FACULDADE DE TECNOLOGIA DE AMERICANA

Curso de Segurança da Informação

Eduardo Becker Tagliarini

ANÁLISE DE EFICÁCIA DE FERRAMENTAS DE RECUPERAÇÃO DE ARQUIVOS

Americana, SP

2016

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso de Segurança da Informação

Eduardo Becker Tagliarini

ANÁLISE DE PERFORMANCE DE FERRAMENTAS DE RECUPERAÇÃO DE ARQUIVOS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Segurança da Informação, sob orientação da Prof.ª Dr.ª Maria Cristina Aranda.

Área de concentração: Perícia computacional

Americana, SP

2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Tagliarini, Eduardo Becker
T134a Análise de eficácia de ferramentas de recuperação de arquivos./ Eduardo Becker Tagliarini.–Americana: 2016.
40f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Profa. Dr. Maria Cristina Aranda

1. Perícia computacionalI. Aranda, Maria Cristina. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.3

Eduardo Becker Tagliarini

ANÁLISE DE PERFORMANCE DE FERRAMENTAS DE RECUPERAÇÃO DE ARQUIVOS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: perícia computacional

Americana, 20 de junho de 2016.

Banca Examinadora:

Maria Cristina Aranda (Presidente)
Doutora
Fatec - Americana

Wagner Siqueira Cavalcante (Membro)
Mestre
Fatec - Americana

Paula de Fonte Sanches (Membro)
Mestre
Fatec - Americana

AGRADECIMENTOS

A Andressa pela amizade e pelos ótimos momentos que compartilhamos.

A minha filha Juliana sempre presente em minha vida.

As amizades que fiz durante o curso, pessoas estas com quem tive a oportunidade de conviver e em especial ao amigo Neder.

A professora Doutora Maria Cristina Aranda que aceitou me orientar neste trabalho.

A Cristiane, companheira e amiga por ter estado presente minha vida, alegrando-me e participando durante toda a graduação.

DEDICATÓRIA

Aos meus pais, responsáveis pelos ensinamentos e por terem proporcionado condições para toda minha formação.

RESUMO

O presente trabalho teve por escopo analisar a performance de ferramentas de recuperação de arquivos excluídos, que fossem baseadas em *data carving*. O estudo contemplou cinco ferramentas, sendo três de uso em ambientes Linux e de licença GNU, e outras duas de uso em ambiente Microsoft Windows e proprietárias. A metodologia de análise consistiu na criação de uma partição NTFS, a qual foi toda ocupada inicialmente com arquivos de texto puro e de áudio do tipo MP3. Posteriormente fez-se a exclusão parcial e aleatória desses arquivos para permitir a inserção de arquivos de imagens. Todos os arquivos foram então excluídos. Fez-se então a criação do arquivo clone da partição. Esse arquivo foi então submetido a análise com os *softwares* de recuperação de arquivos previamente definidos. Dos *softwares* analisados, três obtiveram eficiência na recuperação dos arquivos de imagem apagados próximos enquanto que outros dois não obtiveram resultado na recuperação das imagens excluídas, quando utilizado o modo automatizado.

Palavras Chave: perícia computacional, recuperação de arquivos, *data carving*

ABSTRACT

This work was scope to analyze the performance of deleted files recovery tools, which were based on data carving. The study included five tools, three use in Linux and GNU, and the other two use in Microsoft Windows and proprietary environment. The analysis methodology involved creating an NTFS partition, which was all occupied initially with plain text files and MP3 audio type. Later it became part and random deletion of these files to allow insertion of image files. All files were then deleted. then, did the creation of the clone file partition. This file was then subjected to analysis with the previously defined file recovery software. The software analyzed three achieved efficiency in the recovery of deleted image files next while the other two did not get a result in the recovery of deleted images when using the automated mode.

Keywords: *computer forensics, file recorving, data carving*

SUMÁRIO

LISTA DE FIGURAS E TABELAS

LISTA DE SIGLAS

CFTT - *Computer Forensic Tool Testing Program*

ECA - Estatuto da Criança e Adolescente

FAT -*File Allocatoin Table*

FTK - *Forensic Tool Kit*

GB - gigabyte

MB - megabyte

NIJ - *National Institute of Justice*

NIST - *National Institute of Standards and Technology*

NTFS - *New Technology File System*

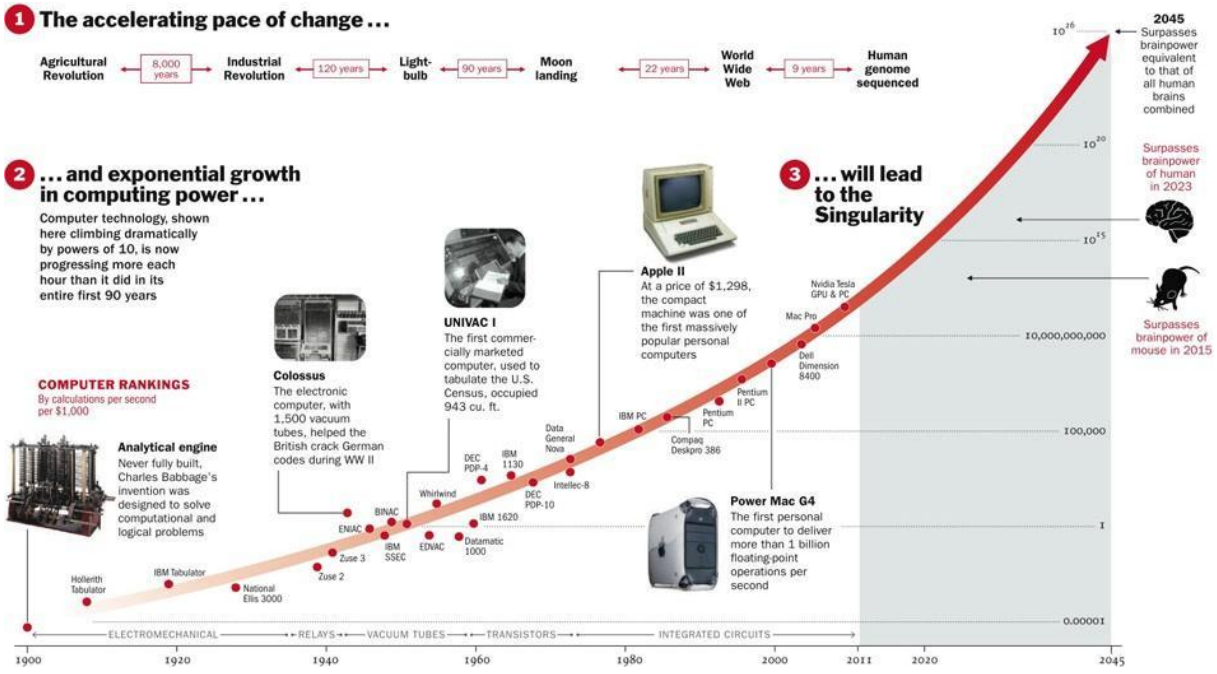
Windows NT - Windows *New Technology*

www - *World Wide Web*

1 INTRODUÇÃO

A evolução do computador desde sua invenção não ocorreu como previsto pelo audacioso Gordon Moore (figura 1), ao propor uma lei na qual afirmava que a velocidade dos computadores dobraria a cada dois anos. Apesar disto não ter ocorrido, tal crescimento se deu mais rápido, pois a velocidade dos processadores dobraria a cada 18 meses e não 24 como previsto por Moore (SÁ, 2016).

Figura 1: evolução do avanço da computação ao longo do tempo. Fonte: http://publicadosbrasil.blogspot.com.br/2015/11/novos-chips-da-intel-nao-conseguem.html (acesso em 30/06/2016).



Essa rápida evolução dos computadores trouxe dois benefícios diretos aos usuários, além do ganho de desempenho, a redução do tamanho dos computadores, bem como a redução de seu custo, fazendo com que tais equipamentos não ficassem mais restritos a grandes corporações, universidades ou instituições públicas, mas sim pudessem estar presentes nas residências das pessoas e até mesmo em suas mãos, como hoje ocorre com os *smartphones*, como demonstra pesquisa realizada pela Nielsen Ibope, na qual indica que mais de 70 milhões de brasileiros utilizam este dispositivo no dia a dia (BRIGATTO, 2016).

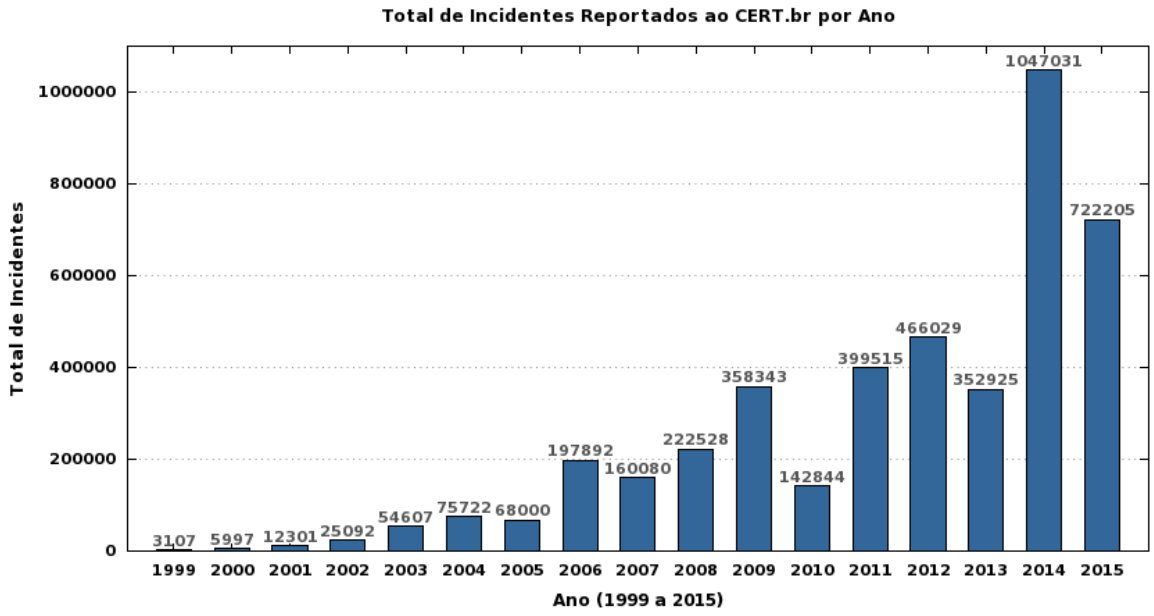
Além da popularização dos sistemas computacionais, outro grande avanço que

ocorreu foi o desenvolvimento da *World Wide Web* (www), que permitiu a comunicação entre os usuários dos diversos computadores localizados ao redor do mundo em poucos milissegundos, algo realmente surpreendente e que viria a modificar em muito o modo como as pessoas se relacionam entre si, e até mesmo a relação de comércio e prestação de serviços (WENDT, 2013).

Diante do uso do computador não mais apenas para fins profissionais e de estudo acadêmico, mas agora para como ferramenta de uso doméstico para diversão, entretenimento, negócios e prestação de serviços, muitas empresas e órgãos públicos passaram a ofertar serviços e produtos na web (WENDT, 2013).

Na contramão dos benefícios proporcionados pelos adventos do microccomputador e da Internet, segundo dados da Cert.BR, entre os anos de 2013 e 2014 houve um crescimento de quase 500% no número de delitos virtuais, passando de 85 mil notificações em 2013 para 450 mil ações delituosas notificadas no ano de 2014. Como demonstrado na figura 2, o número de ocorrências delituosas envolvendo sistemas computacionais aumentou vertiginosamente nos últimos anos, fato este que pode ser atribuído a diversas causas como a inclusão digital, aumento da disponibilidade de diversos serviços na *web*, seja por órgãos públicos ou empresas privadas, ou por instituições bancárias, entre outras.

Figura 2: Fonte Gráfico de incidentes reportados ao Cert.Br entre os anos de 1999 e 2015.
http://www.cert.br/stats/incidentes/ (acesso em 29/05/2016)



Com a massificação do uso dos computadores, bem como da comunicação por meio destes, também houve o crescimento da prática dos chamados delitos cibernéticos (Figura 3, ELEUTÉRIO e MACHADO, 2011). Isto fez com que houvesse a publicação da Lei Federal 12.737 (BRASIL, 2012), de 30 de novembro de 2012, que tipifica as condutas praticadas mediante o uso de sistemas computacionais como crime, uma vez que nosso Código Penal data de 1940.

Figura 3: Comparativo entre os anos de 2006 e 2011 dos crimes virtuais denunciados. Fonte: http://papodehomem.com.br/phishing-engenharia-social-como-escapar-de-golpes-na-internet/ (acesso em 30/06/2016).

Além da edição da Lei federal 12.737 (BRASIL, 2012), foi publicada também a Lei Federal 12.735 de 30 de novembro de 2012 (BRASIL, 2012), na qual se reestruturam os órgãos de polícia judiciária para que passem a conter setores especializados na apuração e combate a ações delituosas envolvendo sistemas computacionais.

A tipificação das condutas delituosas praticadas no mundo virtual pela lei 12.737 (BRASIL, 2012) foi um grande avanço no combate ao crime de pedofilia, pois em conjunto com o artigo 241-A do Estatuto da Criança e Adolescente (BRASIL, 1990), encerram-se todas as possibilidades de condutas que podem ser praticadas para o crime de pedofilia com o uso de sistemas computacionais, conforme observa-se:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
>
> § 1º Nas mesmas penas incorre quem:
>
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
>
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
>
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

As condutas tipificadas nos incisos I e II do parágrafo 1º do artigo 241-A do ECA (BRASIL, 1990) devem ser vistas com cautela pelas empresas que disponibilizam a seus funcionários, para a realização de suas atribuições, sistemas computacionais, acesso à Internet e e-mail, pois casos estes venham a cometer alguma das condutas tipificadas no artigo citado, a empresa poderá ser responsabilizada (SPERAZINI, 2006).

No intento de minimizar a ocorrência de tal situação, a CERT, grupo americano de segurança na Internet, juntamente com o Serviço Secreto dos Estados Unidos e a revista CSO, apresentaram o resultado de pesquisa, na qual foram eleitas as dez melhores maneiras de se prevenir crimes praticados na Internet, conforme expõe-se (SPERAZINI, 2006):

Empregar um funcionário dentro da empresa para monitoramento de conteúdo:

1) Elaborar, por escrito, uma política para práticas inapropriadas;
2) Solicitar aos funcionários que assinem um termo de compromisso às políticas implementadas;
3) Monitorar conexões com a Internet;
4) Elaboração periódica de relatórios sobre uso inapropriado e abuso dos meios eletrônicos da empresa;
6) Criar programas para educação e conscientização de funcionários quanto ao crime eletrônico;
7) Desenvolver uma política de segurança corporativa;
8) Criar programas para educação de novos funcionários;
9) Promover avaliações de risco periódicas; e
10) Conduzir auditorias de segurança periódicas dentro da empresa.

O interessante é que ao se implementar a última ação citada, realizar periodicamente auditorias de segurança dentro da empresa, o responsável por tal tarefa pode adotar como um dos procedimentos realizados a recuperação de arquivos apagados, utilizando para isso métodos empregados nos procedimentos de computação forense.

Dentre os procedimentos a serem adotados conforme SPERAZINI (2006):

i. correta identificação dos equipamentos;
ii. preservação da prova;
iii. extração, recuperação e indexação dos dados existente e apagados;
iv. análise dos dados extraídos;
v. elaboração de relatório com os resultados.

Como o resultado dos trabalhos realizados durante um exame pericial se destinam à Justiça, o *National Institute of Justice* (NIJ), por meio do *National Institute of Standards and Technology* (NIST), realizou um estudo em diferentes programas de recuperação de dados, denominado de *Computer Forensic Tool Testing Program* (CFTT), visando assim validar o uso de ferramentas nas Cortes americanas (FISHER, 2001).

1.1 FERRAMENTAS DE RECUPERAÇÃO DE ARQUIVOS

Atualmente existem diversos programas destinados a recuperação de arquivos apagados, alguns até mesmo nativos dos sistemas operacionais Microsoft Windows e Linux. Entretanto, nem todos possuem as características necessárias para a realização de uma perícia computacional e tampouco foram aprovados pelo projeto de validação CFTT (UNITED STATE OF AMERICA[1], 2014) realizado pelo NIST.

Dentre os programas que foram aprovados e validados no projeto CFTT pode-se citar o Autopsy/Sleuth kit, Encase, Foremost, Forensic Toolkit (FTK) e o Photorec (UNITED STATE OF AMERICA, 2014).

Para auxiliar na escolha de qual programa utilizar na recuperação de arquivos apagados, pretende-se avaliar a eficiência dos programas acima citados na de recuperação de dados, no que tange a recuperação de arquivos de imagem do tipo JPG que tenham sido excluídos de mídia de armazenamento de dados, que utilizavam sistema de arquivo do tipo NTFS (*New Technology File System*).

1.1.1 AUTOPSY/SLEUTH KIT

O Autopsy e o Sleuth kit são programas *open source* gratuitos, de alta eficiência de análise de mídias de armazenamento de dados, smartphones e imagens de discos de dados, bem como na recuperação destes quando apagados (http://www.sleuthkit.org/autopsy/).

O Autopsy é uma plataforma dedicada a realização de perícia computacional, baseada numa interface gráfica para o conjunto de aplicativos integrantes do Sleuth kit (figuras 4 e 5). Tal plataforma pode ser utilizada em ambiente Linux, OS X e Microsoft Windows (http://www.sleuthkit.org/autopsy/).

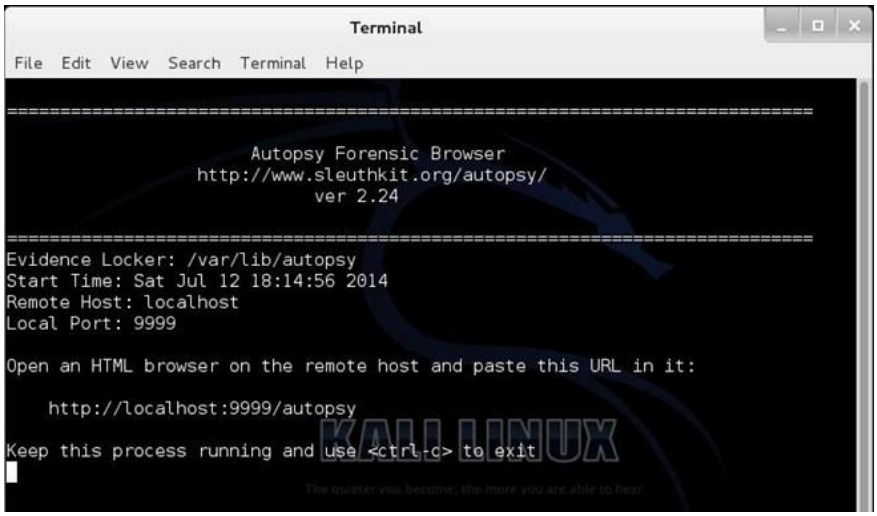
Autopsy foi projetado para ser uma plataforma *end-to-end* com módulos que vêm com ele fora do pacote e outros que estão disponíveis a partir de terceiros. Alguns dos módulos oferecem:

Figura 4: vista da tela inicial na interface gráfica do Autopsy.

- Análise Timeline - visualização em interface gráfica ;
- Hash Filtragem – permite identificar ou ignorar arquivos identificados por hash
- Pesqusia por palavra-chave - permite pesquisa por palavra-chave presente nos arquivos;
- Artefatos web – extrai o histórico, favoritos e cookies dos navagadores Firefox, Chrome e IE.
- Data Carving - Recupere arquivos apagados de espaço não alocado usando PhotoRec;
- Multimédia – Extraí informação EXIF contidas nas fotos e permite assistir vídeos.

Podem ser utilizados na recuperação de dados de mídias de armazenamento que utilizam sistema de arquivos do tipo FAT, ExFat, NTFS, ext2, ext3 e ext4.

Figura 5: vista de tela no terminal do Linux indicando o funcionamento Autopsy/Sleuth kit.



1.1.2 ENCASE

Este aplicativo é proprietário, de plataforma gráfica (figura 6) para ser utilizada com computadores com sistema operacional Microsoft Windows, produzido pela Guidance, possuindo diversos recursos a serem empregados na execução de mídias de armazenamento de dados (ELEUTÉRIO E MACHADO, 2011). Possui uma *suite* para recuperação de arquivos apagados.

Pode ser utilizado na recuperação de dados de mídias de armazenamento que utilizam sistema de arquivos do tipo FAT, ExFat, NTFS e ext2.

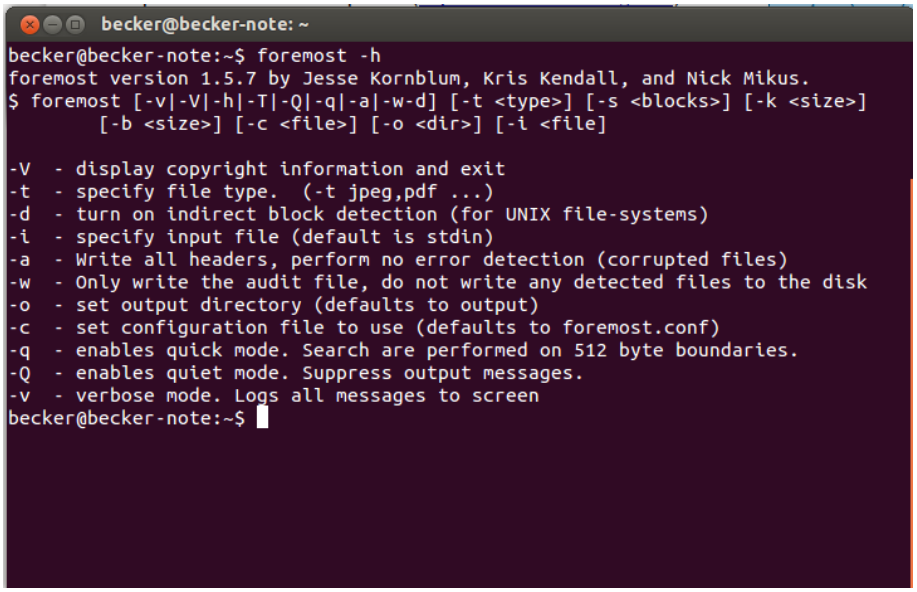
Figura 6: Encarte do aplicativo Encase Forensic versão 6.

1.1.3 FOREMOST

É um programa *open source* para recuperar arquivos apagados (figura 7), que se baseia na busca de informações de metadados presentes nos cabeçalhos e rodapés dos arquivos, processo este denominado de *data carving*. Pode ser utilizado diretamente em mídias de armazenamento de dados ou ainda com a imagem de tais mídias. Originalmente foi desenvolvido pela Força Aérea Americana, sendo posteriormente disponibilizado ao público em geral(http://foremost.sourceforge.net/).

Pode ser utilizado na recuperação de dados de mídias de armazenamento que utilizam sistema de arquivos do tipo FAT, NTFS, ext2, ext3 e ext4.

Figura 7: vista do terminal exibindo auxílio de uso do Foremost.

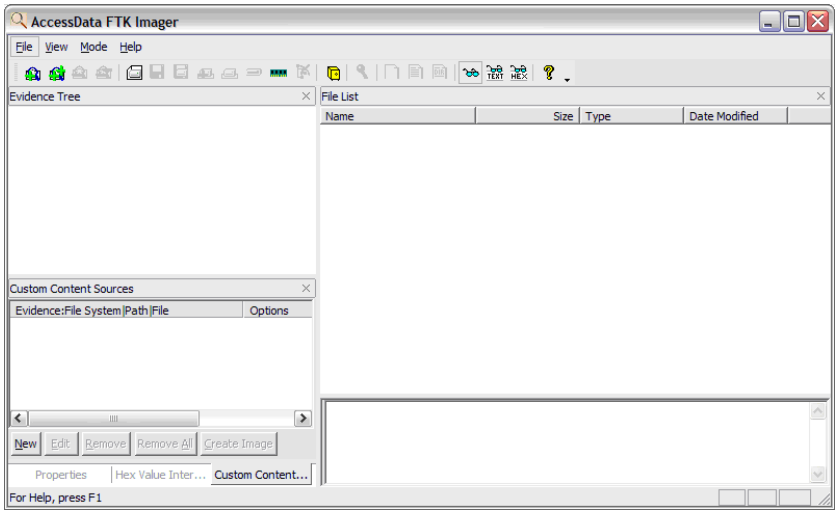


1.1.4 FTK IMAGER

O FTK Imager é um *software* proprietário desenvolvido pela AccessData (figura 8) que tem por principal funcionalidade realizar a criação de arquivos clones de unidade de armazenamento de dados que serão examinadas (MADEIRA, 2012).

Apesar da principal funcionalidade do FTK Imager ser o de gerar arquivos clones, ele também possui funcionalidade para exportar e visualizar arquivos da unidade de interesse (Madeira, 2012).

Figura 8: tela inicial do aplicativo FTK Imager.



Pode ser utilizado na recuperação de dados de mídias de armazenamento que utilizam sistema de arquivos do tipo FAT, ExFat (recuperação parcial), NTFS e ext2.

1.1.5 PHOTOREC

É um programa de recuperação de arquivos apagados (figura 9) a partir de mídias de armazenamento do dados do tipo disco rígido, memória *flash*, CD-ROM. É aplicação de distribuição livre, *open source* multiplataforma, podendo ser utilizado em computadores com sistema operacional Microsof Window, Linux, Mac OS X, Sun Solaris, FreeBSD e DOS.

Pode ser utilizado na recuperação de dados de mídias de armazenamento que utilizam sistema de arquivos do tipo FAT, ExFat, NTFS, ext2, ext3, ext4 e HFS+ (http://www.cgsecurity.org/wiki/PhotoRec).

Figura 9: imagem ilustrativa do Photorec. Fonte: www.cgsecurity.org (acesso em 29/05/2016).

2 METODOLOGIA

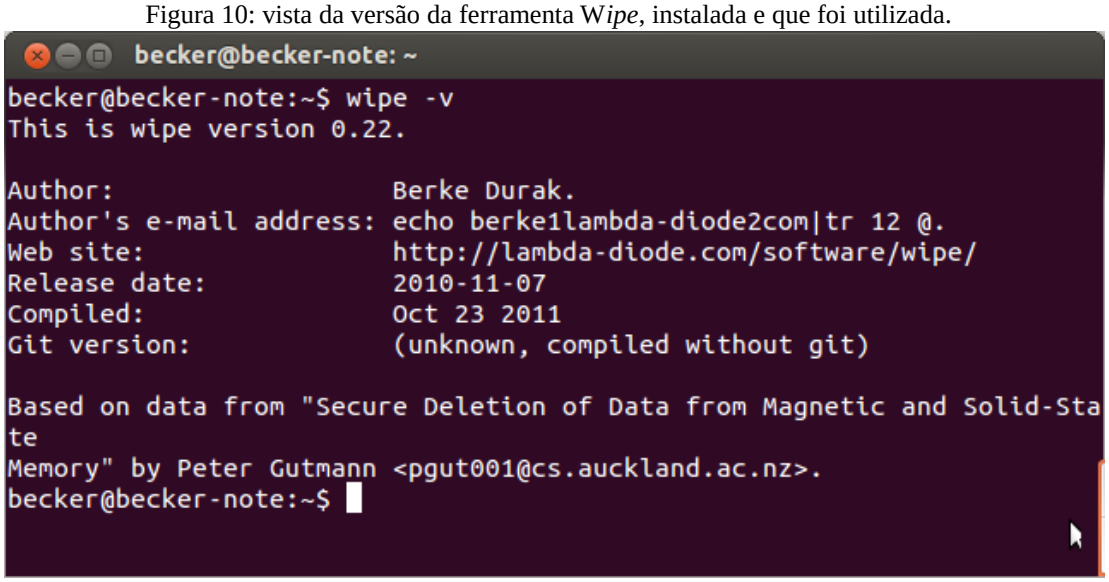
A metodologia de análise para comparar o desempenho dos *softwares* a serem testados, consistiu na criação de uma partição de 200 MB (megabytes) em um dispositivo móvel de armazenamento de dados de 2.0 GB (gigabytes) de capacidade nominal de armazenamento, que será posteriormente submetido a análise pelos programas selecionados para este ensaio, que deverão recuperar os arquivos de imagem que serão inseridos na memória e posteriormente excluídos.

Para a realização do presente trabalho, serão necessárias duas estações de trabalho, uma dotada com distro do sistema Linux e outra dotada com o sistema operacional Microsoft Windows 7. Todas as etapas envolvidas na criação da partição que será examinada serão realizadas na estação de trabalho com sistema operacional Linux, inclusive as análises com os programas Autopsy/Sleuth kit, Foremost e Photorec, enquanto que a estação de trabalho com sistema Microsoft Windows, será utilizada para as análises empregando os programas Encase e FTK Imager.

2.1 TÉCNICA DE *WIPE*

Antes de se criar a partição o dispositivo de memória, foi submetida a técnica de *wipe*, que consiste na sobrescrita de todos os setores pelo caractere “0” (zero). Para realizar tal procedimento utilizou-se a ferramenta W*ipe* (figura 10).

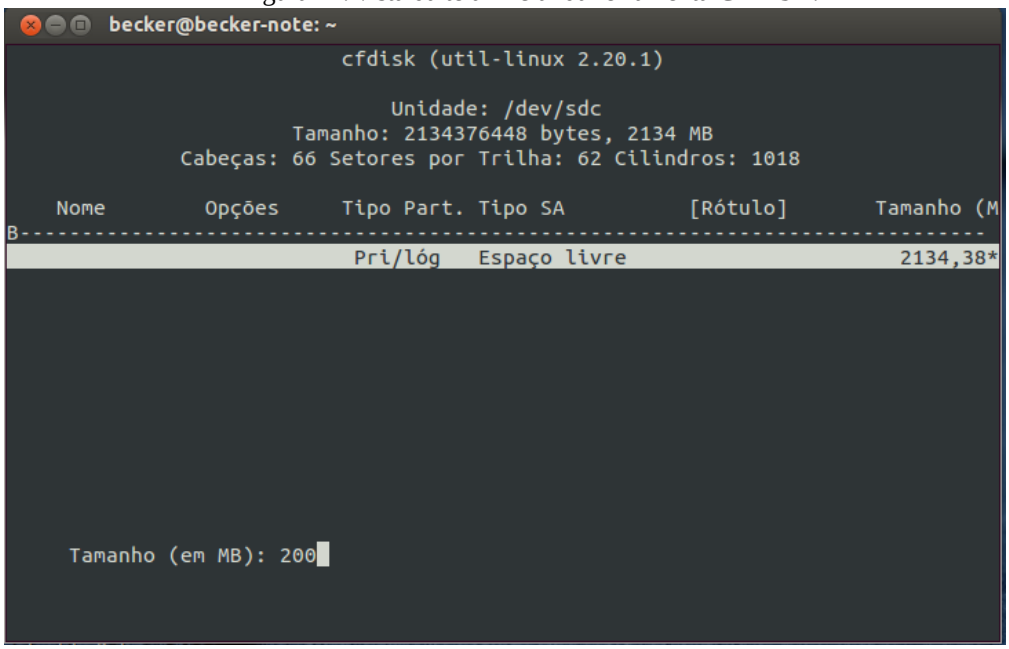
Figura 10: vista da versão da ferramenta W*ipe*, instalada e que foi utilizada.



2.2 CRIANDO A PARTIÇÃO

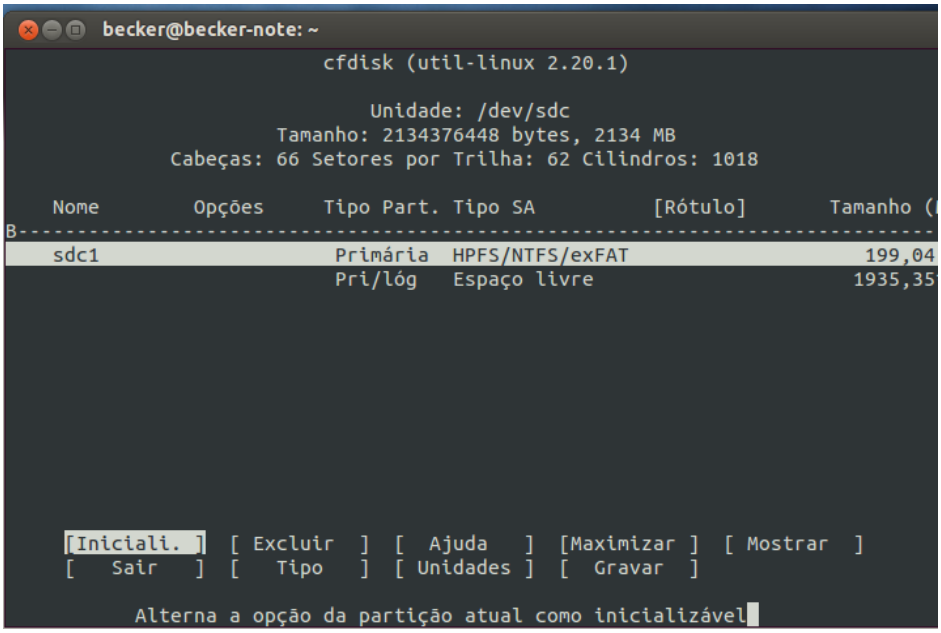
Na sequência foi feita a criação de uma partição de 200 MB utilizando para isso a ferramenta CFDISK, nativa dos sistemas operacionais Linux (figura 11).

Figura 11: vista da tela inicial da ferramenta CFDISK.



O sistema de arquivos escolhida foi o NTFS (figura 12), por ser o padrão utilizado nas plataformas do sistema operacional Microsoft Windows, a partir do Windows NT, e por ser esse o sistema operacional mais utilizado no mundo (DAQUINO, 2015).

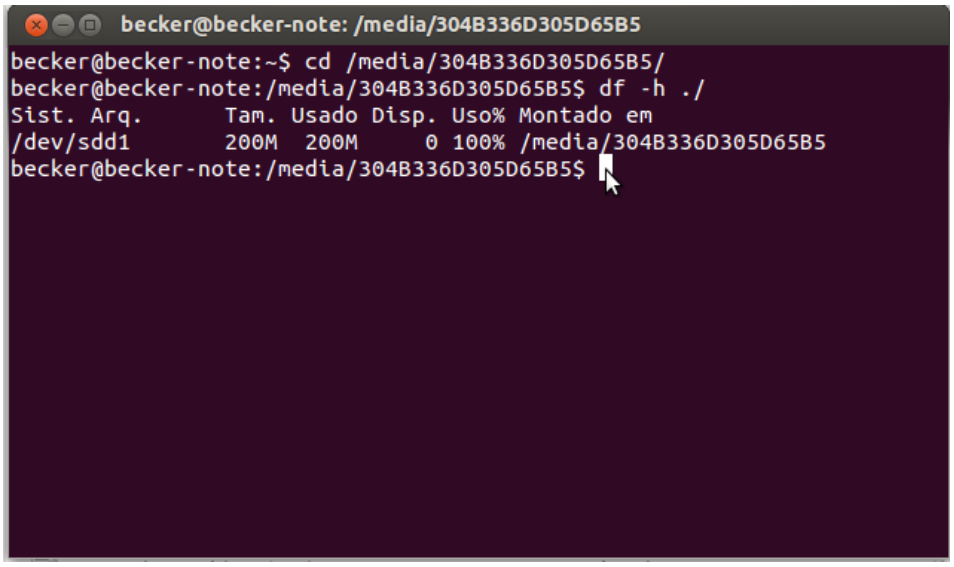
Figura 12: vista da tela da ferramenta CFDISK antes de finalizar a gravação da formatação da partição criada.



2.3 DOS ARQUIVOS INSERIDOS E EXCLUÍDOS

Antes dos arquivos de imagem serem copiados para a partição, esta foi totalmente preenchida (figura 13) com 8275 arquivos, sendo 51 de áudio do tipo MP3 e os outros 8224 de texto puro (.txt), como demonstrado abaixo pela execução do comando *df*, e o *ls* combinado com o *wc*.

Figura 13: informação de que a partição criada estava totalmente ocupada.



$ ls | wc -l //o uso combinado dos comando ls e wc -l informa a quantidade de arquivos existentes no diretório
8275

$ ls *.txt | wc -l //o uso combinado dos comando ls e wc com os parâmetro utilizados indica o total de arquivos de texto existentes no diretório
8224

$ ls *.mp3| wc -l //o uso combinado dos comando ls e wc com os parâmetro utilizados indica o total de arquivos de áudio existentes no diretório
51

Posteriormente, parte desses arquivos foram excluídos de modo aleatório, para que quando da inserção dos um mil e trezentos arquivos de imagem, estes apresentassem fragmentação. Após a inserção dos arquivos de imagem, fez-se a exclusão de todos os arquivos armazenados.

$ ls /media/304B336D305D65B5/*.jpg | wc -l //o uso combinado dos comando ls e wc com os parâmetro utilizados indica o total de arquivos de imagem existentes no diretório
1300

Cumpridas essas etapas de inclusão e exclusão dos arquivos, foi gerada uma imagem clone da unidade de armazenamento, da qual a partição fazia parte. A imagem clone foi denominada de “tcc.dd”, utilizando-se para isso o programa dd, como demonstrado a seguir.

$ sudo dd if=/dev/sdd of=/home/.../tcc.dd //comando para criar arquivo dd da memória
4168704+0 registros de entrada
4168704+0 registros de saída
2134376448 bytes (2,1 GB) copiados, 161,199 s, 13,2 MB/s

Os *softwares* de recuperação de arquivos e as respectivas versões que foram utilizadas são:

- Autopsy/Sleuth kit v2.24
- Foremost v1.5.7
- Photorec v6.11.3
- FTK Imager v3.2
- Encase v6.19

Sendo as quatro primeiras de licença GNU e gratuitas e a última devidamente licenciada.

2.4 UTILIZANDO O AUTOPSY/SLEUTH KIT

Os programas Autopsy/Sleuth kit é uma combinação de aplicação da interface gráfica do Autopsy que permite utilizar de modo amigável as ferramentas que fazem parte da *suite* de aplicativos do Sleuth Kit, que utiliza linhas de comando para executar suas funcionalidades.

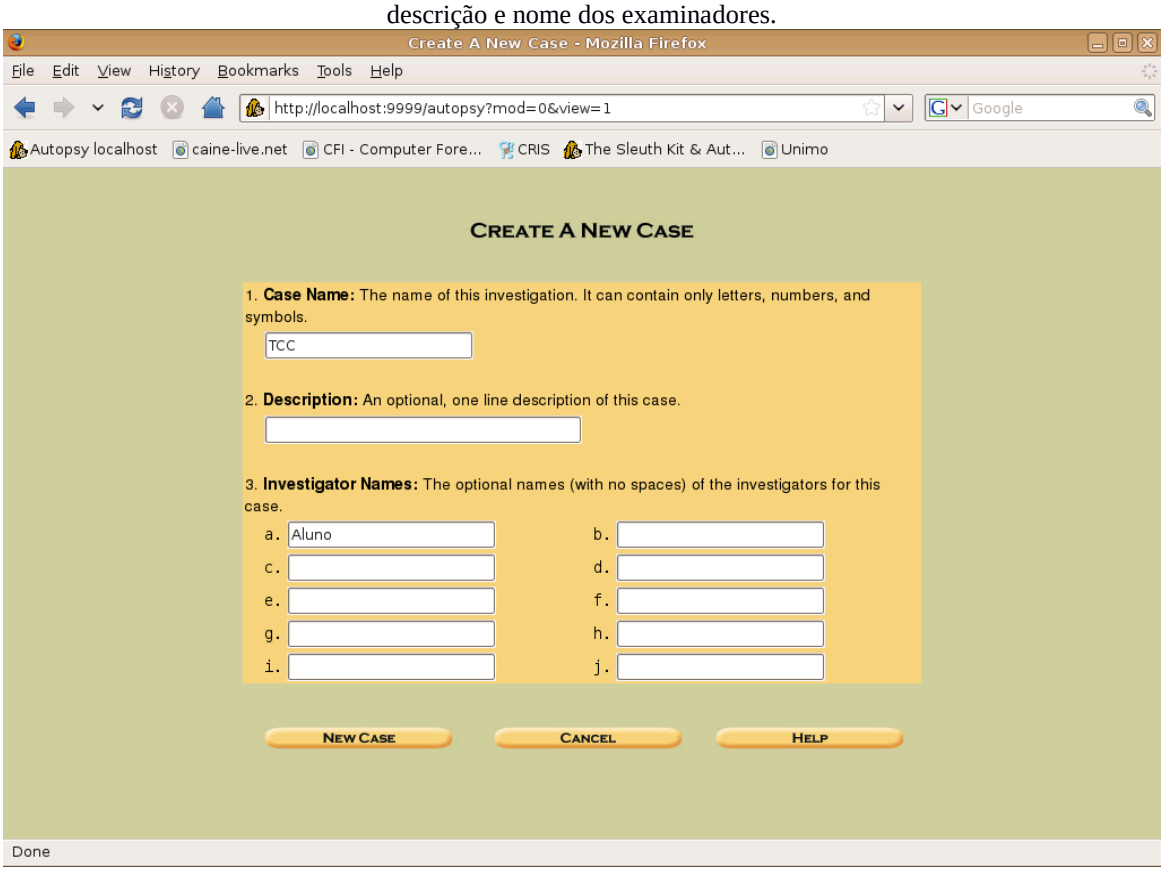
Isso já se observa ao iniciar o programa, sendo necessário para isso abrir o terminal para digitar a linha de comando de chamada do Autopsy/Sleuth kit. Estando o programa instalado é exibido no terminal de que o programa está ativo.

Com o programa já ativo, deve-se abrir um navegador e inserir o caminho indicado no terminal para que se possa então acessar a tela inicial do Autopsy (figura 4). Deve-se então clicar no ícone *New Case* para se iniciar a criação de um novo caso e assim utilizar o programa.

Após clicar em *New Case* é exibida uma sequência de janelas, com campos a serem preenchidos com informações relacionadas ao caso examinado, como número do caso, nome do examinador, fuso horário, caminho onde está armazenado a imagem a ser examinada dentre outras informações.

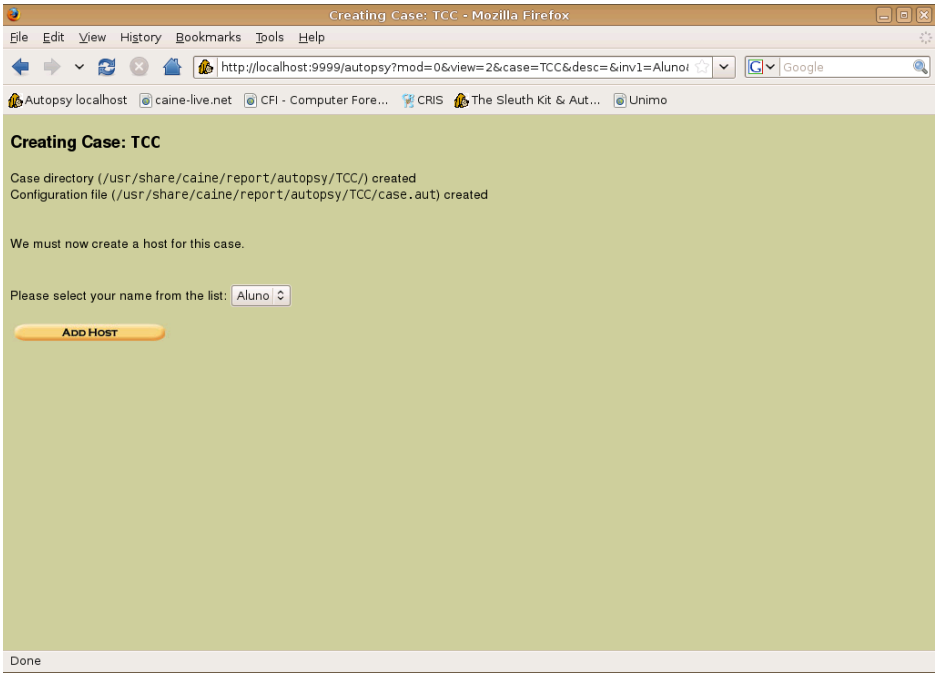
A figura 14 ilustra a tela de inserção de dados quando da criação do novo caso, tais como número do caso, nome dos investigadores e descrição do caso. Ao final da inserção dos dados, deve-se clicar em *New Case* para finalizar o processo de criação do caso.

Figura 14: tela inserção dos dados primários do caso criado no programa Autopsy, como número do caso, descrição e nome dos examinadores.



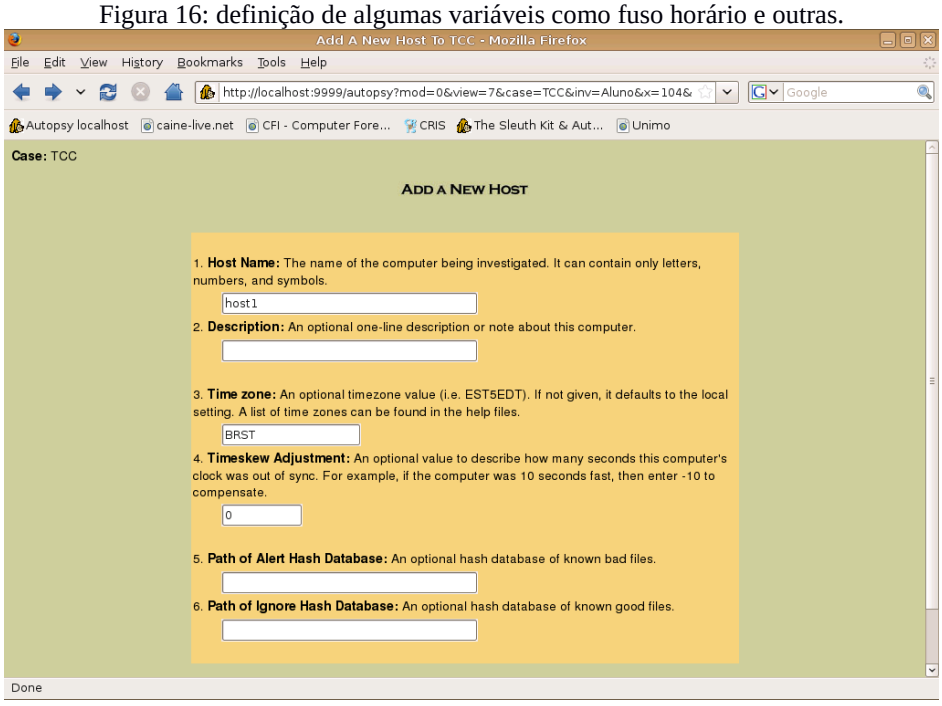
A figura 15 ilustra a tela seguinte, na qual são informados os dados do caso. Para seguir deve-se clicar em *Add Host*.

Figura 15: tela sequencial a da figura anterior, na qual é informado que o caso foi criado. E o caminho do diretório onde os dados serão armazenados.



A figura 16 ilustra a tela seguinte, na qual são solicitados alguns dados, tais como nome do *host*, descrição do computador, fuso horário e informação de banco de dados de número hash de arquivos para serem buscados ou ignorados durante o processo de análise.

Figura 16: definição de algumas variáveis como fuso horário e outras.

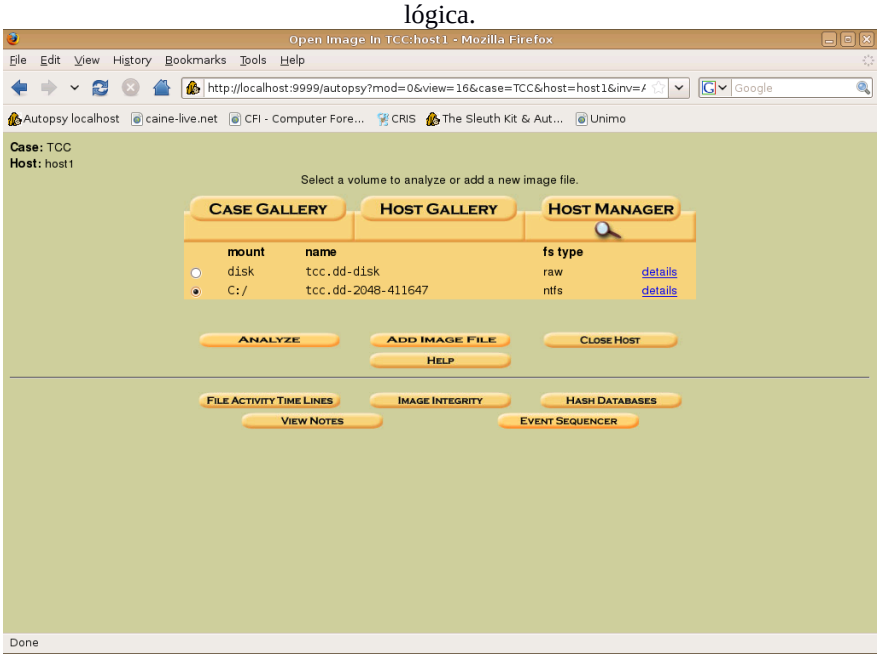


A figura 17 indica o caminho do arquivo que será examinado, solicita definição e se será realizado o cálculo da função *hash* MD5 para o arquivo analisado e informa detalhes sobre o sistema de arquivo.

Figura 17: exibição de informações sobre o arquivo de imagem a ser examinados.

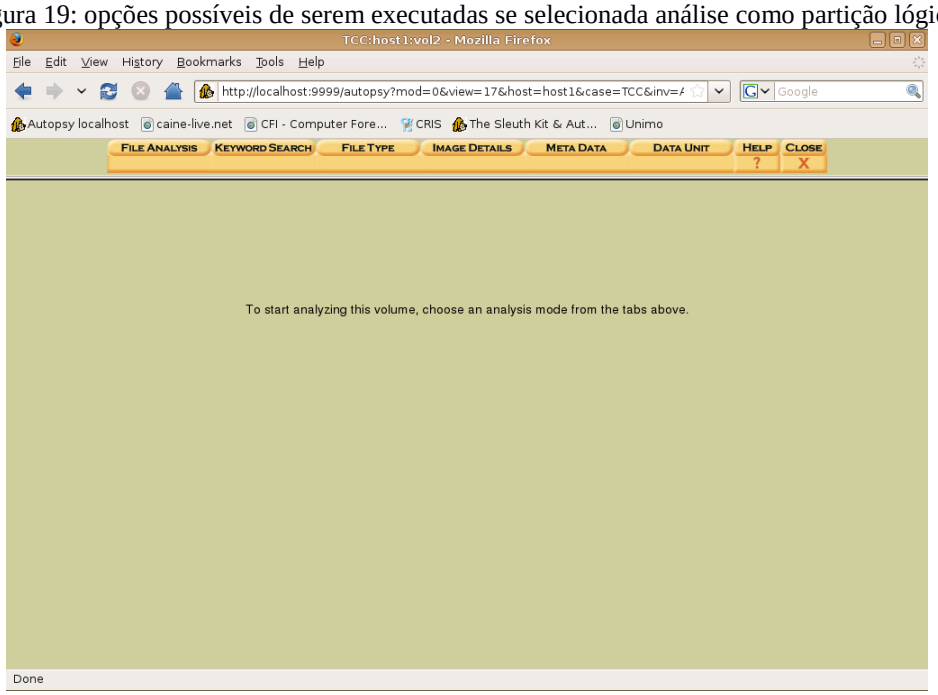
A figura 18 ilustra a tela seguinte, na qual são exibidos as possibilidades de análise do caso, seja como uma unidade física ou como uma unidade lógica. A opção selecionada para este estudo foi a segunda.

Figura 18: tela de opção de análises que podem ser realizadas, seja como um arquivo *raw* ou como partição lógica.



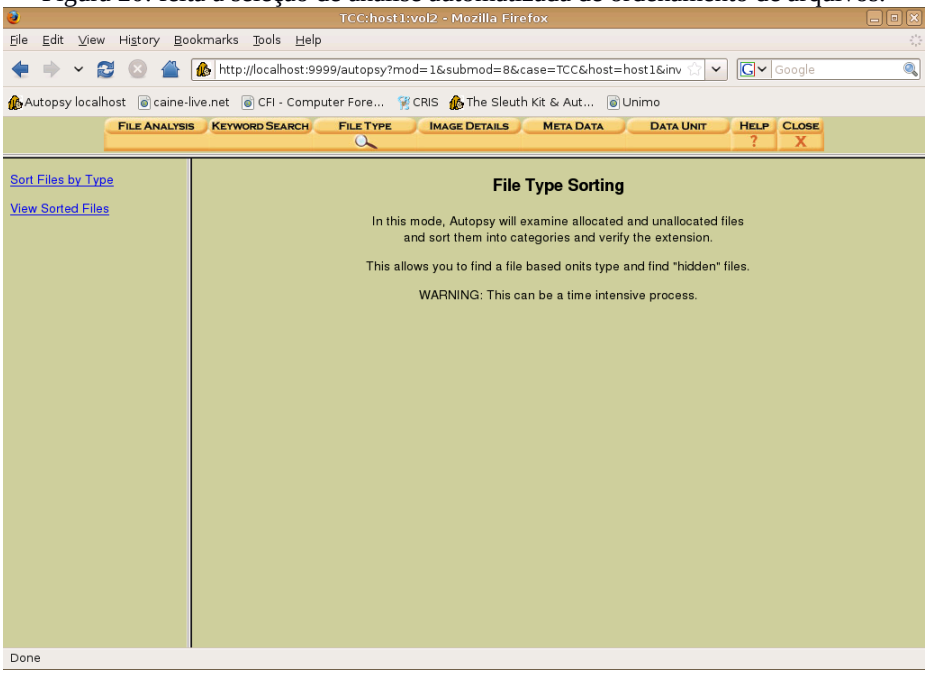
Após feita a seleção, é exibida uma tela na qual são disponibilizados os tipos de análises ofertados pela ferramenta (figura 19). Neste estudo foi selecionada opção de análise por tipo de arquivo (*File Type*).

Figura 19: opções possíveis de serem executadas se selecionada análise como partição lógica.



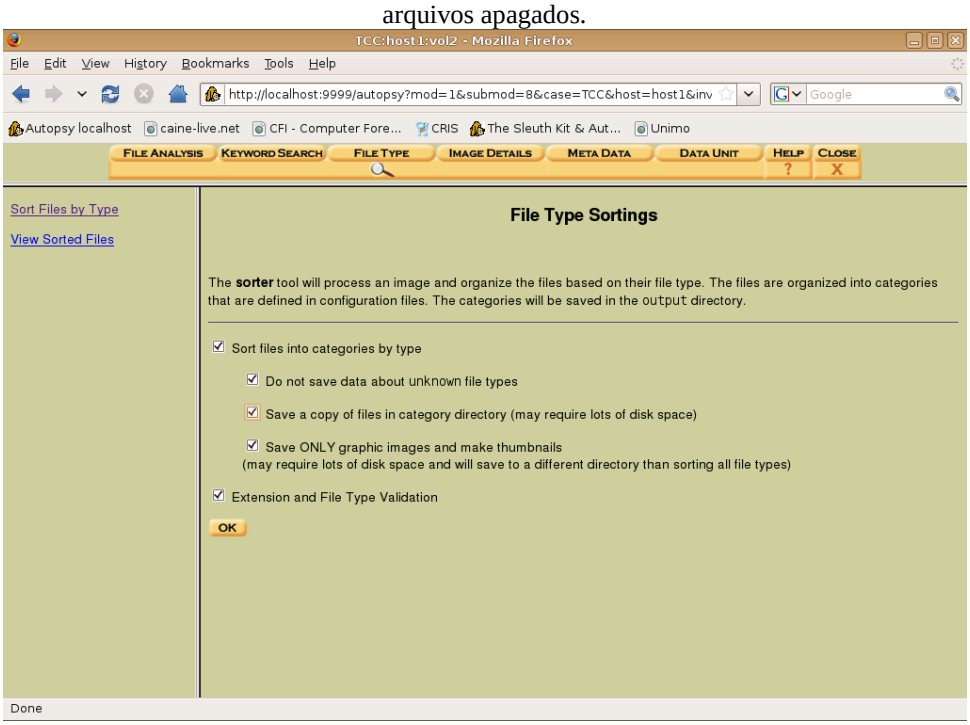
A figura 20 ilustra a tela seguinte na qual é informada que o programa examinara a área alocada e não alocada na busca por arquivos, os quais serão ordenados pela extensão.

Figura 20: feita a seleção de análise automatizada de ordenamento de arquivos.



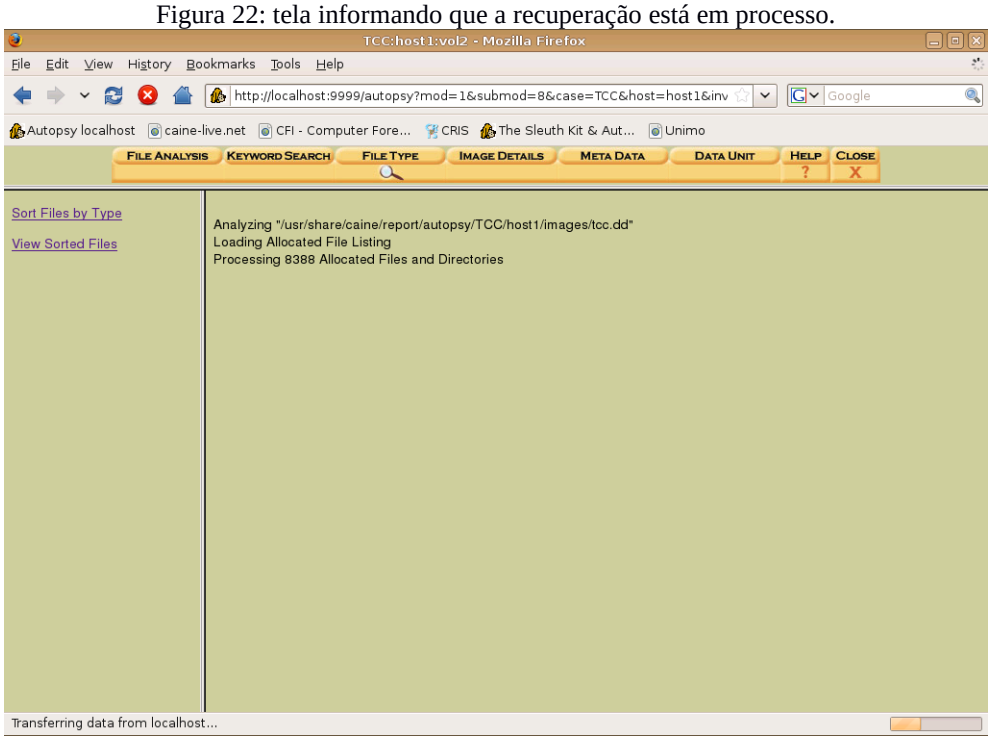
A figura 21 exibe a tela seguinte, no qual é solicitada a definição de parâmetros antes do início da recuperação automatizada dos arquivos excluídos.

Figura 21: exibição de opções de configuração a serem definidas antes da recuperação automatizada dos arquivos apagados.



Após a definição dos parâmetros, deve-se clicar em OK para que o processo seja iniciado. A figura 22 exibe a tela com informações de que o processo foi iniciado.

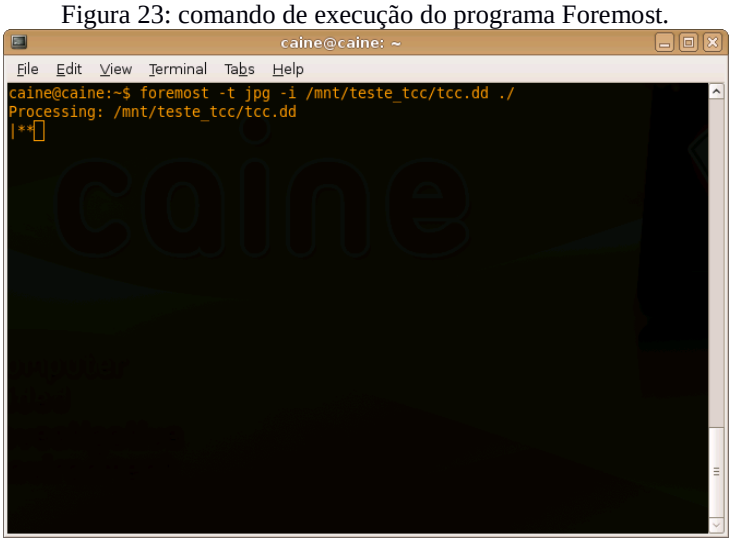
Figura 22: tela informando que a recuperação está em processo.



2.5 UTILIZANDO O FOREMOST

O programa Foremost não possui interface gráfica, sendo toda sua execução feita mediante linha de comando, A figura 23 ilustra a linha de comando para execução do programa, sendo necessário para isso informar a extensão do tipo de arquivo que se deseja recuperar, o caminho da unidade ou arquivo clone onde será feita a recuperação e o diretório onde as arquivos recuperados serão salvos.

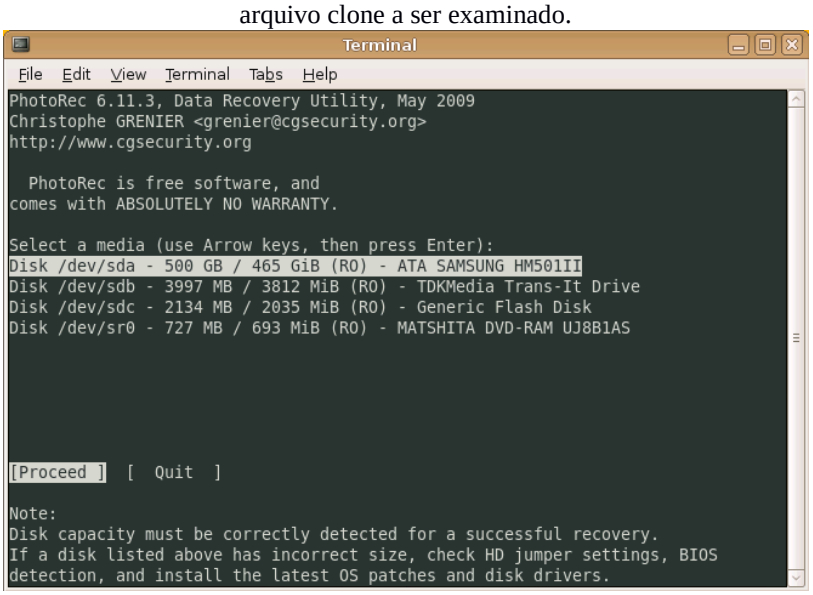
Figura 23: comando de execução do programa Foremost.



2.6 UTILIZANDO O PHOTOREC

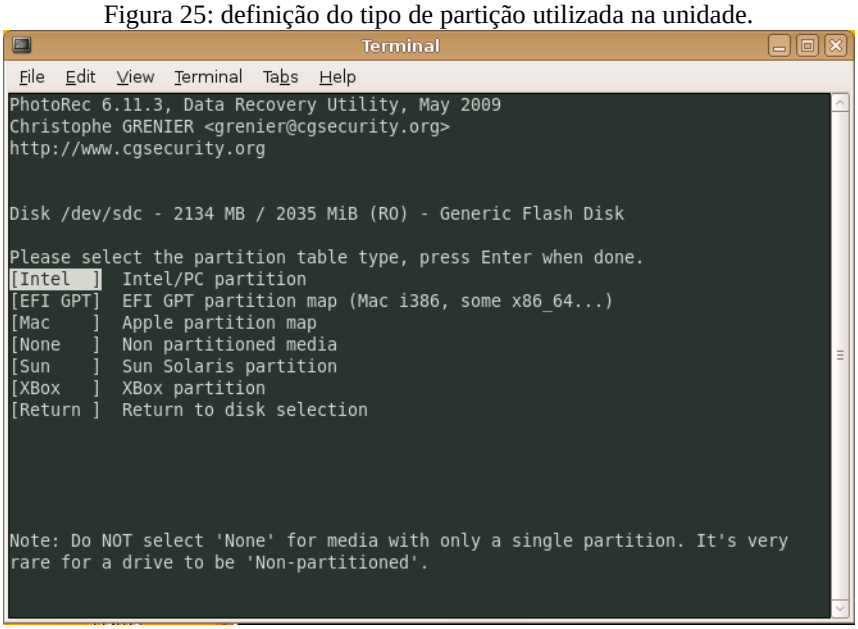
Assim como o Foremost o Photorec também é um programa que não possui interface gráfica, sendo toda sua execução feita via linha de comando no terminal do Linux (figuras de 24 à 26).

Figura 24: tela inicial do programa Photorec, solicitando definição de qual unidade de armazenamento está o arquivo clone a ser examinado.



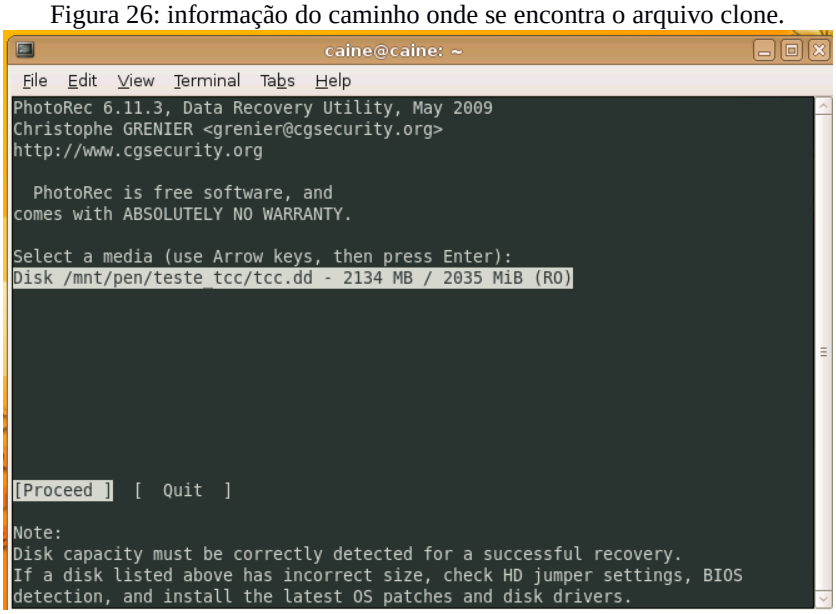
Após a definição da unidade física que será analisada, é solicitada a definição do sistema de arquivos da partição examinada (figura 25).

Figura 25: definição do tipo de partição utilizada na unidade.



Posteriormente, é solicitado a informação do caminho onde se encontra o arquivo clone que será objeto do exame (figura 26).

Figura 26: informação do caminho onde se encontra o arquivo clone.



3.7 UTILIZANDO O ENCASE

O programa Encase oferece uma plataforma gráfica amigável e de fácil interação para o examinador.

Assim como os demais programas também possui etapa de criação do caso, informação do caminho da unidade que será examinada e onde o resultado da análise será armazenado (figuras de 27 à 29).

Figura 27: tela inicial quando da execução do programa Encase.

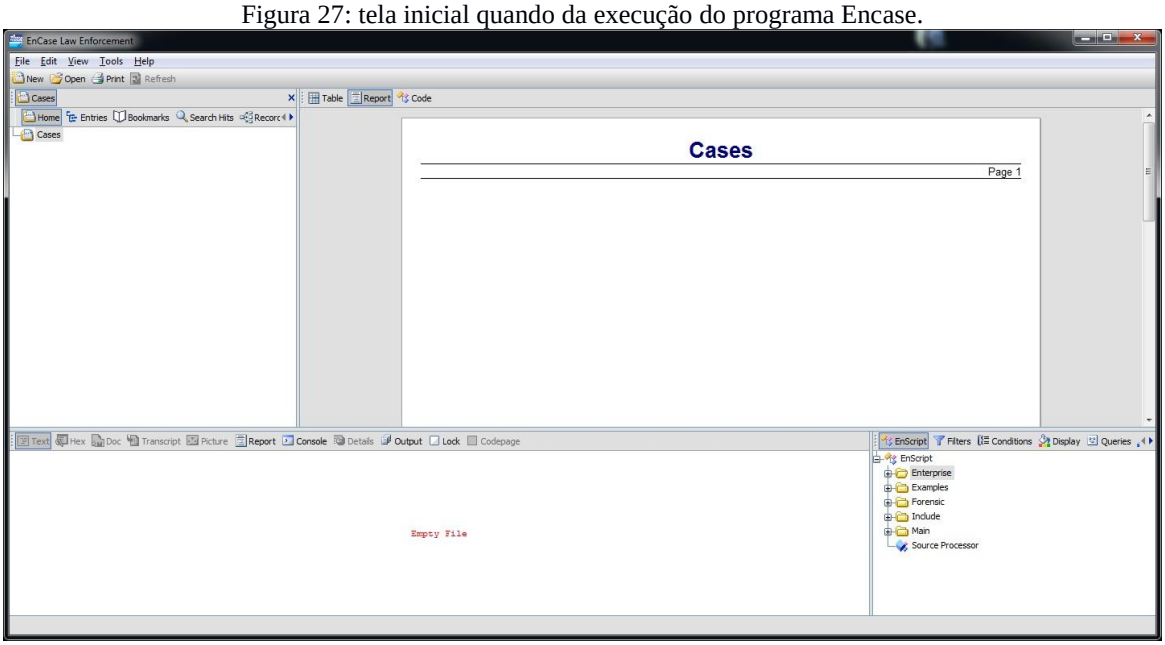


Figura 28: inserção do caminho onde o arquivo clone a ser examinado se localiza.

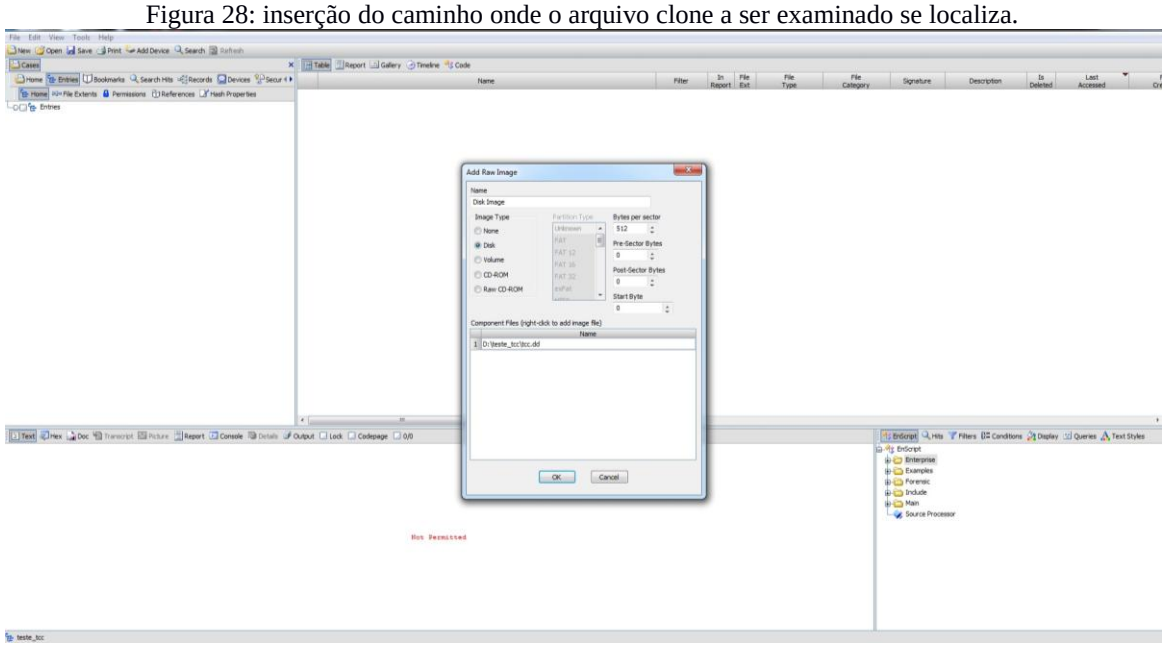
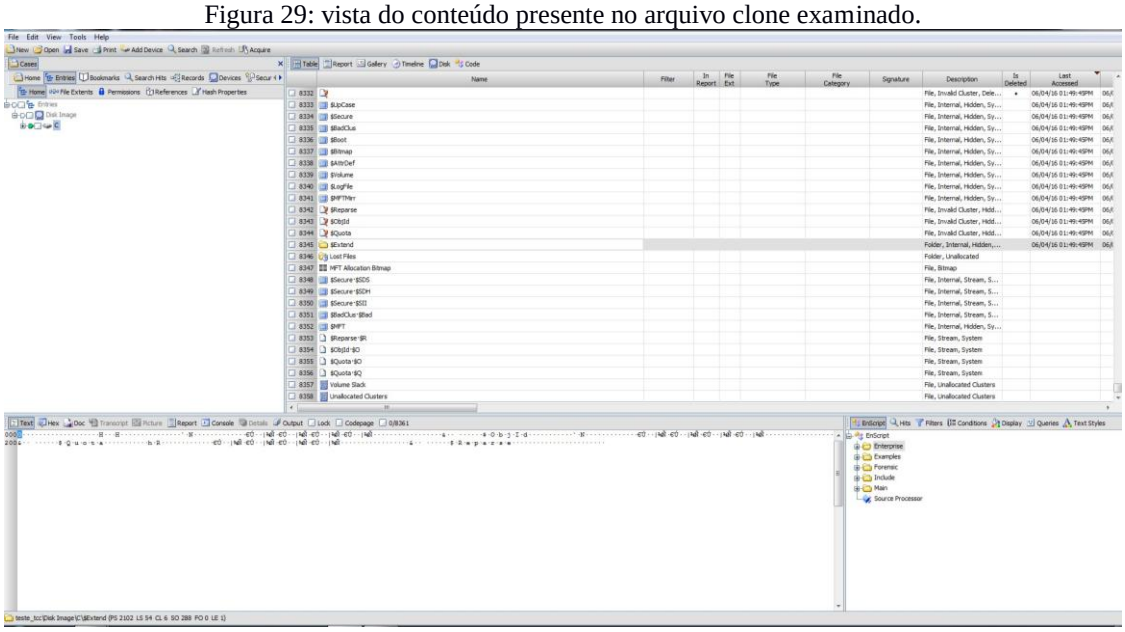


Figura 29: vista do conteúdo presente no arquivo clone examinado.



3.8 UTILIZANDO O FTK IMAGER

O FTK Imager assim como o Encase e o Autopsy possui interface gráfica, mas diferente dos outros dois, a interface é bem mais simples de ser utilizada (figura 8).

Como nos demais programas testados o FTK Imager também possui uma inserção da unidade ou clone que será examinado, mas não há necessidade de criar o caso, informando os dados do caso e o local onde o resultado da análise será armazenado. Isto é feito no momento da recuperação do(s) arquivo(s) de interesse, de modo individual (Figura 30).

Figura 30: tela do FTK Imager exibindo os dados encontrados no arquivo clone examinado.

3 RESULTADOS

A avaliação do desempenho das ferramentas utilizadas na recuperação dos arquivos, foi baseada na capacidade de recuperar corretamente os arquivos de imagem excluídos considerando o montante deste tipo de arquivo. Como demonstração matemática desta capacidade, fez-se cálculo matemático direto no qual a quantidade de arquivos de imagem recuperados foi dividia pelo total de arquivos de imagem que foram excluídos.

$$Eficacia = \frac{quantidadedearquivosrecuperados}{quantidadedearquivosexcludos}$$

A tabela I exibe os resultados obtidos por cada um dos programas testados, na eficácia de recuperar os um mil e trezentos arquivos de imagem apagados.

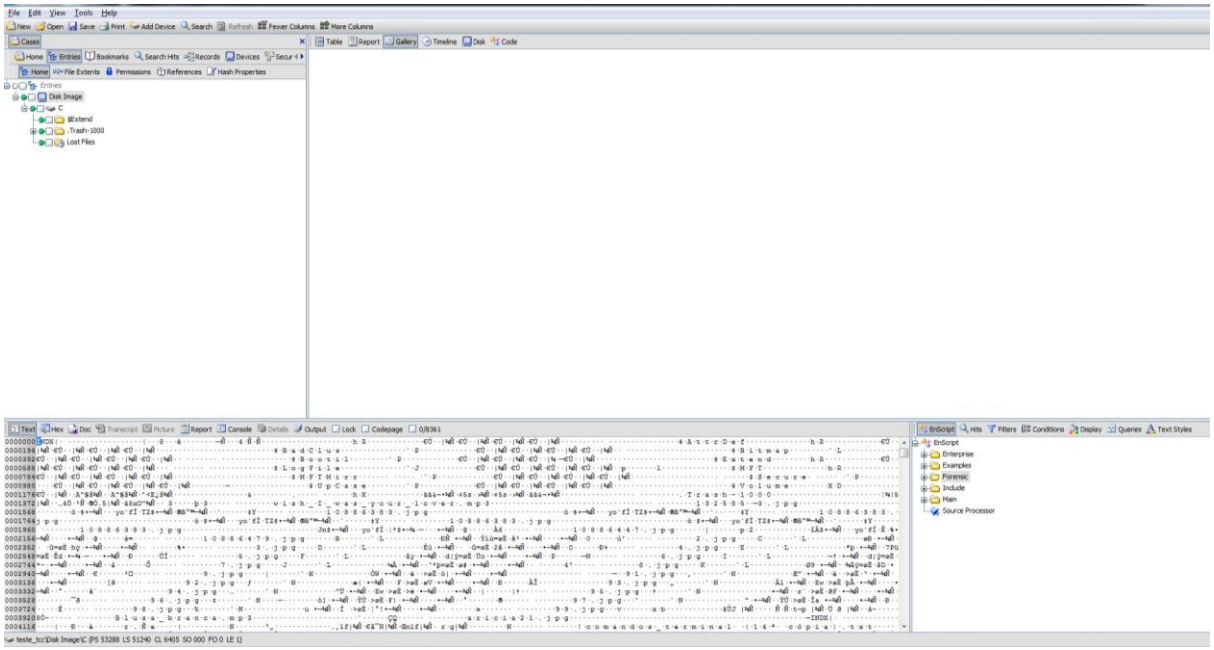
Tabela I: apresentação dos programas testados, quantidade de arquivos apagados e quantidade de arquivos que recuperados.

Programa	**Total de arquivos apagados**	**Total de arquivos Recuperados**	**Eficiência (%)**
Autopsy/Sleuth kit	1300	1331	99,23
Foremost	1300	1276	96,53
Photorec	1300	1210	93,07
Encase	1300	Não recuperou	0
FTK Imager	1300	Não recuperou	0

Os resultados observados permitem que se façam algumas inferências pelo desempenho extraordinário que os *softwares* de licença GNU quando comparados os *softwares* proprietários.

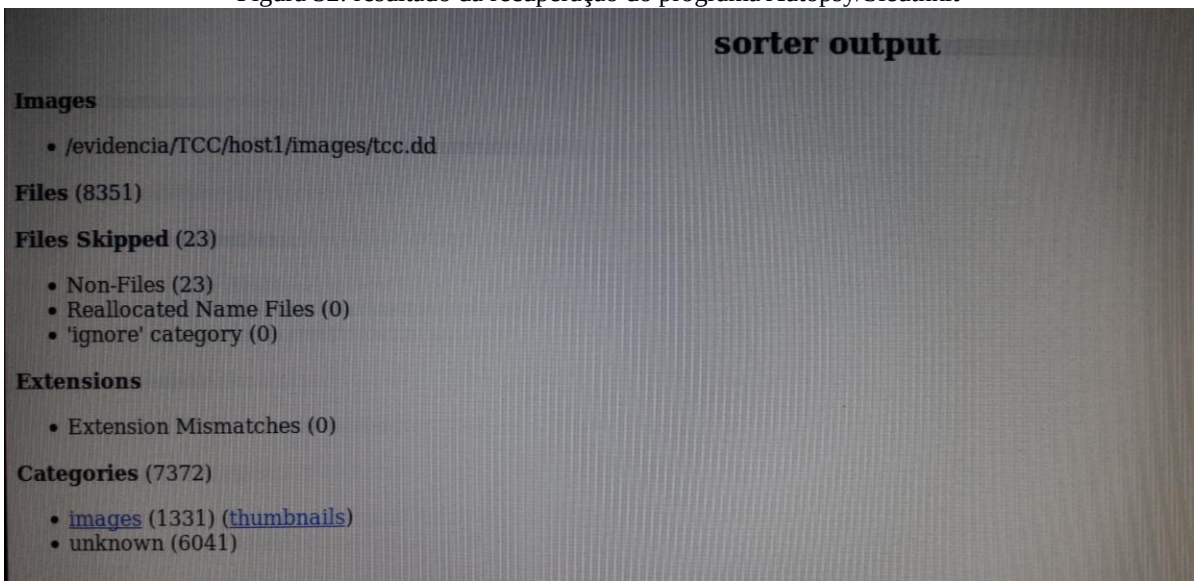
A primeira delas é que toda preparação da mídia foi feita utilizando estação de trabalho de sistema operacional Linux e programas nativos desse sistema, em especial a criação da partição, fato este que pode ter sido um dos fatores para a não recuperação automatizada de nenhum arquivo por parte do Encase e do FTK Imager (figuras 30 e 31).

Figura 31: tela do Encase que quando solicita-se a exibição de arquivos de imagem presentes e apagados, nenhum foi exibido.



Já em relação aos *softwares* Autopsy/Sleuth kit (figura 32), Foremost e Photorec (figura 33). O primeiro apresentou 100% de eficiência na recuperação de todos os arquivos de imagem apagados, entretanto, indicou a recuperação de arquivos de imagem falso positivos, pois houve a indicação de recuperação de um número maior de arquivos do que realmente havia.

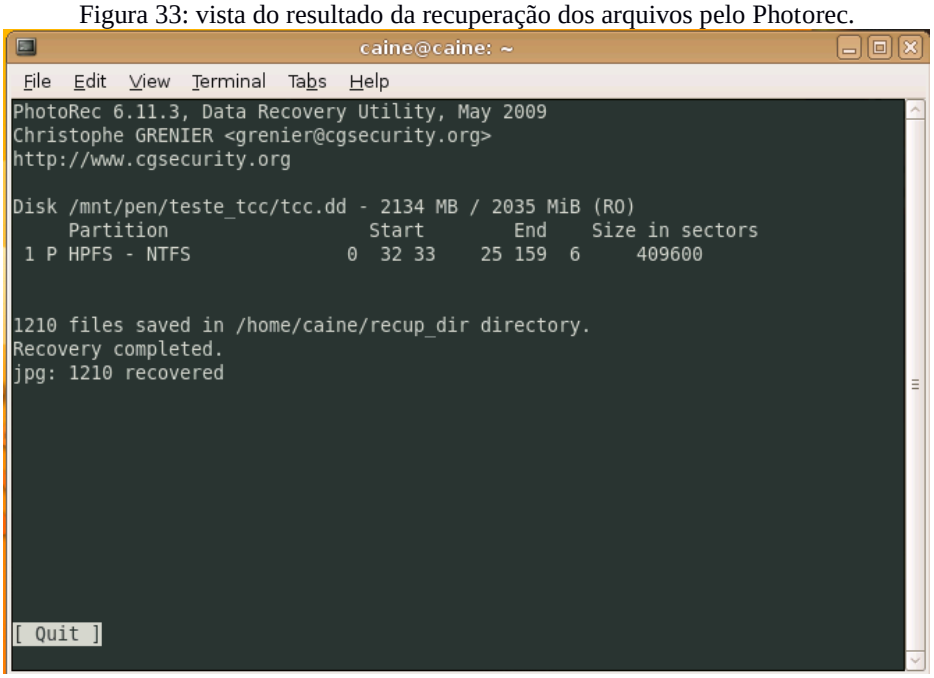
Figura 32: resultado da recuperação do programa Autopsy/Sleuthkit



Já o Foremost e Photorec apresentaram uma eficiência da ordem de 98,15% e 93,07%, respectivamente. O Foremost assim como o Autopsy/Sleuth kit, também computou

em sua estatística a recuperação de arquivos de imagem falso positivos, no total de 21 arquivos. Reduzindo essa quantidade do total indicado pelo programa, chega-se a uma eficiência da ordem de 96,53%.

Figura 33: vista do resultado da recuperação dos arquivos pelo Photorec.



4 CONSIDERAÇÕES FINAIS

Os ensaios realizados para análise de performance na comparação de cinco ferramentas de recuperação de arquivos excluídos, permitiu observar que ferramentas de uso em sistemas operacionais Linux foram eficientes na recuperação dos arquivos de imagem excluídos, quando comparadas as ferramentas de uso em sistema operacional Microsoft Windows, as quais não foram eficazes na recuperação dos arquivos.

Dentre as ferramentas testadas, a que teve melhor desempenho foi o programa Autopsy/Sleuth kit, seguido do Foresmost e do Photorec. Apesar do melhor desempenho dos programas Autopsy/Sleuth kit e Foremost, ambos recuperaram arquivos falso positivos, enquanto que o Photorec não.

Diante dos resultados obtidos, propõe-se que novos ensaios sejam realizados, analisando a eficácia de recuperação em outros sistemas de arquivos, como ext2, ext3, ext4, reseifers etc, mensurar o tempo demandado para realizar a recuperação dos arquivos, a quantidade de arquivos falsos positivos e falsos negativos recuperados, disponibilidade de uso em sistemas operacionais distintos, possibilidade de uso sem instalação das ferramentas, para assim se tenham mais variáveis a serem consideradas na eleição das melhores ferramentas de recuperação de arquivos excluídos.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Lei 8.069, de 13 de julho de 1990. Dispõe sobre o estatuto da criança e do Adolescente e dá outras providências. Disponível em http://www.planalto.gov.br/ccivil_03/leis/L8069Compilado.htm. Acesso em: 05/06/2016.

BRASIL. Lei 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 05/06/2016.

BRASIL. Lei 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 05/06/2016.

BRIGATTO, Gustavo. **Número de usuários de smarphones no Brasil cresce 48% no 3º trimestre**. Valor Econômico. 24/11/2015. Disponível em http://www.valor.com.br/empresas/4327844/numero-de-usuarios-de-smartphones-no-brasil-cresce-48-no-3-trimestre. Acesso em: 29/05/2016.

DAQUINO, F. **Windows 7 continua sendo o sistema opercional maus usado no mundo**. Maio/2015. Disponível em http://www.tecmundo.com.br/windows-7/79298-windows-7-continua-sendo-sistema-operacional-usado-mundo.htm. Acesso em: 05/06/2016.

ELEUTÉRIO, P.M.S.; MACHADO, M.P. **DESVENDANDO A COMPUTAÇÃO FORENSE**. 1. São Paulo: Novatec, 2011. 200 p.

FISHER, G.E. **Computer Forensic Guidance**. ITL Bulletin. November-2001. NIST, Washington, 2001. Disponível em http://www.cftt.nist.gov/itlbulletin.html. 2001. Acesso em: 29/05/2016.

FOREMOST. Disponível em http://foremost.sourceforge.net/ Acesso em 29/05/2016.

MADEIRA, D. **LinEn e FTK Imager, aquisição forense em Linux**. Disponível em http://dan-scientia.blogspot.com.br/2012/01/linen-e-ftk-imager-aquisicao-forense-em.html. 07/Jan/2012. Acesso em: 29/05/2016.

PHOTOREC. Disponível em http://www.cgsecurity.org/wiki/PhotoRec Acesso em: 29/05/2016.

SÁ, L.F. **A Lei de Moore e a Lei do Lagarto**. Isto É. São Paulo, São Paulo, 06 maio 2016. Ano 39, 2422. p. 58.

SPERAZINI, P.A.P. **A responsabilidade advinda: Crime eletrônico bate às portas do mundo corporativo**. Disponível em http://www.direitonet.com.br/artigos/exibir/2962/A-responsabilidade-advinda-Crime-eletronico-bate-as-portas-do-mundo-corporativo. Acesso em: 29/05/2016

TONETTO, M. **Fraudes virtuais crescem 500% em um ano no Brasil; saiba como se defender**. Disponível em http://zh.clicrbs.com.br/rs/noticias/noticia/2015/07/fraudes-virtuais-crescem-500-em-um-ano-no-brasil-saiba-como-se-defender-4792272.html. Acesso em: 29/05/2016

UNITED STATE OF AMERICA[1]. **Computer Forensic Tool Testing**. Disponível em http://www.cftt.nist.gov/. 2014. Acesso em: 29/05/2016.

UNITED STATE OF AMERICA[2]. Homeland Scurity. **Encase Forensic v7.09.05. Test Results for Graphics File Carving Tool**. 2014.

UNITED STATE OF AMERICA[3]. Homeland Scurity. **FTK v4.1. Test Results for Graphics File Carving Tool**. 2014.

UNITED STATE OF AMERICA[4]. Homeland Scurity. **PhotoRec v7.0-WIP. Test Results for Graphics File Carving Tool**. 2014.

UNITED STATE OF AMERICA[5]. Homeland Scurity. **The Sleut Kit (TSK) 3.2.2/Auposy 2.24**. **Test Results for Deleted File Recovery and Active File Listening Tool**. 2014.

VECCHIA, E.D. **Perícia Digital Da Investigação à Análise Forense**. 1. Campinas: Millennium, 2014. 279 p.

WENDT, E.; JORGE, H.V.N. **Crimes Cibernéticos. Ameaças e Procedimentos de Investigação**. 2 ed. Rio de Janeiro: Brasport, 2013. 369 p.