Aula 06
Forense Computacional

Ferramentas Open Source - Continuação

Agenda

- ✓ Gerar imagem do Pendrive
- ✓ Cadeia de Custódia
- ✓ Montar Imagem
- ✓ MACtimes
- ✓ PTK
- ✓ Wiping
- ✓ Particionamento da Mídia

Gerar imagem do Pendrive

- ✓ Crie uma pasta para o caso que será investigado
  - ➢ **# *mkdir /home/pneukamp/caso_teste***
  - ➢ **# chmod 777 */home/pneukamp/*caso_teste/**
- ✓ Crie uma pasta para armazenar as evidencias e as informações sobre o caso.
  - ➢ **# mkdir */home/pneukamp/*caso_teste/evidencias**
- ✓ Preencha o Formulário de Cadeia de Custódia em: **Aplicativos → Forense Digital → 1 – Coleta dos Dados → Cadeia de Custódia → Formulário**:
  - ➢ *Complete todas as células com as informações de seu pendrive*
  - ➢ *Salve em: **/home/pneukamp/caso_teste/evidencias/Cust_Caso-teste.xls***

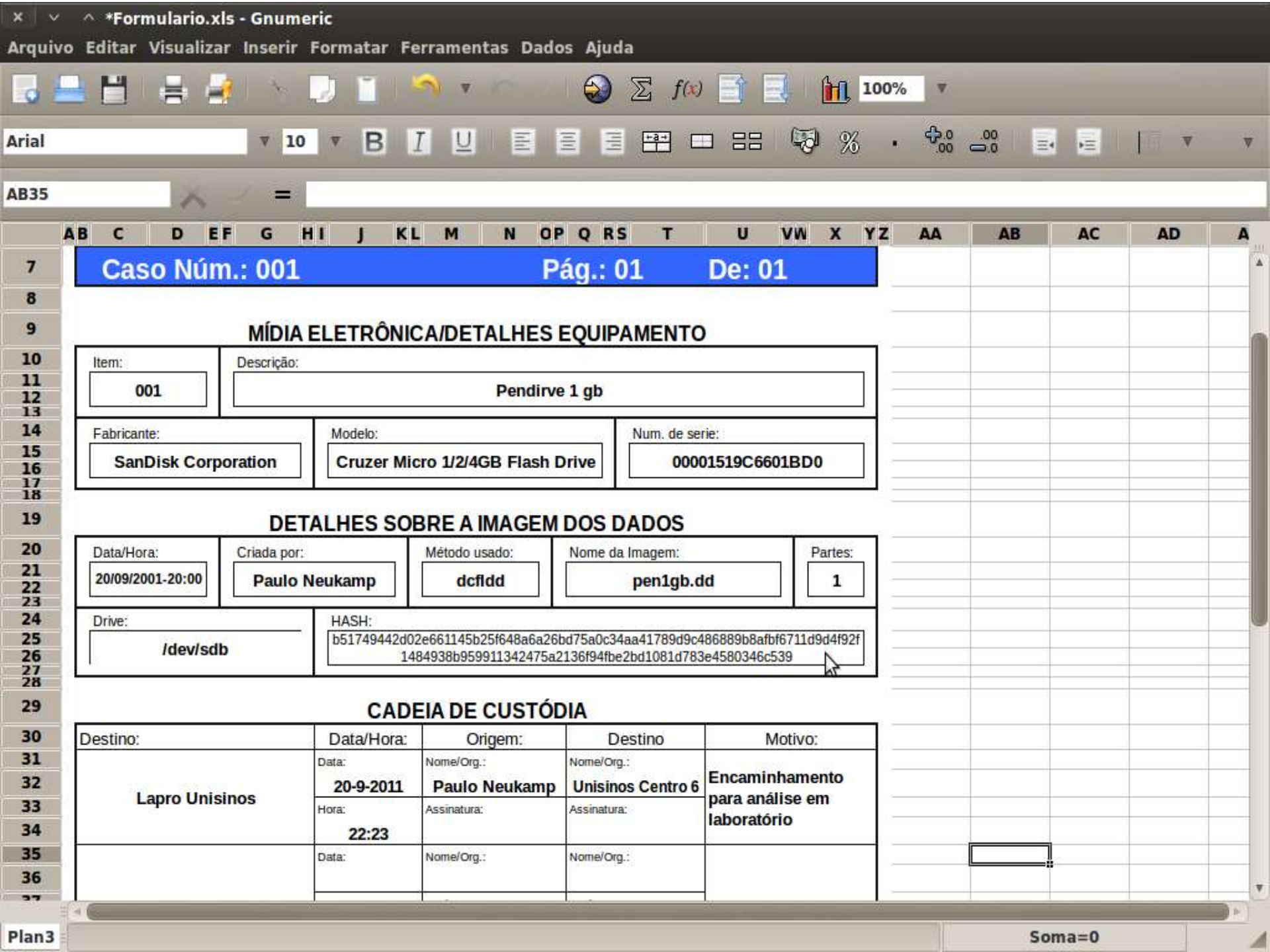

*Formulario.xls - Gnumeric
Arquivo Editar Visualizar Inserir Formatar Ferramentas Dados Ajuda
100%
Arial
10
AB35
Caso Núm.: 001 Pág.: 01 De: 01
MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO
Item:
001
Descrição:
Pendirve 1 gb
Fabricante:
SanDisk Corporation
Modelo:
Cruzer Micro 1/2/4GB Flash Drive
Num. de serie:
00001519C6601BD0
DETALHES SOBRE A IMAGEM DOS DADOS
Data/Hora:
20/09/2001-20:00
Criada por:
Paulo Neukamp
Método usado:
dcfldd
Nome da Imagem:
pen1gb.dd
Partes:
1
Drive:
/dev/sdb
HASH:
b51749442d02e661145b25f648a6a26bd75a0c34aa41789d9c486889b8afbf6711d9d4f92f
1484938b959911342475a2136f94fbe2bd1081d783e4580346c539
CADEIA DE CUSTÓDIA
Destino:
Data/Hora:
Origem:
Destino
Motivo:
Lapro Unisinos
Data:
20-9-2011
Hora:
22:23
Nome/Org.:
Paulo Neukamp
Assinatura:
Nome/Org.:
Unisinos Centro 6
Assinatura:
Encaminhamento para análise em laboratório
Data:
Nome/Org.:
Nome/Org.:
Plan3
Soma=0

Imagem do Pendrive

✓ Gerar imagem de seu pendrive.

 # dcfldd if=/dev/sdb hash=sha256,sha512
sha256log=/home/pneukamp/caso_teste/evidencias/sha256.txt
sha512log=/home/pneukamp/caso_teste/evidencias/sha512.txt
hashconv=after conv=noerror,sync
of=/home/pneukamp/caso_teste/evidencias/pen1GB-caso1.dd

root@iceman:/home/pneukamp/caso_teste/evidencias# ls -lh

total 962M

-rw-r--r-- 1 root root 961M 2012-04-03 00:08 pen1GB-caso1.dd

-rw-r--r-- 1 root root 81 2012-04-03 00:08 sha256.txt

-rw-r--r-- 1 root root 145 2012-04-03 00:08 sha512.txt

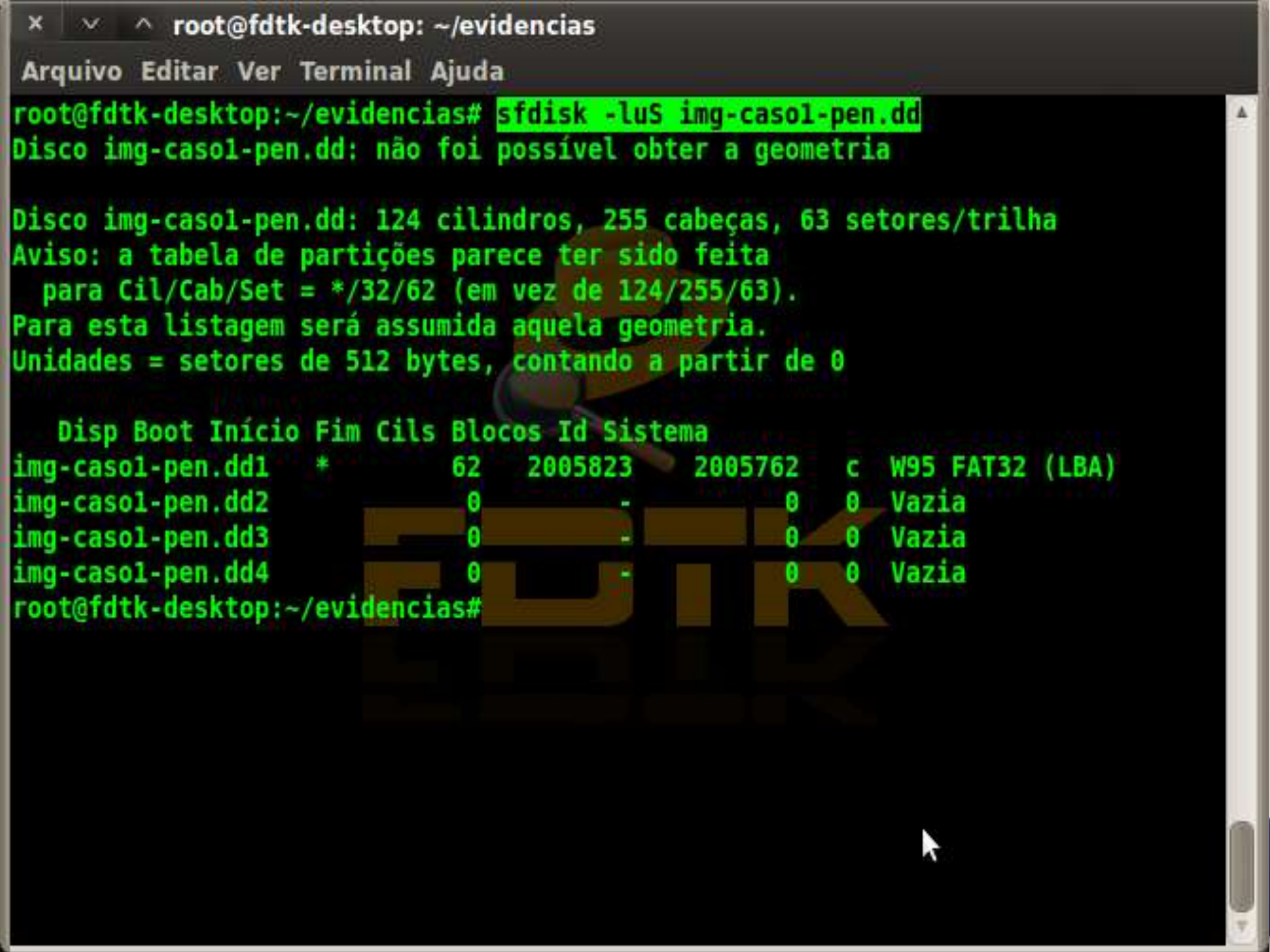
Atualize as informações no Formulário de Custódia

Montar imagem

- ✓ **Montando Imagens para Exame e Análise das evidências.**
- Uma imagem bit a bit de um disco é chamada de imagem raw.
- As imagens raw podem ser geradas de um disco inteiro com + de 1 partição chamadas de imagens raw físicas, pois geram uma imagem fiel do disco, não importando qual é o seu conteúdo.
- O outro tipo de imagem raw é chamado de imagem raw lógica, esta é gerada a partir de uma partição do disco físico (HD). Neste momento surge um problema pois o loopback do linux não monta imagens raw físicas (HD's) somente imagens raw lógicas, pois o loopback possui uma limitação simples, ele não interpreta a tabela de partições que está nos setores iniciais de uma imagem raw física.
- Para ser possível então contornar esta limitação do loopback é necessário executar alguns comando a fim de descobrir qual é a estrutura interna da imagem que pretendemos montar.

 # sfdisk -LuS /home/pneukamp/caso_teste/evidencias/pen1GB-caso1.dd

http://fdtk.com.br/www/2009/01/montando-imagens/

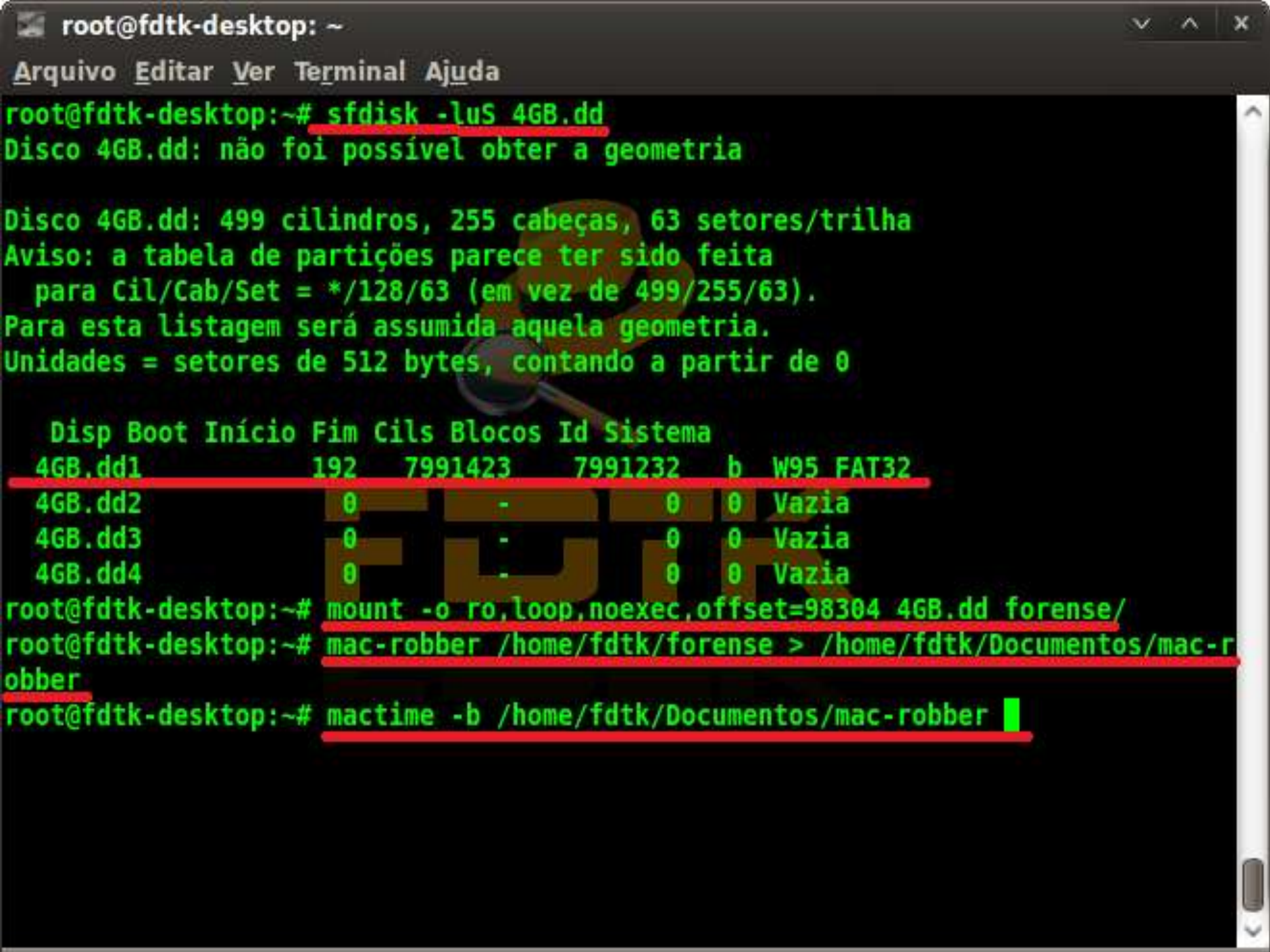

root@fdtk-desktop: ~/evidencias
Arquivo Editar Ver Terminal Ajuda
root@fdtk-desktop:~/evidencias# sfdisk -luS img-caso1-pen.dd
Disco img-caso1-pen.dd: não foi possível obter a geometria
Disco img-caso1-pen.dd: 124 cilindros, 255 cabeças, 63 setores/trilha
Aviso: a tabela de partições parece ter sido feita
para Cil/Cab/Set = */32/62 (em vez de 124/255/63).
Para esta listagem será assumida aquela geometria.
Unidades = setores de 512 bytes, contando a partir de 0
Disp Boot Início Fim Cils Blocos Id Sistema
img-caso1-pen.dd1 * 62 2005823 2005762 c W95 FAT32 (LBA)
img-caso1-pen.dd2 0 - 0 0 Vazia
img-caso1-pen.dd3 0 - 0 0 Vazia
img-caso1-pen.dd4 0 - 0 0 Vazia
root@fdtk-desktop:~/evidencias#

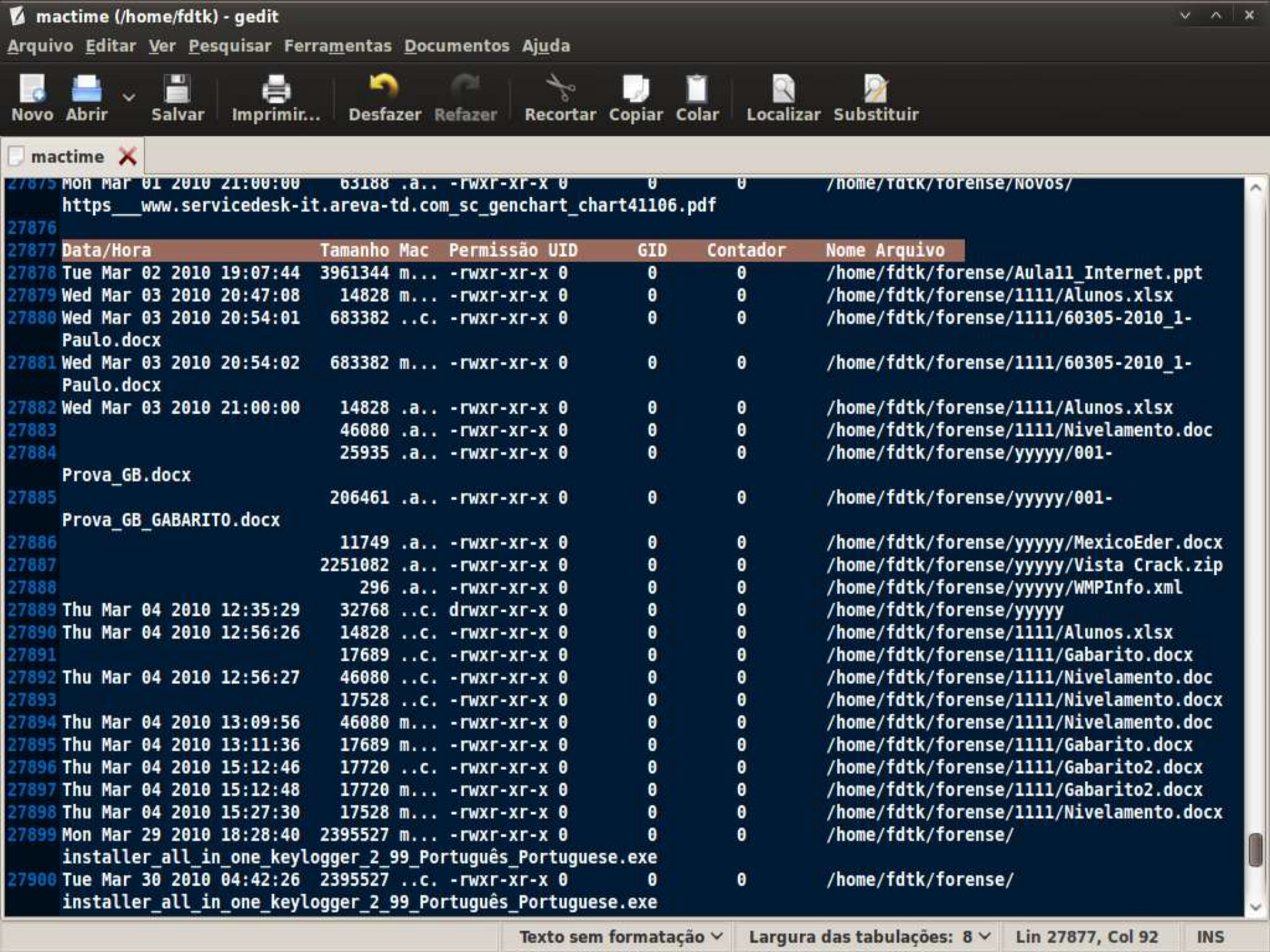
Montar imagem

- ✓ A saída do comando sfdisk mostra que a imagem raw física tem apenas uma partição iniciando no setor 62, é do tipo vfat e que cada setor tem 512 bytes.
- ✓ Como o loopback não compreende a tabela de partições, para montarmos a imagem raw, será necessário informar ao loopback onde ele deverá começar a ler a partição (offset).
- ✓ A resposta para esta questão é possível através de um simples cálculo de multiplicação entre o setor inicial da partição e o número de bytes por setor (62*512=31744), com este resultado é possível montar a imagem

- ***# mount -o loop, ro, noexec, offset=31744 /home/fdtk/caso_teste/evidencias/pen1GB-caso1.dd /media/USB***

http://fdtk.com.br/www/2009/01/montando-imagens/


root@fdtk-desktop: ~
Arquivo Editar Ver Terminal Ajuda
root@fdtk-desktop:~# sfdisk -luS 4GB.dd
Disco 4GB.dd: não foi possível obter a geometria
Disco 4GB.dd: 499 cilindros, 255 cabeças, 63 setores/trilha
Aviso: a tabela de partições parece ter sido feita
para Cil/Cab/Set = */128/63 (em vez de 499/255/63).
Para esta listagem será assumida aquela geometria.
Unidades = setores de 512 bytes, contando a partir de 0
Disp Boot Início Fim Cils Blocos Id Sistema
4GB.dd1 192 7991423 7991232 b W95 FAT32
4GB.dd2 0 - 0 0 Vazia
4GB.dd3 0 - 0 0 Vazia
4GB.dd4 0 - 0 0 Vazia
root@fdtk-desktop:~# mount -o ro,loop,noexec,offset=98304 4GB.dd forense/
root@fdtk-desktop:~# mac-robber /home/fdtk/forense > /home/fdtk/Documentos/mac-robber
root@fdtk-desktop:~# mactime -b /home/fdtk/Documentos/mac-robber


mactime (/home/fdtk) - gedit
Arquivo Editar Ver Pesquisar Ferramentas Documentos Ajuda
Novo Abrir Salvar Imprimir... Desfazer Refazer Recortar Copiar Colar Localizar Substituir
mactime
27875 Mon Mar 01 2010 21:00:00 63188 .a.. -rwxr-xr-x 0 0 0 /home/fdtk/forense/Novos/
https___www.servicedesk-it.areva-td.com_sc_genchart_chart41106.pdf
27876
27877 Data/Hora Tamanho Mac Permissão UID GID Contador Nome Arquivo
27878 Tue Mar 02 2010 19:07:44 3961344 m... -rwxr-xr-x 0 0 0 /home/fdtk/forense/Aula11_Internet.ppt
27879 Wed Mar 03 2010 20:47:08 14828 m... -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/Alunos.xlsx
27880 Wed Mar 03 2010 20:54:01 683382 ..c. -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/60305-2010_1-
Paulo.docx
27881 Wed Mar 03 2010 20:54:02 683382 m... -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/60305-2010_1-
Paulo.docx
27882 Wed Mar 03 2010 21:00:00 14828 .a.. -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/Alunos.xlsx
27883 46080 .a.. -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/Nivelamento.doc
27884 25935 .a.. -rwxr-xr-x 0 0 0 /home/fdtk/forense/yyyyy/001-
Prova_GB.docx
27885 206461 .a.. -rwxr-xr-x 0 0 0 /home/fdtk/forense/yyyyy/001-
Prova_GB_GABARITO.docx
27886 11749 .a.. -rwxr-xr-x 0 0 0 /home/fdtk/forense/yyyyy/MexicoEder.docx
27887 2251082 .a.. -rwxr-xr-x 0 0 0 /home/fdtk/forense/yyyyy/Vista Crack.zip
27888 296 .a.. -rwxr-xr-x 0 0 0 /home/fdtk/forense/yyyyy/WMPInfo.xml
27889 Thu Mar 04 2010 12:35:29 32768 ..c. drwxr-xr-x 0 0 0 /home/fdtk/forense/yyyyy
27890 Thu Mar 04 2010 12:56:26 14828 ..c. -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/Alunos.xlsx
27891 17689 ..c. -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/Gabarito.docx
27892 Thu Mar 04 2010 12:56:27 46080 ..c. -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/Nivelamento.doc
27893 17528 ..c. -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/Nivelamento.docx
27894 Thu Mar 04 2010 13:09:56 46080 m... -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/Nivelamento.doc
27895 Thu Mar 04 2010 13:11:36 17689 m... -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/Gabarito.docx
27896 Thu Mar 04 2010 15:12:46 17720 ..c. -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/Gabarito2.docx
27897 Thu Mar 04 2010 15:12:48 17720 m... -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/Gabarito2.docx
27898 Thu Mar 04 2010 15:27:30 17528 m... -rwxr-xr-x 0 0 0 /home/fdtk/forense/1111/Nivelamento.docx
27899 Mon Mar 29 2010 18:28:40 2395527 m... -rwxr-xr-x 0 0 0 /home/fdtk/forense/
installer_all_in_one_keylogger_2_99_Português_Portuguese.exe
27900 Tue Mar 30 2010 04:42:26 2395527 ..c. -rwxr-xr-x 0 0 0 /home/fdtk/forense/
installer_all_in_one_keylogger_2_99_Português_Portuguese.exe
Texto sem formatação
Largura das tabulações: 8
Lin 27877, Col 92
INS

PTK - Mozilla Firefox

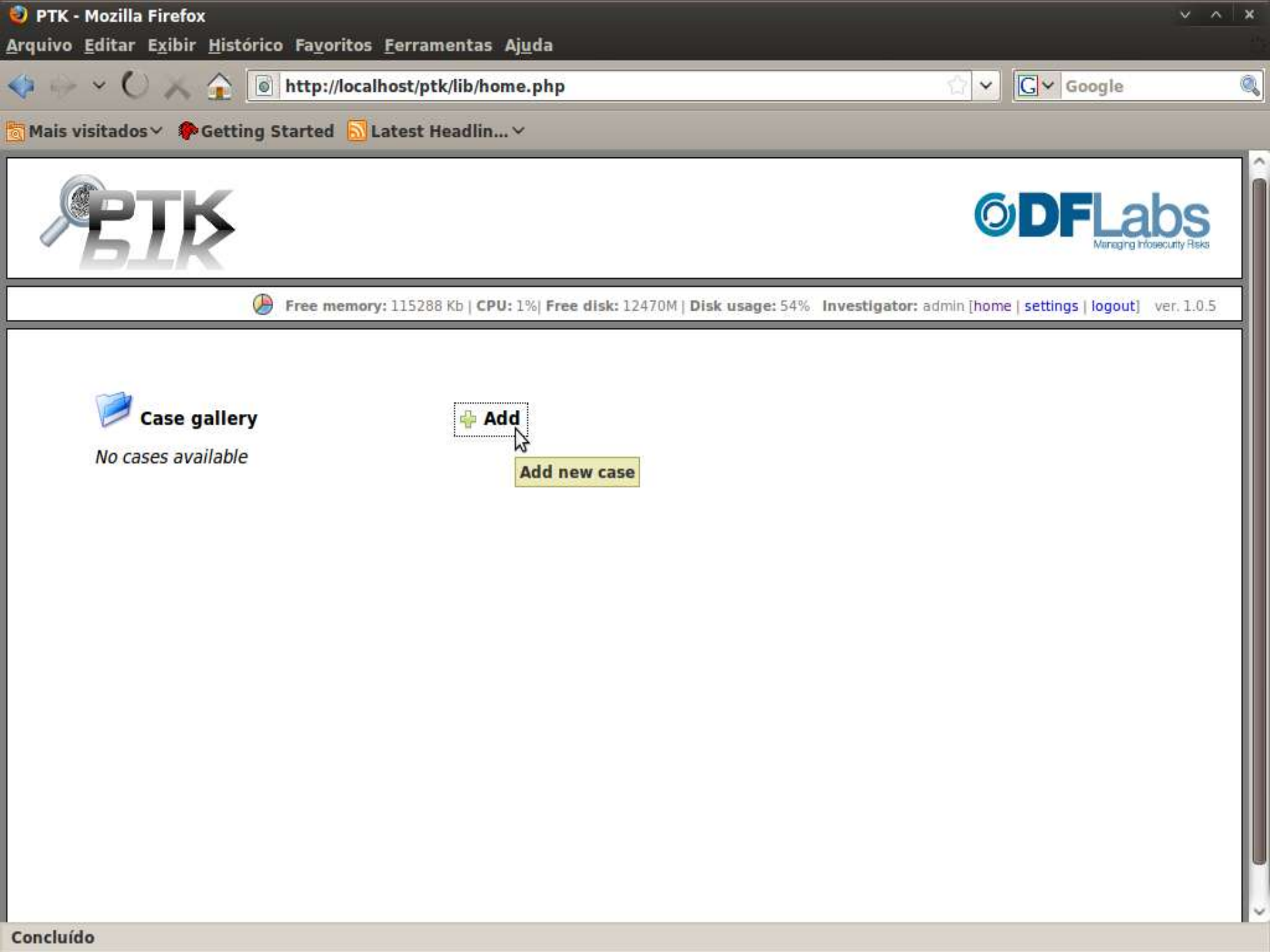
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

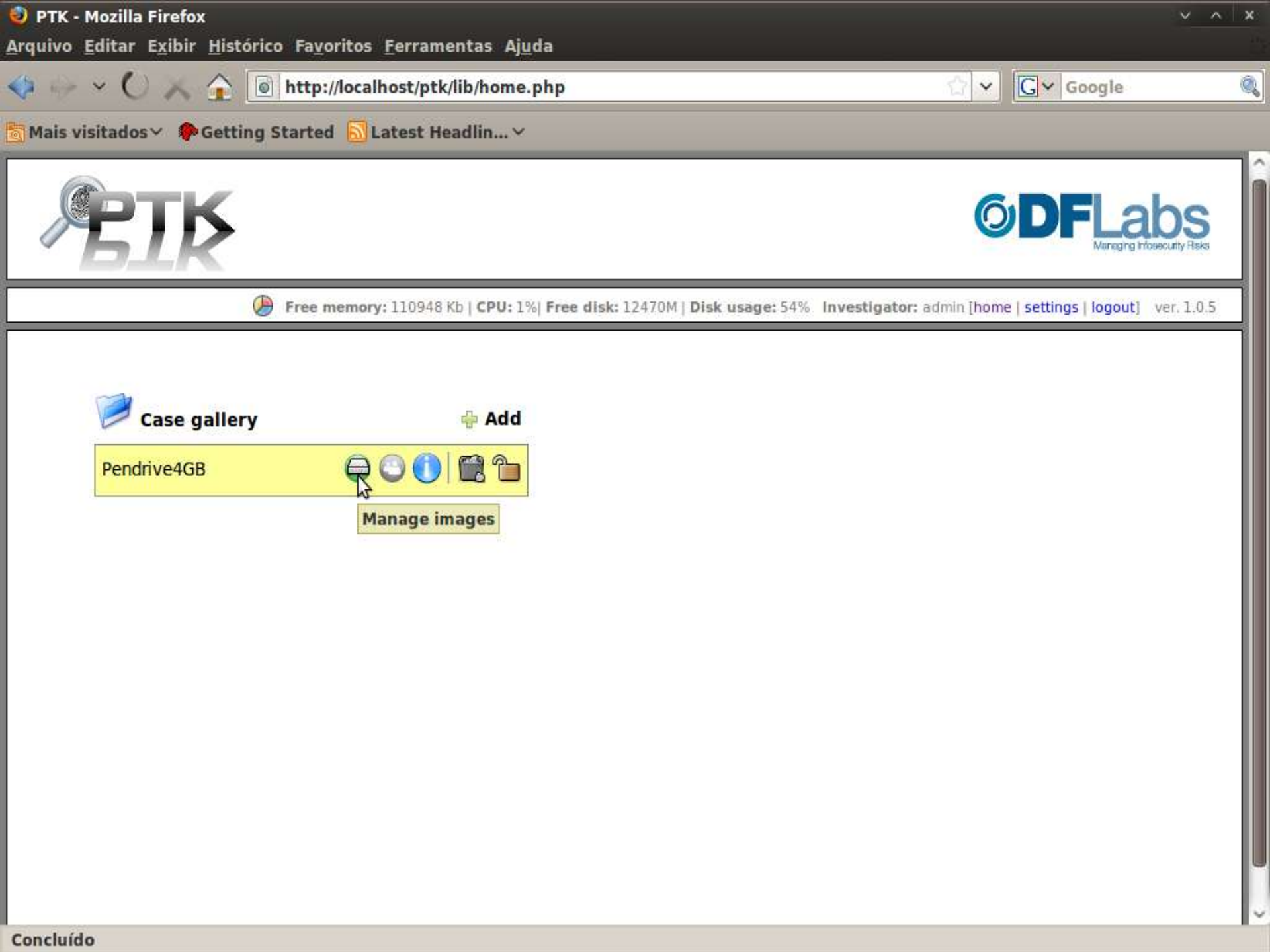
http://localhost/ptk/index.php

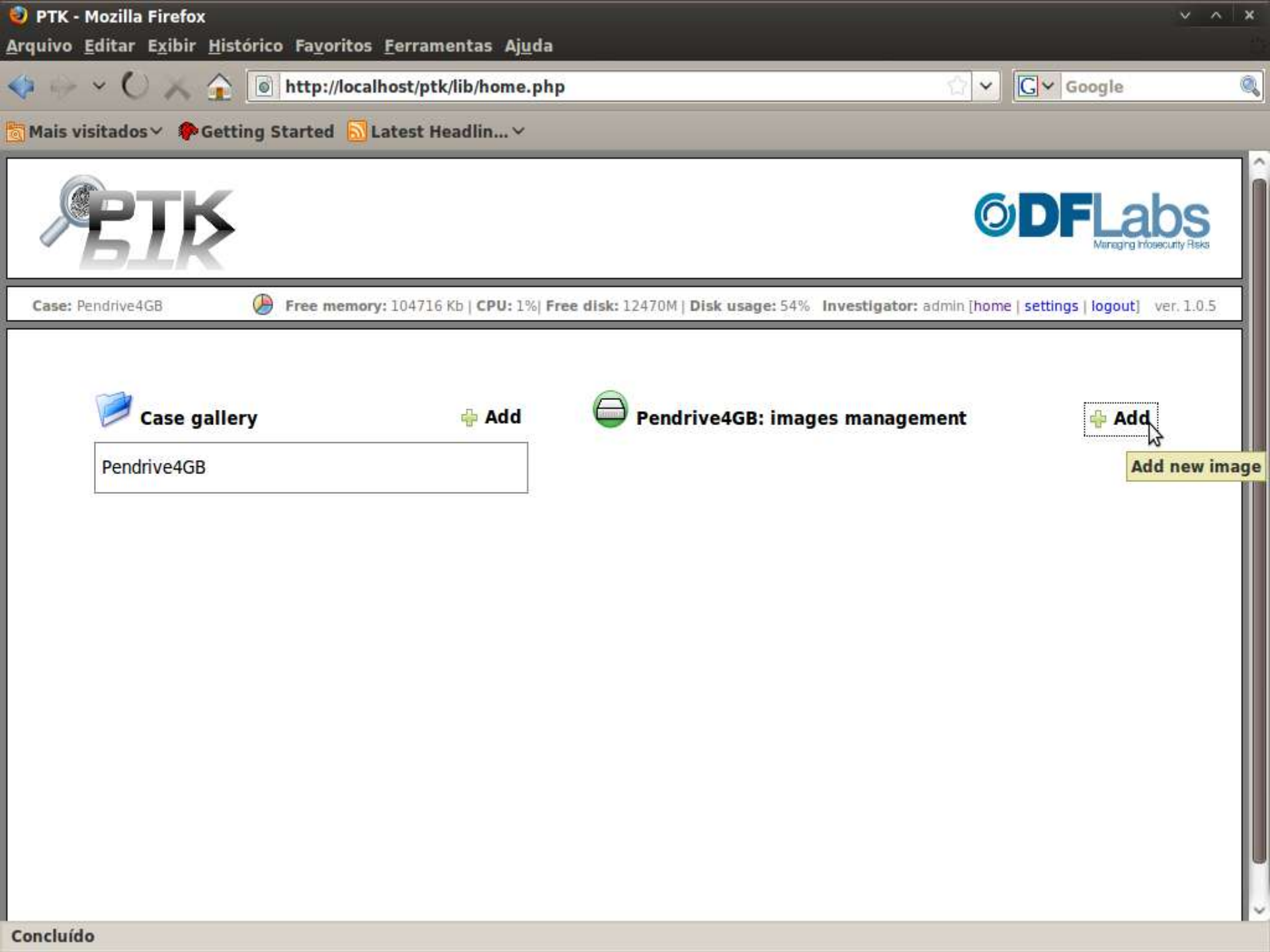
Google

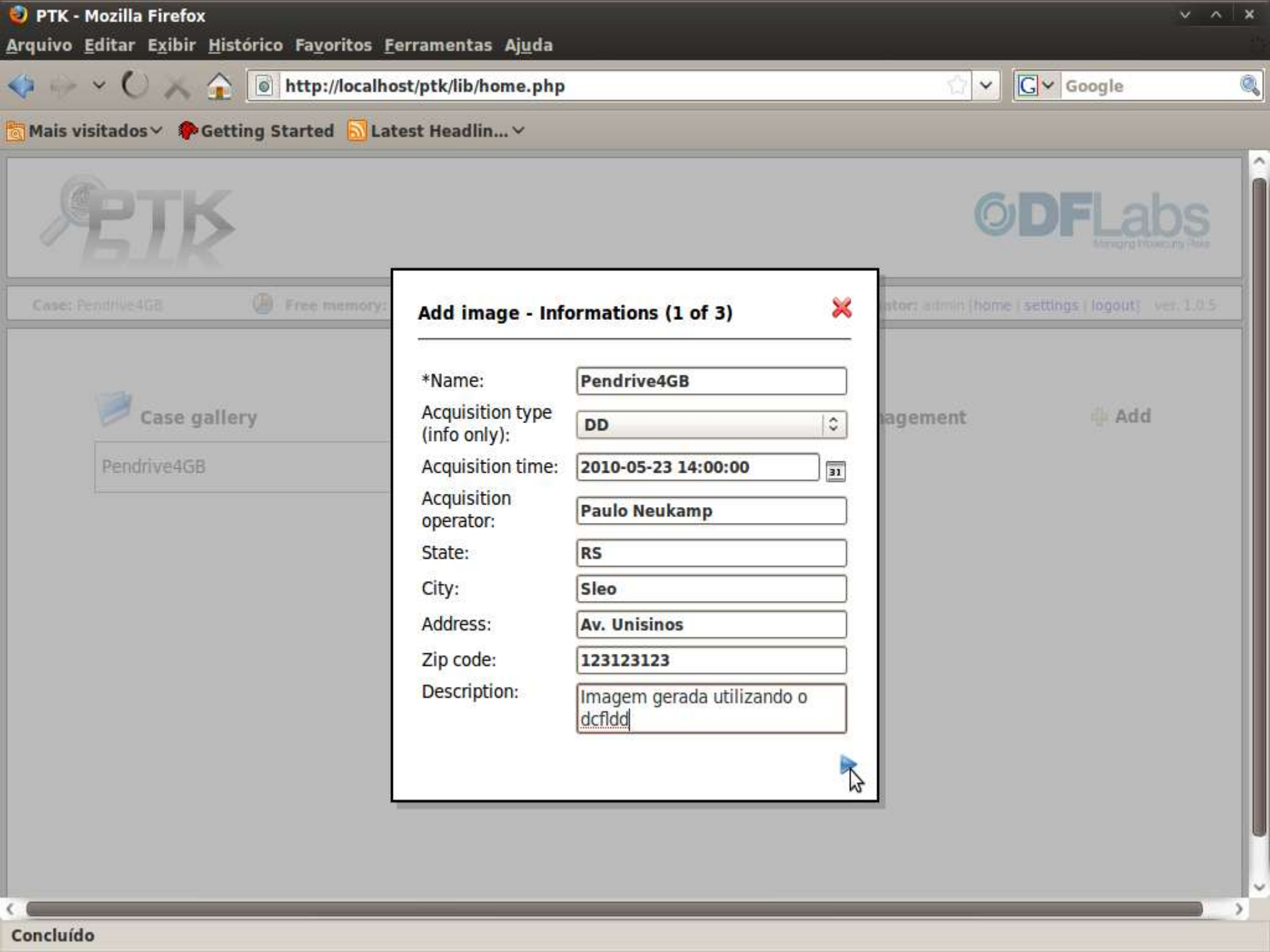
Mais visitados Getting Started Latest Headlin...

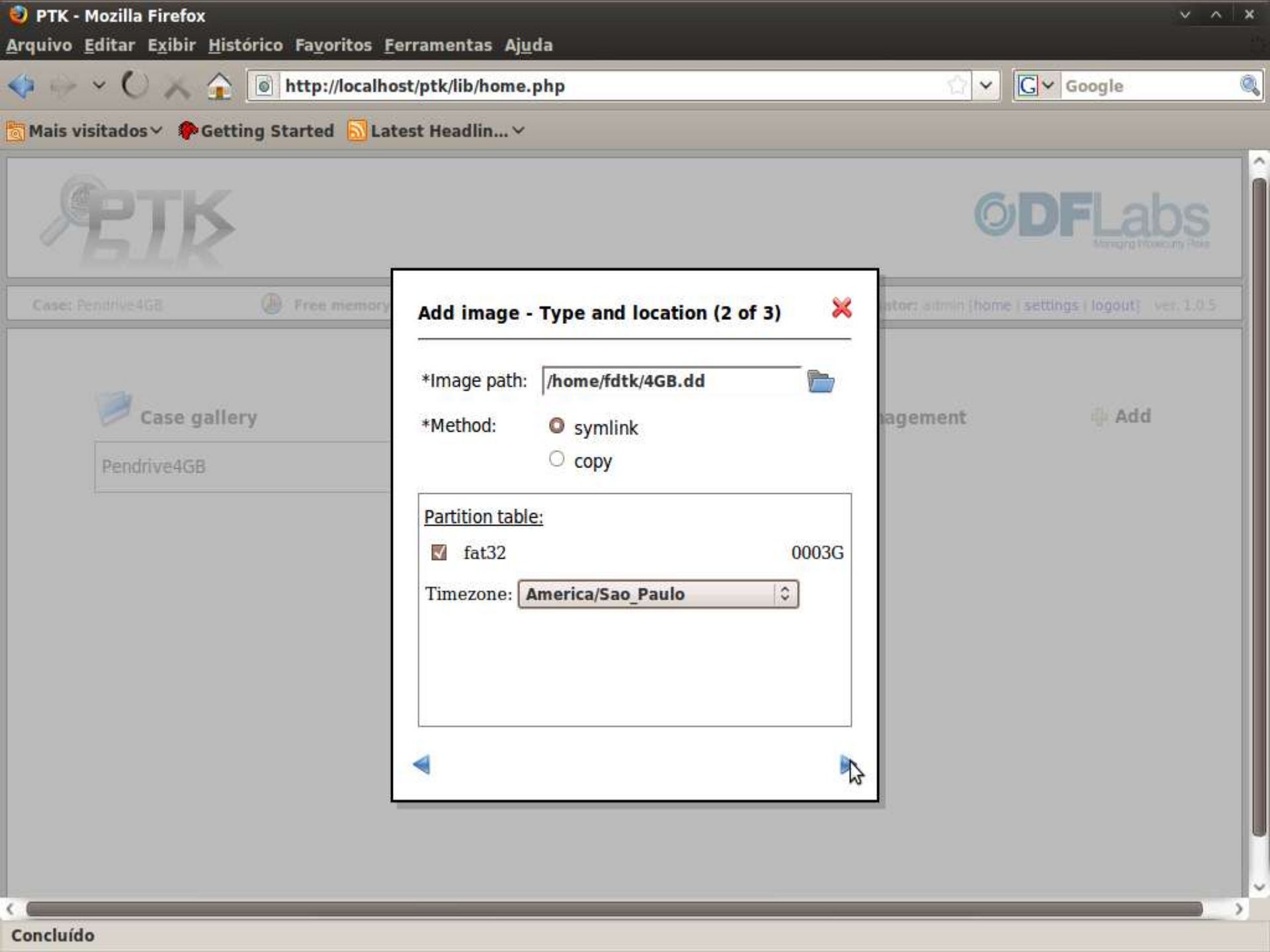
Concluído

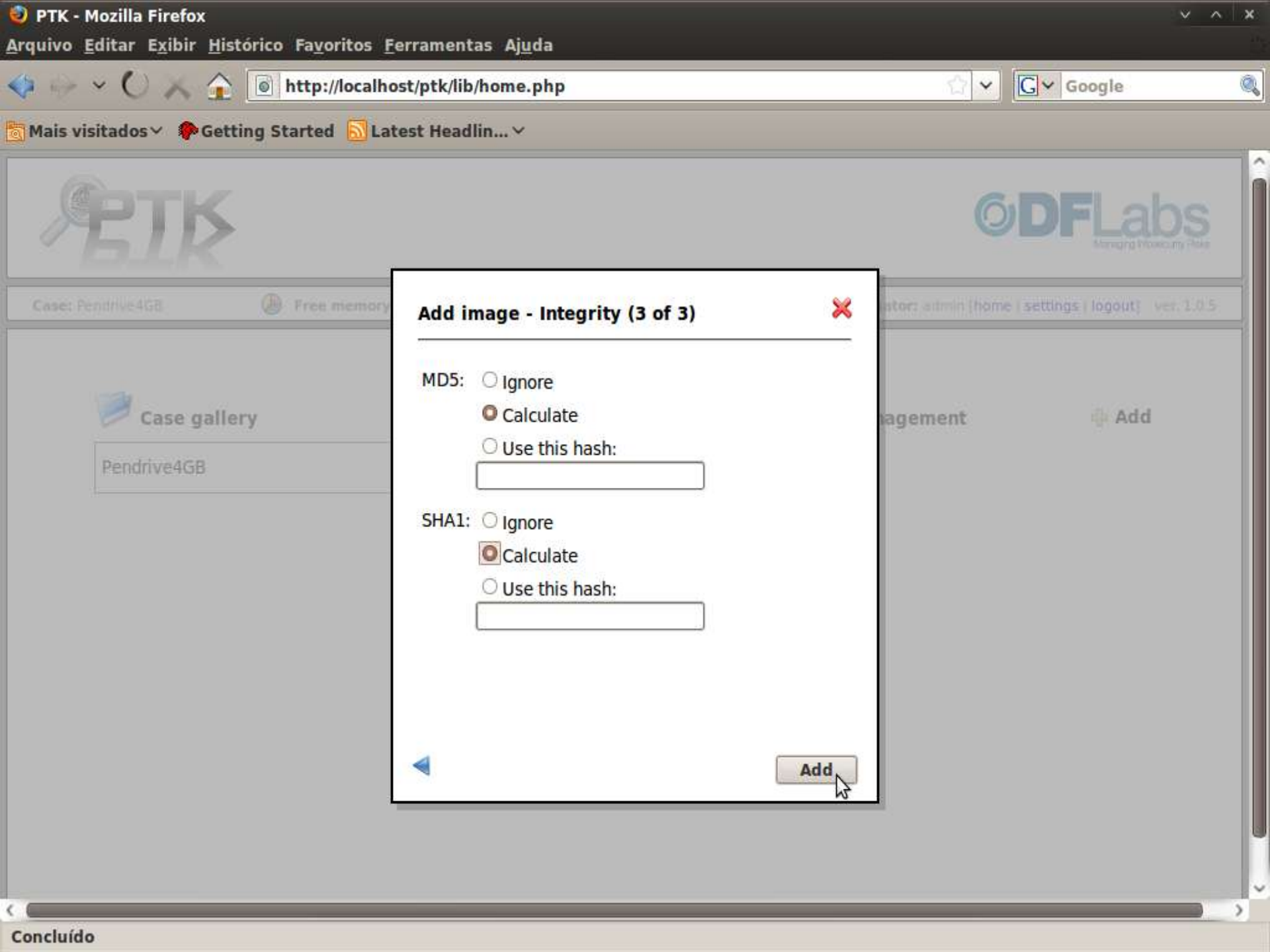

PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/home.php
Google
Mais visitados
Getting Started
Latest Headlin...
PTK
DFLabs
Managing Infosecurity Risks
Free memory: 115288 Kb | CPU: 1%| Free disk: 12470M | Disk usage: 54% Investigator: admin [home | settings | logout] ver. 1.0.5
Case gallery
No cases available
Add
Add new case
Concluído

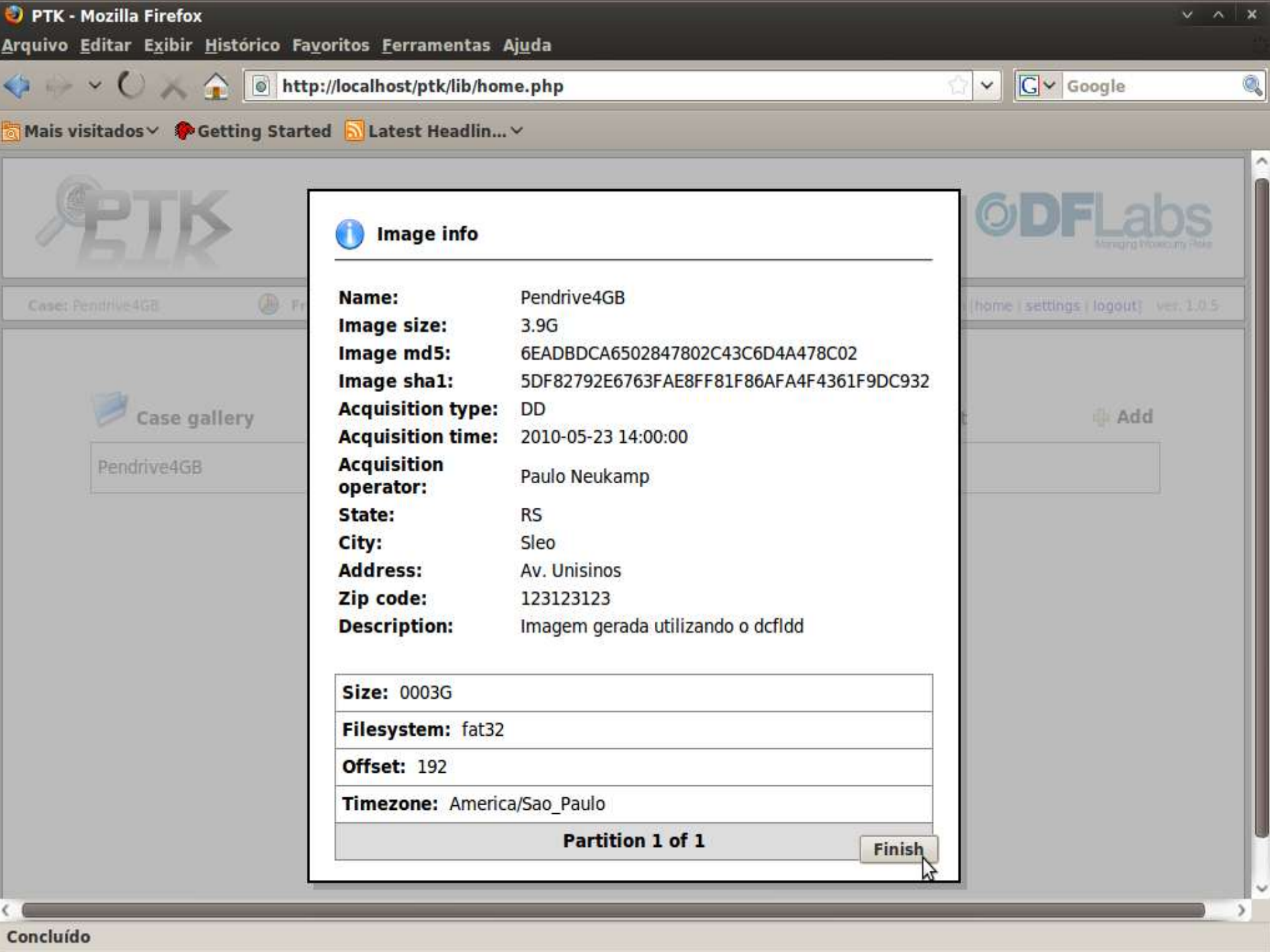

PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/home.php
Google
Mais visitados
Getting Started
Latest Headlin...
PTK
DFLabs
Managing Infosecurity Risks
Free memory: 110948 Kb | CPU: 1%| Free disk: 12470M | Disk usage: 54% Investigator: admin [home | settings | logout] ver. 1.0.5
Case gallery
Add
Pendrive4GB
Manage images
Concluído

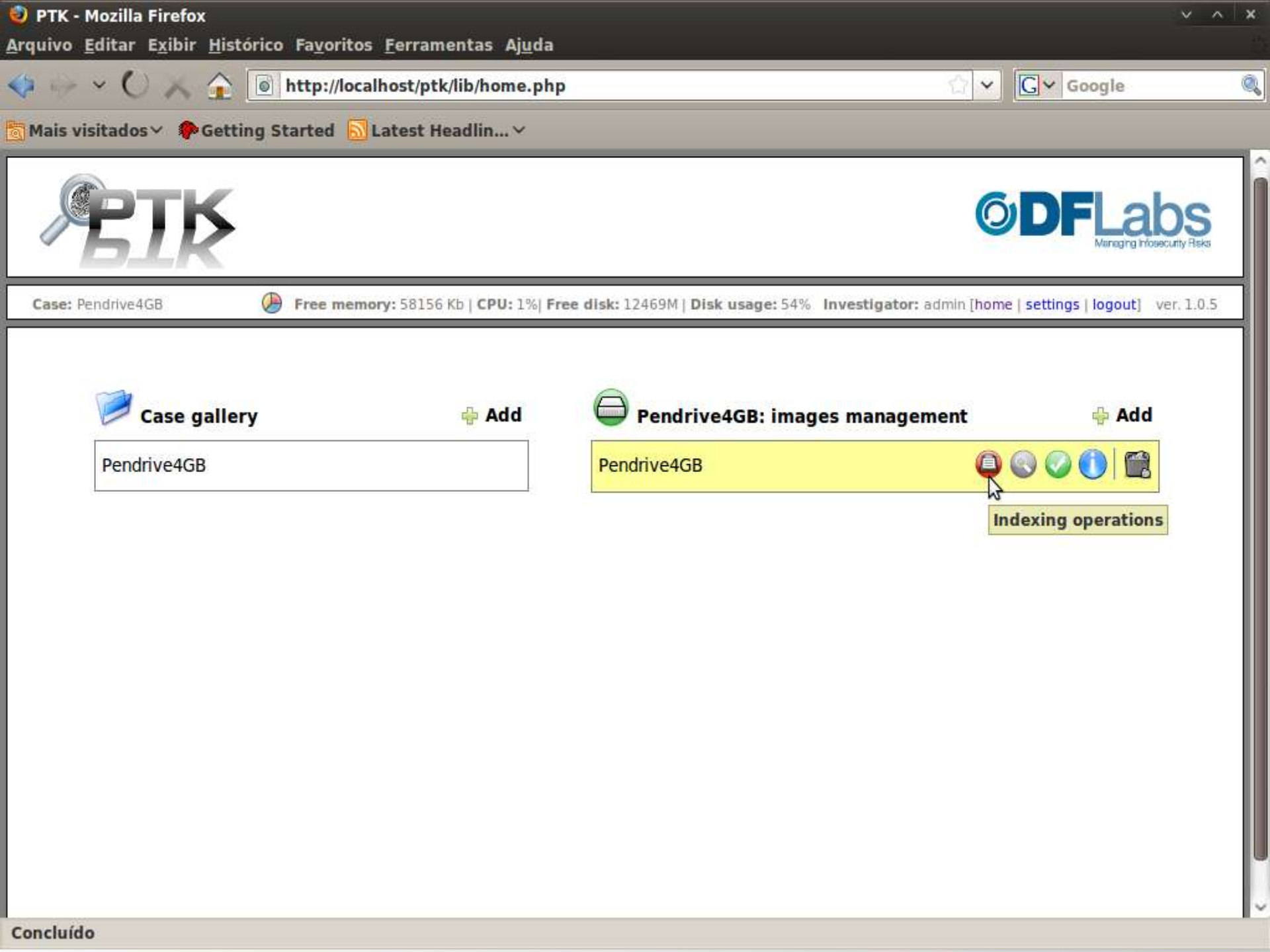

PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/home.php
Google
Mais visitados
Getting Started
Latest Headlin...
PTK
DFLabs
Managing Infosecurity Risks
Case: Pendrive4GB
Free memory: 104716 Kb | CPU: 1%| Free disk: 12470M | Disk usage: 54%
Investigator: admin [home | settings | logout]
ver. 1.0.5
Case gallery
Add
Pendrive4GB
Pendrive4GB: images management
Add
Add new image
Concluído

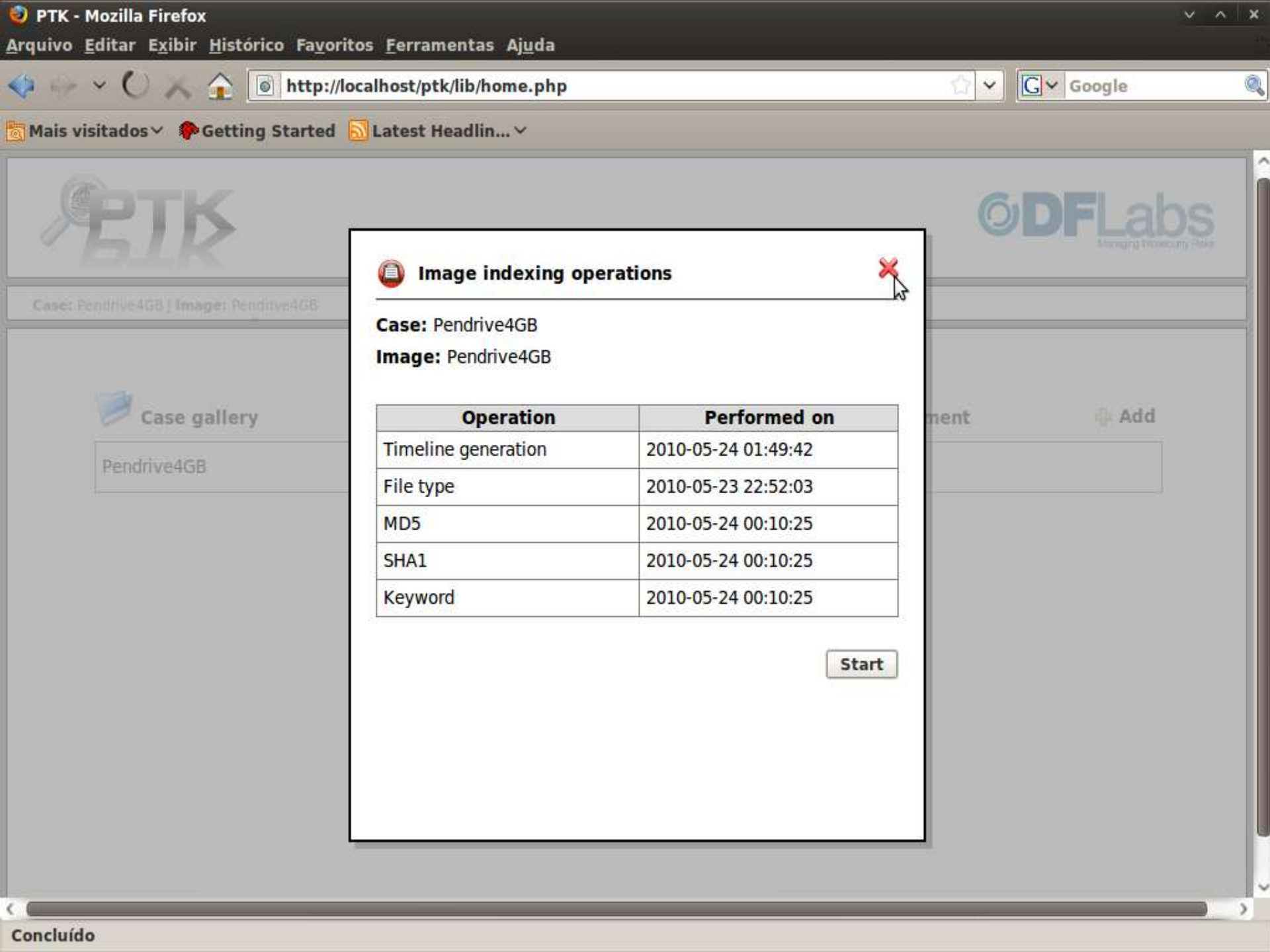

PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/home.php
Google
Mais visitados
Getting Started
Latest Headlin...
PTK
DFLabs
Case: Pendrive4GB
Free memory:
admin [home | settings | logout] ver. 1.0.5
Case gallery
Pendrive4GB
Add
Add image - Informations (1 of 3)
*Name:
Pendrive4GB
Acquisition type (info only):
DD
Acquisition time:
2010-05-23 14:00:00
Acquisition operator:
Paulo Neukamp
State:
RS
City:
Sleo
Address:
Av. Unisinos
Zip code:
123123123
Description:
Imagem gerada utilizando o dcfldd
Concluído

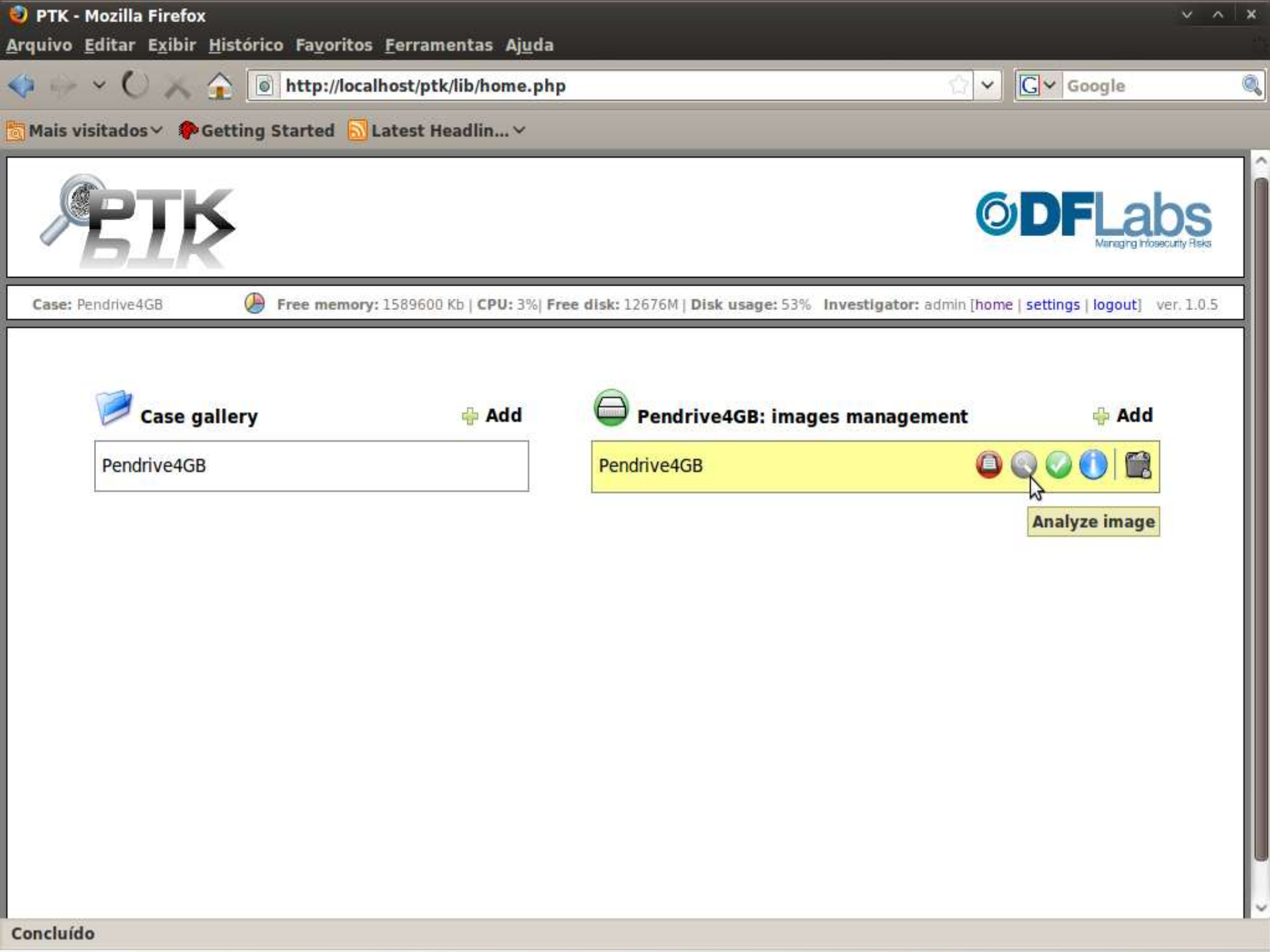

PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/home.php
Google
Mais visitados
Getting Started
Latest Headlin...
PTK
DFLabs
Case: Pendrive4GB
Free memory
admin [home | settings | logout] ver. 1.0.5
Case gallery
Pendrive4GB
Add
Add image - Type and location (2 of 3)
*Image path:
/home/fdtk/4GB.dd
*Method:
symlink
copy
Partition table:
fat32
0003G
Timezone:
America/Sao_Paulo
Concluído

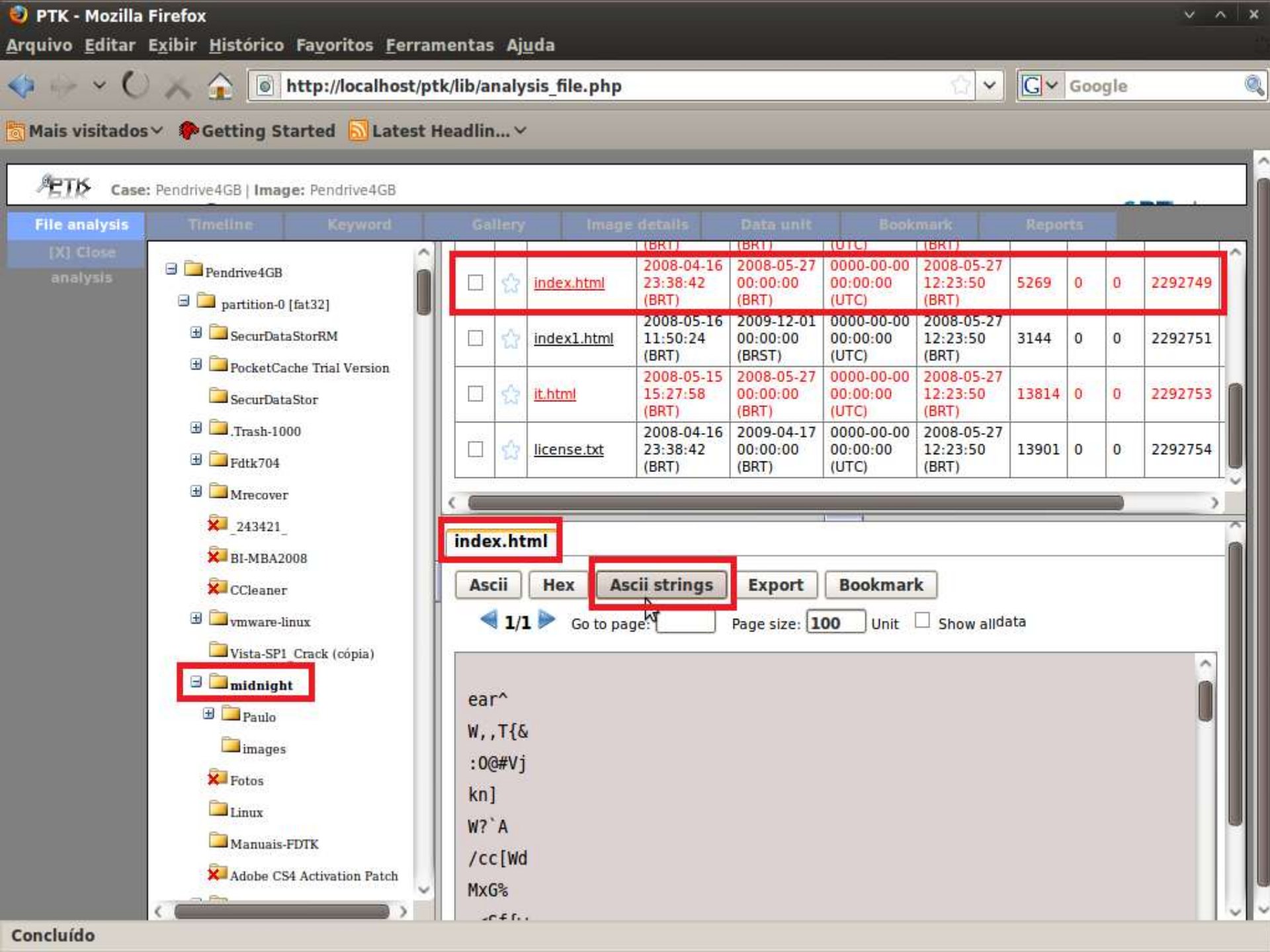

PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/home.php
Google
Mais visitados
Getting Started
Latest Headlin...
PTK
DFLabs
Case: Pendrive4GB
Free memory
home | settings | logout
ver. 1.0.5
Case gallery
Pendrive4GB
Add
Add image - Integrity (3 of 3)
MD5:
Ignore
Calculate
Use this hash:
SHA1:
Ignore
Calculate
Use this hash:
Add
Concluído

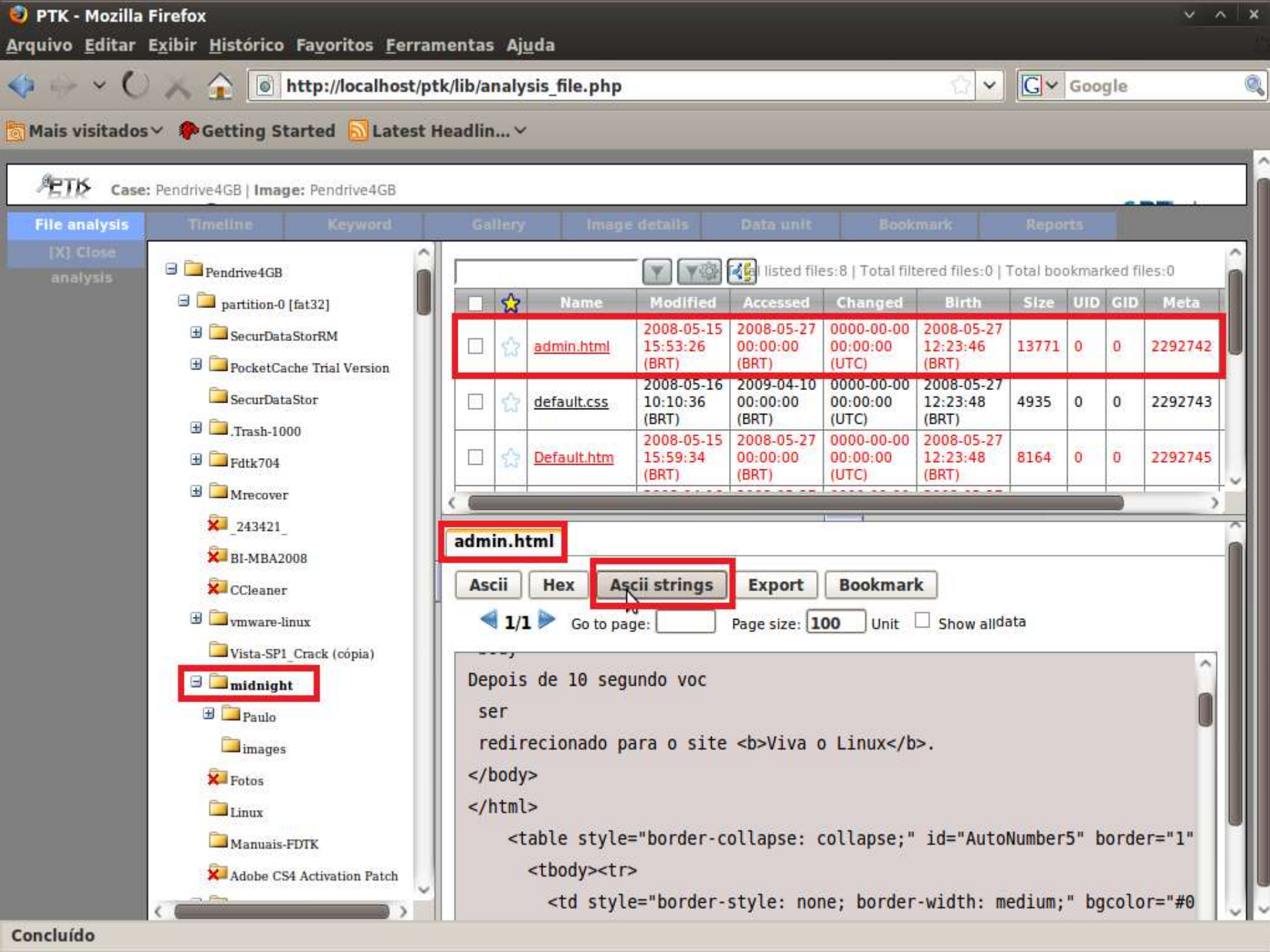

PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/home.php
Google
Mais visitados
Getting Started
Latest Headlin...
PTK
DFLabs
Case: Pendrive4GB
[home | settings | logout]
ver. 1.0.5
Case gallery
Add
Pendrive4GB
Image info
Name: Pendrive4GB
Image size: 3.9G
Image md5: 6EADBDCA6502847802C43C6D4A478C02
Image sha1: 5DF82792E6763FAE8FF81F86AFA4F4361F9DC932
Acquisition type: DD
Acquisition time: 2010-05-23 14:00:00
Acquisition operator: Paulo Neukamp
State: RS
City: Sleo
Address: Av. Unisinos
Zip code: 123123123
Description: Imagem gerada utilizando o dcfldd
Size: 0003G
Filesystem: fat32
Offset: 192
Timezone: America/Sao_Paulo
Partition 1 of 1
Finish
Concluído

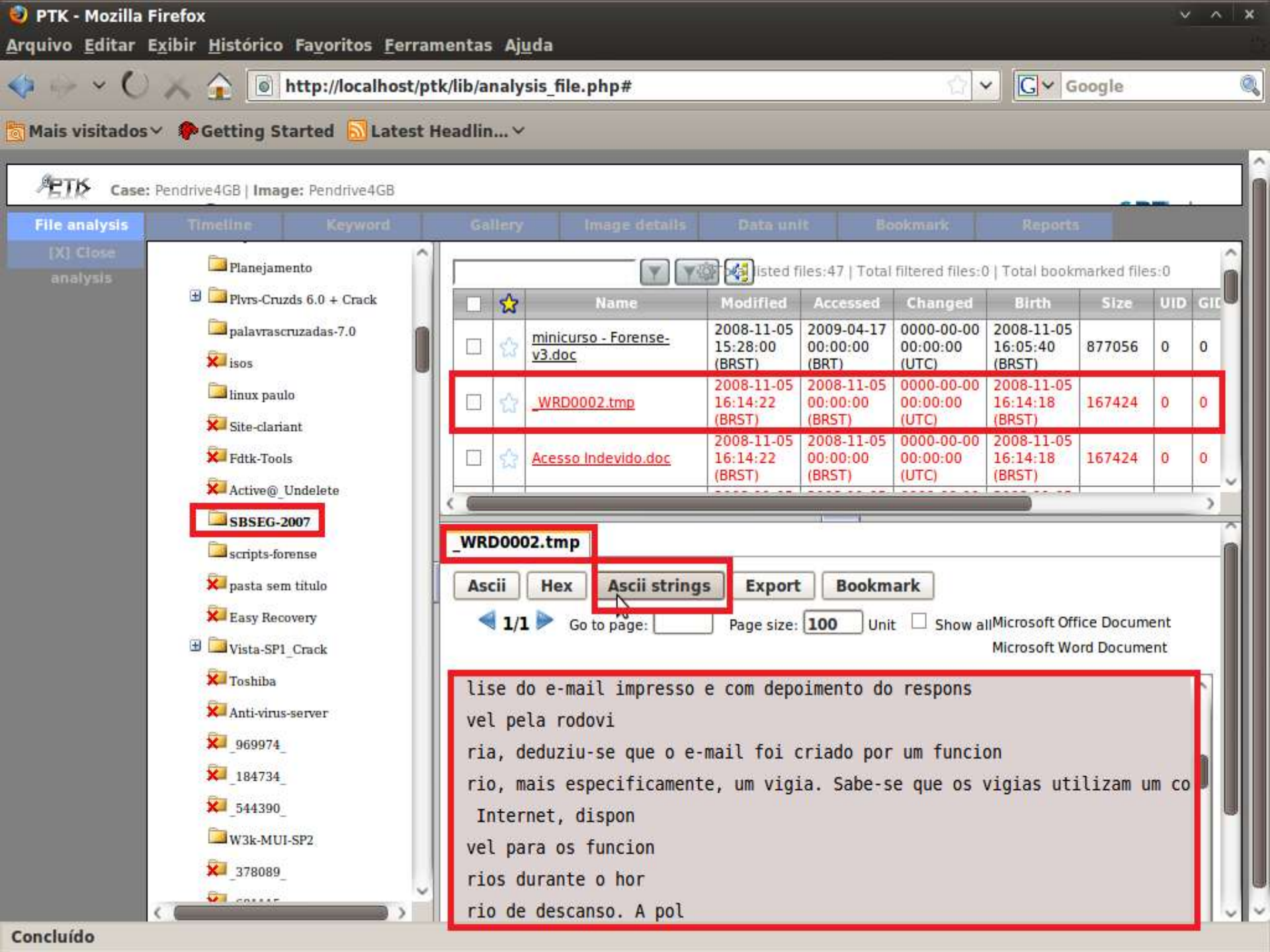

PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/home.php
Google
Mais visitados
Getting Started
Latest Headlin...
PTK
DFLabs
Managing Infosecurity Risks
Case: Pendrive4GB
Free memory: 58156 Kb | CPU: 1%| Free disk: 12469M | Disk usage: 54%
Investigator: admin [home | settings | logout]
ver. 1.0.5
Case gallery
Add
Pendrive4GB
Pendrive4GB: images management
Add
Pendrive4GB
Indexing operations
Concluído


PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/home.php
Google
Mais visitados
Getting Started
Latest Headlin...
PTK
DFLabs
Case: Pendrive4GB | Image: Pendrive4GB
Case gallery
Add
Pendrive4GB
Image indexing operations
Case: Pendrive4GB
Image: Pendrive4GB
Operation
Performed on
Timeline generation
2010-05-24 01:49:42
File type
2010-05-23 22:52:03
MD5
2010-05-24 00:10:25
SHA1
2010-05-24 00:10:25
Keyword
2010-05-24 00:10:25
Start
Concluído


PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/home.php
Google
Mais visitados
Getting Started
Latest Headlin...
PTK
DFLabs
Managing Infosecurity Risks
Case: Pendrive4GB
Free memory: 1589600 Kb | CPU: 3%| Free disk: 12676M | Disk usage: 53%
Investigator: admin [home | settings | logout]
ver. 1.0.5
Case gallery
Add
Pendrive4GB
Pendrive4GB: images management
Add
Pendrive4GB
Analyze image
Concluído


PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/analysis_file.php
Google
Mais visitados
Getting Started
Latest Headlin...
Case: Pendrive4GB | Image: Pendrive4GB
File analysis
[X] Close analysis
Timeline
Keyword
Gallery
Image details
Data unit
Bookmark
Reports
Pendrive4GB
partition-0 [fat32]
SecurDataStorRM
PocketCache Trial Version
SecurDataStor
.Trash-1000
Fdtk704
Mrecover
_243421_
BI-MBA2008
CCleaner
vmware-linux
Vista-SP1_Crack (cópia)
midnight
Paulo
images
Fotos
Linux
Manuais-FDTK
Adobe CS4 Activation Patch
index.html 2008-04-16 23:38:42 (BRT) 2008-05-27 00:00:00 (BRT) 0000-00-00 00:00:00 (UTC) 2008-05-27 12:23:50 (BRT) 5269 0 0 2292749
index1.html 2008-05-16 11:50:24 (BRT) 2009-12-01 00:00:00 (BRST) 0000-00-00 00:00:00 (UTC) 2008-05-27 12:23:50 (BRT) 3144 0 0 2292751
it.html 2008-05-15 15:27:58 (BRT) 2008-05-27 00:00:00 (BRT) 0000-00-00 00:00:00 (UTC) 2008-05-27 12:23:50 (BRT) 13814 0 0 2292753
license.txt 2008-04-16 23:38:42 (BRT) 2009-04-17 00:00:00 (BRT) 0000-00-00 00:00:00 (UTC) 2008-05-27 12:23:50 (BRT) 13901 0 0 2292754
index.html
Ascii
Hex
Ascii strings
Export
Bookmark
1/1
Go to page:
Page size: 100
Unit
Show all data
ear^
W,,T{&
:O@#Vj
kn]
W?`A
/cc[Wd
MxG%
Concluído


PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/analysis_file.php
Google
Mais visitados
Getting Started
Latest Headlin...
Case: Pendrive4GB | Image: Pendrive4GB
File analysis
Timeline
Keyword
Gallery
Image details
Data unit
Bookmark
Reports
[X] Close analysis
Pendrive4GB
partition-0 [fat32]
SecurDataStorRM
PocketCache Trial Version
SecurDataStor
.Trash-1000
Fdtk704
Mrecover
_243421_
BI-MBA2008
CCleaner
vmware-linux
Vista-SP1_Crack (cópia)
midnight
Paulo
images
Fotos
Linux
Manuais-FDTK
Adobe CS4 Activation Patch
listed files:8 | Total filtered files:0 | Total bookmarked files:0
Name
Modified
Accessed
Changed
Birth
Size
UID
GID
Meta
admin.html
2008-05-15 15:53:26 (BRT)
2008-05-27 00:00:00 (BRT)
0000-00-00 00:00:00 (UTC)
2008-05-27 12:23:46 (BRT)
13771
0
0
2292742
default.css
2008-05-16 10:10:36 (BRT)
2009-04-10 00:00:00 (BRT)
0000-00-00 00:00:00 (UTC)
2008-05-27 12:23:48 (BRT)
4935
0
0
2292743
Default.htm
2008-05-15 15:59:34 (BRT)
2008-05-27 00:00:00 (BRT)
0000-00-00 00:00:00 (UTC)
2008-05-27 12:23:48 (BRT)
8164
0
0
2292745
admin.html
Ascii
Hex
Ascii strings
Export
Bookmark
1/1
Go to page:
Page size: 100
Unit
Show all data
Depois de 10 segundo voc
ser
redirecionado para o site Viva o Linux.
</body>
</html>
<table style="border-collapse: collapse;" id="AutoNumber5" border="1"
<tbody><tr>
<td style="border-style: none; border-width: medium;" bgcolor="#0
Concluído


PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/analysis_file.php#
Google
Mais visitados
Getting Started
Latest Headlin...
Case: Pendrive4GB | Image: Pendrive4GB
File analysis
[X] Close analysis
Timeline
Keyword
Gallery
Image details
Data unit
Bookmark
Reports
Planejamento
Plvrs-Cruzds 6.0 + Crack
palavrascruzadas-7.0
isos
linux paulo
Site-clariant
Fdtk-Tools
Active@_Undelete
SBSEG-2007
scripts-forense
pasta sem titulo
Easy Recovery
Vista-SP1_Crack
Toshiba
Anti-virus-server
_969974_
_184734_
_544390_
W3k-MUI-SP2
_378089_
listed files:47 | Total filtered files:0 | Total bookmarked files:0
Name
Modified
Accessed
Changed
Birth
Size
UID
GID
minicurso - Forense-v3.doc
2008-11-05 15:28:00 (BRST)
2009-04-17 00:00:00 (BRT)
0000-00-00 00:00:00 (UTC)
2008-11-05 16:05:40 (BRST)
877056
0
0
_WRD0002.tmp
2008-11-05 16:14:22 (BRST)
2008-11-05 00:00:00 (BRST)
0000-00-00 00:00:00 (UTC)
2008-11-05 16:14:18 (BRST)
167424
0
0
Acesso Indevido.doc
2008-11-05 16:14:22 (BRST)
2008-11-05 00:00:00 (BRST)
0000-00-00 00:00:00 (UTC)
2008-11-05 16:14:18 (BRST)
167424
0
0
_WRD0002.tmp
Ascii
Hex
Ascii strings
Export
Bookmark
1/1
Go to page:
Page size: 100
Unit
Show all
Microsoft Office Document
Microsoft Word Document
lise do e-mail impresso e com depoimento do respons
vel pela rodovi
ria, deduziu-se que o e-mail foi criado por um funcion
rio, mais especificamente, um vigia. Sabe-se que os vigias utilizam um co
Internet, dispon
vel para os funcion
rios durante o hor
rio de descanso. A pol
Concluído

PTK - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

http://localhost/ptk/lib/analysis_file.php#

Mais visitados Getting Started Latest Headlin...

Case: Pendrive4GB | Image: Pendrive4GB

File analysis | Timeline | Keyword | Gallery | Image details | Data unit | Bookmark | Reports

[X] Close analysis

- _666343_
- Nova pasta
- Dicionário Aurélio
- BrOffice-3.1-Br
- _401031_
- Themes
- Wallpaper
- _083265_
- _092656_
- _551796_
- Nova Pasta
- _aime
- _126390_
- _128218_
- Controle Geral
- A.Lenda.Do.Tesouro.Perdido.2
- Novos
- Novos-Areva
- Areva
- HistAreva

otal listed files:2 | Total filtered files:0 | Total bookmarked files:0

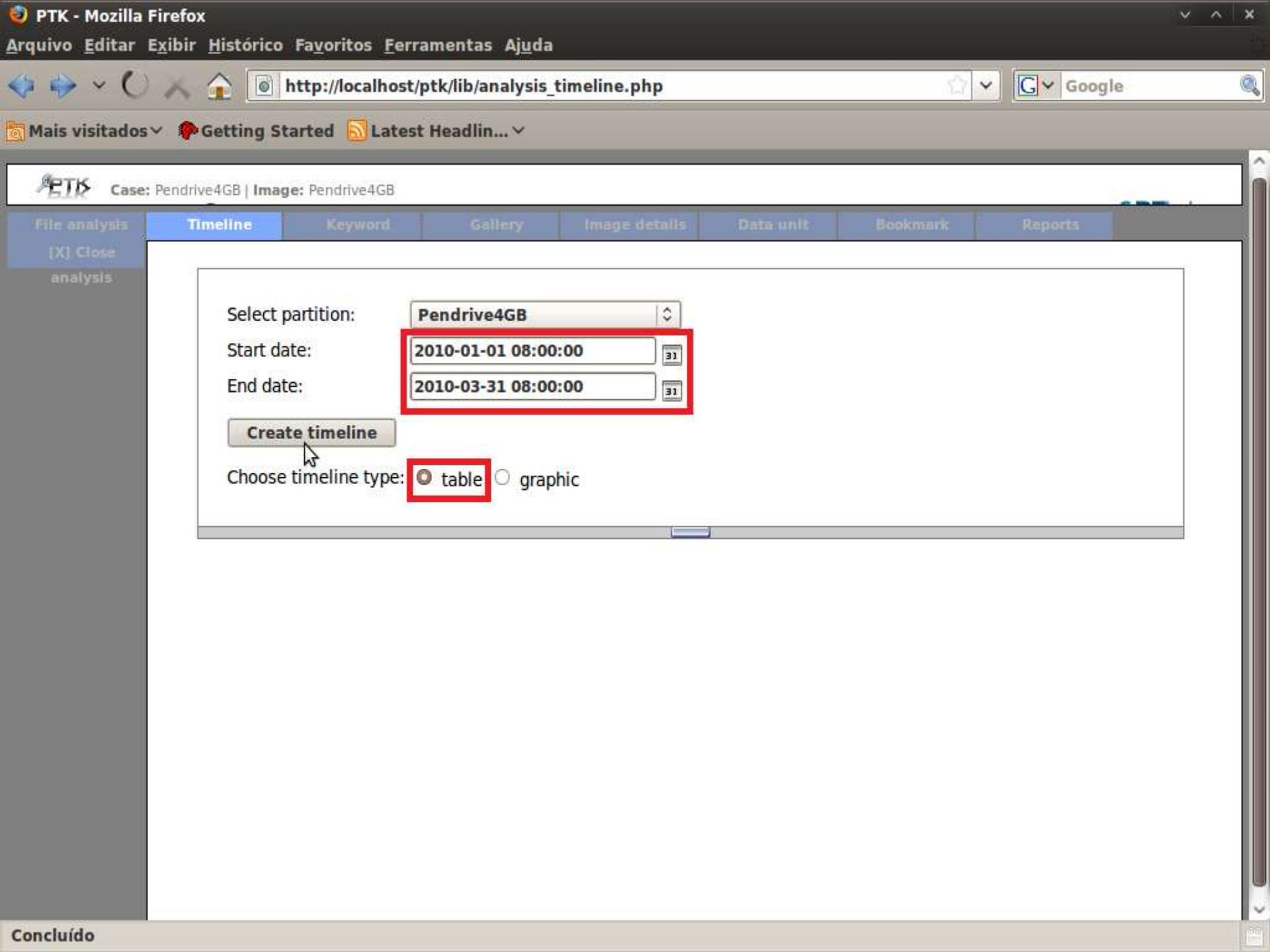
Name	Modified	Accessed	Changed	Birth	Size	UID	GID	Meta
Zune Widescreen.jpg	2008-08-16 02:26:36 (BRT)	2010-04-30 00:00:00 (BRT)	0000-00-00 00:00:00 (UTC)	2009-05-09 19:05:14 (BRT)	676135	0	0	116545543
Zune.jpg	2008-08-21 22:56:08 (BRT)	2010-04-30 00:00:00 (BRT)	0000-00-00 00:00:00 (UTC)	2009-05-09 19:05:14 (BRT)	266981	0	0	116545545

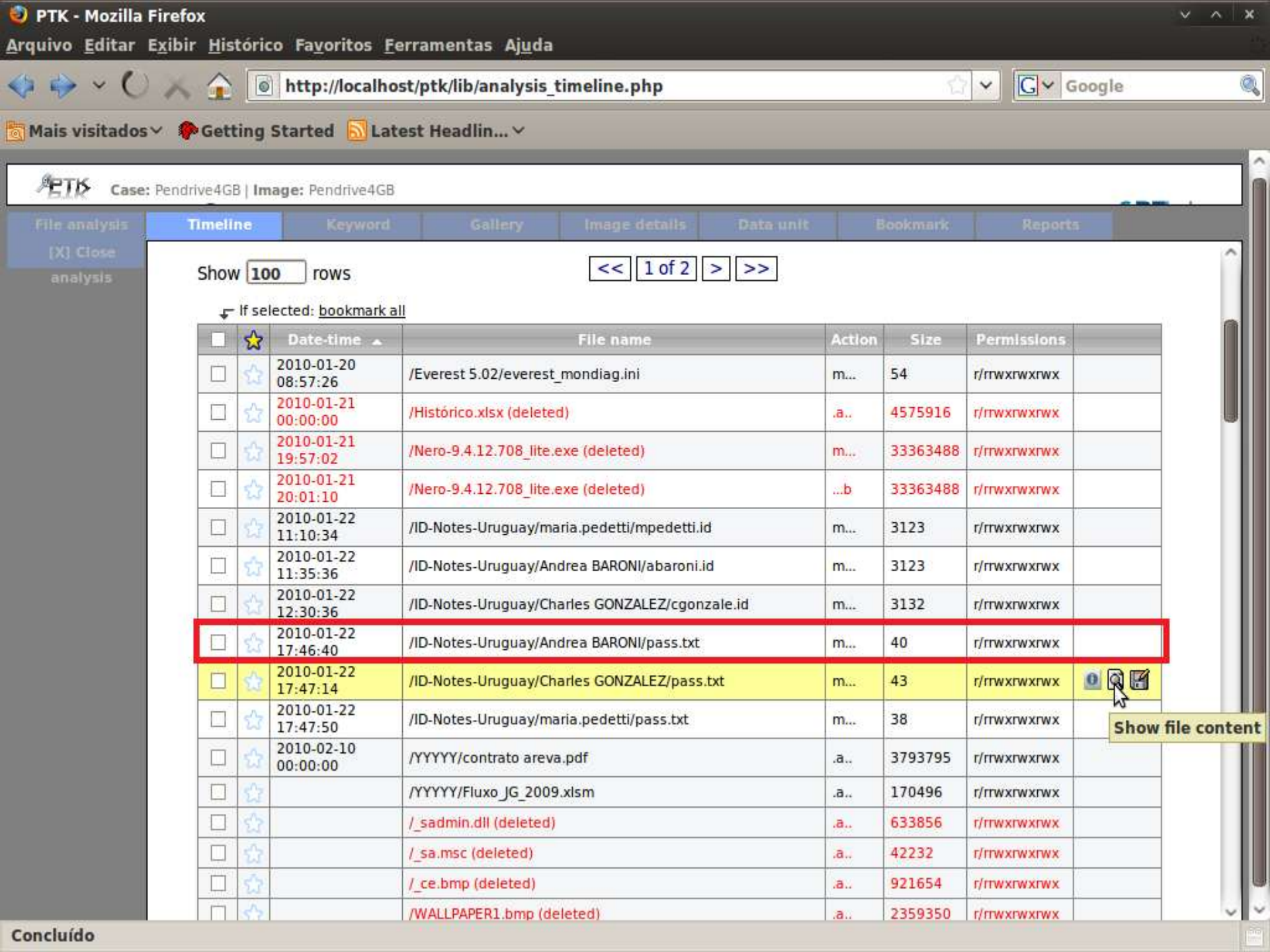
Zune.jpg

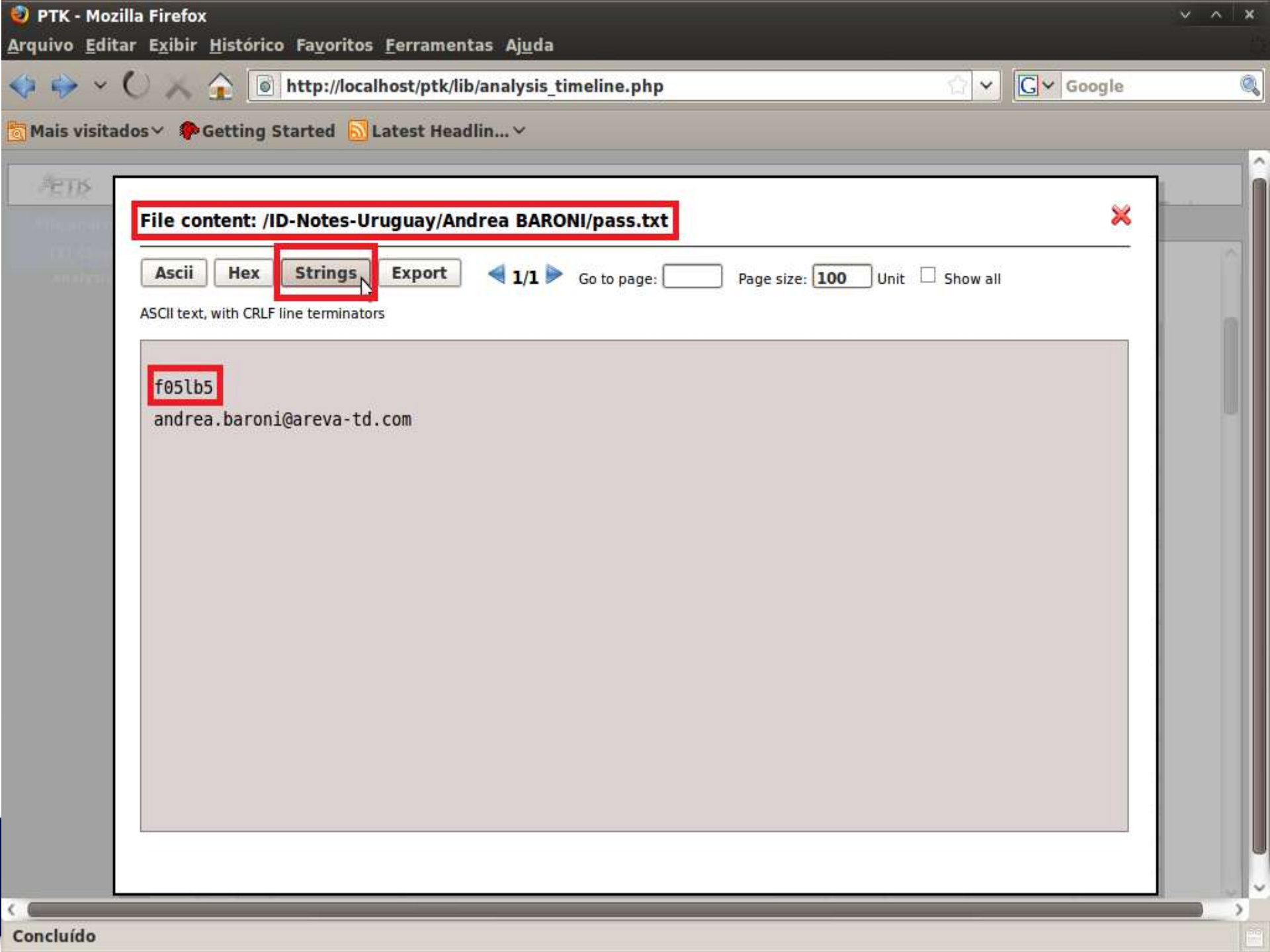
Ascii | Hex | Ascii strings | Preview | Export | Bookmark

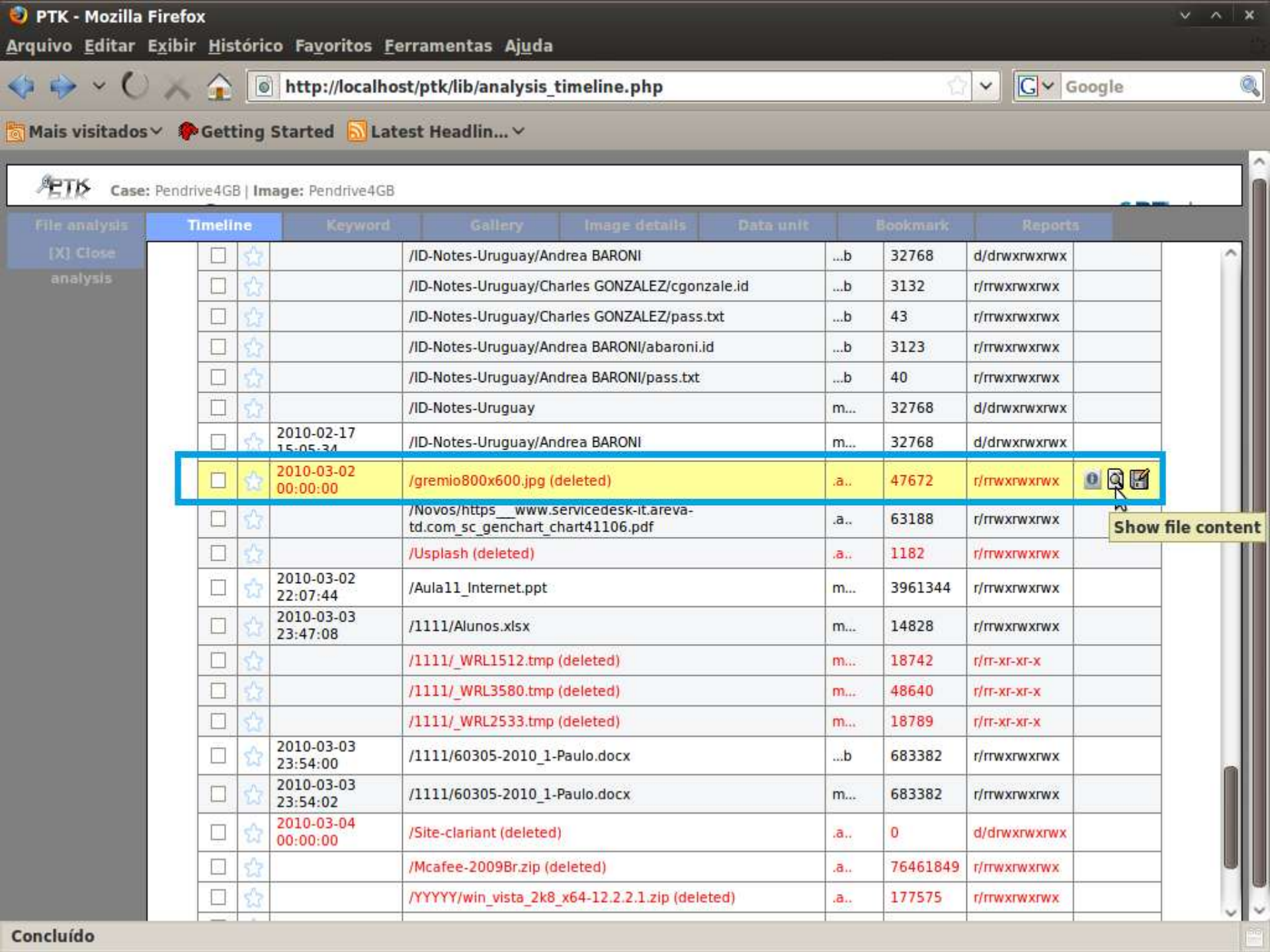
JPEG image data, JFIF standard 1.01

http://localhost/ptk/lib/analysis_file.php#


PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/analysis_timeline.php
Google
Mais visitados
Getting Started
Latest Headlin...
Case: Pendrive4GB | Image: Pendrive4GB
File analysis
[X] Close analysis
Timeline
Keyword
Gallery
Image details
Data unit
Bookmark
Reports
Select partition:
Pendrive4GB
Start date:
2010-01-01 08:00:00
End date:
2010-03-31 08:00:00
Create timeline
Choose timeline type:
table
graphic
Concluído


PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/analysis_timeline.php
Google
Mais visitados
Getting Started
Latest Headlin...
Case: Pendrive4GB | Image: Pendrive4GB
File analysis
[X] Close analysis
Timeline
Keyword
Gallery
Image details
Data unit
Bookmark
Reports
Show 100 rows
<< 1 of 2 > >>
If selected: bookmark all
Date-time
File name
Action
Size
Permissions
2010-01-20 08:57:26 /Everest 5.02/everest_mondiag.ini m... 54 r/rrwxrwxrwx
2010-01-21 00:00:00 /Histórico.xlsx (deleted) .a.. 4575916 r/rrwxrwxrwx
2010-01-21 19:57:02 /Nero-9.4.12.708_lite.exe (deleted) m... 33363488 r/rrwxrwxrwx
2010-01-21 20:01:10 /Nero-9.4.12.708_lite.exe (deleted) ...b 33363488 r/rrwxrwxrwx
2010-01-22 11:10:34 /ID-Notes-Uruguay/maria.pedetti/mpedetti.id m... 3123 r/rrwxrwxrwx
2010-01-22 11:35:36 /ID-Notes-Uruguay/Andrea BARONI/abaroni.id m... 3123 r/rrwxrwxrwx
2010-01-22 12:30:36 /ID-Notes-Uruguay/Charles GONZALEZ/cgonzale.id m... 3132 r/rrwxrwxrwx
2010-01-22 17:46:40 /ID-Notes-Uruguay/Andrea BARONI/pass.txt m... 40 r/rrwxrwxrwx
2010-01-22 17:47:14 /ID-Notes-Uruguay/Charles GONZALEZ/pass.txt m... 43 r/rrwxrwxrwx
2010-01-22 17:47:50 /ID-Notes-Uruguay/maria.pedetti/pass.txt m... 38 r/rrwxrwxrwx
2010-02-10 00:00:00 /YYYYY/contrato areva.pdf .a.. 3793795 r/rrwxrwxrwx
/YYYYY/Fluxo_JG_2009.xlsm .a.. 170496 r/rrwxrwxrwx
/_sadmin.dll (deleted) .a.. 633856 r/rrwxrwxrwx
/_sa.msc (deleted) .a.. 42232 r/rrwxrwxrwx
/_ce.bmp (deleted) .a.. 921654 r/rrwxrwxrwx
/WALLPAPER1.bmp (deleted) .a.. 2359350 r/rrwxrwxrwx
Show file content
Concluído


PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/analysis_timeline.php
Google
Mais visitados
Getting Started
Latest Headlin...
File content: /ID-Notes-Uruguay/Andrea BARONI/pass.txt
Ascii
Hex
Strings
Export
1/1
Go to page:
Page size: 100
Unit
Show all
ASCII text, with CRLF line terminators
f05lb5
andrea.baroni@areva-td.com
Concluído


PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/analysis_timeline.php
Google
Mais visitados
Getting Started
Latest Headlin...
Case: Pendrive4GB | Image: Pendrive4GB
File analysis
[X] Close analysis
Timeline
Keyword
Gallery
Image details
Data unit
Bookmark
Reports
/ID-Notes-Uruguay/Andrea BARONI ...b 32768 d/drwxrwxrwx
/ID-Notes-Uruguay/Charles GONZALEZ/cgonzale.id ...b 3132 r/rrwxrwxrwx
/ID-Notes-Uruguay/Charles GONZALEZ/pass.txt ...b 43 r/rrwxrwxrwx
/ID-Notes-Uruguay/Andrea BARONI/abaroni.id ...b 3123 r/rrwxrwxrwx
/ID-Notes-Uruguay/Andrea BARONI/pass.txt ...b 40 r/rrwxrwxrwx
/ID-Notes-Uruguay m... 32768 d/drwxrwxrwx
2010-02-17 15:05:34 /ID-Notes-Uruguay/Andrea BARONI m... 32768 d/drwxrwxrwx
2010-03-02 00:00:00 /gremio800x600.jpg (deleted) .a.. 47672 r/rrwxrwxrwx
/Novos/https__www.servicedesk-it.areva-td.com_sc_genchart_chart41106.pdf .a.. 63188 r/rrwxrwxrwx
/Usplash (deleted) .a.. 1182 r/rrwxrwxrwx
2010-03-02 22:07:44 /Aula11_Internet.ppt m... 3961344 r/rrwxrwxrwx
2010-03-03 23:47:08 /1111/Alunos.xlsx m... 14828 r/rrwxrwxrwx
/1111/_WRL1512.tmp (deleted) m... 18742 r/rr-xr-xr-x
/1111/_WRL3580.tmp (deleted) m... 48640 r/rr-xr-xr-x
/1111/_WRL2533.tmp (deleted) m... 18789 r/rr-xr-xr-x
2010-03-03 23:54:00 /1111/60305-2010_1-Paulo.docx ...b 683382 r/rrwxrwxrwx
2010-03-03 23:54:02 /1111/60305-2010_1-Paulo.docx m... 683382 r/rrwxrwxrwx
2010-03-04 00:00:00 /Site-clariant (deleted) .a.. 0 d/drwxrwxrwx
/Mcafee-2009Br.zip (deleted) .a.. 76461849 r/rrwxrwxrwx
/YYYYY/win_vista_2k8_x64-12.2.2.1.zip (deleted) .a.. 177575 r/rrwxrwxrwx
Show file content
Concluído

PTK - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

http://localhost/ptk/lib/analysis_timeline.php

Google

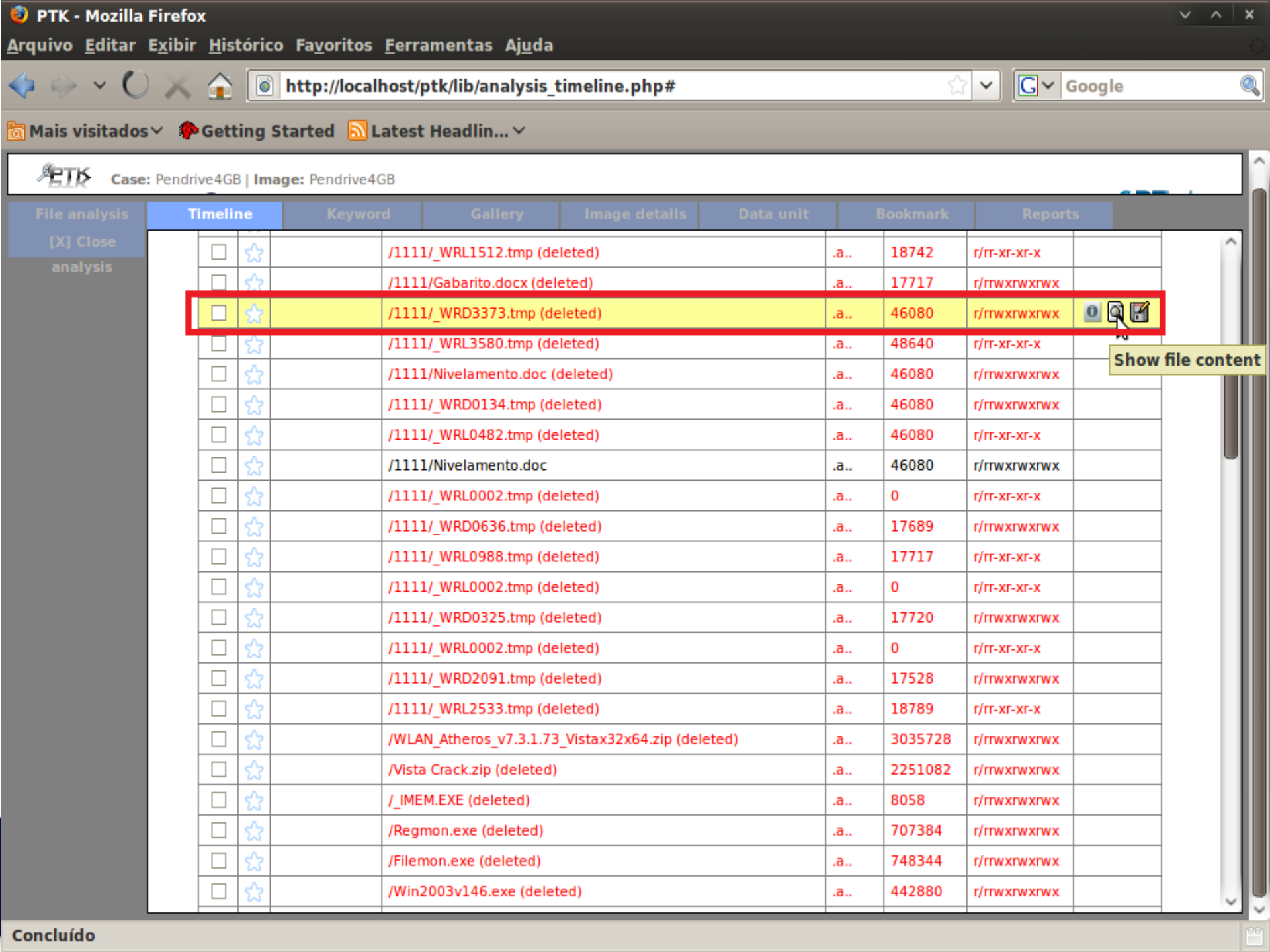
Mais visitados Getting Started Latest Headlin...

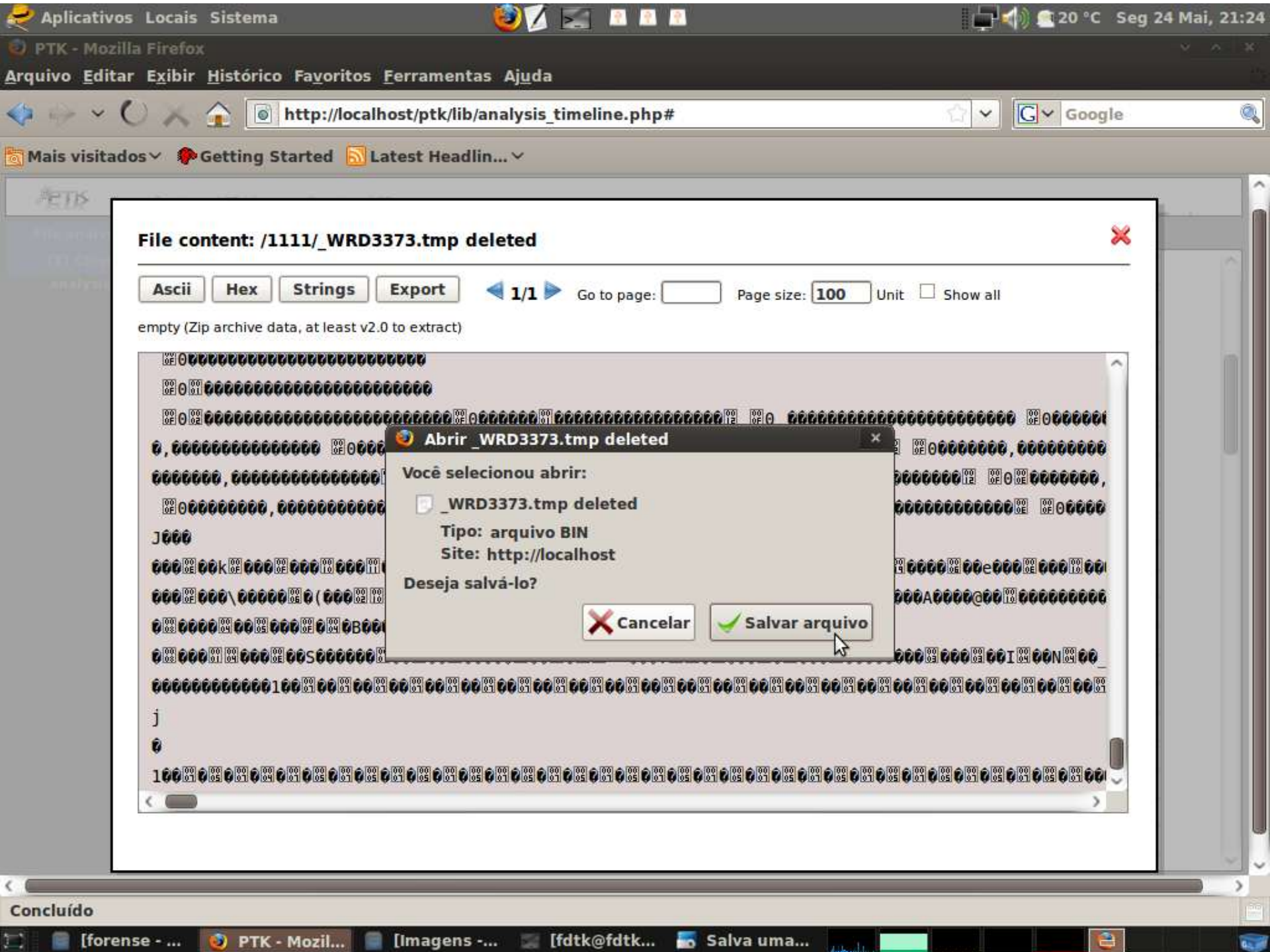
File content: /gremio800x600.jpg deleted

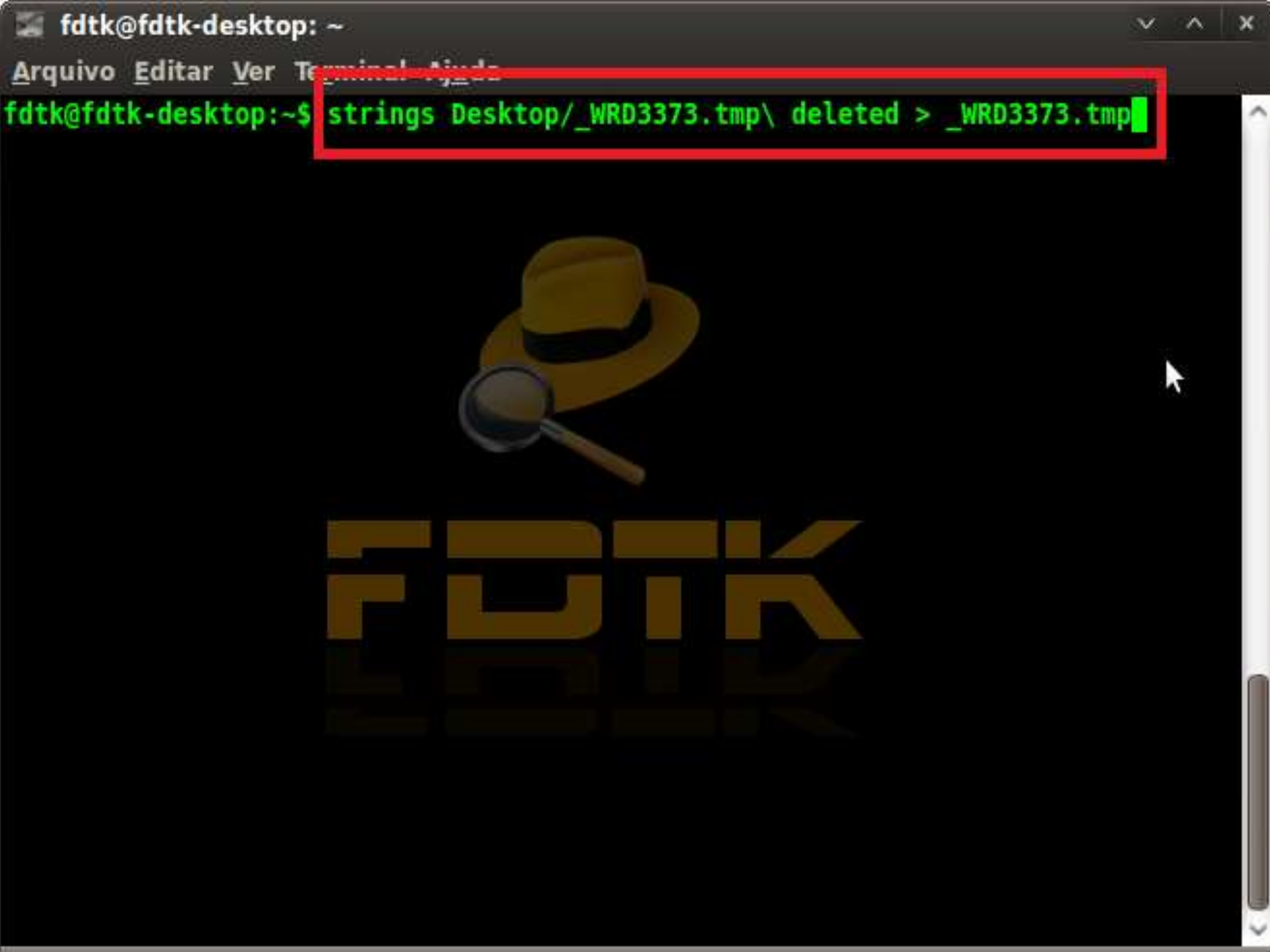
Ascii | Hex | Strings | Preview | Export

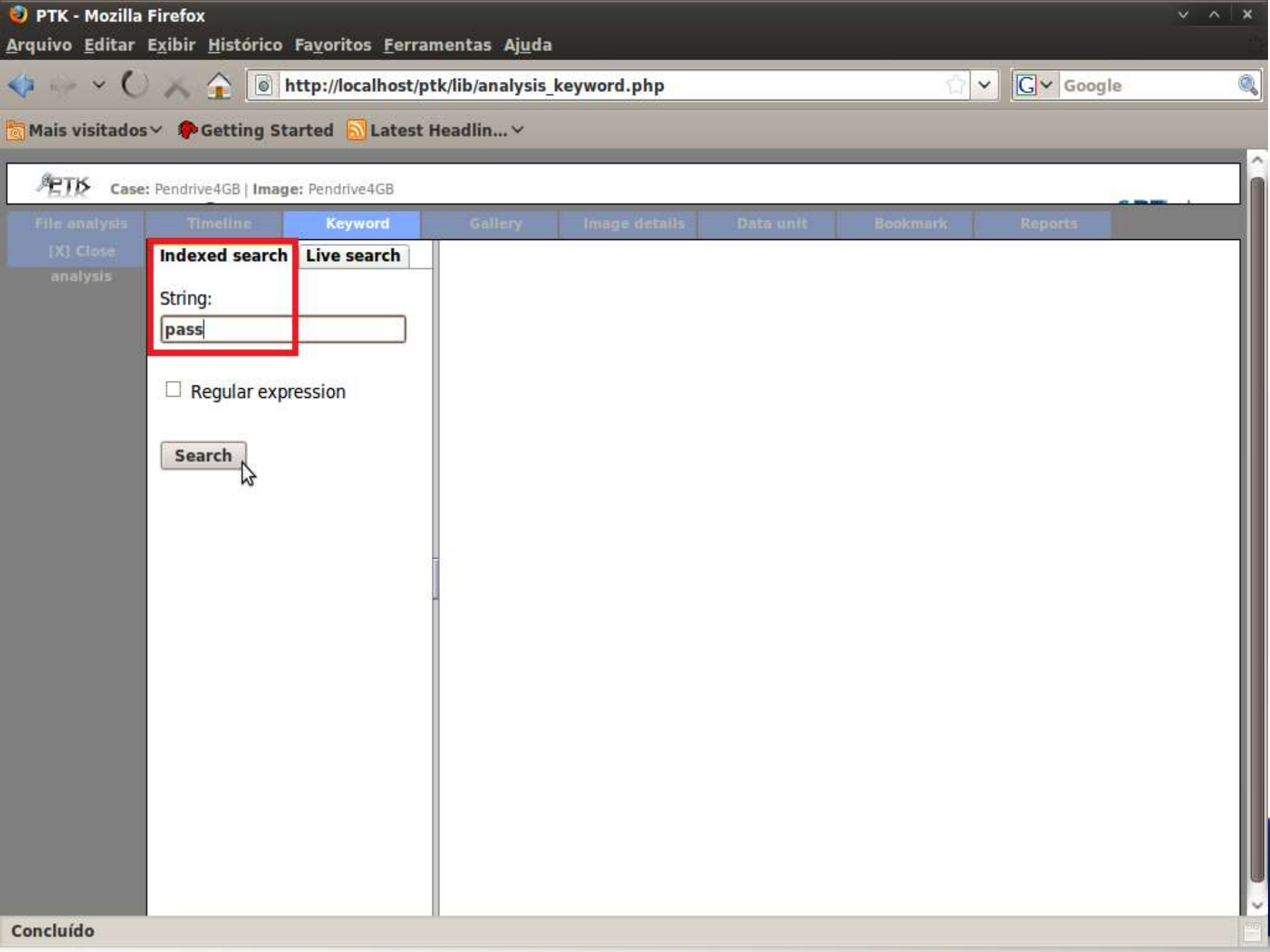
JPEG image data, JFIF standard 1.02

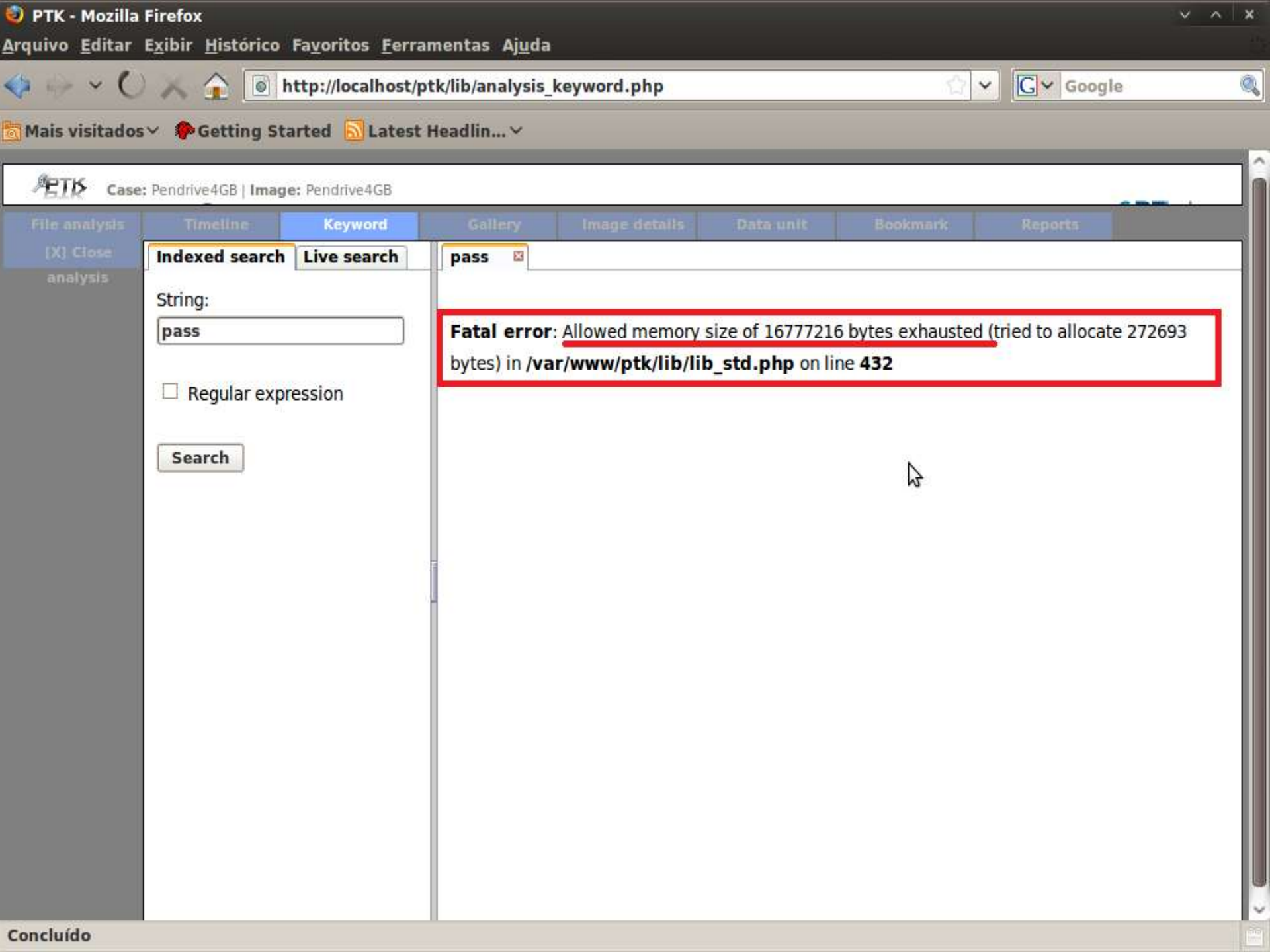
http://localhost/ptk/lib/picture.php?offset=192&inode=563&name=gremio800x600.jpg+deleted


PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/analysis_timeline.php#
Google
Mais visitados
Getting Started
Latest Headlin...
Case: Pendrive4GB | Image: Pendrive4GB
File analysis
[X] Close analysis
Timeline
Keyword
Gallery
Image details
Data unit
Bookmark
Reports
/1111/_WRL1512.tmp (deleted) .a.. 18742 r/rr-xr-xr-x
/1111/Gabarito.docx (deleted) .a.. 17717 r/rrwxrwxrwx
/1111/_WRD3373.tmp (deleted) .a.. 46080 r/rrwxrwxrwx
/1111/_WRL3580.tmp (deleted) .a.. 48640 r/rr-xr-xr-x
/1111/Nivelamento.doc (deleted) .a.. 46080 r/rrwxrwxrwx
/1111/_WRD0134.tmp (deleted) .a.. 46080 r/rrwxrwxrwx
/1111/_WRL0482.tmp (deleted) .a.. 46080 r/rr-xr-xr-x
/1111/Nivelamento.doc .a.. 46080 r/rrwxrwxrwx
/1111/_WRL0002.tmp (deleted) .a.. 0 r/rr-xr-xr-x
/1111/_WRD0636.tmp (deleted) .a.. 17689 r/rrwxrwxrwx
/1111/_WRL0988.tmp (deleted) .a.. 17717 r/rr-xr-xr-x
/1111/_WRL0002.tmp (deleted) .a.. 0 r/rr-xr-xr-x
/1111/_WRD0325.tmp (deleted) .a.. 17720 r/rrwxrwxrwx
/1111/_WRL0002.tmp (deleted) .a.. 0 r/rr-xr-xr-x
/1111/_WRD2091.tmp (deleted) .a.. 17528 r/rrwxrwxrwx
/1111/_WRL2533.tmp (deleted) .a.. 18789 r/rr-xr-xr-x
/WLAN_Atheros_v7.3.1.73_Vistax32x64.zip (deleted) .a.. 3035728 r/rrwxrwxrwx
/Vista Crack.zip (deleted) .a.. 2251082 r/rrwxrwxrwx
/_IMEM.EXE (deleted) .a.. 8058 r/rrwxrwxrwx
/Regmon.exe (deleted) .a.. 707384 r/rrwxrwxrwx
/Filemon.exe (deleted) .a.. 748344 r/rrwxrwxrwx
/Win2003v146.exe (deleted) .a.. 442880 r/rrwxrwxrwx
Show file content
Concluído


Aplicativos Locais Sistema
20 °C Seg 24 Mai, 21:24
PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/analysis_timeline.php#
Google
Mais visitados
Getting Started
Latest Headlin...
File content: /1111/_WRD3373.tmp deleted
Ascii
Hex
Strings
Export
1/1
Go to page:
Page size: 100
Unit
Show all
empty (Zip archive data, at least v2.0 to extract)
Abrir _WRD3373.tmp deleted
Você selecionou abrir:
_WRD3373.tmp deleted
Tipo: arquivo BIN
Site: http://localhost
Deseja salvá-lo?
Cancelar
Salvar arquivo
Concluído
[forense - ...
PTK - Mozil...
[Imagens -...
[fdtk@fdtk...
Salva uma...


fdtk@fdtk-desktop: ~
Arquivo Editar Ver Terminal Ajuda
fdtk@fdtk-desktop:~$ strings Desktop/_WRD3373.tmp\ deleted > _WRD3373.tmp
FDTK

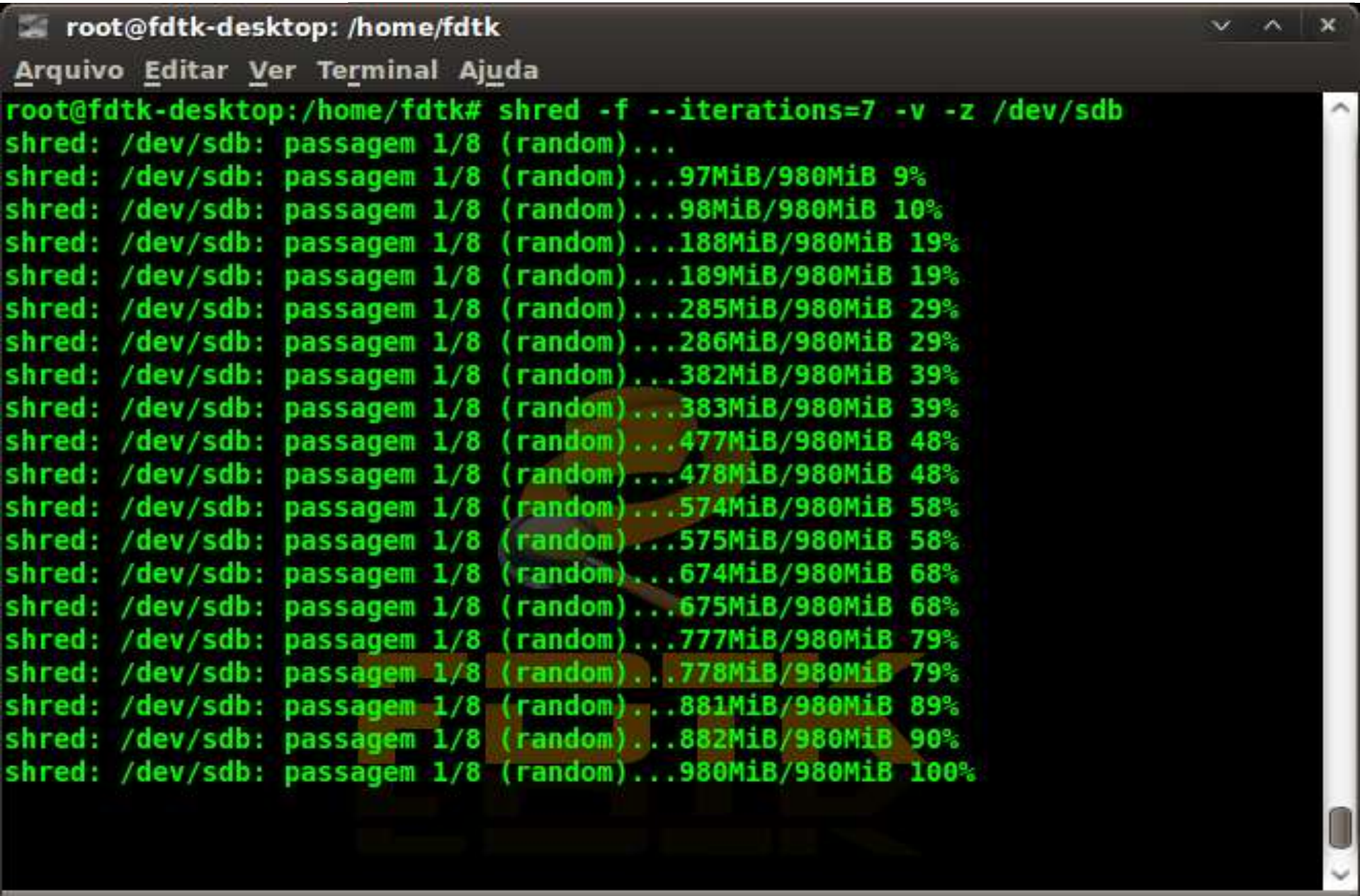

PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/analysis_keyword.php
Google
Mais visitados
Getting Started
Latest Headlin...
Case: Pendrive4GB | Image: Pendrive4GB
File analysis
[X] Close analysis
Timeline
Keyword
Gallery
Image details
Data unit
Bookmark
Reports
Indexed search
Live search
String:
pass
Regular expression
Search
Concluído


PTK - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://localhost/ptk/lib/analysis_keyword.php
Google
Mais visitados
Getting Started
Latest Headlin...
Case: Pendrive4GB | Image: Pendrive4GB
File analysis
Timeline
Keyword
Gallery
Image details
Data unit
Bookmark
Reports
[X] Close analysis
Indexed search
Live search
pass
String:
pass
Regular expression
Search
Fatal error: Allowed memory size of 16777216 bytes exhausted (tried to allocate 272693 bytes) in /var/www/ptk/lib/lib_std.php on line 432
Concluído

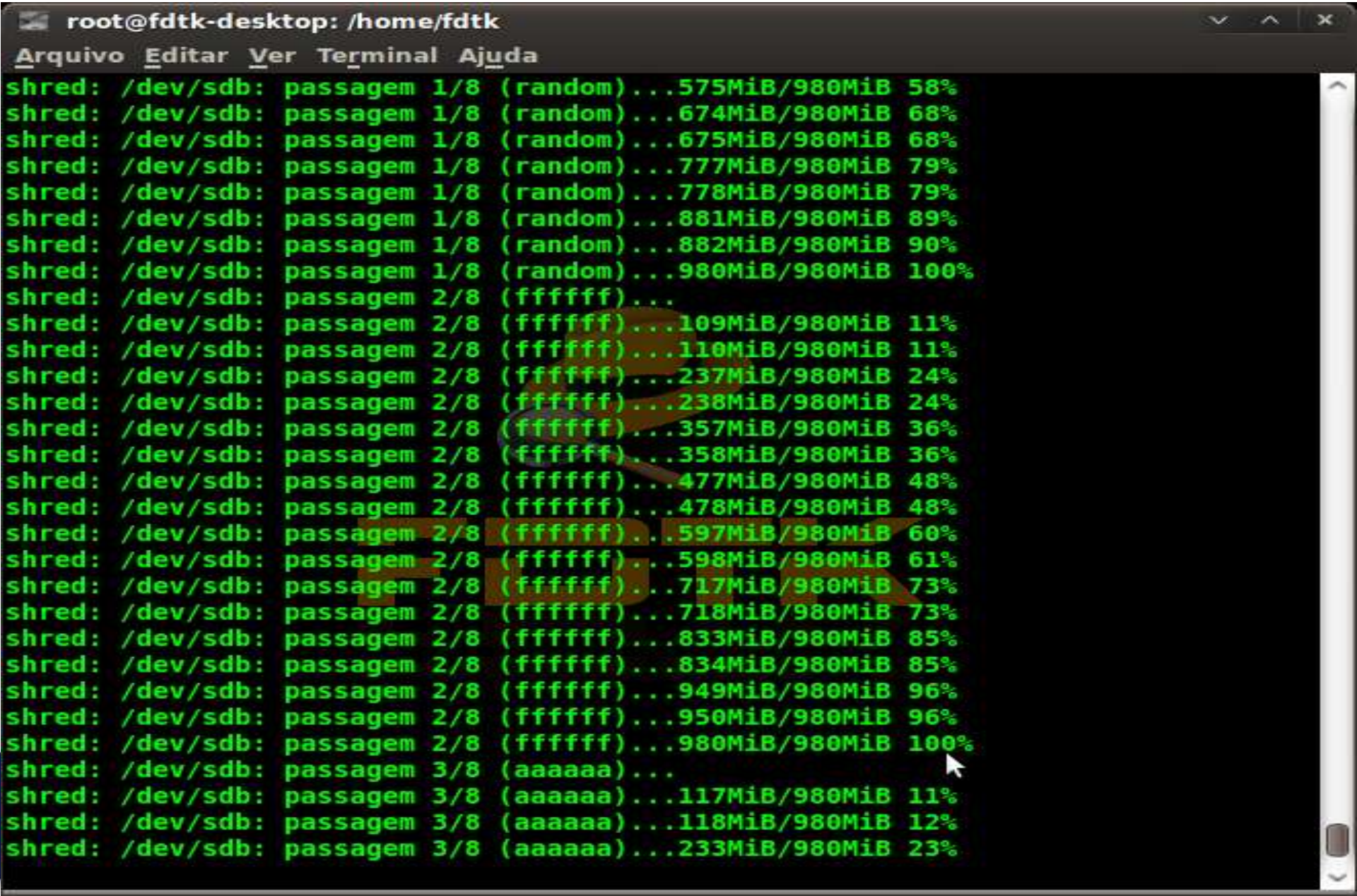
Wiping

- ✓ Manter seu Kit Forense em devidas condições;
- ✓ Rotina de checar cabos, adaptadores, mídias e etc.;
- ✓ Ter a mão um conjunto de HD's de diversas capacidades de armazenamento devidamente sanitizados.
- ✓ **Wipe** – Utilitário que efetua sobrescrita com números aleatórios ou zeros e uns no disco inteiro ou na área de um arquivo.
- ✓ Uso wipe [opção] arquivo.....
  - # ***wipe -f -i -Q 7 /dev/sdb***
- **Shred** – Utilitário que efetua sobrescrita com números aleatórios ou zeros e uns no disco inteiro ou na área de um arquivo.
- ✓ Uso shred [opções]... arquivo.....
  - ***# shred -f --iteraction=7 -v -z /dev/sdb***
    - ***-f*** → *force;*
    - ***--iteraction=7*** → *7 passes;*
    - ***-v*** → *modo verbose;*
    - ***-z*** → *após o sétimo passe realiza um oitavo gravando zeros.*

Wiping

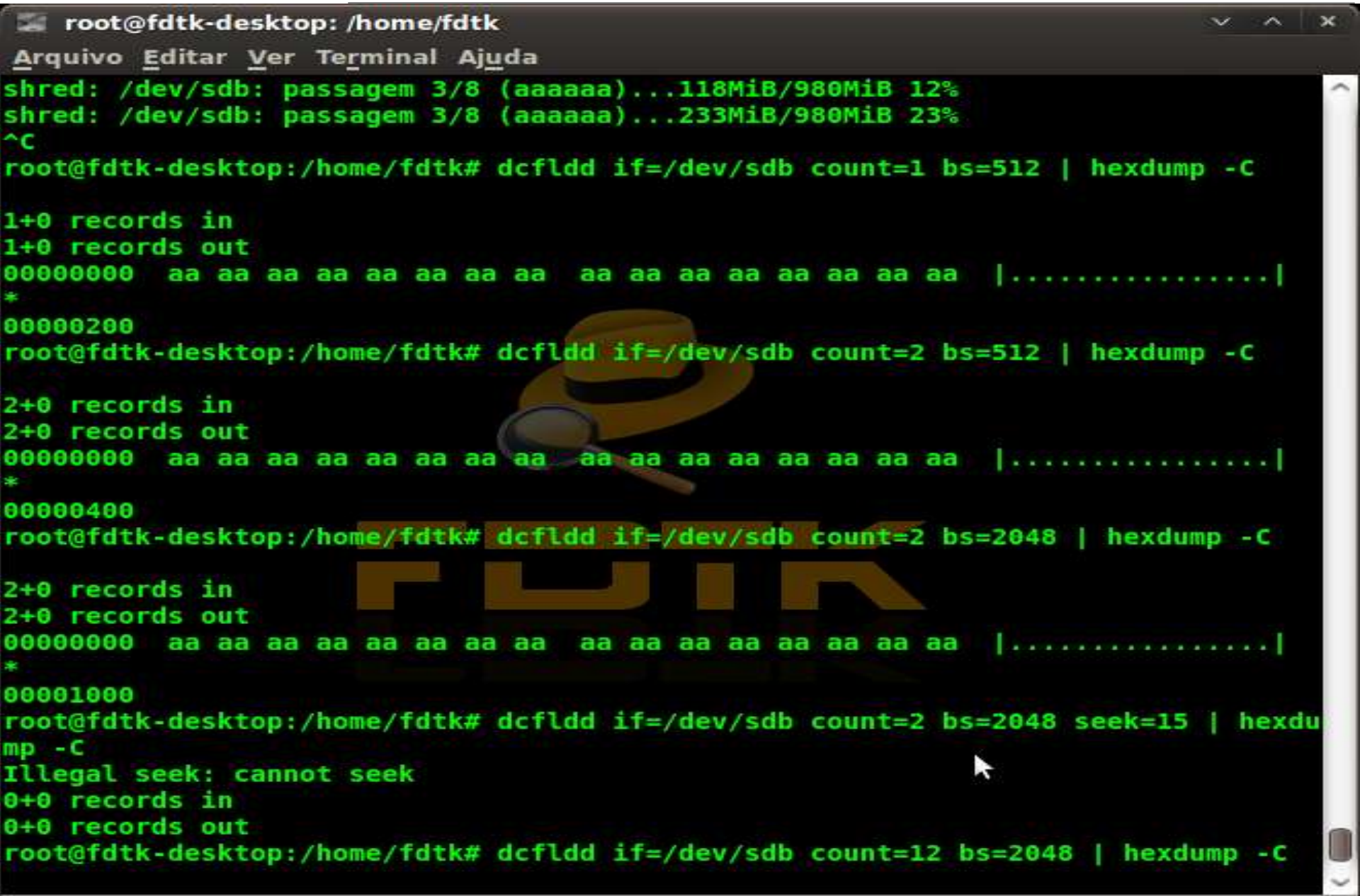

root@fdtk-desktop: /home/fdtk
Arquivo Editar Ver Terminal Ajuda
root@fdtk-desktop:/home/fdtk# shred -f --iterations=7 -v -z /dev/sdb
shred: /dev/sdb: passagem 1/8 (random)...
shred: /dev/sdb: passagem 1/8 (random)...97MiB/980MiB 9%
shred: /dev/sdb: passagem 1/8 (random)...98MiB/980MiB 10%
shred: /dev/sdb: passagem 1/8 (random)...188MiB/980MiB 19%
shred: /dev/sdb: passagem 1/8 (random)...189MiB/980MiB 19%
shred: /dev/sdb: passagem 1/8 (random)...285MiB/980MiB 29%
shred: /dev/sdb: passagem 1/8 (random)...286MiB/980MiB 29%
shred: /dev/sdb: passagem 1/8 (random)...382MiB/980MiB 39%
shred: /dev/sdb: passagem 1/8 (random)...383MiB/980MiB 39%
shred: /dev/sdb: passagem 1/8 (random)...477MiB/980MiB 48%
shred: /dev/sdb: passagem 1/8 (random)...478MiB/980MiB 48%
shred: /dev/sdb: passagem 1/8 (random)...574MiB/980MiB 58%
shred: /dev/sdb: passagem 1/8 (random)...575MiB/980MiB 58%
shred: /dev/sdb: passagem 1/8 (random)...674MiB/980MiB 68%
shred: /dev/sdb: passagem 1/8 (random)...675MiB/980MiB 68%
shred: /dev/sdb: passagem 1/8 (random)...777MiB/980MiB 79%
shred: /dev/sdb: passagem 1/8 (random)...778MiB/980MiB 79%
shred: /dev/sdb: passagem 1/8 (random)...881MiB/980MiB 89%
shred: /dev/sdb: passagem 1/8 (random)...882MiB/980MiB 90%
shred: /dev/sdb: passagem 1/8 (random)...980MiB/980MiB 100%

Wiping


root@fdtk-desktop: /home/fdtk
Arquivo Editar Ver Terminal Ajuda
shred: /dev/sdb: passagem 1/8 (random)...575MiB/980MiB 58%
shred: /dev/sdb: passagem 1/8 (random)...674MiB/980MiB 68%
shred: /dev/sdb: passagem 1/8 (random)...675MiB/980MiB 68%
shred: /dev/sdb: passagem 1/8 (random)...777MiB/980MiB 79%
shred: /dev/sdb: passagem 1/8 (random)...778MiB/980MiB 79%
shred: /dev/sdb: passagem 1/8 (random)...881MiB/980MiB 89%
shred: /dev/sdb: passagem 1/8 (random)...882MiB/980MiB 90%
shred: /dev/sdb: passagem 1/8 (random)...980MiB/980MiB 100%
shred: /dev/sdb: passagem 2/8 (ffffff)...
shred: /dev/sdb: passagem 2/8 (ffffff)...109MiB/980MiB 11%
shred: /dev/sdb: passagem 2/8 (ffffff)...110MiB/980MiB 11%
shred: /dev/sdb: passagem 2/8 (ffffff)...237MiB/980MiB 24%
shred: /dev/sdb: passagem 2/8 (ffffff)...238MiB/980MiB 24%
shred: /dev/sdb: passagem 2/8 (ffffff)...357MiB/980MiB 36%
shred: /dev/sdb: passagem 2/8 (ffffff)...358MiB/980MiB 36%
shred: /dev/sdb: passagem 2/8 (ffffff)...477MiB/980MiB 48%
shred: /dev/sdb: passagem 2/8 (ffffff)...478MiB/980MiB 48%
shred: /dev/sdb: passagem 2/8 (ffffff)...597MiB/980MiB 60%
shred: /dev/sdb: passagem 2/8 (ffffff)...598MiB/980MiB 61%
shred: /dev/sdb: passagem 2/8 (ffffff)...717MiB/980MiB 73%
shred: /dev/sdb: passagem 2/8 (ffffff)...718MiB/980MiB 73%
shred: /dev/sdb: passagem 2/8 (ffffff)...833MiB/980MiB 85%
shred: /dev/sdb: passagem 2/8 (ffffff)...834MiB/980MiB 85%
shred: /dev/sdb: passagem 2/8 (ffffff)...949MiB/980MiB 96%
shred: /dev/sdb: passagem 2/8 (ffffff)...950MiB/980MiB 96%
shred: /dev/sdb: passagem 2/8 (ffffff)...980MiB/980MiB 100%
shred: /dev/sdb: passagem 3/8 (aaaaaa)...
shred: /dev/sdb: passagem 3/8 (aaaaaa)...117MiB/980MiB 11%
shred: /dev/sdb: passagem 3/8 (aaaaaa)...118MiB/980MiB 12%
shred: /dev/sdb: passagem 3/8 (aaaaaa)...233MiB/980MiB 23%

✓*dcfldd if=/dev/sdb count=1 bs=512 | hexdump -C*

Wiping



✓ *# dcfldd pattern=00 of=/dev/sdb*

Wiping

```
root@fdtk-desktop: /home/fdtk
Arquivo Editar Ver Terminal Ajuda
root@fdtk-desktop:/home/fdtk# dcfldd pattern=00 of=/dev/sdb
31232 blocks (976Mb) written.
31361+0 records in
31360+0 records out
root@fdtk-desktop:/home/fdtk# dcfldd if=/dev/sdb count=1 bs=512 | hexdump -C

1+0 records in
1+0 records out
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000200
root@fdtk-desktop:/home/fdtk# dcfldd textpattern=abcde count=1 bs=512 seek=2 of=
/dev/sdb

1+0 records in
1+0 records out
root@fdtk-desktop:/home/fdtk# dcfldd if=/dev/sdb count=3 bs=512 | hexdump -C

00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
3+0 records in
3+0 records out
*
00000400  61 62 63 64 65 61 62 63  64 65 61 62 63 64 65 61  |abcdeabcdeabcdea|
00000410  62 63 64 65 61 62 63 64  65 61 62 63 64 65 61 62  |bcdeabcdeabcdeab|
00000420  63 64 65 61 62 63 64 65  61 62 63 64 65 61 62 63  |cdeabcdeabcdeabc|
00000430  64 65 61 62 63 64 65 61  62 63 64 65 61 62 63 64  |deabcdeabcdeabcd|
00000440  65 61 62 63 64 65 61 62  63 64 65 61 62 63 64 65  |eabcdeabcdeabcde|
00000450  61 62 63 64 65 61 62 63  64 65 61 62 63 64 65 61  |abcdeabcdeabcdea|
00000460  62 63 64 65 61 62 63 64  65 61 62 63 64 65 61 62  |bcdeabcdeabcdeab|
00000470  63 64 65 61 62 63 64 65  61 62 63 64 65 61 62 63  |cdeabcdeabcdeabc|
00000480  64 65 61 62 63 64 65 61  62 63 64 65 61 62 63 64  |deabcdeabcdeabcd|
```

Wiping

- ✓ *dcfldd if=/dev/sdb count=1 bs=512 | hexdump -C*
  - ➢ *count=1 → Um Setor*
  - ➢ *bs=512 → Tamanho do Setor*
- ✓ dcfldd textpattern=abcde count=1 bs=512 seek=2 of=/dev/sdb
  - ➢ *count=1 → Um bloco*
  - ➢ *bs=512 → 512 bytes*
  - ➢ seek=2 → Salta n blocos

```
root@fdtk-desktop: /home/fdtk
Arquivo Editar Ver Terminal Ajuda
root@fdtk-desktop:/home/fdtk# dcfldd pattern=00 of=/dev/sdb
31232 blocks (976Mb) written.
31361+0 records in
31360+0 records out
root@fdtk-desktop:/home/fdtk# dcfldd if=/dev/sdb count=1 bs=512 | hexdump -C

1+0 records in
1+0 records out
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000200
root@fdtk-desktop:/home/fdtk# dcfldd textpattern=abcde count=1 bs=512 seek=2 of=
/dev/sdb

1+0 records in
1+0 records out
root@fdtk-desktop:/home/fdtk# dcfldd if=/dev/sdb count=3 bs=512 | hexdump -C

00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
3+0 records in
3+0 records out
*
00000400  61 62 63 64 65 61 62 63  64 65 61 62 63 64 65 61  |abcdeabcdeabcdea|
00000410  62 63 64 65 61 62 63 64  65 61 62 63 64 65 61 62  |bcdeabcdeabcdeab|
00000420  63 64 65 61 62 63 64 65  61 62 63 64 65 61 62 63  |cdeabcdeabcdeabc|
00000430  64 65 61 62 63 64 65 61  62 63 64 65 61 62 63 64  |deabcdeabcdeabcd|
00000440  65 61 62 63 64 65 61 62  63 64 65 61 62 63 64 65  |eabcdeabcdeabcde|
00000450  61 62 63 64 65 61 62 63  64 65 61 62 63 64 65 61  |abcdeabcdeabcdea|
00000460  62 63 64 65 61 62 63 64  65 61 62 63 64 65 61 62  |bcdeabcdeabcdeab|
00000470  63 64 65 61 62 63 64 65  61 62 63 64 65 61 62 63  |cdeabcdeabcdeabc|
00000480  64 65 61 62 63 64 65 61  62 63 64 65 61 62 63 64  |deabcdeabcdeabcd|
```

FDTK

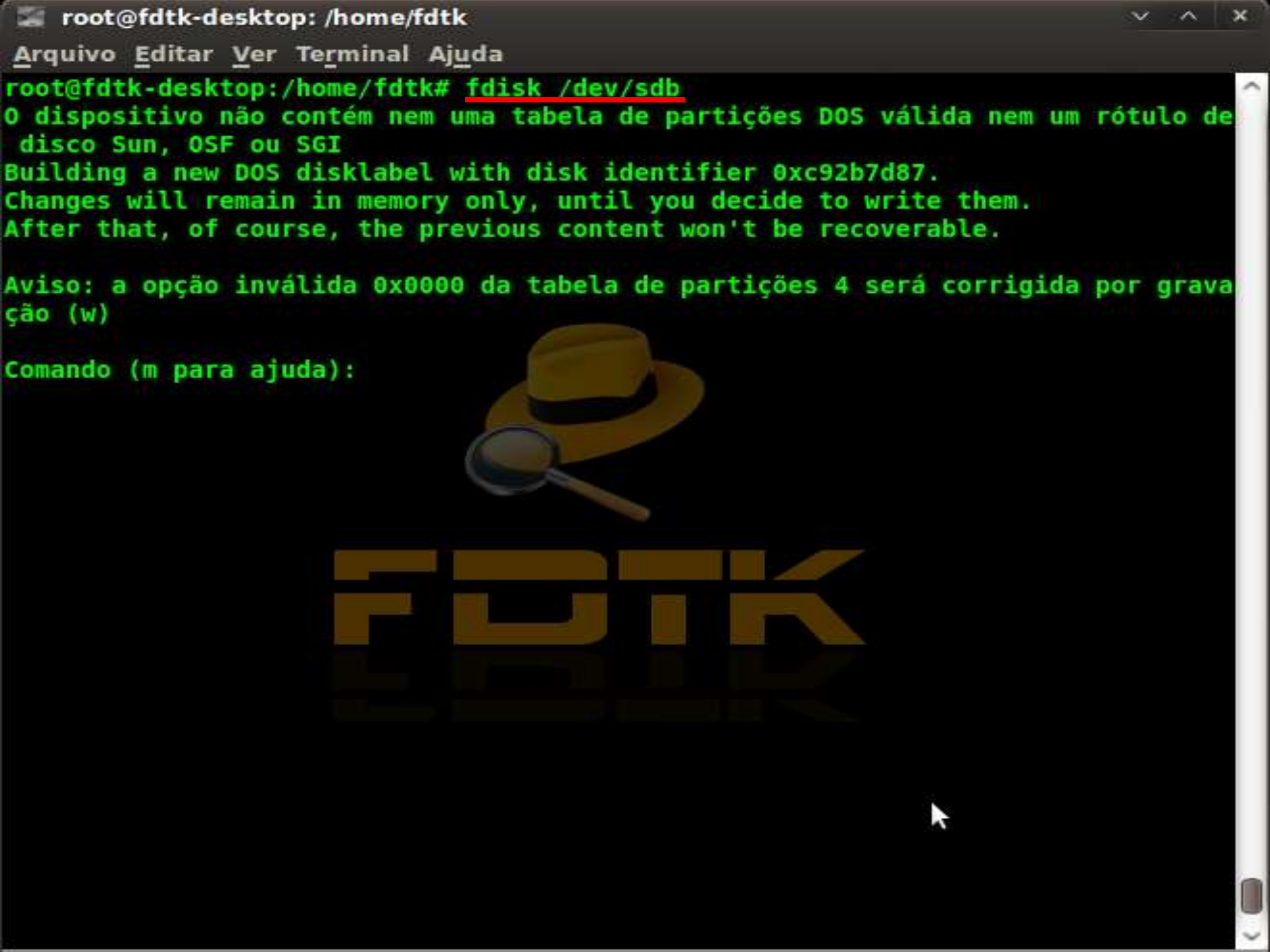
Wiping

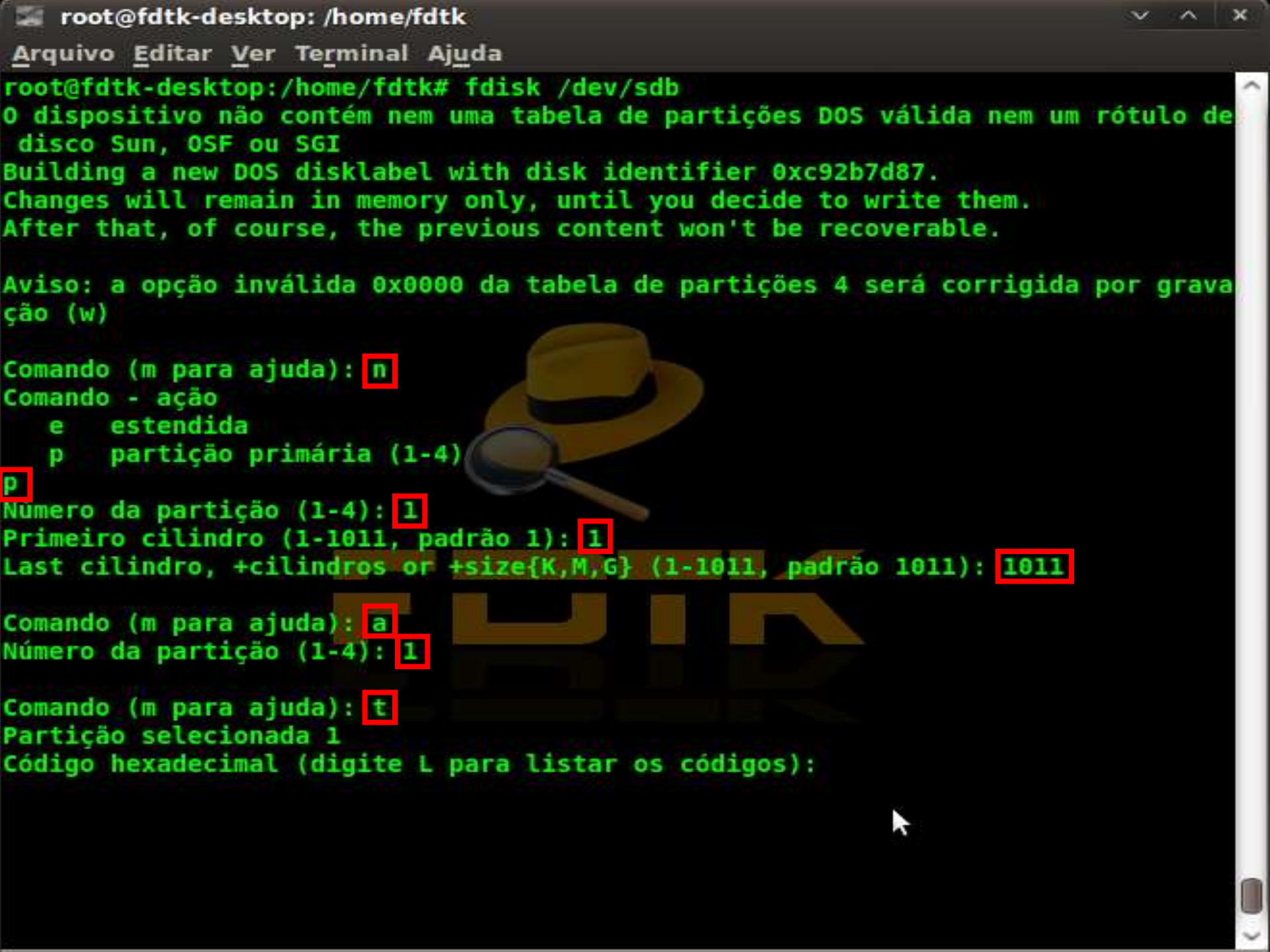
- **http://www.dc3.mil/dcfl/dcflAbout.php**

Defense Computer Forensics Laboratory

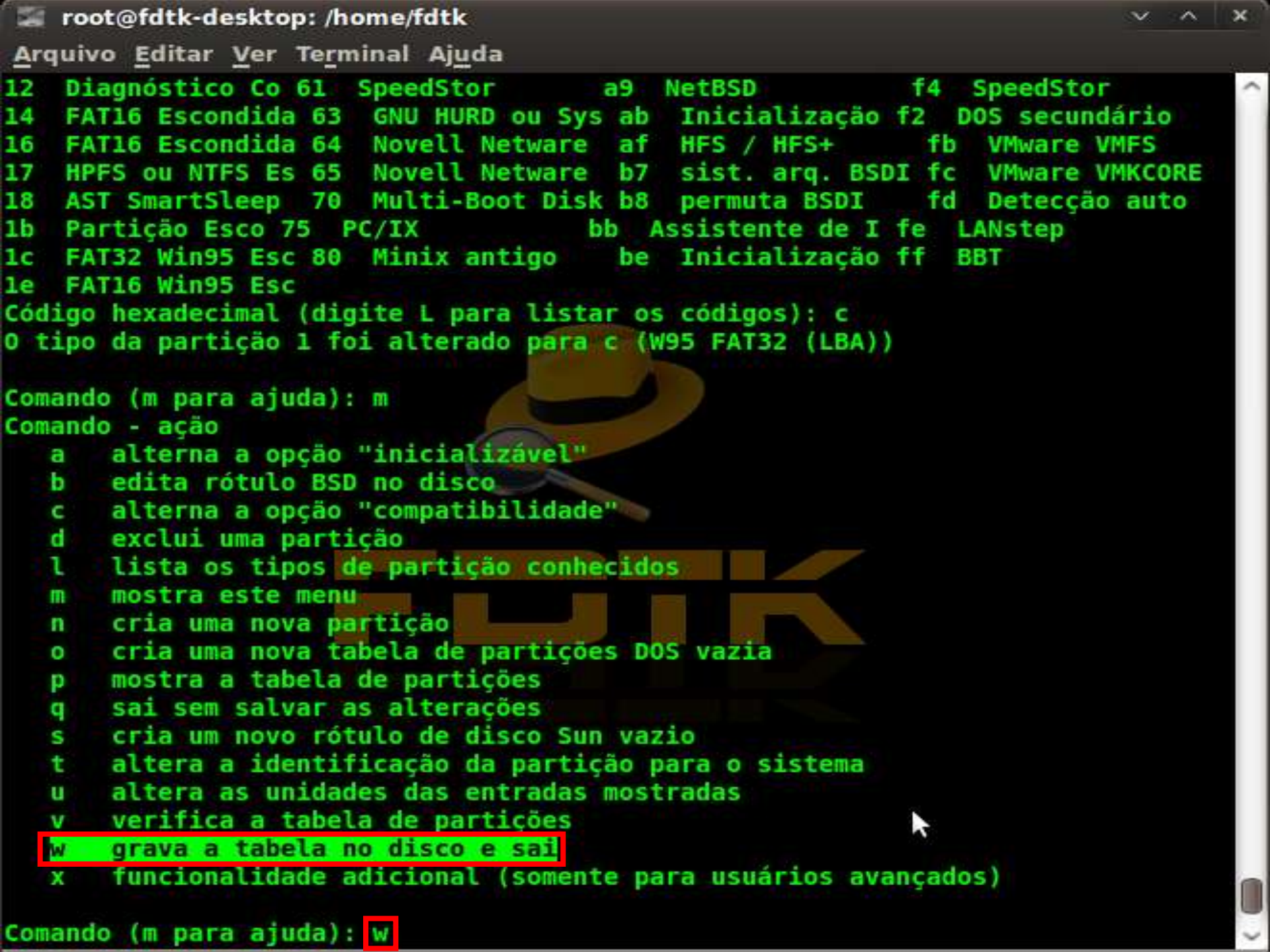
Particionamento da Mídia

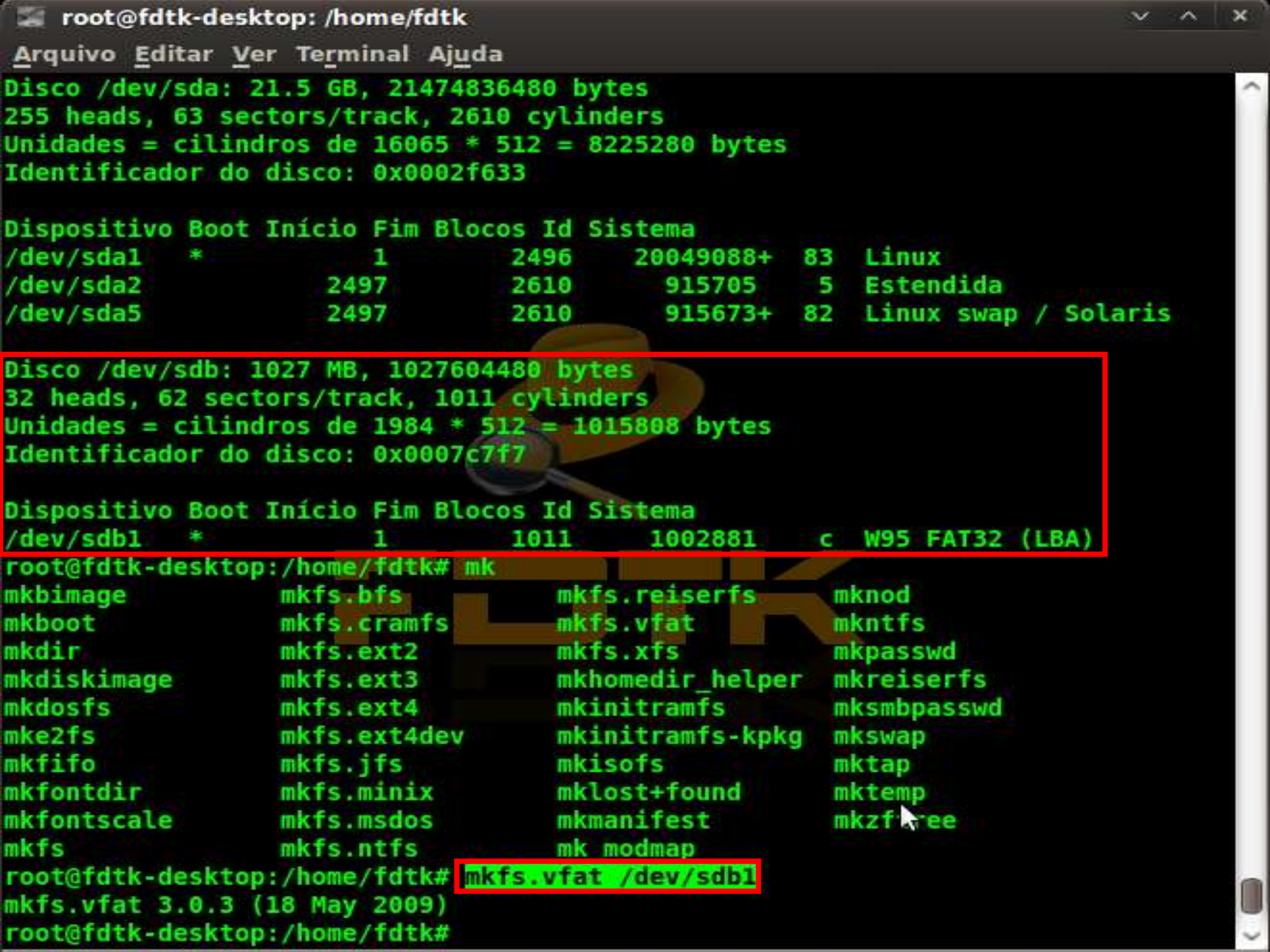
- ✓ ***# fdisk /dev/sdb***
  - ➢ **n** = para criar uma nova partição
  - ➢ **p** = para torná-la primaria
  - ➢ **1** = ela será a primeira partição primaria
  - ➢ Aceitar o padrão ou digite **1** para iniciar do primeiro cilindro
  - ➢ Caso queira definir o tamanho da partição (ex. +20000M=20Gb) ou aceite usar todo o espaço
  - ➢ **a** = ativará a partição para boot
  - ➢ **1** = para escolher a partição 1
  - ➢ **t** = para alterar o tipo de partição
  - ➢ **L**= listar tipos ou **83 = Linux**, **c = W95 FAT32 (LBA)**
  - ➢ **W** = grava a tabela no disco e sai
- ✓ **# mkfs.ext3 /dev/sdb1 -- # mkfs.vfat /dev/sdb1**
- ✓ **Ok!** A mídia está pronta para ser utilizada em qualquer coleta de dados.


root@fdtk-desktop: /home/fdtk
Arquivo Editar Ver Terminal Ajuda
root@fdtk-desktop:/home/fdtk# fdisk /dev/sdb
O dispositivo não contém nem uma tabela de partições DOS válida nem um rótulo de
disco Sun, OSF ou SGI
Building a new DOS disklabel with disk identifier 0xc92b7d87.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.
Aviso: a opção inválida 0x0000 da tabela de partições 4 será corrigida por grava
ção (w)
Comando (m para ajuda):
FDTK


root@fdtk-desktop: /home/fdtk
Arquivo Editar Ver Terminal Ajuda
root@fdtk-desktop:/home/fdtk# fdisk /dev/sdb
O dispositivo não contém nem uma tabela de partições DOS válida nem um rótulo de
disco Sun, OSF ou SGI
Building a new DOS disklabel with disk identifier 0xc92b7d87.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.
Aviso: a opção inválida 0x0000 da tabela de partições 4 será corrigida por grava
ção (w)
Comando (m para ajuda): n
Comando - ação
e estendida
p partição primária (1-4)
p
Numero da partição (1-4): 1
Primeiro cilindro (1-1011, padrão 1): 1
Last cilindro, +cilindros or +size{K,M,G} (1-1011, padrão 1011): 1011
Comando (m para ajuda): a
Número da partição (1-4): 1
Comando (m para ajuda): t
Partição selecionada 1
Código hexadecimal (digite L para listar os códigos):


root@fdtk-desktop: /home/fdtk
Arquivo Editar Ver Terminal Ajuda
Comando (m para ajuda): t
Partição selecionada 1
Código hexadecimal (digite L para listar os códigos): L
0 Vazia 24 DOS NEC 81 Linux antigo/Mi bf Solaris
1 FAT12 39 Plan 9 82 Linux swap / So c1 DRDOS/sec (FAT1
2 root XENIX 3c Recuperação d 83 Linux c4 DRDOS/sec (FAT1
3 usr XENIX 40 Venix 80286 84 Unidade C: OS/2 c6 DRDOS/sec (FAT1
4 FAT16 < 32 M 41 Boot PReP PPC 85 Estendida Linux c7 Syrinx
5 Estendida 42 SFS 86 Conjunto de vol da Dados Não-FS
6 FAT16 4d QNX4.x 87 Conjunto de vol db CP/M / CTOS / .
7 HPFS ou NTFS 4e QNX4.x 2ª part 88 Linux texto pla de Utilitário Del
8 AIX 4f QNX4.x 3ª part 8e Linux LVM df BootIt
9 AIX inicializá 50 DM OnTrack 93 Amoeba e1 Acesso DOS
a Gerenc. Inicial 51 DM6 OnTrack Aux 94 Amoeba BBT e3 DOS R/O
b W95 FAT32 52 CP/M 9f BSD/OS e4 SpeedStor
c W95 FAT32 (LBA) 53 DM6 OnTrack Aux a0 Hibernação IB eb sist. arq. BeOS
e W95 FAT16 (LBA) 54 DM6 OnTrack a5 FreeBSD ee GPT
f Win95 (LBA) Par 55 EZ-Drive a6 OpenBSD ef EFI (FAT-12/16/
10 OPUS 56 Golden Bow a7 NeXTSTEP f0 Inicialização
11 FAT12 Escondida 5c Edisk Priam a8 Darwin UFS f1 SpeedStor
12 Diagnóstico Co 61 SpeedStor a9 NetBSD f4 SpeedStor
14 FAT16 Escondida 63 GNU HURD ou Sys ab Inicialização f2 DOS secundário
16 FAT16 Escondida 64 Novell Netware af HFS / HFS+ fb VMware VMFS
17 HPFS ou NTFS Es 65 Novell Netware b7 sist. arq. BSDI fc VMware VMKCORE
18 AST SmartSleep 70 Multi-Boot Disk b8 permuta BSDI fd Detecção auto
1b Partição Esco 75 PC/IX bb Assistente de I fe LANstep
1c FAT32 Win95 Esc 80 Minix antigo be Inicialização ff BBT
1e FAT16 Win95 Esc
Código hexadecimal (digite L para listar os códigos): 1c


root@fdtk-desktop: /home/fdtk
Arquivo Editar Ver Terminal Ajuda
12 Diagnóstico Co 61 SpeedStor a9 NetBSD f4 SpeedStor
14 FAT16 Escondida 63 GNU HURD ou Sys ab Inicialização f2 DOS secundário
16 FAT16 Escondida 64 Novell Netware af HFS / HFS+ fb VMware VMFS
17 HPFS ou NTFS Es 65 Novell Netware b7 sist. arq. BSDI fc VMware VMKCORE
18 AST SmartSleep 70 Multi-Boot Disk b8 permuta BSDI fd Detecção auto
1b Partição Esco 75 PC/IX bb Assistente de I fe LANstep
1c FAT32 Win95 Esc 80 Minix antigo be Inicialização ff BBT
1e FAT16 Win95 Esc
Código hexadecimal (digite L para listar os códigos): c
O tipo da partição 1 foi alterado para c (W95 FAT32 (LBA))
Comando (m para ajuda): m
Comando - ação
a alterna a opção "inicializável"
b edita rótulo BSD no disco
c alterna a opção "compatibilidade"
d exclui uma partição
l lista os tipos de partição conhecidos
m mostra este menu
n cria uma nova partição
o cria uma nova tabela de partições DOS vazia
p mostra a tabela de partições
q sai sem salvar as alterações
s cria um novo rótulo de disco Sun vazio
t altera a identificação da partição para o sistema
u altera as unidades das entradas mostradas
v verifica a tabela de partições
w grava a tabela no disco e sai
x funcionalidade adicional (somente para usuários avançados)
Comando (m para ajuda): w


root@fdtk-desktop: /home/fdtk
Arquivo Editar Ver Terminal Ajuda
Disco /dev/sda: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Unidades = cilindros de 16065 * 512 = 8225280 bytes
Identificador do disco: 0x0002f633
Dispositivo Boot Início Fim Blocos Id Sistema
/dev/sda1 * 1 2496 20049088+ 83 Linux
/dev/sda2 2497 2610 915705 5 Estendida
/dev/sda5 2497 2610 915673+ 82 Linux swap / Solaris
Disco /dev/sdb: 1027 MB, 1027604480 bytes
32 heads, 62 sectors/track, 1011 cylinders
Unidades = cilindros de 1984 * 512 = 1015808 bytes
Identificador do disco: 0x0007c7f7
Dispositivo Boot Início Fim Blocos Id Sistema
/dev/sdb1 * 1 1011 1002881 c W95 FAT32 (LBA)
root@fdtk-desktop:/home/fdtk# mk
mkbimage mkfs.bfs mkfs.reiserfs mknod
mkboot mkfs.cramfs mkfs.vfat mkntfs
mkdir mkfs.ext2 mkfs.xfs mkpasswd
mkdiskimage mkfs.ext3 mkhomedir_helper mkreiserfs
mkdosfs mkfs.ext4 mkinitramfs mksmbpasswd
mke2fs mkfs.ext4dev mkinitramfs-kpkg mkswap
mkfifo mkfs.jfs mkisofs mktap
mkfontdir mkfs.minix mklost+found mktemp
mkfontscale mkfs.msdos mkmanifest
mkfs mkfs.ntfs mk_modmap
root@fdtk-desktop:/home/fdtk# mkfs.vfat /dev/sdb1
mkfs.vfat 3.0.3 (18 May 2009)
root@fdtk-desktop:/home/fdtk#