

# Aula 08

# Forense Computacional

## Caso 1

# Agenda

---

- ✓ E-mail dos alunos (Vagner)
- ✓ Baixar evidências
- ✓ Ler documentos;
- ✓ Aplicar os conhecimentos;
- ✓ Responder as questões do caso;

- ✓ O sistema em questão é um caso fictício, que foi criado para aplicar os conhecimentos e ferramentas utilizadas em uma investigação.
- ✓ Sua missão é analisar o conteúdo de um disquete apreendido e responder algumas perguntas. O que torna este desafio único, é que você vai precisar de ler o relatório policial antes de continuar o desafio.
- ✓ Assim como em uma investigação real, você terá algumas informações para utilizar como base e algumas evidências, mas cabe a você com suas habilidades técnicas, descobrir as respostas.

- ✓ O arquivo image.zip, pode ser baixado do site da disciplina ou ftp do Professor:

[http://professor.unisinos.br/pneukamp/arquivos/Forense-2012\\_1/Aula-8.zip](http://professor.unisinos.br/pneukamp/arquivos/Forense-2012_1/Aula-8.zip)

<ftp://pneukamp.dyndns.info/caso1.zip>

Neste arquivo constam a imagem a ser periciada e mais algumas informações relevantes sobre o caso!

✓ Perguntas que devem ser respondidas:

1. Quem é o fornecedor de maconha de Joe Jacob e qual é o endereço do seu fornecedor?
2. Quais dados cruciais estão disponível no arquivo coverpage.jpg e por que é esses dados cruciais?
3. Quais (se houver) outras escolas além de Smith Hill, Joe Jacobs é visto freqüente?
4. Para cada evidência, demonstre os procedimentos e ações adotadas pelo suspeito para mascará-los?
5. Que processos você (o investigador) usou para examinar o conteúdo de cada evidência?

- ✓ **Conferir o MD5 da Imagem**

```
# md5sum image.zip > image.md5
```

***Comparar a saída “image.md5” com a fornecida com a documentação***

- ✓ **Descompactar a imagem para iniciar a perícia**

```
# unzip image.zip
```

```
# ls -lh
```

- ✓ **Dar uma rápida olhada no conteúdo da imagem**

```
# strings -e s image > strings.txt
```

```
# file image
```

- ✓ **Ver o conteúdo da Imagem**

```
# hexdump -C image
```

- ```
# ls -alh /mnt
```

```
drwxr-xr-x 2      root      root      7168      Dec 31 1969 ./
drwxr-xr-x 21     root      root      4096      Oct 12 15:30 ../
-rwxr-xr-x 1      root      root      15585     Sep 11 08:30 cover\page.jpgc\| | | | | | | | | *
-rwxr-xr-x 1      root      root      1000      May 24 08:20 schedu~1.exe*
```

✓ **Fazer uma cópia dos arquivos para uma pasta “ /home/fdtk/Aula8/caso1”**

✓ `# cp /mnt/* /home/fdtk/Aula8/caso1`

✓ **Ver o tipo e detalhes dos arquivos**

✓ `# file /home/fdtk/Aula8/caso1/*`

✓ **Ver o conteúdo dos arquivos**

✓ `# hexdump -C “caso1/cover page.jpgc” | less`

✓ `# hexdump -C caso1/schedu~1.exe | less`



✓ Como o Linux permite descompactar arquivos exe, o que tem dentro dele?

✓ `# unzip -v caso1/schedu~1.exe`

*latter case the central directory and zipfile comment will be found on the last disk(s) of this archive.*

✓ Putz! Agora ferrou!!! Esta dizendo que não encontrou a assinatura, que não se trata de um arquivo zipado ou que é um disco de um conjunto formado por mais partes.....

✓ **Vamos tentar algo diferente**

# *mkdir fix*

# *cp caso1/schedu~1.exe fix*

# *cd fix*

# *zip -F schedu~1.exe*

*zip: reading Scheduled Visits.xls*

*zip warning: schedu~1.exe would be truncated.*

*Retry with option -qF to truncate, with -FF to attempt full recovery*

# *zip -FF schedu~1.exe*

*zip: reading Scheduled Visits.xls compressed size 2282, actual size 950 for Scheduled Visits.xls*

*zip warning: schedu~1.exe has been truncated.*

✓ E agora, como será que ficou o arquivo?

```
# unzip -v schedu~1.exe
```

Archive: schedu~1.exe

| Length | Method | Size  | Ratio | Date     | Time  | CRC-32   | Name                 |
|--------|--------|-------|-------|----------|-------|----------|----------------------|
| -----  | -----  | ----- | ----- | ----     | ----  | -----    | ----                 |
| 16896  | Defl:N | 938   | 94%   | 05-23-02 | 11:20 | 8d6055c7 | Scheduled Visits.xls |
| -----  | -----  | ---   | ----- |          |       |          |                      |
| 16896  |        | 938   | 94%   |          |       |          | 1 file               |

✓ Tentamos novamente?

```
$ unzip schedu~1.exe
```

Archive: schedu~1.exe

```
[schedu~1.exe] Scheduled Visits.xls password:
```

Qual senha usar? Tentei algumas!!!!

```
password incorrect--reenter:
```

```
skipping: Scheduled Visits.xls
```

```
incorrect password
```

# Caso 1

✓ Voltei a imagem para procurar algo como senha!!

```
# cd /home/fdtk/aula8/
```

```
# hexdump -C image | grep passwd
```

```
# hexdump -C image | grep pass
```

```
# hexdump -C image | grep pw
```

```
00cec0 ...(...(...(...(...(..... 00cf00
.....pw=goodtimes..... 00cf40 .....
```

```
$ unzip schedu~1.exe
```

```
Archive: schedu~1.exe [schedu~1.exe] Scheduled Visits.xls password: goodtimes
```

```
inflating: Scheduled Visits.xls
```

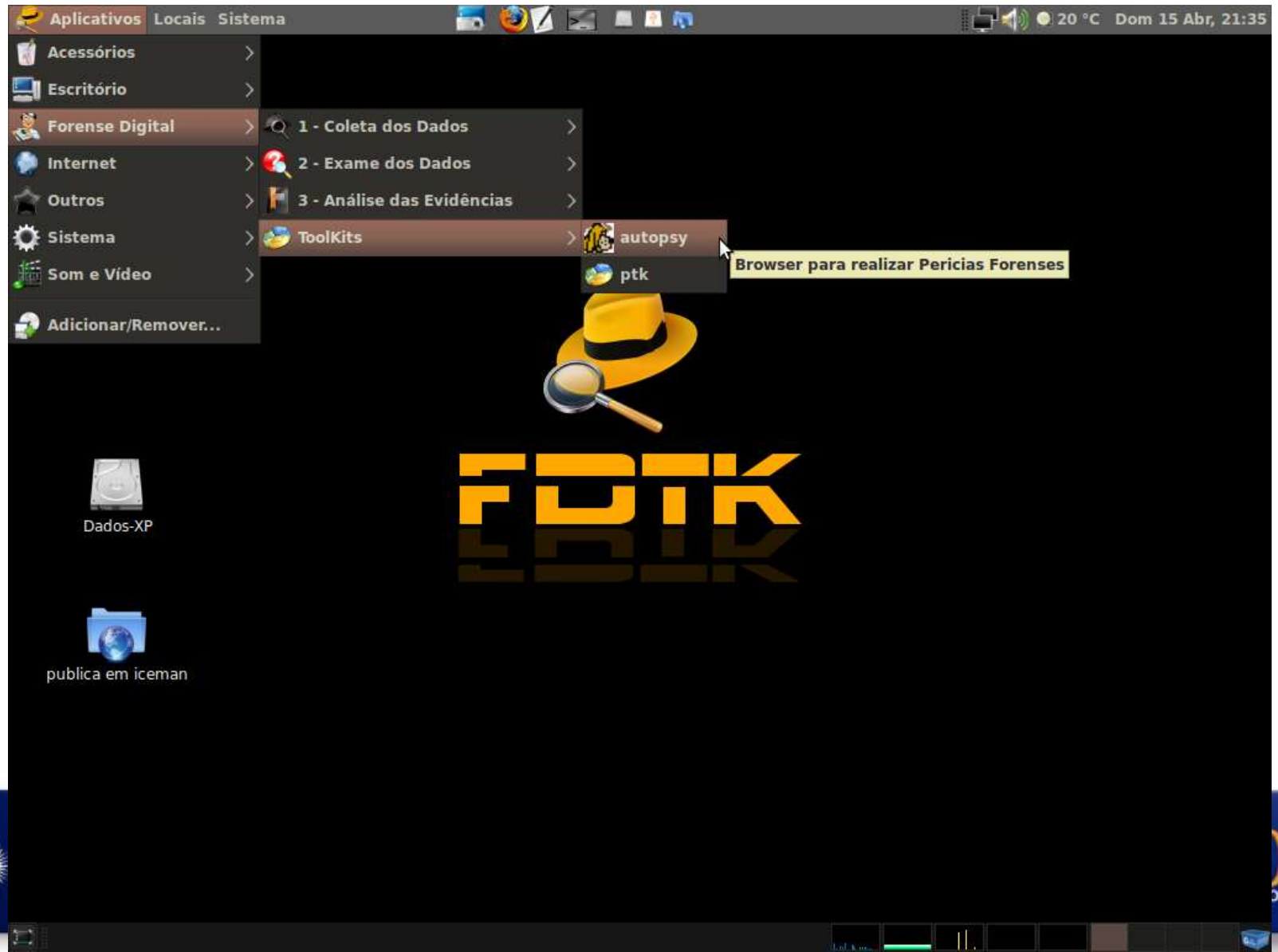
```
error: invalid compressed data to inflate
```

```
$ ls -l "Scheduled Visits.xls"
```

```
-rwxr-xr-x  1          root      root      0          May 23   11:20    Scheduled\ Visits.xls*
```

## ✓ Tentando com o autopsy

# Caso 1



WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

## Autopsy Forensic Browser 2.24

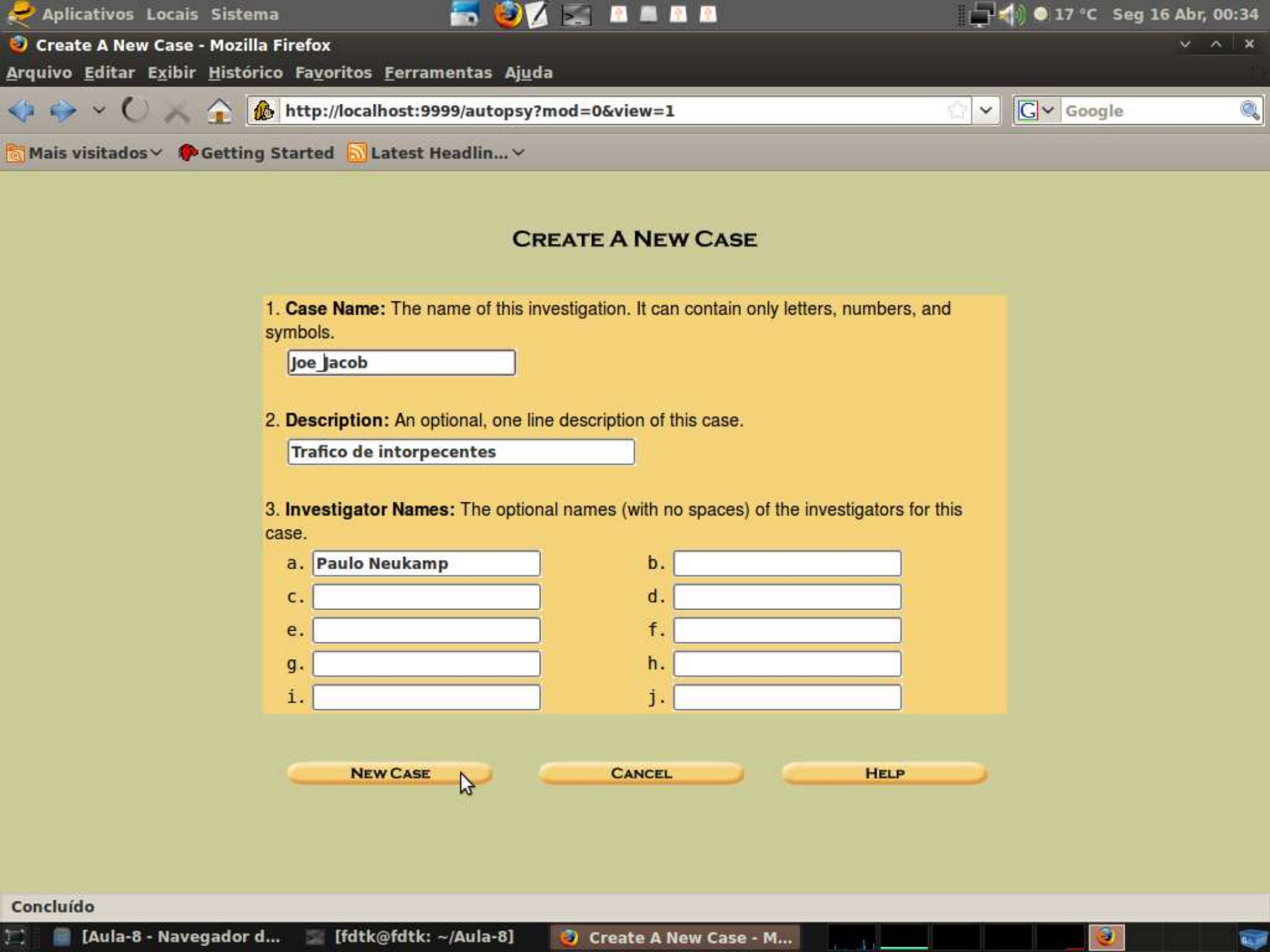


<http://www.sleuthkit.org/autopsy/>

OPEN CASE

NEW CASE

HELP



## CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

Joe Jacob

2. **Description:** An optional, one line description of this case.

Tráfico de intorpecentes

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. Paulo Neukamp

b.

c.

d.

e.

f.

g.

h.

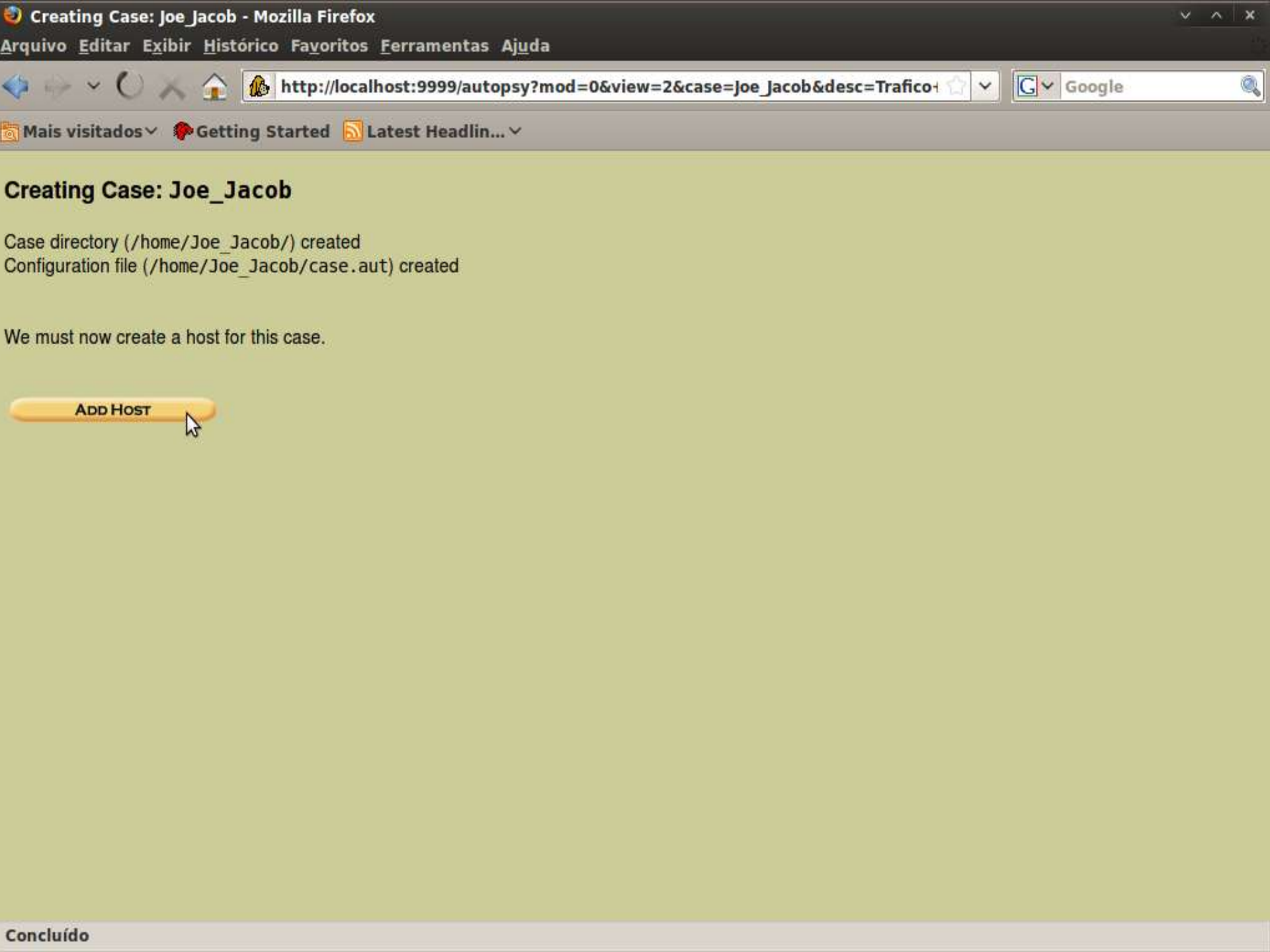
i.

j.

NEW CASE

CANCEL

HELP



## Creating Case: Joe\_Jacob

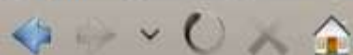
Case directory (/home/Joe\_Jacob/) created

Configuration file (/home/Joe\_Jacob/case.aut) created

We must now create a host for this case.

ADD HOST





Case: Joe\_Jacob

## ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

ADD HOST

CANCEL

HELP

## Adding host: Disk1 to case Joe\_Jacob


Host Directory (/home/Joe\_Jacob/Disk1/) created

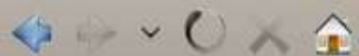
Alert Database has not been indexed - it will be as an md5sum file

---

Configuration file (/home/Joe\_Jacob/Disk1/host.aut) created

We must now import an image file for this host

**ADD IMAGE** 



Case: Joe\_Jacob

Host: Disk1

No images have been added to this host yet

Select the Add Image File button below to add one

ADD IMAGE FILE

CLOSE HOST

HELP

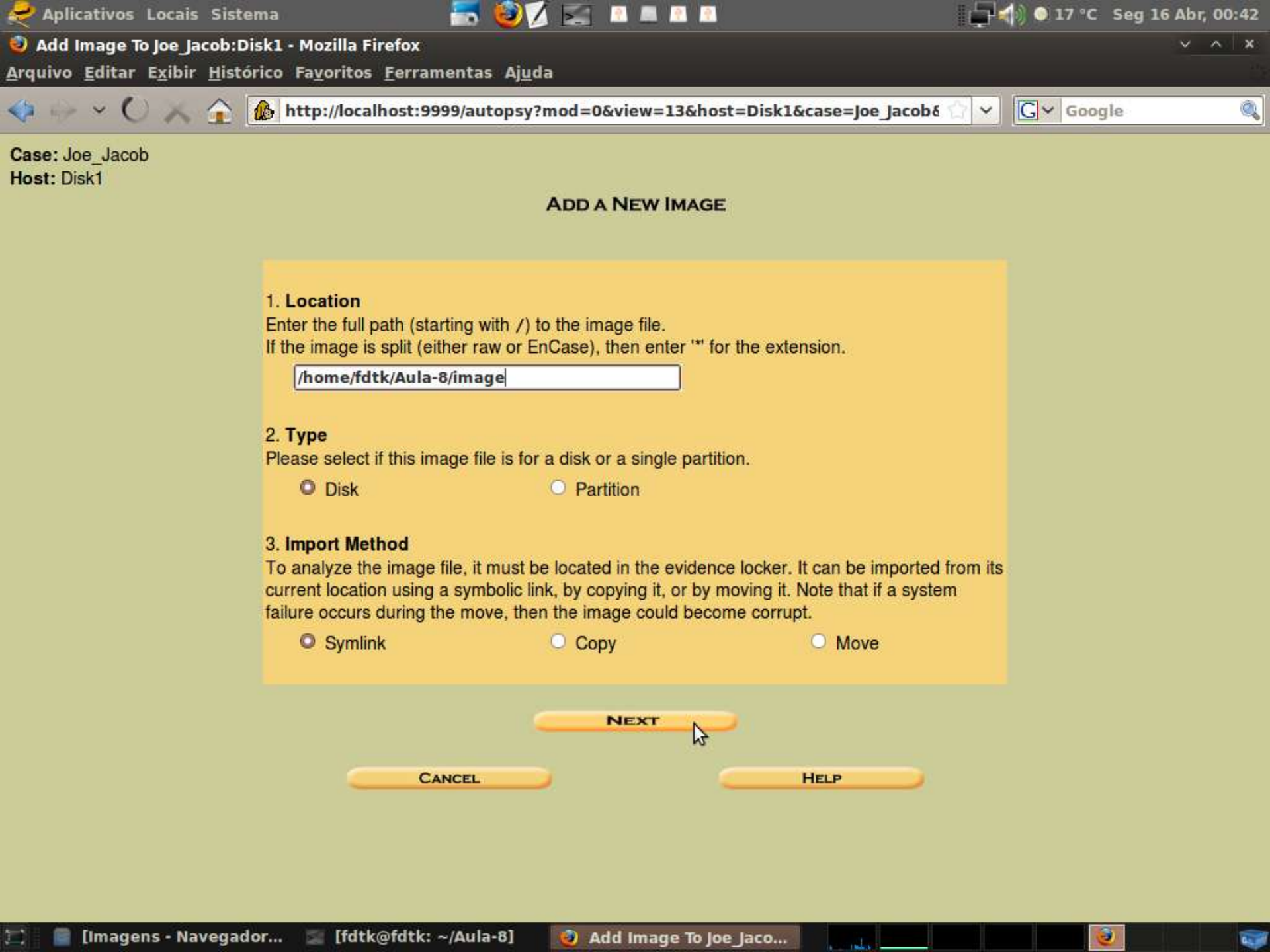
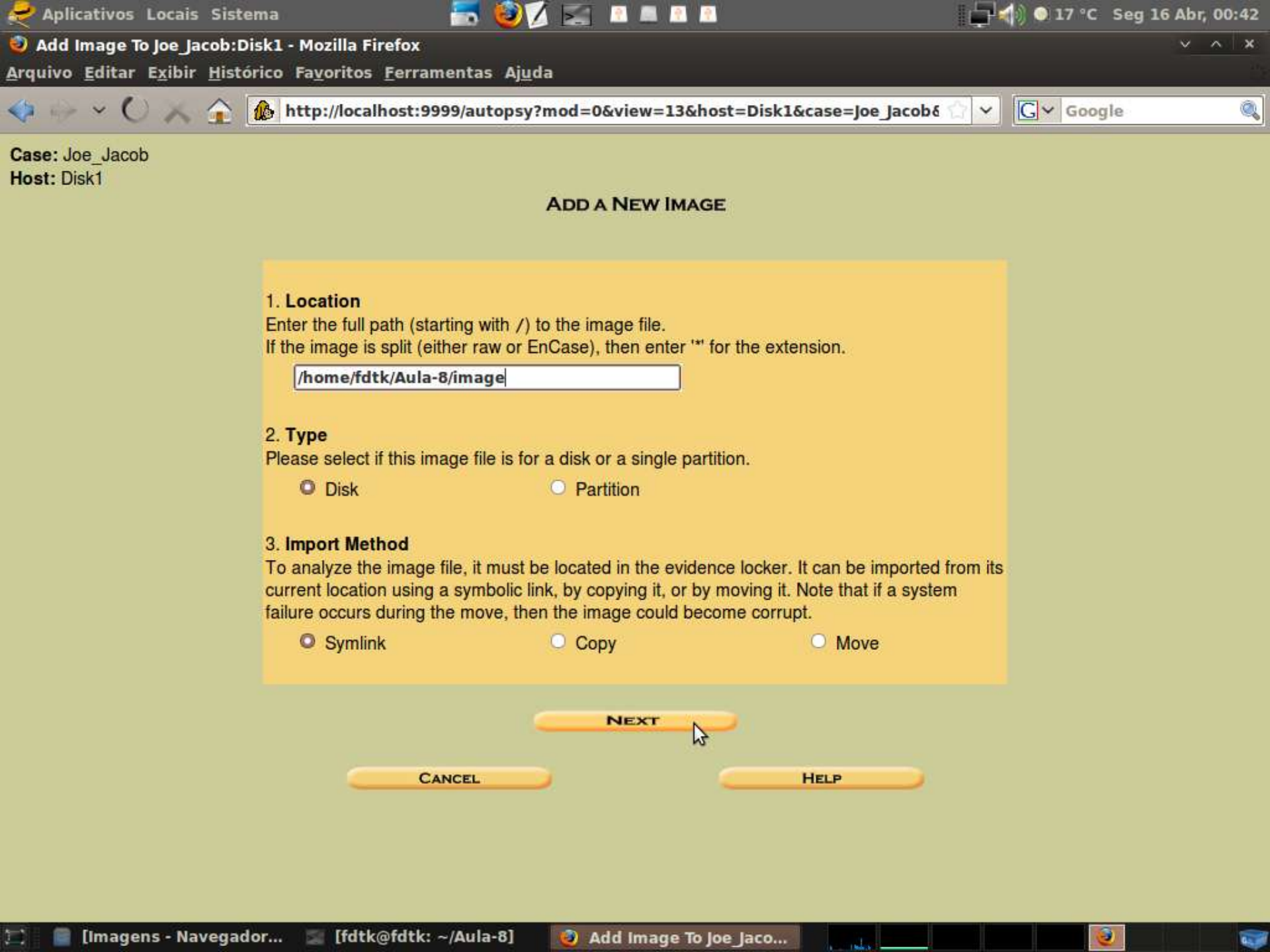
FILE ACTIVITY TIME LINES

IMAGE INTEGRITY

HASH DATABASES

VIEW NOTES

EVENT SEQUENCER



## Image File Details

**Local Name:** images/image

**Data Integrity:** An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

- ☐ Ignore the hash value for this image.
- ☐ Calculate the hash value for this image.
- ☒ Add the following MD5 hash value for this image:

b676147f63923e1f428131d59b1d6a72

☒ Verify hash after importing?

## File System Details

Analysis of the image file shows the following partitions:

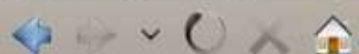
ADD

CANCEL

HELP

For your reference, the mmls output was the following:





FILE ANALYSIS

KEYWORD SEARCH

FILE TYPE

IMAGE DETAILS

META DATA

DATA UNIT

HELP

CLOSE

## Directory Seek

Enter the name of a directory that you want to view.

C: /

VIEW

## File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

|         |                                          |                              |                              |                              |       |   |   |                       |
|---------|------------------------------------------|------------------------------|------------------------------|------------------------------|-------|---|---|-----------------------|
| v / v   | <a href="#">\$FAT1</a>                   | 0000-00-00<br>00:00:00 (UTC) | 0000-00-00<br>00:00:00 (UTC) | 0000-00-00<br>00:00:00 (UTC) | 4608  | 0 | 0 | <a href="#">45780</a> |
| v / v   | <a href="#">\$FAT2</a>                   | 0000-00-00<br>00:00:00 (UTC) | 0000-00-00<br>00:00:00 (UTC) | 0000-00-00<br>00:00:00 (UTC) | 4608  | 0 | 0 | <a href="#">45781</a> |
| v / v   | <a href="#">\$MBR</a>                    | 0000-00-00<br>00:00:00 (UTC) | 0000-00-00<br>00:00:00 (UTC) | 0000-00-00<br>00:00:00 (UTC) | 512   | 0 | 0 | <a href="#">45779</a> |
| d / d   | <a href="#">\$OrphanFiles/</a>           | 0000-00-00<br>00:00:00 (UTC) | 0000-00-00<br>00:00:00 (UTC) | 0000-00-00<br>00:00:00 (UTC) | 0     | 0 | 0 | <a href="#">45782</a> |
| r / r   | <a href="#">cover<br/>page.jpgc</a>      | 2002-09-11<br>08:30:52 (BRT) | 2002-09-11<br>00:00:00 (BRT) | 2002-09-11<br>08:50:27 (BRT) | 15585 | 0 | 0 | <a href="#">8</a>     |
| ✓ r / r | <a href="#">Jimmy<br/>Jungle.doc</a>     | 2002-04-15<br>14:42:30 (BRT) | 2002-09-11<br>00:00:00 (BRT) | 2002-09-11<br>08:49:49 (BRT) | 20480 | 0 | 0 | <a href="#">5</a>     |
| r / r   | <a href="#">Scheduled<br/>Visits.exe</a> | 2002-05-24<br>08:20:32 (BRT) | 2002-09-11<br>00:00:00 (BRT) | 2002-09-11<br>08:50:38 (BRT) | 1000  | 0 | 0 | <a href="#">11</a>    |

## File Browsing Mode

In this mode, you can view file and directory contents.

File contents will be shown in this window.

More file details can be found using the Metadata link at the end of the list (on the right).

You can also sort the files using the column headers

FILE ANALYSIS

KEYWORD SEARCH

FILE TYPE

IMAGE DETAILS

META DATA

DATA UNIT

HELP

CLOSE

## Directory Seek

Enter the name of a directory that you want to view.

C: /

VIEW

## File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

|         |                                          |                              |                              |                              |       |   |   |                       |
|---------|------------------------------------------|------------------------------|------------------------------|------------------------------|-------|---|---|-----------------------|
| d / d   | <a href="#">sorphanFiles/</a>            | 0000-00-00<br>00:00:00 (UTC) | 0000-00-00<br>00:00:00 (UTC) | 0000-00-00<br>00:00:00 (UTC) | 0     | 0 | 0 | <a href="#">45/82</a> |
| r / r   | <a href="#">cover<br/>page.jpgc</a>      | 2002-09-11<br>08:30:52 (BRT) | 2002-09-11<br>00:00:00 (BRT) | 2002-09-11<br>08:50:27 (BRT) | 15585 | 0 | 0 | <a href="#">8</a>     |
| ✓ r / r | <a href="#">Jimmy<br/>Jungle.doc</a>     | 2002-04-15<br>14:42:30 (BRT) | 2002-09-11<br>00:00:00 (BRT) | 2002-09-11<br>08:49:49 (BRT) | 20480 | 0 | 0 | <a href="#">5</a>     |
| r / r   | <a href="#">Scheduled<br/>Visits.exe</a> | 2002-05-24<br>08:20:32 (BRT) | 2002-09-11<br>00:00:00 (BRT) | 2002-09-11<br>08:50:38 (BRT) | 1000  | 0 | 0 | <a href="#">11</a>    |

ASCII ([display](#) - [report](#)) \* Hex ([display](#) - [report](#)) \* ASCII Strings ([display](#) - [report](#)) \* [Export](#) \* [Add Note](#)

File Type: Microsoft Office Document Microsoft Word Document

Deleted File Recovery Mode

ASCII String Contents Of File: C:/Jimmy Jungle.doc

bjbj

Jimmy Jungle

626 Jungle Ave Apt 2

Jungle, NY 11111

Jimmy:

Dude, your pot must be the best

it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when yo

These kids, they tell me marijuana isn

t addictive, but they don

t stop buying from me. Man, I

m sure glad you told me about targeting the high school students. You must have some experience. It

s like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I

m an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!

I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you

Thanks,

Joe



FILE ANALYSIS

KEYWORD SEARCH

FILE TYPE

IMAGE DETAILS

META DATA

DATA UNIT

HELP

CLOSE



## Keyword Search of Allocated and Unallocated Space

Enter the keyword string or expression to search for:



pw

pw=

☒ ASCII ☐ Unicode☐ Case Insensitive☐ grep Regular Expression

SEARCH

EXTRACT STRINGS

EXTRACT UNALLOCATED

[Regular Expression Cheat Sheet](#)

**NOTE:** The keyword search runs grep on the image.

A list of what will and what will not be found is available [here](#).

## Previous Searches

passwd|ascii (0)

passwd|unicode (0)

senha|ascii (0)

senha|unicode (0)

pw|ascii (1)

pw|unicode (0)

## Predefined Searches

CC

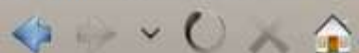
SSN2

IP

SSN1

Date





FILE ANALYSIS

KEYWORD SEARCH

FILE TYPE

IMAGE DETAILS

META DATA

DATA UNIT

HELP

CLOSE

Searching for ASCII: Done

Saving: Done

1 hits- [link to results](#)

Searching for Unicode: Done

Saving: Done

0 hits

[New Search](#)**1 occurrence of pw was found**

Search Options:

ASCII

Case Sensitive

Sector 103 ([Hex](#) - [Ascii](#))

1: 288 (pw=good)

**pw was not found**

Search Options:

Unicode

Case Sensitive

◀ PREVIOUS

NEXT ▶

EXPORT CONTENTS

ADD NOTE

ASCII ([display](#) - [report](#)) \* Hex ([display](#) - [report](#)) \* ASCII Strings ([display](#) - [report](#))

File Type: data

Sector: 103

Status: Allocated

[Find Meta Data Address](#)

ASCII String Contents of Sector 103 in image-0-0

pw=goodtimes

## ✓ Tentando outras técnicas

```
# cp image image.fix
```

```
# losetup /dev/loop0 image.fix
```

```
# dosfsck -u /jimmyj~1.doc -f -r /dev/loop0
```

*dosfsck 2.8, 28 Feb 2001, FAT32, LFN*

*Undeleting JIMMYJ~1.DOC*

*Wrong checksum for long file name "Scheduled Visits.exe ". (Short name SCHEDU~1.EXE may have changed without updating the long name)*

*1: Delete LFN*

*2: Leave it as it is.*

*3: Fix checksum (attaches to short name SCHEDU~1.EXE)*

*? 3*

*/cover page.jpgc*

*Contains a free cluster (420). Assuming EOF.*

*/cover page.jpgc*

*File size is 15585 bytes, cluster chain length is 0 bytes.*

*Truncating file to 0 bytes.*

*/Scheduled Visits.exe*

*File size is 1000 bytes, cluster chain length is > 1024 bytes.*

*Truncating file to 1000 bytes.*

*Reclaimed 31 unused clusters (15872 bytes) in 1 chain. Perform changes ? (y/n) y*

*/dev/loop0: 4 files, 73/2847 clusters*

# Caso 1

```
# losetup -d /dev/loop0
```

```
# mount -o ro,loop image.fix /mnt
```

```
# ls -la /mnt
```

*total 48*

```
drwxr-xr-x  2      root      root      7168      Dec 31      1969      ./
drwxr-xr-x 21      root      root      4096      Oct 12      15:30      ../
-rwxr-xr-x  1      root      root      1000      May 24      08:20      Scheduled\ Visits.exe\ \ \ \ \ \ *
-rwxr-xr-x  1      root      root      0          Sep 11      08:30      cover\ page.jpgc\ \ \ \ \ \ \ \ \ \ *
-rwxr-xr-x  1      root      root      15872     Dec 31      1979      fsck0000.rec*
-rwxr-xr-x  1      root      root      20480     Apr 15      2002      jimmyj~1.doc*
```

```
# mkdir fix2
```

```
# cp /mnt/* fix2
```

```
# umount /mnt
```

```
# file fix2/*
```

*fix2/Scheduled Visits.exe :*

*Zip archive data, at least v2.0 to extract*

fix2/cover page.jpgc  
(DPI), 96 x 96

```
:empty fix2/fsck0000.rec: JPEG image data, JFIF standard 1.01, resolution
```

fix2/jimmyj~1.doc: Microsoft Office document data

# Caso 1

```
# dd if=image of=Scheduled_Visits.zip bs=512 skip=104 count=5
```

```
# head -1000c Scheduled_Visits.zip |diff - files/schedu~1.exe
```

```
# unzip -v Scheduled_Visits.zip
```

Archive: Scheduled\_Visits.zip

| Length | Method | Size  | Ratio | Date     | Time  | CRC-32   | Name                 |
|--------|--------|-------|-------|----------|-------|----------|----------------------|
| -----  | -----  | ----- | ----- | ----     | ----  | -----    | ----                 |
| 16896  | Defl:N | 2270  | 87%   | 05-23-02 | 11:20 | 8d6055c7 | Scheduled Visits.xls |
| -----  | -----  | ---   |       |          |       |          | -----                |
| 16896  | 2270   | 87%   |       |          |       |          | 1 file               |

```
# unzip Scheduled_Visits.zip
```

Archive: Scheduled\_Visits.zip [Scheduled\_Visits.zip] Scheduled Visits.xls password:

**goodtimes**

inflating: Scheduled Visits.xls

```
$ ls -l "Scheduled Visits.xls"
```

```
-rw-rw-rw- 1 root root 16896 May 23 11:20 Scheduled\ Visits.xls
```

```
$ file "Scheduled Visits.xls"
```

Scheduled Visits.xls: Microsoft Office document data

```
$ mv "Scheduled Visits.xls" Scheduled_Visits.xls
```