

UNIVERSIDADE DO SAGRADO CORAÇÃO

RAFAEL SANTIAGO FRANCISCO

**ANÁLISE DE FERRAMENTAS DE RECUPERAÇÃO
DE DADOS E PERÍCIA FORENSE COMPUTACIONAL
APLICADA EM AMBIENTE WINDOWS, LINUX,
SMARTPHONES IOS E ANDROID**

BAURU
2016

RAFAEL SANTIAGO FRANCISCO

**ANÁLISE DE FERRAMENTAS DE RECUPERAÇÃO
DE DADOS E PERÍCIA FORENSE COMPUTACIONAL
APLICADA EM AMBIENTE WINDOWS, LINUX,
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
2016

Francisco, Rafael Santiago

F8197a

Análise de Ferramentas de Recuperação de dados e Perícia Forense Computacional Aplicada em Ambiente Windows, Linux, Smartphones Ios e Android / Rafael Santiago Francisco. -- 2016.
82f. : il.

Orientador: Prof. Dr. Elvio Gilberto da Silva.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade do Sagrado Coração – Bauru – SP.

1. Perícia Forense Computacional. 2. Recuperação de Dados. 3. Smartphones. 4. Computadores. I. Silva, Elvio Gilberto da. II. Título.

RAFAEL SANTIAGO FRANCISCO

**ANÁLISE DE FERRAMENTAS DE RECUPERAÇÃO DE DADOS E
PERÍCIA FORENSE COMPUTACIONAL APLICADA A
COMPUTADORES E SMARTPHONES IOS E**

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, 6 de dezembro de 2016.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus pela saúde e disposição que tem me dado, iluminando meu caminho em todo desenvolvimento deste trabalho.

Aos meus pais Gilson Francisco e Meire Ferreira Santiago Francisco, pelo apoio, confiança, educação, amor, carinho e ajuda em todos os sentidos.

A minha querida namorada Larissa Bergamo, pela compreensão, pelo carinho, pela paciência com minhas ausências.

Ao meu orientador Elvio Gilberto da Silva, por me aceitar como orientando e pelo total apoio, dedicação, atenção e aprendizado.

Aos professores Henrique e Patrick, pela ajuda na elaboração e ajustes no trabalho.

Agradeço, também, aos meus verdadeiros amigos, pela companhia, pela amizade que sempre me ajudaram nos momentos em que necessitei.

RESUMO

O desenvolvimento tecnológico proporciona à sociedade cada vez mais comodidades e vantagens em todos os aspectos da vida moderna. Os acessos à Internet aumentam a cada dia, provenientes de organizações, governamentais ou não, ou simplesmente de usuários comuns, tendo em vista o nível cada vez maior de usabilidade de recursos computacionais. *Smartphones*, *tablets* e telefones celulares fazem parte de uma realidade que há poucos anos atrás não existia. Atualmente existem milhares de pessoas utilizando essas tecnologias. O uso dessas tecnologias agregadas aos serviços disponibilizados pelas operadoras de telefonia celular e a constante evolução do *hardware* disseminada pelos fabricantes de aparelhos, faz com que os atuais equipamentos tornem-se um valioso repositório de informações. Do ponto de vista da perícia forense, esses equipamentos tornaram-se um grande desafio na busca de arquivos e informações do proprietário, que podem assim materializar um delito ou simplesmente comprovar o seu envolvimento em atos que estejam em investigação policial ou empresarial. É com o objetivo de solucionar tais problemas, que surge a computação forense. O objetivo deste trabalho foi analisar softwares de perícia forense computacional para auxiliar o usuário na escolha da ferramenta mais adequada para a recuperação de arquivos deletados em dispositivos de armazenamento com os sistemas operacionais Windows e Linux, e smartphones com sistema operacional Android e iOS, os quais não possuem a mesma facilidade de acesso ao seu hardware comparado a um desktop ou notebook, tornando assim muitas vezes o processo invasivo e com alto grau de complexidade. Para atingir o objetivo proposto foram utilizadas as ferramentas “Recuva”, “MiniTool”, “Remo Recover”, “DiskDigger”, “Wondershare Dr. Fone”, “Scalpel” e “ExtUndelete”.

Palavras-Chave: Perícia Forense Computacional. Recuperação de Dados. Smartphones. Computadores.

ABSTRACT

The technological development provides society more and more amenities and advantages in every aspect of the modern life. The accesses to the Web rise daily, steaming from organizations, governmental or not, or simply from common users, having in sight the growing level of usage of the computational resources. Smartphones, tablets and cell phones are part of a reality which, few years ago, did not exist. Nowadays there are thousands of people using these technologies. The use of these technologies put together with the services made available by the cell phone operators and the constant evolution of the hardware, disseminated by the appliance manufacturers, makes the current equipment a valuable repository of information. From the forensic expertise point of view, these equipments have become a great challenge in the search of files and informations of the user. Which may then materialize a crime or simply prove its involvement in actions which are being under police or company investigation. It is with the goal of solving such problems that the forensics computing emerges. The goal of this paper was to analyze computing forensic expertise softwares to help the user in the choice of the most adequate tool for the recovery of deleted files in storage devices with the Windows and Linux operational systems, and smartphones with and Android and iOS operational system, which do not have the same access facility to its hardware when compared to a desktop or a notebook, making the process, then, often, invasive and with a high complexity degree. To reach the proposed goal, the following tools were used "Recuva", "MiniTool", "Remo Recover", "DiskDigger", "Wondershare Dr. Fone", "Scalpel" e "ExtUndelete".

Keywords: Computing Forensic Expertise. Data Recovery. Smartphones. Computers.

SUMÁRIO

1 INTRODUÇÃO	12
2 OBJETIVOS	14
2.1 OBJETIVO GERAL	14
2.2 OBJETIVOS ESPECÍFICOS	14
3 REVISÃO DA LITERATURA	15
3.1 HISTÓRICO DOS CELULARES	15
3.2 SISTEMA OPERACIONAL WINDOWS.....	15
3.3 SISTEMA OPERACIONAL LINUX	16
3.4 SISTEMA OPERACIONAL ANDROID	17
3.5 SISTEMA OPERACIONAL IOS.....	17
4.6 CONCEITOS DA PÉRICIA FORENSE COMPUTACIONAL.....	18
3.7 ETAPAS DA INVESTIGAÇÃO	19
3.7.1 Coleta	19
3.7.2 Exame.....	20
3.7.3 Análise	20
4.8 PROCEDIMENTOS BÁSICOS UTILIZADOS NA PERÍCIA FORENSE COMPUTACIONAL	21
3.8.1 Busca e apreensão	22
3.8.2 Transporte dos equipamentos apreendidos.....	23
3.8.3 Encaminhamento do material para a análise	23
3.8.4 Processo de identificação dos artefatos	23
3.8.5 Cadeia de custódia	24
3.9 FERRAMENTAS DE RECUPERAÇÃO DE DADOS.....	25
3.9.1 Recuva.....	25
3.9.2 Diskdigger	25
3.9.3 Remo Recover	26
3.9.4 Wondershare dr.fone	26
3.9.5 Scalpel	26
3.9.6 Extundelete.....	27
3.10 FERRAMENTAS DE COMPUTAÇÃO FORENSE.....	27
3.10.1 Forensictoolkit.....	27

3.10.2 Encase.....	27
3.10.3 Helix.....	28
3.11 TÉCNICAS ANTI-FORENSE	28
3.11.1 Limpeza de rastros	28
3.11.2 Criptografia	29
3.11.3 Esteganografia.....	29
3.11.4 Uso de rootkits.....	30
4 TRABALHOS CORRELATOS.....	31
5 METODOLOGIA	33
5.1 TESTES FEITOS PARA RECUPERAÇÃO DE DADOS.....	35
5.1.1 Recuva.....	36
5.1.2 Minitool	40
5.1.3 RemoRecover.....	42
5.1.4 DiskDigger	44
5.2 SOFTWARES UTILIZADOS PARA RECUPERAÇÃO NO SISTEMA OPERACIONAL ANDROID	46
5.2.1 Remo Recover for Android	46
5.2.2 Diskdigger	48
5.2.3 Wondershare Dr. Fone	50
6.3 SOFTWARES UTILIZADOS PARA RECUPERAÇÃO NO SISTEMA OPERACIONAL IOS	53
6.3.1 Wondershare Dr. Fone	53
5.4 SOFTWARES UTILIZADOS PARA RECUPERAÇÃO NO SISTEMA OPERACIONAL LINUX.....	55
5.4.1 Scalpel.....	55
5.4.2 Extundelete.....	57
6 RESULTADOS.....	59
7 CONSIDERAÇÕES FINAIS	72
REFERENCIAS.....	74
APÊNDICE A – TABELAS DE RECUPERAÇÃO DE ARQUIVOS EM CADA SOFTWARE UTILIZADO.....	77
APÊNDICE B – TABELAS DE RECUPERAÇÃO DE ARQUIVOS EM CADA SISTEMA OPERACIONAL UTILIZADO.....	79

APÊNDICE C – TABELA DE RECUPERAÇÃO DE ARQUIVOS ENTRE OS SISTEMAS OPERACIONAIS UTILIZADOS.....80

APÊNDICE D – TABELA DE RECUPERAÇÃO DE ARQUIVOS POR TIPO DE ARQUIVOS.....80

LISTA DE ILUSTRAÇÕES

Figura 1 – Evolução das Telas Iniciais do Ios.	18
Figura 2 – Ciclo de uma Investigação.	21
Figura 3 - Mídias Removíveis mais Comuns.	22
Figura 5 - Plataformas E Seus respectivos Softwares de Recuperação de Dados. ...	35
Figura 6 – Arquivos Utilizados Para os Testes de Recuperação de Dados.	36
Figura 7 – Assistente do Software Recuva.	37
Figura 8 – Assistente do Software Recuva, Tela Para Escolha de Arquivos a Ser Recuperados.	37
Figura 9 – Assistente do Software Recuva, Tela para localizar os arquivos a Serem Recuperados.	38
Figura 10 – Assistente do Software Recuva, Tela para Iniciar a busca por arquivos apagados.	39
Figura 11 – Arquivos Encontrados Pelo Recuva.	40
Figura 12 – Assistente do Minitool.	40
Figura 13 – Fullscan Minitool.	41
Figura 14 – Arquivos Encontrados pelo Minitool.	41
Figura 15 – Tela Inicial do Remo Recover.	42
Figura 16 – Seleção de Arquivos a Serem Recuperados.	43
Figura 17 – Seleção de Arquivos a Serem Recuperados.	43
Figura 18 – Interface Inicial do Software Diskdigger.	44
Figura 19 – Tela onde o usuário pode Escolher as Opções de Busca.	45
Figura 20 – Arquivos Recuperados pelo Diskdigger.	45
Figura 21 – Tela Principal do Software Remo Recover para Android.	46
Figura 22 – Tela com as Partições do Smartphone no Remo Recover For Android.	47

Figura 23 – Tela com as opções de Busca do Remo Recover For Android.....	47
Figura 24 – Tela com os arquivos com possibilidade de Recuperação no Remo Recover For Android.	48
Figura 25 – Tela com a Leitura dos arquivos no Diskdigger.	49
Figura 26 – Tela com a Leitura dos arquivos no Diskdigger.	49
Figura 27 – Tela com os Arquivos Encontrados no Diskdigger.....	50
Figura 28 – Tela inicial do Wondershare Dr.Fone.....	51
Figura 29 – Wondershare Dr. Fone analisando o Android.	51
Figura 30 –Seleção de Arquivos a Serem Recuperados.....	52
Figura 31 –Pasta arquivos Recuperados.	53
Figura 32 – Tela Inicial do Wondershare Dr.Fone.....	54
Figura 33 – Wondershare Dr. Fone Analisando o Iphone.	54
Figura 34 –Seleção de arquivos a serem Recuperados.....	55
Figura 35 – Tela com saída de Amostra do Scalpel.....	56
Figura 36 – Tela com Saída de Amostra do Scalpel.	56
Figura 37 –Partição a Serem Recuperados.	57
Figura 38 – Extundelete Durante a Recuperação De Dados.	58
Figura 39 – Resultados Obtidos Pelo Software Diskdigger.....	59
Figura 40 – Resultados Obtidos Pelo Software Recuva.....	60
Figura 41 – Resultados Obtidos pelo Software: Minitool.....	61
Figura 42 – Resultados Obtidos Pelo Software: Remo Recover.....	61
Figura 43 – Tabela Gráfica de Recuperação do Remo Recover.....	62
Figura 44 – Tabela Gráfica de Recuperação do Diskdigger.....	63
Figura 45 – Tabela Gráfica de Recuperação do Wondershare Dr.Fone.	63
Figura 46 – Tabela Gráfica de Recuperação do Wondershare Dr.Fone.	64
Figura 47 – Tabela Gráfica de Recuperação do Extundelete.....	65

Figura 48 – Tabela Gráfica de Recuperação do Scalpel.....	65
Figura 49 – Comparação Entre Softwares na Plataforma Windows.....	66
Figura 50 – Comparação Entre Softwares na Plataforma Android.....	67
Figura 51 – Comparação Entre Softwares na Plataforma Linux.....	68
Figura 52 – Comparativos Entre os Sistemas Operacionais.	69
Figura 53 – Comparativos Entre os Sistemas Operacionais.	70
Figura 54 –Tabela Geral.	701

1 INTRODUÇÃO

A primeira geração de computadores modernos surgiu em 1946, e sua principal característica era o uso de válvulas, utilizando quilômetros de cabos, possuindo dimensões gigantes e atingindo temperaturas bem elevadas. Todas sua programação eram escrito na linguagem de máquinas (GUGIK, 2009).

Os primeiros aparelhos telefônicos surgiram com a finalidade de tornar a comunicação mais eficiente e fácil, a primeira empresa que mostrou o aparelho funcionando foi a Motorola em 1973. Os celulares não eram tão portáteis tinha dimensões quase 30 centímetros e pesavam em média 1kg (JORDÃO, 2009).

A tecnologia tem evoluído rapidamente, e cada vez mais as pessoas estão utilizando-a tanto para o lazer quanto para trabalho, conseqüentemente, pessoas mal intencionadas também tiram proveito dessa situação enganando e roubando dados, invadindo sistemas de empresas, desenvolvendo vírus, e vários outros crimes ligados a computação.

À medida que a tecnologia invade o mercado com uma extraordinária quantidade de periféricos, quase nunca compatíveis entre si, como *smartphones*, *tablets*, *notebooks*, *desktops* dentre outros, além de armazenamentos como cloud, pen drives, hd's externos, etc, tudo isso somado a enorme quantidade de redes sociais, que já atingem todo o planeta, como Facebook, Twitter, LinkedIn, etc., faz-se necessária uma especialização e conhecimentos para atuar na área, cada vez maiores.

Os computadores tornaram-se importantes para grande parte das atividades da vida atual, desde empresas ligadas à área relacionadas a saúde, empresas privadas e até mesmo para usuário domésticos. O grande avanço foi útil para benefícios de todos, os *smartphone* atualmente têm a mesma capacidade de realizar atividades de um computador, porém seu tamanho é extremamente reduzido facilitando seu manuseio e, assim, despertando o interesse de adquirir aparelhos celulares. Com estes grandes avanços, acaba abrindo portas para os Cybercrimes.

Cybercrimes traz grandes perigos a sociedade que vive com os crimes e as violência no cotidiano Cada vez tem se tornado frequente a invasão em computadores e dispositivos por criminosos mal intencionados que estão à procura de conseguir dinheiro e enganar o usuário se passando por uma instituição financeira. Os cybercriminosos utilizam canais para roubo como: senhas cartão de

crédito, envio de boletos de cobranças online, pagamento adiantado, transações bancárias não autorizadas ou cobranças de cartões de crédito (ASSIS, 2010).

Atualmente, os crimes virtuais estão cada vez mais presentes. O acesso à internet, tornou-se uma das principais ferramentas de novos crimes cometidos por pessoas que descobriram e aprenderam a utilizar softwares específicos para tal fim. Tais indivíduos se beneficiam pelo acesso anônimo que a Internet proporciona para praticar crimes, tornando fácil a ação de criminosos que buscam invadir sistemas, tanto para obter dados pessoais ou dados bancários. Devido á essa nova necessidade, surgiu a Perícia Forense Computacional.

A Perícia Forense computacional é uma área que está se desenvolvendo muito rapidamente graças à necessidade de instituições estarem atuando no combate aos crimes eletrônicos. Nessa área, são estudadas as formas de aquisição, prevenção, recuperação e análise de dados em dispositivos de armazenamento, e ao mesmo tempo, procura-se caracterizar crimes de informática de acordo com as evidências digitais encontradas no sistema invadido.

Em termos a Perícia Forense Computacional abrange todas as questões relacionadas aos crimes praticados na Internet ou fora dela, chamados cibercrimes. Estudando como coletar evidências de crimes e violações, analisar e documentar casos, esta ciência, relativamente nova, segue as principais metodologias internacionais usadas e adotadas por todos os países do mundo na investigação de crimes e delitos comuns.

A Computação Forense consiste, basicamente, no uso de métodos científicos para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidência digital. A aplicação desses métodos nem sempre ocorre de maneira simples.

Este trabalho acadêmico ambicionou contribuir, estabelecendo comparações entre diferentes ferramentas, com o intuito de verificar quais têm melhor desempenho na recuperação de dados.

2 OBJETIVO

A seguir serão apresentados os objetivos desta pesquisa.

2.1 OBJETIVO GERAL

Analisar *softwares* de perícia forense computacional sob o ponto de vista da recuperação de arquivos deletados em dispositivos de armazenamento com os sistemas operacionais Windows e Linux e smartphones com sistema operacional Android e iOS.

2.2 OBJETIVOS ESPECÍFICOS

- a) Efetuar um levantamento teórico sobre perícia forense computacional e ferramentas para recuperação de dados;
- b) Pesquisar *softwares* específicos de recuperação de dados nos ambientes Windows, Linux, Android e iOS;
- c) Investigar técnicas forenses de recuperação de dados;
- d) Levantar estratégias para análise periciais nos sistemas operacionais objetos de estudo desta pesquisa;
- e) Realizar a recuperação de dados em cada um dos sistemas operacionais estudados;
- f) Coletar resultados e analisá-los a fim de elaborar um quadro comparativo dos *softwares* analisados;

3 REVISÃO DA LITERATURA

A seguir apresenta-se um breve estudo, abordando tópicos relacionados a perícia forense e recuperação de dados.

3.1 HISTÓRICO DOS CELULARES

A invenção do telefone foi inspirada no funcionamento do telégrafo, que foi criado em 1835 e permitia a comunicação entre pontos distantes, porém esta comunicação era em códigos e não por sons. Em 1888 foi possível produzir as primeiras ondas de rádio, e assim, foi descoberto um método de transmitir informações por meio destas ondas. Desta forma a comunicação através de ondas de rádio ao passar do tempo foi aprimorada, dando o ponto de partida à comunicação via telefone fixo, e também ao que se transformaria posteriormente no telefone celular (PEIXOTO, 2007).

Segundo Peixoto (2007), a primeira ligação telefônica utilizando-se um aparelho portátil foi feita no dia 03 de abril de 1973 pela Motorola, o aparelho utilizado nesse telefonema possuía 25cm de comprimento e 7cm de largura e pesava um quilo, com uma bateria que se esgotava em 20 minutos.

Em 1993 surgiram os aparelhos celulares pequenos e baratos capazes de mandar mensagens, o famoso SMS (*short message servisse*), e com o tempo surgiram os celulares com cores, com capacidade de se conectar à internet, câmeras para tirar fotos e vídeos (JORDÃO, 2009).

3.2 SISTEMA OPERACIONAL WINDOWS

O Windows lançado em novembro de 1985 é um sistema operacional desenvolvido pela Microsoft, até então era necessário uso de comandos no MS-DOS para realização de algumas tarefas, e com desenvolvimento do Windows 1.0 foi possível utilizar o mouse para ter contato com a interface através de uma seta (MICROSOFT, 2015).

Assim, de acordo com autor citado anteriormente, o Windows começou a evoluir, e 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 apresentado, e juntamente com o

Windows 3.1 vendeu mais de 10 milhões de cópias nos 2 primeiros anos. Em 1995 o Windows 95 foi lançado obtendo um recorde de 7 milhões de cópias vendidas nas 5 primeiras semanas.

No ano 1998 surgiu o Windows 98, essa versão foi a primeira do Windows projetada especificamente para os usuários, que foi relatado como um sistema operacional “ótimo para trabalhar e jogar” (MICROSOFT, 2015).

Segundo a Microsoft (2015) foi lançado em 2001 os sistemas operacionais Windows XP, com disponibilidade em 25 idiomas. Um ato que aconteceu em 8 de Abril de 2014 foi o término do suporte para poder investir seus recursos do Windows XP, que foi lançado em 2001 e, por 12 anos, graças ao seu bom desempenho, e estabilidade foi o sistema operacional mais utilizado no mundo. Em 2006 a 2015 foram lançados novos sistemas operacionais: Windows Vista, Windows 7, Windows 8 e Windows 10 que atualmente são os sistemas operacionais mais utilizados em computadores pessoais do mundo.

3.3 SISTEMA OPERACIONAL LINUX

O software Linux, foi desenvolvido pelo finlandês Linus Torvalds, quando começou a estudar ciência da computação na Universidade de Helsinki na Finlândia, Após dois anos de estudo aproveitou o conhecimento que tinha obtido sobre linguagem C, para o desenvolvimento da sua própria implementação (ALECRIM, 2011).

Segundo o autor supracitado, em 1991, Linus Torvalds decidiu desenvolver um sistema operacional mais poderoso que o Minix, que era uma versão gratuita do Unix. Nesse ano Linus já disponibilizou a versão do Kernel 0.02, Linus continuou trabalhando em seu projeto até que em 1994, ele disponibilizou a versão 1.0 do Kernel, e no mesmo ano, Linus Torvalds disponibilizou abertamente seu projeto, somente programadores aderiam ao uso, pois só era possível a atualização através de linhas de comandos.

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

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

3.4 SISTEMA OPERACIONAL ANDROID

O sistema operacional Android foi criado em 2008, é a plataforma mobile mais popular do mundo, atualmente pertence à empresa da Google. Este sistema operacional baseado em Linux é projetado para dispositivos móveis (BARROS, 2015).

O Android se tornou grande arma do Google nos últimos anos, é extremamente popular, ganhou rapidamente grande público tanto com os modelos mais simples como os modelos tops de linha.

Fato curioso, todas as versões desse sistema operacional possuíram o nome de alguma comida, a versão mais atual Android 6.0.

3.5 SISTEMA OPERACIONAL IOS

O sistema operacional iOS foi produzido pela Apple no ano de 2007, sendo desenvolvido primeiramente para iPhones. Atualmente todos os aparelhos da Apple utilizam esse sistema. Em julho de 2008 foi lançado o “iPhone OS 2”, acompanhado com uma novidade, a Apple Store, que é uma loja online onde os usuários podem baixar e comprar adquirindo aplicativos e músicas. Um ano depois em 2009 foi lançado o “iPhone OS 3” trazendo ainda mais recursos que ainda faltava no IOS (TROYACK; YANG, 2013).

No ano de 2010 ocorreu uma alteração “iPhone OS” passou a se chamar “iOS”. Nessa época, o sistema da Apple já era bem conhecido por ser bastante seguro em relação à *malwares* e outros tipos de ameaças, quase totalmente bloqueado para desenvolvedores e *hackers*.

Nos anos de 2011, 2012 e 2013 foram lançados na ordem os iOS 5, 6 e 7, todos exibindo características novas e recursos atraindo a atenção como o Siri, por exemplo, que é um aplicativo que permite o usuário fazer várias tarefas por simples comandos de voz (TROYACK; YANG, 2013).

A versão mais atual do IOS hoje é o iOS 9.2.1. A Figura 1 ilustra a evolução da tela inicial de cada uma das versões do iOS até a versão 9.

Figura 1 – Evolução das telas iniciais do IOS.



Fonte: Tryack e Yung (2013).

Nota: Adaptado pelo autor.

4.6 CONCEITOS DA PÉRICIA FORENSE COMPUTACIONAL

A Perícia Computacional pode ser definida como um grupo de técnicas utilizadas para efetuar preservar, recuperar e adquirir evidências digitais processadas, armazenadas ou transmitidas por meios computadores e a internet.

Segundo Weyer (2011), o termo perícia forense está totalmente ligado ao mundo policial, e até pouco tempo não tinha vínculo com a computação. Mas devido a grande aumento do uso do computador e da internet, ocorreram novos crimes, e assim, a necessidade dessa área.

Existem vários exames forenses na área de informática os principais tipos de exames são os seguintes:

- a) **Exames em dispositivos de armazenamento computacional:** são os tipos de exames mais solicitados na computação forense, tratando de examinar arquivos, sistemas e *softwares* instalados em todo tipo de dispositivos de armazenamento eletrônico. Existem três fases para esse

tipo de exame, que são: formalização preservação, análise e extração (KAMIYA, 2014).

- b) **Exames em aparelhos de telefone celular:** assim como nos exames já citados, trata-se de um exame para extrair e analisar arquivos de telefones celulares (KAMIYA, 2014).
- c) **Exames e procedimentos em locais de crime de informática:** procedimentos que devem ser seguidos pelos peritos no local do crime para não deteriorar equipamentos e nem modificar ou apagar provas eletrônicas (KAMIYA, 2014).

É importante reforçar que dependendo das circunstâncias, as informações coletadas podem ter sido manipuladas de forma a induzir o perito a tirar conclusões erradas sobre o caso. Sendo assim, é notória a responsabilidade e a importância do perito a ele confiada (WEYER, 2011).

3.7 ETAPAS DA INVESTIGAÇÃO

As fases de condução de um processo de investigação podem-se dividir em quatro etapas, tais como: coleta dos dados, exame dos dados, análise das informações, quais serão descritas a seguir.

3.7.1 Coleta

Almeida (2016) destaca que a fase de coleta de dados representa basicamente a organização e recuperação de todas as informações contidas na cópia dos dados adquiridos, ou seja, todas as ações deverão ser efetuadas no espelho ou na imagem do disco, mantendo o material original intacto e protegido. Essa etapa é de grande valor para o processo investigatório, pois as análises dos indícios serão realizadas a partir de seu resultado obtido.

Assim, é dividido os discos rígidos em camadas, cuja a mais superficial possui os arquivos visíveis aos usuários de computador, enquanto que nas camadas mais internas encontramos os arquivos ocultos, criptografados, temporários e apagados, além de fragmentos de arquivos entre outras informações (ALMEIDA, 2016).

Segundo o autor supracitado, as informações deletadas podem ficar intactas por meses, ou até mesmo, por anos devido ao esquema de alto desempenho do sistema de arquivos, que evita movimentos do cabeçote de disco preservando os dados agregados. Isso não apenas reduz a fragmentação do conteúdo de um arquivo individual, como também reduz retardos ao se percorrer diretórios para acessar um arquivo.

3.7.2 Exame

O ato de extrair, localizar e filtrar somente as informações que possam contribuir, de forma positiva, em uma investigação ocorre nesta etapa, Considera-se esta, a etapa mais trabalhosa do processo de investigação criminal, principalmente pela quantidade de diferentes tipos de arquivos existentes, o que exige que o perito esteja ainda mais concentrado e preparado a identificar e recuperar esses dados. O perito ao identificar que são arquivos maliciosos, pode contar com a utilização de ferramentas que possibilitem filtrar essas extensões para diminuir seu trabalho (ALMEIDA, 2016).

3.7.3 Análise

Os vestígios encontrados consistem no exame dos arquivos extraídos nas etapas anteriores, a fim de identificar evidências digitais presentes no material examinado que tenham relação a investigado. Essa relação se estabelece através das exigências elaborada pela autoridade solicitante presente no laudo. Tendo a necessidade de ser óbvio e específico, pois analisar individualmente todo o conteúdo do dispositivo de armazenamento computacional tende a ser inviável, gastando um tempo muito vasto do perito nos exames forenses. O uso de programas que emulem uma máquina virtual pode ser muito interessante para entender as operações efetuadas pelos usuários dos computadores a serem examinados. Essa emulação é feita sem modificar os dados das cópias realizadas na fase de preservação (ALMEIDA, 2016).

Portanto, ao cumprir a fase de análise dos dados, cabe ao perito realizar a padronização do estudo efetuado através da elaboração do laudo pericial, indicando

o resultado e apresentando as evidências digitais encontradas nos materiais examinados. No laudo devem constar as principais operações realizadas.

A Figura 2 ilustra o ciclo das etapas da investigação.

Figura 2 – Ciclo de uma investigação.



Fonte: Neukamp (2015).

4.8 PROCEDIMENTOS BÁSICOS UTILIZADOS NA PERÍCIA FORENSE COMPUTACIONAL

O próprio procedimento policial que antecede a investigação é de grande importância para que se alcance um resultado final satisfatório. O controle aos procedimentos básicos de um caso desde o seu início até o fim é o mínimo necessário para garantir o sucesso (COSTA, 2003 citado por DAMACENA, 2014).

Durante a realização do trabalho o perito pode deparar com situações questionáveis que venham danificar, e até mesmo dificultar totalmente, o processo de análise pericial (DAMACENA, 2014).

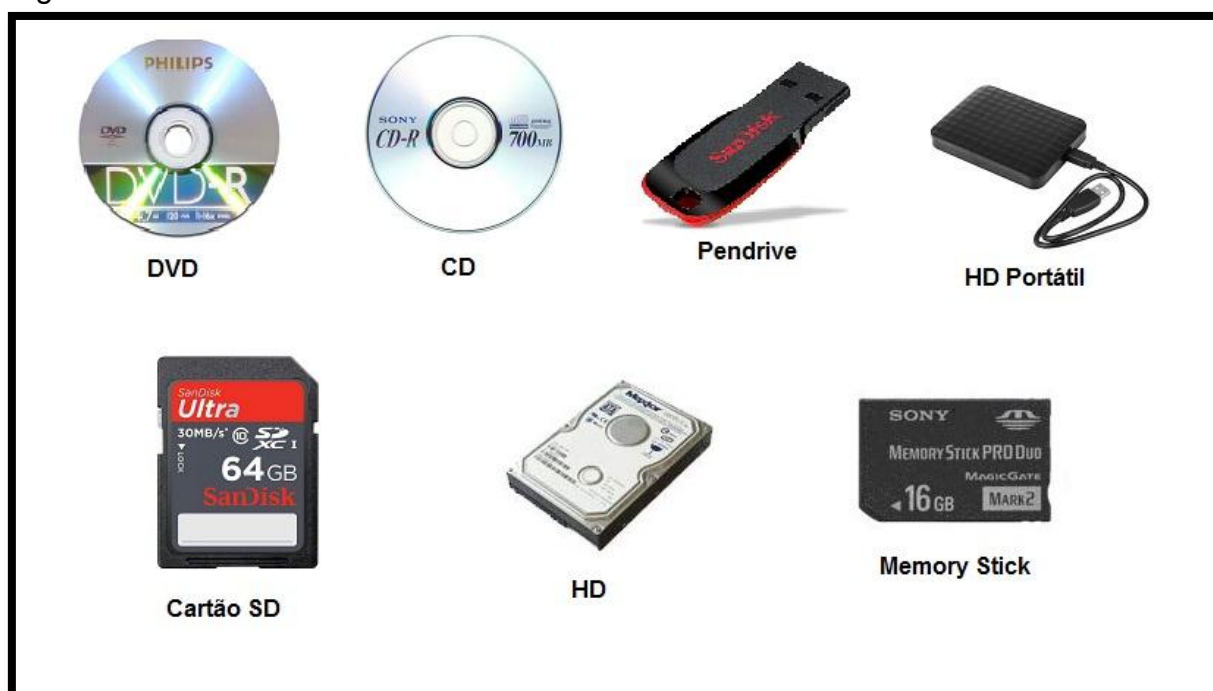
Os procedimentos considerados básicos que orientam a direção correta de um caso, do começo até o fim, e que podem determinar o sucesso da investigação, do ponto de vista da preservação das provas, serão expostos a seguir (DAMACENA, 2014).

3.8.1 Busca e apreensão

Segundo Damacena (2014), busca e apreensão consiste em reunir o máximo de objetos com possível valor pericial. É necessário que o perito computacional tenha eficiência técnica para efetuar a busca por dados em inúmeros dispositivos computacionais, que vão de um simples computador até um servidor, passando por diversos dispositivos como câmeras portáteis e celulares.

O perito computacional que esteja cumprindo o seu trabalho na fase de busca e apreensão deve ser cauteloso a todo e qualquer dispositivo que poderá formar em fonte de dados e em seguida em informações valiosas. Antes de sair do local da apreensão, o perito deve realizar uma busca detalhista por mídias removíveis, as quais podem conter dados que futuramente possam oferecer evidências valiosas ao caso. (DAMACENA, 2014). A Figura 3 mostra os dispositivos de armazenagem mais frequentemente encontrados.

Figura 3 - Mídias removíveis mais comuns.



Fonte: Elaborada pelo autor.

Como pode ser observado na Figura 3, qualquer material que seja dispositivo de armazenagem de dados pode constituir-se em uma fonte de informação.

3.8.2 Transporte dos equipamentos apreendidos

De acordo com Costa (2008), para que a proteção aconteça, é necessário o cuidado ao transportar sistemas que constituirão as fontes de informação no processo de análise; todos os artefatos devem ser transportados em uma temperatura baixa, em locais protegidos por materiais que absorvam impacto, como plástico bolha. Manuais e documentos devem ser embalados em sacos plásticos ou protegidos de outra forma. Apesar de hoje em dia estes componentes serem bem menos sensíveis ao manuseio e transporte, deve-se ter muito cuidado no manejo do material apreendido.

Ainda de acordo com o autor anteriormente citado, as caixas contendo o material de análise devem ser fixadas no veículo de transporte para que não ocorra pancadas ou tombos, podendo seriamente danificar e comprometer o trabalho pericial.

3.8.3 Encaminhamento do material para a análise

Após recebimento dos equipamentos computacionais e as mídias removíveis, o responsável pela ação policial deve preparar os documentos necessários e enviar todo material apreendido o mais rápido possível ao laboratório para análise forense. Quanto antes for iniciado os trabalhos maiores a probabilidade de sucesso na investigação (DAMACENA, 2014).

Antes de se realizar qualquer ação de inicialização do sistema operacional deve-se primeiro efetuar as normas adequadas para a realização pericial. A inicialização não controlada do sistema pode danificar os dados armazenados, como, alterar a sequência das evidências e conseqüentemente inibir a caracterização de uma prova (DAMACENA, 2014).

3.8.4 Processo de identificação dos artefatos

A identificação dos artefatos consiste em uma etapa em documentar a fase de investigação desde seu início, apontando em documento o órgão solicitante da perícia, as características do material e a data do recebimento, assim como os

dados referentes ao perito responsável pelo acontecimento, hora e data, e o fim dos trabalhos realizados de cada exame (DAMACENA, 2014).

A documentação detalhada sobre cada objeto adquirido e periciado e os resultados obtidos, são cruciais para a elaboração de um laudo pericial adequado (MELO, 2009 citado por DAMACENA, 2014).

3.8.5 Cadeia de custódia

Segundo Freitas (2006), a cadeia de custódia mostra e prova onde as evidências se encontravam no determinado momento, e quem era responsável por elas durante a investigação da perícia.

Caso a defesa questione a veracidade das evidências, alegando possíveis alterações ou substituições, existe o que se conhece como cadeia de custódia. Trata-se de uma documentação do histórico de evidência (FREITAS, 2006). A Figura 4 mostra um exemplo do documento.

Figura 4 – Formulário de Cadeia de Custódia.

Caso Num.: 053203		Pag.: 01		De: 05	
MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO					
Item:	Descrição:				
00001	HD de Notebook com 80GB de capacidade				
Fabricante:	Modelo:	Num. de série:			
TOSHIBA	MK4026GAX	85MC7639T			
DETALHES SOBRE A IMAGEM DOS DADOS					
Data/Hora:	Criado por:	Método usado:	Nome da Imagem:	Partes:	
20/5/2007 15:30	Paulo A. Neukamp	dcfidd	053203_01.dd	01	
Drive:	HASH:				
Disco Completo	d243367072088feae98364977441d736				
CADEIA DE CUSTÓDIA					
Seqüência:	Data/Hora:	Origem:	Destino:	Motivo:	
001	Data:	Nome/Org.:	Nome/Org.:	Investigação sobre denúncia de Pedofilia	
	20/5/2007	Sigilo	Lab. Perí. Unisinos		
	Hora:	Assinatura:	Assinatura:		
	16:00				

Fonte: David (2013).

Como pode ser observado na Figura 4, além de registrar as informações sobre o equipamento apreendido, o formulário também guarda informações indispensáveis sobre quem, como e onde realizou-se tal apreensão.

3.9 FERRAMENTAS DE RECUPERAÇÃO DE DADOS

A seguir serão apresentados alguns softwares utilizados para recuperação de arquivos deletados.

3.9.1 Recuva

O Recuva é um dos programas gratuitos para recuperação de arquivos que foram deletados acidentalmente ou eliminados da lixeira no Windows, que precisa voltar no tempo e recuperar um arquivo que foi apagado por engano. Ele faz uma varredura em buscas de arquivos nos HDs do computador, em busca de vestígios de dados que possam ser restaurados, e utilizados novamente. O Recuva oferece ainda um recurso para refinar a pesquisa dos dados apagados, com isso, o usuário consegue configurar o *Software* para buscar, tais como: Imagens, músicas, documentos, vídeo, arquivos compactados e e-mails. Após ter sido encontrado os arquivos, o Recuva mostra detalhes do arquivos, como data de modificação e tamanho (INFODICAS, 2012).

3.9.2 Diskdigger

O DiskDigger é uma ferramenta gratuita feita na medida para usar o sistema para recuperar fotos e arquivos perdidos acidentalmente. O DiskDigger faz uma análise no disco, detectando arquivos deletados, a exibição pode ser dos arquivos isoladamente, ou através de uma árvore de diretórios, oferece a possibilidade de buscar pelo nome, facilitando o trabalho de procura pelo arquivo. Funciona para Windows e Android, mas com versão específica para Windows e outra versão específica para aparelhos que utilizam Android (ALVES, 2014).

3.9.3 Remo Recover

O Remo Recover é um *software* de recuperação de dados perdidos e apagados do computador, *notebook* ou qualquer outra mídia de armazenamento. Funciona para as plataformas Windows e Android, recuperando dados de vídeo, áudio, som, texto, além de ser capaz de recuperar pastas inteiras que foram deletadas. (HAMMERSCHMIDT, 2013).

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

3.9.4 Wondershare dr.fone

O Wondershare Dr.Fone é um *software* de recuperação de dados que recupera arquivos de som, vídeo, imagens e texto. Esse programa também recupera mensagens e contatos do *smartphone*. 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 específica para aparelhos que utilizam iOS e outra versão específica para aparelhos que utilizam Android (WONDERSHARE, 2016).

Este *software* é pago, mas é possível utilizar uma versão de testes gratuitamente.

3.9.5 Scalpel

Segundo Almeida (2009), Scalpel é uma ferramenta poderosa que consegue recuperar, com um bom índice de sucesso, ficheiros que foram apagados acidentalmente. Também é possível identificar e reconstruir arquivos em partições corrompidas, em espaço não alocado, mesmo após a instalação de um novo sistema operacional, desde que os blocos de dados necessários ainda existam, funciona especificamente em Linux.

3.9.6 Extundelete

O Extundelete é um *software* de recuperação de dados, recupera arquivos apagados contidos em sistemas de arquivos ext3 e ext4, amplamente utilizados em sistemas Linux, um ótimo *software* para recuperação de dados (FERREIRA, 2014).

O programa é inteiramente comandado por comandos “DOS”, o que dificulta sua utilização por pessoas com menos conhecimento de informática.

3.10 FERRAMENTAS DE COMPUTAÇÃO FORENSE

Além das ações de reunir cópias de segurança de evidências, documentação, pesquisa e outros, o investigador precisa de *softwares* específicos para realizar tarefas forenses. A seguir são apresentadas algumas ferramentas.

3.10.1 Forensictoolkit

Neste *software* é possível encontrar as principais funcionalidades para a realização de exames forenses em dispositivos de armazenamento de dados. Com esta ferramenta é possível criar imagens, analisar o registro, conduzir uma investigação, decodificar os arquivos, recuperar senhas de arquivos criptografados, identificar esteganografia e construir um relatório. Como pode ser visto, possui vários recursos que podem ser utilizados em todas as fases de um exame computacional forense (VARGAR, 2009).

3.10.2 Encase

A EnCase é uma ferramenta que possui diversos recursos que ajudam o profissional no seu trabalho de exames de perícia em Computação Forense em dispositivos de armazenamento de dados. Através deste *software* também é possível recuperar imagem (HENRIQUE, 2013).

3.10.3 Helix

A ferramenta Helix é uma ferramenta que possui opções para recuperação de dados, listagem de processos, análise de memória, recuperação de credenciais de acesso como logins e senhas, entre diversos outros itens importantes durante uma análise pericial (SAMPAIO, 2013).

Através do Helix é possível descobrir quais aplicativos estão sendo executado no momento em que a perícia no equipamento é realizada, isso é de grande importância no caso de se estar procurando um *malware*, tornando possível uma análise no aplicativo através de ferramentas que possibilite descobrir o que este aplicativo faz, e como ele se comporta, buscando um entendimento mais profundo.

3.11 TÉCNICAS ANTI-FORENSE

As técnicas Anti-Forenses representam um campo relativamente novo, e enquadram vários tipos de atividades, tais como: limpeza de registros, ataques contra ferramentas forenses, entre outras, as quais serão apresentadas a seguir.

3.11.1 Limpeza de rastros

Diversos softwares disponíveis podem ser preparados para zerar e sobrescrever arquivos de dados. Assim, essas ferramentas utilizam múltiplos métodos de escritas, e conseqüentemente qualquer tentativa de recuperação se torna inviável ou até impossível, de ser executado (KESLER, 2007).

Entretanto, os *softwares* utilizados pelos criminosos para limpar seus rastros não são inteiramente perfeitos, e podem criar um caminho de vestígios adicionais (CARVEY, 2007).

Portanto, muitas destas ferramentas não desempenham tudo o que prometem fazer, e frequentemente deixam rastros para trás como nome e, data de criação, tamanho do arquivo e exclusão dos arquivos removidos, entre outros dados que podem encontrar os invasores (BURKE, 2006).

3.11.2 Criptografia

Criptografia, de origem grega que significa “escrita secreta”, é uma técnica utilizada para escrever em códigos, transforma a informação em sua forma original e legível para um texto confuso, buscando garantir a privacidade do dado original (ALMEIDA, 2011).

Ainda segundo o autor anteriormente citado, essa técnica é muito utilizada na transferência de dados frágil através de comunicação insegura, pois, mesmo que pessoas não autorizadas consigam visualizar o texto criptografado, apenas o dono da chave criptográfica conseguirá realizar o processo inverso e chegar aos dados originais.

A criptografia esconde o conteúdo de uma mensagem, tornando-a confuso para pessoas não autorizadas, mas a existência da mensagem é conhecida. Classificada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que se pode usar para proteger dos riscos.

Na computação, as técnicas mais conhecidas envolvem o conceito de chaves, as chamadas chaves criptográficas. Trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação (ALECRIM, c2009, p. 22).

3.11.3 ESTEGANOGRAFIA

A esteganografia é uma palavra de origem grega e significa “escrita encoberta”. É o uso de técnicas para fazer com que uma forma escrita seja disfarçada em outra, a fim de mascarar o seu verdadeiro sentido, tendo como objetivo a comunicação em segredo (ALMEIDA, 2011).

Os dois métodos (criptografia e esteganografia) podem ser combinados para aumento da segurança. Por exemplo, pode-se criptografar uma mensagem e em seguida, utilizar a técnica de esteganografia, trocando-se os bits menos significativos de uma imagem digitalizada pelos bits da mensagem criptografada, e então transmitir a imagem. Se a imagem for interceptada, o adversário primeiro precisará descobrir a mensagem dentre os bits da imagem, e, após isso, poderá tentar de criptografá-la (KOBUSZEWSKI, 2004, p. 52).

Segundo Coutinho (2008), criptografia com esteganografia não se deve confundir, pois o primeiro esconde o conteúdo de uma mensagem alterando ilegível, mas a existência da mensagem é conhecida, pois oculta o significado da mensagem, já o segundo oculta a existência da mensagem, esconde o fato de que a mensagem existe.

3.11.4 Uso de rootkits

A partir do ano de 1997 surgiram os rootkits. Esses programas conseguem modificar dinamicamente os módulos do núcleo do sistema operacional. Sendo assim, estes programas maliciosos modificam a funcionalidade de um sistema sem a necessidade de uma reinicialização do mesmo (ROHR, 2010).

De acordo com Barwinski (2009), os rootKits são programas desenvolvidos para ocultar a presença de ataques e permitir acesso futuro em sistema operacional, e também utilizada para obter privilégios de super-usuário.

Segundo McClure, Scambray e Kurtz (2003), cada rootkits normalmente consiste em quatro grupos de ferramentas, todas organizadas para o tipo de plataforma e versão. Sendo capaz de ocultar um processo, arquivo ou chave do registro.

Portanto, cada rootkit pode se instalar em diversos níveis do sistema, em cada nível, o rootkit se estabelece de uma forma diferente e requer estratégias diferenciadas para ser detectado (MCCLURE; SCAMBRAV; KURTZ, 2003).

4 TRABALHOS CORRELATOS

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

É possível encontrar algumas ferramentas para recuperação de dados para as diversas plataformas existentes, entretanto, não se encontram pesquisas ou artigos científicos com uma análise mais profunda das técnicas utilizadas, bem como dos resultados obtidos. Encontram-se apenas descrições simples sobre o funcionamento destas ferramentas e resultados genéricos no próprio site dos desenvolvedores.

Dessa forma, a intenção deste trabalho é contribuir com informações, análises e resultados relevantes sobre recuperação focando em ambiente Windows, Linux, *Smartphones* IOS e Android.

Os trabalhos correlatos pesquisados para o desenvolvimento desta proposta foram:

- a) No que diz respeito a técnicas utilizadas para coleta e análise de vestígios digitais, já foram desenvolvidos trabalhos semelhantes a este como, por exemplo, o trabalho de Almeida (2011, 46 p.) que visa descrever a Perícia Forense Computacional, bem como as técnicas empregadas na extração e análise dos dados de mídias de armazenamento digital e os aspectos jurídicos envolvidos na atuação do perito.
- b) No que tange a fundamentação teórica da perícia forense computacional, conceitos, etapas de uma investigação, procedimentos e ferramentas utilizadas por peritos para investigar um cenário de crime computacional, já foram desenvolvidos trabalhos semelhantes a este como, por exemplo, o trabalho de Damanena (2014, 120 p.) aborda também o tema computação em nuvem, os conceitos, características, modelos e provedores. Por fim, mostra um estudo de caso para verificar se conteúdo de arquivos disponibilizados em provedores de

armazenamento em nuvem são alterados durante o processo de upload, armazenamento e download.

- c) Na parte tocante ao desenvolvimento da tecnologia, crimes virtuais, roubo, perda de dados, dependência por aparelhos eletrônicos, e a importância da segurança da informação e a perícia forense, que tem o objetivo de proteger dados importantes e resolver crimes virtuais, já foram desenvolvidos trabalhos semelhantes a este como, por exemplo, o trabalho de Kamiya (2014, 58 p.). 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.

5 METODOLOGIA

Este trabalho foi desenvolvido em duas fases: na primeira foi realizado um estudo explorando os aspectos teóricos, e uma etapa prática na qual foram utilizados *softwares* de recuperação de dados, e feita a comparação entre os mesmos em computadores com Windows, Linux e *smartphones* com iOS e Android.

Na primeira fase foram estudados materiais teóricos de diversos assuntos de extrema importância para o desenvolvimento do trabalho.

De início foi realizada uma pesquisa, abordando os celulares e sua evolução, chegando até aos dias atuais, os sistemas operacionais mais utilizados atualmente, demonstrando um pouco sobre o que é Android, iOS, Linux e Windows. Esta etapa do trabalho visou demonstrar a relevância do sistema operacional para a perícia forense, considerando os sistemas mais atualizados.

Foi escrito um capítulo sobre conceito de perícia forense computacional e suas aplicações visando abranger essa área, e ao mesmo tempo explorar onde estas técnicas forenses podem ser utilizadas.

Todas as etapas da investigação foram abordadas, relatando quais são os procedimentos que o perito deve ter na cena do crime, e quais os passos a seguir para que não ocorra nenhuma perda de informação.

O estudo realizado sobre os conceitos dos procedimentos utilizados na perícia forense computacional visou demonstrar a grande importância dos procedimentos que são efetuados na busca e apreensão, e também o transporte dos equipamentos apreendidos, sendo necessário um cuidado extremamente cuidadoso para a preservação das provas para que não ocorra nenhum dano ao equipamento.

Também foi desenvolvido um capítulo sobre técnicas anti-forense, tendo como meta explicar como alguns programas em computadores podem realizar limpezas de rastros de criminosos. 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.

Já na segunda fase houve a parte prática, a qual será detalhada na sequência.

Para a recuperação em *smartphones* foram utilizados dois aparelhos de uso próprio, um iPhone modelo 4s utilizando o iOS versão: 8.0.2 (12A405), e um Samsung modelo Win utilizando Android na versão 4.1.2.

Para os testes realizados em computadores foram considerados os sistemas operacionais Windows (Windows 7) e (Kali Linux 2.0). Será projetado um cenário utilizando uma única máquina física de uso próprio com a seguinte configuração de hardware: *Notebook* ASUS, processador Intel Core i7-3537U CPU@ 2.00Hz, memória RAM de 8 GB.

Como está pesquisa tem caráter qualitativo, onde a pesquisa qualitativa está mais relacionada no levantamento de dados sobre motivações de um grupo, em compreender e interpretar determinados comportamentos, a opinião e as expectativas dos indivíduos de uma população, portanto não teve o intuito de se prender apenas a números como resultados.

Os testes no smartphone Android foram realizados utilizando um cartão de memória de 16Gb, já no IOS foi utilizada a própria memória interna de 8Gb do dispositivo móvel.

Os testes realizados no sistema Windows e Linux contaram um *HD Externo* de 500 Gb.

A quantidade de arquivos investigados, bem como seus tipos, foram definidos uma quantidade de arquivos satisfatória pelo autor deste trabalho, e podem ser vistos a seguir

- a) 50 arquivos Texto (".doc");
- b) 50 arquivos Música (".mp3");
- c) 50 arquivos Vídeo (".mp4");
- d) 50 arquivos Imagens(".jpeg")

Desse modo, o dispositivos continham 200 arquivos diversos e 4 pastas. Após os arquivos serem inseridos, tanto o cartão de memória como o *HD Externo* foram formatados na modalidade "Formatação Rápida" e, após a formatação, programas de recuperação de dados foram executados para recuperar os arquivos apagados.

O motivo da escolha dos *softwares* elencados a seguir deve-se ao fato de pertencerem a categoria de *softwares* gratuitos, e também, pelo fato de serem ferramentas mais populares.

A Figura 5 ilustra as plataformas e *softwares* selecionados para utilização neste trabalho.

Figura 5 - Plataformas e seus respectivos softwares de recuperação de dados.

Software	iOS	Android	Windows	Linux
Recuva				
MiniTool				
DiskDigger				
RemoRecover				
Wondershare Dr. Fone				
Scalpel				
ExtUndelete				

Fonte: Elaborada pelo autor.

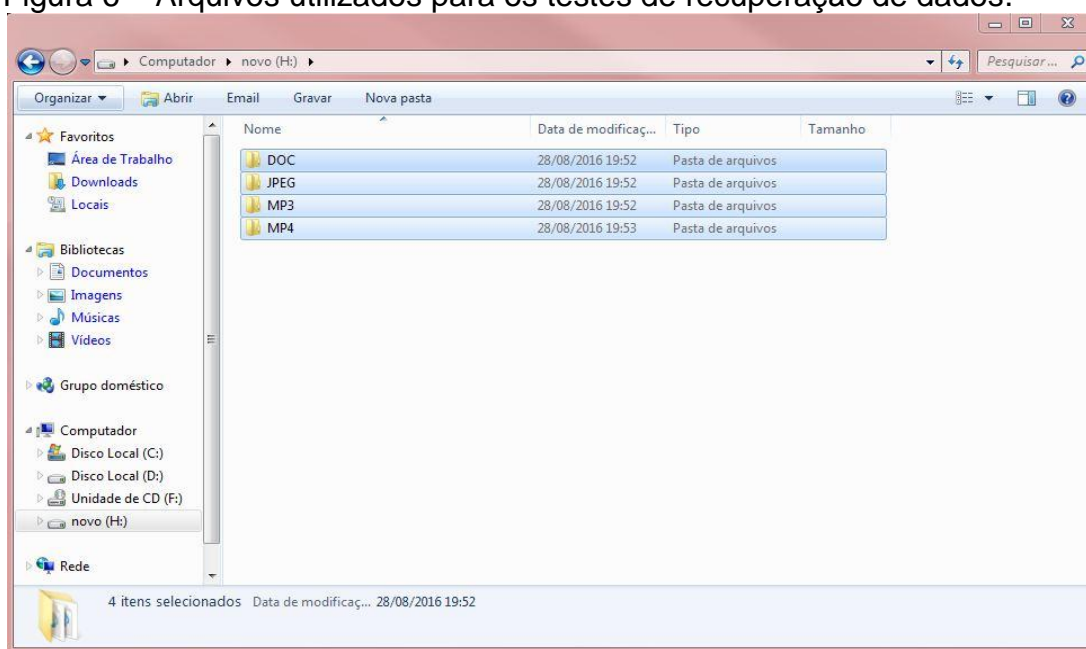
Como pode ser observado na Figura 5, a comparação entre os *softwares* ocorreu de forma vertical (entre *softwares* semelhantes em uma mesma plataforma), e horizontal (comparação do mesmo *software* rodando em plataformas diferentes), visando assim demonstrar quais apresentam maior capacidade de recuperação.

Para exibir e comparar os resultados obtidos foram elaboradas tabelas e gráficos no Microsoft Excel com a porcentagem de recuperação de cada *software* utilizado em cada um dos dispositivos de armazenamento de acordo com o seu tipo (texto, vídeo, áudio, arquivos em geral).

5.1 Testes feitos para recuperação de dados.

Primeiramente foi criada uma nova partição no HD Externo para poder gravar os arquivos utilizados nos testes. Foram separados 50 arquivos de cada tipo em suas respectivas pastas como pode ser visto na Figura 6.

Figura 6 – Arquivos utilizados para os testes de recuperação de dados.



Fonte: Elaborada pelo autor. (2016).

5.1.1 Recuva

Os testes realizados no *software* Recuva foram idênticos ao MiniTool, os arquivos do HD Externo foram apagados e a recuperação dos arquivos foi realizada.

Portanto, ao apagar um arquivo, o arquivo continua ali até que algum outro ocupe seu espaço, assim, utilizando o *software* o mais breve possível maior é a chance de recuperar todos os documentos perdidos. O Recuva recupera apenas os arquivos que ainda não foram sobrescritos por outros dados quaisquer.

Após sua instalação, o *software* mostra a tela do assistente de utilização, que acompanha o usuário do decorrer do processo de recuperação, como pode ser observado na Figura 7.

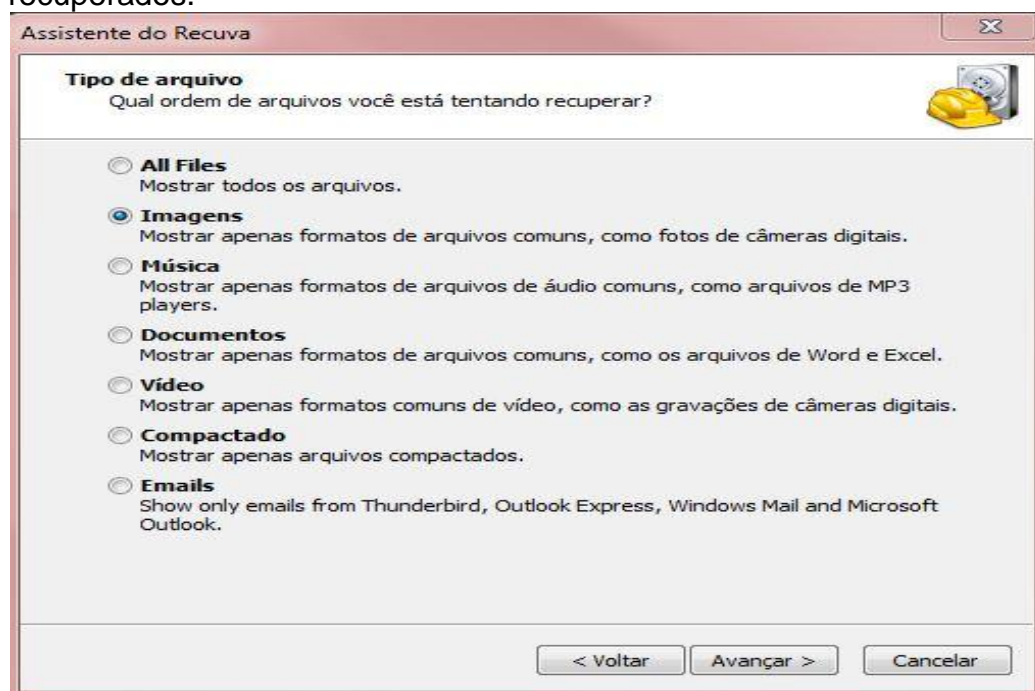
Figura 7 – Assistente do software Recuva.



Fonte: Recuva (2016).

Este próximo passo apresenta a sequência do “Assistente do Recuva”. Nessa opção o *software* indica quais tipos de arquivos o usuário pode escolher, como o tipo de mídia, arquivo e até e-mails para serem inseridos em sua busca; de início a opção “imagens foi escolhida, conforme exibe a Figura 8.

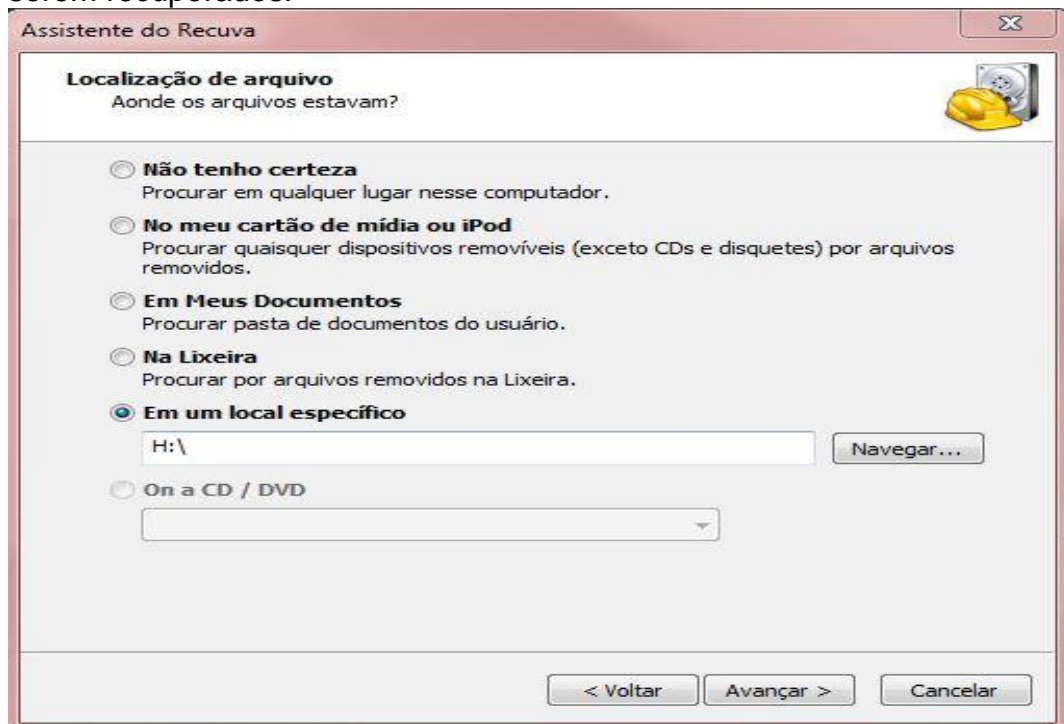
Figura 8 – Assistente do software Recuva, tela para escolha de arquivos a ser recuperados.



Fonte: Recuva (2016).

Na sequência o *software* solicitou o local onde os arquivos se encontravam. O usuário pode escolher entre cinco opções, caso o usuário não saiba o local clique em “Não tenho certeza” e o programa irá fazer uma varredura em todo o computador. A princípio a opção escolhida foi: “Em um local específico, “Unidade H:\”. Esta é a unidade onde o *HD externo* está alocado, como demonstra a Figura 9.

Figura 9 – Assistente do software Recuva, tela para localizar os arquivos a serem recuperados.



Fonte: Recuva (2016).

Após a escolha do local onde os arquivos se encontram o usuário se depara com uma tela na qual o assistente do *software* exibe uma opção para “Ativar verificação profunda”. Essa opção pode demorar horas em um dispositivo de grande capacidade de armazenamento, porém, vasculha mais profundamente em busca de arquivos. Esta especificidade pode ser verificada na Figura 10.

Figura 10 – Assistente do software Recuva, tela para iniciar a busca por arquivos apagados.



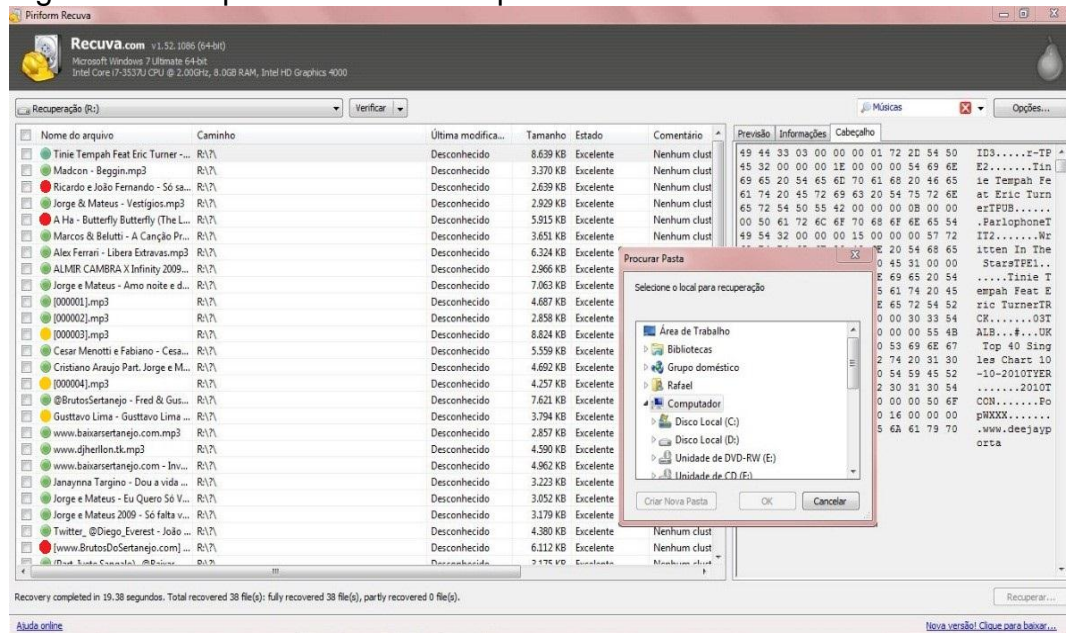
Fonte: Recuva (2016).

Na sequência, os arquivos com possibilidade de recuperação são demonstrados, no centro estão concentrados todos os arquivos que foram perdidos atualmente do computador. Pode ser observado que ao lado esquerdo do nome de cada arquivo, haverá sempre um círculo colorido. Cada cor dos círculos representa uma informação:

- a) Círculo Vermelho: é uma notificação de que o arquivo não poderá ser recuperado. O arquivo foi sobrescrito por outro arquivo, portanto, tornou-se irrecuperável.
- b) Círculo Laranja: é uma notificação de que as chances de o arquivo ser recuperado integralmente são poucas, mas não impossível. O arquivo pode estar corrompido, ou pode estar normal.
- c) Círculo Verde: é uma notificação de que o arquivo pode ser recuperado perfeitamente, 100%. Certamente conseguirá recuperar e salvá-lo sem qualquer empecilho.

Nesta etapa, basta selecionar o arquivo encontrado desejado e clicar em “Recuperar...”, selecionar um local para que o programa possa recuperar esses arquivos e salvá-los. A Figura 11 ilustra este contexto.

Figura 11 – Arquivos encontrados pelo Recuva.



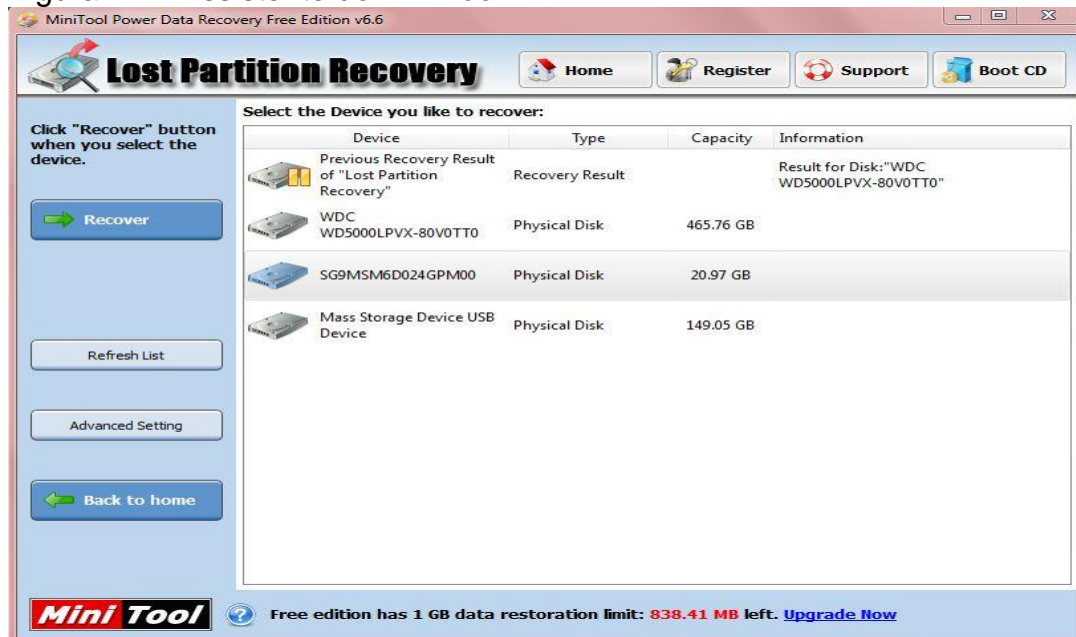
Fonte: Recuva (2016).

5.1.2 Minitool

Depois do *software* instalado e iniciado, o próximo passo foi escolher a partição desejada através do “Assistente do MiniTool” para realizar a recuperação.

O MiniTool exibe todas as partições e discos presente no computador. Conforme apresentado na Figura 12 basta selecionar um deles e iniciar a varredura de busca de tudo o que está danificado e pode ser recuperado.

Figura 12 – Assistente do MiniTool.



Fonte: MiniTool (2016).

O software MiniTool apresentou ainda a opção *FullScan*, a qual tem a função de inspecionar volumes existentes mais profundamente, podendo levar um grande tempo dependendo do tamanho do dispositivo sendo analisado.

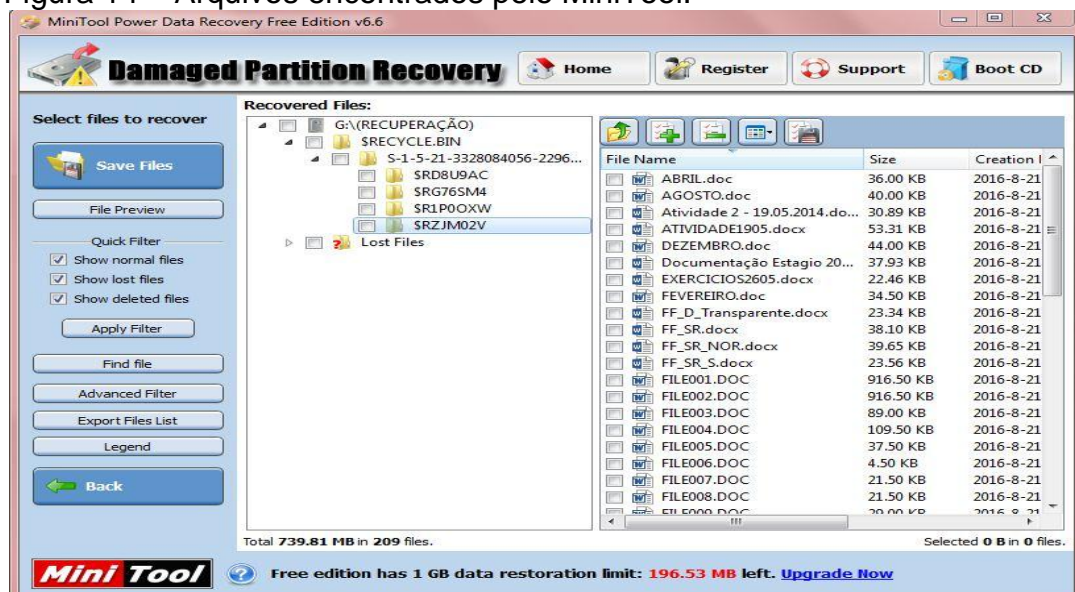
Figura 13 – FullScan MiniTool.



Fonte: MiniTool (2016).

Após a realização do escaneamento os arquivos com possibilidade de recuperação foram exibidos. Para realizar a recuperação do arquivo desejado, bastou selecioná-lo e posteriormente salvá-lo em uma pasta, não sendo sua pasta de origem. A Figura 14 demonstra os arquivos que podem ser recuperados, e os locais onde é possível salvar o arquivo desejado.

Figura 14 – Arquivos encontrados pelo MiniTool.



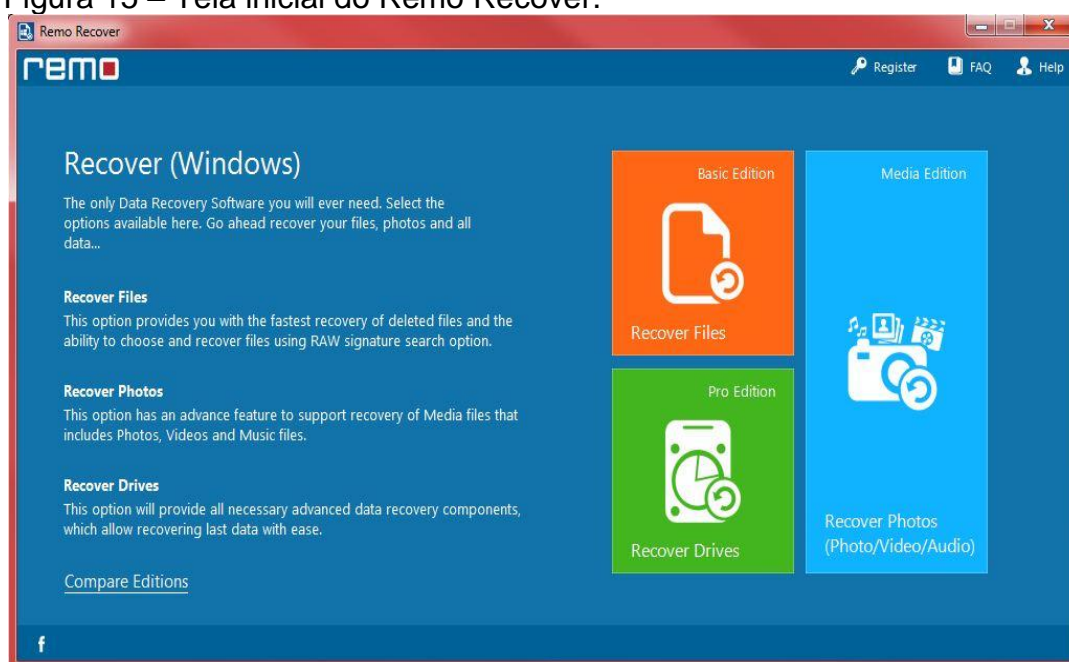
Fonte: MiniTool (2016).

5.1.3 RemoRecover

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

A Figura 15 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 15 – Tela inicial do Remo Recover.

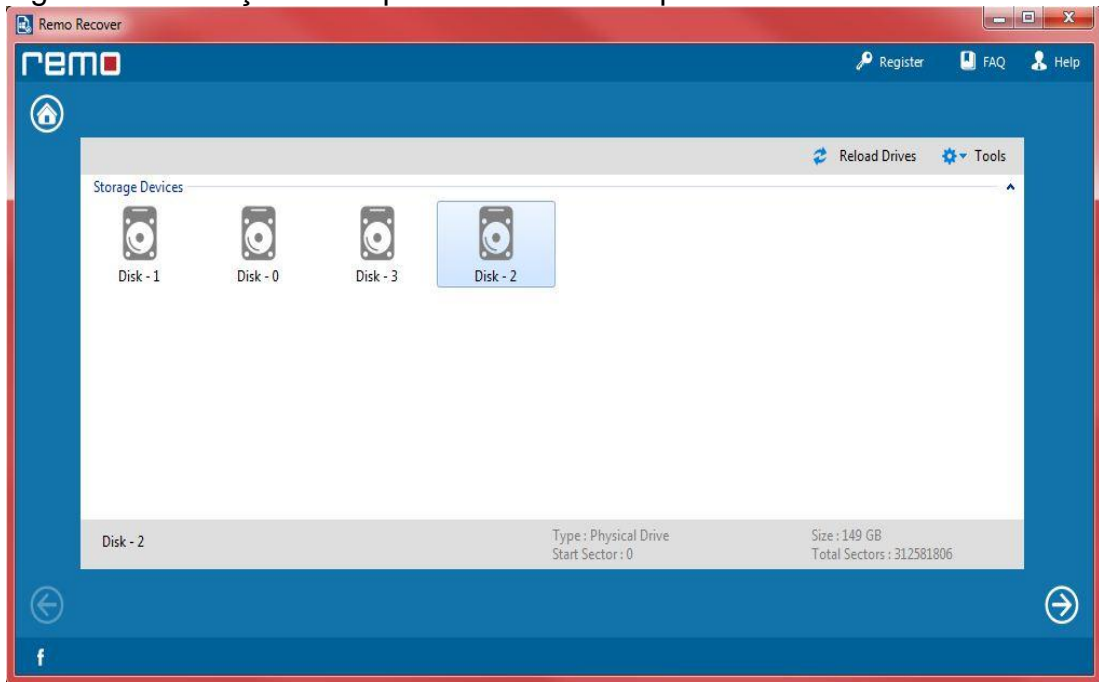


Fonte: Remo Recover. (2016).

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 16.

Figura 16 – Seleção de arquivos a serem recuperados.

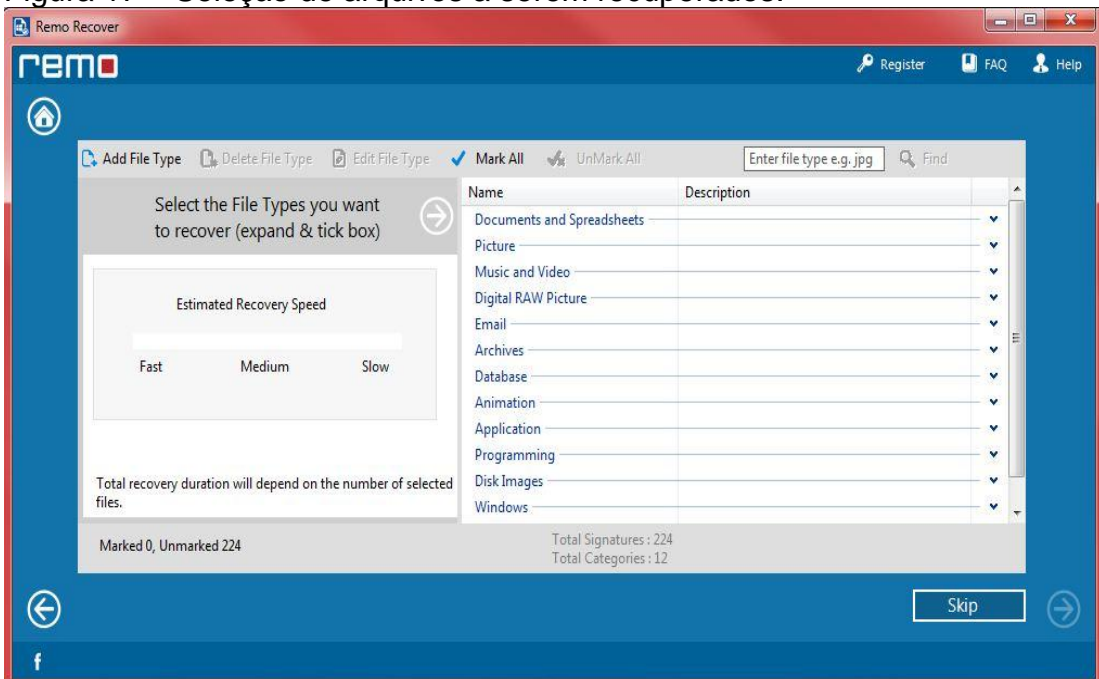


Fonte: Remo Recover. (2016).

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 deseja realmente recuperar, como mostrado na Figura 17.

Figura 17 – Seleção de arquivos a serem recuperados.



Fonte: Remo Recover. (2016).

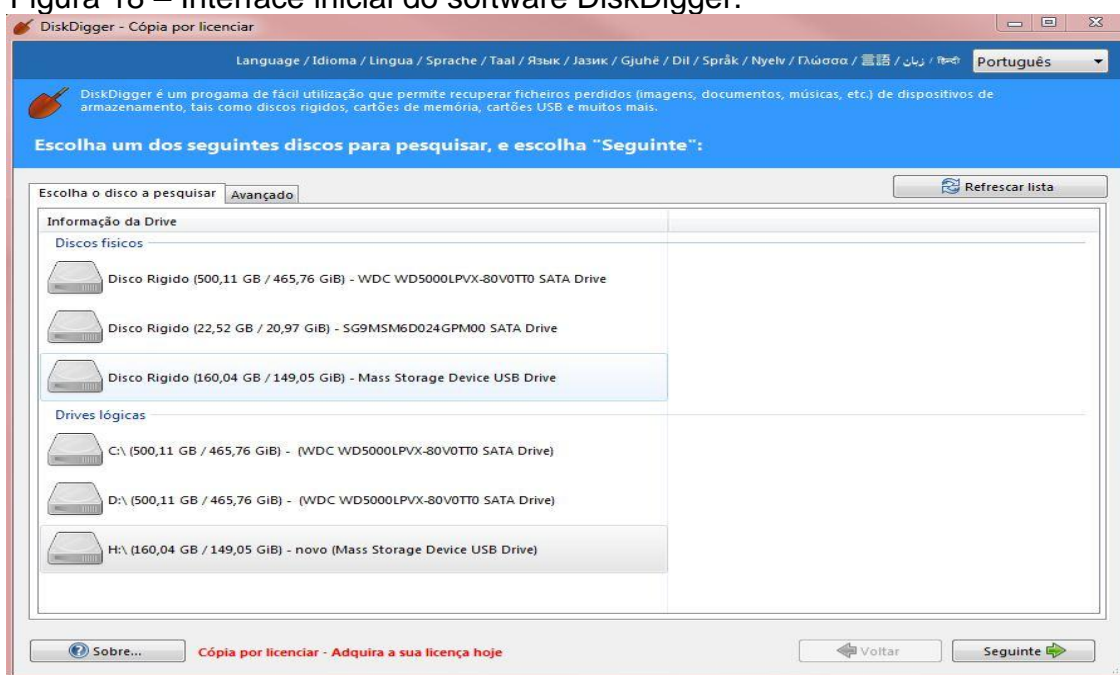
Concluindo, podemos observar pelas Figuras 15, 16 e 17, que o Remo Recover é um *software* bastante fácil e intuitivo, facilitando os usuários mais leigos para que possam interagir com maior facilidade com o *software*.

5.1.4 DiskDigger

Já com o aplicativo em execução, a pesquisa por arquivos apagados teve início. O *software* separou todo o conteúdo pela extensão dos documentos, ou seja, caso fosse uma imagem provinda de uma câmera digital, ela provavelmente se encontrará na seção JPEG ou JPG. Já um arquivo de texto feito no Word na seção DOC, e assim por diante.

A Figura 18 exibe a *interface* inicial do *software*, denotando os discos físicos, *drives* lógicos, evidenciando também o *Hd Externo* utilizado no teste, localizado na opção H:.

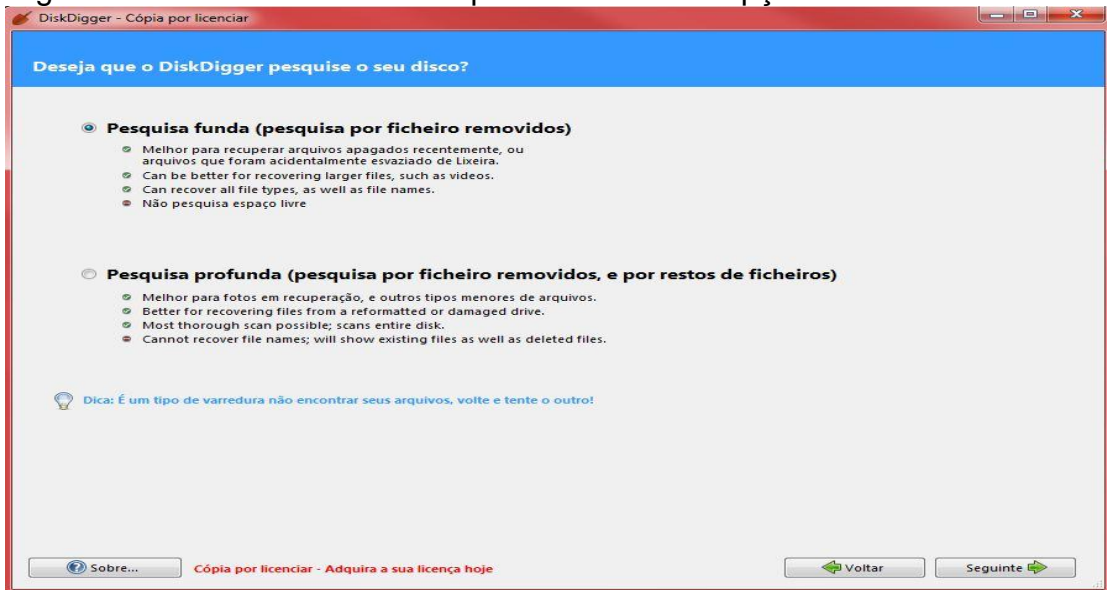
Figura 18 – Interface inicial do software DiskDigger.



Fonte: DiskDigger (2016).

Em seguida o *software* oferece a opção de escolher entre Pesquisa funda (pesquisa por ficheiros removidos) ou Pesquisa profunda (pesquisa por ficheiros removidos, e por restos de ficheiros), conforme ilustra a Figura 19.

Figura 19 – Tela onde o usuário pode escolher as opções de busca.

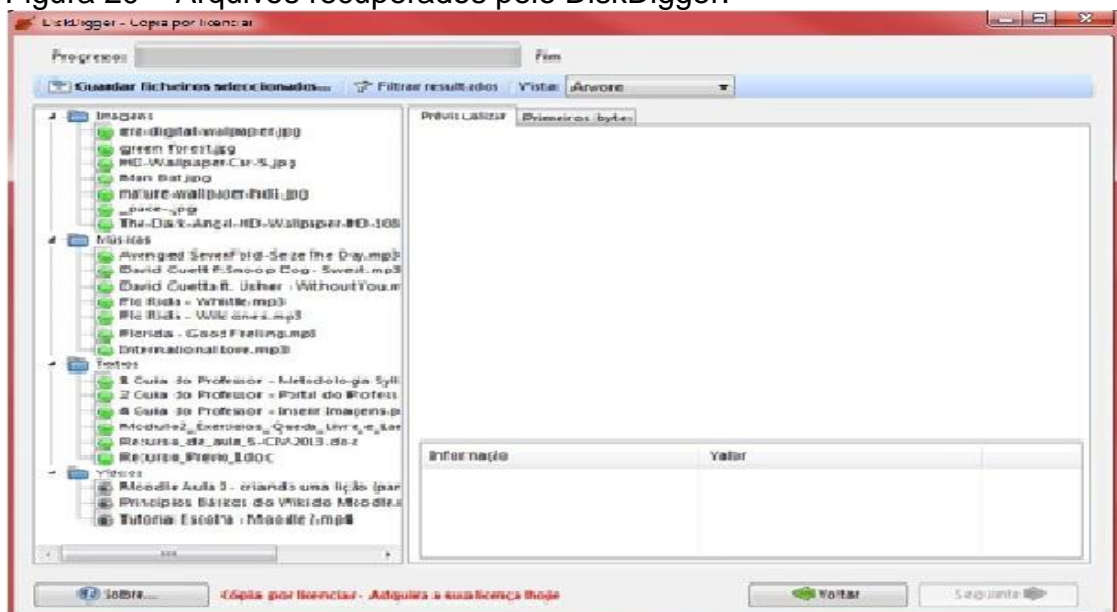


Fonte: DiskDigger (2016).

Um aspecto positivo e interessante é a capacidade de organizar os documentos encontrados por suas extensões, ou seja, cada uma delas possui sua própria categoria, o que facilita a vida do usuário na hora de procurar o arquivo deletado.

Caso uma foto seja apagada, por exemplo, não é preciso ficar vasculhando os arquivos de música ou vídeo, pois a foto estará na categoria de imagens. Para classificar os arquivos deste modo basta deixar a visualização com “Árvore” no DiskDigger, conforme pode ser constatado na Figura 20.

Figura 20 – Arquivos recuperados pelo DiskDigger.



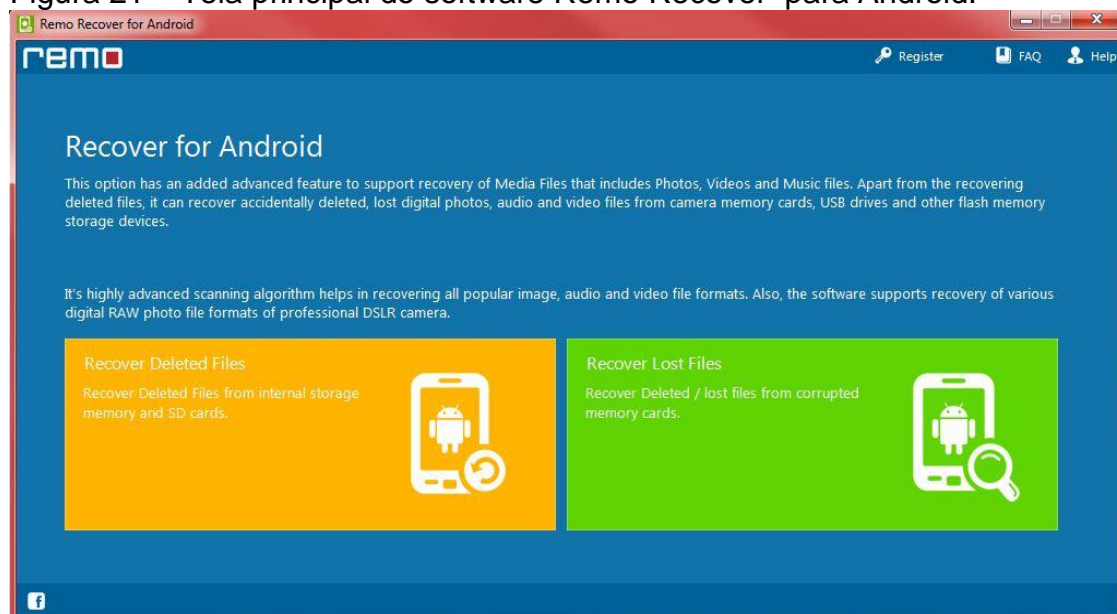
Fonte: DiskDigger (2016).

5.2 Softwares utilizados para recuperação no Sistema Operacional Android

5.2.1 Remo Recover for Android

A Figura 21 exibe a tela inicial do *software* Remo Recover para Android. Nesta tela existem duas opções para o usuário escolher: Recuperar os Arquivos Apagados ou Recuperar Arquivos Perdidos.

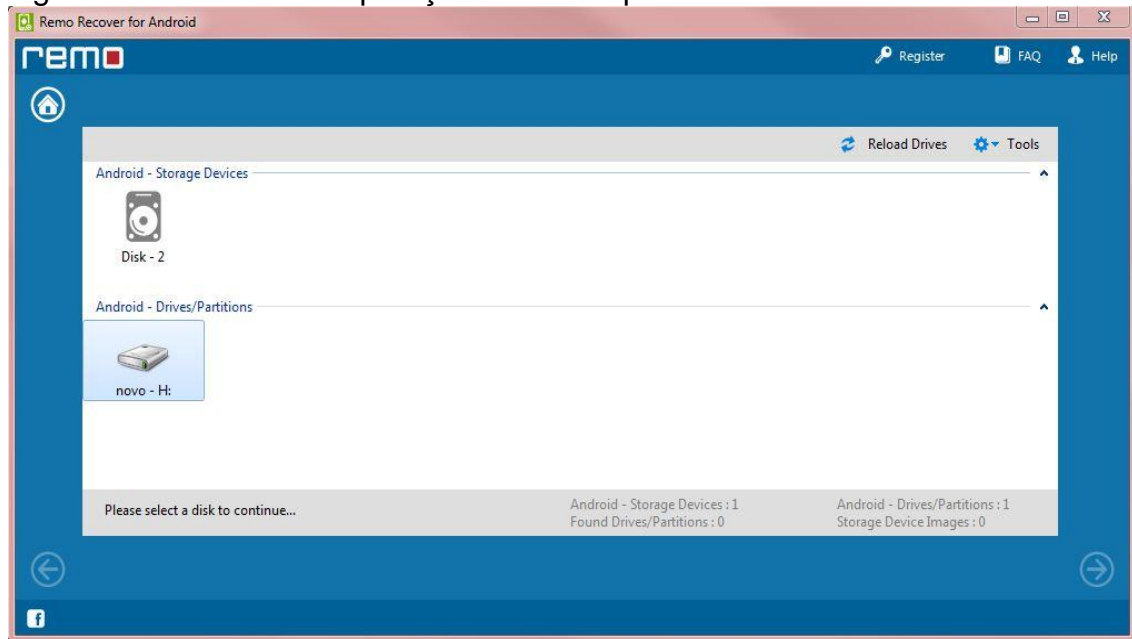
Figura 21 – Tela principal do software Remo Recover para Android.



Fonte: Remo Recover para Android (2016).

Já com *smartphone* plugado e reconhecido pelo aplicativo, uma tela foi exibida com as partições do *smartphone*, a Figura 22 demonstra as partições do *smartphone* testado.

Figura 22 – Tela com as partições do smartphone no Remo Recover for Android.

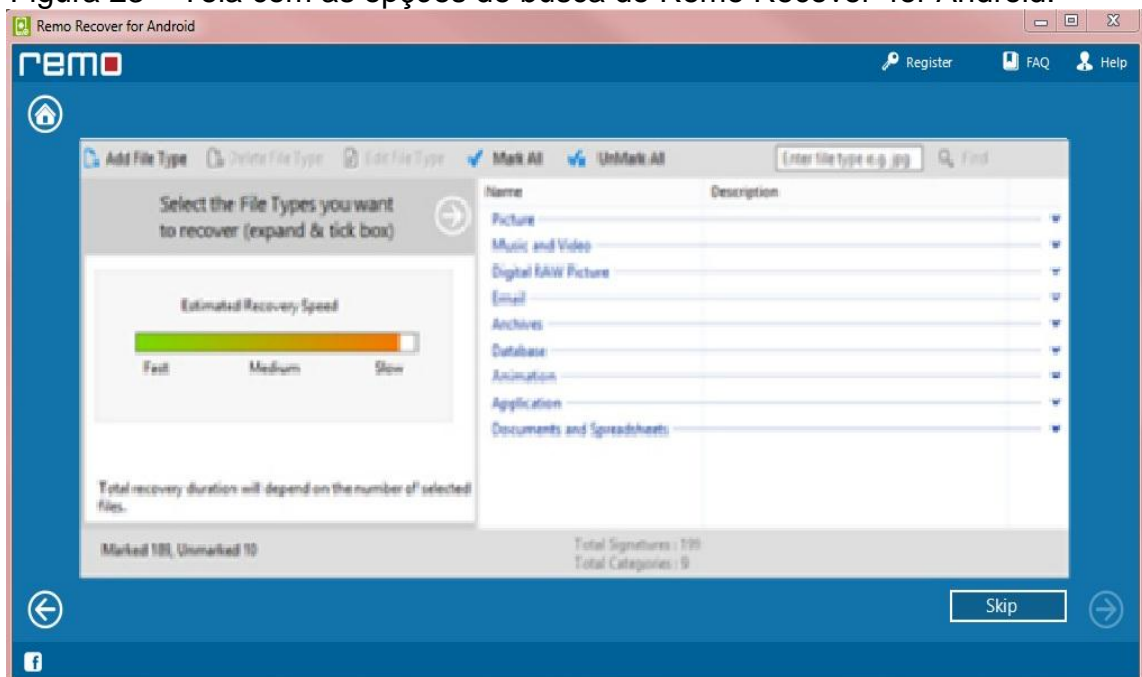


Fonte: Remo Recover for Android (2016).

No próximo passo foi possível escolher a velocidade da busca por arquivos entre rápido, médio e lento. Cada velocidade altera a qualidade da busca: quanto mais lento para a procura, mas arquivos serão encontrados.

Nesta tela também é possível selecionar qual tipo de arquivo procurar, a Figura 23 exhibe estas descrições.

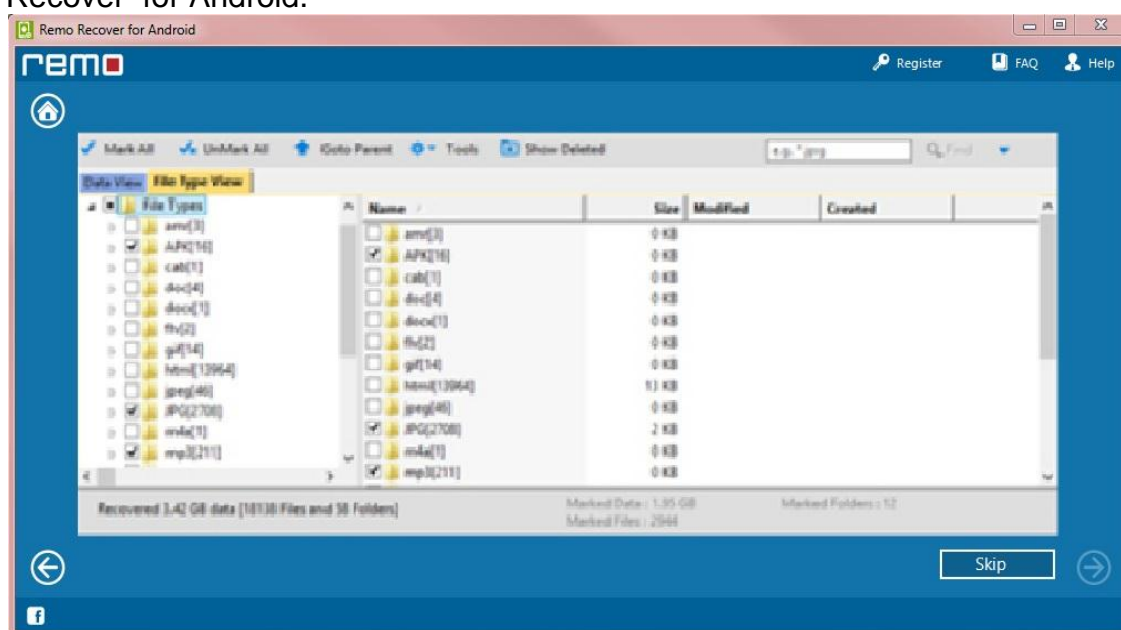
Figura 23 – Tela com as opções de busca do Remo Recover for Android.



Fonte: Remo Recover for Android (2016).

Na sequência, depois do processo de pesquisa concluído, os arquivos que podem ser recuperados são exibidos, conforme mostra a Figura 24. Com isso, basta o usuário selecionar o arquivo que deseja recuperar e salvá-lo em uma partição de seu computador, recordando que o arquivo recuperado não pode ser salvo no local de origem.

Figura 24 – Tela com os arquivos com possibilidade de recuperação no Remo Recover for Android.



Fonte: Remo Recover for Android (2016).

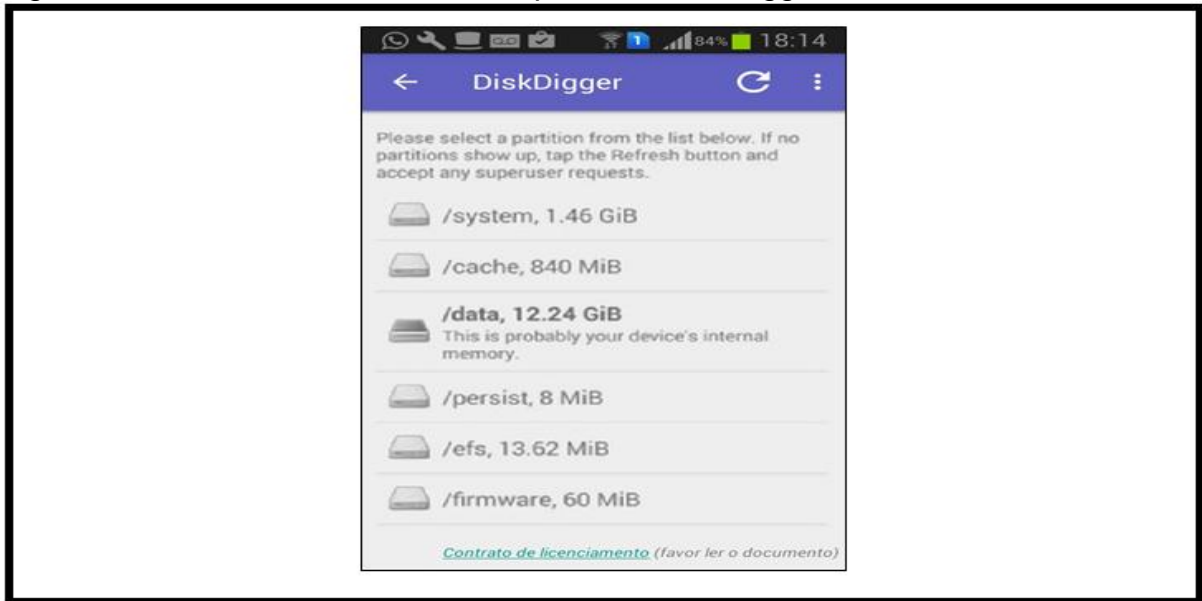
A *interface* é muito intuitiva e simples de usar. Um dos principais detalhes que chamam a atenção é a ausência de botões e opções complicadas, o que deve facilitar a vida de usuários mais leigos.

O programa realmente detecta arquivos deletados ou perdidos com facilidade: basta conectar o seu Android ao PC que o programa reconhece automaticamente o sistema operacional e começa a trabalhar na busca pelos documentos, fotos e vídeos.

5.2.2 Diskdigger

A instalação do *software* é básica, necessitando apenas clicar em botões como avançar, feita a instalação o usuário já poderá optar pela recuperação entre a memória interna do aparelho ou pelo cartão de memória. A Figura 25 exhibe os discos disponíveis para realizar a recuperação.

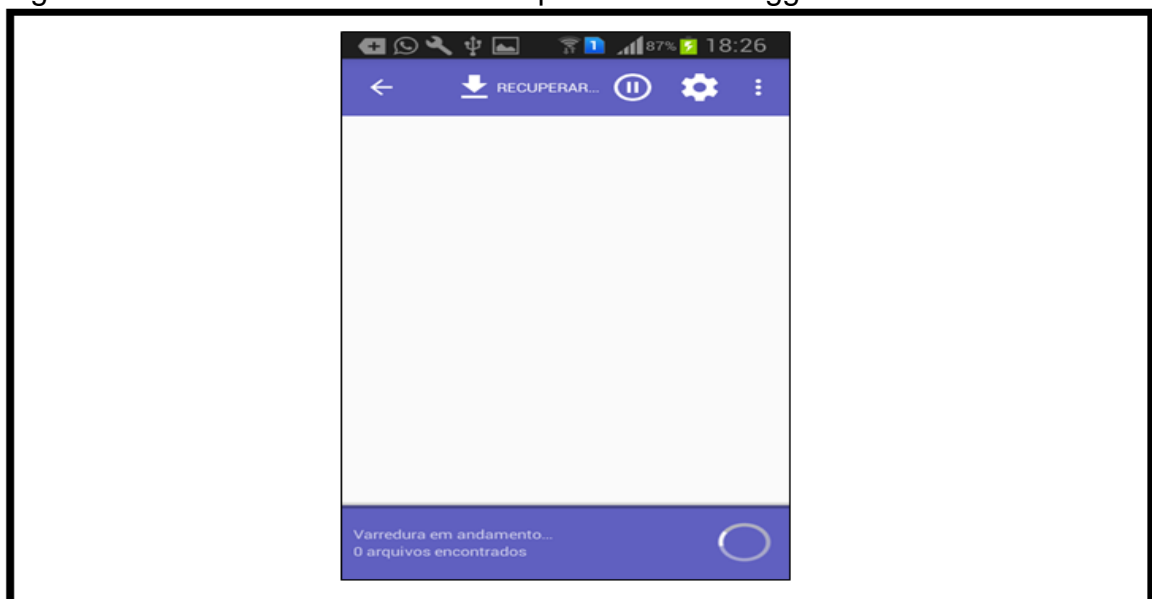
Figura 25 – Tela com a leitura dos arquivos no DiskDigger.



Fonte: DiskDigger (2016).

A Figura 26 exibe o *software* realizando a busca no aparelho *smartphone*, o processo é bastante rápido. No teste utilizado em um cartão SD, o tempo para leitura foi de 8 minutos. Poderá gastar mais tempo caso o cartão seja maior ou esteja muito carregado de arquivos.

Figura 26 – Tela com a leitura dos arquivos no DiskDigger.



Fonte: DiskDigger (2016).

Para facilitar, os arquivos encontrados podem ser organizados por imagens, músicas, vídeos, documentos, arquivos e pacotes. É possível também procurar pelo nome do arquivo. Note que a Figura 27 lista os tipos de arquivos encontrados.

Figura 27 – Tela com os arquivos encontrados no DiskDigger.



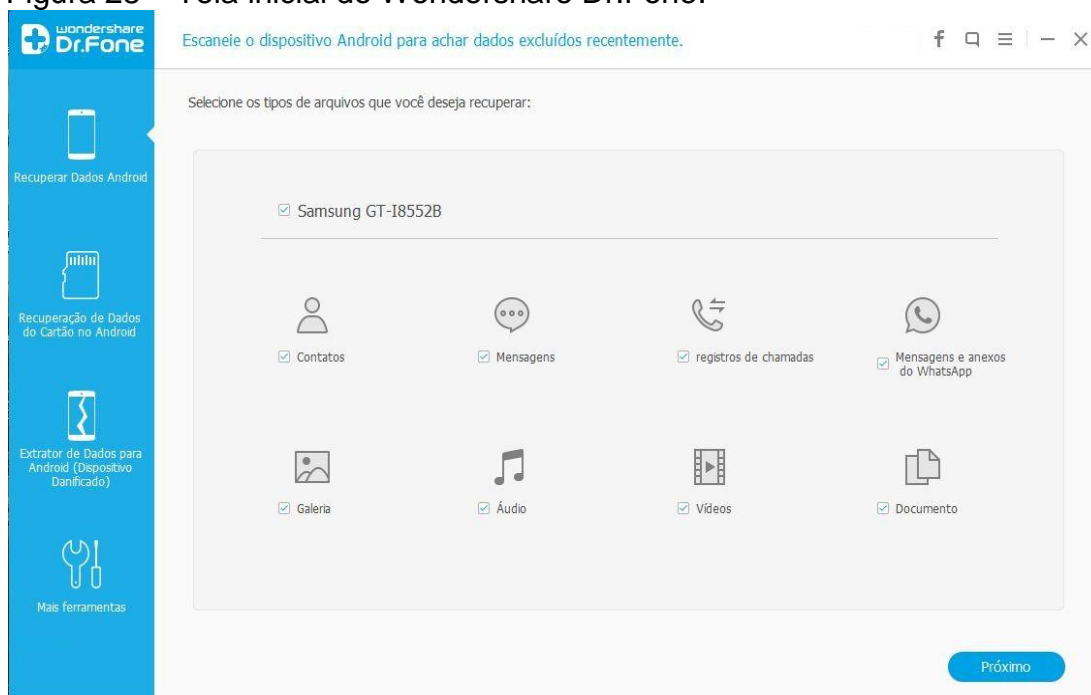
Fonte: DiskDigger (2016).

Após o usuário escolher qual arquivo será recuperado, basta pressionar o botão “OK” para o aplicativo recuperar o arquivo.

5.2.3 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 28.

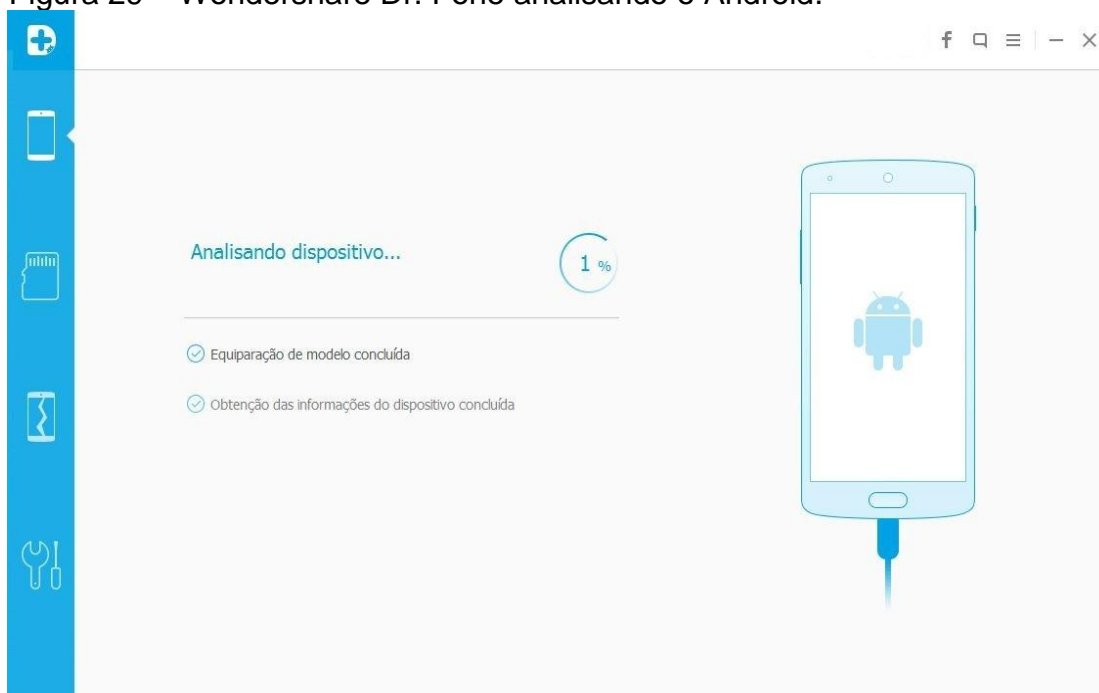
Figura 28 – Tela inicial do Wondershare Dr.Fone.



Fonte: Wondershare Dr. Fone. (2014).

A Figura 29 mostra que ao selecionar os arquivos desejados para recuperação e clicar na opção “Próximo”, o *software* começa a analisar o *smartphone* e, em seguida, mostra os arquivos que podem ser recuperados.

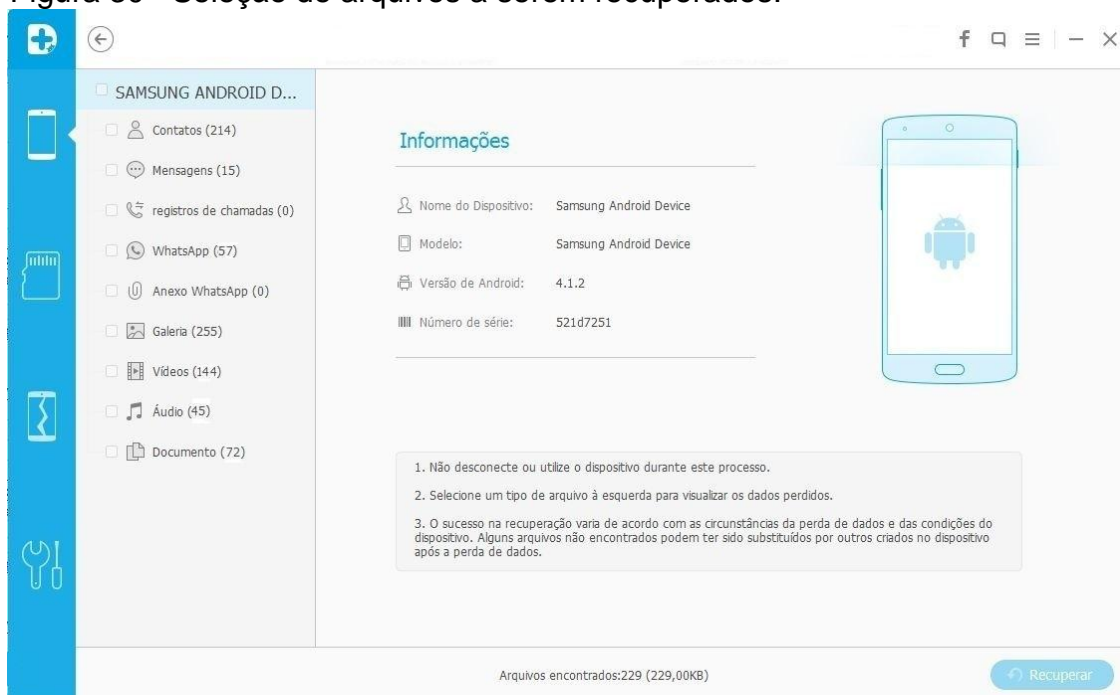
Figura 29 – Wondershare Dr. Fone analisando o Android.



Fonte: Wondershare Dr. Fone. (2016).

É importante destacar que como este é um software voltado especificamente para a recuperação de arquivos em *smartphones*, 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 30.

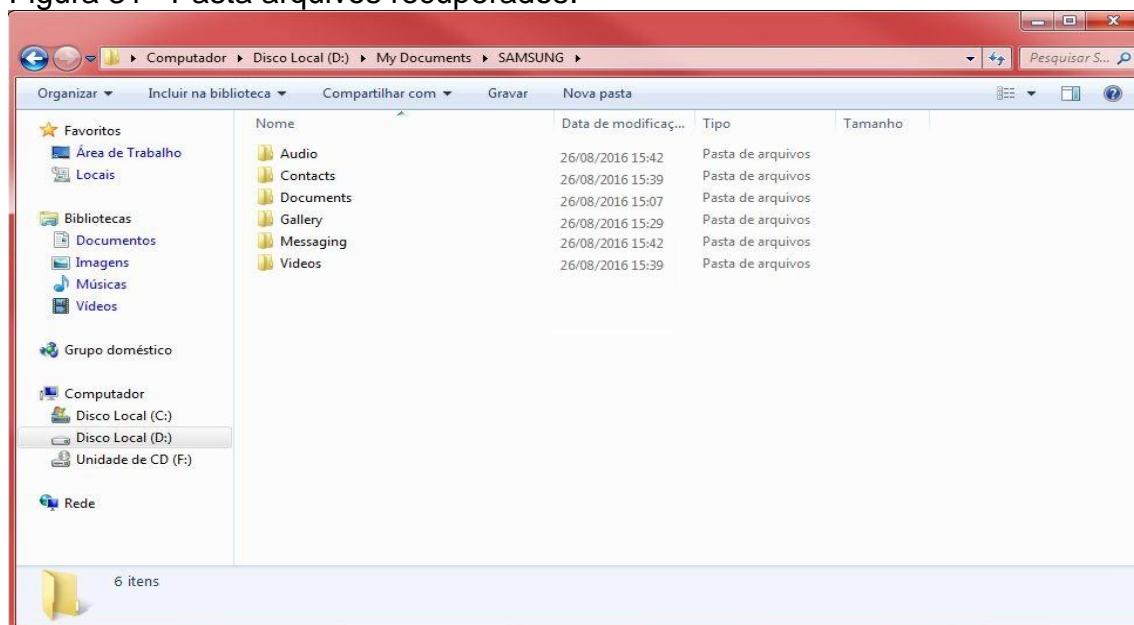
Figura 30 –Seleção de arquivos a serem recuperados.



Fonte: Wondershare Dr. Fone. (2016).

Ao selecionar os arquivos que deseja recuperar, basta o usuário clicar em “Recover” para começar a fazer a recuperação dos dados. Após a recuperação, o *Software* separa em pasta os tipos de arquivos facilitando a visualização. Como mostra na figura 31.

Figura 31 –Pasta arquivos recuperados.



Fonte: Wondershare Dr. Fone. (2016).

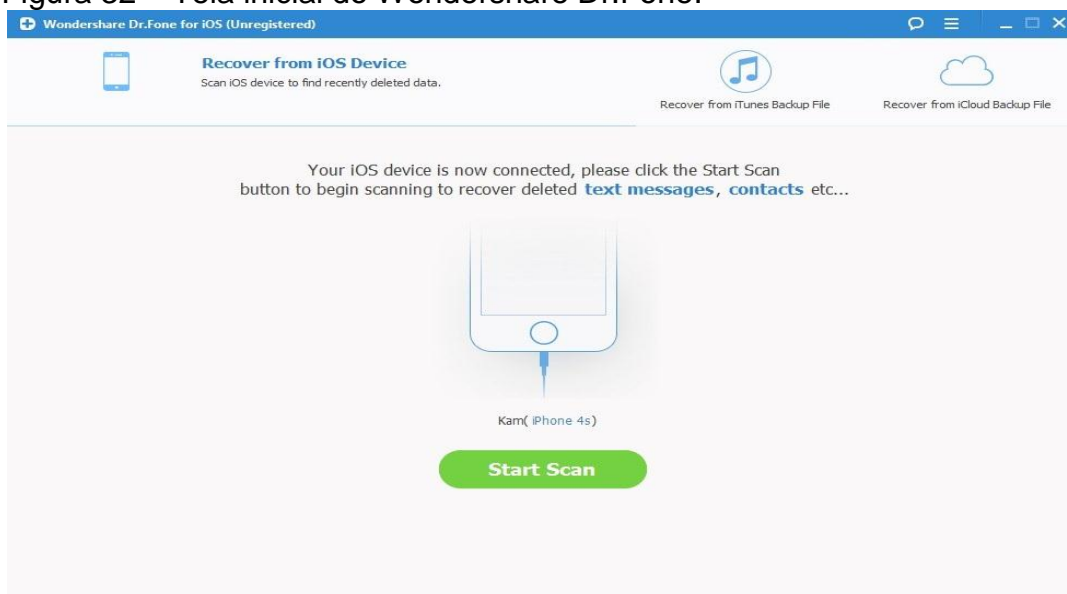
6.3 Softwares utilizados para recuperação no Sistema Operacional IOS

6.3.1 Wondershare Dr. Fone

Os testes realizados no *software* Wondershare Dr. Fone Android foram idênticos ao Wondershare Dr. Fone IOS, os arquivos foram apagados e a recuperação dos arquivos foi realizada.

Basta iniciar o *Software* com o *smartphone* já ligado ao computador para que o Wondershare Dr. Fone identifique o aparelho e ofereça a opção de escaneamento, como pode ser visto na Figura 32.

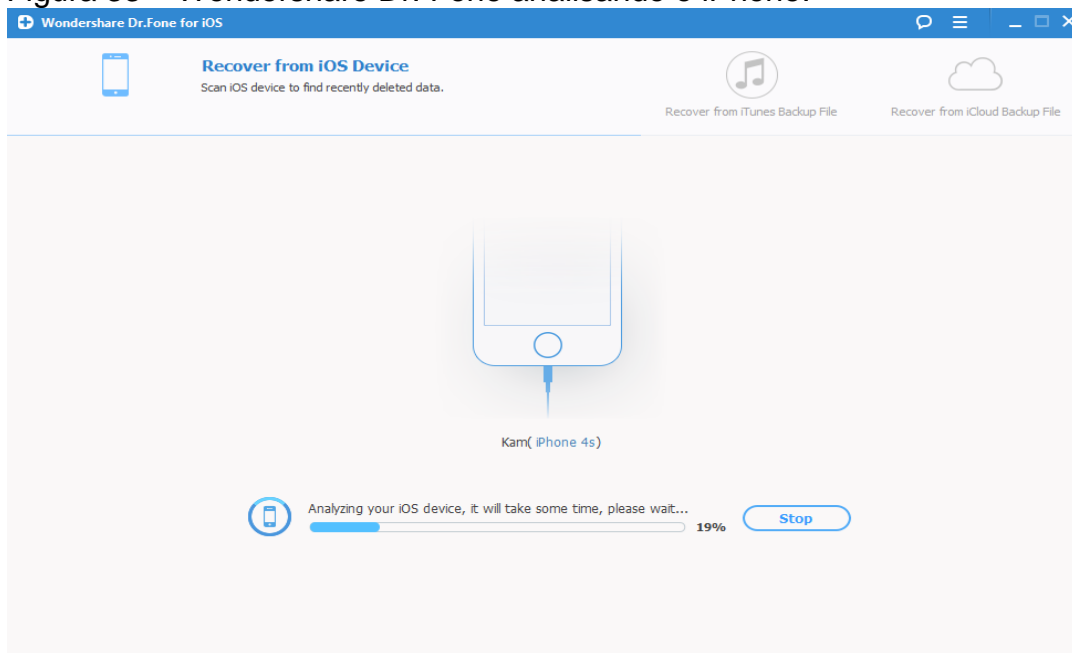
Figura 32 – Tela inicial do Wondershare Dr.Fone.



Fonte: Wondershare Dr. Fone. (2016).

A Figura 33 mostra que ao clicar em “*Start Scan*”, o *software* começa a analisar o *smartphone* e, em seguida, mostra os arquivos que podem ser recuperados.

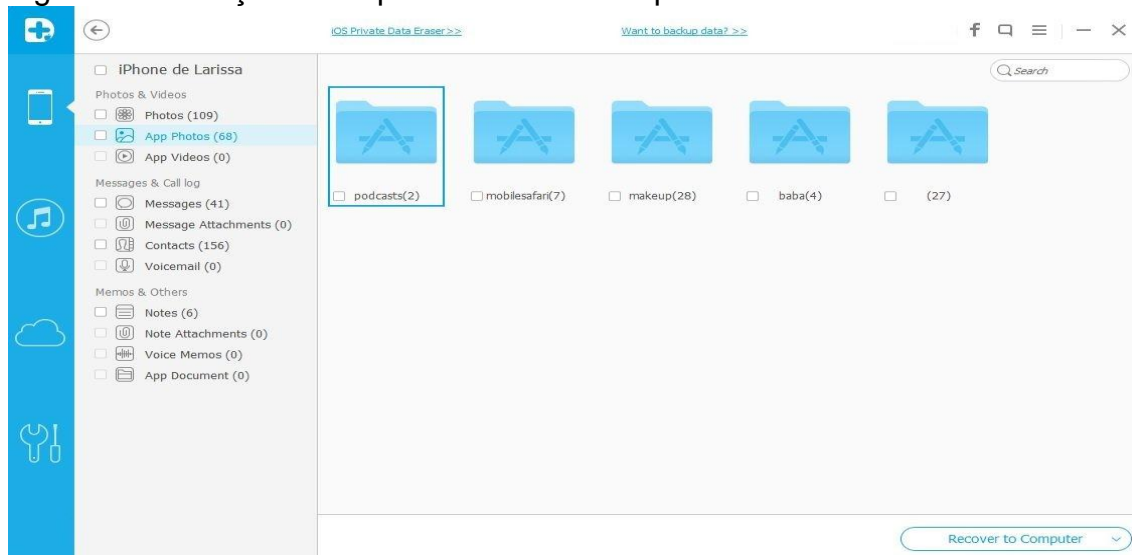
Figura 33 – Wondershare Dr. Fone analisando o iPhone.



Fonte: Wondershare Dr. Fone. (2016).

Vale destacar que não apenas para Android é possível recuperar fotos, vídeos, textos, contatos apagados, mensagens perdidas e até mesmo mensagens do Whatsapp, para iOS também é possível recuperar como pode ser visto na Figura 34

Figura 34 –Seleção de arquivos a serem recuperados.



Fonte: Wondershare Dr. Fone. (2016).

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

5.4 SOFTWARES UTILIZADOS PARA RECUPERAÇÃO NO SISTEMA OPERACIONAL LINUX

5.4.1 Scalpel

Já com o Scalpel aberto foi necessário apenas realizar uma edição de texto. Por utilidade padrão o Scalpel tem seu próprio arquivo de configuração em “/ etc” o caminho do diretório completo é “**sudo nano / etc / scalpel / scalpel.conf** “. Como pode ser visto na Figura 35

Figura 35 – Tela com saída de amostra do Scalpel.

```

root@kali: ~
File Edit View Search Terminal Help
-h Print this help message and exit.
-i Read names of disk images from specified file.
-m Generate/update carve coverage blockmap file. The first 32bit
  unsigned int in the file identifies the block size. Thereafter
  each 32bit unsigned int entry in the blockmap file corresponds
  to one block in the image file. Each entry counts how many
  carved files contain this block. Requires more memory and
  disk. **EXPERIMENTAL**
-n Don't add extensions to extracted files.
-o Set output directory for carved files.
-O Don't organize carved files by type. Default is to organize carved files
  into subdirectories.
-p Perform image file preview; audit log indicates which files
  would have been carved, but no files are actually carved.
-q Carve only when header is cluster-aligned.
-r Find only first of overlapping headers/footers [foremost 0.69 compat mode].
-s Skip n bytes in each disk image before carving.
-t Set directory for coverage blockmap. **EXPERIMENTAL**
-u Use carve coverage blockmap when carving. Carve only sections
  of the image whose entries in the blockmap are 0. These areas
  are treated as contiguous regions. **EXPERIMENTAL**
-V Print copyright information and exit.
-v Verbose mode.
root@kali:~# sudo nano /etc/scalpel/scalpel.conf

```

Fonte: Scalpel (2016).

Pode-se notar na Figura 36 que tudo está comentado com (#). Então, é necessário descomentar o arquivo que irá ser recuperado antes do Scalpel ser executado.

No exemplo a seguir, a recuperação foi feita na extensão de arquivos ‘.jpg’, para isto basta simplesmente descomentar ‘.jpg’ na seção do arquivo para o arquivo de configuração do Scalpel.

Figura 36 – Tela com saída de amostra do Scalpel.

```

root@kali: ~
GNU nano 2.4.3 File: /etc/scalpel/scalpel.conf Modified
# AOL ART files
# art y 150000 \x4a\x47\x04\x0e \xcf\xc7\xcb
# art y 150000 \x4a\x47\x03\x0e \xd0\xcb\x00\x00
#
# GIF and JPG files (very common)
# gif y 5000000 \x47\x49\x46\x38\x37\x61 \x00\x3b
# gif y 5000000 \x47\x49\x46\x38\x39\x61 \x00\x3b
# jpg y 200000000 \xff\xd8\xff\xe0\x00\x10 \xff\xd9
#
# PNG
# png y 20000000 \x50\x4e\x47? \xff\xfc\xfd\xfe
#
# BMP (used by MSWindows, use only if you have reason to think there are
# BMP files worth digging for. This often kicks back a lot of false
# positives
#
# bmp y 100000 BM??\x00\x00\x00
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

```

Fonte: Scalpel (2016).

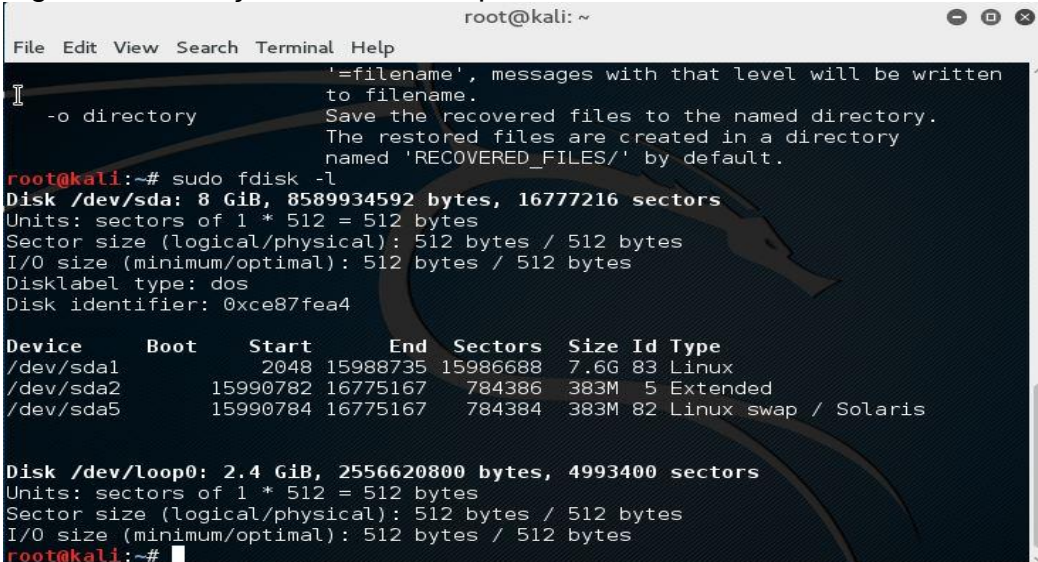
Já no terminal basta digitar a seguinte sintaxe. O “/ dev/sda1” é uma localização do dispositivo de onde o arquivo já está eliminado.

O “-o switch” indica um diretório de saída, onde se pode recuperar os arquivos apagados. É importante certificar-se de que este diretório está vazio antes de executar qualquer comando, caso contrário um erro ocorrerá.

5.4.2 Extundelete

Após o *software* instalado foi necessário rodar o comando "**sudo fdisk -l** " para saber o nome das partições do seu computador, com pode ser visto na Figura 37.

Figura 37 –Partição a serem recuperados.



```

root@kali: ~
File Edit View Search Terminal Help
'=filename', messages with that level will be written
to filename.
-o directory Save the recovered files to the named directory.
The restored files are created in a directory
named 'RECOVERED_FILES/' by default.
root@kali:~# sudo fdisk -l
Disk /dev/sda: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xce87fea4

Device Boot Start End Sectors Size Id Type
/dev/sda1 2048 15988735 15986688 7.6G 83 Linux
/dev/sda2 15990782 16775167 784386 383M 5 Extended
/dev/sda5 15990784 16775167 784384 383M 82 Linux swap / Solaris

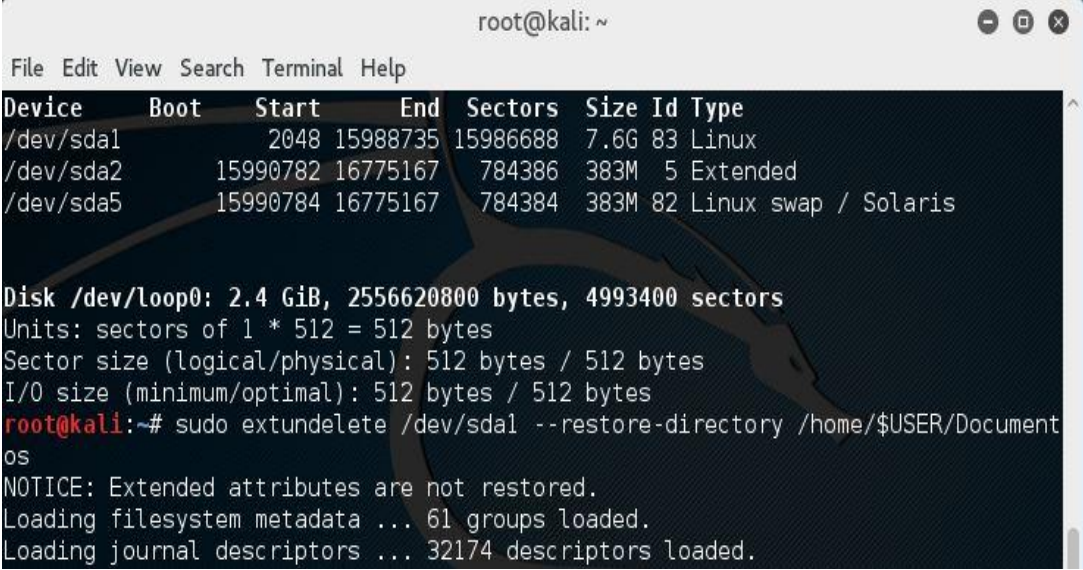
Disk /dev/loop0: 2.4 GiB, 2556620800 bytes, 4993400 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
root@kali:~#

```

Fonte: ExtUndelete (2016).

Foi criada uma pasta para armazenar os arquivos recuperados, feito isto, foi dado o comando “**sudo extundelete /dev/sda1 --restore-directory /home/\$USER/Documentos**” que especifica o caminho a ser salvo os arquivos recuperados. A Figura 38 mostra um exemplo de como a tela é exibida nesse momento.

Figura 38 – ExtUndelete durante a recuperação de dados.



```
root@kali: ~  
File Edit View Search Terminal Help  
Device Boot Start End Sectors Size Id Type  
/dev/sda1 2048 15988735 15986688 7.6G 83 Linux  
/dev/sda2 15990782 16775167 784386 383M 5 Extended  
/dev/sda5 15990784 16775167 784384 383M 82 Linux swap / Solaris  
  
Disk /dev/loop0: 2.4 GiB, 2556620800 bytes, 4993400 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
root@kali:~# sudo extundelete /dev/sda1 --restore-directory /home/$USER/Documents  
os  
NOTICE: Extended attributes are not restored.  
Loading filesystem metadata ... 61 groups loaded.  
Loading journal descriptors ... 32174 descriptors loaded.
```

Fonte: ExtUndelete (2016).

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 executá-lo sem dificuldades.

6 RESULTADOS

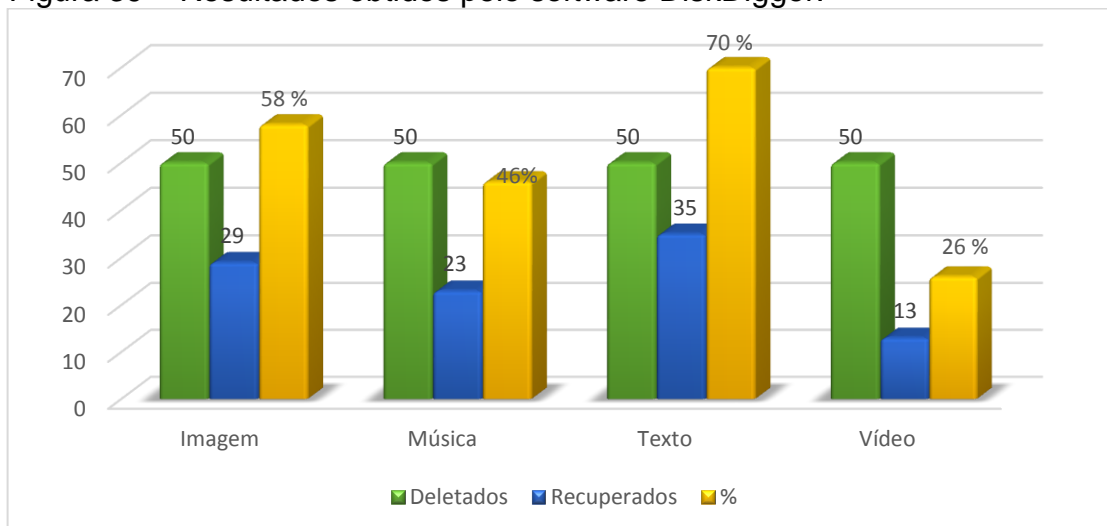
Os resultados obtidos pelos *softwares* testados foram tabulados no Excel, gerando tabelas com os resultados individuais de cada programa. O número de arquivos contidos no *HD externo* e *smartphone* foram de 200 arquivos, divididos entre imagens, músicas, textos e vídeos.

6.1 RECUPERAÇÃO DE ARQUIVOS NO SOFTWARE DISKDIGGER - PLATAFORMA WINDOWS

Conforme ilustra a Figura 39 o DiskDigger obteve maior recuperação nos arquivos de imagens e textos. Já a recuperação dos arquivos de vídeos e músicas não obteve tanto sucesso, devido aos tamanhos dos arquivos serem maiores, arquivos no formato “.doc” com tamanho superior a 5Mb tiveram recuperação parcial, ou seja, faltavam páginas nos arquivos.

Nos testes realizados, o programa mostrou um bom desempenho no quesito tempo de recuperação, levando em conta que a busca por arquivos levou cerca de aproximadamente 50 minutos.

Figura 39 – Resultados obtidos pelo software DiskDigger.



Fonte: Elaborada pelo autor.

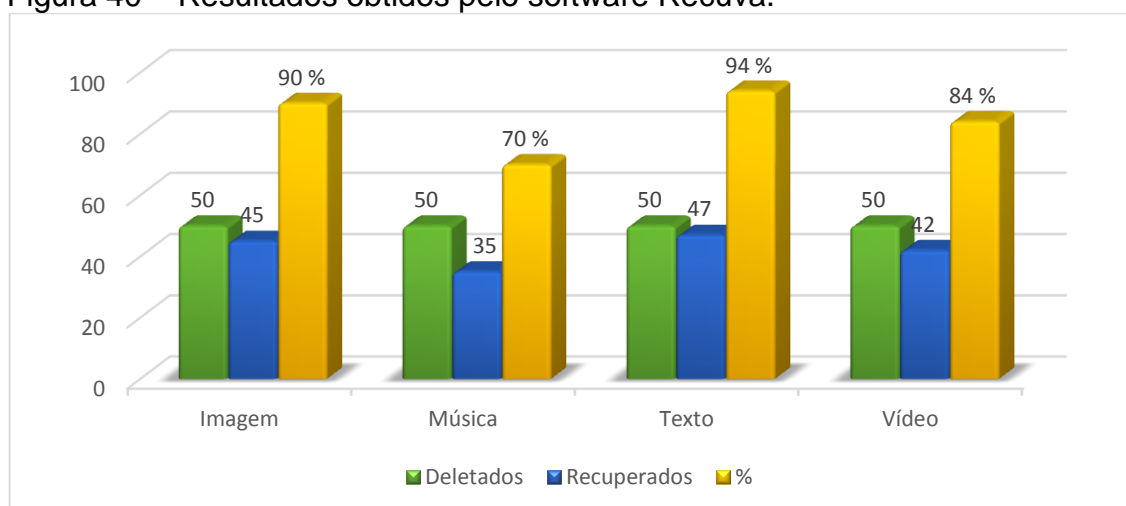
6.2 RECUPERAÇÃO DE ARQUIVOS NO SOFTWARE RECUVA - PLATAFORMA WINDOWS

A recuperação pelo *software* Recuva mostrou-se muito eficiente com arquivos nas extensões “.jpg”, “.doc”.

A quantidade de arquivos recuperados exibida na Figura 40, foi obtida com uma busca avançada no *software*. Com a busca normal a quantidade de arquivos recuperados foi menor. O tempo gasto pelo *software* na busca por arquivos foi de aproximadamente 3 horas. O programa pode ser adquirido em sua versão paga, o que aumenta seu poder de recuperação.

Pode ser considerado que, o Recuva teve este grande sucesso na recuperação, pelo fato do tempo elevado na varredura de arquivos perdidos.

Figura 40 – Resultados obtidos pelo software Recuva.



Fonte: Elaborado pelo autor (2016).

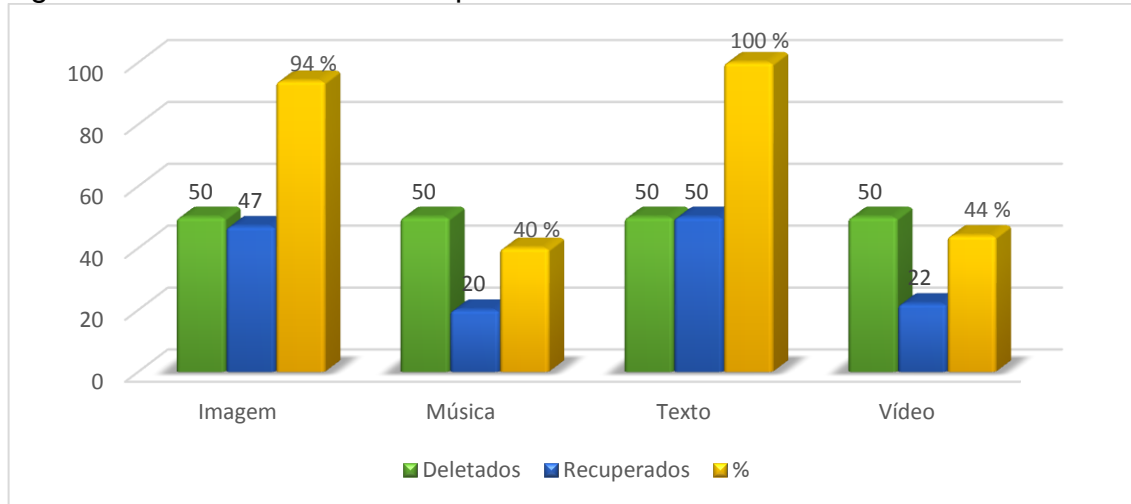
6.3 RECUPERAÇÃO DE ARQUIVOS NO SOFTWARE MINITOOL - PLATAFORMA WINDOWS

Como pode ser observado na Figura 41, o MiniTool teve um grande número de arquivos recuperados para imagens e texto, recuperando 47 arquivos de imagens e 50 arquivos de texto, mas não foi tão eficiente com arquivos de música e vídeo, recuperando somente 20 arquivos e 22 arquivos respectivamente.

Ao contrário de muitos softwares que recuperam dados corrompidos, o programa apresentou opção de *FullScan*, foi notado que no momento de analisar

arquivos de imagens e texto, o tempo aumentava no escaneamento totalizando aproximadamente 2 horas.

Figura 41 – Resultados obtidos pelo software: MiniTool.

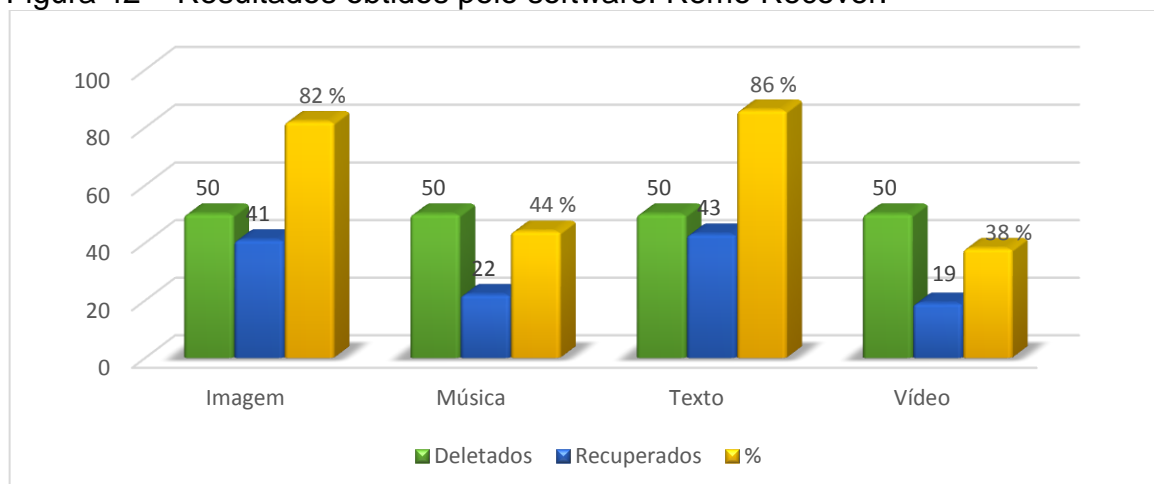


Fonte: Elaborado pelo autor (2016).

6.4 RECUPERAÇÃO DE ARQUIVOS NO SOFTWARE REMO RECOVER - PLATAFORMA WINDOWS

O Remo Recover teve uma performance parecida com o MiniTool, o Remo Recover teve melhores resultados com arquivos de texto recuperando 43 arquivos e 41 arquivos de imagens, e piores resultados com arquivos de música recuperando apenas 22 arquivos e vídeo recuperando 19 arquivos, como pode ser visto na Figura 42. O tempo de escaneamento foi de aproximadamente 1 hora.

Figura 42 – Resultados obtidos pelo software: Remo Recover.

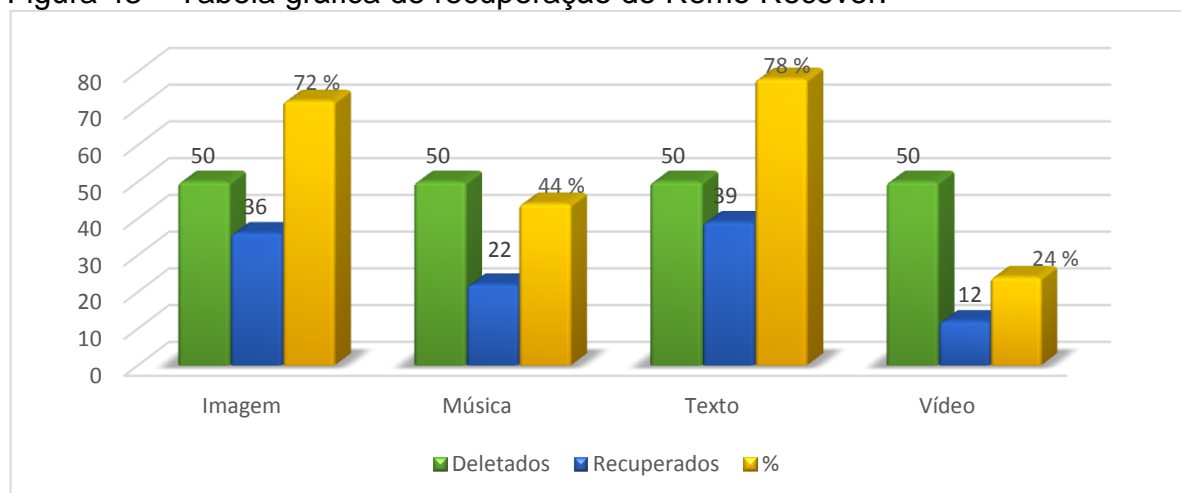


Fonte: Elaborado pelo autor (2016).

Recuperação de arquivos no Software Remo Recover - Plataforma Android.

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 imagens, 22 de músicas, 39 de textos e apenas 12 de vídeos, como pode ser visto nas Figuras 43. Neste *Software* é possível escolher a velocidade da busca entre rápido médio e lento, foi escolhido a opção médio, o desempenho apresentado pode levar em consideração a opção de busca escolhida. O Tempo recuperação aproximadamente 30 minutos.

Figura 43 – Tabela gráfica de recuperação do Remo Recover.



Fonte: Elaborado pelo autor (2016).

Recuperação de arquivos no Software DiskDigger- Plataforma Android.

A recuperação no *software* DiskDigger pode ser considerada muito precária na recuperação de arquivos de grande tamanho, como vídeos ou músicas, dependendo do tamanho do arquivo o *software* não consegue nem encontrá-los. Apenas arquivo .jpg obteve uma boa recuperação, como ilustra a Figura 44.

O tempo de localização dos arquivos deletados foi aproximadamente 8 minutos.

Figura 44 – Tabela gráfica de recuperação do DiskDigger.



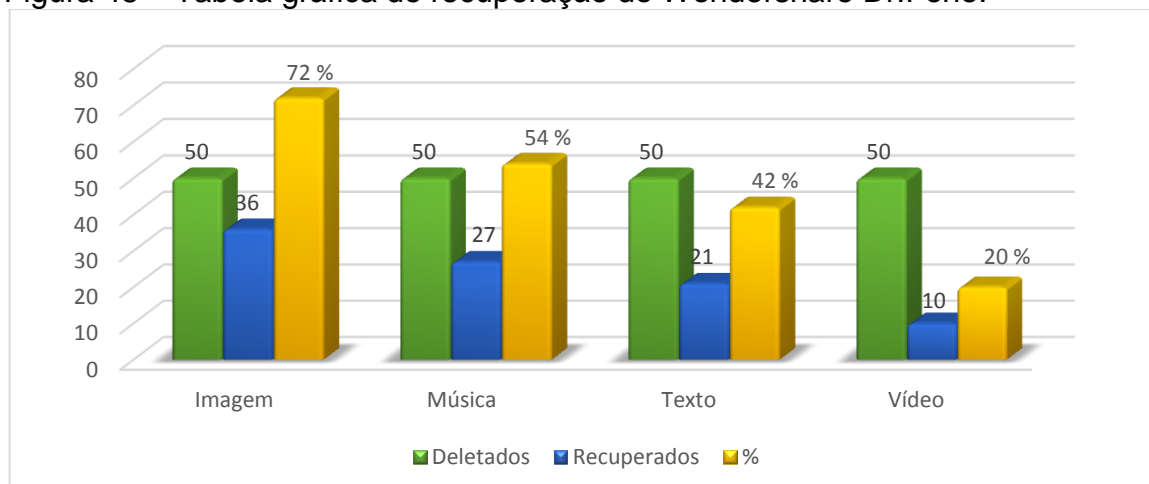
Fonte: Elaborado pelo autor (2016).

Recuperação de arquivos no Software Wondershare Dr.Fone- Plataforma Android

A recuperação no *software* Wondershare Dr.Fone - Plataforma Android se mostrou um pouco mais superior ao seu concorrente na plataforma iOS, conforme exibe a Figura 45. O programa recuperou poucos arquivos .MP4 (Vídeos), não atingiu nem 60% de recuperação nos arquivos .mp3 (músicas), seu maior desempenho foi na recuperação arquivos de .JPG (Imagem).

O tempo decorrido para a listagem dos arquivos foi de aproximadamente 1 hora.

Figura 45 – Tabela gráfica de recuperação do Wondershare Dr.Fone.



Fonte: Elaborado pelo autor (2016).

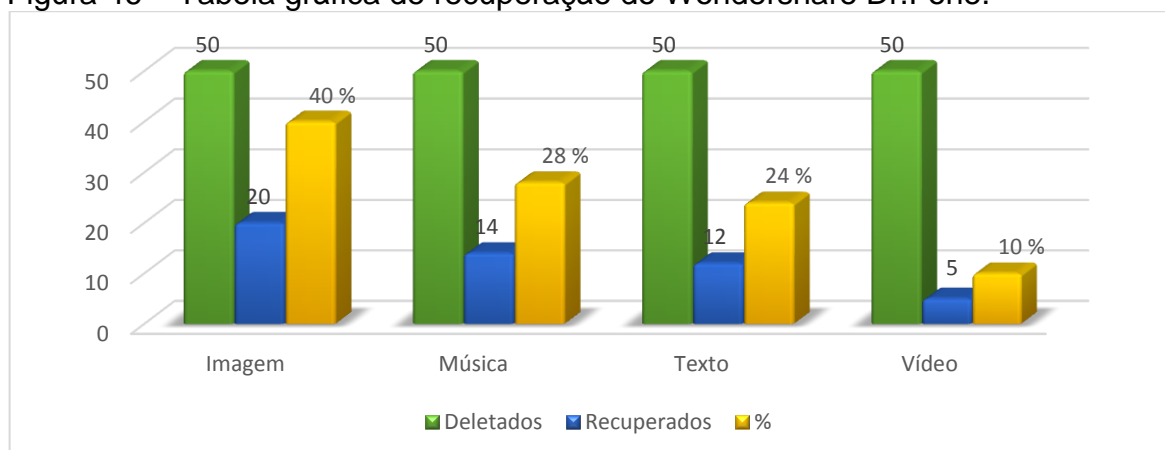
Recuperação de arquivos no Software Wondershare Dr.Fone- Plataforma IOS

A recuperação no *software* Wondershare Dr.Fone - Plataforma iOS se mostrou um pouco mais inferior, conforme exibe a Figura 46 é possível verificar que o programa recuperou poucos arquivos .MP4 (Vídeos), não atingiu nem 50% de recuperação nos arquivos .JPG (Imagem) .MP3 (músicas) .TXT (Texto).

Para baixo índice de recuperação pode ser levado em consideração o fato do sistema iOS ser mais protegido com uma segurança mais eficiente.

O tempo decorrido para a listagem dos arquivos foi o mesmo tempo no Android, aproximadamente 1 hora.

Figura 46 – Tabela gráfica de recuperação do Wondershare Dr.Fone.



Fonte: Elaborado pelo autor (2016).

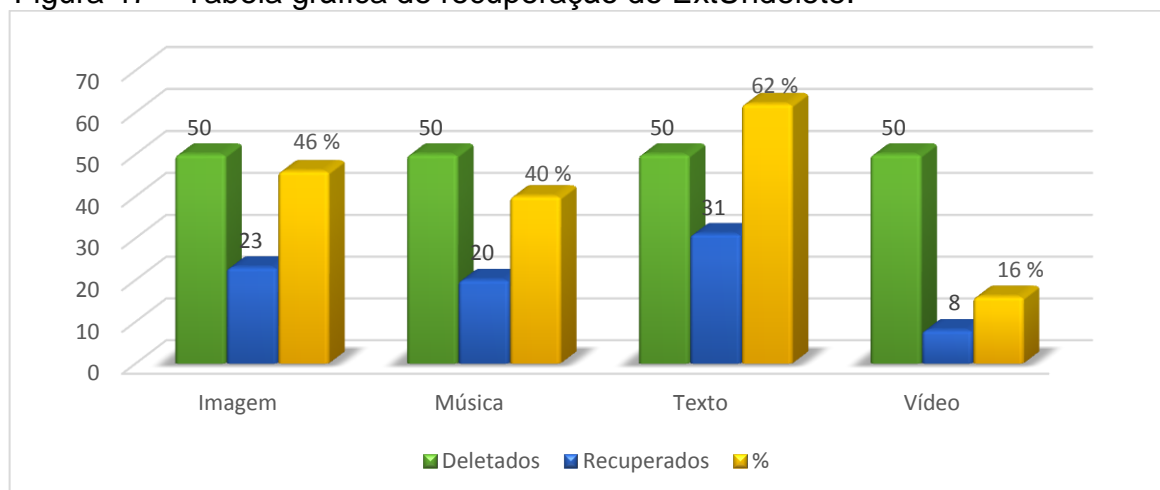
Recuperação de arquivos no Software ExtUndelete - Plataforma Linux.

A mesma sistemática do *software* Scalpel foi confirmada no ExtUndelete, por se tratarem de *softwares* parecidos, conforme o site da ExtUndelete (2013) descreve. A recuperação foi muito semelhante, a diferença encontrada foi na recuperação de arquivos de imagens e vídeo, em que o ExtUndelete obteve um desempenho inferior ao do Scalpel.

A Figura 47 ilustra o desempenho do *software* ExtUndelete, deixando claro que a recuperação de música e texto foi semelhante ao do Scalpel.

O tempo para localização dos arquivos foi aproximadamente 12 minutos.

Figura 47 – Tabela gráfica de recuperação do ExtUndelete.



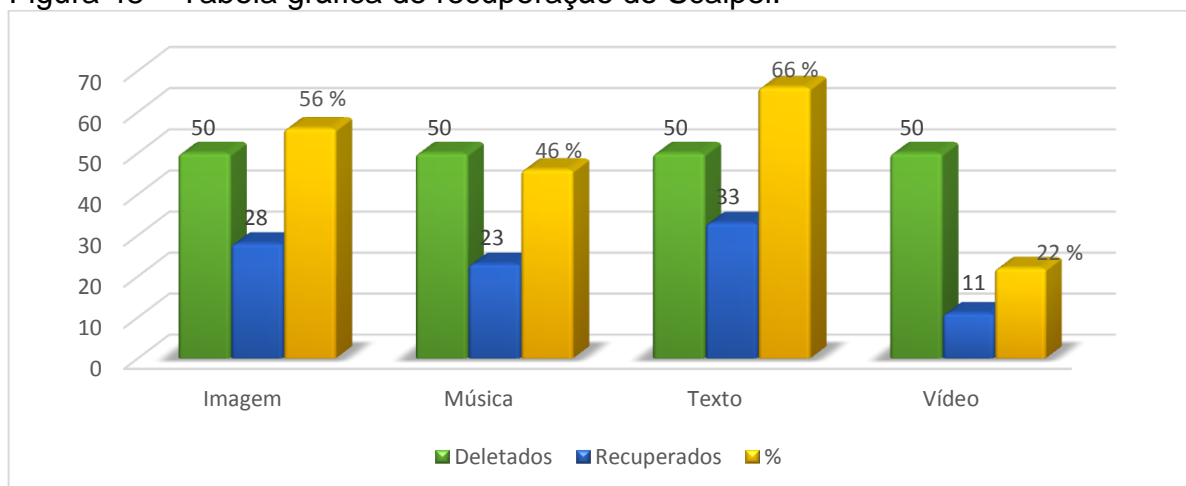
Fonte: Elaborado pelo autor (2016).

Recuperação de arquivos no Software Scalpel - Plataforma Linux.

O *software* também não obteve uma boa recuperação para arquivos de vídeos e músicas, semelhante aos outros *softwares*. Os arquivos mais recuperados foram os de imagens e textos, conforme ilustra a Figura 48.

O tempo de busca pelos arquivos deletados foi aproximadamente 14 minutos.

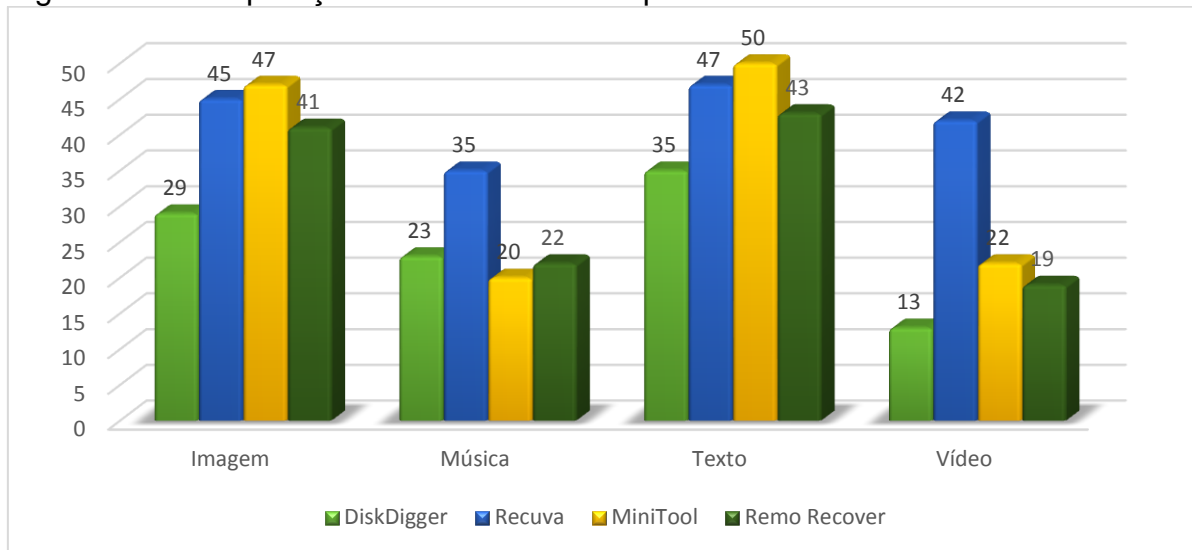
Figura 48 – Tabela gráfica de recuperação do Scalpel.



Fonte: Elaborado pelo autor (2016).

Um quadro comparativo foi elaborado demonstrando especificamente o número de arquivos recuperados por cada *software* na plataforma Windows.

Figura 49 – Comparação entre softwares na plataforma Windows.



Fonte: Elaborado pelo autor (2016).

Analisando a Figura 49, é notável que o Recuva é levemente superior aos outros, recuperando 45 arquivos de imagens, 35 de músicas, 47 de textos e 42 de vídeos, perdendo apenas na recuperação de arquivos de texto e imagem para o MiniTool que recuperou 47 imagens e 50 textos enquanto o Recuva recuperou 45 imagens e 47 textos.

Mesmo assim, todos os *softwares* tiveram um desempenho semelhante, conseguindo recuperar mais arquivos de texto e imagem.

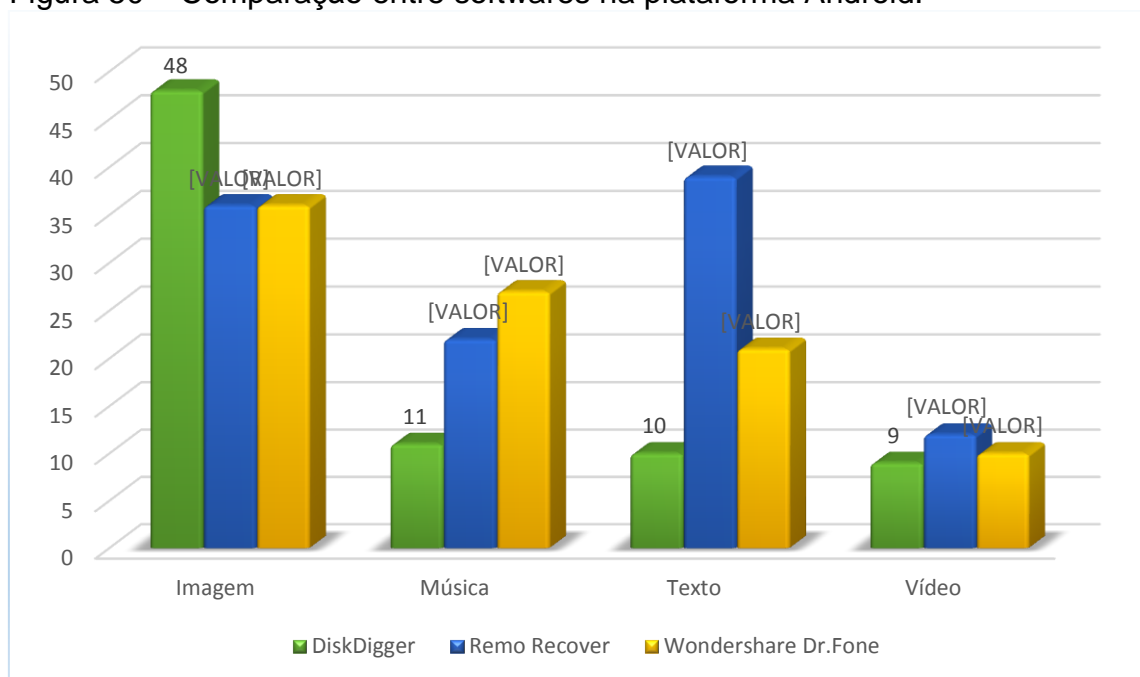
Em questão de tempo, o que mais demorou também foi o Recuva, que demorou aproximadamente 3 horas para concluir a recuperação.

Em termos de conveniência e facilidade de uso, o que mais possui uma *interface* amigável é o RemoRecover.

Vale lembrar que dentre estes *softwares* o único traduzido para o português é o Recuva e DiskDigger, para todos os outros, o usuário precisará saber um pouco de inglês para poder entender o *software* com mais facilidade.

Outro quadro comparativo foi elaborado demonstrando especificamente o número de arquivos recuperados por cada *software* na plataforma Android.

Figura 50 – Comparação entre softwares na plataforma Android.



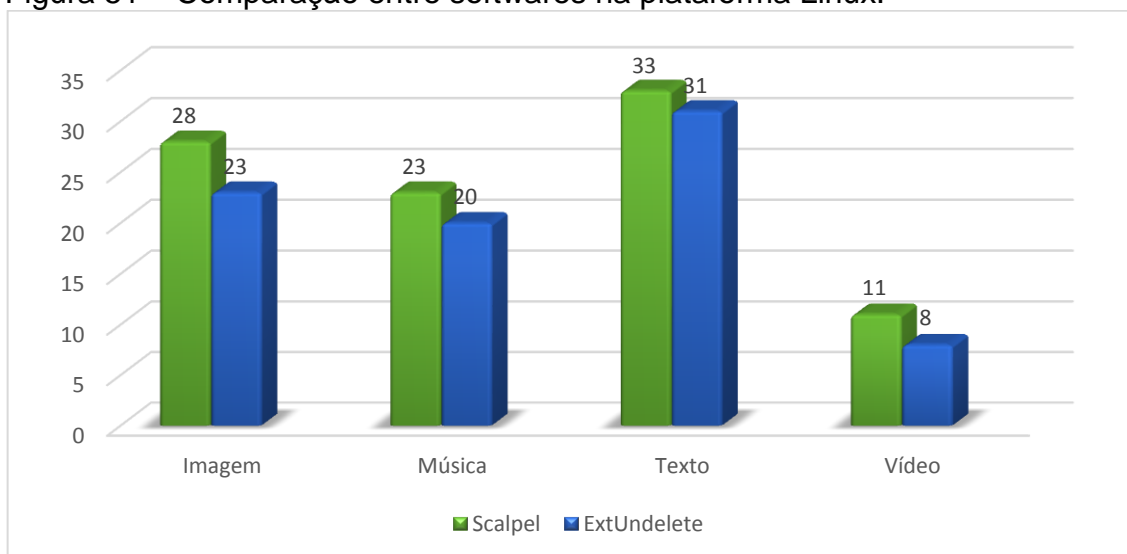
Fonte: Elaborado pelo autor (2016).

Através da Figura 50, ficou evidente que os dois *softwares* de recuperação são muito semelhantes. A quantidade de arquivos de músicas e vídeos recuperados foi baixa, houve uma grande perda de arquivos considerados de tamanho grande (acima de 10Mb).

A recuperação de arquivos de imagem foi considerada boa, uma vez que ambos *softwares* realizaram recuperação semelhante aos programas do Windows, por exemplo. A recuperação em imagens foi considerada normal e aceitável dentro dos parâmetros de recuperação das outras plataformas.

A Figura 51 exibe a comparação entre os *softwares* utilizados na plataforma Linux.

Figura 51 – Comparação entre softwares na plataforma Linux.



Fonte: Elaborado pelo autor (2016).

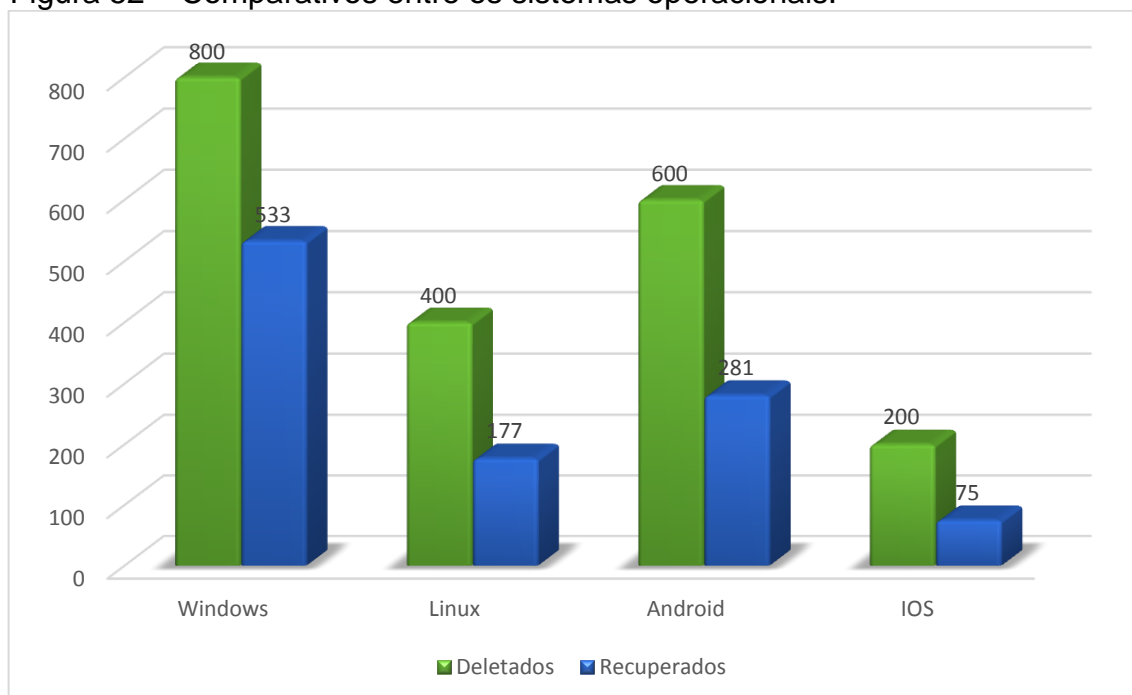
Observando a figura 51, fica claro que ambos *softwares* tiveram um desempenho semelhante e com resultados pouco satisfatório.

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 15 minutos já foi possível obter resultados.

Um quarto quadro foi desenvolvido demonstrando uma comparação entre a recuperação dos quatro sistemas operacionais utilizados.

Figura 52 – Comparativos entre os sistemas operacionais.



Fonte: Elaborado pelo autor (2016).

Analisando a Figura 52, foi constatado que o sistema operacional com maior arquivos recuperados foi o Windows; isso se deve ao fato de que os *softwares* desta plataforma realizam uma busca com um tempo elevado pelos arquivos deletados.

Comparando Android e Linux, a diferença na recuperação não foi tão grande, uma vez que a análise no Android utilizou três *softwares* e o Linux utilizou-se apenas dois.

Fica evidente também que a Plataforma Windows, por ser a mais utilizada pelos usuários, possui mais assistência nos *softwares* e maiores funcionalidades do que as outras.

Recuperação de pôr tipo de arquivos.

Um quadro foi elaborado conforme ilustra a Figura 53, demonstrando a quantidade de arquivos recuperados nas categorias de imagem, texto, música e vídeo.

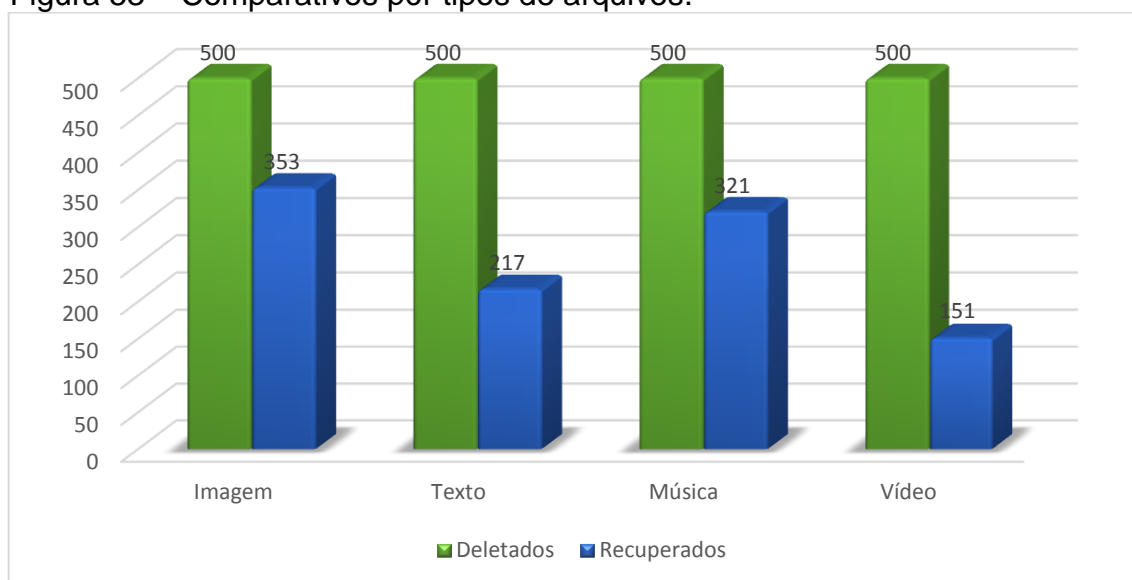
Ficou evidente que os arquivos com mais facilidade para recuperação foram os de Imagens (JPG) os arquivos de vídeos foram os que apresentaram menor quantidade de arquivos recuperados, vários *softwares* nem mesmo listaram os arquivos nos testes realizado, arquivos com tamanhos inferior a 10Mb foram

recuperados em muitos *software*, mas fica claro que a recuperação de vídeos ainda é precária.

Já a recuperação em música pode ser considerada viável, muitos arquivos foram recuperados, e a maioria dos programas pelo menos encontra os arquivos apagados; alguns *softwares* são incapazes de recuperar os arquivos mesmo listados.

Os arquivos de texto sofrem problemas semelhantes aos de vídeo, muitos textos não são listados e sua recuperação fica inviável, embora uma quantidade aceitável tenha sido recuperada.

Figura 53 – Comparativos pôr tipos de arquivos.



Fonte: Elaborado pelo autor (2016).

Um último quadro foi elaborado conforme ilustra a Figura 54, com a intenção de demonstrar uma visão geral de todos os resultados obtidos

Figura 54 - Tabela Geral.

Recuperação de Arquivos na Plataforma Windows.									
Tipo de arquivo	Deletados Fa	DiskDigger		Recuva		MiniTool		Remo Recover	
		Recuperados		Recuperados		Recuperados		Recuperados	
		Fa	Fr (%)	Fa	Fr(%)	Fa	Fr(%)	Fa	Fr(%)
Imagem	50	29	58,00	45	90,00	47	94,00	41	141,38
Música	50	23	46,00	35	70,00	20	40,00	22	95,65
Texto	50	35	70,00	47	94,00	50	100,00	43	122,86
Vídeo	50	13	26,00	42	84,00	22	44,00	19	146,15
Total	200	100		169		139		125	

Recuperação de Arquivos na Plataforma Android.							
Tipo de arquivo	Deletados Fa	DiskDigger		Remo Recover		Wondershare Dr.Fone	
		Recuperados		Recuperados		Recuperados	
		Fa	Fr (%)	Fa	Fr(%)	Fa	Fr(%)
Imagem	50	48	96,00	36	72,00	36	37,50
Música	50	11	22,00	22	44,00	27	122,73
Texto	50	10	20,00	39	78,00	21	105,00
Vídeo	50	9	18,00	12	24,00	10	55,56
Total	200	78		109		94	

Recuperação de arquivos na Plataforma IOS

Wondershare Dr.Fone			
Tipo de arquivo	Deletados Fa	Recuperados	
		Fa	Fr (%)
Imagem	50	20	40,00
Música	50	14	28,00
Texto	50	12	24,00
Vídeo	50	5	10,00
Total	200	51	102

Recuperação de Arquivos na Plataforma Linux.

Tipo de arquivo	Deletados Fa	Scalpel		ExtUndelete	
		Recuperados		Recuperados	
		Fa	Fr (%)	Fa	Fr (%)
Imagem	50	28	56,00	23	46,00
Música	50	23	46,00	20	40,00
Texto	50	33	66,00	31	62,00
Vídeo	50	11	22,00	8	16,00
Total	200	95		82	

Recuperação de por tipo de arquivos

Tipo de arquivo	Deletados Fa	Recuperados	
		Fa	Fr (%)
Imagem	500	353	70,60
Texto	500	217	43,40
Música	500	321	64,20
Vídeo	500	151	30,20
Total	2000	1042	

Comparativo de Recuperação entre as plataformas.

Plataforma	Deletados Fa	Recuperados	
		Fa	Fr(%)
Windows	800	533	66,63
Linux	400	177	44,25
Android	600	281	46,83
IOS	200	51	25,50
Total	2000	1042	

Fonte: Elaborada pelo autor.

7 CONSIDERAÇÕES FINAIS

Considerando a grande crescente de informações utilizadas em aparelhos eletrônicos, é indispensável a utilização de técnicas de perícia forense computacional na recuperação de dados, uma vez que a possibilidade de roubo ou até mesmo perda de informações se torna cada vez mais alta.

Diversas ferramentas de recuperação de dados são desenvolvidas com finalidade de recuperar dados perdidos ou deletados, tanto para uso pessoal quanto corporativo. Devido está grande necessidade na perícia forense atualmente, fica cada vez mais evidente no mercado a necessidades de *softwares* com estas funções.

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.

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

Em geral o *software* que teve melhor desempenho foi Recuva, da plataforma Windows. Apesar de demorar um pouco mais na recuperação, foi o que mais conseguiu recuperar dados.

Como segunda melhor performance ficou o MiniTool, o qual de 200 arquivos deletados recuperou 139, confirmando um excelente desempenho. Ficando muito abaixo da média o software DiskDigger recuperou somente 100 arquivos. Com os testes realizados fica claro que o tempo gasto na busca pelos arquivos interfere em sua recuperação, pois o Recuva gastou cerca de 3 horas para realizar a checagem por arquivos deletados, confrontando diretamente com o DiskDigger, que demorou 50 minutos e recuperou 100 arquivos.

A performance da plataforma Linux foi relativamente bom, deixando a desejar na recuperação de arquivos de vídeo; embora todas as outras plataformas também sofram com este problema, por se tratar de Linux, esperava-se um desempenho melhor.

O desempenho na plataforma IOS e Android foi um pouco mais satisfatório no Android, talvez isso se deve ao fato de possuir uma segurança no iOS mais eficiente, dificultando na procura de arquivos deletados.

Um ponto observado é a dificuldade de se remover por completo alguns arquivos, pois cada vez mais ferramentas sofisticadas surgirão. Nesse sentido pode-se realizar uma pesquisa futura com possibilidade de analisar novas ferramentas de recuperação.

Também em projetos futuros, seria interessante a utilização de outros tipos de arquivos como RAR, PDF, MOV, WAV, ZIP, XLSX, realizar outros tipos de formatações e pesquisar técnicas forenses em busca de arquivos deletados em outras plataformas, como Windows Phone uma vez que a quantidade de plataformas só aumenta.

REFERÊNCIAS

ALMEIDA, R. N. **Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais**. Disponível em: <<http://www.fatecsp.br/dti/tcc/tcc0035.pdf>>. Acesso em: 30 mar. 2016.

ALECRIM, E. Criptografia. **Infowester**, c2009. Disponível em: <<http://www.infowester.com/criptografia.php>>. Acesso em: 16 abr. 2016.

ALMEIDA, R. Q. Foremost e Scalpel - Recuperação de arquivos. **Linha de código**, 2009. Disponível em: <<http://www.linhadecodigo.com.br/artigo/2968/foremost-e-scalpel-recuperacao-de-arquivos.aspx>> Acesso em: 10 abr. 2016.

ALECRIM, E. O que é Linux e qual a sua história?. **Infowester**, 2011. Disponível em: <http://www.infowester.com/historia_linux.php> Acesso em: 06 abril. 2016.

ALVES, P. DiskDigger recupera dados apagados do seu PC e Android com um clique. **Tecnundo**, 2014. Disponível em: <<http://www.techtudo.com.br/tudo-sobre/diskdigger.html>> Acesso em: 10 abr. 2016.

ASSIS, P. Conheça os cybercrimes e aprenda a se defender deles. **Tecnundo**, 2010. Disponível em: <<http://www.tecnundo.com.br/conexao/3486-conheca-os-cybercrimes-e-aprenda-a-se-defender-deles.htm>> Acesso em: 06 abr. 2016.

BARROS, T. Cinco anos de Android: relembre a história e todas as versões do sistema. **Tecnudo**, 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: 05 abr. 2016.

BARROS, T. Conheça o Android, o sistema operacional móvel do Google. **Tecnudo**, 2015. Disponível em: <<http://www.techtudo.com.br/tudo-sobre/android.html>> Acesso em: 05 abr. 2016.

BARWINSKI, L. O que é rootkit?. **Tecnundo**, 2009. Disponível em: <<http://www.tecnundo.com.br/antivirus/2174-o-que-e-rootkit-.htm>>. Acesso em: 16 Abr. 2016.

COUTINHO, P. S. **Esteganografia**. Disponível em: <http://www.gta.ufrj.br/grad/08_1/estegano/index.html>. Acesso em: 02 jul. 2013.

COSTA, D. M. **Boas Práticas para Perícia Forense**. Disponível em: <<http://bibdig.poliseducacional.com.br/document/?down=174>> Acesso em: 18 Abr. 2016.

DAVID, R. **Realizando Perícia**. Disponível em: <<http://www.ebah.com.br/content/ABAAAA-hcAE/realizando-pericia>> Acesso em: 03 Abr. 2016.

DAMACENA, B. L. C. **Desafios da Perícia Forense em um Ambiente de Computação nas Nuvens**. Disponível em:

<https://webcache.googleusercontent.com/search?q=cache:R4i1zgX__9wJ:https://revisa.uniupl.net/ojs/index.php/tc_si/article/view/1911/988+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 25 Abr. 2016.

EULER, G. Recuva – Recupera fotos e arquivos apagados acidentalmente. **Infodicas**, 2012. Disponível em:< http://www.infodicas.com.br/dicas_tuto/recuva-recupera-fotos-e-arquivos-apagados-acidentalmente> Acesso em: 10 Abr. 2016.

FERREIRA, R. Saiba como recuperar arquivos apagados no Linux usando o extundelete. **Linux descomplicado**, 2014. Disponível em:<<http://www.linuxdescomplicado.com.br/2014/02/saiba-como-recuperar-arquivos-apagados.html>>Acesso em: 09 Abr. 2016.

FREITAS, R. F. **Perícia Forense Aplicada à Informática**. 1ª. Rio de Janeiro: Brasport, 2006. Disponível em:<<https://books.google.com.br/books?id=HT-MhC3RxR0C&pg=PA1&dq=per%C3%ADcia+computacional&hl=pt-BR&sa=X&ved=0ahUKEwir4fPHwK3MAhVDjZAKHc7PD9MQ6AEINDAA#v=onepage&q=per%C3%ADcia%20computacional&f=false>>. Acesso em: 19 Abr. 2016.

GUGIK, G. 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: 09 abr. 2016.

HAMMERSCHMIDT, R. Remo Recover for Android. 2013. Disponível em: <<http://www.baixaki.com.br/download/remo-recover-for-android.htm>>. Acesso em 08 out. 2016.

HENRIQUE, M. EnCase Forensic – Recuperando Dados. **100security**, 2013. Disponível em:< <http://www.100security.com.br/encase-forensic-recuperando-dados/>> Acesso em: 21 Abr. 2016.

JORDÃO, F. História: a evolução do celular. **Tecmundo**, 2009. Disponível em: <<http://www.tecmundo.com.br/celular/2140-historia-a-evolucao-do-celular.htm>>. Acesso em: 28 mar. 2016.

KAMIYA, V. S. **Perícia Forense Computacional Aplicada a Computadores e Smartphones e Android**. 2014. 58 f. Trabalho de conclusão de curso (Graduação em Ciência da Computação) - Universidade do Sagrado Coração, Bauru, 2014.

KOBUSZEWSKI, A. **Protótipo para Ocultação de Textos**. Disponível em:<http://www.bc.furb.br/docs/MO/2004/305290_1_1.pdf>. Acesso em: 16 abr. 2016.

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. **Hackers expostos segredos e soluções para a segurança de redes**. 4ª. Campus, 2003.

MICROSOFT, Uma história do Windows. **Windows**, 2015. Disponível em:<<http://windows.microsoft.com/pt-br/windows/history#T1=era0>> Acesso em: 05 abr. 2016.

- NEUKAMP, P. A. Forense Digital.**fdtk**, 2015. Disponível em: <<http://fdtk.com.br/wiki/tiki-index.php?page=Inicial>> Acesso em: 08 abr. 2016.
- PEIXOTO, B. F. **O Desenvolvimento da Telefonia Celular pré-paga no Brasil e o Consumo da População de Baixo Poder Aquisitivo: Análise dos Fatores Determinantes do Período Recente**. 2007. Trabalho de conclusão de curso (Graduação em Ciências Econômicas) - Universidade Federal da Bahia, Salvador, 2007. Disponível em: <<http://www.repositorio.ufba.br:8080/ri/bitstream/ri/9758/1/Monografia%20completa%20Berenice.pdf>> Acesso em: 28 mar. 2016.
- RINALDI, C. Android 6.0 Marshmallow - todas as principais funções explicadas. **Androidpit**, 2016. Disponível em: <<http://www.androidpit.com.br/android-m-dispositivos-data-lancamento-funcoes>> Acesso em: 05 abr. 2016.
- ROHR, A. **Rootkits: Conheça as Ameaças que Ficam Invisíveis no Sistema**. Disponível em: <<http://g1.globo.com/Noticias/Tecnologia/0,,MUL1499791-6174,00-ROOTKITS+CONHECA+AS+AMEACAS+QUE+FICAM+INVISIVEIS+NO+SISTEMA.html>>. Acesso em: 16 Abr. 2016.
- SAMPAIO, M. Linux Forense. **Infocrime**, 2013. Disponível em: <<http://www.infocrime.com.br/2013/09/linux-forense/>> Acesso em: 21 Abr. 2016.
- TROYACK, L.; YUNG, R. 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: 03 abr. 2016.
- VARGAS, R. Novo Forensic Toolkit 3.0. **Imasters**, 2009. Disponível em: <<http://imasters.com.br/artigo/14668/gerencia-de-ti/novo-forensic-toolkit-30/>> Acesso em: 21 abr. 2016.
- WEYER, A. S. **Perícia computacional – ferramentas, técnicas disponíveis e estudo de caso**. 2011. Trabalho de conclusão de curso (Curso de Tecnologia em Redes de Computadores) - Universidade Luterana do Brasil, Canoas, 2011. Disponível em: <http://www.ulbra.inf.br/joomla/images/documentos/TCCs/2011_02/PROJETO_R_C_ALEX_SANDRO_WEYER.pdf> Acesso em: 10 mar. 2016.
- WONDERSHARE, O Software Nº1 do Mundo na Recuperação de Dados para Android. **Wondershare**, 2016. Disponível em: <<http://www.wondershare.com.br/data-recovery/android-data-recovery.html>> Acesso em: 09 abr. 2016.
- WONDERSHARE, O Software Nº1 do Mundo na Recuperação de Dados do iPhone e iPad. **Wondershare**, 2016. Disponível em: <<http://www.wondershare.com.br/data-recovery/iphone-data-recovery.html>> Acesso em: 09 abr. 2016.

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

Tabela 1 - Recuperação de arquivos no Software DiskDigger - Plataforma Windows

Tipo de arquivo	Deletados		Recuperados	
	Fa	Fr (%)	Fa	Fr (%)
Imagem	50	25,00	29	58,00
Música	50	25,00	23	46,00
Texto	50	25,00	35	70,00
Vídeo	50	25,00	13	26,00
Total	200	100,00	100	200,00

Fonte: Elaborada pelo Autor (2016).

Tabela 2 - Recuperação de arquivos no Software Recuva - Plataforma Windows

Tipo de arquivo	Deletados		Recuperados	
	Fa	Fr (%)	Fa	Fr (%)
Imagem	50	25,00	45	90,00
Música	50	25,00	35	70,00
Texto	50	25,00	47	94,00
Vídeo	50	25,00	42	84,00
Total	200	100,00	169	338,00

Fonte: Elaborada pelo Autor (2016).

Tabela 3 - Recuperação de arquivos no Software MiniTool - Plataforma Windows

Tipo de arquivo	Deletados		Recuperados	
	Fa	Fr (%)	Fa	Fr (%)
Imagem	50	25,00	47	94,00
Música	50	25,00	20	40,00
Texto	50	25,00	50	100,00
Vídeo	50	25,00	22	44,00
Total	200	100,00	139	278,00

Fonte: Elaborada pelo Autor (2016).

Tabela 4 - Recuperação de arquivos no Software Remo Recover - Plataforma Windows

Tipo de arquivo	Deletados		Recuperados	
	Fa	Fr (%)	Fa	Fr (%)
Imagem	50	25,00	41	82,00
Música	50	25,00	22	44,00
Texto	50	25,00	43	86,00
Vídeo	50	25,00	19	38,00
Total	200	100,00	125	250,00

Fonte: Elaborada pelo Autor (2016).

Fa: Frequência absoluta.

Fr: Frequência relativa. Estas notações aplicam-se a todas as tabelas.

Tabela 5 - Recuperação de arquivos no Software DiskDigger - Plataforma Android

Tipo de arquivo	Deletados		Recuperados	
	Fa	Fr (%)	Fa	Fr (%)
Imagem	50	25,00	48	96,00
Música	50	25,00	11	22,00
Texto	50	25,00	10	20,00
Vídeo	50	25,00	9	18,00
Total	200	100,00	78	156,00

Fonte: Elaborada pelo Autor (2016).

Tabela 6 - Recuperação de arquivos no Software Remo Recover - Plataforma Android

Tipo de arquivo	Deletados		Recuperados	
	Fa	Fr (%)	Fa	Fr (%)
Imagem	50	25,00	36	72,00
Música	50	25,00	22	44,00
Texto	50	25,00	39	78,00
Vídeo	50	25,00	12	24,00
Total	200	100,00	109	218,00

Fonte: Elaborada pelo Autor (2016).

Tabela 7 - Recuperação de arquivos no Software Wondershare Dr.Fone - Plataforma Android

Tipo de arquivo	Deletados		Recuperados	
	Fa	Fr (%)	Fa	Fr (%)
Imagem	50	25,00	36	72,00
Música	50	25,00	27	54,00
Texto	50	25,00	21	42,00
Vídeo	50	25,00	10	20,00
Total	200	100,00	94	188,00

Fonte: Elaborada pelo Autor (2016).

Tabela 8 - Recuperação de arquivos no Software Wondershare Dr.Fone - Plataforma IOS

Tipo de arquivo	Deletados		Recuperados	
	Fa	Fr (%)	Fa	Fr (%)
Imagem	50	25,00	20	40,00
Música	50	25,00	14	28,00
Texto	50	25,00	12	24,00
Vídeo	50	25,00	5	10,00
Total	200	100,00	51	102,00

Fonte: Elaborada pelo Autor (2016).

Tabela 9 - Recuperação de arquivos no Software ExtUndelete - Plataforma Linux

Tipo de arquivo	Deletados		Recuperados	
	Fa	Fr (%)	Fa	Fr (%)
Imagem	50	25,00	23	46,00
Música	50	25,00	20	40,00
Texto	50	25,00	31	62,00
Vídeo	50	25,00	8	16,00
Total	200	100,00	82	164,00

Fonte: Elaborada pelo Autor (2016).

Tabela 10 - Recuperação de arquivos no Software Scalpel - Plataforma Linux

Tipo de arquivo	Deletados		Recuperados	
	Fa	Fr (%)	Fa	Fr (%)
Imagem	50	25,00	28	56,00
Música	50	25,00	23	46,00
Texto	50	25,00	33	66,00
Vídeo	50	25,00	11	22,00
Total	200	100,00	95	190,00

Fonte: Elaborada pelo Autor (2016).

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

Tabela 9 - Recuperação de Arquivos na Plataforma Windows.

Tipo de arquivo	DiskDigger			Recuva		MiniTool		Remo Recover	
	Deletados Fa	Recuperados Fa	Recuperados Fr (%)	Recuperados Fa	Recuperados Fr (%)	Recuperados Fa	Recuperados Fr (%)	Recuperados Fa	Recuperados Fr (%)
Imagem	50	29	58,00	45	90,00	47	94,00	41	141,38
Música	50	23	46,00	35	70,00	20	40,00	22	95,65
Texto	50	35	70,00	47	94,00	50	100,00	43	122,86
Vídeo	50	13	26,00	42	84,00	22	44,00	19	146,15
Total	200	100		169		139		125	

Fonte: Elaborada pelo Autor (2016).

Tabela 10 - Recuperação de Arquivos na Plataforma Android.

Tipo de arquivo	Deletados Fa	DiskDigger		Remo Recover		Wondershare Dr.Fone	
		Recuperados Fa	Fr (%)	Recuperados Fa	Fr(%)	Recuperados Fa	Fr(%)
Imagem	50	48	96,00	36	72,00	36	37,50
Música	50	11	22,00	22	44,00	27	122,73
Texto	50	10	20,00	39	78,00	21	105,00
Vídeo	50	9	18,00	12	24,00	10	55,56
Total	200	78		109		94	

Fonte: Elaborada pelo Autor (2016).

APÊNDICE C – TABELA DE RECUPERAÇÃO DE ARQUIVOS ENTRE OS SISTEMAS OPERACIONAIS UTILIZADOS

Tabela 12 - Comparativo de Recuperação entre as plataformas.

Plataforma	Deletados		Recuperados	
	Fa	Fr (%)	Fa	Fr (%)
Windows	800	66,63	533	
Linux	400	44,25	177	
Android	600	46,83	281	
IOS	200	25,50	51	
Total	2000		1042	

Fonte: Elaborada pelo Autor (2016).

APÊNDICE D – TABELA DE RECUPERAÇÃO DE ARQUIVOS POR TIPO DE ARQUIVOS

Tabela 13- Recuperação de por tipo de arquivos

Tipo de arquivo	Deletados		Recuperados	
	Fa	Fr (%)	Fa	Fr (%)
Imagem	500	70,60	353	
Texto	500	43,40	217	
Música	500	64,20	321	
Vídeo	500	30,20	151	
Total	2000		1042	

Fonte: Elaborada pelo Autor (2016).

