FACULDADES INTEGRADAS DE CARATINGA

FACULDADE DE CIÊNCIA DA COMPUTAÇÃO

Análise Qualitativa de Ferramentas Forenses para Recuperação de Arquivos

HÁRRISON VITOI CUNHA

FIC/CARATINGA

2012

HÁRRISON VITOI CUNHA

Análise Qualitativa de Ferramentas Forenses para Recuperação de Arquivos

Monografia apresentado à Faculdade de Ciência da Computação das Faculdades Integradas de Caratinga como exigência parcial da disciplina de Trabalho de Conclusão de Curso I, sob orientação do Professor Msc. Jacson Correia Rodrigues da Silva.

FIC/CARATINGA

2012

HÁRRISON VITOI CUNHA

Análise Qualitativa de Ferramentas Forenses para Recuperação de Arquivos

Monografia submetida à Comissão examinadora designada pelo Curso de Graduação em Ciência da Computação como requisito para obtenção do grau Bacharel.

_____

Prof. Msc Fabrícia Pires Souza Tiola

Faculdades Integradas de Caratinga

_____

Prof. Msc Jacson Correia Rodrigues da Silva

Faculdades Integradas de Caratinga

_____

Prof. Msc Míriam de Souza Monteiro

Faculdades Integradas de Caratinga

FIC/CARATINGA

2012

AGRADECIMENTOS

Gostaria de agradecer primeiramente a Deus por tudo que tem feito em minha e por ter me iluminado na minha caminhada até hoje. Em seguida gostaria de agradecer a todos os meus familiares que desde o início do curso sempre me deram apoio para que eu pudesse concluir o curso de Ciência da Computação com muita garra e determinação.

RESUMO

A computação forense é uma área da ciência da computação que trabalha com crimes cibernéticos, onde ela aborda diversos deles mencionados por GUIMARÃES (2003), como por exemplo: pornografia infantil, acesso à conta bancária e obtenção de arquivos pessoais. Portanto, segundo REIS (2002), alguns métodos são utilizados para realizar esses crimes. São eles: identificar o arquivo, definir o objetivo da invasão, verificar vulnerabilidades, verificar se pode haver comprometimento, reconhecer o sistema e limpar os rastros de arquivos.

Em propósito, o presente trabalho teve por objetivo analisar quatorze ferramentas forense livre como: autopsy, encase, foremost, forensix, fdtk, ftk, glary undelete, ifile recovery, pandora, recuva, scalpel, sleuth kit, testdisk, e the coroner's toolkit, visando recuperar diversos arquivos de um *pendrive*, sendo que a análise ocorreu de duas formas: primeiro o *pendrive* foi analisado com arquivos no total de 1,37 GB, e segundo, ele foi analisado novamente porém com arquivos no total de 578 MB. Assim, todo esse processo de recuperação foi baseado em cinco critérios de acordo com a norma ISO/9126 (ISO 9126, 1996). São eles: funcionamento, usabilidade, desempenho, confiabilidade e portabilidade.

Portanto, o resultado que se obteve durante a análise e recuperação dos arquivos, foi que a ferramenta iFile Recovery apresentou 100% de aproveitamento em todos os critérios, sendo ela portável para Windows. Já a ferramenta que obteve o melhor resultado para o sistema operacional GNU/Linux foi a TestDisk com 96% de aproveitamento.

Palavras Chaves: computação forense, recuperação de arquivos, segurança, dados apagados, técnicas anti-forense, sistema de arquivos, ferramentas e critérios.

ABSTRACT

The forensics computer is an area of computer science that deals with cyber crimes, where it discusses several of them mentioned by GUIMARÃES (2003), as for example: child pornography, bank account access and personal files achievement. Therefore, according REIS (2002) some methods are used to carry out these crimes. They are: identify the file, define the objective of the invasion, check for vulnerabilities, check if there can be compromise, recognize the system and clear the tracks of the files.

As purpose, the present study aimed to analyze fourteen forensic free tools like: autopsy, encase, foremost, forensix, fdtk, ftk, glary undelete, ifile recovery, pandora, recuva, scalpel, sleuth kit, testdisk, and the coroner's toolkit, aiming to recover multiple files from a *pendrive*, being that the analysis took place in two ways: first the *pendrive* was analyzed with files totaling 1,37 GB, and then it was examined again but with a total of 578 MB. So, this whole process of recovery has been based on five criteria in accordance with ISO/9126 (ISO 9126, 1996). They are: operation, usability, performance, reliability, and portability.

Therefore, the result that was obtained during analysis and recovery of files, was that the tool iFile Recovery presented 100% of use in all criteria, being it portable to Windows. Yet the tool which obtained the best result for the GNU/Linux operating system was the TestDisk with 96% of utilization.

KEY-WORDS: Forensics Computer, Recovery of Files, Security, Erased Data, Anti-forensics Techniques, Systems of Files, Tools and Criteria.

LISTA DE TABELA

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

A palavra forense, segundo GOLDMAN (2010), entende-se como uma área policial onde é feito toda uma análise de um material coletado para investigação da cena do crime. A computação forense é uma área da Ciência da Computação que atua na área criminal no qual ela descobre, preserva, restaura e analisa todas as evidências encontradas na cena do crime.

Com isso, para solucionar os crimes ocorridos na Internet, como arquivos que foram obtidos ilegalmente de algum usuário, ferramentas são utilizadas e quatro métodos de investigação, segundo TAVARES (2007), devem ser seguidos: coleta de dados, exame, análise e resultados obtidos.

Assim, para cada sistema operacional existe um sistema de arquivos onde em cada um deles há uma tabela chamada tabela de arquivos que tem por função armazenar todos os arquivos. Segundo OLIVEIRA (2003), todo arquivo possui propriedades como nome, tipo do arquivo, tamanho, data e hora de criação, data de acesso, data de modificação e com isso cada sistema de arquivo define de uma forma diferente regras capazes de identificar o arquivo.

Portanto, como os dados obtidos ilegalmente na Internet são armazenados em disco e após são apagados, necessita-se de aplicativos para a examinação e análise de um réu sobre os dados que possuía, e com isso o atual trabalho tem por objetivo analisar ferramentas livres, como autopsy, encase, foremost, forensix, fdtk, ftk, glary undelete, iFile Recovery, pandora, recuva, scalpel, sleuth kit, testdisk, e the coroner's toolkit afim de categorizar qual delas melhor se adapta ao caso de recuperação de arquivos.

Desta forma, existem diversos sistemas de arquivos que são utilizados em vários sistemas operacionais e com isso, o atual trabalho apresenta apenas os sistemas de arquivos que são utilizados pelas plataformas Windows e Linux. Os sistemas de arquivos FAT16, FAT32, NTFS e VFAT são utilizados no Windows. Em contra partida, os sistemas EXT2, EXT3, EXT4, REISERFS, XFS e JFS são utilizados pelo GNU/Linux.

Assim, a análise será baseada nos critérios da norma ISO/9126 (ISO 9126, 1996) como funcionalidade, desempenho, confiabilidade, e portabilidade em relação a dois sistemas operacionais: Windows e GNU/Linux. Por fim, o motivo de se utilizar essas ferramentas é que elas foram analisadas com frequência em diversos trabalhos como: NASCIMENTO (2010), ASSUMPÇÃO (2010), VIOTTI (2012), foram analisadas por

diversos autores na internet como: MOTTAa (2009), MOTTAb (2009), MOTTAc (2009), MOTTAd (2009), AUTOPSY (2012), ENCASE (2012), FDTK (2012), FORENSIX (2012), TESTDISK (2012) e pelo site como por exemplo: FDTK (2012), GLARY UNDELETE (2012), iFILE RECOVERY (2012), PANDORA (2012), RECUVA (2012), no qual foi demonstrado a importância delas para o caso de recuperação de arquivos.

Visto que a computação forense é uma área de extrema importância, devido à falta de segurança na Internet e que é uma área que trabalha visando solucionar problemas como o furto de dados pessoais, esse trabalho visou contribuir na área, efetuando análise das ferramentas citadas anteriormente.

Segundo TAVARES (2007), a área forense existe há muitos anos, porém, há pouco tempo ela vem sendo utilizada no ramo da tecnologia, sendo que seu objetivo é reunir o máximo de evidências possíveis em diversos dispositivos computacionais, para que essas evidências sejam utilizadas para provar que realmente o crime aconteceu.

Mesmo a área forense sendo nova no ramo da tecnologia, ela oferece diversas ferramentas, para que os profissionais possam desvendar os crimes ocorridos na Internet. Porém, devido à quantidade de ferramentas disponíveis, torna-se complicado a escolha de qual utilizar além de faltar uma abordagem sobre as características de cada ferramenta e seu grau de utilidade. Portanto, o objetivo desse trabalho foi categorizar qual das quatorzes ferramentas selecionadas melhor se adapta ao caso de recuperação de arquivos e apresentar conceitos fundamentais sendo que no capítulo 1 é abordado tópicos como: o que é computação forense, o que é um sistema de arquivos, como ocorre o armazenamento no disco, estrutura de um sistema de arquivo, propriedades, tipos de sistema de arquivos, as ferramentas selecionadas para o trabalho, técnicas anti-forense e por fim os critérios de avaliação.

Já no capítulo 2, é apresentado como foram realizadas as análises de cada ferramenta, sendo que ocorreram em uma máquina local no qual ela de minha propriedade, e quais foram os resultados que elas apresentaram diante dos critérios: funcionamento, usabilidade, desempenho, confiabilidade e portabilidade, e por fim na subseção 2.2 é explicado o porquê da não utilização de algumas ferramentas. No capítulo 3 são apresentados os resultados obtidos diante das análises e na subseção 3.1 é explanado de forma resumida os dados obtidos no capítulo 2.

Portanto, no capítulo 4 é apresentado uma tabela de comparação entre as ferramentas utilizadas, sendo que logo abaixo é descrito de forma clara que a ferramenta iFile Recovery foi a melhor ferramenta para Windows e a ferramenta TestDisk foi a melhor

para o sistema operacional GNU/Linux.

1. REFERENCIAL TEÓRICO

A computação forense é uma área da Ciência da Computação que trabalha com crimes ocorridos na Internet, oferecendo recursos como ferramentas a fim de solucionar este problema. Atualmente os crimes cibernéticos vêm acontecendo de forma frequente onde um dos principais é o furto de dados e arquivos pessoais, que segundo (GUIMARÃES, 2003; ARGOLO, 2005), tem o objetivo de acessar contas bancárias objetivando desviar dinheiro, obter fotos e vídeos pornográficos infantis, inserir vírus ao enviar um email objetivando obter senha, login e arquivos, e monitorar a máquina utilizando um programa.

Segundo TAVARES (2007), a computação forense analisa toda a cena do crime baseando-se em quatro métodos: coleta dos dados, examinação dos dados, análise das informações obtidas e obtenção de resultados. A coleta de dados consiste em coletar todas as evidências encontradas, manter a integridade dos dados, ou seja, mantê-los seguros para não haver perda e identificar as ferramentas que serão utilizadas para resolver o problema. O segundo método a ser utilizado é a examinação dos dados onde é identificado e filtrado todos os dados que forem importantes. O terceiro método consiste em analisar as informações, relacionar as pessoas ligadas ao crime, relacionar o local onde ocorreu o fato e através dessa análise, fazer a reconstrução da cena do crime para chegar a um resultado satisfatório.

Entretanto, segundo OLIVEIRA (2003), trabalhar com os métodos de investigação envolve seriedade, pois são informações pessoais que estão sendo analisadas. Com isso, o resultado que se obtém em cada método mencionado anteriormente, provém das informações contidas no sistema de arquivos do sistema operacional, onde todo arquivo criado é armazenado em uma tabela chamada tabela de arquivos. É importante ressaltar que todo arquivo possui propriedades como nome de origem, tipo, tamanho, data e hora de criação, data de acesso e com isso cada sistema de cada sistema operacional, define regras capazes de identificar os arquivos na tabela de arquivos.

Embora todo arquivo armazenado no disco possua atributos que o fazem ser identificados, segundo TANEMBAUM (2010), eles também possuem métodos como:

- método de criação: indica que ele foi criado sem informação alguma.
- método de exclusão: refere-se ao fato de caso o arquivo não precise ser mais

utilizado, ele é removido, e através disso, espaço é liberado em disco.

- método de abertura: indica que o arquivo antes de ser executado, precisa que seus atributos sejam carregados na memória para aí sim o usuário conseguir usá-lo.
- método de fechamento do arquivo: refere-se ao fato de que a partir do momento que o acesso ao arquivo não acontece mais, ele deve ser fechado para liberar espaço na tabela de arquivos.
- método de leitura: refere-se que o arquivos precisam ser carregados da memória para ser utilizado.
- método de escrita: refere-se à escrita de dados no arquivo.
- método anexar: indica que só é possível acrescentar dados na parte final do arquivo.
- método procurar: refere-se que para ter acesso aos arquivos, é preciso identificar onde se encontram para que o ponteiro de arquivos possa apontar para o local onde estão e através disso, eles poderem ser lidos ou escritos.
- método obter atributos: indica que para um arquivo ser executado, os processos, ou seja, os programas precisam obter os atributos do arquivo para que possam ser exibidos.
- método definir atributos: refere-se à alteração dos atributos de um arquivo após sua criação.
- método renomear arquivo: refere-se ao fato de poder renomear o nome de origem de um arquivo.

Segundo (INFOWESTERa, 2007; TANENBAUM, 2010), ao serem gravados na tabela, eles precisam ser armazenados no disco rígido onde é formado por cinco componentes como: pratos, eixos, cabeça, braço e atuador. Os pratos são os locais onde os dados serão armazenados, sendo cada um deles feito de alumínio, revestidos por um material magnético e por uma camada protetora. Eles ficam localizados sobre um eixo responsável por fazê-los girarem durante a gravação onde eles são divididos em trilhas e cada uma delas é dividida em setores, onde geralmente tem uma capacidade de armazenamento de 512 bytes. A cabeça, ou seja, o cabeçote é responsável por gravar os arquivos nos pratos, sendo que há uma bobina com impulsos magnéticos que aciona o disco a fim de realizar a gravação dos dados. O cabeçote fica localizado na extremidade do braço, onde sua função é posicionar o cabeçote sobre os pratos. Portanto, o componente

chamado atuador é o responsável por realizar o movimento do braço sobre os pratos.

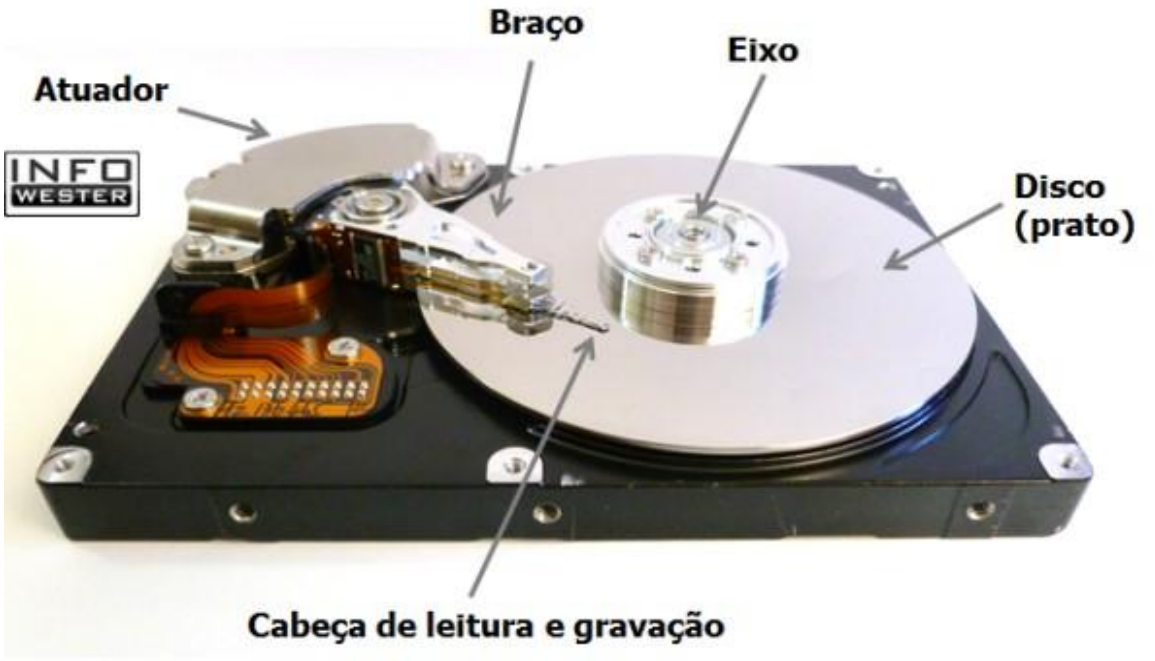

Figura 1 – Disco Rígido

Fonte: infowester

A próxima seção apresenta os sistemas de arquivos que são mais utilizados atualmente em computadores e *pendrive*s.

1.3. SISTEMA DE ARQUIVOS

Essa seção apresenta como cada sistema de arquivos funciona e quais as suas características.

O sistema de arquivos FAT16 segundo (INFOWESTERd, 2003; MICROSOFTa, 2012), possui uma capacidade de armazenamento onde cada setor ou cluster do disco, comporta 2Kb, 4Kb, 8Kb, 16Kb e 32Kb. Assim, um arquivo de tamanho 60 Kb ao ser criado, utiliza dois espaços de trinta e dois *kbytes*, onde, sobrará espaço em alguns dos *clusters* e através disso, esse espaço ficará inutilizável porque o sistema de arquivo não permite que ele seja utilizado pelos demais arquivos.

Segundo (INFOWESTERd, 2003; MICROSOFT, 2006), o sistema de arquivos FAT32 possui uma capacidade de armazenamento de apenas 4 Kb, pois, assim espaços não são desperdiçados como no *FAT16*. Assim, segundo MICROSOFT (2012), ele se torna mais consistente pelo simples fato de atuar com quinze por cento a mais de eficiência em

relação ao *FAT*.

Ainda segundo a (INFOWESTERe, 2011; MICROSOFTb, 2012), apesar do FAT16 e o FAT32 trabalharem com endereçamento limitado, o NTFS não tem um limite para armazenar dados. Com isso, ele utiliza 64 *bits* em cada setor do disco, sendo assim definido a quantidade de dados que podem ser armazenados nas partições NTFS. Uma característica importante é quanto à tolerância a falhas, onde ele utiliza um arquivo de *log* que registra tudo que acontece com o sistema operacional em relação aos arquivos. Assim, quando há um desligamento repentino da máquina, o sistema operacional ao ser inicializado, verifica no arquivo de *log* quais as funções que não foram executadas corretamente e a partir disso ele executa as funções corretas para resolver o problema. Portanto, esse arquivo fica armazenado no disco rígido sendo que permissões são definidas com o intuito de restringir o acesso a certas funcionalidades e arquivos relacionados ao sistema operacional.

Já no GNU/Linux, um sistema de arquivo muito utilizado segundo KERNEL (2012), é o EXT2, onde os espaços de armazenamento no sistema são chamados de blocos. Esses blocos possuem uma capacidade de armazenamento de 1024, 2048 e 4096 *bytes*, sendo que blocos menores representam menos espaço desperdiçado. Cada arquivo armazenado nos blocos possui um inode (*index*) onde sua estrutura é formada por ponteiros que apontam para os metadados de um objeto. Os metadados de um arquivo são o nome, permissão, tamanho, data de criação e data de modificação. Portanto, vários blocos podem ser reservados para um usuário.

Outro sistema de arquivo utilizado na plataforma GNU/Linux segundo (INFOWESTERc, 2003; KERNEL, 2012) é o EXT3, que trabalha com um método chamado *journaling* que verifica todas as mudanças correntes no sistema de arquivos. Cada informação obtida pelo journaling é armazenada em outro espaço do sistema operacional também chamado de *journal* (registro de *log*). Assim, o sistema de arquivos aplica as mudanças necessárias e em seguida remove as informações que foram obtidas pelo *journaling*. Portanto, o EXT3 possui uma camada chamada de *journaling block device (JBD)* que tem por objetivo implantar o *journaling* em diversos sistemas de arquivos. O JBD trabalha com um método onde ao invés de gravar os arquivos em bytes, ele grava blocos que sofreram mudanças no sistema de arquivos, sendo que facilita encontrar as operações que não foram realizadas adequadamente.

Assim, o sistema de arquivo EXT4 segundo (VIVAAOLINUXa, 2012; KERNEL, 2012), suporta partições de 1 EB (*exabyte*) e arquivos com tamanho até 16 TB (*terabytes*),

sendo que essas delimitações podem não ser úteis em servidores de pequeno porte, e sim para os de grande porte. Portanto, ele apresenta uma vantagem em relação ao EXT3, onde a pré-alocação de arquivos ou programas ocorre quando algum deles precisa utilizar espaços no disco rígido, e o próprio EXT4 reserva o espaço e através disso, nenhum outro arquivo ou programa pode utilizar aquele espaço.

O próximo sistema de arquivos utilizado também pelo GNU/Linux segundo (INFOWESTERb, 2007; KERNEL, 2012), é o ReiserFS. Ele também utiliza um método chamado journaling, onde tem por objetivo manter os dados em um perfeito estado quando houver situações inesperadas como desligamento repentino de uma máquina. Assim, utilizando o *journaling* o sistema de arquivos armazena as ações que podem ser realizadas em um arquivo (criação, alteração, exclusão) em um local chamado *journal*, ou seja, um arquivo de *log*. Esse arquivo tem por objetivo armazenar tudo que ocorre em um sistema de arquivos, pois, as informações são gravadas antes que ocorra alguma mudança no sistema. Isso se deve ao fato de que havendo um desligamento repentino de uma máquina, o sistema de arquivos executará todas as ações contidas no arquivo de *log* que não foram realizadas.

Além dos demais sistemas de arquivos mencionados anteriormente, há também o XFS que segundo KERNEL (2012), é um sistema de arquivo que trabalha com o método *journaling* e com isso ele suporta arquivos de grande extensão e sistema de arquivos extensos. Através disso, ele utiliza a forma de armazenamento *BTrees*, ou seja, em forma de árvore onde facilita encontrar arquivos e ajuda no desempenho do sistema de arquivo.

Outro sistema de arquivos também utilizado é o VFAT, onde segundo (VIVAAOLINUXc, 2006; KERNEL, 2012), ele é uma extensão do FAT16 e FAT32 e não tem suporte ao *journaling*. Ele é utilizado para transferir arquivos entre os sistemas operacionais Windows e Linux instalados em uma mesma máquina, pois, assim é possível que sejam escritos e lidos arquivos por ambos. Assim, segundo HARDWARE (2005), o VFAT enfrentara um grande problema quanto ao armazenamento de arquivos com nomes longos, sendo que os mesmos não podiam ser nomeados com caracteres acima de onze, sendo que desses onze, oito caracteres eram para o nome principal e os demais para a extensão. Com isso, acessando os arquivos via DOS, é possível apenas visualizar o nome apenas com alguns caracteres, e já via Windows, é possível visualizar por completo o nome.

Já o sistema de arquivo JFS, segundo (VIVAAOLINUXb, 2012; KERNEL, 2012), é um sistema que utiliza 64 *bits* em servidores. Ele possui vantagens como ser capaz de selecionar os setores do disco rígido que estão com defeito, fazer uso de pouco processador

e uso de *journaling* a fim de manter a integridade dos metadados em caso de um desligamento repentino de uma máquina. Em contra partida, ele também possui desvantagens como baixa transferência de arquivos, objetiva não trabalhar com arquivos pequenos e quanto ao espaço de armazenamento em cada partição, ele suporta apenas dois *terabytes*.

Portanto, os sistemas de arquivos citados anteriormente podem ser realizados com diversas ferramentas, e com isso a próxima seção apresenta as características das ferramentas selecionadas.

1.4 FERRAMENTAS

Esta seção tem como objetivo descrever de forma geral como cada uma das catorze ferramentas funcionam.

A ferramenta Autopsy segundo AUTOPSY (2012) é acessada em um servidor *web* onde ela é baseada em casos, ou seja, a cada nova investigação é criado um novo caso. Com isso, para iniciar um caso é preciso preencher o nome do caso, descrever de forma simples qual é o objetivo daquele caso, e por último, preencher os nomes dos investigadores que realizarão os testes. A seguir, é preciso preencher outras informações como o nome do host, ou seja, o nome da máquina que será analisada e uma simples descrição da mesma. A partir desse momento, é preciso inserir arquivos que contenham uma cópia da máquina que foi invadida e através dessa inserção, o perito pode começar a realizar a busca pelos arquivos apagados.

Após a busca ser realizada na ferramenta, é preciso verificar os dados que foram recuperados e com isso, ela é capaz de diferenciar cada tipo de arquivo. Se o arquivo recuperado aparecer com o nome em vermelho, significa que ele estava em um espaço de memória que ainda não foi realocado. Caso o arquivo apareça com o nome na cor bordô, significa que o espaço que ele estava ocupando, já foi realocado. Por fim, outro fator importante é que a ferramenta classifica cada arquivo recuperado de acordo com sua extensão, e cada espaço alocado ou não por um arquivo, é verificado permitindo a revelação dos dados e arquivos ocultos.

A ferramenta The Sleuth Kit segundo VIOTTI (2012) é um conjunto de ferramentas que são instaladas juntamente com a ferramenta Autopsy, sendo ela utilizada através de uma interface gráfica para que se torne de fácil manuseio e visualização. Outro ponto importante da ferramenta é quanto a sua utilização em multiplataforma, ou seja, pode

ser instalada tanto no Windows como no Linux.

Já a ferramenta Encase, segundo ENCASE (2012), é baseada na plataforma Windows sendo ela muito utilizada por peritos na área de investigação digital. Ela trabalha com criação de imagem de vários tipos de discos, ou seja, é feito uma cópia de mídias como disquetes, *pendrive*s e HD's. Essa cópia é chamada de *Encase Evidence File*, onde ela é capaz de analisar todas as cópias de uma só vez. Portanto, ela é capaz de reconstruir dados apagados sendo que o perito pode realizar essa operação, visualizando, ordenando e analisando os dados, os arquivos, através de uma interface gráfica.

Outra ferramenta apresentada é a FDTK, que segundo (FDTK, 2012; FDTKa, 2012) é de utilização livre onde ela objetiva realizar a coleta de dados para fins investigativos. Ela é baseada no sistema operacional GNU/Linux, onde ela engloba diversas ferramentas capazes de solucionar cada etapa de um processo de investigação. Portanto, ela vem sendo desenvolvida periodicamente sendo que ela não só oferece diversas ferramentas, mas também uma interface muito amigável, possuindo menus de navegação sendo eles em português, possuindo editores de texto, aplicativos para reproduzir filmes e sons.

Outra ferramenta apresentada é a Foremost, que segundo NASCIMENTO (2010) é código livre, ou seja, código fonte aberto sendo utilizada no sistema GNU/Linux a fim de recuperar arquivos contidos como por exemplo em imagens de disco. Para recuperar um arquivo, ela busca sempre pelo cabeçalho, legendas e pela estrutura de dados. Assim, ela suporta os seguintes sistemas de arquivos: Ext2, Ext3, Ext4, ReiserFS, FAT16, FAT32 e NTFS, onde também suporta arquivos com algumas extensões como .jpg, .gif, .png, .exe, .pdf, .doc, .rar, e .htm durante a análise de recuperação dos mesmos.

A próxima ferramenta apresentada é a Forensix, que segundo FORENSIX (2012) também engloba diversas ferramentas, sendo elas utilizadas através de uma interface gráfica. Ela foi desenvolvida por Fred Cohen onde ela é baseada na plataforma GNU/Linux e tem por objetivo auxiliar na documentação e no exame das informações coletadas. Portanto, ela possui características como produzir imagens de várias mídias como por exemplo disco rígido, disquete, cartão de memória, e por fim, ela produz imagens de diversos sistemas de arquivos sendo que ela possui também uma documentação que descreve as funcionalidades das ferramentas, além de permitir que uma busca seja feita através de palavras chaves, ser capaz de detectar o tipo de arquivo através de um conteúdo e por fim analisar todos os arquivos apagados.

Já a ferramenta FTK, segundo ASSUMPÇÃO (2010), é capaz de analisar

arquivos, decodifica-los, obter senhas que foram roubadas e além do mais, ela cria imagens de algumas mídias (*pendrive*, disco rígido, disquete), sendo capaz também de gerar relatórios baseando-se nos dados que foram coletados. Assim, ela é reconhecida pelo fato de ser eficiente na coleta de dados durante uma investigação e por conseguir processar uma grande quantidade de dados.

Além das ferramentas apresentadas anteriormente, outra ferramenta a ser apresentada é a Glary Undelete, que segundo (MOTTAa, 2009; GLARY UNDELETE, 2012), é uma ferramenta simples de utilizar onde ela é capaz de recuperar diversos tipos de arquivos de dispositivos como disco rígido, *pendrive* e cartão de memória. Assim, ela trabalha com dois tipos de sistemas de arquivos chamados FAT e NTFS, onde ela consegue também recuperar arquivos da lixeira que foram apagados ou que foram excluídos por um vírus. Com isso, para iniciar a recuperação dos arquivos, basta selecionar o dispositivo a ser analisado e em seguida basta clicar no botão "Pesquisa". Assim, com a busca finalizada, basta selecionar os arquivos que deseja recuperar, em seguida clicar em "Recuperar" e após isso, selecionar o destino onde serão salvos.

A ferramenta iFile Recovery segundo (MOTTAb,2009; iFILE RECOVERY, 2012) é uma ferramenta de livre utilização onde tem a capacidade de recuperar arquivos que foram apagados da lixeira, arquivos que foram deletados por algum vírus ou por qualquer outro motivo. Com isso, ela é capaz de recuperar qualquer tipo de arquivo (arquivos de texto, músicas, fotos) de dispositivos como disco rígido, *pendrive* e cartão de memória. Ela trabalha com os sistemas de arquivos FAT32 e NTFS. Portanto, para recuperar os arquivos, basta selecionar o dispositivo a ser analisado e em seguida escolher o modo de recuperação.

A ferramenta Pandora segundo (MOTTAd, 2009; PANDORA, 2012) é uma ferramenta livre, onde ela recupera diversos tipos de arquivos que foram deletados de dispositivos como disco rígido, cartão de memória e *pendrive*. Ela trabalha com o sistema de arquivos FAT e NTFS, sendo que existem três métodos para recuperá-los. O primeiro é o chamado de *Browse* que significa que a busca é realizada de forma rápida. O segundo método é o chamado de *Search* onde é permitido que a busca seja feita pelo nome do arquivo. E por fim, o terceiro método chamado *Deep Scan* é capaz de recuperar arquivos de um *pendrive* formatado.

A ferramenta Recuva segundo (MOTTAc, 2009; RECUVA, 2012) é uma ferramenta de livre utilização, onde ela é utilizada para recupera diversos tipos de arquivos em diversos dispositivos como disco rígido, cartão de memória e *pendrive*. Assim, para

recuperar os arquivos basta selecionar o dispositivo a ser examinado e após isso selecionar qual dos arquivos devem ser recuperados. Com isso, caso o recuva não consiga recuperar os arquivos de maior importância, basta utilizar o método *deep scan* que realizará uma busca mais detalhada. Por fim, o recuva possui alguns recursos como: recuperar arquivos deletados, recuperar arquivos em discos formatados, recuperar emails deletados, recuperar músicas, recuperar arquivos de texto.

A ferramenta Scalpel segundo NASCIMENTO (2010), é fundamentada na ferramenta foremost, onde ela tem por objetivo tornar seu desempenho cada vez melhor. Ela é mais utilizada em sistemas GNU/Linux, porém também pode ser utilizada em outras plataformas, bastando compilar os códigos fontes no sistema operacional. Sua última versão foi lançada em agosto de 2011 sendo que ela suporta sistemas de arquivos como Ext2, Ext3, Ext4, ReisersFS, Fat16, Fat32 e NTFS. Portanto, ela trabalha na linha de comando sendo capaz de recuperar arquivos com algumas extensões: .gif, .jpg, .png, .bmp,.doc, .ost, .htm, .pdf, .txt, .zip e .java.

A ferramenta TestDisk segundo TESTDISK (2012), é um software que possui uma alta capacidade de recuperação de arquivos, sendo que ela foi criada para atender a uma situação que é a recuperação de partições. Ela possui várias funções como: reconstruir os sistemas de arquivos FAT12, FAT16, FAT32, FAT e NTFS, sendo que ela também é capaz de obter de volta os arquivos perdidos no sistema de arquivo FAT. Com isso, outro fator importante na ferramenta, é que ela oferece dois tipos recursos para utilizá-la: iniciante e o avançado. Ela pode ser utilizada no sistema operacional Windows, GNU/Linux, DOS e Mac.

A ferramenta The Coroner's Toolkit segundo VIOTTI (2012), é um conjunto de ferramentas bastante utilizadas na área forense. Ela foi desenvolvida por Wietr Venema e Dan Farmer, onde seu lançamento ocorreu no ano de 2000 e a partir disso, ela foi expandida onde surgiu a ferramenta the sleuth kit. Ela possui três programas integrados sendo eles chamados de *grave-robber, mactime* e *lazarus*. O programa *grave-robber* é capaz de obter informações de uma máquina alvo ou de uma imagem criada a partir de um disco rígido. Essa busca pelas informações funciona da seguinte forma: é coletado todos os atributos dos arquivos, é coletado informações do estado da memória, arquivos apagados, arquivos executáveis, atributos dos arquivos removidos, o estado em que a rede se encontra, informações sobre o usuário, informações de arquivos ainda contido na imagem criada, e por fim, é realizado a cópia dos arquivos de configuração. Já a ferramenta *mactime*, é capaz de produzir um relatório contendo todos os acessos ocorridos nos

arquivos a partir de seus atributos gerados pela ferramenta *grave-robber*. Por fim, a ferramenta *lazarus* tem por objetivo reconstruir a estrutura de arquivos apagados.

Como mencionado anteriormente, segundo RODRIGUES (2010), em uma investigação são utilizadas ferramentas que são capazes de recuperar arquivos em máquinas, porém, esse processo não é simples, pois existem técnicas que são utilizadas para dificultar o processo da coleta de dados. Essas técnicas são chamadas de anti-forense, onde elas têm por objetivo tentar apagar totalmente um arquivo, sendo que ele não é totalmente apagado a não ser que seja sobrescrito. Portanto, essas técnicas envolvem também outro procedimento muito utilizado que nada mais é do que a ocultação de dados. Esse procedimento tem o mesmo objetivo das técnicas anti-forenses, porém, ele não apaga os arquivos. Como o próprio nome diz, ele oculta, esconde os dados com o intuito de dificultar ao máximo a sua obtenção. Com isso, existe outra técnica chamada WIPE no qual ela sobrescreve por diversas vezes o espaço liberado de um arquivo excluído, a fim de tornar mais difícil a recuperação do mesmo GOLDMAN (2010).

Além de essas técnicas serem utilizadas, outro fator importante segundo RODRIGUES (2010), é que existem ferramentas que são capazes de limpar todos os rastros deixados pelos arquivos ao serem apagados. Esse processo é realizado utilizando ferramentas, sendo que podem ficar para trás rastros como pedaço do nome, tipo do arquivo e data de criação, e através disso, o processo de investigação é facilitado.

As ferramentas autopsy, encase, foremost, forensix, fdtk, ftk, glary undelete, iFile recovery, pandora, recuva, scalpel, sleuth kit, testdisk, e the coroner's toolkit foram analisadas baseando-se em cinco critérios que seguiam a norma ISO/9126 (ISO 9126, 1996): funcionamento, usabilidade, desempenho, confiabilidade e portabilidade.

1.6 CRITÉRIOS

Essa seção tem por objetivo explicar como que as ferramentas serão analisadas com base nos critérios propostos, sendo que foram encontrados na norma ISO/9126 (ISO/91226, 1996).

Segundo a norma ISO/9126 para se analisar um *software* quanto ao funcionamento é preciso verificar sua capacidade de realizar funções e atender as necessidades esperadas. Assim, uma funcionalidade é dividida em cinco partes: adequação, acurácia, interoperabilidade, segurança de acesso e conformidade. A adequação de um *software* refere-se ao conjunto de funções onde é verificado se o que ele se propõe a fazer é

realmente adequado de acordo com as necessidades. Já a acurácia de um *software*, refere-se à apresentação de resultados onde eles podem ter sido gerados de forma correta ou não. Quando o software é capaz de se interagir com outros sistemas, ele está sendo analisado quanto à interoperabilidade. Outro fator importante é a segurança de acesso ao sistema, pois, é um fator que implica na segurança do *software* onde certas informações não devem ser expostas a certos usuários e nesse contexto entra a conformidade, no qual tem por objetivo garantir que o *software* esteja funcionando dentro dos padrões como normas e leis.

Outro critério analisado no presente trabalho foi quanto à usabilidade, sendo que segundo a norma ISO/9126 o usuário avalia o *software* à medida que vai utilizando. Esse critério é divido em três subcaracterísticas: inteligibilidade, apreensibilidade e operacionalidade. Um *software* é analisado quanto à inteligibilidade quando o usuário consegue reconhecer como ele funciona e através disso, ele pode ou não utiliza-lo. Já a subcaracterística apreensibilidade, refere-se à facilidade de se utilizar o *software*. E por fim, a subcaracterística operacionalidade avalia a interface do *software*, onde ela é o ponto principal que levará o usuário a utilizá-lo ou não.

Assim, outro critério analisado foi quanto ao desempenho, que segundo a norma ISO/9126 ele é medido a partir do momento que o usuário faz uma solicitação de alguma função do *software* e com isso o tempo de resposta faz com que seja medido a sua capacidade de retornar algo solicitado. Portanto, o desempenho está relacionado ao ambiente onde o *software* será executado, pois, isso implica no tempo de resposta ao usuário e havendo uma demora no retorno, gera insatisfação do mesmo. Entretanto, é preciso que o desempenho do *software* seja monitorado a todo o momento a fim de mantê-lo em um nível satisfatório para utilizá-lo.

O próximo critério analisado junto às ferramentas foi quanto à confiabilidade, sendo que segundo a norma ISO/9126 o desempenho do software é avaliado sobre um tempo determinado. O desempenho refere-se ao tempo que ele consegue se manter funcionando mesmo havendo falhas. Entretanto, todo software possui falhas e para provar que são tolerantes a elas, eles não devem interromper seu funcionamento independente do que aconteça. Embora, verificar como funciona a recuperação do software em caso de alguma falha, o torna mais confiável para uso.

O último critério que foi analisado foi quanto à portabilidade, sendo que segundo a norma ISO/9126 refere-se à adaptação do software em diferentes ambientes, sendo ele capaz de realizar suas funções normalmente. Segundo a norma ISO/9126 o fator portabilidade torna o software um produto de qualidade, pois, ele deve se adaptar aos

sistemas operacionais de forma a atender a cultura das empresas.

Portanto, uma Tabela foi criada na subseção 3.2 a fim de comparar qual das ferramentas analisadas melhor se adaptou ao caso de recuperação de arquivos.

2. METODOLOGIA

O presente trabalho foi desenvolvido para apresentar qual a melhor ferramenta melhor se adaptou ao caso de recuperação de arquivos. Assim, para se aplicar ao estudo, as ferramentas livres como: autopsy, encase, foremost, forensix, fdtk, ftk, glary undelete, iFile Recovery, pandora, recuva, scalpel, sleuth kit, testdisk, e the coroner's toolkit foram analisadas baseando-se na norma NBR ISO/ 9126 (ISO 9126, 1996) onde é listado alguns critérios e dentre eles foram selecionados os seguintes: funcionamento, usabilidade, desempenho, confiabilidade e portabilidade.

Com isso, a análise das ferramentas selecionadas e a recuperação dos arquivos aconteceram em uma máquina local sendo ela de minha propriedade que possui as seguintes configurações: 4 Gb de memória – DDR3, 500 Gb de HD, bateria de 6 células e um processador i3. Para a coleta dos dados, cada ferramenta utilizada foi instalada na máquina e através disso foi estabelecido que as análises aconteceriam utilizando-se um *pendrive* de 2 Gb de tamanho, que utilizava o sistema de arquivo FAT. O motivo de ter escolhido esse sistema de arquivos foi pelo fato de ser o mais utilizado nos dispositivos. Com isso cada ferramenta foi testada em várias situações sendo:

- Primeira: cada ferramenta foi analisada utilizando o *pendrive* contendo no total, duzentos e trinta e seis arquivos resultando em um tamanho de 1,37 Gb.
- Segunda: cada ferramenta foi analisada baseando-se no *pendrive* formatado.
- Terceira: cada ferramenta foi analisada baseando-se no *pendrive* com arquivos apagados.
- Quarta: cada ferramenta foi analisada novamente utilizando o *pendrive*, porém, contendo no total 578 MB de arquivos.
- Quinta: cada ferramenta foi analisada baseando-se no *pendrive* formatado.
- Sexta: cada ferramenta foi analisada baseando-se no *pendrive* com os arquivos apagados.

E por fim, cada ferramenta foi analisada de acordo com critérios estabelecidos, sendo que em cada situação da análise foi estipulado um tempo de cinco minutos para que as ferramentas conseguissem analisar e recuperar os arquivos do *pendrive*. Com esse tempo

estimado, todas elas conseguiram fazer a análise por completa em um tempo inferior a cinco minutos.

2.1 Ferramentas Utilizadas

Essa seção apresenta como cada ferramenta utilizada se comportou diante das análises e da recuperação dos arquivos. Em seguida, serão apresentadas informações de como elas se comportaram quanto aos critérios propostos.

2.1.1 Ferramenta Glary Undelete:

Funcionamento: Durante o processo de análise do *pendrive* em todos os estados em que ele foi testado, a ferramenta se apresentou muito capacitada a realizar todas as suas funcionalidades que foram requisitadas. Com isso, seu funcionamento permaneceu em excelente estado e com certeza apresentou os resultados que eram esperados como o perfeito estado dos arquivos. Portanto, ela levou três minutos para ser instalada, analisou os arquivos apagados e em um tempo de dois minutos ela recuperou os arquivos.

Usabilidade: Quanto ao critério usabilidade, à ferramenta é muito simples de utilizar pelo fato de possuir uma interface gráfica agradável e com isso, seguindo todas as funcionalidades, a recuperação dos arquivos ocorreu de forma rápida. Portanto, com toda a eficiência na análise dos arquivos, um fator que chamou atenção foi à facilidade de instalação, facilidade de utilizar as funcionalidades apresentadas, a facilidade de utilizar os menus, e pelo fato dela ser autoexplicativa e toda em português.

Desempenho: Na medida em que a ferramenta começou a ser executada, pode-se perceber que seu desempenho não se alterava quando uma funcionalidade era requisitada. Com isso, o seu tempo para responder a cada funcionalidade que era requisitada foi de cinco segundos. Portanto, para analisar o *pendrive* nos estados em foi mencionado anteriormente, a ferramenta foi capaz de recuperar os arquivos dentro de um tempo de dois minutos, sendo que o tempo estimado era de cinco minutos.

Confiabilidade: Quanto à confiabilidade, foi medido o seu desempenho onde ela

foi capaz de recurar totalmente e parcialmente os arquivos de 1,37 Gb e em seguida os de 578 Mb, em pouco menos de cinco minutos. Com isso, nesse meio tempo não houve arquivos corrompidos, sendo que apresentaram um ótimo estado de funcionamento. Portanto, ela apresentou bons resultados e se mostrou confiável, pois trabalhou de forma íntegra e correta.

Portabilidade: Por fim, a ferramenta se portou muito bem diante do ambiente Windows, pois, ela não é portável para o sistema Linux. E através disso, ela apresentou resultados seguros além de um bom desempenho. Com isso, apresentou também uma interface agradável e de fácil utilização, sendo que desempenhou com muita eficiência as suas funções.

Pendrive com os arquivos 1,37 Gb: Durante a execução, a ferramenta não foi capaz de analisar os arquivos que continham no *pendrive*. Além disso, ela não apresentou ao usuário uma mensagem informando o porquê a mídia não foi analisada. Portanto, esse fator de não analisar os arquivos existentes, apresentou um ponto negativo para ela.

Pendrive Formatado 1,37 Gb: A ferramenta não conseguiu recuperar os arquivos do *pendrive* formatado. Assim, como também ela não apresentou uma mensagem informando ao usuário o porquê não foi possível recuperar os arquivos. Portanto, esse fator demonstra um ponto negativo para a ferramenta, pois na hora de utilizá-la, esse fator de não ser capaz de trabalhar com *pendrive* formatado, vai ser levado em consideração.

Pendrive com os arquivos apagados 1,37 Gb: A ferramenta apresentou um rápido funcionamento onde de forma eficiente ela conseguiu recuperar duzentos e doze arquivos de duzentos e trinta e seis, sendo que eles totalizaram 1,25 Gb. Outro fator importante foi o fato de analisar rapidamente o *pendrive* e conseguir listar todos os arquivos. Portanto, em questão de desempenho, ela não apresentou falha em momento algum, porém, só deixou a desejar na questão de não recuperar totalmente os arquivos.

Pendrive com os arquivos 578 Mb: Durante sua execução, ela não apresentou nenhum erro e também nenhuma funcionalidade requisitada apresentou problemas. Portanto, durante a análise do *pendrive*, ela foi capaz de recuperar cento e vinte e nove arquivos, resultando em um total de duzentos e setenta e sete mega. Portanto, eles

permaneceram em perfeito estado.

Pendrive Formatado 578 Mb: A ferramenta mais uma vez não foi capaz de recuperar os arquivos do *pendrive* formatado. Com isso, ela também não informou o porquê os arquivos não puderam ser recuperados. Portanto, quanto ao seu funcionamento, ela apresentou um bom resultado devido a funcionar de maneira correta e segura, além de cada funcionalidade atender de forma satisfatória quando solicitadas.

Pendrive com os arquivos apagados 578 Mb: A ferramenta recuperou rapidamente os arquivos de forma em que eles permaneceram em perfeito estado. Outro fator importante foi que ela não apresentou falhas de execução, o que resultou em um bom desempenho e uma boa análise e recuperação dos arquivos. Porém, ela recuperou apenas duzentos e vinte e três arquivos, resultando em quatrocentos e vinte e sete mega dos quinhentos e setenta e oito mega, totalizando 427 Mb. Portanto, isso demonstrou que não foi recuperado de forma íntegra os arquivos e que em um caso de investigação esses arquivos poderiam fazer falta.

2.1.2 Ferramenta iFileRecovery:

Funcionamento: Durante a instalação, a ferramenta apresentou bons resultados onde suas funcionalidades são de fácil utilização. Assim, elas atenderam de forma satisfatória quando foram solicitadas, sendo que durante a análise dos arquivos seu funcionamento ocorreu de forma simples e eficiente onde os arquivos que foram recuperados em cada fase testada junto ao *pendrive* permaneceram intactos, ou seja, não sofreram nenhum dano. Portanto, o seu funcionamento se manteve cem por cento sem nenhum erro.

Usabilidade: A ferramenta em si é muito agradável e simples de utilizar pelo fato de possuir uma interface gráfica com poucas funcionalidades, porém muito eficientes. Além disso, é fácil de encontrar na interface as funcionalidades, pois, elas são bem visíveis e simples de entender. Portanto, o que a ferramenta demonstrou foi à facilidade de instalação, facilidade de utilizar as funcionalidades apresentadas, a facilidade de utilizar os menus, e pelo fato de ser autoexplicativa e toda em português.

Desempenho: Durante a análise dos arquivos, toda funcionalidade que foi requisitada para que de fato os arquivos pudessem ser recuperados, apresentou um ótimo desempenho, pois não travaram em momento algum devido ao ótimo funcionamento. Com isso, o tempo de resposta a partir do momento em que foi solicitada a verificação dos arquivos e a partir do momento em que foram recuperados, ela se tornou ainda mais agradável, pois não apresentou falha. Portanto, seu desempenho levou em média de cinco minutos para recuperar quase todos.

Confiabilidade: Quanto à confiabilidade, o desempenho da ferramenta não apresentou falhas e com isso pode-se perceber que ela é confiável, pois os arquivos recuperados permaneceram em um ótimo estado. Com isso, pelo fato dela ter apresentado um bom funcionamento, pode-se concluir que ela possui um alto grau de eficiência, pois não houve arquivos corrompidos, sendo que apresentaram um ótimo estado de funcionamento.

Portabilidade: Por fim, a ferramenta se portou muito bem diante do ambiente Windows, pois, ela não é portável para o sistema Linux. E através disso, ela apresentou resultados seguros além de um bom desempenho. Com isso, apresentou também uma interface agradável e de fácil utilização, sendo que desempenhou com muita eficiência as suas funções.

Pendrive com os arquivos de 1,37 Gb: Durante a análise dos dados, a ferramenta apresentou um bom desempenho onde conseguiu recuperar cento e setenta e dois arquivos dos duzentos e trinta e seis, somando assim em um total de 1,26 Gb. Assim, o processo de recuperação em si, aconteceu de forma simples e eficiente onde os arquivos recuperados permaneceram em perfeito estado. Portanto, ela desempenhou um bom trabalho ao recuperá-los com diversas extensões.

Pendrive Formatado 1,37 Gb: A ferramenta apresentou um excelente resultado, onde ela conseguiu recuperar cento e setenta e dois arquivos dos duzentos e trinta e seis. Além disso, seu desempenho foi excelente, onde não houve falhas e os arquivos permaneceram em um bom estado de utilização. Portanto, foi recuperado 1,26 Gb dos arquivos sendo que houve perda, mas pelo fato de ter sido capaz de resgatar somente os arquivos do *pendrive* formatado, já apresenta um ponto positivo.

Pendrive com os arquivos apagados 1,37 Gb: A ferramenta mais uma vez apresentou um ótimo resultado na recuperação dos arquivos, onde ela conseguiu recuperar cento e setenta e dois arquivos dos duzentos e trinta e seis, totalizando 1,26 Gb dos arquivos. Com isso, pode-se perceber que houve perda de arquivos durante a recuperação, mas isso não colocou a prova o seu grau de importância. Portanto, os arquivos permaneceram em um ótimo estado.

Pendrive com os arquivos 578 Mb: A ferramenta não apresentou nenhuma falha na análise e recuperação dos arquivos, sendo que foi recuperado trezentos e setenta e nove arquivos dos duzentos e sessenta e quatro, totalizando 739 Mb de arquivos. Com isso, a análise foi rápida e segura sendo que mais uma vez os arquivos permaneceram em excelente estado. Portanto, durante a recuperação dos arquivos a ferramenta mostrou alguns atributos como, por exemplo, o tamanho do arquivo, quando foi acessado, quando foi criado, quando foi modificado, e com isso ela demonstrou ser uma ferramenta completa e eficiente em relação a qualquer tipo de arquivo.

Pendrive Formatado 578 Mb: A ferramenta apresentou novamente um excelente resultado onde seu desempenho foi muito bom e muito eficiente, sendo que todos os arquivos não se corromperam. Foi recuperado duzentos e sessenta e sete arquivos dos duzentos e sessenta e quatro, totalizando 594 Mb de arquivos, ou seja, obteve o mesmo resultado da análise anterior. Portanto, mais uma vez a ferramenta atendeu de forma satisfatória em relação às funcionalidades, pois elas se desempenharam de forma muito eficaz.

Pendrive com os arquivos apagados 578 Mb: Durante a análise, a ferramenta trabalhou de forma eficiente sendo que todos os arquivos foram muito bem recuperados. Foi recuperado duzentos e sessenta e sete arquivos dos duzentos e sessenta e quatro, totalizando 594 Mb de arquivos, o que demonstrou que ela desempenhou suas funcionalidades da mesma forma em relação as demais situações. Portanto, mais uma vez ela apresentou eficiência na recuperação de qualquer tipo de arquivo.

2.1.3 Ferramenta Pandora:

Funcionamento: Durante a análise em todos os estados do *pendrive*, a ferramenta atendeu de forma satisfatória a cada funcionalidade requisitada, pois cada uma delas era simples de se utilizar, e com isso no final da análise a ferramenta conseguiu recuperar quase todos os arquivos sem que nenhum fosse corrompido. Portanto, ela é de fácil instalação e também se apresentou muito bem funcionando em todo momento da análise.

Usabilidade: A medida em que a ferramenta foi sendo utilizada, percebeu-se que toda funcionalidade era simples de se utilizar pelo simples fato de possuir uma boa interface gráfica. Portanto, é fácil utilizar as funcionalidades apresentadas, fácil de utilizar os menus, é autoexplicativa e toda em português.

Desempenho: Durante a análise de recuperação dos arquivos, cada funcionalidade que era requisitada, levava poucos segundos para ser executada, ou seja, o seu tempo de resposta foi muito pequeno, o que fez dela uma ferramenta eficiente. Com isso, o tempo de resposta a partir do momento em que foi solicitada a verificação dos arquivos e a partir do momento em que foram recuperados, foi de dois minutos e meio sendo que o tempo estimado foi de cinco minutos.

Confiabilidade: A ferramenta conseguiu manter seu bom desempenho do início ao fim da análise, não havendo falhas na execução e nem arquivos corrompidos. Portanto, seu nível de confiança é extremamente alto, pois em nenhum momento nada aconteceu de errado e cada funcionalidade trabalhou da melhor forma possível. Com isso, pelo fato dela ter apresentado um bom funcionamento, pode-se concluir que ela possui um alto grau de eficiência, pois não houve arquivos corrompidos, sendo que apresentaram um ótimo estado de funcionamento.

Portabilidade: A ferramenta foi utilizada apenas para ambiente Windows, e com isso, ela conseguiu manter seu excelente funcionamento e seu bom desempenho através de cada funcionalidade requisitada. Com isso, seu grau de confiança se tornou cada vez mais elevado pelo fato de em momento algum ter ocorrido falha de execução. Portanto, ela se desempenhou muito bem no Windows já que ela não é portável para Linux.

Pendrive com os arquivos 1,37 Gb: A ferramenta não foi capaz de analisar e recuperar os arquivos mesmo não sendo apagados do *pendrive*. Com isso, ela não informou em momento algum o porquê de não ser possível recuperar os arquivos já que eles estavam no *pendrive* normalmente.

Pendrive Formatado 1,37 Gb: A ferramenta foi capaz de recuperar os arquivos do *pendrive* formatado. Durante a análise, ela não analisou de forma eficiente, pois mesmo assim ela recuperou todos os arquivos, totalizando em 1,37 Gb de arquivos. Portanto, um ponto positivo foi que ela conseguiu recuperar arquivos de um *pendrive* formatado. Esse fator demonstra toda a sua utilidade para os usuários.

Pendrive com os arquivos apagados 1,37 Gb: Durante a análise, a ferramenta apresentou uma recuperação rápida e eficiente, porém alguns arquivos com extensão ".avi", ".jpeg" e uma imagem de um sistema operacional ".iso", não foram recuperados totalmente. Com isso, foi recuperado arquivos a menos, onde resultou em um total de 1,33 Gb. Portanto, retirando a questão em que alguns arquivos não foram totalmente recuperados, a ferramenta apresentou um alto grau de eficiência.

Pendrive com os arquivos 578 Mb: A ferramenta não foi capaz de analisar e recuperar os arquivos mesmo não sendo apagados do *pendrive*. Com isso, ela não informou em momento algum o porquê de não ser possível recuperar os arquivos já que eles estavam no *pendrive* normalmente.

Pendrive Formatado 578 Mb: A ferramenta foi capaz de recuperar todos os arquivos que continham no *pendrive* antes dele ser formatado. Com isso, sua análise levou em média de quinze minutos para verificar os arquivos que foram deletados e recuperar duzentos e sessenta arquivos dos duzentos e sessenta e quatro, totalizando assim em 573 Mb de arquivos, sendo que cada um permaneceu em perfeito estado para utilização. Portanto, o fato de não ser tão rápida na recuperação dos arquivos, comprova sua eficiência para recuperá-los.

Pendrive com os arquivos apagados 578 Mb: Durante a análise, a ferramenta manteve seu funcionamento em perfeito estado e através disso conseguiu recuperar quase todos os arquivos, pois alguns deles que tinham como extensão ".mpg" e "mp3", não foram

totalmente recuperados. Com isso, foi recuperado duzentos e sessenta arquivos dos duzentos e sessenta e quatro, totalizando assim em 573 Mb de arquivos. Portanto, a ferramenta foi capaz de recuperar apenas os arquivos que foram inseridos no *pendrive* quando ele foi formatado pela segunda.

2.1.4 Ferramenta Recuva :

Funcionamento: A ferramenta é fácil de instalar e com isso, ela apresentou um excelente funcionamento durante a análise, o que resultou na recuperação dos arquivos sem que houvesse nenhum erro. Portanto, cada funcionalidade da ferramenta apresentou resultados corretos, o que demonstrou uma alta capacidade de lidar com diferentes tipos e tamanhos de arquivos, onde todos se mantiveram em perfeito estado.

Usabilidade: Quanto ao fator usabilidade, na medida em que cada funcionalidade da ferramenta foi solicitada, cada uma delas atendeu de forma muito eficiente, pois, eram de fácil utilização. Portanto, sua interface é muito agradável e simples de se utilizar, sendo que ela demonstrou facilidade de instalação e de se utilizar as funcionalidades apresentadas com por exemplos os menus, e pelo fato de ser autoexplicativa e toda em português.

Desempenho: Quanto ao desempenho, na medida em que cada funcionalidade da ferramenta foi sendo requisitada, o tempo de resposta para executá-las foi extremamente pequeno, o que resultou no seu bom funcionamento e por consequência na fácil utilização. Portanto, a ferramenta foi capaz de recuperar todos os arquivos em três minutos sendo que o tempo estimado foi de cinco minutos.

Confiabilidade: Quanto à confiabilidade, a ferramenta conseguiu manter seu desempenho sem que houvesse nenhuma falha de execução. Isso demonstrou que falhas são difíceis de acontecer e cada vez mais ela se torna mais confiável pelo simples fato de trabalhar com eficiência e de manter os arquivos sem que eles sejam corrompidos.

Portabilidade: A ferramenta é portável para o sistema Windows, onde ela apresentou resultados que demonstrou a sua capacidade de recuperar os arquivos, diante do sistema. Portanto, ela se manteve funcionando e desempenhando muito bem diante das

funcionalidades que foram solicitadas na análise.

Pendrive com os arquivos 1,37 Gb: Durante a análise dos arquivos a ferramenta apresentou um resultado satisfatório onde cada arquivo recuperado se manteve em perfeito estado de utilização. Com isso, os arquivos foram utilizados novamente onde foi verificado se havia algum deles corrompidos. Portanto, foi recuperado duzentos e vinte e quatro arquivos dos duzentos e trinta e seis analisados, totalizando 1,24 Gb dos arquivos existentes, onde a ferramenta conseguiu trabalhar muito bem com diversas extensões dos mesmos.

Pendrive Formatado 1,37 Gb: A ferramenta conseguiu recuperar os arquivos do *pendrive* formatado, sendo que arquivos que já tinham sido apagados também foram recuperados. No total, foram recuperados trezentos e sessenta e seis arquivos dos duzentos e trinte e seis, onde apresentaram um total de 2,25 Gb. Portanto, pode-se notar que arquivos a mais foram recuperados. Em fim, o ponto chave da ferramenta foi ela ter sido capaz de recuperar algo mesmo a mídia estando formatada.

Pendrive com os arquivos apagados 1,37 Gb: Durante a análise dos arquivos apagados, a ferramenta recuperou uma quantidade menor de arquivos. Assim, foram recuperados cento e noventa e nove arquivos dos duzentos e trinta e seis analisados, totalizando em 1,33 Gb de arquivos, sendo que além dos arquivos que foram apagados, outros também foram recuperados. Portanto, isso demonstra a eficiência da ferramenta em buscar por arquivos antigos também.

Pendrive com os arquivos 578 Mb: A ferramenta apresentou um bom desempenho ao recuperar os arquivos que foram inseridos após a formatação do *pendrive*. Portanto, a ferramenta recuperou cento e catorze arquivos, sendo que noventa e três deles foram totalmente recuperados e vinte e um recuperados parcialmente. Assim, esses arquivos resultaram em 366 Mb, onde a recuperação aconteceu em um minuto e vinte segundos.

Pendrive Formatado 578 Mb: A ferramenta apresentou um bom desempenho durante a análise dos arquivos, sendo que ela foi capaz de recuperar setecentos e cinquenta e três arquivos sendo todos eles totalmente recuperados. Eles resultaram em um total de 1,64 Gb, onde a recuperação deles ocorreu em um tempo de dois minutos e vinte segundos.

Portanto, pode-se perceber que a ferramenta recuperou muitos arquivos além dos duzentos e sessenta e quatro (578 Mb).

Pendrive com os arquivos apagados 578 Mb: Durante a análise a ferramenta recuperou duzentos e sessenta e quatro arquivos, sendo que quarenta e cinco deles foram recuperados totalmente e duzentos e dezenove foram parcialmente. Com isso, a recuperação ocorreu em 152.29 segundos, onde nenhum deles apresentou nenhuma falha ao ser executado. Portanto, o fato dela ter sido capaz de lidar com arquivos com diversas extensões, ela comprovou o quão é eficiente.

2.1.5 Ferramenta Autopsy :

Funcionamento: A ferramenta apresentou um resultado satisfatório quanto ao seu funcionamento, pois apresentou uma rápida instalação de no máximo cinco minutos, e três minutos para recuperar os duzentos e trinta e seis arquivos, que por consequência tinham um tamanho total de 1,37 Gb. Em fim, sua execução ocorreu de forma simples, rápida e segura.

Usabilidade: Quanto à usabilidade, a ferramenta é de fácil utilização, pois, basta apenas utilizar cada funcionalidade e a partir desse momento recuperar os arquivos. Portanto, sua interface é muito agradável e simples de se utilizar, sendo que demonstrou facilidade de instalação, facilidade de utilizar as funcionalidades apresentadas, facilidade de utilizar os menus, e pelo fato de ser autoexplicativa e toda em português.

Desempenho: Na medida em que foi sendo solicitado a recuperação dos arquivos, a ferramenta respondeu de forma rápida e clara, onde ela se manteve funcionando do início ao fim da recuperação do arquivos sem apresentar nenhum erro, falha. Portanto, ela desempenhou uma boa recuperação dentro de um prazo de dois minutos, sendo que o tempo estimado foi de cinco minutos.

Confiabilidade: A ferramenta se apresentou de uma forma confiável, pois, durante o processo de recuperação dos arquivos, nenhum erro ocorreu, e depois de recuperados, eles voltaram a funcionar exatamente da mesma forma antes de serem recuperados e em outra etapa da recuperação eles se mostraram corrompidos. Portanto, os arquivos se

apresentaram em diferentes estados durante a recuperação.

Portabilidade: Por fim, a ferramenta foi facilmente instalada na plataforma Linux, onde seu desempenho foi muito bom, seu grau de confiabilidade se manteve, foi de fácil utilização, e com isso não apresentou qualquer tipo de erro durante a análise dos arquivos.

Pendrive com os arquivos 1,37 Gb: A ferramenta apresentou um bom resultado na análise e recuperação dos arquivos, onde todos eles apresentaram um ótimo funcionamento. Com isso, durante a análise não houve erro de execução e os duzentos e trinta e seis arquivos se mostraram corrompidos. Assim, a ferramenta apresentou um alto grau de confiança, pois, os arquivos foram recuperados normalmente.

Pendrive Formatado 1,37 Gb: A ferramenta não foi capaz de recuperar os arquivos do *pendrive* formatado. Com isso, durante o processo de análise do mesmo, a ferramenta não apresentou nenhum alerta de o porquê não foi possível recuperar os arquivos.

Pendrive com os arquivos apagados 1,37 Gb: A ferramenta foi eficaz na recuperação dos arquivos apagados, pois todos os duzentos e trinta e seis arquivos foram recuperados apresentando um bom estado de execução. Portanto, ela se mostrou muito confiável e fácil de lidar quando foi requisitado a recuperação dos arquivos.

Pendrive com os arquivos 578 Mb: Durante a análise a ferramenta não apresentou nenhum erro, porém ela recuperou uma quantidade de arquivos a mais do que já existia. Ela recuperou um total de quatrocentos e dezessete arquivos, resultando em 941 Mb. Portanto, isso demonstra uma alta capacidade de recuperar arquivos antigos, onde todos eles estão em perfeito estado de uso.

Pendrive Formatado 578 Mb: A ferramenta não foi capaz de recuperar os arquivos do *pendrive* formatado. Com isso, durante o processo de análise do mesmo, a ferramenta não apresentou nenhum alerta de o porquê não foi possível recuperar os arquivos.

Pendrive com os arquivos apagados 578 Mb: A ferramenta durante a análise de recuperação dos arquivos apresentou um bom desempenho, porém, recuperou mais arquivos do que o esperado. Foi recuperado setecentos e trinta arquivos, resultando em

1,36 Gb. Assim, isso demonstra que ela desempenha muito bem seu papel recuperando diversos tipos de arquivos.

2.1.6 TestDisk:

Funcionamento: A ferramenta apresentou um resultado satisfatório quanto ao funcionamento, pois em momento algum ela apresentou demora em recuperar os arquivos, que por consequência tinham um tamanho total de 1,37 Gb e com isso, a recuperação dos mesmos ocorreu de forma rápida, pois o funcionamento da ferramenta não apresentou falhas.

Usabilidade: Quanto à usabilidade, a ferramenta é de fácil utilização, pois, basta apenas utilizar cada funcionalidade e a partir desse momento recuperar os arquivos. Portanto, sua interface é muito agradável e simples de se utilizar, sendo que demonstrou facilidade de instalação, facilidade de utilizar as funcionalidades apresentadas, e pelo fato de ser autoexplicativa e toda em inglês.

Desempenho: Na medida em que cada funcionalidade foi sendo solicitada para que fosse possível realizar a recuperação dos arquivos, a ferramenta respondeu de forma rápida e clara, onde ela manteve seu desempenho do início ao fim da análise sem apresentar nenhuma falha. Portanto, ela levou em média de quatro minutos para recuperar os arquivos sendo que o tempo estimado foi de cinco minutos.

Confiabilidade: A ferramenta se apresentou de uma forma confiável, pois, durante o processo de recuperação dos arquivos, nenhum erro foi apresentado, e com isso os arquivos foram recuperados em perfeitas condições para o uso. Assim, ela demonstrou toda sua capacidade de lidar com diferentes tipos de arquivos de forma segura.

Portabilidade: A ferramenta se portou muito bem diante do ambiente Linux, pois, ela não é portável para o sistema Windows. E através disso, ela apresentou resultados seguros além de um bom desempenho. Com isso, apresentou também uma interface agradável e de fácil utilização, sendo que desempenhou com muita eficiência as suas funções.

Pendrive com os arquivos 1,37 Gb: A ferramenta apresentou um bom resultado na análise e recuperação dos arquivos, onde todos foram recuperados e com isso apresentaram um ótimo estado de funcionamento. Durante a análise não houve erro de execução e com isso a ferramenta demonstrou um alto grau de confiança, pois, os arquivos foram recuperados de forma rápida de modo a apresentarem um ótimo estado para reutilização.

Pendrive Formatado 1,37 Gb: A ferramenta não foi capaz de recuperar os arquivos após o *pendrive* ter sido formatado. Assim, percebe-se que ela não é tão eficiente.

Pendrive com os arquivos apagados 1,37 Gb: A ferramenta foi eficaz na recuperação dos arquivos apagados, onde todos foram recuperados e com isso permaneceram em um ótimo estado. Assim, a ferramenta não obteve nenhuma falha de execução, o que demonstrou que ela é confiável e que além de tudo consegue trabalhar com diferentes tipos de arquivos.

Pendrive com os arquivos 578 Mb: Durante a análise a ferramenta não apresentou nenhum erro de execução, e com isso ela recuperou arquivos além dos que já existiam. Ela recuperou quatrocentos e dezessete arquivos, resultando em 941 Mb. Portanto, ela demonstrou uma alta capacidade de obter novamente arquivos antigos.

Pendrive Formatado 578 Mb: A ferramenta não foi capaz de recuperar os arquivos após o *pendrive* ter sido formatado. Assim, percebe-se que ela não é tão eficiente.

Pendrive com os arquivos apagados 578 Mb: A ferramenta foi eficaz na recuperação dos arquivos que foram apagados, sendo que todos foram recuperados e com isso permaneceram em um ótimo estado de funcionamento. Portanto, ela se mostrou muito confiável e fácil de lidar com qualquer tipo de arquivo.

Concluindo o trabalho, uma tabela foi criada com o objetivo de mostrar a comparação entre as ferramentas e apontar qual delas melhor atende ao caso de recuperação de arquivos.

2.2 Justificativa da não utilização de algumas ferramentas

As ferramentas Encase, Forensix, e The Coroners Toolkit foram encontradas para serem utilizadas no trabalho, com isso, o fato delas não terem sido utilizadas foi por motivo em que não foi possível compilá-las no terminal do sistema GNU/Linux e pelo fato de possuir um alto grau de complexidade de utilização.

A ferramenta FTK não foi utilizada, pois não foi possível realizar a sua instalação, devido ao alto grau de complexidade de uso. Já as ferramentas Foremost, Scalpel e The Sleuth Kit foram encontradas, e através disso, elas possuíam um manual de como utiliza-las, sendo que ele não condizia com a ferramenta. Portanto, foi seguido todas as instruções do manual das ferramentas, pois, não eram tão compreensível de entender, e com isso não foi possível utiliza-las nos testes de recuperação dos arquivos.

3. RESULTADOS

O resultado das análises das ferramentas foi baseado nos critérios propostos anteriormente:

- Funcionamento: medirá quantos arquivos foram recuperados.
- Usabilidade: medirá as diversas funcionalidades e características existentes no sistema (o sistema é em português? Possui interface gráfica? Possui menu? É autoexplicativo?)
- Desempenho: medirá como a ferramenta se manteve ao recuperar os arquivos, estimando um tempo de cinco minutos para a recuperação dos mesmos.
- Confiabilidade: medirá quantos arquivos foram recuperados de forma em que executaram normalmente após a análise.
- Portabilidade: medirá o desempenho e o funcionamento no sistema operacional.
- Avaliação das ferramentas: foi avaliada a partir da soma das porcentagens que lhes foram atribuídas, dividido pelo número total de critérios.

3.1 Dados estatísticos das ferramentas testadas

- Ferramenta Autopsy:

- *Pendrive* com arquivos no total de 1,37 Gb: Foram recuperados os 236 arquivos, porém eles se apresentaram corrompidos.
- *Pendrive* com os arquivos apagados no total de 1,37 Gb: Foram recuperados os 236 arquivos sem apresentar nenhum problema de execução.
- *Pendrive* arquivos apagados 1,37 Gb: Foram recuperados os 236 arquivos sem apresentar nenhum problema de execução.
- *Pendrive* arquivos 578 Mb: Foram recuperados 417 arquivos (941 Mb) sendo 264 arquivos originais do teste e arquivos que não estavam visíveis ou que já tinham sido apagados.
- *Pendrive* formatado 578 MB: Não foi recuperado nenhum arquivo.
- *Pendrive* arquivos apagados 578 Mb: Foram recuperados 730 arquivos (1,36 Mb) dos 264 arquivos, o que demonstrou a capacidade da ferramenta recuperar arquivos antigos que já tinham sido apagados.

- Ferramenta Glary Undelete:

- *Pendrive* com arquivos no total de 1,37 Gb: Não foi recuperado nenhum arquivo.
- *Pendrive* formatado com arquivos no total de 1,37 Gb: Não foi recuperado nenhum arquivo.
- *Pendrive* com arquivos apagados no total de 1,37 Gb: Foram recuperados 212 arquivos (1,25 Gb) dos 236 arquivos originais.
- *Pendrive* com arquivos no total de 578 Mb: Foram recuperados 129 arquivos (277 MB) dos 264 arquivos originais.
- *Pendrive* formatado com arquivos no total de 578 MB: Não recuperou nenhum arquivo.
- *Pendrive* com arquivos apagados no total 578 Mb: Foram recuperados 223 arquivos (127 Mb) dos 264 arquivos.

- Ferramenta iFile Recovery:

- *Pendrive* com arquivos no total de 1,37 Gb: Foram recuperados 172 arquivos (1,26 Gb) dos 236 arquivos originais.
- *Pendrive* formatado com arquivos no total de 1,37 Gb: Foram recuperados 172 arquivos (1,26 Gb) dos 236 arquivos originais.
- *Pendrive* com arquivos apagados no total de 1,37 Gb: Foram recuperados 172 arquivos (1,26 Gb) dos 236 arquivos originais.
- *Pendrive* com arquivos no total de 578 Mb: Foram recuperados 379 arquivos (739 MB) dos 264 arquivos originais.
- *Pendrive* formatado com arquivos no total de 578 MB: Foram recuperados 267 arquivos (594 Mb) dos 264 arquivos originais, sendo que Foi recuperado a ferramenta foi capaz de recuperar alguns arquivos que não estavam visíveis ou que foram apagados.
- *Pendrive* com arquivos apagados no total de 578 Mb: Foram recuperados 267 arquivos (594 Mb) dos 264 arquivos originais, onde a ferramenta apresentou uma capacidade de recuperar arquivos que foram apagados.

- Ferramenta Pandora:

- *Pendrive* com arquivos no total de 1,37 Gb: Não foi recuperado nenhum arquivo.

- *Pendrive* formatado com arquivos no total de 1,37 Gb: Foram recuperados todos os 236 arquivos (1,37 Gb).
- *Pendrive* com arquivos apagados no total de 1,37 Gb: Foram recuperados 225 arquivos (1,33 Gb) dos 236 arquivos originais.
- *Pendrive* com arquivos no total de 578 Mb: Não foi recuperado nenhum arquivo.
- *Pendrive* formatado com arquivos no total de 578 MB: Foram recuperados 260 arquivos (573 Mb) dos 264 arquivos originais.
- *Pendrive* com arquivos apagados no total de 578 Mb: Foram recuperados 260 arquivos (573 Mb) dos 264 arquivos originais.

- Ferramenta Recuva:

- *Pendrive* com arquivos no total de 1,37 Gb: Foram recuperados 224 arquivos (1,24 Gb) dos 236 arquivos (1,37 Gb).
- *Pendrive* formatado com arquivos no total de 1,37 Gb: Foram recuperados 366 arquivos (2,25 Gb) dos arquivos originais, sendo que a ferramenta foi capaz de recuperar arquivos que não era possível de visualizar.
- *Pendrive* com arquivos apagados no total de 1,37 Gb: Foram recuperados 199 arquivos (1,33 Gb) dos 236 arquivos originais.
- *Pendrive* com arquivos no total de 578 Mb: Foram recuperados 114 arquivos (366 Mb) dos 264 arquivos originais, sendo que 93 foram recuperados totalmente e 21 recuperados parcialmente.
- *Pendrive* formatado com arquivos no total de 578 MB: Foram recuperados 753 arquivos (1,64 Gb) dos 264 arquivos originais, sendo que a ferramenta recuperou arquivos que estavam apagados.
- *Pendrive* com arquivos apagados no total de 578 Mb: Foram recuperados 264 arquivos (573 Mb) dos 264 arquivos originais, sendo que 45 arquivos foram recuperados totalmente e 219 recuperados parcialmente.

- Ferramenta TestDisk:

- *Pendrive* com arquivos no total de 1,37 Gb: Foram recuperados os 236 arquivos (1,37 Gb).
- *Pendrive* formatado com arquivos no total de 1,37 Gb: Não foi recuperado nenhum arquivo.
- *Pendrive* com arquivos apagados no total de 1,37 Gb: Foram recuperados os 236 arquivos (1,37 Gb).

- *Pendrive* com arquivos no total de 578 Mb: Foram recuperados 417 arquivos (941 Mb) dos 264 arquivos originais, sendo que a ferramenta recuperou arquivos além dos que já existiam no *pendrive*.
- *Pendrive* formatado com arquivos no total de 578 MB: Não foi recuperado nenhum arquivo.
- *Pendrive* com arquivos apagados no total de 578 Mb: Foram recuperados os 236 arquivos (1,37 Gb).

3.2. Análise das Ferramentas

Durante a análise das ferramentas bons resultados foram obtidos, pois a maioria dos arquivos que foram recuperados apresentaram um excelente estado de funcionamento e os demais arquivos permaneceram corrompidos. Outro fator importante é que elas foram capazes de recuperar arquivos de qualquer extensão e de qualquer tamanho. Através disso, cálculos foram realizados utilizando a quantidade de arquivos recuperados em cada estado em que o *pendrive* foi testado, e com base nos resultados uma porcentagem foi obtida de acordo para cada critério.

Tabela 1 – Comparação entre as Ferramentas

Critérios / **Ferramentas**	RECUPERA-ÇÃO ARQUIVOS	USABILI-DADE	TEMPO DE RECUPERA-ÇÃO	INTEGRIDADE DOS ARQUIVOS	SISTEMA OPERACIO-NAL	MÉDIA
AUTOPSY	100%	100%	60%	99,9%	100%	91,9%
GLARY UNDELETE	100%	100%	80%	80%	100%	92%
IFILE RECOVERY	100%	100%	100%	100%	100%	100%
PANDORA	100%	100%	93%	98%	100%	98,2%
RECUVA	100%	100%	60%	79%	100%	87,8%
TEST DISK	100%	100%	80%	100%	100%	96%

Portanto, os resultados exibidos na Tabela 1 apresentam que todas as ferramentas tiveram um rendimento de 100% quanto ao funcionamento. Quanto à usabilidade, elas também apresentaram 100% de rendimento. Quanto ao tempo de recuperação dos arquivos,

as ferramentas apresentaram um resultado de 94%, o que demonstra que a maioria dos arquivos foram recuperados. Quanto à integridade dos arquivos, elas apresentaram um resultado superior a 90%, o que demonstra que a maioria deles permaneceram em perfeito estado. Por fim, quanto à portabilidade, todas as ferramentas apresentaram 100% de funcionamento nos respectivos sistemas operacionais.

Posteriormente, gráficos são apresentados exibindo os resultados da análise das ferramentas em cada critério, sendo que em cada gráfico os respectivos números se referem a: 0%, 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, 100%.

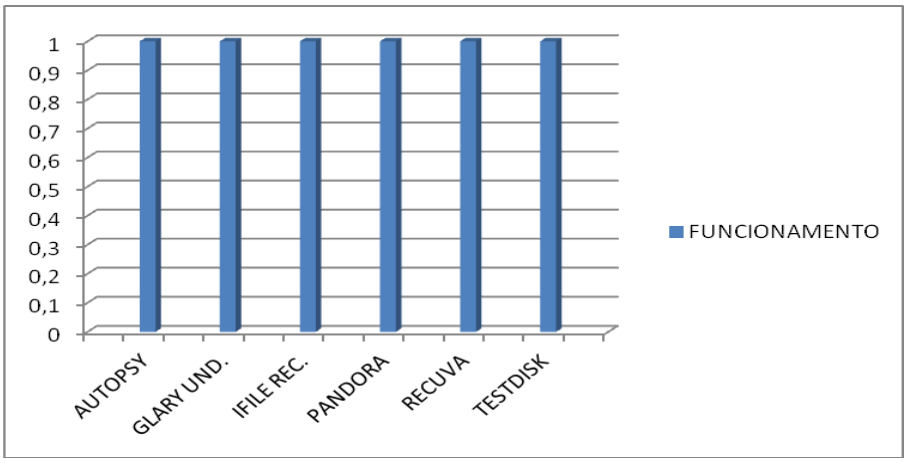

Figura 2 – Critério Funcionamento

De acordo com o Gráfico 2, conclui-se que todas as ferramentas apresentaram 100% no quesito funcionamento, sendo que todos os arquivos que foram recuperados apresentaram um ótimo estado de funcionamento. Portanto, todas as ferramentas são altamente capazes de recuperar arquivos de diversas extensões e com diversos tamanhos.

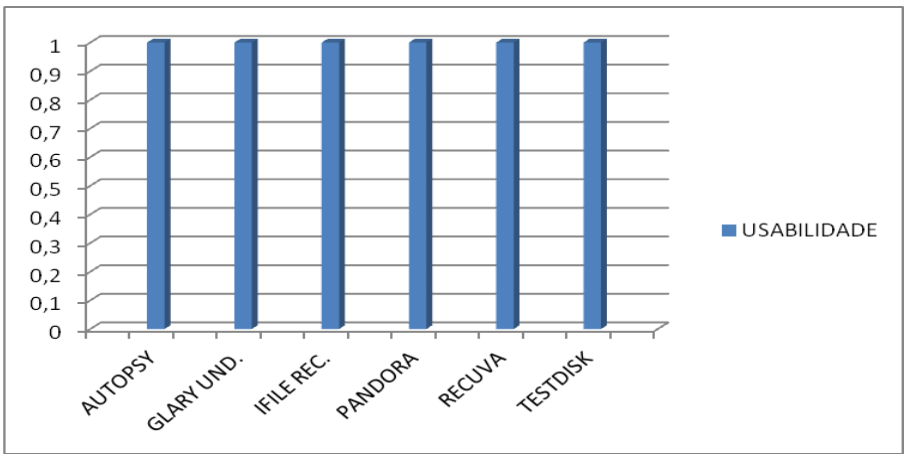

Figura 3 – Critério Usabilidade

De acordo com o Gráfico 3, os resultados apresentados demonstram que todas as ferramentas também obtiveram 100% no quesito usabilidade, sendo que todas possuem uma interface amigável a tornando muito bem explicativa, de fácil entendimento e utilização. Portanto, conclui-se que todas elas oferecem diversas funcionalidades compreensíveis e através disso, torna-se possível o usuário interagir mais facilmente com elas.

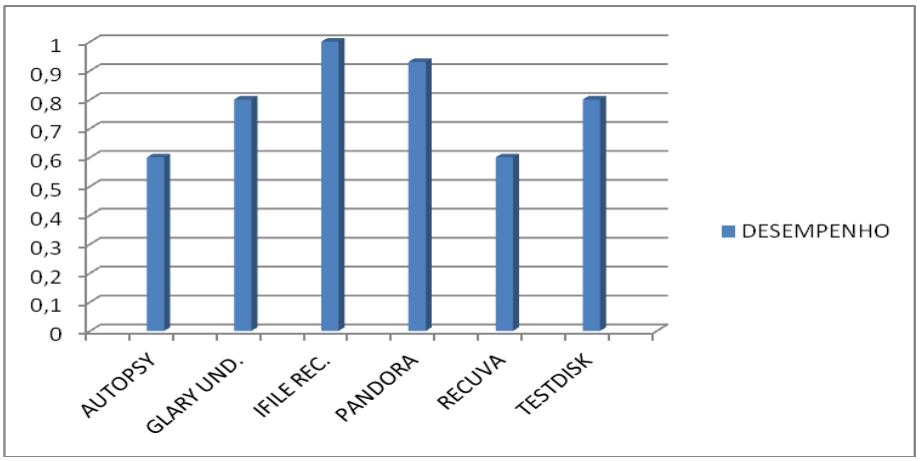

Figura 4 – Critério Desempenho

De acordo com o Gráfico 4, a ferramenta que obteve o melhor desempenho ao recuperar os arquivos em um prazo de cinco minutos foi a iFile Recovery com 100%. Portanto, as demais ferramentas mantiveram uma média superior a 50% no quesito desempenho, o que demonstra a capacidade de recuperar arquivos em um pequeno tempo.

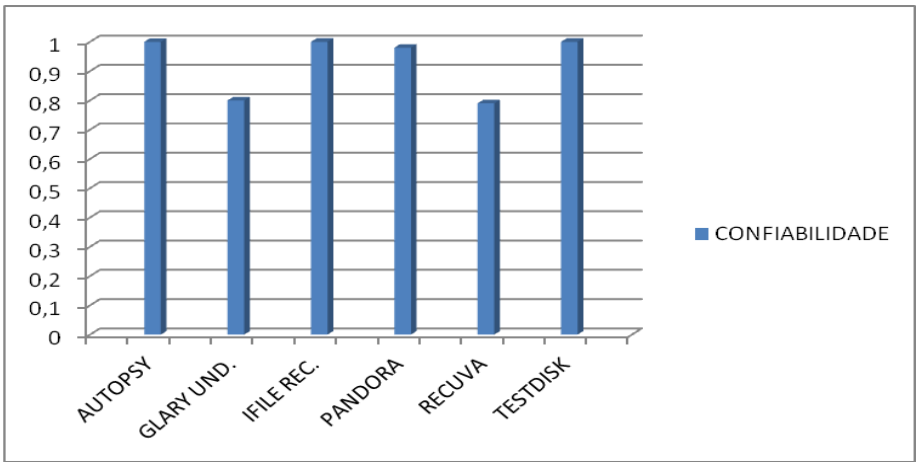

Figura 5 – Critério Confiabilidade

De acordo com o Gráfico 5, todas as ferramentas apresentaram bons resultados quanto a confiabilidade, sendo que os arquivos que foram recuperados em cada uma das ferramentas, apresentaram um ótimo estado de utilização. Portanto, as ferramentas que se apresentaram mais confiáveis foram a Autopsy, iFile Recovery e a TestDisk. Portanto, todas as ferramentas mantiveram uma média superior a 70%.

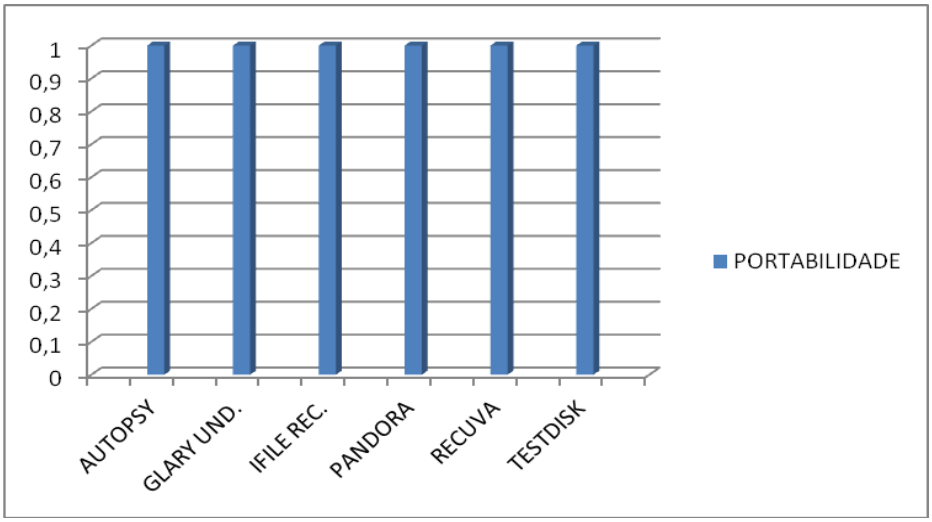

Figura 6 – Critério Portabilidade

De acordo com o Gráfico 6, conluí-se que todas as ferrmentas se portaram muito bem diante dos respectivos sistemas operacionais em que eram portáveis, apresentando assim 100% de aproveitamento. Portanto, todas funcionaram muito bem sendo que em momento algum qualquer erro ocorreu devido ao sistema operacional.

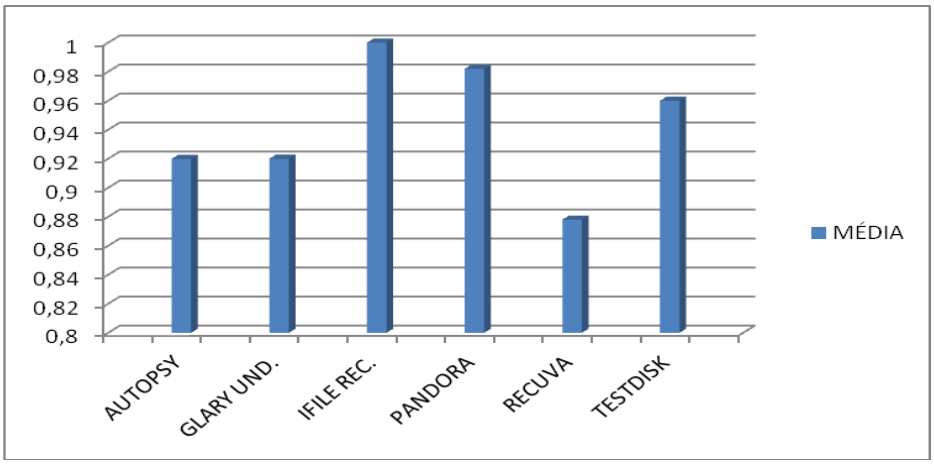

Figura 7 – Média entre as Ferramentas

No Gráfico 7 é apresentado o resultado geral entre as ferramentas baseando-se nos resultados dos gráficos anteriores. Para chegar ao resultado final para cada ferramenta, foi desenvolvido um cálculo sendo que em cada critério elas obtiveram uma porcentagem como resultado. Assim, as porcentagens obtidas em cada ferramenta foram somadas e no final essa soma foi divida pela quantidade de critérios. Portanto, baseando-se nesse cálculo, a ferramenta que obteve a melhor porcentagem sendo de 100% em todos os critérios, foi a iFile Recovery. A segunda melhor ferramenta foi a Pandora, atingindo assim uma porcentagem de 98%. Além dessas, outra ferramenta que apresentou bons resultados e obteve uma porcentagem de 96% foi a TestDisk. Por fim, as demais ferramentas como Autopsy, Glary Undelete e Recuva, obtiveram uma porcentagem abaixo de 92% pelo fato de não terem apresentado resultados tão concisos quanto às demais.

4. CONCLUSÃO

As ferramentas testadas nesse trabalho apresentaram um ótimo funcionamento, foram fáceis de utilizar, apresentaram um ótimo desempenho, sendo que os arquivos recuperados apresentaram um excelente estado e por fim funcionaram muito bem em cada sistema operacional em que eram portáveis.

Assim, a partir das informações obtidas durante a análise das ferramentas e a partir dos dados inseridos na Tabela 1, conclui-se que a melhor ferramenta para recuperar arquivos no sistema Windows foi a iFile Recovery, sendo que em todos os critérios ela apresentou um resultado com 100% de aproveitamento. Já a ferramenta que melhor atendeu no sistema GNU/Linux foi a TestDisk onde apresentou 100% de aproveitamento no funcionamento e na usabilidade, 80% no tempo de recuperação dos arquivos e 100% quanto a integridade dos mesmos e quanto a portabilidade no sistema operacional GNU/Linux.

Concluindo, todo esse trabalho que foi desenvolvido pode servir futuramente como uma base para que novos estudos venham a ser realizados a fim de buscar novas informações sobre as ferramentas, testando-as de maneiras diferentes utilizando diversos dispositivos computacionais a fim de obter novos resultados e reforçar cada vez mais o grau de importância delas na área forense.

REFERÊNCIAS

ARGOLO, Frederico Henrique Bohm. **Análise Forense em sistemas GNU/Linux.** UFRJ. Abril. 2005.

ASSUMPÇÃO, Marcelo. **Ferramentas: FTK 3.0.** Disponível em: <http://direitobitebyte.blogspot.com.br/2010/12/ferramentas-ftk-30.html>. Dezembro.2010.

AUTOPSY. **Autopsy Forensic Browser.** Disponível em: < https://sites.google.com/a/cristiantm.com.br/forense/ferramentas/autopsy-forensic-browser > Data de Acesso: 1 de setembro.2012

ENCASE. **Encase.** Disponível em: <http://www.gta.ufrj.br/grad/07_1/forense/encase.html>. Data de Acesso: 2 de setembro. 2012.

FDTK. **Forense Digital Toolkit (FDTK).** Disponível em: <https://sites.google.com/a/cristiantm.com.br/forense/ferramentas/livecd/forense-digital-toolkit-fdtk /> Data de Acesso: 2 de setembro. 2012.

FDTKa. **FDTK-UbuntuBr – Forense Digital Toolkit.** Disponível em: <http://fdtk.com.br/www/sobre/ >. Data de Acesso: 2 de setembro. 2012.

FORENSIX. **Forensix.** Disponível em: <http://www.gta.ufrj.br/grad/07_1/forense/forensix.html>. Data de Acesso: 3 de setembro. 2012.

GLARY UNDELETE. **Glary Undelete.** Disponível em: <https://www.glarysoft.com/glary-undelete/>. Data de acesso: 21 de novembro.2012.

GUIMARÃES, José Augusto Chaves. NETO, Mário Furlaneto. **Crimes na Internet: elementos para uma reflexão sobre a ética informacional.** Brasília. Jan/Mar. 2003.

GOLDMAN, Alfredo. **Artigo sobre Computação Forense.** Universidade de São Paulo. Instituto de Matemática e Estatística. Disponível em:

<http://grenoble.ime.usp.br/~gold/cursos/2008/movel/gradSemCorrecao/FelipeBulleC.pdf> Novembro. 2010. Data de acesso: 8 de maio. 2012.

HARDWARE. **VFAT.** Disponível em: <http://www.hardware.com.br/termos/vfat>. Junho. 2005.

iFILERECOVERY. **iFILE RECOVERY.** Disponível em: <http://www.ifilerecovery.com/>. Data de acesso: 21 de novembto.2012.

INFOWESTERa. **Características e funcionamento dos HDs (discos rígidos).** Disponível em: < http://www.infowester.com/hd.php >. Maio. 2007. Data de acesso: 20 de abril. 2012.

INFOWESTERb. **Introdução ao sistema de arquivos ReiserFS.** Disponível em: <http://www.infowester.com/reiserfs.php>. Maio. 2007. Data de acesso: 17 de junho. 2012.

INFOWESTERc. **Sistema de arquivos ext3.** Disponível em: <http://www.infowester.com/linext3.php>. Setembro. 2003. Data de acesso: 17 de junho. 2012.

INFOWESTERd. **Sistemas de arquivos FAT16 e FAT32.** Disponível em: <http://www.infowester.com/fat.php>. Julho. 2003. Data de acesso: 17 de junho. 2012.

INFOWESTERe. **Sistema de arquivos NTFS.** Disponível em: <http://www.infowester.com/ntfs.php >. Abril. 2011. Data de acesso: 17 de junho. 2012.

ISO 9126. **Normas de Qualidade de Software.** Disponível em: <www.iso.org/>. 1996.

KERNEL. **The Linux Kernel Archives.** Disponível em: <http://kernel.org/pub/linux/kernel/v3.0/linux-3.7-rc6.tar.bz2>. Junho. 2012. Data de acesso: 20 de junho. 2012.

MICROSOFT. **Descrição do Sistema de Arquivos FAT32.** Disponível em: <http://support.microsoft.com/kb/154997/pt-br>. Agosto. 2006.

MICROSOFTa. **Tamanho máximo da partição usando o sistema de arquivo FAT16.** Disponível em: <http://support.microsoft.com/kb/118335/pt-br>. Data de acesso: 21 de novembro. 2012.

MICROSOFTb. **Comparando sistemas de arquivos NTFS e FAT.** Disponível em: <http://windows.microsoft.com/pt-BR/windows-vista/Comparing-NTFS-and-FAT-file-systems>. Data de acesso: 21 de novembro de 2012.

MOTTAa, Sérgio. **Recupere arquivos apagados acidentalmente com o Glary Undelete.** Disponível em: < http://www.softdownload.com.br/recupere-arquivos-apagados-glary-undelete.html >. 20 de março. 2009.

MOTTAb, Sérgio. **Recupere arquivos deletados com o iFileRecovery.** Disponível em: < http://www.softdownload.com.br/recupere-arquivos-deletados-ifilerecovery.html >. 20 de março. 2009.

MOTTAc, Sérgio. **Recupere arquivos com o Recuva.** Disponível em: < http://www.softdownload.com.br/recupere-arquivos-apagados-com-o-recuva.html >. 20 de março. 2009.

MOTTAd, Sérgio. **Recupere arquivos apagados com o Pandora Recovery.** Disponível em: < http://www.softdownload.com.br/recupere-arquivos-deletados-pandora-recovery.html >. 20 de março. 2009.

NASCIMENTO, Joscilene dos Santos. **Análise de Ferramentas Forenses de Recuperação de Dados.** Faculdade de Tecnologia de João Pessoa – PB. 2010.

OLIVEIRA, Rômulo Silva de. CARISSIMI, Alexandre da Silva. TOSCANI, Simão Sirineo. **Sistemas Operacionais**. Fevereiro 2003. 2ª edição.

PANDORA. **Pandora.** Disponível em: <http://www.pandorarecovery.com/>. Data de acesso: 21 de novembro. 2012.

RECUVA. **Recuva.** Disponível em: <http://www.piriform.com/recuva>. Data de acesso: 21 de novembro. 2012.

REIS, Marcelo Abdalla dos. **Análise de Intrusões em Sistemas Computacionais: Técnicas, Procedimentos e Ferramentas.** UNICAMP. 2002.

RODRIGUES, Thalita Char; FOLTRAM JR, Dierone César. **Análise de Ferramentas Forenses na Investigação Digital.** V.2, Nº.3, Dez/2010.

TANEMBAUM, Andrew Stuart. **Sistemas Operacionais Modernos.** 3º edição. 2010.

TAVARES, Diego. **Forense Computacional.** Novembro. 2007. PET-Computação.

TESTDISK. **TestDisk, Recuperação de Dados.** Disponível em: <http://www.cgsecurity.org/wiki/TestDisk >. Data de acesso: 21 de novembro. 2012.

VIOTTI, Alberto Luiz Alves. **Possibilidade do uso de software livre como ferramentas de análise em investigações digitais.** Disponível em: <http://pt.scribd.com/doc/46446302/24/Tabela-7-%E2%80%93-Ferramentas-do-The-Sleuth-Kit-para-sistema-de-arquivos%E2%80%93-TSK>. Data de Acesso: 1 de setembro. 2012.

VIVAAOLINUXa. **Sistema de arquivos ext4.** Disponível em: <http://www.vivaolinux.com.br/artigo/Sistemas-de-arquivos-para-GNU-Linux?pagina=4>. Junho. 2012. Data de acesso: 24 de junho. 2012.

VIVAAOLINUXb. **Sistema de arquivos JFS.** Disponível em: <http://www.vivaolinux.com.br/artigo/Sistemas-de-arquivos-para-GNU-Linux?pagina=7>. Junho. 2012. Data de acesso: 24 de junho. 2012.

VIVAAOLINUXc. **Sistemas de arquivos suportados pelo Linux.** Disponível em: < http://www.vivaolinux.com.br/artigo/Linux-Sistema-de-arquivos/>. Novembro. 2006. Data de acesso: 24 de junho. 2012.