UNIVERSIDADE SAGRADO CORAÇÃO

VICTOR SAQUETO KAMIYA

PERÍCIA FORENSE COMPUTACIONAL APLICADA A COMPUTADORES E SMARTPHONES IOS E ANDROID

BAURU
2014

VICTOR SAQUETO KAMIYA

PERÍCIA FORENSE COMPUTACIONAL APLICADA A COMPUTADORES E SMARTPHONES IOS E ANDROID

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Dr. Elvio Gilberto da Silva.

BAURU
2014

VICTOR SAQUETO KAMIYA

PERÍCIA FORENSE COMPUTACIONAL APLICADA A COMPUTADORES E SMARTPHONES IOS E ANDROID

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação, sob a orientação do Prof. Dr. Elvio Gilberto da Silva.

Banca examinadora:

_____

Prof. Dr. Elvio Gilberto da Silva
Universidade Sagrado Coração

_____

Prof. Me. Patrick Pedreira Silva
Universidade Sagrado Coração

_____

Prof. Me. Henrique Pachioni Martins
Universidade Sagrado Coração

Bauru, 09 de dezembro de 2014.

RESUMO

Com o desenvolvimento da tecnologia, as pessoas estão cada vez mais dependentes de aparelhos eletrônicos, seja por lazer ou para trabalho. Mas junto com a tecnologia também apareceram novos problemas, como usuários mal intencionados, crimes virtuais, roubo e até perda de dados. Graças ao avanço da tecnologia e da internet e a dependência das pessoas por aparelhos eletrônicos, é muito importante a segurança da informação e a perícia forense, que tem o objetivo de proteger dados importantes e resolver crimes virtuais. Com base nesse contexto, este trabalho analisou e comparou vários softwares de recuperação de dados que podem ser importantes tanto em ajudar a uma investigação criminal quanto a ajudar usuários que perderam dados importantes.

ABSTRACT

Withe the develepment of technology, people are increasingly dependent on electronic devices, either for fun or work. But together with the technology new problems such as malicious users, virtual crimes, theft and even data loss also appeared.Thanks to the develepment of technology and the internet and people's dependence for electronics, the security information and forensics are very important as their obejective is to protect important data and resolve cybercrime. With this context, this paper analyzed and compared various data recovery software that can be important both to help a criminal investigation as to help users who have lost important data.

LISTA DE ILUSTRAÇÕES

Figura 1.....13
Figura 2.....15
Figura 3.....23
Figura 4.....25
Figura 5.....27
Figura 6.....28
Figura 7.....29
Figura 8.....29
Figura 9.....30
Figura 10.....31
Figura 11.....32
Figura 12.....33
Frgura 13.....33
Figura 14.....34
Figura 15.....35
Figura 16.....36
Figura 17.....37
Figura 18.....38
Figura 19.....39
Figura 20.....40
Figura 21.....41
Figura 22.....42
Figura 23.....42
Figura 24.....43
Figura 25.....43
Figura 26.....44
Figura 27.....44
Figura 28.....45
Figura 29.....45
Figura 30.....45
Figura 31.....45
Figura 32.....46

Figura 33.....46
Figura 34.....47
Figura 35.....47
Figura 36.....48
Figura 37.....48
Figura 38.....49
Figura 39.....49
Figura 40.....50
Figura 41.....50

SUMÁRIO

1.1 OBJETIVOS.....9

1.1.1 OBJETIVO GERAL.....9

1.1.2 OBJETIVOS ESPECÍFICOS.....9

1.2 ORGANIZAÇÃO DO TRABALHO.....10

2 REVISÃO DA LITERATURA.....11

2.1 HISTÓRICO DOS CELULARES.....11

2.2 SISTEMA OPERACIONAL ANDROID.....11

2.3 SISTEMA OPERACIONAL IOS.....12

2.4 ANDROID CONTRA IOS.....13

2.6 SISTEMA OPERACIONAL WINDOWS.....14

2.7 SISTEMA OPERACIONAL LINUX.....15

2.8 CRIMES COMPUTACIONAIS.....16

2.9 CRIPTOGRAFIA.....17

2.10 ESTEGANOGRAFIA.....18

2.11 COMPUTAÇÃO FORENSE.....18

2.12 REMO RECOVER.....19

2.13 UNDELETE PLUS.....19

2.14 TESTDISK.....20

2.15 WONDERSHARE DR.FONE.....20

2.16 EASEUS DATA RECOVERY WIZARD 20

2.17 FOREMOST 21

3 TRABALHOS CORRELATOS.....22

4 METODOLOGIA 24

5 TESTES FEITOS PARA RECUPERAÇÃO DE DADOS.....27

6 RESULTADOS OBTIDOS 41

7 CONCLUSÃO 52

REFERENCIAS.....53

APÊNDICE B – TABELAS DE RECUPERAÇÃO DE ARQUIVOS EM CADA SISTEMA OPERACIONAL UTILIZADO.....57

APÊNDICE C – TABELA DE RECUPERAÇÃO DE ARQUIVOS EM PLATAFORMA POR SOFTWARE 58

1 INTRODUÇÃO

A primeira geração de computadores modernos surgiu em 1946, nessa época os computadores eram enormes e tinham como principal característica, o uso de válvulas eletrônicas, e todos os programas eram escritos diretamente na linguagem de máquina. (GUGIK, 2009).

Ainda nessa época, surgiram as primeiras ideias para criar um sistema capaz de efetuar comunicações entre telefones sem fio, mas só em 1973 é que foi apresentado ao mundo o primeiro aparelho funcionando, e em 1983 foram liberados ao público os primeiros modelos de celulares, pesando em média 1 quilo e com aproximadamente 30 centímetros de altura. (JORDÃO, 2009).

Desde então a tecnologia evoluiu muito, computadores não necessitam de válvulas para serem operados e, assim, como celulares são infinitamente mais potentes e seu tamanho diminuiu tanto que chegamos ao ponto de conseguir carregá-los no bolso.Hoje em dia é possível realizar uma ligação dizendo ao *smartphone* o nome da pessoa com quem você deseja falar e até mesmo passear pelas ruas de uma cidade em um país distante facilmente, tudo isso apenas utilizando um computador.

O smartphone é um celular sofisticado, com grande poder computacional e capaz de desempenhar várias funções típicas de um computador. Possui funcionalidades avançadas que podem ser estendidas por meio de programas executados por seu sistema operacional. Os sistemas operacionais dos smartphones permitem que desenvolvedores criem milhares de aplicativos, com várias utilidades. Os telefones celulares estão entre os dispositivos mais populares, sendo os *smartphones* considerados um dos objetos de maior desejo daqueles que gostam de tecnologia. (SIMÃO, 2011 apud AFONSO, 2013).

Com toda essa facilidade, o ser humano passou a depender cada vez mais da tecnologia, escolas, empresas privadas, órgãos do governo, residências, etc. No entanto, toda essa tecnologia também traz grandes perigos, um único problema de ordem técnica é o bastante para arruinar completamente uma instituição.

Segundo Afonso (2013), uma das ameaças que podem colocar em risco a segurança da informação, seja por falha humana ou técnica, é a perda de dados, que pode levar a consequências catastróficas, além disso, outro risco vem por meio de usuários mal intencionados que tem o objetivo de roubar esses dados. Com a

expansão da Internet, computadores e outros dispositivos eletrônicos estão sendo usados para cometer crimes digitais. E-mails que tentam ludibriar o usuário e fazer com que as vítimas instalem um programa em seu computador que será usado para obter seus dados é apenas um exemplo básico de uma das técnicas que são usadas para roubar dados desejados. Com isso, o uso de provas eletrônicas está cada vez mais envolvido em crimes digitais.

A Perícia Forense na área computacional é uma área relativamente nova que está se desenvolvendo rapidamente graças à necessidade de instituições estarem atuando no combate aos crimes eletrônicos e inclui como alguns de seus objetivos a análise de mídias, como, HDs, discos ópticos, pendrives, discos SSD, memória RAM etc. Buscando qualquer conteúdo que possa ser associado a algum tipo de crime digital, tal procedimento utiliza hardware e software específicos, que conseguem acessar sem modificar ou alterar os arquivos armazenados nessas mídias, na procura de evidências para esclarecer um crime digital, podendo ser um roubo, troca de mensagens, alteração de arquivos, cópia não autorizadas de informações sigilosas, compartilhamento de arquivos proibidos, entre outros. (AFONSO, 2013).

O processo de coleta de evidências é regido por leis, toda a evidência deve ser autenticada, ou seja, é preciso que uma testemunha comprove que a prova seja real, mas também existem as evidências as quais não necessitam de testemunho como documentos públicos e publicações oficiais. (SHINDER, 2002 apud COSTA, 2008).

> Para realizar a análise e coleta de evidências são seguidos procedimentos rígidos para que não exista nenhuma irregularidade durante a investigação do fato, o que pode fazer com que o juiz considere a prova inadmissível. (COSTA, 2008).

Os primeiros a chegar à cena do crime devem tomar algumas precauções como não desligar equipamentos, já que os suspeitos podem utilizar mecanismos para destruir provas, e nem modificar nada, para não tornar possíveis provas inválidas e garantir a integridade das evidências, caso a pessoa não seja treinada em forense computacional. (SHINDER, 2002 apud COSTA, 2008).

Este tema foi escolhido com o intuito de fomentar pesquisas sobre técnicas de perícia forense, as quais são utilizadas pelos profissionais da área. Este é um

assunto muito importante, pois essas ferramentas podem ser a chave para recuperar evidencias de computadores e smartphones de suspeitos.

Com base neste contexto, este estudo tem por finalidade realizar um comparativo entre as ferramentas utilizadas na recuperação de arquivos de computadores e celulares smartphones, resultando na confecção de um relatório com informações sobre as características dos softwares analisados, bem como sua eficiência na recuperação de informações.

1.1 OBJETIVOS

Apresenta-se nas seções seguintes o objetivo geral e os objetivos específicos da pesquisa.

1.1.1 Objetivo geral

Analisar softwares de perícia forense computacional, visando auxiliar o usuário na escolha da ferramenta mais adequada para a recuperação de arquivos deletados em dispositivos de armazenamento que trabalhem com Windows ou Linux e smartphones que utilizem os sistemas operacionais iOS ou Android.

1.1.2 Objetivos específicos

a) Pesquisar softwares específicos de recuperação de dados;
b) Estudar técnicas forenses de recuperação de dados;
c) Levantar estratégias para análise pericial em smartphones com sistemas operacionais IOS e Android;
d) Realizar a recuperação de dados em dispositivos móveis que possuam o sistema operacionail *e* Android, bem como, em dispositivos de armazenamento que possuam os sistemas operacionais Windows ou Linux;
e) Coletar resultados e analisá-los a fim de elaborar uma comparação vertical e horizontal entre as plataformas e softwares utilizados, demonstrando quais apresentam maior capacidade de recuperação e qualidade.

1.2ORGANIZAÇÃO DO TRABALHO

O Capítulo 1 apresenta a Introdução do trabalho e da organização do mesmo visando esclarecer a finalidade deste trabalho. No capítulo 2 é possível observar a Revisão da Literatura, onde são abordados tópicos como: A história dos celulares, os sistemas operacionais que foram utilizados como objeto de investigação, e por fim, sobre pericia forense.

Já no capítulo 3 são exibidos trabalhos correlatos enquanto no capítulo 4 encontra-se a metodologia utilizada.

No capítulo 5 são exibidos os testes feitos para recuperação de dados, o capítulo 6 apresenta resultados obtidos com os testes e, então, no capítulo 7 são apresentadas as considerações finais. E para fechar o trabalho, são apresentadas as Referências Bibliográficas consultadas.

2 REVISÃO DA LITERATURA

2.1 HISTÓRICO DOS CELULARES

A idéia do celular surgiu em 1947, mas com a tecnologia da época, não era possível desenvolver um aparelho, só em 1973 foi criado um protótipo e foi feita a primeira ligação de um telefone móvel apara um telefone fixo. (JORDÃO, 2009).

Os primeiros aparelhos disponíveis a comercialização apareceram só em 1983, dez anos após o primeiro teste realizado. Nessa época, os aparelhos mediam cerca de 30 centímetros e pesavam em torno de 1 quilo, além de terem preços muito altos. (RENATO, 2012).

Os aparelhos começaram a evoluir ano após ano, em 1993 surgiram os celulares que podiam mandar mensagens, o famoso SMS (short message service*)*, e com o tempo depois surgiram os celulares com cores, ganharam a possibilidade de se conectar a internet, câmeras para tirar fotos e vídeos, e finalmente evoluíram para os smatphones que usamos atualmente, esses aparelhos se diferenciam de celulares comuns pelo fato de terem um sistema operacional instalado neles, tornando o aparelho muito mais potente e útil. (JORDÃO, 2009).

2.2 SISTEMA OPERACIONAL ANDROID

O Android é um sistema operacional criado inicialmente pela Android Inc., como um sistema operacional baseado em Linux e projetado para dispositivos móveis.

Ainda em 2005, a Google comprou os direitos do sistema operacional e em 2007, junto com a fundação OpenHandset Alliance, o Android foi lançado no mercado. A OpenHandset Alliance é um consórcio de hardware, software, telecomunicações e empresas dedicadas ao avanço aberto de normas para dispositivos móveis, que tem como participantes as empresas Google, Dell, Intel, Motorola, entre outras.

O Android também é famoso pelo seu SDK (Software Development Kit*)* que permite que desenvolvedores criem os mais variados tipos de aplicativos para a plataforma. (AFONSO, 2013).

Ao mesmo tempo em que é uma vantagem, a facilidade para se desenvolver aplicativos para a plataforma, também torna a mesma um pouco mais perigosa, pois existe uma maior chance de se obter malwares desenvolvidos por pessoas mal intencionadas.

Curiosamente, todas as versões desse sistema operacional tiveram o nome de alguma comida, sendo: Android 1.0 (Astro), Android 1.5 (Cupcake), Android 1.6 (Donut), Android 2.0 e 2.1 (Eclair), Android 2.2 (Froyo), Android 2.3 (Gingerbread), Android 3.0 (Honeycomb), Android 4.0 (IcecreamSandwich), Androids 4.1, 4.2 e 4.3 (JellyBean),Android 4.4 (KitKat)(Barros, 2013),e finalmente a versão mais atual, Android 5.0 (Lollipop).

2.3 SISTEMA OPERACIONAL IOS

O sistema operacional iOS foi criado pela Apple em 2007, sendo desenvolvido inicialmente para iPhones, mas atualmente todos os aparelhos da Apple utilizam esse sistema. A Apple pode ser considerada uma das empresas mais inovadoras do mundo, talvez por isso ela possua um dos sistemas operacionais para dispositivos móveis considerado um dos mais eficientes, o iOS. Inicialmente chamado de “iPhone OS”, era um sistema quase inteiramente bloqueado para desenvolvedores e hackers e até hoje, não é possível executar o iOS em *hardware* de terceiros, para competir com seus concorrentes a Apple decidiu focar seus esforços no funcionamento e consistência do dispositivo, e começou a adicionar novos recursos com atualizações do sistema operacional.

De acordo com Jamil (2014):

> Seja no iPhone ou iPad, o iOs é considerado um dos sistemas operacionais mais intuitivos e fáceis de ser trabalhar. Isso porque a sua interface amigável e totalmente voltada para dispositivos móveis facilita a vida de quem o utiliza.

A Apple evoluiu ano após ano seu sistema operacional, e em julho de 2008 foi lançado o “iPhone OS 2”, juntamente com uma novidade, a Apple Store, que é uma loja online onde os usuários podem navegar facilmente, baixar e comprar aplicativos e músicas, e ver anúncios sobre novos produtos. Junto com o sistema operacional, a Apple lançou também seu kit de desenvolvimento, que oferece ferramentas para

seus desenvolvedores. Um ano depois, em junho de 2009 o “iPhone OS 3” veio ao mundo trazendo vários novos recursos que ainda faltavam no IOS. (TROYACK; YANG, 2013).

Em 2010 o “iPhone OS” passou a se chamar simplesmente “iOS” junto com sua quarta versão, nessa época, o sistema da Apple já era conhecido por bastante seguro em relação à malwares e outros tipos de ameaças, pois todo aplicativo desenvolvido, tinha que ser aprovado pela empresa antes de ser disponibilizado na Apple Store.

Nos anos de 2011, 2012 e 2013 foram lançados respectivamente os iOS 5, 6 e 7, todos apresentando características novas e recursos muito interessantes como a Siri, por exemplo, que é um aplicativo que permite o usuário fazer varias tarefas por simples comandos de voz. (TROYACK; YANG, 2013). A versão mais atual do IOS hoje é o iOS 8.1.1. A Figura 1 ilustra a evolução da tela inicial de cada uma das versões do iOS até a versão 7.

Figura 1 - Evolução da tela inicial do iOS.

Fonte: Tryack e Yung (2013).

2.4 ANDROID CONTRA IOS

Esses sistemas operacionais rivais têm vários pontos fortes e fracos, mas neste trabalho, será focada somente a parte de segurança.

Em questão de segurança, o iOS sai na frente, pois o rígido sistema de avaliação de aplicativos e o próprio sistema operacional desenvolvidos pela Apple impedem que muitos malwares cheguem a se espalhar entre os usuários, enquanto que usuários de Android tem que se preocupar mais, já que é muito mais fácil desenvolver aplicativos para o Android e consequentemente desenvolver malwares para a plataforma também.

> Quando olhamos apenas para as tendências de malware, a suposição fácil pode ser de que o sistema iOS é a plataforma mais segura. Um relatório do Departamento de Segurança Interna do Departamento de Justiça dos EUA, publicado no ano passado dos EUA, descobriu que apenas 0,7% de todo o malware móvel tem os dispositivos iOS como alvo, em comparação com os 79% dirigidos aos dispositivos Android. (HULME, 2014).

Se por um lado a liberdade que se tem com o Android traz riscos, por outro lado abre mais possibilidades, ao contrário do iOS que só pode ser executado em aparelhos da Apple, o Android é utilizado em vários aparelhos de terceiros, como Motorola, Samsung, entre outras. (BARROS, 2011).

2.6 SISTEMA OPERACIONAL WINDOWS

O Windows é um sistema operacional desenvolvido pela Microsoft lançado em novembro de 1985, na época esse software era uma inovação, pois até então era necessário digitar comandos no MS-DOS, e com o Windows 1.0 foi possível utilizar o mouse para clicar nas “janelas” da interface.

A partir daí, o Windows evoluiu ano após ano, em dezembro de 1987 foi lançado o Windows 2.0, o qual exibia ícones em sua área de trabalho. Em 1990 o Windows 3.0 foi anunciado, e juntamente com o Windows 3.1 vendeu mais de 10 milhões de copias nos 2 primeiros anos. E já em 1995 o Windows 95 foi lançado estabelecendo um recorde de 7 milhões de copias vendidas nas 5 primeiras semanas.

No ano 1998 surgiu o Windows 98, que foi descrito como um sistema operacional “melhor para trabalhar e jogar”. Essa foi a primeira versão do Windows projetada especificamente para os consumidores.

De 2001 a 2013 foram lançados os sistemas operacionais: Windows XP, Windows Vista, Windows 7 e, finalmente, o Windows 8 que atualmente são os sistemas operacionais mais utilizados em computadores pessoais do mundo. A Figura 2 ilustra todos os sistemas operacionais lançados pela empresa Microsoft.

Um fato significativo que aconteceu recentemente foi o término do suporte do Windows XP, que foi lançado em 2002 e, por 12 anos, foi o sistema operacional mais utilizado no mundo, graças ao seu bom desempenho, estabilidade e fácil manuseio.

Figura 2 - Sistemas operacionais lançados pela MICROSOFT.

16 Bits	**Família NT**	**64 *Bits***
• Windows 1.0 • Windows 2.0 • Windows 3.xx	• Windows NT • Windows 2000 • Windows Neptune • Windows Odyssey	• Windows Server 2008 R2 • Windows Server 2012
32 Bits	***32 e 64 Bits***	***Versões sistemas embarcados***
• Família 9x • Windows 95 • Windows 98 • Windows 98 SE • Windows ME	• Windows XP • Windows Server 2003 • Windows Vista • Windows Server 2008 • Windows 7 • Windows8	• Windows CE • Windows Mobile • Windows Phone

Fonte: Afonso (2013, p. 23).

Em 8 de Abril de 2014, a Microsoft encerrou o suporte para poder investir seus recursos em tecnologias mais modernas, já que sistemas operacionais melhores e mais modernos como o Windows 8 estão disponíveis no mercado.

2.7 SISTEMA OPERACIONAL LINUX

O nome Linux é originado da junção dos nomes Linus e Unix, sendo Linus Torvalds o criador do famoso Linux, e Unixum sistema operacional voltado para servidores, no qual o Linux foi baseado. (MORIMOTO, 2009 apud AFONSO, 2013).

Em 1991, Linus Torvalds decidiu desenvolver, por hobby, um sistema operacional mais poderoso que o Minix, que era uma versão gratuita do Unix e ainda nesse ano Linus já disponibilizou a versão do Kernel 0.02 (núcleo dos sistemas

operacionais). Linus continuou trabalhando em seu projeto até que em 1994, ele disponibilizou a versão 1.0 do Kernel.

O kernel é a parte mais importante do sistema operacional Linux, ele é como um comunicador entre usuário e maquina, e também é responsável por garantir que todos os programas terão acesso aos recursos de que necessitam simultaneamente, como memória RAM, por exemplo, fazendo com que haja um compartilhamento concorrente sem oferecer riscos à integridade da máquina. (MORIMOTO, 2009apud AFONSO, 2013).

Hoje, a versão mais atual e estável do Kernel é a versão 3.14.2, mas já existem versões mais avançadas disponíveis para download, apesar de não serem versões finalizadas e estáveis.

Ao contrário do Windows que é um sistema fechado, o Linux é gratuito e pode ser modificado por qualquer pessoa, pois está sob a licença GPL, que permite que o sistema seja utilizado e modificado por qualquer um, contanto que não o torne fechado.

2.8 CRIMES COMPUTACIONAIS

Definem-se crimes computacionais, ou crimes eletrônicos, como todas as formas de conduta ilegal realizada utilizando um computador, são crimes como: pirataria de software, roubo de dados, espionagem, exploração de brechas em sistemas de terceiros, pishing, spam,entre outros. (COSTA, 2008).

Muitas pessoas definem erroneamente os usuários mal intencionados como *Hackers,* que na verdade são usuários que usam seus conhecimentos na área de informática para invadir outros sistemas, mas sem roubar nem alterar dados ou causar qualquer tipo de dano ao sistema invadido, só realizam a invasão como forma de provar suas habilidades.

Algumas empresas como a Google, por exemplo, já chegaram a oferecer prêmios em dinheiro para *hackers* que descobrissem falhas em seus sistemas (no caso o Chrome OS) fazendo, assim, que tais falhas fossem corrigidas antes do produto final ser lançado para o público.

Crackers *é* o termo correto para os usuários mal intencionados que usam de seus conhecimentos para invadir outros sistemas e cometer crimes como alterar e roubar dados, prejudicando empresas, governos e qualquer usuário necessário, para

obter o que desejam.Além de disso, existem vários outros termos como phreakers, que são especializados em fraudar sistemas de telefones e celulares, existem também os wannabe, que são indivíduos que se auto intitulam como hackers ou crackers, mas não possuem conhecimento profundo o suficiente e acabam utilizam programas de terceiros para realizar invasões, sabendo apenas como utilizá-los, mas sem conhecer a fundo o funcionamento desses programas. (COSTA, 2008).

Um dos maiores erros que as pessoas podem cometer, é pensar estar segura apenas tomando cuidado com e-mails e sites que podem informações de usuário, pois existe uma técnica que criminosos utilizam que nem se quer é preciso ter conhecimento técnico para obter dados e acesso a áreas restritas, é a Engenharia Social.

A Engenharia Social ficou mais conhecida a partir de 1990 através de Kevin Mitnick, que foi considerado pelos EUA como o crackermais famoso de sua história. A Engenharia Social é a habilidade de conseguir dados protegidos e acesso a áreas restritas através de habilidades de persuasão.

> Algumas empresas escondem as informações sobre o lançamento de alguns de seus produtos dentro de cofres, e não é por mero acaso. A Apple revolucionou o mercado de dispositivos móveis com a chegada do iPhone em 2007 e do iPad em 2010, mas imagine se um engenheiro social tivesse conseguido detalhes do desenho do produto e outra empresa lançasse com alguns meses de antecedência. Para dizer o mínimo, isso poderia alterar radicalmente o mercado como conhecemos hoje. (CIPOLI, 2013).

Essa prática se aproveita da falta de treinamento referente a política de segurança de uma empresa por exemplo, onde as pessoas não tem tanto cuidado com as informações que elas possuem, facilitando assim para que o engenheiro social obtenha o que ele deseja daquela empresa.

2.9 CRIPTOGRAFIA

A criptografia é um conjunto de regras criadas para codificar informações, tornando-as incompreensíveis para aqueles que não são nem o emissor nem receptor da mensagem.

Existem muitas variações dessa técnica, mas basicamente, a criptografia funciona desse modo: a mensagem a ser mandada para o receptor, passa pelo codificador com uma chave simétrica, que é transformada em conjuntos de

caracteres sem sentido algum, e é enviada pela internet para o destinatário. Ao chegar ao receptor, a mensagem passa por uma decodificação com uma chave simétrica, tornando-a legível novamente. (PISA, 2013).

2.10 ESTEGANOGRAFIA

A palavra esteganografia veio do grego e significa “escrita oculta”, é uma técnica utilizada muito antes da invenção dos computadores para esconder informações que se desejava passar secretamente para outra pessoa, utilizando tintas “invisíveis”, ou micropontos, que foi utilizado por vários reis e burgueses no passado. Dentro da computação, a esteganografia é utilizada para esconder informações dentro de outros arquivos como imagens, músicas, vídeos e até textos. (MARTINS, 2010).

Um dos usos para a esteganografia é para colocar marca d’água em imagens por motivos de direitos autorais, além desse, existem vários outros usos para essa técnica, infelizmente nem todos são para fins legítimos.

A esteganografia também pode ser utilizada por criminosos para esconder programas maliciosos em arquivos de músicas ou vídeos por exemplo, para roubar dados de usuários inocentes. (WESTPHAL, 2010).

2.11 COMPUTAÇÃO FORENSE

A computação forense é a técnica de adquirir, preservar, retirar e representar dados que foram processados eletronicamente e armazenados em um computador ou outro dispositivo eletrônico, essa técnica surgiu da necessidade da solução de casos de crimes específicos, que envolvem computadores e a internet. (NOBLETT; POLLITT; PRESLEY, 2000).

Atualmente existem vários exames forenses na área de informática com diferentes objetivos, os principais tipos de exames são os seguintes:

a) Exames e procedimentos em locais de crime de informática: são procedimentos que devem ser seguidos pelos peritos no local do crime para não danificar equipamentos nem modificar ou apagar provas eletrônicas. São procedimentos como: mapeamento, identificação e preservação do material;

b) Exames em dispositivos de armazenamento computacional: são os tipos de exames mais solicitados na computação forense, tratando de analisar arquivos, sistemas e programas instalados em todo tipo de dispositivos de armazenamento eletrônico. Existem quatro fases para esse tipo de exame, que são: preservação, extração, analise e formalização, além de serem utilizadas técnicas para quebra de senhas e recuperação de arquivos apagados;
c) Exames em aparelhos de telefone celular: assim como nos exames já citados, trata-se de um exame para analisar e extrair arquivos de telefones celulares, incluindo mas não limitado a lista de contatos do aparelho;
d) Exames de em sites da internet: são exames feitos visando verificar cópias de conteúdo, conteúdos proibidos e investigação do responsável por um domínio de site ou endereço IP.

2.12 REMO RECOVER

O Remo Recover é um software de recuperação de dados perdidos e apagados do computador, notebook ou qualquer outra mídia de armazenamento.

Este software funciona para as plataformas Windows, iOS e Android, recuperando dados de vídeo, áudio, som, texto, além de ser capaz de recuperar pastas inteiras que foram deletadas.

Além de uma versão grátis que foi utilizada neste trabalho, o programa também possui uma versão paga que dá ao usuário um maior suporte.

2.13 UNDELETE PLUS

O Undelete Plus é um software de recuperação de dados deletados que funciona em dispositivos contendo as plataformas Windows ou Android.

Utilizado para recuperar arquivos de texto, música, vídeo e som, o Undelete Plus também está disponível em duas versões, sendo uma grátis com as funcionalidades básicas e uma paga oferecendo mais opções ao usuário.

2.14 TESTDISK

O TestDisk é um software de recuperação de dados “Open Source” licenciado pela GNU General Puplic License, sendo assim um software totalmente grátis.

Além de recuperar dados de som, vídeo, texto e imagens, ele também pode reparar danos causados ao sistema de boot do computador.

2.15 WONDERSHARE DR.FONE

O Wondershare Dr.Fone é um software de recuperação de dados que funciona em sistemas com a plataforma iOS e Android, mas diferente de outros programas com o mesmo objetivo, o Wondershare Dr.Fone possui uma versão especifica para aparelhos que utilizam iOS e outra versão especifica para aparelhos que utilizam Android, sendo que para este trabalho, foram utilizadas ambas as versões.

Além de arquivos de som, vídeo, imagens e texto, esse programa também recupera mensagens e contatos do smartphone.

Este software é pago, mas é possível usá-lo em uma versão de testes gratuitamente caso o usuário tenha interesse.

2.16 EASEUS DATA RECOVERY WIZARD

O EaseUs Data Recovery Wizard é um software de recuperação de dados que funciona para dispositivos na plataforma Windows, iOS e Android sendo possível resgatar dados de som, vídeo, texto e imagens.

Este é um software pago, mas possui um período de testes que foi utilizado para a realização deste trabalho.

2.17 FOREMOST

O Foremost é um software de recuperação de dados desenvolvido por dois agentes da força aérea dos EUA, Kris Kendall e Jesse Kornblum ediferente dos outros softwares citados até agora, funciona especificamente em Linux.

O programa é inteiramente comandado por comandos por comandos DOS, o que dificulta sua utilização por pessoas com menos conhecimento de informática, mas apesar de tudo, é um ótimo software para recuperação de dados.

3 TRABALHOS CORRELATOS

A Perícia Forense Computacional é uma área que está em constante desenvolvimento, contando com uma boa quantidade de informações graças à necessidade atual na área de resoluçãode crimes eletrônicos, apesar de ser uma área relativamente nova.

Acerca dos softwares utilizados, existem vários programas especializados em recuperação de dados, mas poucos estão disponíveis gratuitamente.

No que diz respeito à Perícia forense computacional, já foram desenvolvidos trabalhos semelhantes a este como, por exemplo, o trabalho de Afonso (2013, 86 p.) intitulado “Perícia Forense computacional aplicada a dispositivos de armazenamentos e smartphones Android”, o qual teve como objetivo analisar softwares de perícia forense computacional, para auxiliar o perito forense na escolha da ferramenta para recuperação de arquivos deletados em dispositivos de armazenamento e smartphones com sistema operacional Android.

De acordo com Afonso (2013), os seguintes softwares foram utilizados para atingir os objetivos propostos: Recuva, DiskDigger e Active@ File Recovery para Windows; para Linux: Foremost, Scalpel e TestDisk. E por fim, para o Android: Remo Recover for Android e Undelete.

Os softwares citados anteriormente foram escolhidos por serem gratuitos e de fácil localização em sistemas de buscas, com exceção do Active@ File Recovery, que não é de livre utilização. O método de análise utilizado foi “busca mais avançada” de cada software. (AFONSO, 2013).

Em conformidade com o autor supracitado, para o desenvolvimento da proposta foi montado um ambiente planejado conforme ilustra a Figura 3.

Figura 3 - Ambiente planejado para a realização dos testes.

TIPO DE EQUIPAMENTO/AMBIENTE	CONFIGURAÇÃO
DESKTOP	• MS Windows 7 Ultimate 32-bits • Intel Pentium Dual CPU E2180 @2.00Ghz • 3,00GB RAM • Intel 82945G Express Chipset Family
NOTEBOOK	• MS Windows 7 Ultimate 32-bits • Intel Core i5-321M CPU @2.50GHZ • 8,00GB RAM • Intel HD Graphics 4000
Sistema Operacional Linux Ubuntu 13.10	• Virtualizado no ambiente Windows pelo software “VirtualBox 4.3.2 for Windows hosts, x86/amd64”.

Fonte: Afonso (2013, 86 p.).
Nota: Adaptado pelo autor.

Os testes foram realizados nos três objetos descritos a seguir: pen drive (32Gb), HD Externo (200Gb) e smartphone (32Gb), estes por sua vez foram separados para utilização da seguinte maneira: uma pasta “Músicas” contendo 30 arquivos de extensão “.mp3”; uma pasta “Imagens” contendo 35 arquivos de extensão “.jpeg”; uma pasta “Textos” contendo 20arquivos de extensão “.doc”, e 20arquivos de extensão “.pdf”; e por fim, uma pasta “Vídeos” contendo 20 arquivos de vídeos no formato “.mp4”.

Em resumo, os três dispositivos continham 125 arquivos diversos e 4 pastas. Após os arquivos serem inseridos, o pendrive e HD Externo foram formatados na modalidade “Formatação Rápida”, para que na sequência fossem realizados os testes.

Em suas considerações finais, Afonso (2013) apontou que o sistema operacional com mais arquivos recuperados foi o Windows; segundo o autor, isso ocorreu devido ao fato de que os softwares desta plataforma realizarem uma busca mais demorada pelos arquivos deletados.

Ainda segundo o autor supracitado, comparando os sistemas operacionais Android e Linux, a diferença na recuperação não foi tão grande, uma vez que a análise no Android utilizou somente dois softwares e o Linux contou com três.

Por meio deste trabalho constatou-se que plataforma Windows, por ser a mais utilizada pelos usuários no mundo todo, apresenta mais opções de suporte aos softwares testados, bem como, mais funcionalidades do que as outras.

4 METODOLOGIA

O propósito das pesquisas exploratórias é proporcionar ao usuário maior familiaridade com o problema, objetivando torná-lo mais explícito ou construir uma hipótese. De modo geral, pesquisas realizadas com propósitos acadêmicos, pelo menos inicialmente, assumem um caráter exploratório, pois neste momento é pouco provável que o pesquisador tenha uma definição clara do que irá investigar.(GIL apud AFONSO, 2013).

Este trabalho teve várias etapas que foram seguidas para a obtenção dos resultados, que foram utilizados para comparação entre os *softwares* de recuperação de dados para os sistemas operacionais Windows, Linux, iOS e Android utilizados na execução desse trabalho.

Considerando a natureza delicada em se apanhar e realizar uma série de operações em notebooks, smartphones e computadores particulares ou corporativos, um planejamento foi realizado e etapas foram seguidas, para que evidências não sejam perdidas ou invalidadas.

Dessa forma, esse trabalho foi inicialmente uma pesquisa exploratória, que visou comparar programas para recuperação de dados em computadores com Windows, Linux e smartphones com iOS e Android, visando pesquisar e produzir comparações para análise pericial com os ditos aparelhos.

De início foi produzida uma pesquisa e estudo, abordando os celulares e sua evolução, chegando até aos dias atuais onde usamos smartphones, a tecnologia mais atual em quesito de telefonia móvel.

Um breve estudo sobre os sistemas operacionais mais utilizados atualmente também foi produzido, demonstrando um pouco sobre o que é Linux, Windows, Android, e iOS. Esta etapa do trabalho visa demonstrar a relevância do sistema operacional para a perícia forense, uma vez que, esses são os sistemas mais usados atualmente, e o perito deve possuir um bom conhecimento perante o sistema que irá trabalhar.

Um capítulo sobre crimes digitais e seus fundamentos foi descrito, tendo como caráter explicar como alguns ataques em computadores podem ocorrer. Técnicas como criptografia e esteganografia também estão presentes neste trabalho

para denotar um conhecimento básico sobre como imagens, textos e arquivos podem ser mascarados por criminosos para obter os dados das vítimas.

Todo o conceito de perícia forense computacional e suas aplicações em smartphones, visando buscar o que abrange essa área e onde estas técnicas forenses podem ser utilizadas também foram mencionadas.

Os procedimentos necessários para realizar uma perícia forense foram abordados, relatando quais são os procedimentos que o perito deve ter na cena do crime e quais os passos a seguir para que não ocorra nenhum dano ao equipamento nem perda de dados.

Para os testes que foram realizados em computadores com os sistemas operacionais Windows (Windows 7) e Linux (13.10). Foram selecionadoscinquenta arquivos de cada um dos tipos a seguir: texto (“.doc”), música (“.mp3”), vídeo (“.mp4”) e imagens(“.jpeg”) cada.

Em seguida os respectivos HDs foram formatados e, após a formatação, programas de recuperação de dados pré-determinados foram executados para recuperar os arquivos apagados.

Para a recuperação em smartphones, foram utilizados um iPhone 4s utilizando o iOS versão: 8.0.2(12A405), e um Samsung Ace utilizando Android na versão: 2.3.6

Vale ressaltar que para a recuperação em smartphones com controle de acesso, uma vez que com esta opção ativada o celular será bloqueado, e a recuperação poderá ser feita más por um método diferente.

A Figura 4 ilustra as plataformas e softwares selecionados para utilização neste trabalho.

Figura 4 - Plataformas e seus respectivos softwares de recuperação de dados.

Software	iOS	Android	Windows	Linux
TestDisk				
Undelete Plus				
Remo Recover				
Wondershare Dr. Fone				
Data Recovery Wizard				
Foremost				

Fonte: Elaborada pelo autor.

O motivo da escolha dos softwares elencados anteriormente deve-se ao fato de eles pertencerem à categoria de softwares “freeware”. Todos esses softwares foram utilizados na recuperação de arquivos. No decorrer do trabalho foi feita a descrição de cada programa, sua instalação e utilização.

Um relatório foi feito com a conclusão de cada análise traçada com relação à atividade de recuperação.

Para demonstração e comparação os resultados foram demonstrados em uma planilha com a porcentagem de recuperação de cada software utilizado em cada dispositivo de armazenamento utilizado. No smartphone foi utilizado o mesmo formato de exibição, através de relatórios em planilhas com a quantidade de arquivos recuperados de acordo com o seu tipo (áudio, vídeo, texto, arquivos em geral).

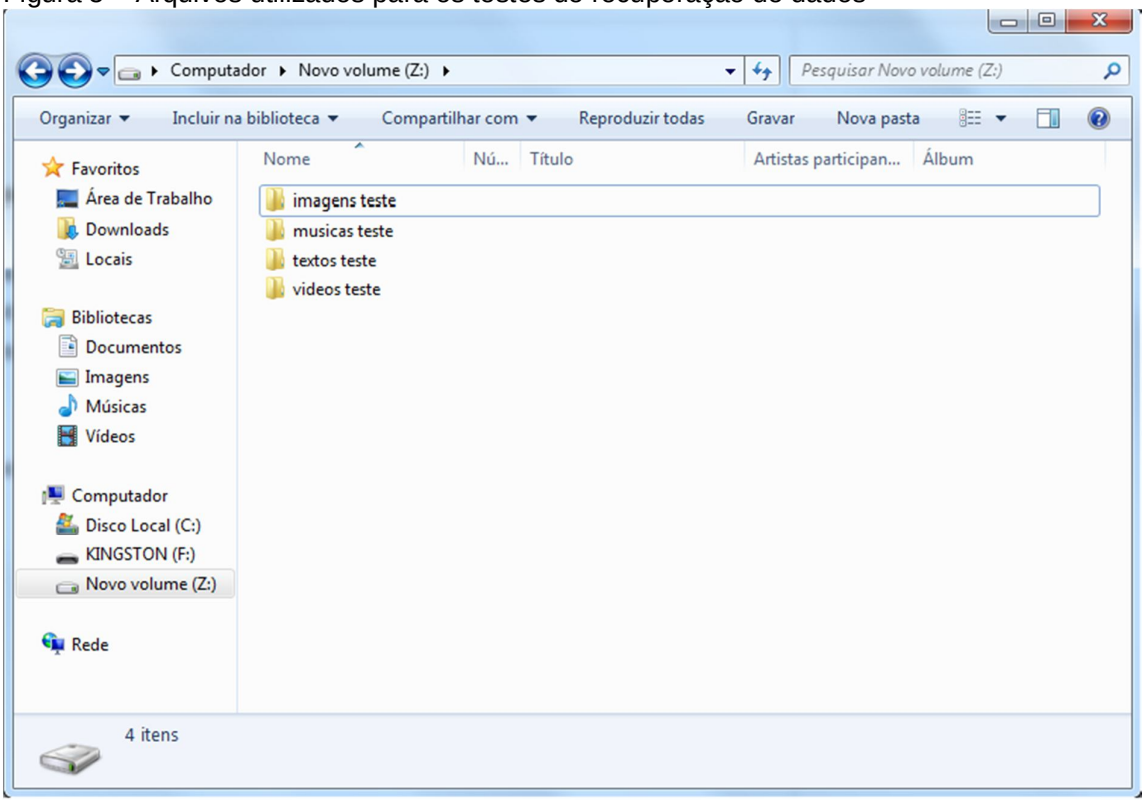
Por fim, estes resultados foram utilizados para evidenciar uma comparação vertical (entre softwares distintos em uma mesma plataforma), e horizontal (comparação do mesmo software rodando em plataformas diferentes), demonstrando quais apresentam maior capacidade de recuperação e qualidade.

Como todos os programas, estes também possuem prós e contras, isto pode ser evidenciado no trabalho para ajudar o usuário da melhor maneira possível a escolher o software mais apropriado para um determinado contexto.

5 TESTES FEITOS PARA RECUPERAÇÃO DE DADOS

Primeiramente foi criada uma nova partição no HD do computador para poder salvar os arquivos utilizados nos testes como pode ser visto na Figura 5, sendo que foram separados 50 arquivos de cada tipo em suas respectivas pastas: para arquivos de imagens em “JPEG”, som em “MP3”, textos em “DOC” e vídeos em “MP4”, e em seguida deleta-los para que fossem recuperados utilizando os seguintes softwares.

Figura 5 – Arquivos utilizados para os testes de recuperação de dados



Fonte: Elaborado pelo autor. (2014).

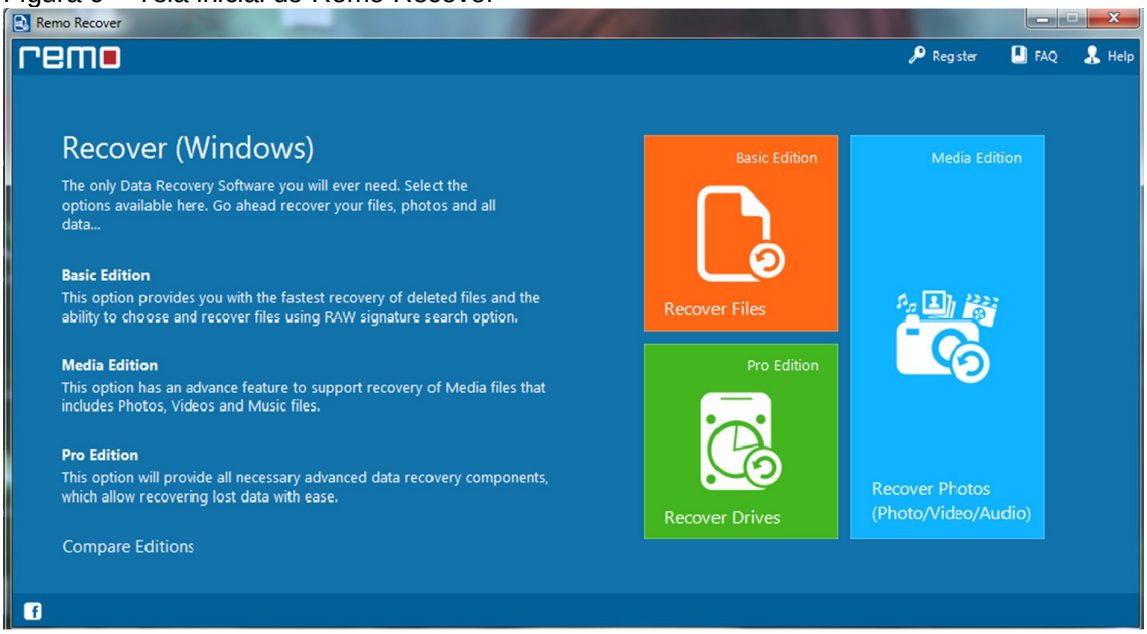
5.1 REMORECOVER

Após a formatação da partição “Z:” na qual estavam salvos os arquivos para testes, foi iniciado o software Remo Recover.

A Figura 6 mostra a tela inicial do software, onde é possível escolher entre 3 opções de acordo com a necessidade do usuário: “Basic edition” que oferece uma opção mais rápida de recuperação para arquivos deletados ou perdidos, “Media

edition” que oferece as mesmas opções da escolha anterior, mas para recuperar mais arquivos, como: vídeos, fotos e som, e a opção “Por edition”, que oferece as opções de recuperação de arquivos em partições apagadas ou formatadas, englobando todo tipo de arquivo

Figura 6 – Tela inicial do Remo Recover

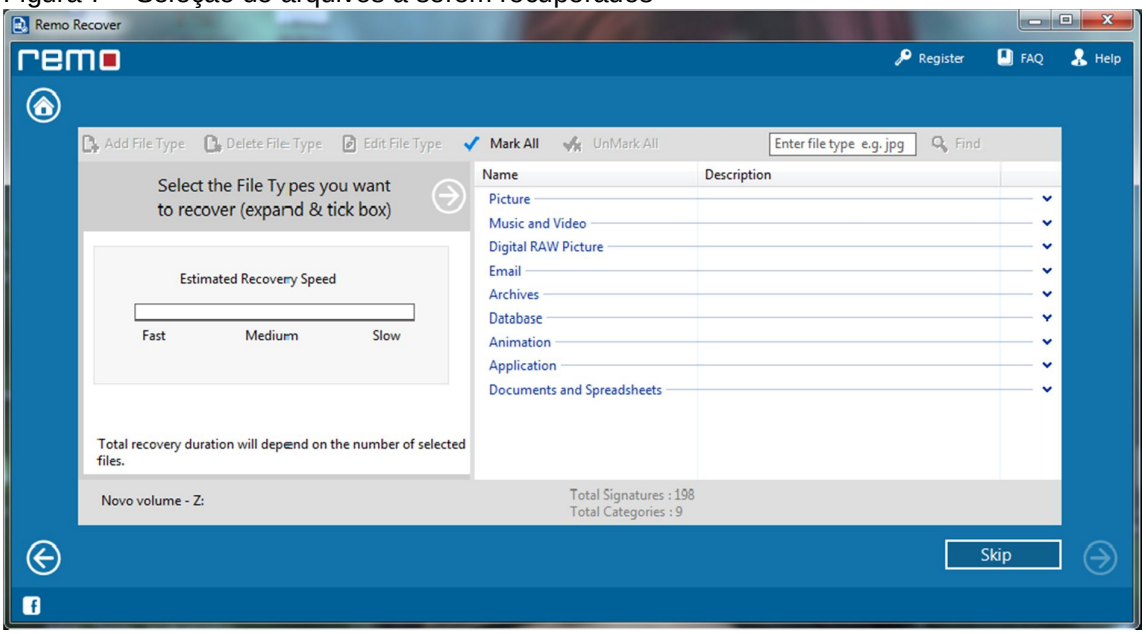


Fonte: Remo Recover. (2014).

No próximo passo, o software exibe os HD’s identificados para que o usuário escolha de qual deles é desejada a recuperação de dados.

Feito isto, é possível escolher exatamente que tipo de arquivo o usuário pretende recuperar, como é mostrado na Figura 7.

Figura 7 – Seleção de arquivos a serem recuperados

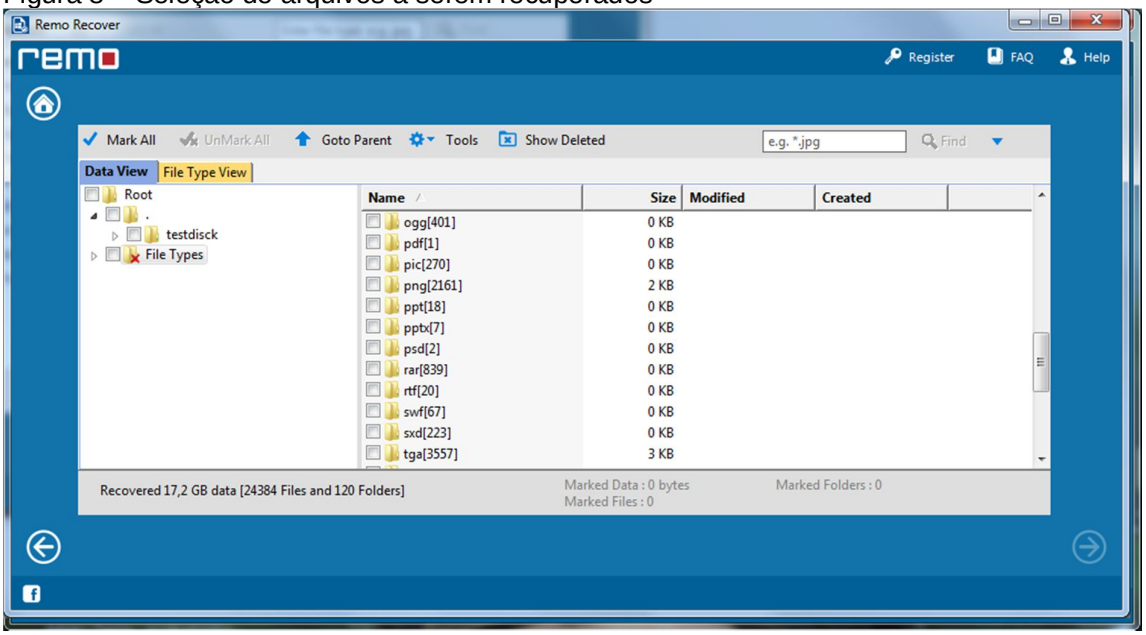


Fonte: Remo Recover. (2014).

É importante lembrar, que quanto mais tipos de arquivos são escolhidos, mais tempo o software leva para fazer o escaneamento e recuperação.

Após o processo de escaneamento, basta o usuário escolher os arquivos que ele deseja realmente recuperar, como mostrado na Figura 8.

Figura 8 – Seleção de arquivos a serem recuperados



Fonte: Remo Recover. (2014).

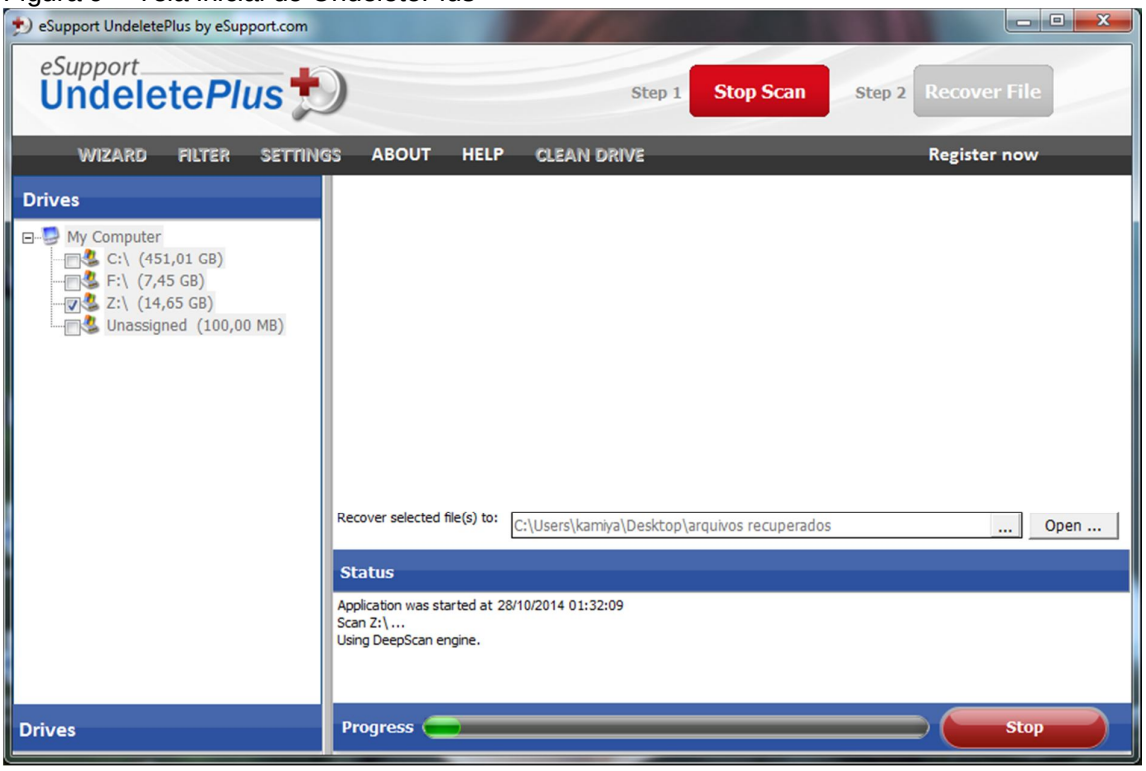
Concluindo, podemos observar pelas Figuras 6, 7 e 8, que o Remo Recover é um software bastante fácil e intuitiva que facilita bastante e permite que usuários mais leigos possam interagir com maior facilidade com o software.

5.2 UNDELETEPLUS

Assim como para o Remo Recover, o teste utilizando o UndeletePlus foi feito após a formatação da partição “Z:” contendo os arquivos de testes.

O UndeletePlus é um software bem simplificado, já na tela inicial a sua esquerda, é possível escolher de qual HD ou dispositivo de armazenamento o usuário deseja recuperar os dados e no centro da tela é possível selecionar o local de destino para os arquivos a serem recuperados, como pode ser observado na Figura 9.

Figura 9 – Tela inicial do UndeletePlus



Fonte: UndeletePlus. (2014).

Existe também a barra de ferramentas na parte superior da janela que oferece opções adicionais ao usuário e ajuda caso seja necessário.

Após selecionar o HD a ser recuperado e o destino dos arquivos, basta clicar em “Start Scam” para iniciar o processo de escaneamento e “Recover Files” para a recuperação de dados.

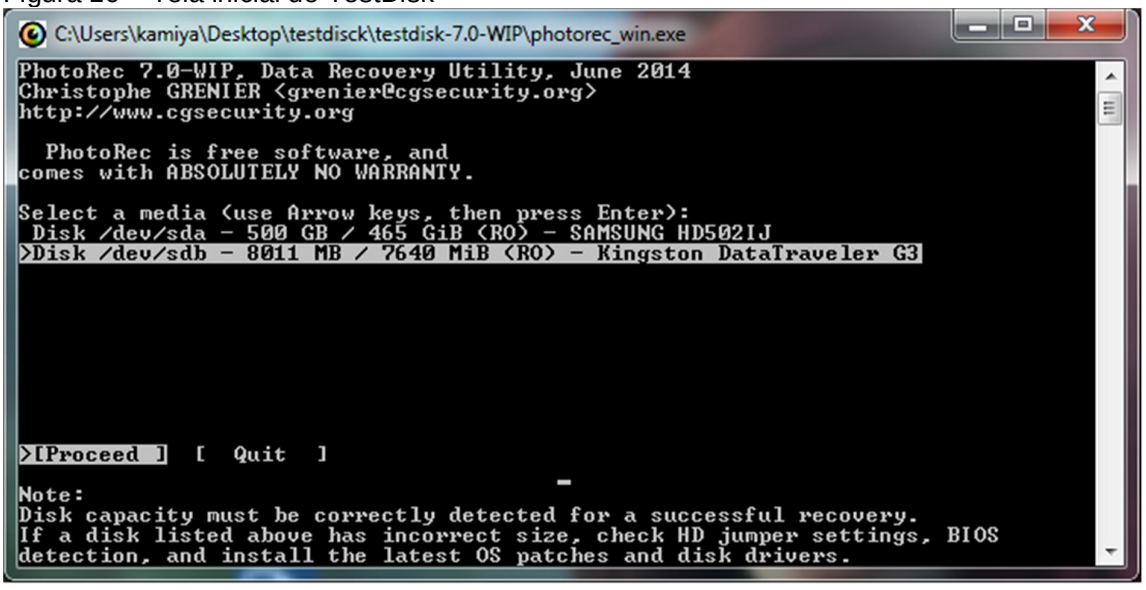
No final das contas, o UndeletePlus é um software simples e fácil de se executar, ainda é possível entrar em “settings” e escolher na aba “DeepScam” a qualidade contra a velocidade do escaneamento, dando ao usuário a opção de fazer um escaneamento rápido de baixa qualidade ou um escaneamento lento mas com alta qualidade.

5.3 TESTDISK

Ao contrário dos outros softwares já apresentados, o TestDisk tem uma interface um pouco menos amigável e exige que o usuário tenha um pouco mais de conhecimento para poder utilizar o programa sem maiores dificuldades.

Na tela inicial do software, o usuário pode escolher entre os dispositivos detectados para realizar a recuperação, como mostra a figura 10.

Figura 10 – Tela inicial do TestDisk

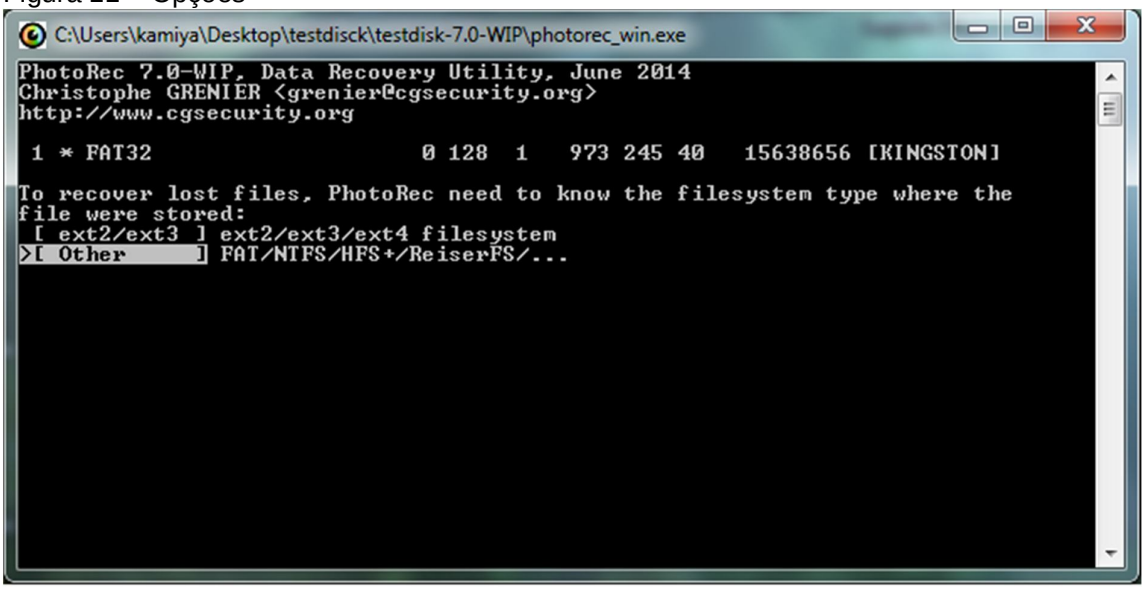


Autor: TestDisk. (2014).

Para interagir com o TestDisk, o mouse é dispensado e o usuário utiliza as setas do teclado para escolher a opção desejada.

Ao escolher o dispositivo a executar a recuperação, o usuário também precisa escolher o tipo de sistema de arquivo que a plataforma utiliza, no caso da Figura 11, foi escolhida a opção “other” pois contém o tipo de sistema de arquivo correto.

Figura 11 – Opções

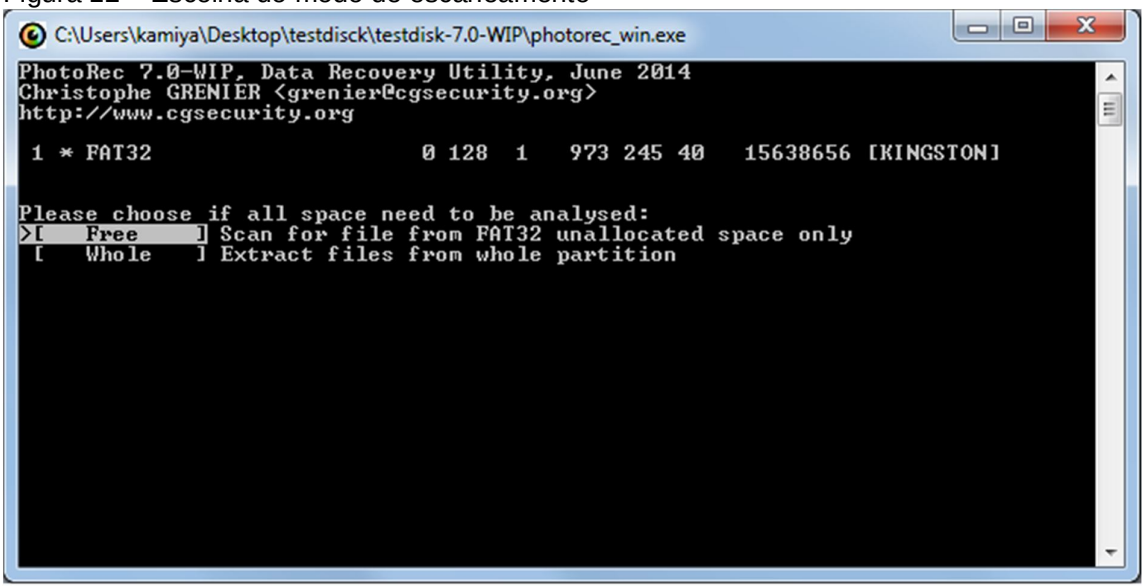


Fonte: TestDisk. (2014).

Na tela seguinte o software oferece duas opções: escanear somente o espaço livre do dispositivo ou extrair arquivos da partição inteira, como visto na figura 12.

Essas opções vão determinar se o software vai escanear somente o espaço livre em busca de arquivos perdidos ou apagados por engano, ou se será necessário escanear o dispositivo inteiro recuperando tudo o que for possível.

Figura 12 – Escolha do modo de escaneamento

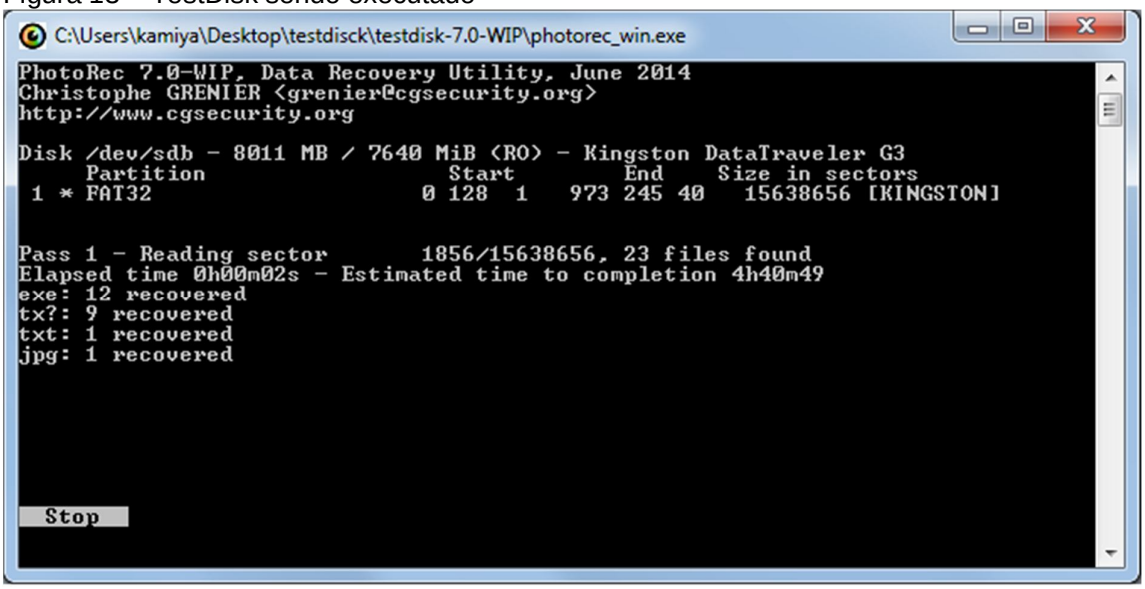


Fonte: TestDisk. (2014).

Feita a escolha, o programa oferece algumas opções de onde salvar os arquivos recuperados, para salvar na pasta padrão, basta apertar a letra “y”.

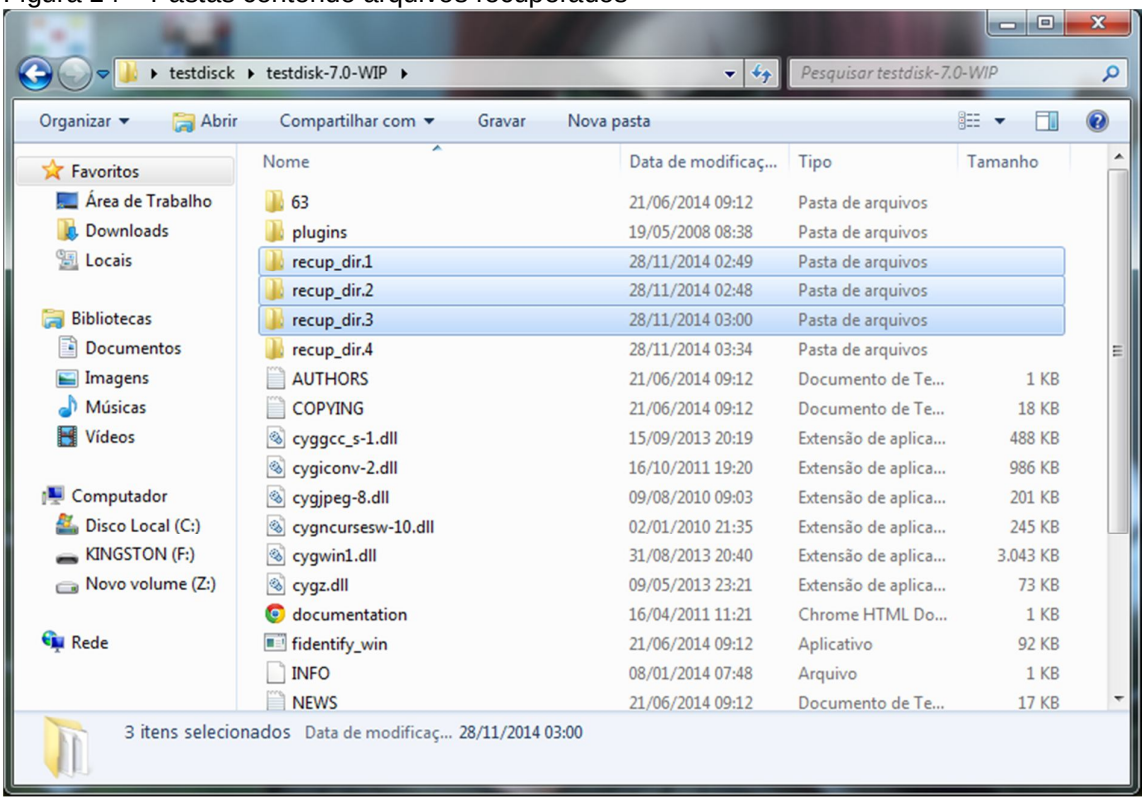
As Figuras 13 e 14, mostram respectivamente o software agindo na recuperação de dados, e o local padrão onde os arquivos recuperado podem ser achados

Figura 13 – TestDisk sendo executado



Fonte: TestDisk. (2014).

Figura 14 – Pastas contendo arquivos recuperados



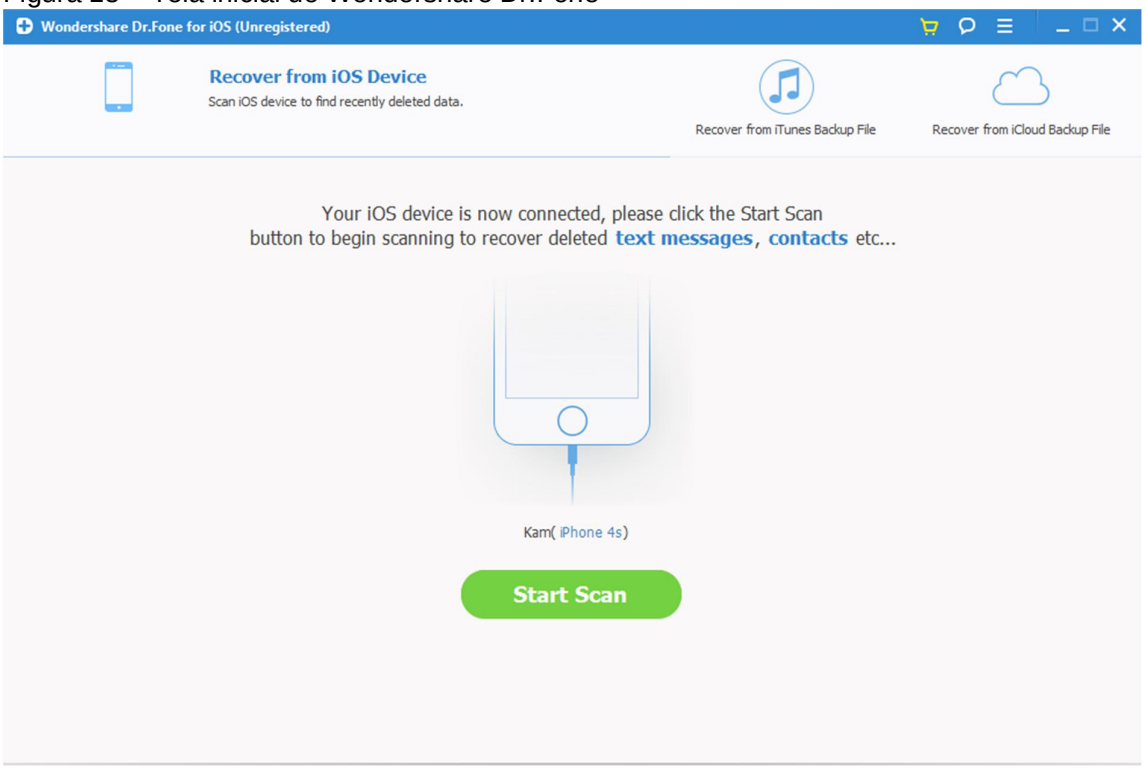
Fonte: TestDisk. (2014).

Para poder interagir com o TestDisk é necessário certo conhecimento na área de informática por parte do usuário, pois não é muito intuitivo e a falta de uma interface amigável pode afastar algumas pessoas.

5.4 WONDERSHARE DR. FONE

Feita a instalação do software, basta iniciá-lo com o smartphone já ligado ao computador para que o Wondershare Dr. Fone identifique o aparelho e ofereça a opção de escaneamento do smartphone, como pode ser visto na figura 15.

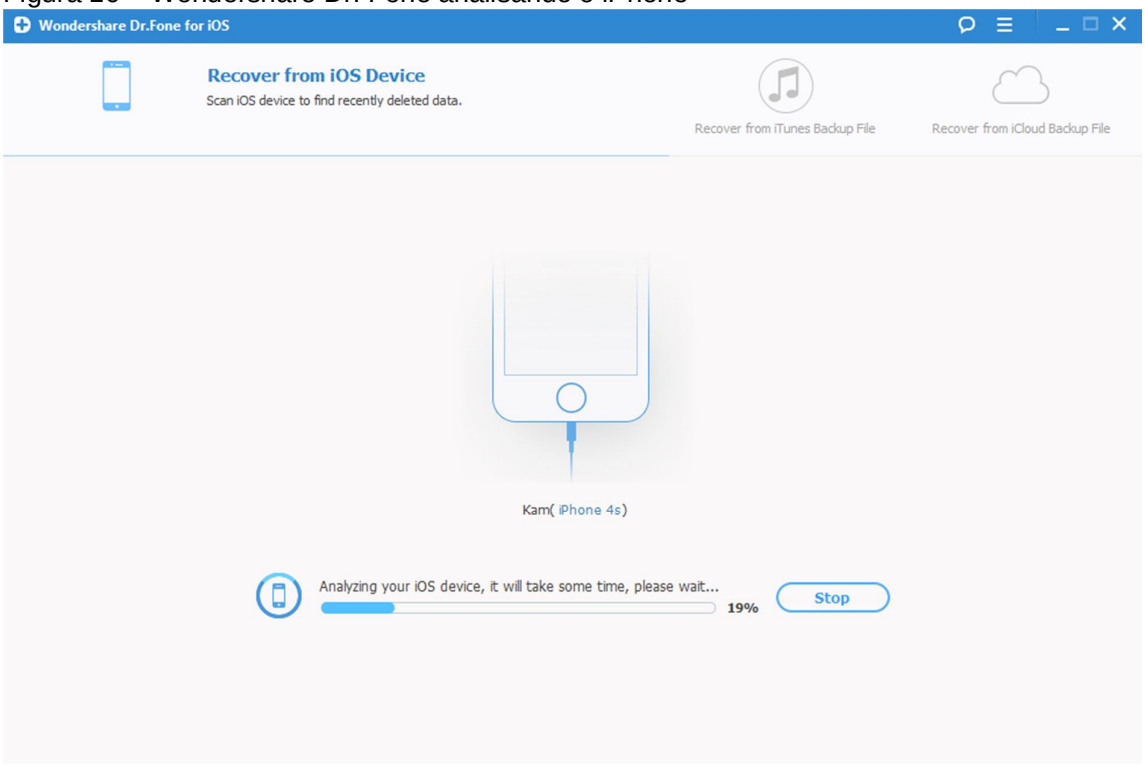
Figura 15 – Tela inicial do Wondershare Dr.Fone



Fonte: Wondershare Dr. Fone. (2014).

A Figura 16 mostra que ao clicar em “Start Scan”, o software começa a analisar o smartphone e, em seguida, mostra os arquivos que podem ser recuperados.

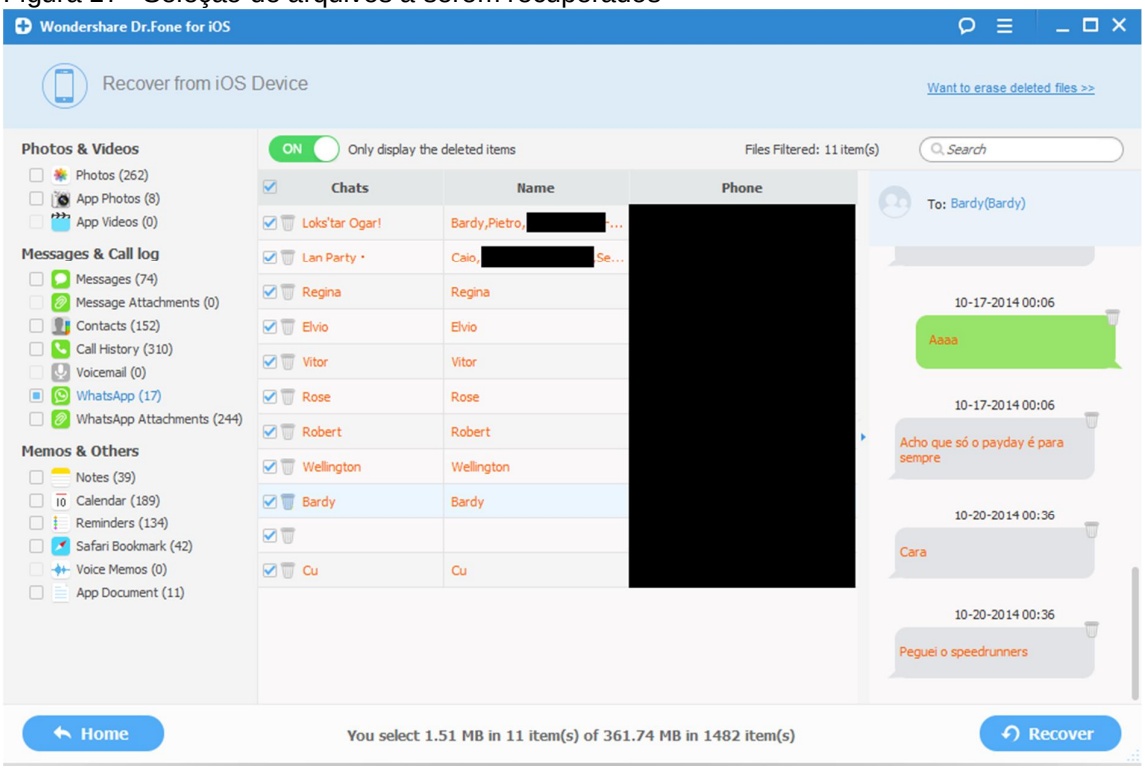
Figura 16 – Wondershare Dr. Fone analisando o iPhone



Fonte: Wondershare Dr. Fone. (2014).

É importante destacar que como este é um software voltado especificamente para a recuperação de arquivos em smarphones, ele também pode ajudar a recuperar não só fotos, vídeos e textos, mas também contatos apagados, mensagens perdidas e até mesmo mensagens do Whatsapp como pode ser visto na Figura 17, porém, não é possível recuperar músicas utilizando este software.

Figura 17 –Seleção de arquivos a serem recuperados



Fonte: Wondershare Dr. Fone. (2014).

Ao selecionar os arquivos que deseja recuperar, basta o usuário clicar em “Recover” para começar a fazer a recuperação dos dados.

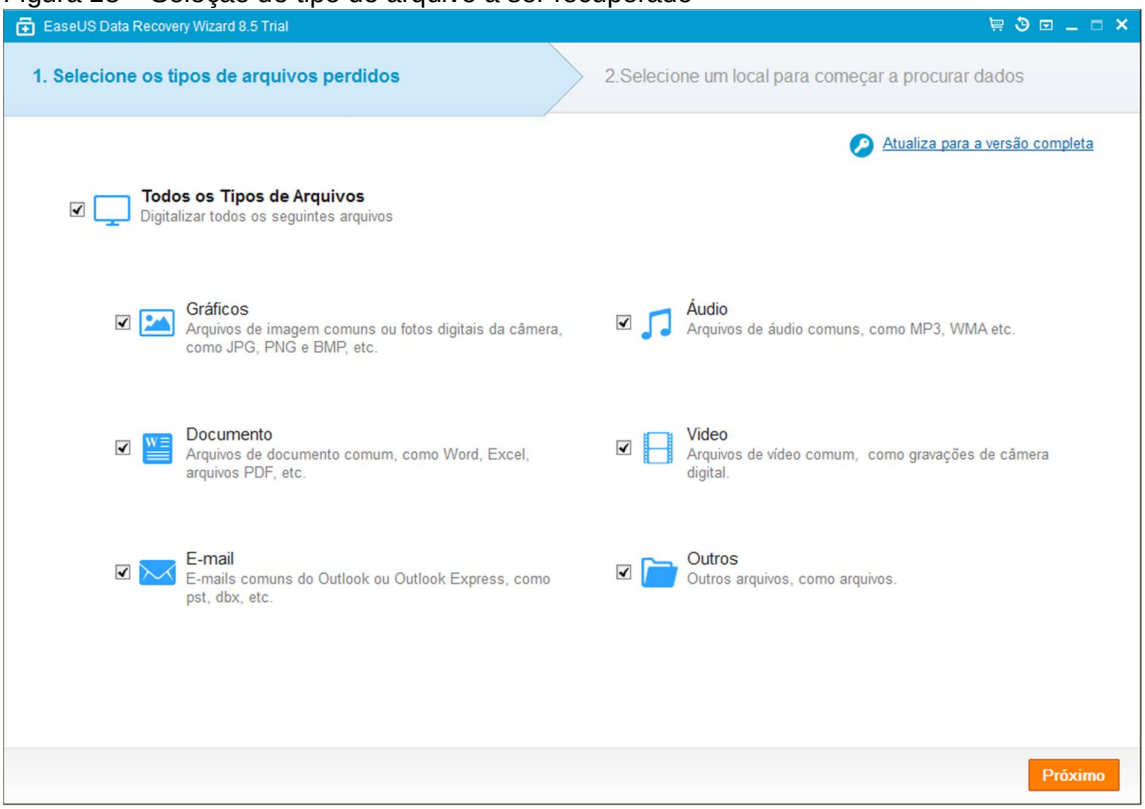
O único problema deste este software é que a versão grátis não realiza a recuperação de dados em si, apenas detecta os arquivos que podem ser recuperados.

Para a recuperação de dados ser feita realmente, é necessário comprar software, portanto não foi possível terminar o teste com o Wondershare Dr. Fone.

5.5 EASEUS DATA RECOVERY WIZARD

Ao ser iniciado, o EaseUS Data Wizard Recovery oferece uma interface bastante simples e fácil de entender, dando ao usuário a escolha de escolher que tipos de arquivos devem ser recuperados. A Figura 18 mostra como é a tela inicial deste software.

Figura 18 – Seleção de tipo de arquivo a ser recuperado



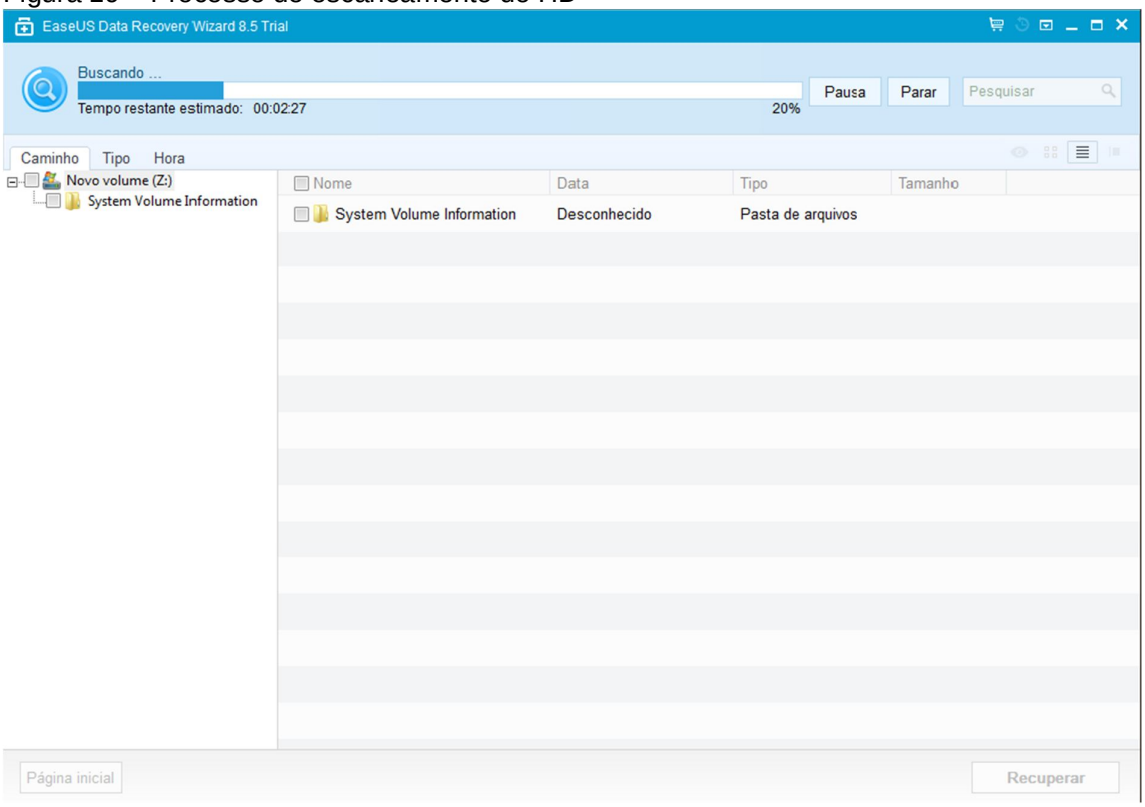
Fonte: EaseUS Data Recovery Wizard. (2014).

Na próxima etapa, o usuário deve escolher entre os dispositivos detectados pelo software, aquele que deve ser escaneado para realizar a recuperação de dados.

Feita a escolha, o software inicia uma varreduta no HD escolhido e ao mesmo tempo já cria uma lista dos arquivos encontrados e possíveis de serem recuperados.

A Figura 19 mostra o software no meio desse pocesso.

Figura 19 – Processo de escaneamento do HD



Fonte: EaseUS Data Recovery Wizard. (2014).

Terminado o escaneamento, é possível escolher quais arquivos serão recuperados e ao clicar em “Recuperar”, uma nova janela se abre para escolher onde os arquivos recuperados deverão ser salvos.

É importante destacar que o EaseUS Data Recovey Wizard em sua versão grátis, permite que o usuário recupere somente 2GB de arquivos, obrigando o usuário a comprar o software caso seja necessário recuperar mais do que o limite permitido.

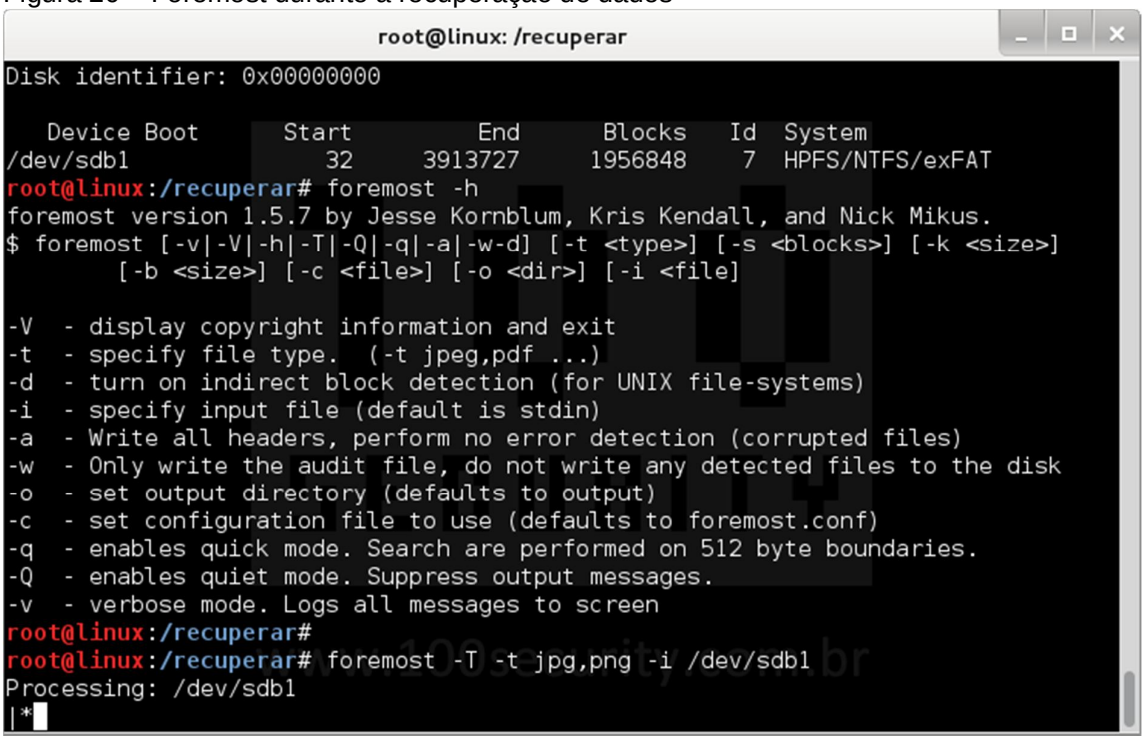
5.6 FOREMOST

Para realizar este teste, antes foi necessário emular uma máquina virtual com o sistema operacional Linux na versão 13.10 utilizando o software Oracle VM Virtual Box.

Primeiramente foi criado um pasta para armazenar os arquivos recuperados, feito isto e já com o programa aberto, foi dado o comando “foremost – T” que

especifica a saída padrão, o comando “foremost –t jpeg,doc,mp3,mp4” para informar que tipo de arquivo é procurado e “foremost –i” para informar o dispositivo de saída. A figura 20 mostra um exemplo de como a tela é exibida nesse momento.

Figura 20 – Foremost durante a recuperação de dados



Fonte: Henrique ([2014?])

Encerrado o processo, foi possível constatar alguns arquivos recuperados na pasta criada anteriormente para salvar os arquivos recuperados.

Apesar de ser um software muito eficiente, o usuário deve ter um certo grau de conhecimento para poder executa-lo sem dificuldades.

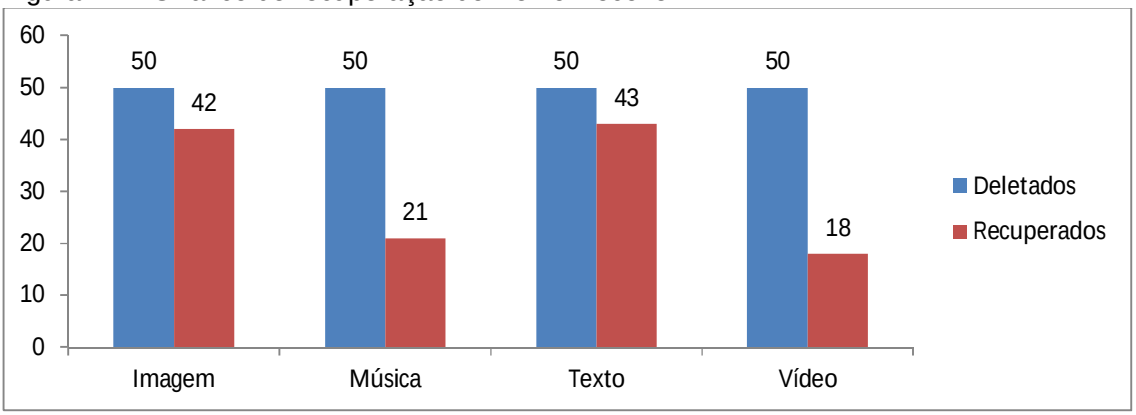
Infelizmente não foi possível realizar testes utilizando o WonderShare Dr. Fone, pois apesar de escanear e identificar arquivos apagados, a versão grátis não permite realizar a recuperação dos dados.

6 RESULTADOS OBTIDOS

Os resultados obtidos na realização dos teste foram colocados em uma tabela no Excel para realizar as comparações necessárias entre os softwares e plataformas.

A seguir serão exibidas as tabelas mostrando o desempenho de cada software individualmente, começando pelo Remo Recover.

Figura 21 – G´rafico de recuperação do Remo Recover



Fonte: Elaborado pelo autor. (2014).

Figura 22 – Tabela de recuperação de dados do Remo Recover.

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	42	33,87
Música	50	25,00	21	16,94
Texto	50	25,00	43	34,68
Vídeo	50	25,00	18	14,52
Total	200	100,00	124	100,00

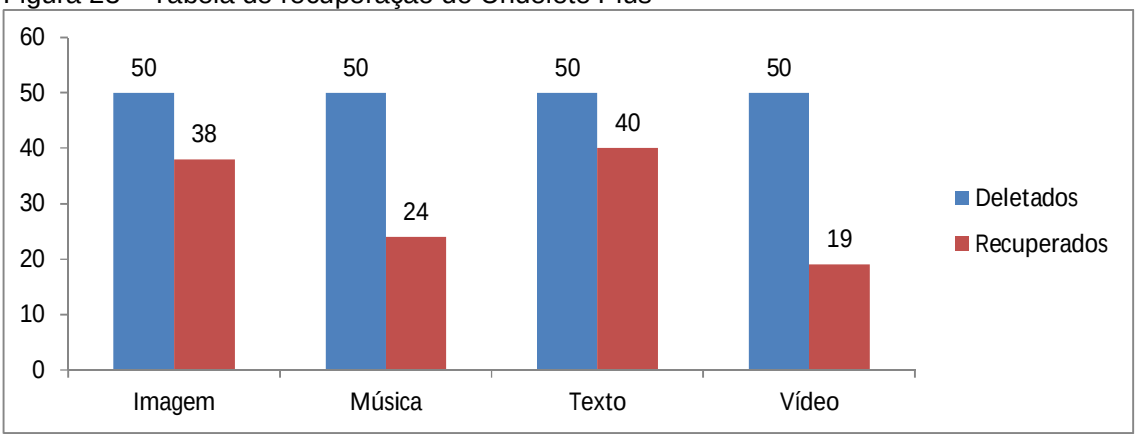
Fonte: Elaborado pelo autor. (2014).

Como pode ser observado na Figura 21 e na Figura 22, o Remo Recover teve um grande número de arquivos recuperados para imagens e texto, recuperando 42 arquivos de imagens e 43 arquivos de texto, mas não foi tão eficiente com arquivos de música e vídeo, recuperando somente 21 arquivos e 18 arquivos respectivamente.

O Undelete Plus teve uma performance parecida pois assim como o Remo Recover, teve melhores resultados com arquivos de texto conseguindo recuperar 40 arquivos e imagem conseguindo recuperar 38 arquivos, e piores resultados com

arquivos de áudio recuperando apenas 24 arquivos e vídeo recuperando 19 arquivos, como pode ser visto na Figura 23 e na Figura 24.

Figura 23 – Tabela de recuperação do Undelete Plus



Fonte: Elaborado pelo autor. (2014).

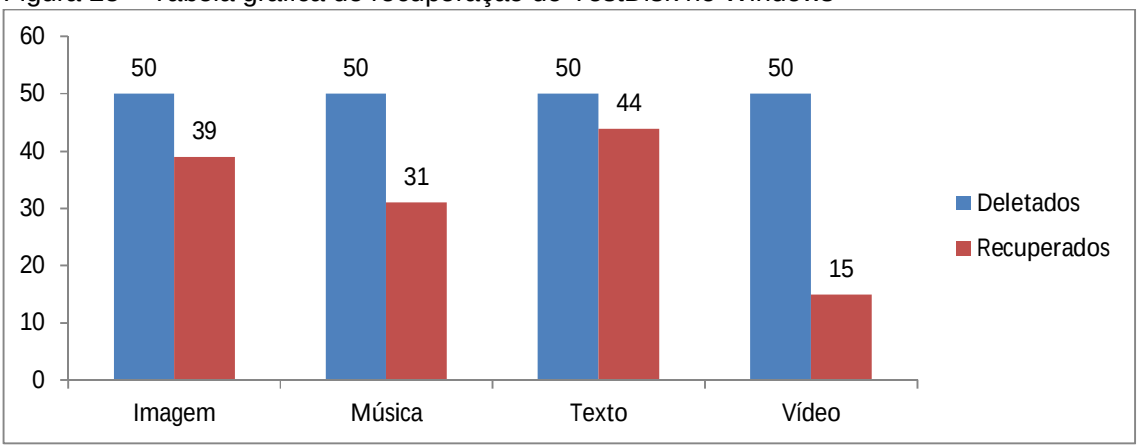
Tabela 24 – Tabela de recuperação de dados do Undelete Plus

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	38	31,40
Música	50	25,00	24	19,83
Texto	50	25,00	40	33,06
Vídeo	50	25,00	19	15,70
Total	200	100,00	121	100,00

Fonte: Elaborado pelo autor. (2014).

O TestDisk obteve um resultado pior no Window e melhor no Linux, como pode ser visto nas Figuras 25, 26, 27 e 28.

Figura 25 – Tabela gráfica de recuperação do TestDisk no Windows



Fonte: Elaborado pelo autor. (2014).

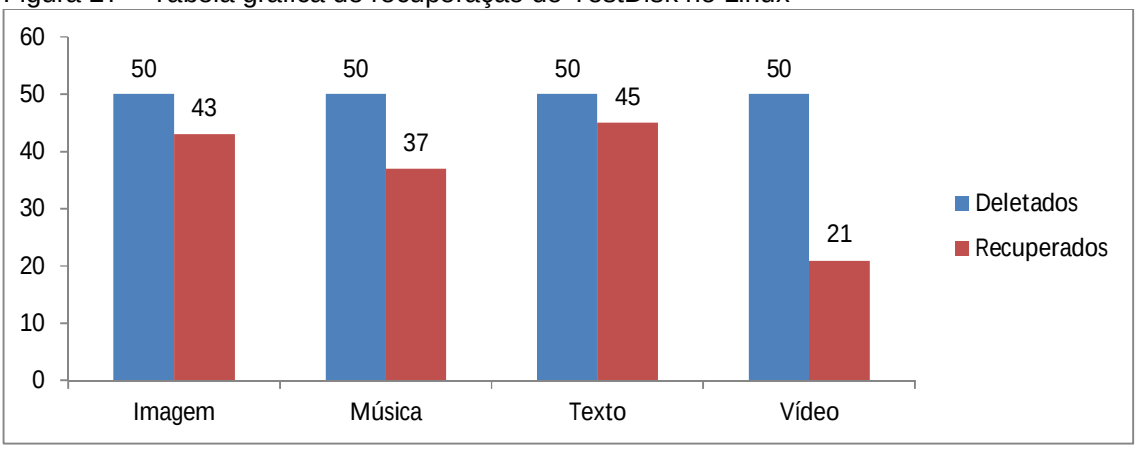
Figura 26 – Tabela de recuperação do TestDisk no Windows

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	39	30,23
Música	50	25,00	31	24,03
Texto	50	25,00	44	34,11
Vídeo	50	25,00	15	11,63
Total	200	100,00	129	100,00

Fonte: Elaborada pelo Autor. (2014).

A seguir as tabelas do TestDisk no Linux.

Figura 27 – Tabela gráfica de recuperação do TestDisk no Linux



Fonte: Elaborado pelo autor. (2014).

Figura 27 – Tabela de recuperação do TestDisk no Linux

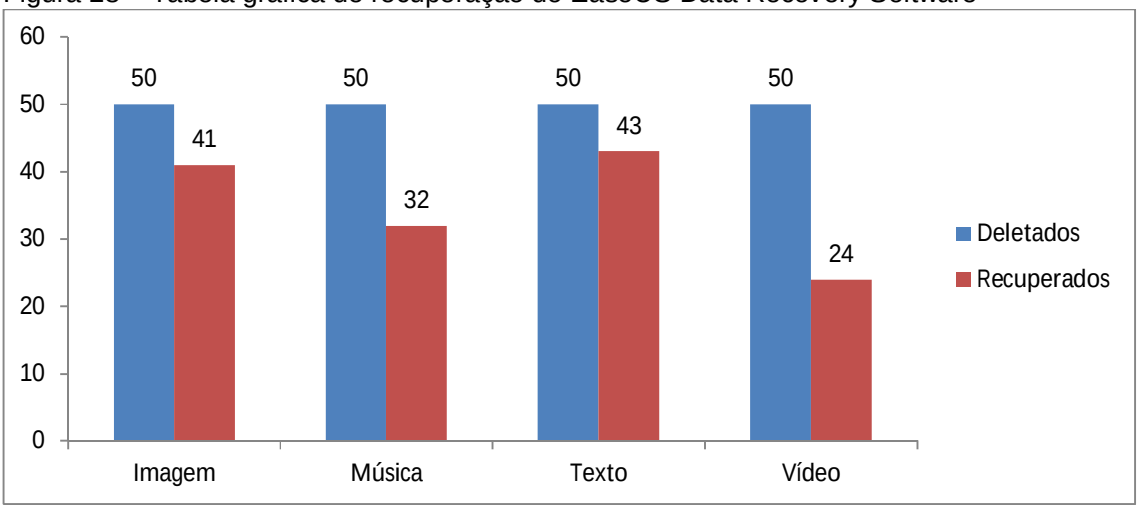
	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	43	29,45
Música	50	25,00	37	25,34
Texto	50	25,00	45	30,82
Vídeo	50	25,00	21	14,38
Total	200	100,00	146	100,00

Fonte: Elaborada pelo Autor. (2014).

É possível para todo tipo de arquivo, o TestDisk foi melhor sendo executado no Linux onde recuperou 43 arquivos de imagem, 37 de música, 45 de texto e 21 de vídeo, enquanto no Windows, foram recuperados 39 arquivos de imagem, 31 de música, 44 de texto e 15 de vídeo.

O software EaseUS Data Recovery Wizard também teve um desempenho muito bom, conseguindo recuperar vários arquivos, sendo eles 43 de texto, 41 de imagem e 32 áudio, como pode ser visto na Figura 28 e na Figura 29.

Figura 28 – Tabela gráfica de recuperação do EaseUS Data Recovery Software



Fonte: Elaborado pelo autor. (2014).

Figura 29 – Tabela de recuperação do EaseUS Data Recovery Software

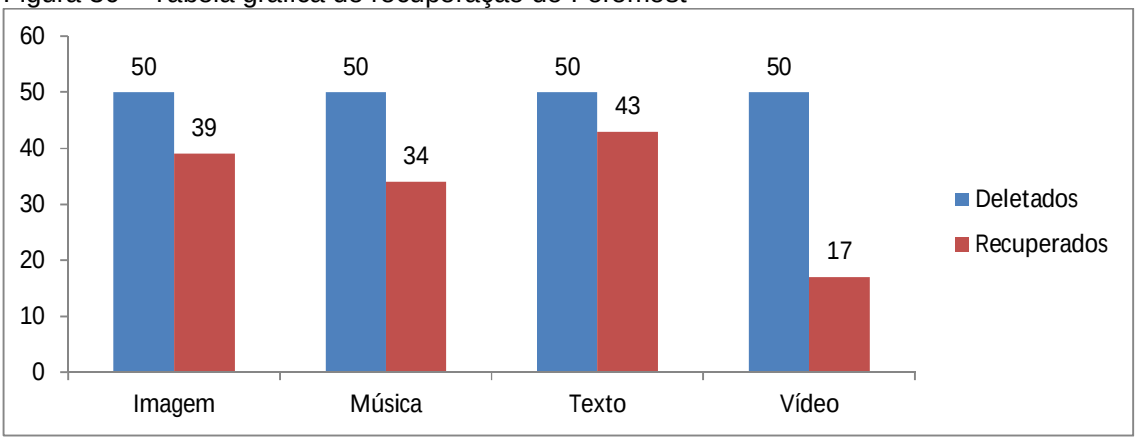
	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	41	29,29
Música	50	25,00	32	22,86
Texto	50	25,00	43	30,71
Vídeo	50	25,00	24	17,14
Total	200	100,00	140	100,00

Fonte: Elaborado pelo autor. (2014).

Apenas arquivos de vídeo ficaram com uma taxa de recuperação baixa, com apenas 24 arquivos recuperados, quase metade dos arquivos deletados, arquivos de imagem, música e texto tiveram uma taxa de recuperação mais satisfatória.

As Figuras 30 e 31 mostram a taxa de recuperação de arquivos do Foremost, software que foi usado utilizando Linux.

Figura 30 – Tabela gráfica de recuperação do Foremost



Fonte: Elaborado pelo autor. (2014).

Figura 31 – Tabela de recuperação do Foremost

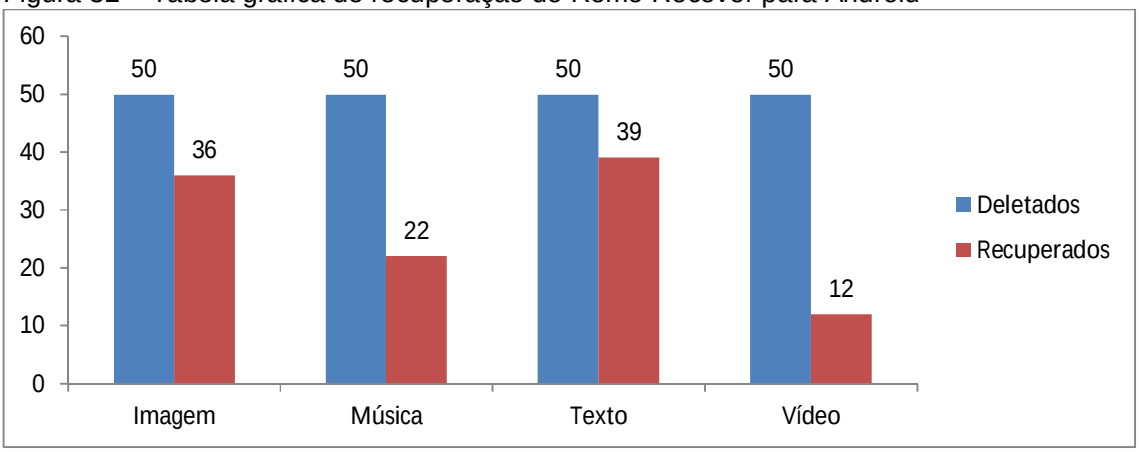
	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	39	29,32
Música	50	25,00	34	25,56
Texto	50	25,00	43	32,33
Vídeo	50	25,00	17	12,78
Total	200	100,00	133	100,00

Fonte: Elaborado pelo autor. (2014).

Seu desempenho também foi bastante satisfatório, recuperando 39 dos arquivos de imagem, 34 de música e 43 texto, deixando a desejar somente com arquivos de vídeo sendo recuperados apenas 17 arquivos.

Analisando o Remo Recover para a plataforma Android não conseguiu recuperar tantos arquivos quanto os outros softwares, ficando com um resultado um pouco abaixo do esperado, recuperando 36 arquivos de imagem, 22 de música, 39 de texto e apenas 12 de vídeo, como pode ser visto nas Figuras 32 e 33.

Figura 32 – Tabela gráfica de recuperação do Remo Recover para Android



Fonte: Elaborado pelo autor. (2014).

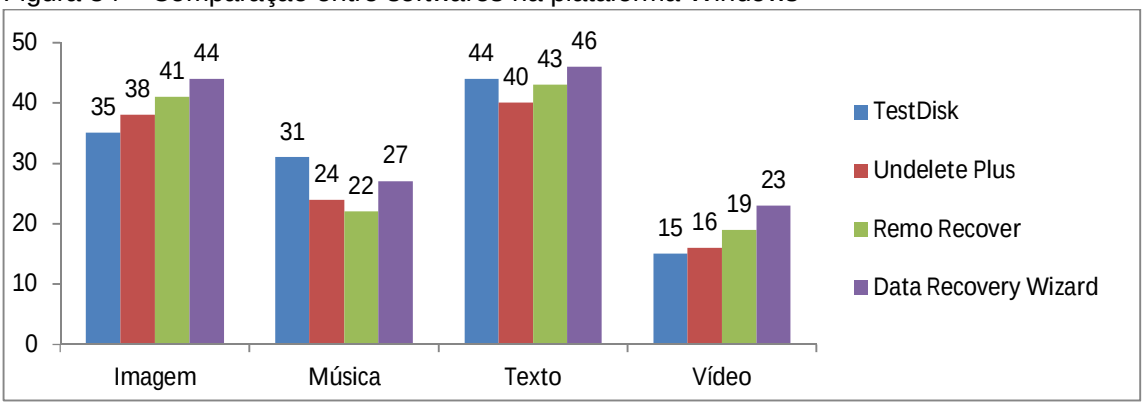
Figura 33 – Tabela de recuperação do Remo Recover para Android

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	36	33,03
Música	50	25,00	22	20,18
Texto	50	25,00	39	35,78
Vídeo	50	25,00	12	11,01
Total	200	100,00	109	100,00

Fonte: Elaborado pelo autor. (2014).

A Figura 34 e a Figura 35 a seguir, mostram uma comparação entre todos os softwares utilizados na plataforma Windows e o quanto foi possível recuperar de cada arquivo.

Figura 34 – Comparação entre softwares na plataforma Windows



Fonte: Elaborado pelo autor. (2014).

Figura 35 - Recuperação de Arquivos na Plataforma Windows.

		TestDisk		Undelete Plus		Remo Recover		Data Recovery Wizard	
	Deletados	Recuperados		Recuperados		Recuperados		Recuperados	
Tipo de arquivo	Fa	Fa	Fr (%)	Fa	Fr(%)	Fa	Fr(%)	Fa	Fr(%)
Imagem	50	35	70,00	38	76,00	41	82,00	44	125,71
Música	50	31	62,00	24	48,00	22	44,00	27	87,10
Texto	50	44	88,00	40	80,00	43	86,00	46	104,55
Vídeo	50	15	30,00	16	32,00	19	38,00	23	153,33
Total	200	125		118		125		140	

Fonte: Elaborada pelo Autor (2014).

Analisando as Figura 35, é notável que o EaseUS Data Recovery Wizard é levemente superior ao outros, recuperando 44 arquivos de imagem, 46 de música e 23 de vídeo, perdendo apenas na recuperação de arquivos de áudio para o TestDisk que recuperou 31 enquanto o Data Recovery Wizard recuperou apenas 27.

Mesmo assim, todos os softwares tiveram um desempenho semelhante, conseguindo recuperar mais arquivos de texto e imagem, uma quantidade média de arquivos de áudio, e poucos vídeos.

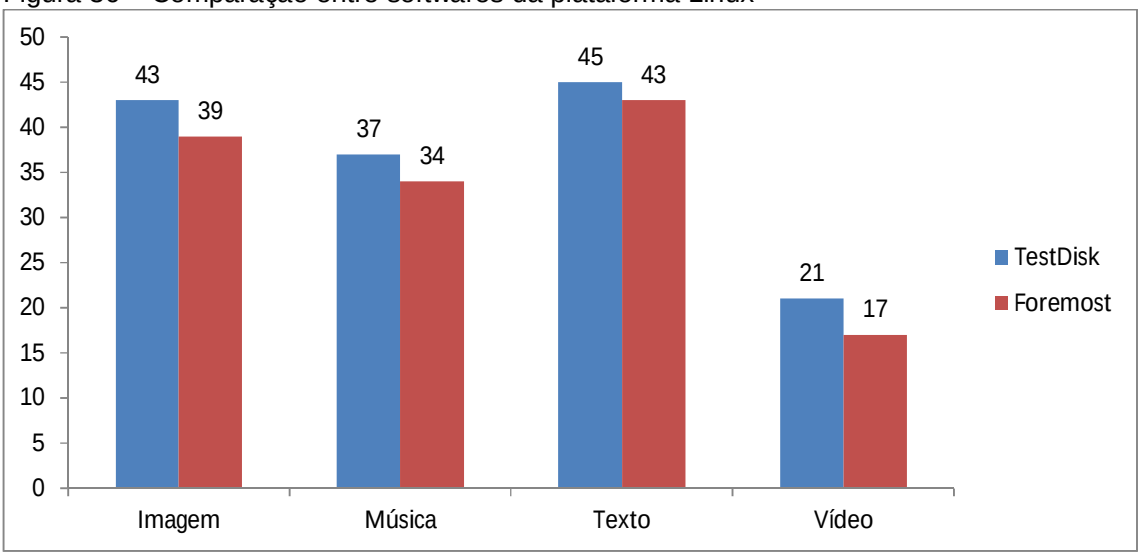
Em questão de tempo, o que mais demorou também foi o Ease Data Recovery Wizard, que demorou entre 15 e 30 minutos para concluir a recuperação.

Em termos de conveniência e facilidade de uso, o unico que deixou um pouco a desejar foi o TestDisk, que não possui uma interface amigável e pode parecer um pouco confuso no começo.

Vale lembrar que dentre estes softwares o único traduzido para o português é o EaseUS Data Recovery Wizard, para todos os outros, o usuário precisará saber um pouco de inglês para poder entender o software com mais facilidade.

A Figura 29 exibe a comparação entre os softwares utilizados na plataforma Linux.

Figura 36 – Comparação entre softwares da plataforma Linux



Fonte: Elaborado pelo autor. (2014).

Figura 37 - Recuperação de Arquivos na Plataforma Linux.

		TestDisk		Foremost	
	Deletados	Recuperados		Recuperados	
Tipo de arquivo	Fa	Fa	Fr (%)	Fa	Fr (%)
Imagem	50	43	86,00	39	78,00
Música	50	37	74,00	34	68,00
Texto	50	45	90,00	43	86,00
Vídeo	50	21	42,00	17	34,00
Total	200	146		133	

Fonte: Elaborado pelo autor. (2014).

Observando as figuras 36 e 37, fica claro que ambos softwares tiveram um desempenho semelhante e com bons resultados, recuperando a maior parte dos arquivos de testes.

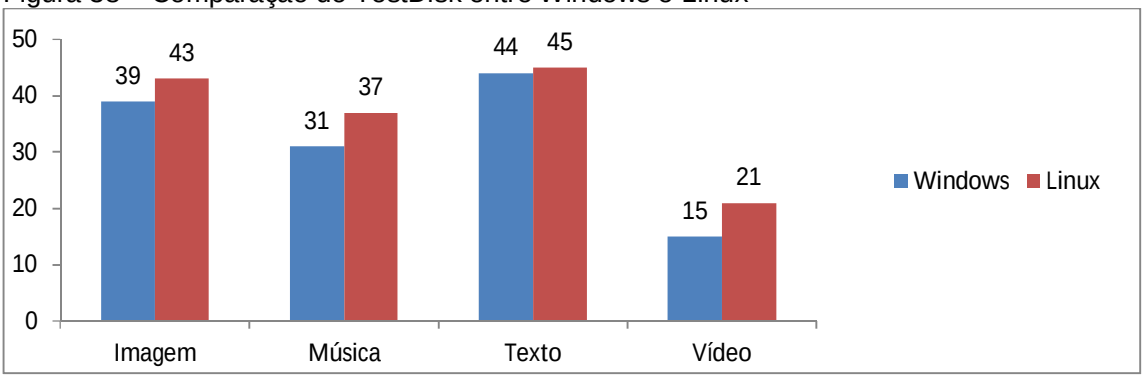
Em questão de interface, de novo, ambos são parecidos pois não utilizam o mouse e não possuem uma interface muito amigável, sendo necessário utilizar

linhas de comando para poder interagir com o software, o que pode afastar alguns usuários sem muito conhecimento.

O tempo decorrido no processo de recuperação foi baixo para os dois, em menos de 10 minutos já foi possível obter resultados.

A Figura 38 mostra em seguida o desempenho do TestDisk fazendo uma comparação de seu desempenho nas plataformas Windows e Linux.

Figura 38 – Comparação do TestDisk entre Windows e Linux



Fonte: Elaborado pelo autor. (2014).

Figura 39 - Recuperação de Arquivos no TestDisk.

		Windows		Linux	
	Deletados	Recuperados		Recuperados	
Tipo de arquivo	Fa	Fa	Fr (%)	Fa	Fr(%)
Imagem	50	39	78,00	43	86,00
Música	50	31	62,00	37	74,00
Texto	50	44	88,00	45	90,00
Vídeo	50	15	30,00	21	42,00
Total	200	129		146	

Fonte: Elaborado pelo autor. (2104).

Analisando as Figuras 38 e 39, percebe-se que em ambas plataformas o TestDisk teve um bom desempenho, mas é um pouco melhor no Linux onde conseguiu recuperar mais arquivos de todos os tipos.

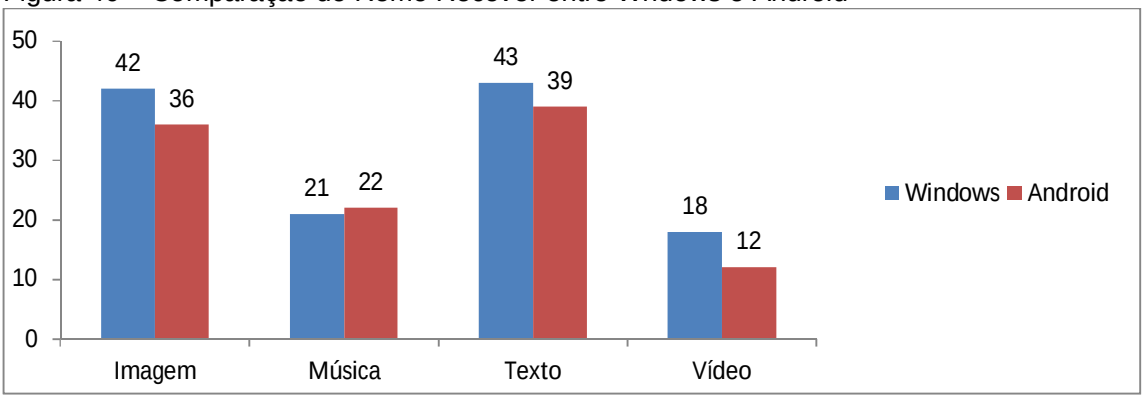
No Linux foram recuperados 43 arquivos de imagem, 37 de música 45 de texto e 21 de vídeo, enquanto to Windows, foram recuperados 39 de imagem, 31 de música, 44 de texto e 15 de vídeo.

Em questão de tempo, levaram aproximadamente o mesmo tempo para realizar a recuperação.

É importante lembrar que o modo de execução no Windows e Linux é um pouco diferente, sendo que no Windows, basta o usuário selecionar as opções desejada, enquanto no Linux é preciso digitar linhas de comando para executar o programa.

Na figura 31, é feita uma comparação do software Remo Recover entre as plataformas Windows e Android.

Figura 40 – Comparação do Remo Recover entre Wndows e Android



Fonte: Elaborado pelo autor. (2014).

A Figura 41

Figura 41 - Recuperação de Arquivos no Remo Recover

		Windows		Android	
	Deletados	Recuperados		Recuperados	
Tipo de arquivo	Fa	Fa	Fr (%)	Fa	Fr(%)
Imagem	50	42	84,00	36	72,00
Música	50	21	42,00	22	44,00
Texto	50	43	86,00	39	78,00
Vídeo	50	18	36,00	12	24,00
Total	200	124		109	

Fonte: Elaborado pelo autor. (2014).

Assim como na comparação anterior do TestDisk, para o Remo Recover também é constatada uma performance parecida para ambas as plataformas, com o Windows perdendo somente nos arquivos de áudio recuperando 21 arquivos, mas recuperando 42 arquivos de imagem, 43 de texto e 18 de vídeo, enquanto para Android foram recuperados 36 de imagem, 22 de música, 39 de texto e 12 de vídeo.

Apesar de ser uma variação do software para Windows, o Remo Recover for Android tem a interface muito similar ao Remo Recover de Windows, o que é um ponto positivo pois é uma interface bastante intuitiva e amigável para usuários sem domínio de informática.

7 CONCLUSÃO

Com o crescente número de informações digitais em aparelhos eletrônicos, é de extrema importância o uso de softwares de recuperação de dados pois a possibilidade de perda ou roubo de dados também é muito alta.

Muitos softwares de recuperação de dados foram desenvolvidos graças a perícia forense que tem ganhado bastante atenção atualmente graças a necessidade de proteger dados importantes.

Desse modo, foram analisadas sete programas especializados na recuperação de dados para as plataformas Windows, Linux, iOS e Android, que são os sistemas operacionais mais populares hoje em dia.

As ferramentas foram testadas e comparadas de diversas maneiras, comparando qual tem mais taxa de recuperação e em qual plataforma tem melhor desempenho.

Além dos softwares analisados, este trabalho também falou um pouco sobre a perícia forense e sobre crimes virtuais.

Em geral o software que teve melhor desempenho foi o EaseUS Data Recovery Software, que apesar de demorar um pouco mais, foi o que mais conseguiu recuperar dados.

Foi possível observar o mesmo software funcionando em duas plataformas diferentes, que foi o caso dos softwares TestDisk que funcionou em Windows e Linux, e o Remo Recovery que funcionou em Windows e Android.

Um ponto interessante é a dificuldade de se remover os dados de um HD completamente, estes softwares de recuperação de dados são muito uteis e conforme o tempo passa, mais e melhores ferramentas como estas surgirão.

REFERENCIAS

AFONSO, Raphael Pinheiro. **Perícia forense computacional aplicada a dispositivos de armazenamentos e smartphones**. 2013.86 f. Trabalho de conclusão de curso (Graduação em Ciência da Computação)- Universidade do Sagrado Coração, Bauru, 2013.

BARROS, Thiago. Cinco anos de Android: relembre a história e todas as versões do sistema.**Techtudo**, 2013. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2013/09/cinco-anos-de-android-relembre-historia-e-todas-versoes-do-sistema.html> Acesso em: 10 abr. 2014.

CIPOLI, Pedro. O que é Engenharia Social?**Canal Tech**, 2012. Disponível em: <http://corporate.canaltech.com.br/o-que-e/seguranca/O-que-e-Engenharia-Social/> Acesso em: 10 maio 2014.

COSTA, Daniel Moraes. **Boas práticas para perícia forense**. 2008. 44 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Faculdade de Jaguariúna, 2008. Disponível em: <http://bibdig.poliseducacional.com.br/document/?view=174>. Acesso em: 10 abr. 2014.

Forense computacional. **Grupo Treinar**, [2014?]. Disponível em: <http://www.grupotreinar.com.br/media/48351/descritivo%20detalhado%20do%20curso%20forense%20computacional_v0.pdf> Acesso em: 20 maio 2014.

GUGIK, Gabriel. A história dos computadores e da computação.**Tecmundo**, 2009.Disponível em:<http://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm>. Acesso em: 15 abr. 2014.

HENRIQUE. Marcos. Recuperar dados usando Foremost, **100secuity**, disponível em: <http://www.100security.com.br/recuperar-dados-usando-foremost/> Acessado em 03 nov. 2014.

HULME, George V. Qual sistema móvel é mais seguro para sua empresa iOS ou Android? **ComputerWorld**, 2014. Disponível em: <http://computerworld.com.br/seguranca/2014/02/04/qual-sistema-movel-e-mais-seguro-para-sua-empresa-ios-ou-android/> Acesso em: 20 maio 2014.

JORDÃO, Fabio. História: a evolução do celular.**Tecmundo**,2009. Disponível em: <http://www.tecmundo.com.br/celular/2140-historia-a-evolucao-do-celular.htm>. Acesso em: 10 abr. 2014.

MARTINS, Elaine. O que é esteganografia?**Tecmundo**, 2010.Disponível em: <http://www.tecmundo.com.br/video/3763-o-que-e-esteganografia-.htm>. Acesso em: 20 maio 2014.

MICROSOFT.Uma história do Windows. **Windows**, 2013. Disponível em:<http://windows.microsoft.com/pt-br/windows/history#T1=era0> Acesso em: 20 maio 2014.

NOBLETT, Michael G.; POLLITT, Mark M.; PRESLEY, Lawrence A. Recovering and Examining Computer Forensic Evidence. **Forensic Science Communications**, [S.l.], v. 2, n. 4, oct. 2000. Disponível em: <http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm> Acesso em: 20 maio 2014.

PISA, Pedro.A evolução do Windows.**Techtudo**, 2012.Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/05/a-evolucao-do-windows.html> Acesso em: 20 maio 2014

RENATO, Flávio. A história dos telefones celulares.**Tecmundo**, 2012. Em Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/06/historia-dos-telefones-celulares.html> Acesso em: 15 abr. 2014.

TROYACK, Leandra; YUNG, Rodrigo. iOS: Abrindo um novo mundo para a tecnologia móvel.**Código Fonte**, 2013. Disponível em: <http://codigofonte.uol.com.br/artigos/ios-abrindo-um-novo-mundo-para-a-tecnologia-movel> Acesso em: 10 abr. 2014

WESTPHAL, Kristy. Steganography Revealed. **Symantec**, 2003.Disponível em: <http://www.symantec.com/connect/articles/steganography-revealed>. Acesso em: 20 maio 2014.

APÊNDICE A – TABELAS DE RECUPERAÇÃO DE ARQUIVOS EM CADA *SOFTWARE* UTILIZADO

Tabela 1 - Recuperação de arquivos no Software Remo Recover - Plataforma Windows

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	42	33,87
Música	50	25,00	21	16,94
Texto	50	25,00	43	34,68
Vídeo	50	25,00	18	14,52
Total	200	100,00	124	100,00

Fonte: Elaborada pelo Autor (2014).

Tabela 2 - Recuperação de arquivos no Software Undelete Plus - Plataforma Windows

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	38	31,40
Música	50	25,00	24	19,83
Texto	50	25,00	40	33,06
Vídeo	50	25,00	19	15,70
Total	200	100,00	121	100,00

Fonte: Elaborada pelo Autor (2014).

Tabela 3 - Recuperação de arquivos no TestDisk - Plataforma Windows

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	39	30,23
Música	50	25,00	31	24,03
Texto	50	25,00	44	34,11
Vídeo	50	25,00	15	11,63
Total	200	100,00	129	100,00

Fonte: Elaborada pelo Autor (2014).

Tabela 4 - Recuperação de arquivos no Software EaseUS Data Recovery Wizard - PlataformaWindows

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	41	29,29
Música	50	25,00	32	22,86
Texto	50	25,00	43	30,71
Vídeo	50	25,00	24	17,14
Total	200	100,00	140	100,00

Fonte: Elaborada pelo Autor (2014).

Tabela 5 - Recuperação de arquivos no Software Remo Recover - Plataforma Android

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	36	33,03
Música	50	25,00	22	20,18
Texto	50	25,00	39	35,78
Vídeo	50	25,00	12	11,01
Total	200	100,00	109	100,00

Fonte: Elaborada pelo Autor (2014).

Tabela 6 - Recuperação de arquivos no SoftwareTestDisk - Plataforma Linux

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	43	29,45
Música	50	25,00	37	25,34
Texto	50	25,00	45	30,82
Vídeo	50	25,00	21	14,38
Total	200	100,00	146	100,00

Fonte: Elaborada pelo Autor (2014).

Tabela 7 - Recuperação de arquivos no Software Foremost - Plataforma Linux

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	50	25,00	39	29,32
Música	50	25,00	34	25,56
Texto	50	25,00	43	32,33
Vídeo	50	25,00	17	12,78
Total	200	100,00	133	100,00

Fonte: Elaborada pelo Autor (2014).

APÊNDICE B – TABELAS DE RECUPERAÇÃO DE ARQUIVOS EM CADA SISTEMA OPERACIONAL UTILIZADO

Tabela 8 - Recuperação de Arquivos na Plataforma Windows.

		TestDisk		Undelete Plus		Remo Recover		Data Recovery Wizard	
	Deletados	Recuperados		Recuperados		Recuperados		Recuperados	
Tipo de arquivo	Fa	Fa	Fr (%)	Fa	Fr(%)	Fa	Fr(%)	Fa	Fr(%)
Imagem	50	35	70,00	38	76,00	41	82,00	44	125,71
Música	50	31	62,00	24	48,00	22	44,00	27	87,10
Texto	50	44	88,00	40	80,00	43	86,00	46	104,55
Vídeo	50	15	30,00	16	32,00	19	38,00	23	153,33
Total	200	125		118		125		140	

Fonte: Elaborada pelo Autor (2014).

Tabela 9 - Recuperação de Arquivos na Plataforma Linux.

		TestDisk		Foremost	
	Deletados	Recuperados		Recuperados	
Tipo de arquivo	Fa	Fa	Fr (%)	Fa	Fr (%)
Imagem	50	43	86,00	39	78,00
Música	50	37	74,00	34	68,00
Texto	50	45	90,00	43	86,00
Vídeo	50	21	42,00	17	34,00
Total	200	146		133	

Fonte: Elaborada pelo Autor (2014).

Tabela 9 - Recuperação de Arquivos na Plataforma Android.

		Remo Recover	
	Deletados	Recuperados	
Tipo de arquivo	Fa	Fa	Fr (%)
Imagem	50	36	72,00
Música	50	22	44,00
Texto	50	39	78,00
Vídeo	50	12	24,00
Total	200	109	

Fonte: Elaborada pelo Autor (2014).

APÊNDICE C – TABELA DE RECUPERAÇÃO DE ARQUIVOS EM PLATAFORMA POR SOFTWARE

Tabela 13 - Recuperação de Arquivos no TestDisk.

Tipo de arquivo		Windows		Linux	
	Deletados	Recuperados		Recuperados	
	Fa	Fa	Fr (%)	Fa	Fr(%)
Imagem	50	39	78,00	43	86,00
Música	50	31	62,00	37	74,00
Texto	50	44	88,00	45	90,00
Vídeo	50	15	30,00	21	42,00
Total	200	129		146	

Fonte: Elaborada pelo Autor (2014).

Tabela 14 - Recuperação de Arquivos no Remo Recover.

		Windows		Android	
	Deletados	Recuperados		Recuperados	
Tipo de arquivo	Fa	Fa	Fr (%)	Fa	Fr(%)
Imagem	50	42	84,00	36	72,00
Música	50	21	42,00	22	44,00
Texto	50	43	86,00	39	78,00
Vídeo	50	18	36,00	12	24,00
Total	200	124		109	

Fonte: Elaborada pelo Autor (2014).

Perícia Forense Computacional Aplicada a Computadores e Smartphones iOS e Android

Victor Saqueto Kamiya, Prof Dr. Elvio Gilberto da Silva, Prof Me. Patrick Pedreira Silva, Prof. Me. Henrique Pachioni Martins.

Centro de ciências Exatas e sociais aplicadas – Universidade do Sagrado Coração (USC)
Caixa Portal 17011 – 160 – Bauru – SP - Brasil

Abstract. *With the evolution of technology, computers and other electronic devices are increasingly being used for business matters, and with that important data are stored on such devices. One of the main threats of information security is the loss or theft of important data. Among the objectives of Computational Forensics, is the analysis of electronic devices to recover deleted data. Based on this context, this work proposes to compare different data recovery software on Windows, Linux, iOS and Android in order to assist the user in choosing the most appropriate tool for data recovery in electronic storage devices.*

Resumo. *Com a evolução da tecnologia, computadores e outros aparelhos eletrônicos estão sendo cada vez mais usados para assuntos de trabalho, e com isso dados importantes estão sendo guardados nesses aparelhos. Uma das principais ameaças da segurança da informação é a perda ou roubo de dados importantes. Dentre os objetivos da Perícia Forense Computacional, está a análise de dispositivos eletrônicos a fim de recuperar dados apagados. Com base neste contexto, este trabalho propõe a comparação entre diferentes softwares de recuperação de dados nas plataformas Windows, Linux, iOS e Android, a fim de auxiliar o usuário na escolha da ferramenta mais adequada para a recuperação de dados em dispositivos de armazenamento eletrônico.*

1. Introdução

A primeira geração de computadores modernos surgiu em 1946, nessa época os computadores eram enormes e tinham como principal característica, o uso de válvulas eletrônicas, e todos os programas eram escritos diretamente na linguagem de máquina. (GUGIK, 2009).

Des de então, a técnologia evoluiu muito, computadores deixaram de usar válvulas eletronicas, diminuiram de tamanho e aumentaram sua capacidade de processamento, o advento da internet conectou pessoas de todo o mundo e celulares passaram a ser um aparelho indispensavel que além de ligações também possuem diversas outras aplicações.

Mas com toda essa facilidade que a técnologia trouxe, também surgiram problemas relacionados a segurança de dados importantes.

Uma das ameaças que podem colocar em risco a segurança da informação, seja por falha humana ou técnica, é a perda de dados, que pode levar a consequências

catastróficas, além disso, outro risco vem por meio de usuários mal intencionados que tem o objetivo de roubar esses dados. Com a expansão da Internet, computadores e outros dispositivos eletrônicos estão sendo usados para cometer crimes digitais. E-mails que tentam ludibriar o usuário e fazer com que as vítimas instalem um programa em seu computador que será usado para obter seus dados é apenas um exemplo básico de uma das técnicas que são usadas para roubar dados desejados. Com isso, o uso de provas eletrônicas está cada vez mais envolvido em crimes digitais. Afonso (2013).

Softwares de recuperação de dados são fundamentais para a resolução de crimes digitais envolvendo dados apagados de HDs, celulares ou qualquer outro dispositivo de armazenamento de dados.

Com base nesse contexto, este trabalho tem o objetivo de analisar softwares de recuperação de dados e realizar comparações entre softwares diferentes na mesma plataforma e comparações do mesmo software entre plataformas diferentes, visando auxiliar o usuário na escolha da ferramenta mais adequada para a recuperação de arquivos deletados em dispositivos de armazenamento que trabalhem com Windows ou Linux e smartphones que utilizem os sistemas operacionais iOS ou Android.

2. Metodologia

No trabalho, foi pesquisado um pouco sobre a historia e evolução do computador e do cellular e também sobre as plataformas Windows, Linux, iOS e Android, além de falar sobre crimes digitais e Pericia Forense Computacional.

Para o desenvolvimento deste trabalho, foram utilizados um computador com windows 7, no mesmo computador foi instalada uma maquina virtual simulando com Linux, e para os testes em smartphones foram utilizados um Iphone 4S e um Samsumg Ace.

Foram utilizados cinquenta arquivos de imagens (“.JPEG”), cinquentar arquivos de som (“.MP3”), cinquenta arquivos de texto (“.DOC”) e cinquenta arquivos de video (“.MP4”) totalizando duzentos arquivos ao todo, que foram salvos em uma partição do HD que foi formatada e posteriormente executados os softwares de recuperação de dados.

A seguir, a Tabela 1 mostra os softwares utilizados e os sistemas operacionais nos quais os softwares funcionam, nela é possível perceber as comparações que foram feitas na vertical, comparando o mesmo software em plataformas diferentes e na horizontal, comparando vários softwares em plataformas diferentes.

Tabela 1 - Plataformas e seus respectivos softwares de recuperação de dados.

Software	iOS	Android	Windows	Linux
TestDisk				
Undelete Plus				
Remo Recover				
Wondershare Dr. Fone				
Data Recovery Wizard				
Foremost				

Fonte: Elaborada pelo autor (2014).

Apesar de nenhum software ter conseguido recuperar 100% dos arquivos, quase todos tiveram um desempenho relativamente bom, recuperando a maior parte dos arquivos apagados durante a formatação do HD.

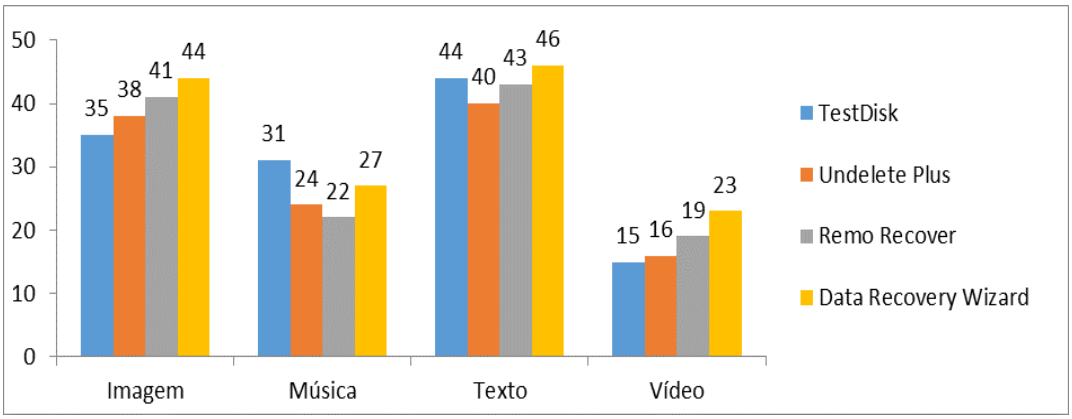
3. Resultados

Após a realização dos testes, os resultados obtidos foram colocados em uma tabela no excel para realizer as comparações propostas no trabalho.

Com exceção do Wondershare Dr. Fone que em sua versão grátis não permite de fato a recuperação de arquivos, todos softwares utilizados nos testes conseguiram recuperar a maioria dos arquivos apagados.

A Tabela 2, mostra a comparação feita entre os softwares utilizados na plataforma Windows, que são: TestDisk, Undelete Plus, Remo Recovery e Data Recovery Wizard, nessa comparação é possível notar que o software com melhor desempenho foi o Data Recovery Wizard, que apesar de não ter conseguido recuperar tantos arquivos de musica quanto o TestDisk, ele superou todos outros softwares na recuperação de imagens, videos e textos.

Tabela 2 – Comparação entre softwares na plataforma Windows.

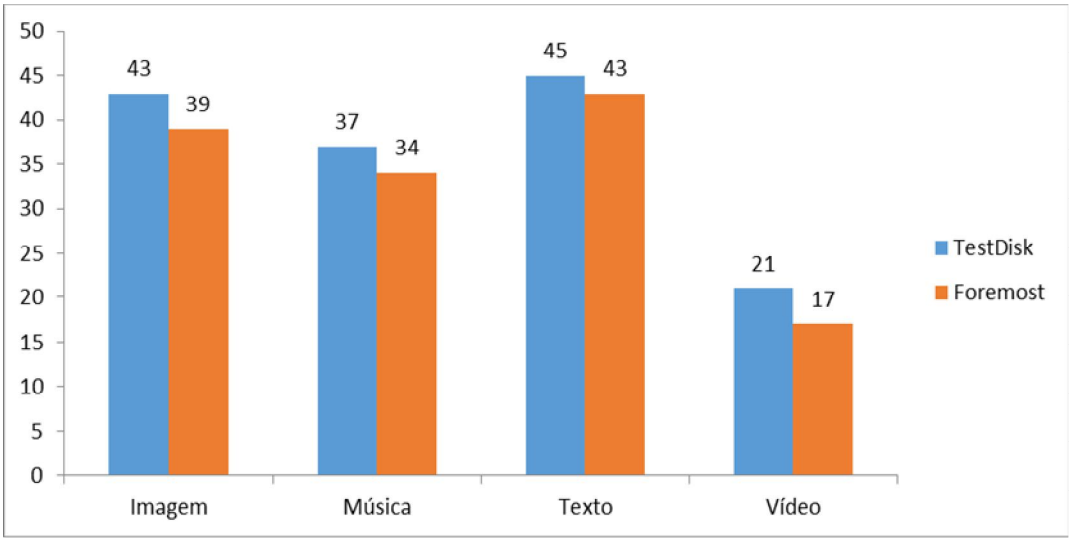


Fonte: Elaborada pelo autor. (2014).

Para todas comparações feitas foram construidas tabelas mostrando quantos arquivos de cada tipo foram recuperados em cada software e em cada plataforma, tornando possível analisar qual software atende melhor as necessidades do usuário.

Na Tabela 3 é possível obsrvar uma comparação feita desse mesmo modo, só que dessa vez para a plataforma Linux, onde foram testados os softwares TestDisk e Foremost.

Tabela 3 – Comparação entre softwares na plataforma Linux.



Fonte: Elaborada pelo autor. (2014).

Aqui também é notável que ambos softwares tiveram um bom desempenho, mas o TestDisk foi um pouco melhor, conseguindo recuperar mais arquivos que o Foremost.

4 Considerações Finais

Com o crescente número de informações digitais em aparelhos eletrônicos, é de extrema importância o uso de softwares de recuperação de dados pois a possibilidade de perda ou roubo de dados importantes para o usuário é muito alta.

Durante os testes foi possível notar que softwares que obtiveram melhor desempenho, também levaram um pouco mais de tempo para realizer a recuperação dos arquivos.

Um ponto interessante é a dificuldade que se tem em apagar um arquivo completamente de um HD ou outro dispositivo de armazenamento de dados, uma vez que atualmente cada vez mais ferramentas de recuperação de dados como as testadas nesse trabalho, são desenvolvidas.

Infelizmente não foi possível realizer uma comparação utilizando o software Wondershare Dr. Fone, pois em sua versão grátis, ele escaneia o dispositivo em busca de arquivos apagados mas não permite realizer a recuperação de fato.

Referencias

AFONSO, Raphael Pinheiro. Perícia forense computacional aplicada a dispositivos de armazenamentos e smartphones. 2013. 86 f. Trabalho de conclusão de curso (Graduação em Ciência da Computação) - Universidade do Sagrado Coração, Bauru, 2013.

GUGIK, Gabriel. A história dos computadores e da computação. Tecmundo, 2009. Disponível em: <http://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm>. Acesso em: 15 abr. 2014.