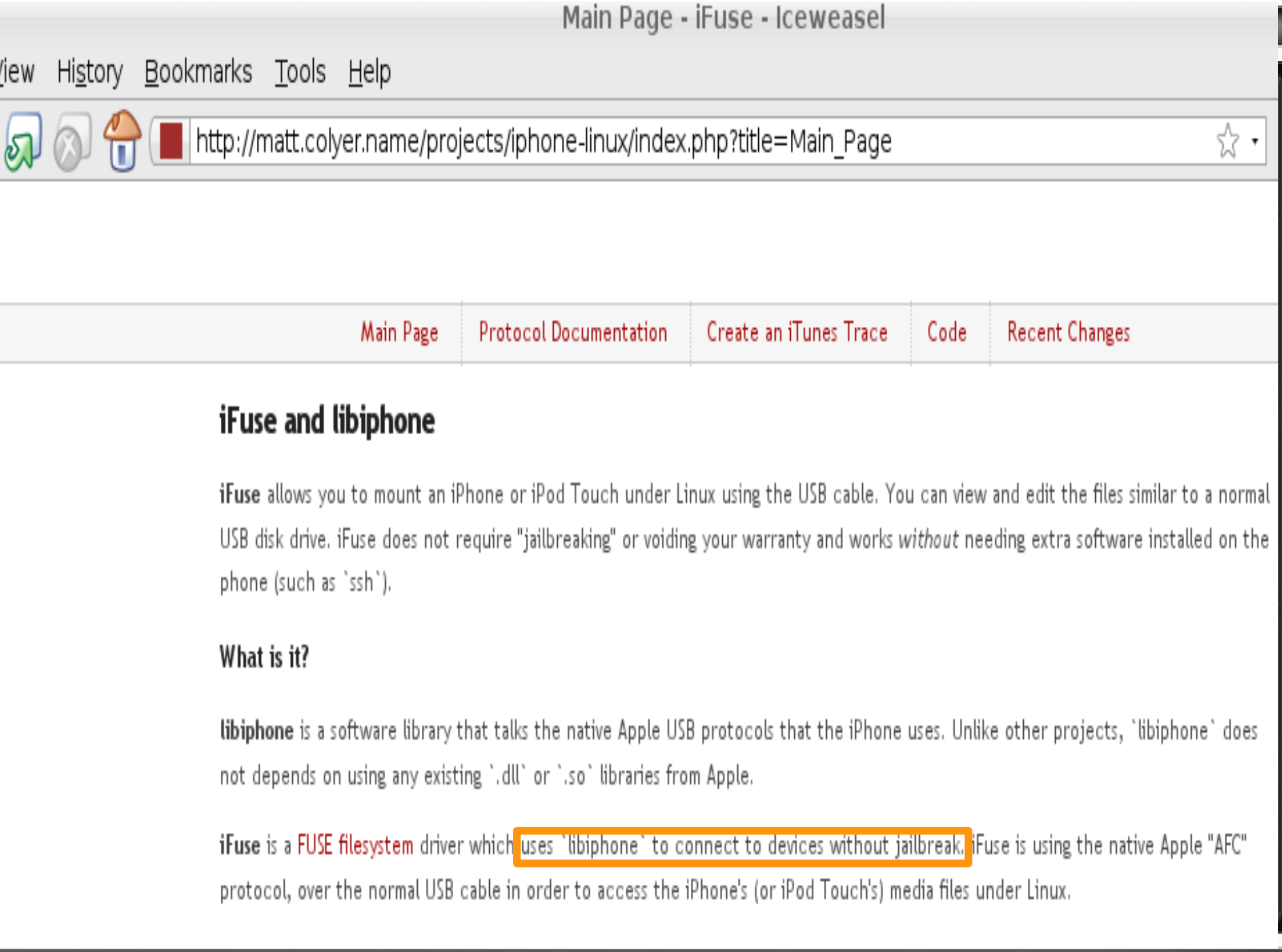
The following figure shows the path of a filesystem call (e.g. stat) in the above *hello world* example:



Filesystems

```
# modprobe fuse
# lsmod | grep fuse
fuse                   43836  2
#
```

Filesystems



e

an iPhone or iPod Touch under Linux using the USB cable. You can view and edit the files similar t

not require "jailbreaking" or voiding your warranty and works *without* needing extra software install

rary that talks the native Apple USB protocols that the iPhone uses. Unlike other projects, `libipho

existing `.dll` or `.so` libraries from Apple.

driver which uses `libiphone` to connect to devices without jailbreak. iFuse is using the native Appl

USB cable in order to access the iPhone's (or iPod Touch's) media files under Linux.

Filesystems

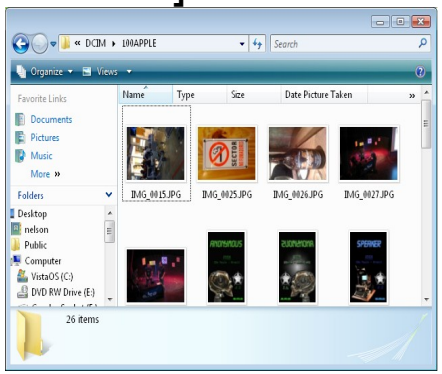
```
# mkdir ~/iphone
# ~/fnt/libiphone/src/ifuse -s ~/iphone
# mount
[...]
lt-ifuse on ~/iphone type fuse.lt-ifuse
(rw,nosuid,nodev)

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

Diretórios

DCIM

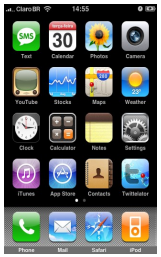
100APPLE

[Fotos e imagens salvas]



999APPLE

[ScreenShots]

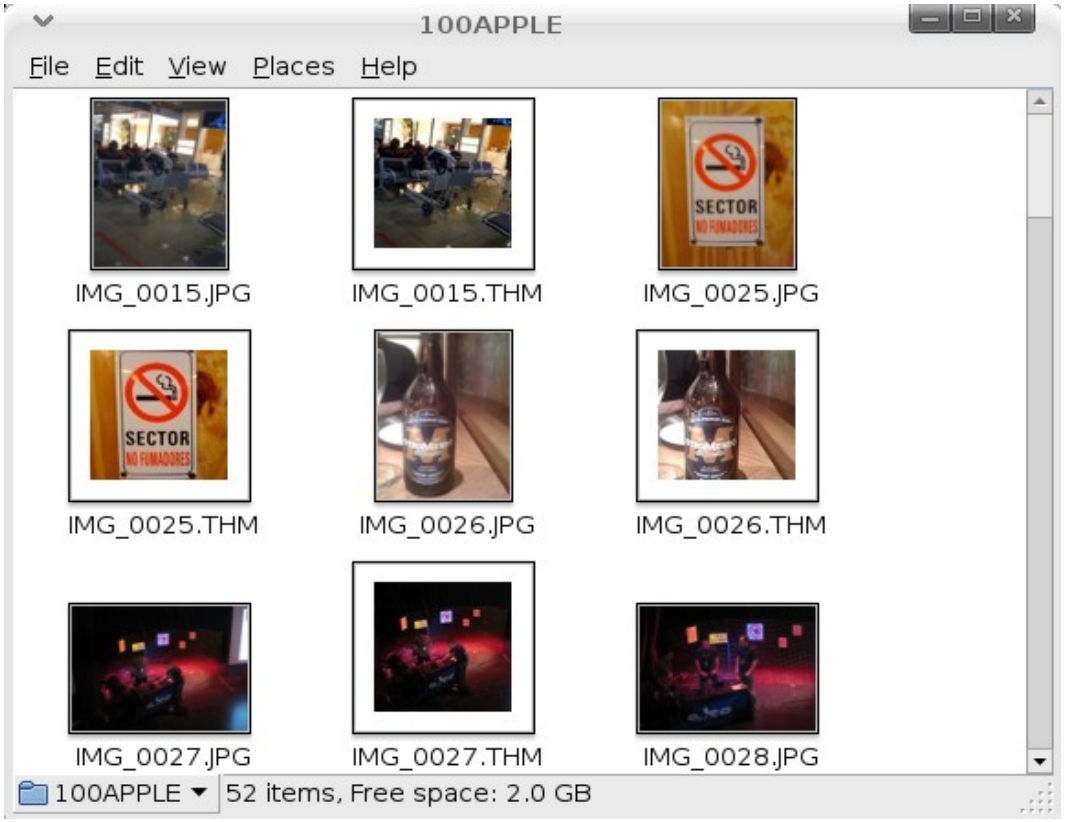


.MISC

[Temporários]

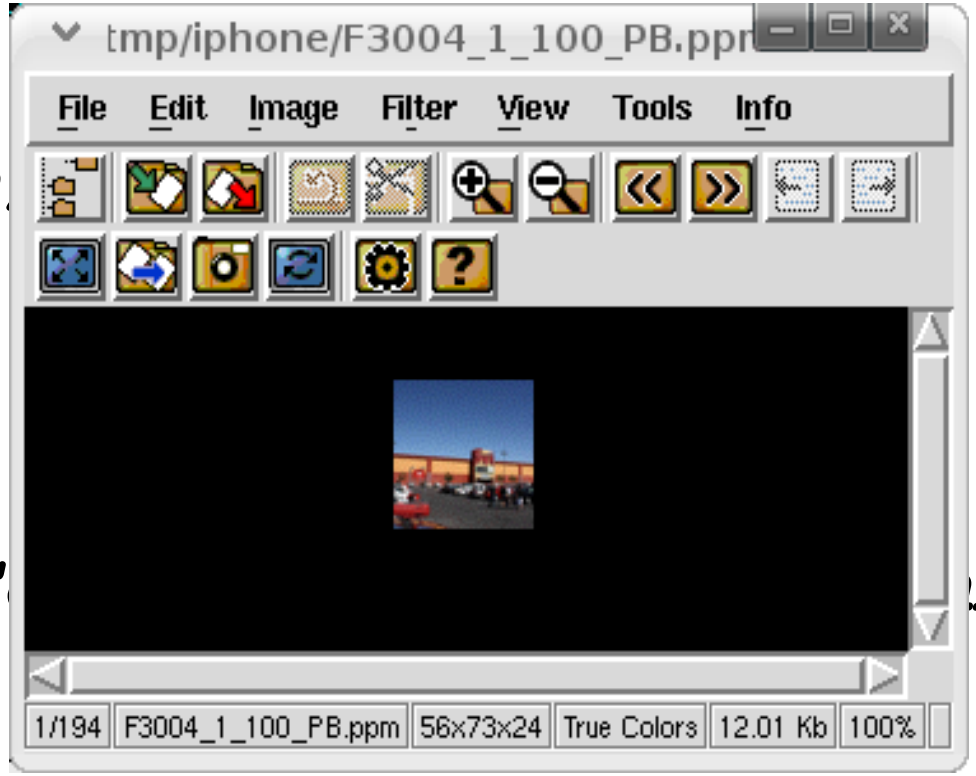
Iphorensics

```
:~/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 .
```

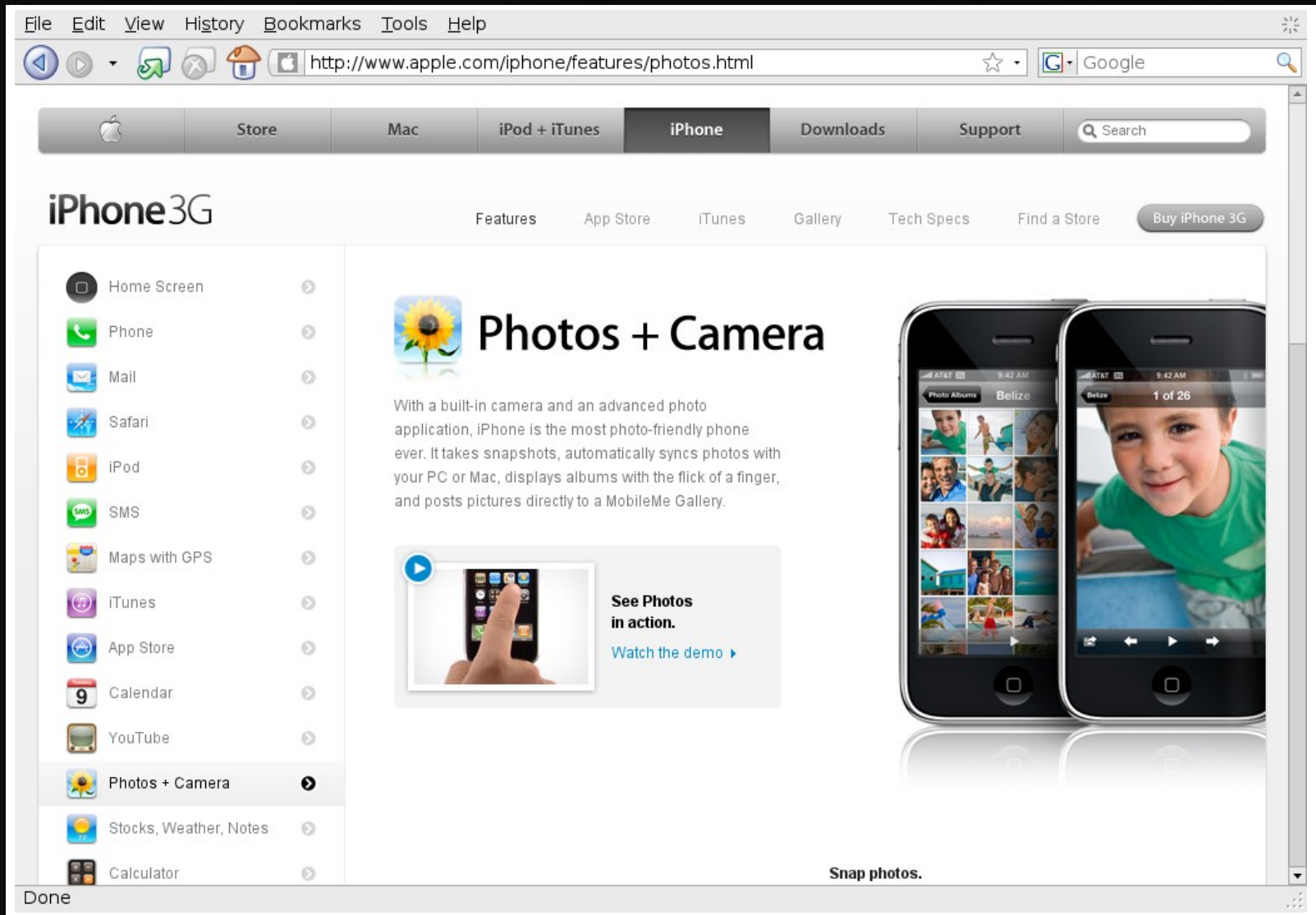


Iphorensics

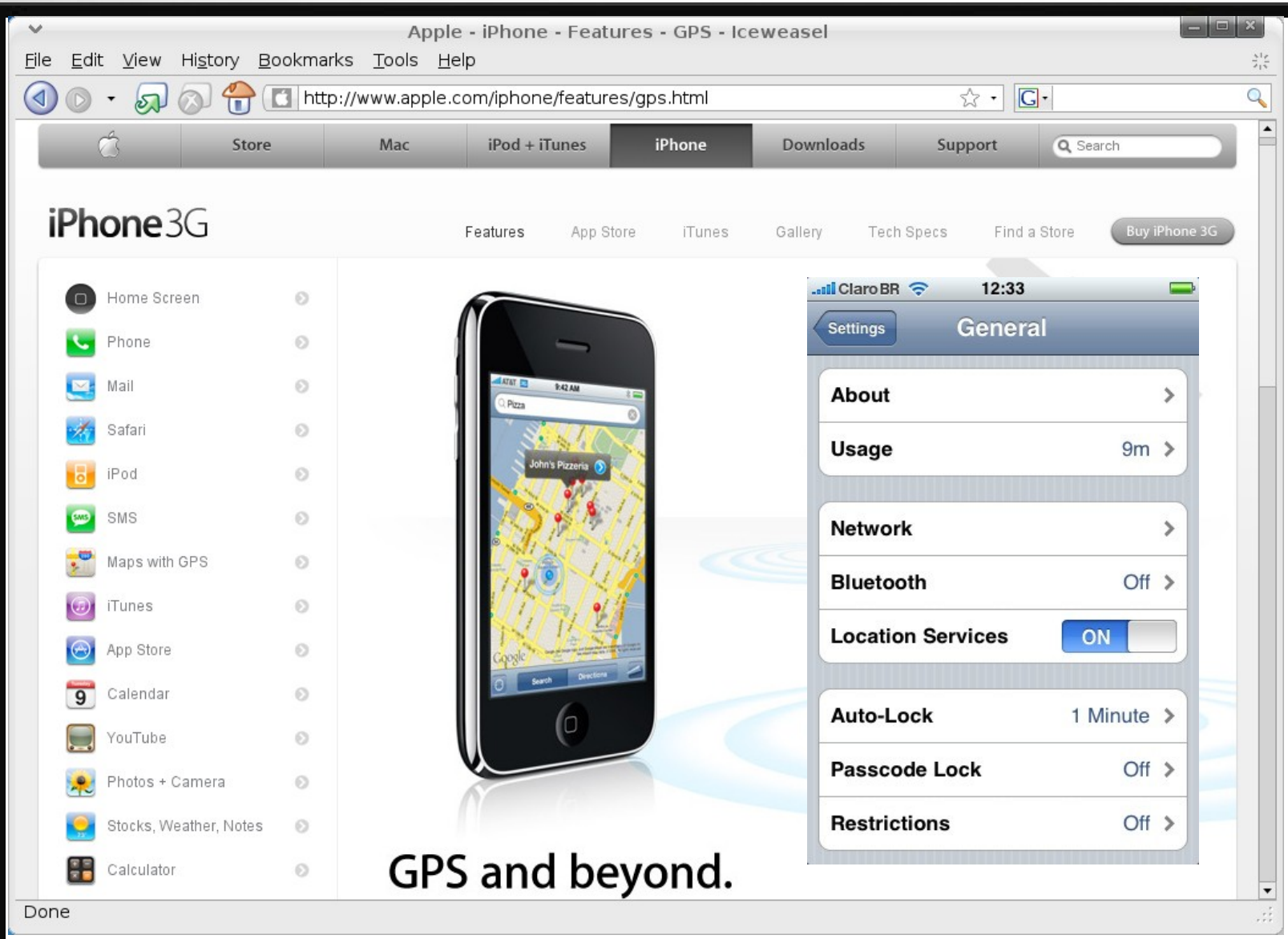
```
$ ls ~/iphone
F3004_1.ithmb
F3009_1.ithmb

$ wine iThmbC                    mb

$ xnview *.ppm
```



Iphorensics



Iphorensics



Iphorensics

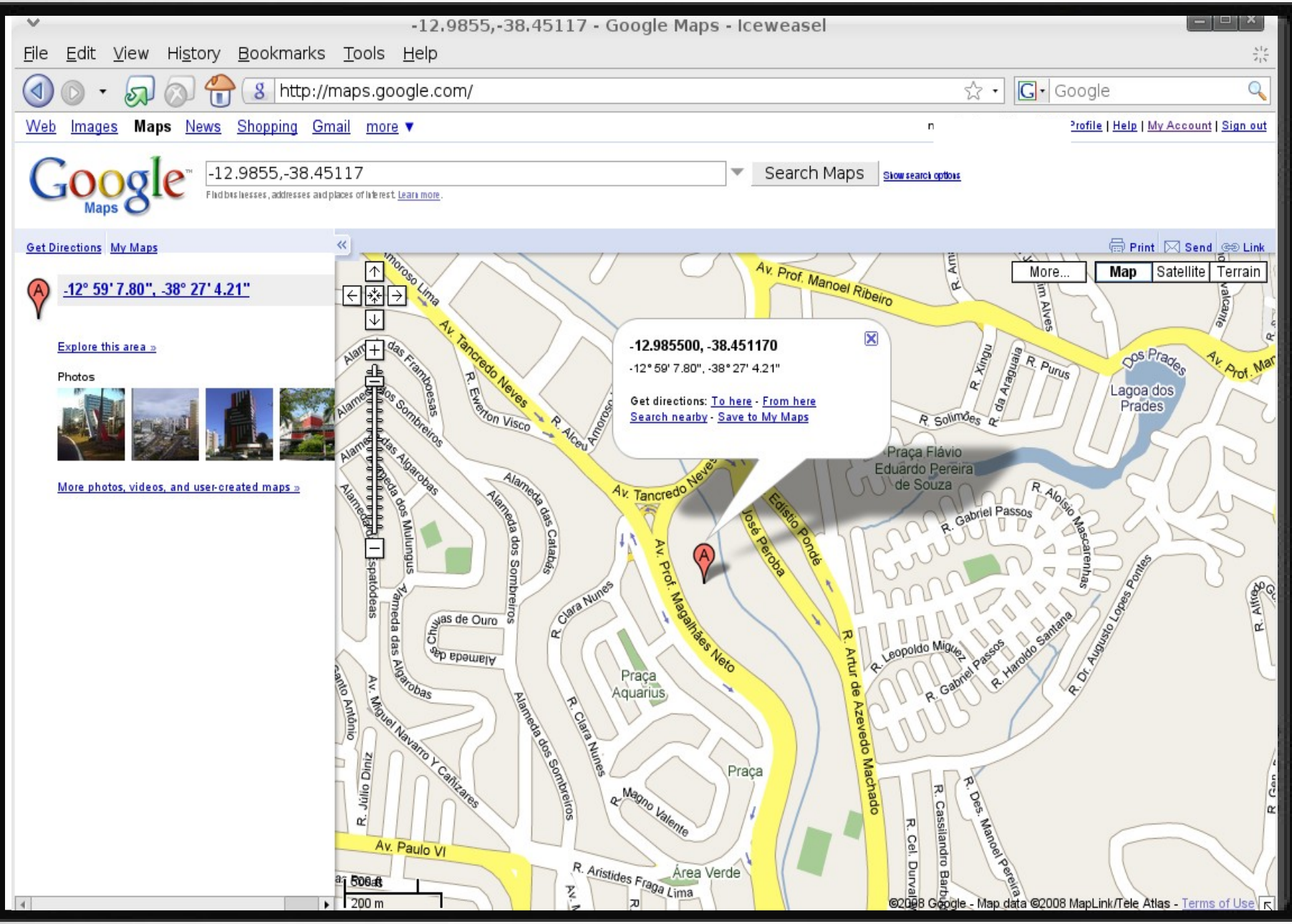
```
# exif IMG_0056.JPG
EXIF tags in 'IMG_0056.JPG' ('Motorola' byte order):
---------------------+-------------------------------------
Tag                  |Value
---------------------+-------------------------------------
Manufacturer         |Apple
Model                |iPhone
Orientation          |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
38.45116666666666666666
```

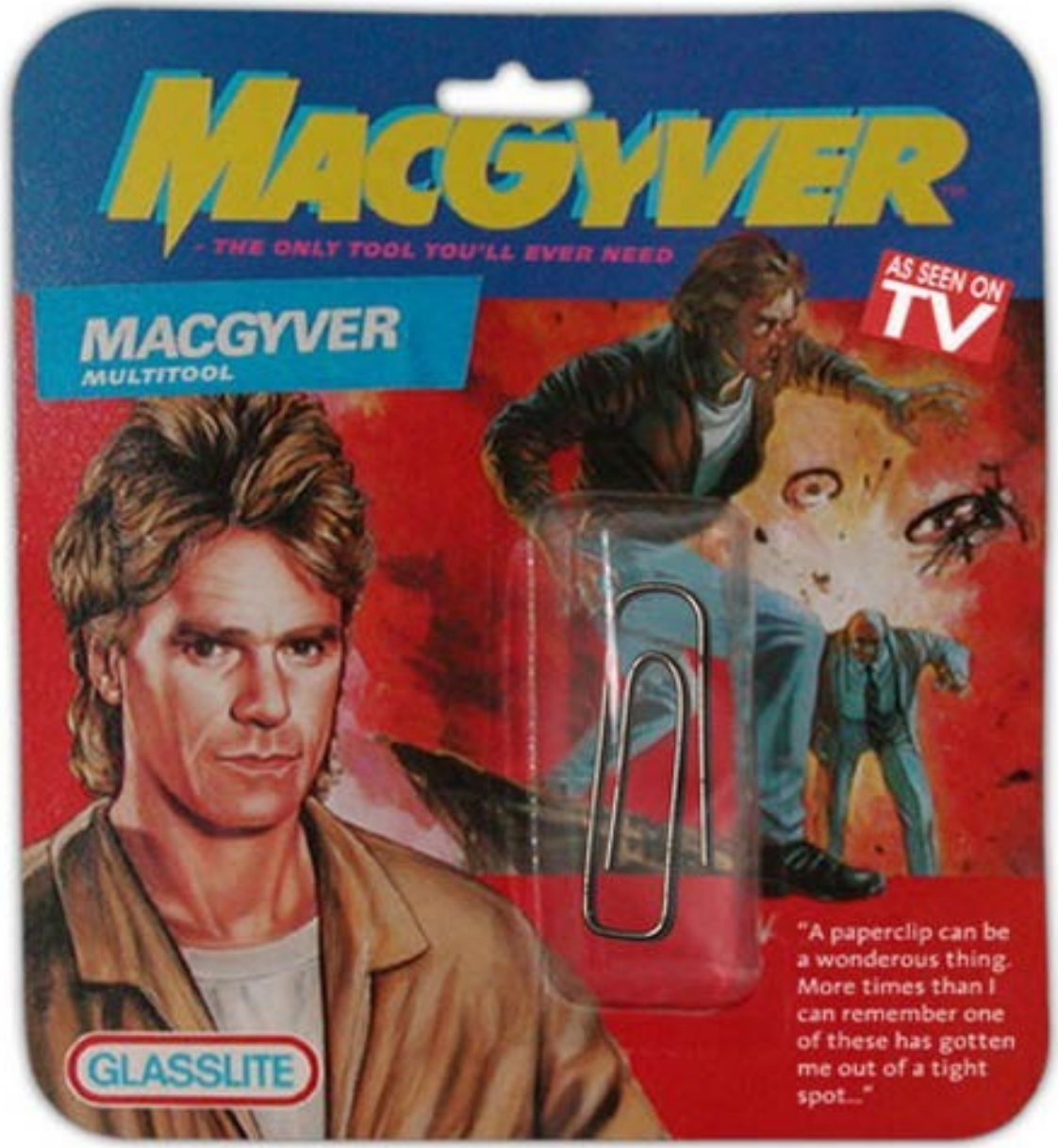
Iphorensics



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


MACGYVER
- THE ONLY TOOL YOU'LL EVER NEED
AS SEEN ON TV
MACGYVER
MULTITOOL
GLASSLITE
"A paperclip can be a wonderous thing. More times than I can remember one of these has gotten me out of a tight spot..."

rols Store Advanced Help

iTunes

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.

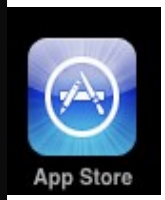
Restore

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