UNIVERSIDADE SAGRADO CORAÇÃO

RAPHAEL PINHEIRO AFONSO

PERÍCIA FORENSE COMPUTACIONAL APLICADA A DISPOSITIVOS DE ARMAZENAMENTOS E SMARTPHONES ANDROID

BAURU
2013

RAPHAEL PINHEIRO AFONSO

PERÍCIA FORENSE COMPUTACIONAL APLICADA A DISPOSITIVOS DE ARMAZENAMENTOS E SMARTPHONES 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
2013

RAPHAEL PINHEIRO AFONSO

PERÍCIA FORENSE COMPUTACIONAL APLICADA A SMARTPHONES

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

Banca examinadora:

_____
Prof. Dr. Elvio Gilberto da Silva
Universidade Sagrado Coração

_____
Prof. Esp. Henrique Pachioni Martins
Universidade Sagrado Coração

_____
Prof. Me. Patrick Pedreira Silva
Universidade Sagrado Coração

Bauru, 25 de Novembro de 2013.

Dedico este trabalho a minha família e a todos os envolvidos.

AGRADECIMENTOS

Aos meus pais Edson e Cristina, pelo apoio, confiança, educação, amor, carinho e ajuda em todos os sentidos.

Ao meu irmão Vitor, pela honra e alegria de ser seu irmão.

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

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

Aos meus verdadeiros amigos, que sempre me ajudaram nos momentos em que necessitei.

Aos funcionários com quem trabalho na USC, pela compreensão e ajuda em todos os momentos.

RESUMO

Com o crescente avanço da tecnologia, a Internet tem se tornado uma das principais ferramentas de comunicação. Vinculada a ela estão todos os tipos de serviços, tais como: pagamentos de contas *online*, compras em *sites*, comunicação em redes sociais, entre outros. Para que isso seja possível, faz-se o uso de computadores, *tablets* e *smartphones*. Porém, esta facilidade pode gerar grandes complicações futuras, tanto para usuários domésticos ou corporativos, uma vez que tem se tornado frequente a invasão de tais dispositivos por criminosos. Uma das ameaças que podem colocar em risco a segurança da informação, e uma das grandes preocupações em TI, é a perda de dados ou sua subtração por criminosos, colocando em risco a segurança das empresas, organizações e indivíduos. Com a expansão da Internet, computadores e outros dispositivos eletrônicos estão sendo usados para cometer crimes digitais. Com isso, o uso de provas eletrônicas está cada vez mais envolvido em crimes digitais. Com base neste contexto este trabalho analisou técnicas e *softwares* de perícia forense computacional, para recuperação de arquivos deletados em dispositivos de armazenamento e *smartphones*, com sistema operacional *Android*. Os resultados demonstraram a capacidade de cada *software* com base nos testes realizados.

Palavras-Chave: Segurança. Perícia Forense. Computadores. *Smartphones*.

ABSTRACT

Due to the increasing technology development, the Internet has become one of the main communication tools. Besides, there are all kind of services related to it, such as online bill payment, on-line stores, social network communication etc. However, such convenience can bring big problems in the future for both home and corporate users since criminals have been hacking such devices more frequently. One of the threats and major concerns in Information Technology that can put the information security at risk is the data loss or stealing by criminals, putting companies, individuals, and organization security at risk. Along with the Internet expansion, computers and others electronic devices are being used to commit cyber crimes. Thus, digital evidence has been used very often in cybercrimes. Thus, the use of electronic evidence is increasingly involved in cybercrime. Based on this context, this paper analyzed computer forensic software's and techniques to recover deleted files in storage and smartphones with Android operating system devices . The results demonstrated the ability of each software based on tests.

Keywords: Security. Forensics. Computers. Smartphones.

SUMÁRIO

LISTA DE FIGURAS E ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ACC	*Advanced Audio Coding*
CLOUD	*Computação em nuvem*
CMD	*Prompt de Comando*
Fitas DAT	*Digital Audio Tape*
GPS	*Global Positioning System*
GSM	*Global System for Mobile Communications ou Groupe Spécial Mobile*
HDs	*Hard Disks*
MP3	*Moving Picture Experts Group 1 (MPEG) Audio Layer 3 (formato de compactação de áudio)*
MS-DOS	*MicroSoft Disk Operating System*
NTFS	*New Technology File System (sistema de arquivos)*
SSD	*Solid State Disk*
TDMA	*Time Division Multiple Access*
TI	*Tecnologia da Informação*
WMA	*Windows Media Audio*

1 INTRODUÇÃO

Na década de 1990, os computadores mal ocupavam espaço no âmbito corporativo, porém ninguém imaginaria que um dia teríamos um em casa e muitos menos no bolso. Nessa época, os computadores eram artigos de luxo e só eram utilizados por empreendimentos que podiam bancar o alto investimento. Atualmente, é difícil imaginar alguém sem computador, até mesmo os menores empreendimentos têm pelos menos um com conexão à Internet. A tecnologia também evoluiu em outros setores e nos últimos 10 anos, os celulares que antes eram verdadeiros itens de luxo tornaram-se mais um item do dia a dia de cada um (MIGUEL, 2010).

Em 1990, eles quase não existiam e os modelos eram muito restritos. Havia celulares com mais de 15 cm e pesando quase 1 Kg. Hoje, eles possuem acesso à internet, navegação via satélite (GPS), câmeras fotográficas e filmadores em HD (*High Definition*) e outros recursos como tecnologia AMOLED[1] e *touchscreen*[2].

Atualmente, devido ao grande uso dos computadores, cada vez mais o ser humano depende deles, seja para empresas privadas, órgãos do governo, escolas, pequenos empreendimentos, residências etc. Esta dependência trazida pelas facilidades que os computadores nos trouxeram pode parecer inofensiva, mas basta um simples problema de ordem técnica e uma instituição pode estar arruinada por completo, caso não esteja preparada para a situação.

Uma das ameaças que podem colocar em risco a segurança da informação, e uma das grandes preocupações em TI, é a perda de dados ou sua subtração por criminosos, colocando em risco a segurança das empresas, organizações e indivíduos. Com a expansão da Internet, computadores e outros dispositivos eletrônicos estão sendo usados para cometer crimes digitais. Com isso, o uso de provas eletrônicas está cada vez mais envolvido em crimes digitais.

Os celulares entraram na lista dos equipamentos utlizados para roubos de informações, invasões, ataque de vírus, entre outros crimes ligados à informática. Atualmente, o mercado de celulares evolui absurdamente e, hoje, têm-se os *smartphones.*

---

[1] Imagens mais nítidas e brilhantes, alta distinção de movimentos, cores reais e muito mais variadas do que o normal, menor espessura e maior flexibilidade.

[2] Tela sensível ao toque, sendo um display eletrônico visual que pode detectar a presença e localização de um toque dentro da área de exibição, por meio de pressão.

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

Com o aumento dos recursos existentes no Sistema Operacional dos dispositivos móveis, a capacidade cada vez maior de processamento e armazenamento, os *smartphones* se tornaram grandes provedores de informações. Assim, a análise pericial nesse tipo de dispositivo pode trazer informações a respeito do seu usuário, devido ao fato de que funcionalidades como: armazenamento de arquivos, histórico de Internet, agenda, contatos, e até mesmo acesso em aplicativos de computação em nuvem, estarão disponíveis no *smartphone.*

Alguns procedimentos devem ser seguidos pelo perito para assegurar que a evidência não seja comprometida, substituída ou perdida (FREITAS, 2007).

A falta de profissionais na área de perícia forense computacional leva muitas pessoas a saírem impunes de crimes cometidos contra pessoas ou empresas.

> Quando o assunto é segurança da informação, os maiores riscos para as empresas são represálias de ex-funcionários e a ausência de recursos adequados para uma preparação adequada. Esta é a conclusão do 12º estudo anual Ernst & Young sobre Segurança da Informação, realizado em âmbito global. A represália de ex-funcionários contra seus ex-empregadores é o motivo de maior preocupação para 75% dos gerentes de TI. (Ernst & Young Terco, 2010).

Muitas vezes, a questão não é apenas a astúcia e o conhecimento do criminoso, mas também a falta de preparo, e até mesmo uma certa “inocência” por parte dos responsáveis da segurança do sistema.

A Perícia Forense Computacional é considerada uma área em expansão. Tornou-se uma prática investigativa importante tanto para empresas quanto para a polícia. A cada dia aparecem novos tipos de crimes que necessitam de pessoal qualificado, em constante atualização, para a realização de coleta das evidências,

preservação e análise, procurando vestígios que possam esclarecer como aconteceu e quem realizou (FARMER; VENEMA, 2007).

De acordo com o dicionário Aurélio (2009), “perícia forense é a prática que um profissional qualificado exerce, neste caso denominado de perito. Vistoria ou exame de caráter técnico e especializado. Conhecimento, ciência”. A Perícia Forense na área computacional inclui análise de mídias, por exemplo, HDs, discos ópticos, *pen drives*, discos SSD, memória RAM etc. Buscando arquivos e conteúdo específico associado a algum tipo de crime digital, tal procedimento utiliza *hardware* e *software* que podem acessar essas mídias sem modificar ou alterar seu conteúdo na procura de evidências para esclarecer um crime digital, podendo ser um roubo, troca de mensagens, alteração de arquivos, cópia não autorizadas de informações sigilosas, compartilhamento de arquivos proibidos (pornografia infantil), acesso não autorizado entre outros.

Os profissionais na área têm regras a seguir, providências definidas a tomar, para que obtenham credibilidade no que fazem; artigos específicos sobre como um capacitado deve proceder em uma investigação para que seu trabalho não tenha sido em vão e desconsiderado em uma audiência judicial, na qual um parecer técnico será necessário. Os peritos devem elaborar o laudo pericial descrevendo minuciosamente o que examinaram, respondendo aos quesitos formulados (QUEIROZ; VARGAS, 2010).

Com base neste contexto, este estudo tem por finalidade realizar um comparativo entre as ferramentas utilizadas na recuperação de arquivos de um dispositivo de armazenamento e em celulares *smartphones*, resultando na confecção de um relatório com informações sobre as características dos *softwares* analisados e suas potencialidades.

2 ORGANIZAÇÃO DO TRABALHO

O Capítulo 1 apresenta a introdução do trabalho.

No Capítulo 2 é apresentada a organização deste trabalho.

Já no Capítulo 3 os objetivos gerais e específicos são detonatos.

No Capítulo 4 o referencial teórico relativo à evolução dos celulares, sistemas operacionais utilizados, segurança da informação e técnicas de perícia forense é apresentado.

Já o Capítulo 5 contém a metodologia explicando o desenvolvimento do objetivo proposto.

No Capítulo 6 estão descritos a análise e os resultados obtidos na realização deste trabalho.

Por fim, o Capítulo 7 contém o fechamento deste estudo através das considerações finais.

3 OBJETIVOS

3.1 Objetivo geral

Analisar *softwares* de perícia forense computacional, para auxiliar o perito forense na escolha da ferramenta para recuperação de arquivos deletados em dispositivos de armazenamento e *smartphones* com sistema operacional Android.

3.2 Objetivos específicos

- Estudar técnicas forenses de recuperação de dados.
- Levantar estratégias para análise pericial em *smartphones* Android.
- Pesquisar *softwares* específicos de recuperação de dados nos ambientes Windows, Linux e Android.
- Realizar a recuperação de dados em cada um dos sistemas operacionais, sendo HD externo e *pen drive:* Windows e Linux, já no *smartphone*: Android.
- Coletar resultados e analisá-los a fim de elaborar um quadro comparativo dos *softwares* analisados.

4 FUNDAMENTAÇÃO TEÓRICA

4.1 Breve histórico sobre celulares

A Agência Nacional de Telecomunicações (ANATEL) assim define o SMC: "Serviço móvel celular é o serviço de telecomunicações móvel terrestre, aberto à correspondência pública, que utiliza sistema de rádio-comunicações com técnica celular, interconectado à rede pública de telecomunicações, e acessado por meio de terminais portáteis, transportáveis ou veiculares, de uso individual".

Telefone celular é um aparelho de comunicação por ondas eletromagnéticas que permite a transmissão bidirecional de voz e dados utilizáveis em uma área geográfica que se encontra dividida em células (de onde provém a nomenclatura celular), cada uma delas servida por um transmissor/receptor.

4.2 Evolução dos celulares

O primeiro aparelho celular que se tem notícia foi desenvolvido pela Ericsson no ano de 1956 e foi denominado Ericsson MTA. O aparelho foi produzido para ser instalado em porta malas de carros devido ao seu tamanho e principalmente seu peso, cerca de 40 kg (ZHANG, 2011).

Zhang (2011) afirma que, o primeiro telefone celular desenvolvido para fins comerciais foi o Motorola *DynaTAC 8000X*, apresentado ao mercado em 1983, quase 30 anos após a criação da Ericsson.

A evolução dos celulares como qualquer outro tipo de tecnologia sofreu para chegar ao patamar de hoje, a indústria de dispositivos móveis geralmente refere-se a essa evolução com “gerações”.

Pode-se classificar, desse modo, a evolução dos celulares em três gerações: a primeira geração contava com celulares não tão portáteis, com celulares de quase 30 centímetros de altura e com preços astronômicos.

A segunda geração se inicia na década de 90, com as fabricantes prontas para lançarem aparelhos com tamanho e peso aceitável. Nesta geração foram agregadas três novas tecnologias bem avançadas para a época: TDMA, CMD e GSM.

Já na terceira geração, os celulares passaram a contar com tecnologias de ponta, graças a muito investimento na área. A implementação de uma câmera em um celular foi um fato bastante revolucionário, assim como o suporte e a reprodução de arquivos MP3, ACC e o WMA.

Atualmente, os *tablets* criaram um novo conceito de dispositivos móveis, tornando-se uma tendência. Os *tablets* são considerados uma evolução dos *smartphones,* porém, não substitutos. O *tablet* nada mais é do que uma mistura dos conceitos de um *notebook* com um *smartphone*, reunindo a mobilidade e facilidades como a tela *touch screen* e aplicativos de fácil utilização, com uma configuração mais poderosa e robusta em comparação com os *smartphones* (PARSONS; OJA, 2012).

Vital (2012) demonstra através da Figura 1 a evolução dos aparelhos celulares em ordem cronológica, detonando a importância do aumento de sua memória, diminuição do tamanho físico, maior poder de processamento; caso isso não ocorresse não seria necessário uma pericia forense.

ANO	**EVOLUÇÃO**
1956	É desenvolvido o primeiro protótipo do celular. Denominado MTA, o aparelho criado pela Ericsson contava com a desvantagem de pesar 40kg.
1973	Surge o Motorola DynaTAC 8000X. Menor e mais leve, a opção marca época como símbolo de status e tecnologia.
1974	O Nokia Mobira Talkman avança e se mostra um aparelho capaz de funcionar por várias horas seguidas.
1989	O Motorola Phone Bag 2900 inova com a transmissão de sinal telefônico mais potente.
1995	Época marcada pela popularização do famoso “tijolão”, semelhante a um telefone sem fio convencional.
1996	Tamanho reduzido, display monocromático e divisão entre as teclas

	de função (na parte superior) e teclado alfanumérico (parte inferior) são as novidades da época.
1997	Surgem os primeiros celulares com antena interna e recursos como o recebimento de mensagens de texto e acesso à internet.
2000	A Motorola anuncia o lançamento do modelo A 6188, primeiro celular com tela *touchscreen* da história.
2002	Surgem os primeiros celulares com inovações como o display colorido, câmera digital integrada e mp3 player.
2004	A Motorola lança os aparelhos mais finos da história, destacando o modelo V3.
2007	É lançado o iPhone, pela Apple, marcando uma nova era na evolução dos celulares. O então smartphone dá origem a sistemas operacionais exclusivos, interação *touchscreen* e instalação de aplicativos.
2008	A operadora Nextel conquista o mercado brasileiro com o chamado “celular de rádio”. A novidade faz uso da tecnologia *Push-to-talk*, permitindo ligações ilimitadas de Nextel para Nextel.
2012	Iphone, Android e Smartphone se tornam termos populares e o celular acumula recursos capazes de substituir computadores em tarefas domésticas e profissionais.

Figura 1 - Telefones Celulares em ordem cronológica.
Fonte: Vital (2012).

A Figura 2 demonstra a evolução dos celulares, exemplificando a diferença entre o primeiro celular criado para fins comercias até os de ultima geração. A diferença entre peso, tamanho, design é evidente desde o ano de 1983 até 2012.

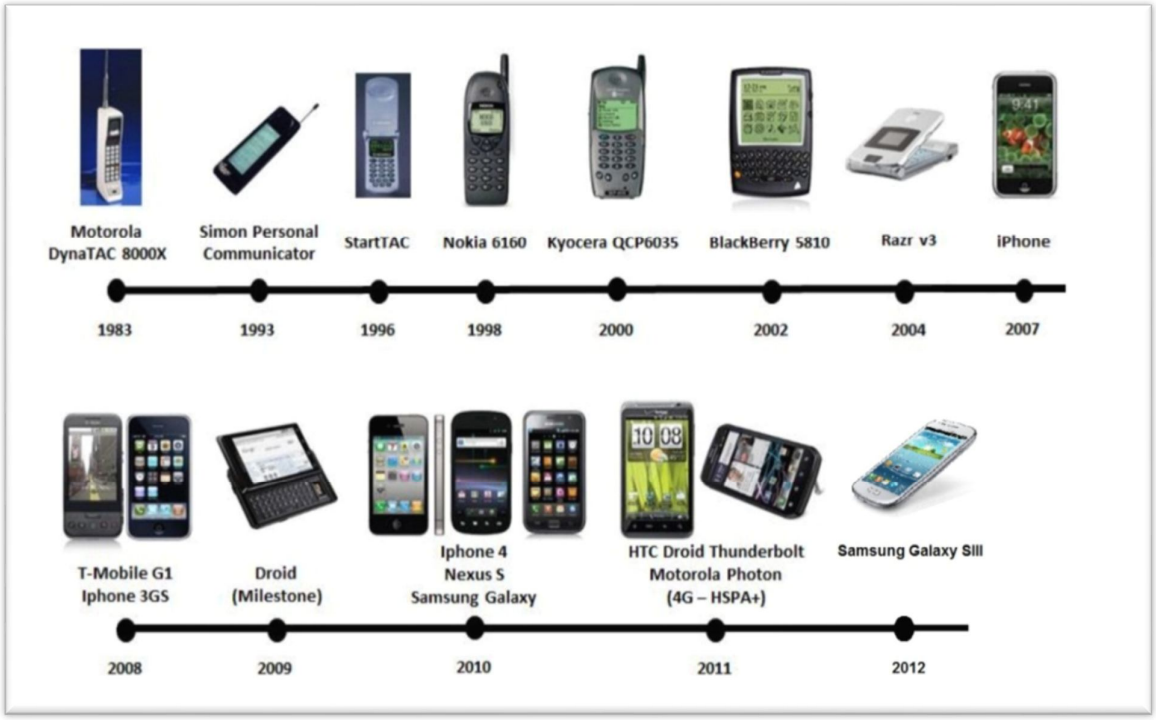

Figura 2 - Evolução dos Telefones Celulares.
Fonte: Simão (2011). Adaptada pelo Autor.

4.3 Celulares nos dias atuais

Os celulares parecem não ter limites na questão evolução. Cada vez novos recursos surgem, melhorias são adicionadas e tudo continua ocupando o mesmo espaço, ou cada vez menos espaço. O recurso que mais espantou a todos foi a apresentação dos primeiros celulares sensíveis ao toque. O aparelho de maior sucesso foi o iPhone, da Apple, porque ele não era apenas sensível ao toque, mas trazia a sensibilidade a múltiplos toques, ou seja, você pode comandá-lo utilizando vários dedos.

Atualmente, temos celulares com diversos sistemas operacionais, como por exemplo, o Android, cujo sistema operacional é baseado no núcleo do Linux para dispositivos móveis, desenvolvido pela Open Handset Alliance, liderada pelo Google e outras empresas. Segundo a Google, mais de 1 milhão e 300 mil aparelhos com este sistema operacional são ativados todos os dias e utilizados por vários

fabricantes de celulares como: HTC, Samsung, Sony, Motorola, LG e, recentemente, a Positivo Informática (ANDROID, 2013).

Os celulares praticamente substituíram computadores e até mesmo os *notebooks*. Um aspecto negativo dessa evolução é que isso trouxe os mesmos riscos já existentes para o computador, como ataques virtuais, roubos de informações, entre outros.

4.3.1 Smartphones

O dispositivo móvel mais conhecido e utilizado atualmente é o celular, mais conhecido também como *smartphone*, ou telefone inteligente traduzindo para o português.

O Smartphone (*telefone inteligente* – tradução livre do inglês) é considerado um telefone móvel com funcionalidades avançadas que são estendidas por meio de programas executados através de um sistema operacional (SMARTPHONE, 2013).

Segundo Zheng (2010, p. 5), “o termo *smartphone* foi inicialmente utilizado por estrategistas de marketing desconhecidos para se referir a uma então nova classe de telefones celulares que poderiam facilitar o acesso e processamento de dados”.

Zheng (2010, p. 6), também descreve que, “além da comunicação de voz tradicional e funcionalidade de mensagens de texto, um *smartphone* normalmente oferece aplicações de gerenciamento de informações pessoais e comunicação sem fio”.

Os sistemas operacionais dos *smartphones* permitem que desenvolvedores criem milhares de programas (aplicativos) adicionais, com diversas utilidades, agregados em *sites* como o Google Play[3]. Geralmente, um *smartphone* possui características mínimas de *hardware* e *software*, sendo as principais a capacidade de conexão com redes de dados para acesso à internet, a capacidade de sincronização dos dados do organizador com um computador pessoal, e uma agenda de contatos que pode utilizar toda a memória disponível do celular – não é

[3] Google Play é a loja online mantida pela Google para distribuição de aplicações, jogos, filmes, música e livros.

limitada a um número fixo de contatos. Um *smartphone* pode ser considerado um telefone celular com as funcionalidades de um PDA[4] (SMARTPHONE, 2013).

Um aparelho de última geração pode ter mais de 64 GB de dados disponíveis e, a exemplo da linha Samsung Galaxy, além de GPS nativo, possui filmadora HD, câmera digital, editores de texto, planilhas eletrônicas e centenas de aplicativos. A integração das funções no dispositivo também é de grande importância. Alguns aplicativos podem utilizar o GPS, o tocador (*player*) de música e a conexão de dados simultaneamente. Com esses recursos, o usuário pode estar conectado com o mundo a qualquer instante, uma revolução se comparado há 10 anos (SMARTPHONE, 2013).

4.4 Abordagem pericial a um s*martphone*

Em 2011, o sistema operacional Android ultrapassou o número de aparelhos vendidos por outros sistemas operacionais para *smartphones*. O sistema tem grande aceitação no mercado. Acredita-se que esta aceitação se deva ao código aberto e ao suporte aos mais modernos recursos e aplicativos disponíveis para tal tipo de equipamento. Dada a capacidade de prover um grande número de funcionalidades ao usuário, um *smartphone* com o sistema Android pode armazenar uma grande quantidade de informações sobre seu proprietário, configurando-se como uma fonte de provas para fatos que se queira explicar ou obter dados para fundamentar uma investigação.

Diferentemente de uma abordagem de aquisição de dados em ambientes computacionais, em que geralmente aqueles podem ser extraídos no estado em que foram encontrados e ficam preservados a partir do momento da sua apreensão, a extração de dados em telefones celulares e *smartphones* normalmente exige a execução de alguma intervenção no dispositivo. Além disso, tendo em vista que utilizam memórias embutidas, cujo acesso, sendo direito ao *hardware*, é delicado e complexo, é preciso instalar aplicativos ou utilizar ferramentas diretamente no dispositivo para que se proceda à aquisição dos dados armazenados e consequentes evidências (ASSOCIATION OF CHIEF POLICE OFFICERS, 2008).

Neste âmbito, o analista pericial deve ter o conhecimento necessário para realizar os procedimentos periciais no dispositivo da forma menos invasiva possível,

[4] Assistente Digital Pessoal, computador de bolso.

controlando o ambiente de maneira a se evitar a perda, a alteração ou mesmo a contaminação de dados tratados como evidências, o que dará maior confiabilidade à perícia (ASSOCIATION OF CHIEF POLICE OFFICERS, 2008).

4.5 Sistema Operacional Windows

A Microsoft começou a desenvolver o Microsoft Windows em setembro de 1981. O Windows só começa a ser tecnicamente considerado como um SO a partir da versão Windows NT, lançada em Julho de 1993. O que havia antes eram sistemas gráficos sendo executados sobre alguma versão dos sistemas compatíveis com DOS, como MS-DOS, PC-DOS ou DR-DOS. Somente o MS-DOS era produzido pela própria Microsoft. (MICROSOFT WINDOWS, 2013).

O MS-DOS é um sistema operativo que não dispõe de *interface* gráfica, funciona através de comandos de texto introduzidos no teclado pelo utilizador. O Windows surgiu inicialmente como uma *interface* gráfica para MS-DOS, que permitia correr programas em modo gráfico, o que permitiu a utilização do mouse, que até à altura era considerado supérfluo em computadores do tipo IBM-PC. (MICROSOFT WINDOWS, 2013).

O Windows é um produto comercial com preços diferenciados para cada uma de suas versões. É o sistema operacional mais utilizado em computadores pessoais no mundo. A Figura 3 demonstra os tipos de sistemas operacionais já criados pela empresa Microsoft. (MICROSOFT WINDOWS, 2013).

16 *Bits*	**Família NT**	**64 *Bits***
Windows 1.0	Windows NT	Windows Server 2008 R2
Windows 2.0	Windows 2000	Windows Server 2012
Windows 3.xx	Windows Neptune	
	Windows Odyssey	
32 *Bits*	**32 e 64 *Bits***	**Versões sistemas embarcados**
Família 9x	Windows XP	
Windows 95	Windows Server 2003	Windows CE
Windows 98	Windows Vista	Windows Mobile
Windows 98 SE	Windows Server 2008	Windows Phone
Windows ME	Windows 7	
	Windows 8	

Figura 3 - Sistemas Operacionais.
Fonte: Elaborado pelo autor (2013).

O impacto deste sistema no mundo atual é muito grande devido ao enorme número de cópias instaladas. Conhecimentos mínimos desse sistema, do seu funcionamento, da sua história e do seu contexto são, na visão de muitos, indispensáveis, mesmo para os leigos em informática. A atual versão estável do Windows para *desktops* é o Windows 8, lançado em 26 de outubro de 2012. Para servidores, o Windows Server 2008 R2 é a versão mais recente e estável.

As primeiras versões do Windows, como a 1.0, 2.0, são compatíveis apenas com partições formatadas em sistema de ficheiros FAT, ou como é chamado, FAT 16. O 3.x poderia ser instalado em FAT 32, porém necessita ser instalado o MS-DOS 7.10, que era incluído nos disquetes de inicialização do Windows 95 OSR2 e Windows 98, necessitando modificar alguns arquivos para permitir seu funcionamento. Ao mudar do 3.1 para o 95B (Windows 95 OSR 2/OSR 2.1), os HD's poderiam ser formatados em FAT 32. Inicialmente lançado com o Windows NT, a tecnologia NTFS é agora o padrão *de fato* para esta classe (MICROSOFT WINDOWS, 2013).

A principal linguagem de programação usada para escrever o código-fonte das várias versões do Windows é o Basic e algumas partes com C++ e Assembly. Até a versão 3.11, o sistema rodava em 16 *bits* (apesar de poder instalar um update chamado *Win32s* para adicionar suporte a programas 32 *bits*). Daí em diante, em 32 *bits*. As versões a partir do XP e Server 2003 estão preparadas para a tecnologia 64 *bits*.

Os sistemas de 64 *bits* não possuem mais suporte para rodar nativamente aplicativos de 16 *bits*, sendo necessário uso de emuladores/máquinas virtuais.

Os *bits* são relacionados ao volume de dados que um microprocessador é capaz de lidar. Se um processador tem uma arquitetura de 64 *bits*, ele é capaz de lidar com dados na ordem de 2^{64}, ou seja, 18446744073709552000. Só que para isso ser possível, é necessário que o sistema operacional seja de 64 *bits*. Caso contrário, ele trabalhará somente com instruções de 32 *bits* (se o sistema for de 32 *bits*). Sistemas operacionais de 64 *bits* também endereçam uma quantidade maior de RAM, suportando até 192GB (Windows 7 Ultimate) ou 128GB (Windows XP Professional), contra 3,2GB dos sistemas de 32 *bits* (MICROSOFT WINDOWS, 2013)

4.6 Sistema Operacional Linux

O nome Linux é uma fusão do nome de seu criador, o finlandês Linus Torvalds com Unix, um sistema operacional de grande porte voltado para servidores, no qual o Linux foi baseado (MORIMOTO, 2009).

O Linux é um sistema operacional, responsável pelo funcionamento do computador, que faz a comunicação entre *hardware* (Impressora, monitor, mouse, teclado) e *software* (aplicativos em geral).

O kernel é o coração do Sistema Operacional Linux. Ele é o responsável por garantir que todos os programas terão acesso aos recursos de que necessitam (memória RAM, por exemplo) simultaneamente, fazendo com que haja um compartilhamento concorrente – mas sem oferecer riscos à integridade da máquina. O Linux tem seu código fonte disponível sob licença GPL para qualquer pessoa utilizar, estudar, modificar e distribuir de acordo com os termos da licença (MORIMOTO, 2009).

Os sistemas operacionais são nada mais do que a junção de fatores como: núcleo do sistema (Kernel Linux), programas (ex.: *Shell*), aplicativos (ex.: navegador Firefox). O que difere uma distribuição da outra é a versão do Kernel utilizada, programas e aplicativos disponibilizados, bem como o fodo da distribuição. Existem distribuições voltadas para todos os tipos de atividade, servidores, desktop, roteadores de redes, *firewall*, *mobile* etc.

Um fato descrito por Morimoto (2009), que deixa claro a diferença que as distribuições podem ter entre si está de acordo com o que oferecem, baseando-se no tamanho em bytes de alguns é que existem distribuições capazes de “rodar” a partir de um simples disquete de 1.44MB até distribuições que ocupam 3 DVD’s de 4.7GB.

Morimoto (2009) cita exemplos de distribuições:

- **Debian:** é uma distribuição focada na estabilidade e existe desde 1996. Atualmente a versão estável se encontra na 7.0. Um fator diferencial do Debian é o gerenciador de pacotes APT que permite a instalação, remoção, atualização e configuração de pacotes de forma simples, fácil, eficaz e segura.

- **Ubuntu:** Distribuição existente desde 2004. É baseada no Debian e também utiliza o gerenciador de pacotes APT. Tem obtido um grande sucesso no mercado Linux nos últimos anos, pois apresenta facilidades em sua instalação e uso para *desktops*. Sua ultima versão é a Ubuntu 13.04 Desktop (i386).
- **Damn Small Linux:** também é uma distribuição baseada no Debian e faz parte de um tipo denominado “mini-distribuições”. Designada para executar aplicativos gráficos em computadores antigos, esta distribuição é muito pequena, possuindo apenas 50 MB de arquivos de instalação. Última versão 4.4.10.
- **Endian Firewall:** é um *firewall* baseado em Linux que pode transformar qualquer computador em um poderoso roteador/firewall. Conta com *interface* Web unificada de acesso e gerenciamento. Atualmente encontra-se na versão 2.5.
- **Android:** sistema operacional mobile da Google, utiliza o Kernel Linux. Não sendo, porém, desenvolvido internamente no kernel e sim, em uma estrutura externa. O Android é desenvolvido com bibliotecas que permitem ao desenvolvedor programar utilizando Java, assim controlando o aparelho por intermédio dessas bibliotecas.

4.7 Sistema Operacional Android

O Android vem a ser um sistema operacional baseado em Linux, projetado principalmente para dispositivos móveis *touchscreen*, como *smartphones* e *tablets*. Inicialmente desenvolvido pela Android Inc., apoiado financeiramente pela Google que em 2005 adquiriu os direitos do sistema operacional. O Android foi lançado em 2007 junto com a fundação da Open Handset Alliance: um consórcio de *hardware*, *software*, telecomunicações e empresas dedicadas ao avanço aberto de normas para dispositivos móveis. Entre as empresas participantes estão Google, HTC, Dell, Intel, Motorola, Qualcomm, Texas Instruments, Samsung, LG, T-Mobile e Nvidia (OPEN HANDSET ALLIANCE, 2010).

A *interface* de usuário do Android é baseada em manipulação direta, utilizando as entradas de toque que correspondem às ações do mundo real para manipulação dos objetos na tela. A resposta à entrada do usuário é projetada para

ser imediata e fornece uma *interface touchscreen*, muitas vezes usando as capacidades do dispositivo de vibração para fornecer *feedback* tátil para o usuário.

São utilizados também dispositivos de *hardware* como, por exemplo, acelerômetros e sensores de proximidade, tornando possível que aplicativos respondam às ações do usuário como ajustar a tela de retrato para paisagem, dependendo de como o dispositivo é orientado, ou permitindo que o usuário dirija um veículo em um jogo de corrida pela rotação do dispositivo, que simula o controle de um volante (ANDROID, c2013b).

O crescimento do Android foi exponencial no último ano, atingindo algumas marcas altamente expressivas como: 700 mil aplicativos desenvolvidos e disponibilizados no Google Play (loja de aplicativos do Android), conta com mais de 1 milhão e 300 mil aparelhos Android ativados. Com esses números, o Android se tornou a plataforma mais utilizada em *smarthphones,* estando em primeiro lugar com 46.8% de todo o mercado (ANDROID, c2013b).

A plataforma Android é composta pelo sistema operacional, o SDK (*Software Development Kit*) e suas aplicações. O SDK é um conjunto de ferramentas disponibilizadas pela empresa Google que forma um ambiente de desenvolvimento para a criação de aplicativos Android.

Uma de suas ferramentas é o ADB (*Android Debug Bridge*), que provê uma *interface* de comunicação com o sistema Android por meio de um computador. Quando conectado por meio dessa *interface*, o computador é capaz de acessar um interpretador de comandos (*shell*), instalar ou remover aplicativos, ler registros históricos (logs), transferir arquivos entre a estação e o dispositivo, dentre outras ações.

O conceito de *sandbox* é utilizado no sistema operacional Android. Esta é uma função pela qual os aplicativos, depois de serem instalados, possuem áreas reservadas, isolando o ambiente de execução dos processos e delimitando o acesso aos recursos. Com isso, as aplicações não podem acessar áreas que não sejam explicitamente permitidas (GOOGLE INC. 2011).

Porém, o acesso a funcionalidades pode ser autorizado por meio de configurações no arquivo “AndroidManisfest.xml”. No momento da instalação do aplicativo, tal arquivo informa ao usuário quais recursos disponíveis no *smartphone* serão utilizados. O usuário pode aceitar a instalação do aplicativo, após ter sido

informado dos recursos que serão utilizados, ou simplesmente recusar a instalação por não concordar com os tipos de funcionalidades que o aplicativo teria que acessar.

4.7.1 O SDK do Android

O SDK do Android é considerado um conjunto de ferramentas que possuem como objetivos fornecer aos desenvolvedores da plataforma um ambiente completo para criação e depuração dos aplicativos Android. O principal aplicativo é o SDK *Manager*, onde é possível baixar as APIs referentes às diferentes versões do Android e executar emuladores do sistema (SIMÃO, 2011).

O SDK também disponibiliza algumas outras ferramentas, como a ferramenta “dx” usada para gerar o arquivo executável Dalvik e da ADB (*Android Debug Bridge*), usada para se conectar a um emulador ou dispositivo Android em modo de depuração USC e realizar algumas ações no sistema via linha de comando (SIMÃO, 2011).

Ainda segundo Simão (2011), o ADB oferece uma *interface* ao dispositivo Android conectado ao computador ou a um emulador Android gerenciado pelo SDK *Manager*. Normalmente encontra-se instalado no diretório <*sdk*>*/plataforma-tools.*

A ferramenta trabalha na arquitetura cliente-servidor com três componentes:

1. Cliente: utilizado por meio de um terminal através da ferramenta ADB na máquina à qual o dispositivo está conectado.
2. Servidor: também fica em execução na máquina à qual o dispositivo está conectado. Executado em segundo plano tem a função de gerenciar a comunicação entre o cliente e o serviço (*daemon*) que está em execução no dispositivo.
3. Serviço (*daemon*): executado em segundo plano no aparelho.

O servidor é inicializado quando um cliente faz uma chamada para realizar uma conexão a um dispositivo Android. Na sequencia quando o servidor estabelece uma conexão com o serviço no dispositivo, comandos ADB podem ser utilizados para gerenciar o aparelho.

Por meio da ADB, via modo de depuração, é possível conectar ao dispositivo Android e obter um *shell*. Pode-se instalar aplicativos, copiar arquivos, obter informações do sistema e obter informações de log (*logcat*).

4.7.2 Estrutura do sistema de arquivos do Android

Os *smartphones* com sistema Android utilizam memória flash. Para que a memória flash possa ser trata de forma convencional pelo sistema, é necessário haver uma camada de firmware chamada FTL (*Flash Translation Layer*), com a finalidade de, juntamente com o subsistema MTD (*Memory Technology Device*), permitir ao sistema trabalhar com a memória como se ela fosse um dispositivo de blocos convencional, a exemplo de um disco rígido, funcionando como um tradutor de requisições (SIMÃO, 2011).

4.7.3 Banco de dados da plataforma Android

O sistema operacional Android optou por utilizar o banco de dados SQLite para prover às aplicações um gerenciador de banco de dados relacional, leve, robusto e de simples utilização. O SQLite é um banco de dados que não necessita de configurações. Utilizado pela Nokia, Mozzila, Skype, Apple, Adobe, Solaris, etc Burnett (2008). Não há restrições para o uso do banco de dados, sendo de domínio público, com código aberto (SIMÃO, 2011).

5.8 Informação

Considerada um resultado do processamento, manipulação e organização de dados, transparecendo uma forma que possa representar uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina) que a recebe (SERRA, 2007).

Seguindo o pensamento de Serra (2007), o conceito de informação leva uma diversidade de significados, do uso quotidiano ao técnico. Genericamente, o conceito de informação está sempre ligado às noções de restrição, comunicação, controle, dados, forma, instrução, conhecimento, significado, estímulo, padrão, percepção e representação de conhecimento.

A informação é um bem valoroso para as organizações e deve ser protegida e cuidada por meio de políticas e regras, da mesma maneira que os recursos financeiros e materiais são tratados. A informação é um ativo de valor, um recurso crítico para realização do negócio (FONTES, 2006).

Nos dias atuais é comum ouvir falar sobre a Era da Informação, o advento da "Era do Conhecimento" ou sociedade do conhecimento. Como a sociedade da informação, a tecnologia da informação, a ciência da informação e a ciência da computação em informática são assuntos e ciências recorrentes na atualidade, a palavra "informação" é frequentemente utilizada sem muita consideração pelos vários significados que adquiriu ao longo do tempo.

4.9 Sistemas de informação

Para Laudon e Laudon (1999), um sistema de informação pode ser definido como um conjunto de componentes inter relacionados trabalhando juntos para coletar, recuperar, processar, armazenar e distribuir informações com a finalidade de facilitar o planejamento, o controle, a coordenação, a análise e o processo decisório em organizações.

Todo sistema de informação que manipule dados e gere informações, usando ou não recursos de tecnologia da informação, também pode ser considerado genericamente como um sistema de informação. Por exemplo, o sistema de informação organizacional pode ser descrito como a organização e seu vários subsistemas interno, contemplando ainda o meio ambiente externo (SISTEMA DE INFORMAÇÃO, 2013).

Pode ser considerada também uma coleção de atividades que regulam o compartilhamento e a distribuição de informações e o armazenamento de dados relevantes ao gerenciamento de uma empresa.

Sistemas de informação podem oferecer suporte à tomada de decisão, de acordo com todas as variáveis que representam o estado da organização.

4.10 Segurança da Informação

De acordo com Barbosa (2009), os sistemas de informação podem ser entendidos como um conjunto organizado de pessoas, *hardware*, *software*, redes de

comunicações e recursos de dados que coleta, transforma e dissemina informações em uma organização.

É um termo vindo do latim *informationem*, “delinear”, “conceber ideia”, ou seja, dar forma ou moldar na mente. A segurança da informação está relacionada com proteção de um conjunto de informações, com a intenção de preservar o valor que possuem para um individuo ou uma organização.

> Quando falamos em segurança da informação, estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações dentro das necessidades do cliente (LYRA, 2008, p.4).

Os sistemas de informação possuem características básicas como os atributos de confidencialidade, integridade, disponibilidade e autenticidade. Este tipo de segurança não é restrito somente a sistemas computacionais, podendo ser utilizado em informações eletrônicas, ou sistemas de armazenamento, podendo ser aplicado em todos os aspectos de proteção de informação e dados.

O conceito de Segurança Informática ou Segurança de Computadores está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si (BÖGER; JUNIOR, 2008).

Segundo Lyra (2008), as características de um sistema seguro são:

- **confidencialidade**: capacidade de um sistema de permitir que alguns usuários acessem determinadas informações ao mesmo tempo em que impede que outros, não autorizados, a vejam;
- **integridade**: a informação deve estar correta, ser verdadeira e não estar corrompida;
- **disponibilidade**: a informação deve estar disponível para todos que precisarem dela para a realização dos objetivos empresariais.

Lyra (2008) define que além desses três aspectos principais, tem-se:

- **autenticidade**: garantir que um usuário é de fato quem alega ser;
- **legalidade**: garante que o sistema esteja aderente à legislação pertinente;

- **privacidade**: capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações (por exemplo, o sistema de voto eletrônico);
- **não-repúdio**: assegura que alguém não possa negar autoria de alguma informação que efetivamente tenha gerado;
- **auditoria**: capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque.

Já um incidente de informação é a ocorrência de eventos específicos que podem causar a interrupção nos processos de negócios em consequência da violação de alguns aspectos listados acima (LYRA, 2008).

Fatores como greves, manifestações, intempéries da natureza etc., também podem causar incidentes de segurança, devido ao fato de afetarem a disponibilidade e a integridade da informação.

4.11 Políticas de Segurança de Informação (PSI)

A Política de Segurança de Informações (PSI) pode ser considerada um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico, pelo gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela organização para que sejam assegurados seus recursos computacionais e suas informações (TCU, 2008).

Segundo Ferreira (2006), a segurança pode ser ramificada em quatro grandes classes:

- **segurança computacional:** conceitos e técnicas utilizadas para proteger o ambiente informatizado contra eventos inesperados que podem causar prejuízo;
- **segurança lógica:** prevenção contra acesso não autorizado;
- **segurança física:** procedimentos e recursos para prevenir acesso não autorizado, dano e interferência nas informações e instalações físicas da organização;

- **continuidade de negócio:** estrutura de procedimentos para reduzir, a um nível aceitável, o risco de interrupção ocasionada por desastres ou falhas por meio da combinação de ações de prevenção e recuperação.

4.12 Classes da Segurança da Informação

Outras classes de problemas de segurança que podem ser geradas através da má operação de recursos ou ataques ao sistema, são descritas a seguir:

- **ativo da Informação**: a informação é considerada um bem de grande valor para processos de negócios da organização, mas também a tecnologia deve ser considerada, o meio que suporta, que mantém e que permite a informação existir, sendo utilizada por pessoas que a manipulam e o ambiente onde ela está inserida;
- **ataque**: é considerado um incidente de segurança caracterizado pela existência de um agente que busca obter algum tipo retorno em informações, por questões financeiras ou por outros motivos;
- **vulnerabilidade**: ativos de informação possuem vulnerabilidades ou fraquezas que podem gerar, intencionalmente ou não, a indisponibilidade, a quebra de confidencialidade ou integridade. A vulnerabilidade de um ativo é o seu ponto fraco;
- **ameaça**: considerado um ataque em potencial a um ativo da informação, vem a ser um agente externo que, aproveitando-se da vulnerabilidade, poderá quebrar um ponto fraco que nunca será efetivamente explorado;
- **probabilidade**: é a chance de uma falha de segurança ocorrer, levando-se em conta as vulnerabilidades do ativo e as ameaças que venham a explorar esta vulnerabilidade. Existe a possibilidade de ter um ativo com várias vulnerabilidades, mas sem ameaças de ataque, o que nos leva a uma probabilidade próxima à nula;
- **impacto**: os ativos de informação possuem valores diferentes e são medidos pelas consequências que possam causar aos processos de negócio suportados pelo ativo em questão. Quanto maior for o valor do

ativo, maior será o impacto de um eventual incidente que possa ocorrer;

- **controle**: é todo e qualquer mecanismo utilizado para diminuir as fraquezas (ou vulnerabilidades) de um ativo de informação, seja um equipamento, tecnologia, pessoa ou processo.

4.13 Ciclo de vida da Informação

A identificação das necessidades e dos requisitos da informação são os estimuladores do ciclo de vida da informação. A partir de definições dá-se sequência ao processo de obtenção, tratamento, armazenamento, distribuição, uso e descarte da informação.

A Figura 4 abaixo denota um organograma representando o fluxo seguido pela informação em uma organização, ou seja, o caminho realizado pela informação desde sua obtenção até seu descarte (LYRA, 2008).

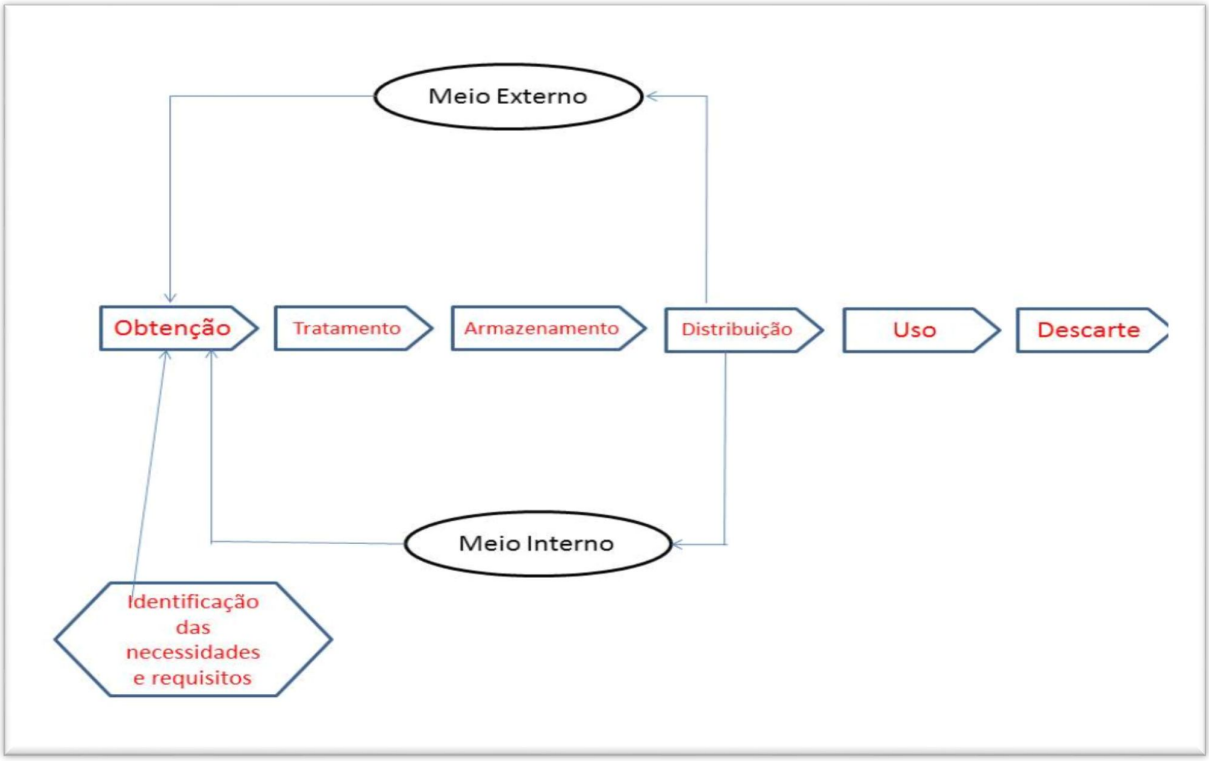

Figura 4 - Ciclo de Vida da Informação.
Fonte: Lyra (2008). Adaptado pelo Autor.

4.14 Perícia Forense

A Perícia Forense consiste, basicamente, no uso de métodos científicos para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidência digital com validade probatória em juízo. A aplicação desses métodos nem sempre se dá de maneira simples, uma vez que encontrar uma evidência digital em um computador pode ser uma tarefa muito árdua.

De acordo com Costa (2008), a perícia forense trabalha investigando o fato de um crime buscando materializar o ato criminoso por meio da confecção de provas de ordem técnico-científica, que comprovem a veracidade do fato, de forma a não deixar dúvida sobre as evidências investigadas.

A perícia forense aplicada à informática, também referenciada como computação forense computacional, criminalística computacional, forense digital, investigação eletrônica e perícia eletrônica, é a aplicação de conhecimentos em informática de técnicas de investigação com a finalidade de obtenção de evidências de crimes digitais (PIMENTA, 2007).

4.15 Computação Forense

Computação Forense é a ciência que trata do exame, análise e investigação de um incidente computacional, ou seja, que envolvam a computação como meio, sob a óptica forense, sendo ela civil ou penal. Na criminalística, a Computação Forense trata o incidente computacional na esfera penal, determinando causas, meios, autoria e consequências (COSTA, 2005).

A Computação Forense pode ser considerada uma área de pesquisas que busca investigar soluções para problemas relacionados à coleta, organização, classificação e análise de evidências digitais. Sobre a coleta e organização, procuram-se abordagens para reduzir a utilização errônea e ingênua de possíveis evidências importantes (COSTA, 2005).

Já a respeito da classificação, buscam-se soluções que permitam categorizar as evidências de modo a reduzir o esforço técnico necessário durante sua análise.

Finalmente, na análise, objetiva-se investigar a fonte geradora de um determinado documento, bem como sua autenticidade. (ROCHA; GOLDENSTEIN, 2008).

Pela identificação da fonte originadora procura-se identificar o modelo particular de um dispositivo de captura (scanner, câmera, impressora), ou o dispositivo exato, que fez a captura de um determinado documento. Na detecção de manipulações, procura-se estabelecer a autenticidade de um documento ou expor quaisquer manipulações que este possa ter sofrido.

Segundo Vargas (2007), a análise forense de um sistema envolve um ciclo de coleta de dados e processamentos das informações coletadas. Quanto mais precisos os dados, melhor e mais abrangente a avaliação pode ser. Os dados originais permanecem protegidos em um estado puro; qualquer análise deve ser realizada em uma cópia dos dados do computador.

4.16 Procedimentos para uma Perícia Forense

A perícia forense possui quatro procedimentos básicos, onde todas as evidências devem ser a) identificadas; b) preservadas; c) analisadas; d) apresentadas. As tarefas envolvidas em uma investigação se enquadram em um destes grupos (FREITAS 2006).

Conforme Freitas (2006), a identificação das evidências denota que, diferentes crimes resultam em diferentes evidências. Por exemplo, em um caso de acesso não autorizado, o perito deverá procurar por arquivos de log, conexões e compartilhamentos suspeitos, já em casos de pornografia, buscará por imagens armazenadas no computador, histórico dos sites visitados recentemente, arquivos temporários do *browser*, etc.

Em consequência disso, a habilidade do perito em identificar as evidências vai depender da sua familiaridade com o tipo de crime cometido e dos programas e Sistemas Operacionais envolvidos. Freitas (2006) ainda descreve que para se encontrar evidências deve-se: a) procurar por dispositivos de armazenamento (*hardwares*): *laptops*, HDs, disquetes, Cds, DVDs, *drives* Zip/Jaz, memory Keys, *pen drives*, câmeras digitais, MP3 player, fitas DAT, Pocket PC, celulares, *smartphones*, dispositivos de *backup* ou qualquer equipamento que possa armazenar evidências; b) procurar por informações relacionadas ao caso: anotações, nomes de pessoas, datas, nomes de empresas e instituições, números de telefones, documentos

impressos etc; c) distinguir entre evidências relevantes e irrelevantes em uma análise ao vivo.

4.17 Preservando evidências

Em uma investigação forense a regra número um a ser seguida é não destruir ou alterar as provas. Logo, as evidencias precisam ser preservadas de tal forma que não haja dúvida alguma de sua veracidade. E para que as evidencias não sejam comprometidas, substituídas ou perdidas durante o transporte ou manuseio no laboratório, Freitas (2006) sugere que, sempre sejam seguidos os seguintes passos:

- sempre que possível, criar imagens do sistema investigado, conhecido como duplicação pericial, para que as evidências digitais possam ser analisadas depois;
- caso seja necessária uma análise ao vivo, salvar as evidências em CDs e bloqueá-los contra regravação;
- todas as evidências devem ser lacradas em sacos e etiquetas;
- cada etiqueta deverá conter um número para a identificação das evidências, o número do caso, a data e o horário em que a evidência foi coletada e o nome da pessoa que a está levando para custódia;
- etiquetar todos os cabos e componente do computador para que depois possam ser montados corretamente quando chegar no laboratório;
- os HDs deverão ser armazenados em sacos antiestéticos, para evitar danos e corrompimento dos dados;
- cuidado no transporte das provas, cuidado com líquidos, umidade, impacto, sujeira, calor excessivo, eletricidade e estática;
- após o transporte, as evidências deverão ser armazenadas e trancadas para evitar adulteração até o momento em que poderão ser examinadas e analisadas;
- caso exista necessidade de mudanças nesta fase, ela sempre deverá ser documentada e justificada (cadeia de custódia).

4.18 Restauração de Dados

Caso um arquivo seja apagado e logo após esvaziada a lixeira do sistema operacional, esse arquivo ainda não foi completamente apagado, ele ainda existe em seu dispositivo de armazenamento de dados, seja ele um HD externo, *pen drivre*, cartão de memória, *smartphone*, disco rígido e até mesmo um cartão de memória.

De acordo com Julien (2012), essa particularidade é gerada pelo sistema operacional que remove apenas a referência do arquivo apagado na tabela de alocação de arquivos e libera a área do disco utilizada para gravação de novos dados. Devido a essa área não estar sendo sobrescrita por novos arquivos, existe a possiblidade de recuperação dos arquivos que estavam alocados naquela região.

A quantidade de programas para recuperação de arquivos é grande, tanto para os pagos quanto para os gratuitos. A restauração em *pen drives* é a mesma realizada em unidades físicas, mas a recuperação em *smartphones* pode ser diferente.

A polícia pode utilizar a recuperação de dados forenses para explorar os computadores dos suspeitos do crime. Caso um (a) suspeito (a) tenha excluído arquivos, mídia ou *e-mails* que podem conter elementos da prova do delito, a recuperação de dados forenses pode extrair partes de dados excluídos para uso em um Tribunal. Técnicas semelhantes auxiliam outros usuários de computador que podem ter excluído acidentalmente um importante arquivo ou precisam de acesso aos negócios antigos ou documentos pessoais (JULIEN, 2012).

4.19 Softwares de restauração

4.19.1 Softwares para Windows

4.19.1.1 DiskDigger

O DiskDigger é um *software* (ferramenta) gratuito capaz de realizar uma varredura completa em seus discos de armazenamento internos e externos na busca de arquivos excluídos na tentativa de recuperá-los. O aplicativo faz uma busca minuciosa em todos os setores do seu HD, podendo também vasculhar a

memória de *pen drives*, câmeras e outros aparelhos conectados ao PC (DISKDIGGER, 2013).

Com uma *interface* intuitiva, bem organizada e fácil de usar, pode-se recuperar vários arquivos apagados de diversas extensões e formatos.

4.19.1.2 Recuva

O *software* é gratuito e oferece uma forma fácil de recuperação de arquivos apagados do disco rígido, *pen drive*, câmeras digitais, cartão de memória, HD Externo, entre outros.

O Recuva funciona até mesmo com discos rígidos formatados. Isso é possível porque a maioria dos processos de formatação, seja para instalação de um novo sistema operacional ou apenas para desocupar espaço, não apaga os dados imediatamente. Cabe ao programa, portanto, trazer esses arquivos supostamente apagados de volta (NARDUCI, 2013).

Possui também uma versão portátil, compatível com Windows XP, Vista, 7 e 8, podendo ser instalado em vários idiomas.

4.19.1.3 Active@ File Recovery

Ferramenta utilizada para recuperar arquivos acidentalmente deletados, mesmo que eles já tenham sido apagados da lixeira. Ele pesquisa o HD em busca dos arquivos apagados e exibe todos em uma lista. O Active @File Recovery trabalha com os sistemas FAT, FAT32 e NTFS (ACTIVE @FILE RECOVERY, 2013).

O *software* pode ser utilizado para recuperar discos rígidos IDE, SATA, SATA II e SCSI, disquetes e outras mídias (CompactFlash, SmartMedia, Sony MemoryStick, USB Hard Drive, USB Flash Memory).

Possui uma versão gratuita na qual é possível realizar uma recuperação considerada básica; já sua versão paga conta com várias opções a mais e uma busca muito mais qualificada. O programa suporta as versões a seguir do Windows: 8, 7, Vista, Server 2008, Server 2003 e XP.

4.19.2 Softwares para Linux

4.19.2.1 Foremost

Software de console utilizado para recuperar arquivos com base em seus cabeçalhos, rodapés e estruturas de dados internas. O *software* permite trabalhar em arquivos de imagem gerados por softwares de perícia forense, como dd, Safeback, Encase, etc. Ferramenta livre para qualquer sistema Linux (FOREMOST, 2013).

4.19.2.2 Scalpel

Resultado de uma completa reedição da ferramenta foremost. Tendo o Linux como sistema operacional preferencial, ele é considerado um *software opensource*; entretanto pode ser utilizado em ambientes Windows e Mac OS X, para isso basta compilar seu código fonte no sistema escolhido.

O Scalpel é um recuperador de arquivos, de alto desempenho, que lê um banco de dados de definições de cabeçalho e rodapé e extrai os arquivos desejados de um conjunto de arquivos de imagem ou dispositivos raw. O *software* é independente de tipo de partição e consegue extrair arquivos de partições FATx, NTFS, ext2/3 ou partições raw. É útil tanto para investigações forenses como para recuperação de arquivos (ALMEIDA, 2013).

Nesta ferramenta, o processo de recuperação pode ser demorado, dependendo do tamanho do HD e de quantos arquivos existem para serem recuperados.

4.19.2.3 TestDisk

O TestDisk é um *software* OpenSource e é licenciado sob os termos da *GNU General Public License*, utilizado para ajudar a recuperar partições perdidas, arquivos apagados ou perdidos e/ ou tornar discos não inicializáveis em inicializáveis quando estes estão com problemas, certos tipos de vírus ou erro humano.

Algumas das utilidades do TestDisk são: corrigir a tabela de partição, recuperar partição apagada; recuperar o setor de inicialização FAT32 do seu *backup*; reconstruir o setor de *boot*; corrigir tabelas FAT; restaurar arquivos do FAT,

exFAT, NTFS, ext2 *filesystem*, FAT16, FAT32, EXT3, ReiserFS, XFS, LVM e Linux Raid (TESTDISK, 2013).

O *software* possui recursos para usuários iniciantes e avançados. Para usuários que pouco sabem sobre técnicas de recuperação de dados, o TesDisk pode ser usado para coletar informações detalhadas sobre um disco não-boot que pode ser enviado para um técnico para analise posterior. Já usuários com maior conhecimento podem achar o TestDisk uma ferramenta útil na realização de recuperação local (TESTDISK, 2013).

4.19.3 Softwares para Android

4.19.3.1 Remo Recover for Android

Aplicativo cuja função é recuperar arquivos perdidos, que foram apagados acidentalmente em *smartphones* com SO da Google (Android). Além disso, ele restaura os dados após uma formatação de cartão SD, tais como arquivos APK, músicas, vídeos e imagens (HAMMERSCHMIDT, 2013).

Vigorosamente, o aplicativo verifica tanto a memória do telefone interna e externa do dispositivo, para identificar arquivos excluídos ou perdidos, quanto arquivos de pacote de aplicativos Android (APK) e restaurá-los para reutilização.

4.19.3.2 Undelete

O Undelete é um aplicativo para a plataforma Android, que permite recuperar qualquer tipo de arquivo que foi excluído do cartão SD ou armazenamento interno do *smartphone*.

O aplicativo pode ser baixado diretamente pelo *smartphone* ou pelo computador no site do Google Play. Possui um tamanho de 2,4 e está na versão de língua inglesa (GOOGLE PLAY, 2013).

Com suporte para mais de 1000 tipos de arquivos, o Undelete pode ser utilizado caso o usuário deseje recuperar arquivos de vídeos, músicas, arquivos de testos, entre outros. O Undelete também pode seguramente limpar e destruir arquivos de modo que os mesmos ficaram impossíveis de serem recuperados, (GOOGLE PLAY, 2013).

- Características do *software:*
- Segurança limpar / rasgar arquivos
- Recupera arquivos com documentos, imagens, vídeos, músicas, arquivos e binários.
- Geração pré-visualização miniatura.
- Operações em lote.
- Pasta de restauração personalizada.

Obs.: o *smartphone* precisará estar com acesso ao *Root* habilitado.

4.20 Root em Smartphones Android

Os sistemas operacionais modernos possuem níveis de permissões para acessos controlados, os quais impedem que pessoas não autorizadas acessem documentos de outros usuários, ou mesmo o acesso de documentos entre usuários. Isso também impede que qualquer um modifique ou apague os arquivos que constituem o sistema operacional (ROOT, 2013).

Root (2013) ainda descreve que o Android é um sistema operacional Linux. Ao menos, sua base é Linux. Por cima do Linux no Android temos a Dalvik, uma espécie de “motor” semelhante, em funcionamento, ao que temos com o Java nos *desktops*. Esse motor, a Dalvik, se encarrega de desenhar a *interface* do sistema e dos programas, além de executar o código, repassando ao sistema Linux as instruções necessárias para a comunicação com o hardware do dispositivo.

Entretanto, a Dalvik deve respeitar as permissões do sistema Linux, que também inclui seu próprio sistema de permissões. Isso torna o sistema Android bastante seguro do ponto de vista técnico.

Existem truques no Android capazes de deixá-lo ainda mais “acessível”, o Root, o qual é uma espécie de desbloqueio nos smartphones com o SO da Google que dá ainda mais “poder” ao dono do celular.

Isso significa que, quando o Root é realizado no aparelho, o que se consegue, na verdade, é obter alguns privilégios de administrador – o chamado “Superusuário”.

Segundo Karasinski (2012), é por meio do Root (além de, em alguns aparelhos, ser necessário também o desbloqueio do bootloader ou a utilização de

programas específicos, como o Rom Manager, por exemplo) que você é capaz de inserir algumas ROMs com versões personalizadas do Android, como as famosas MIUI e Cyanogen MOD.

Além disso, muitas ferramentas só podem ser utilizadas caso seu aparelho possua privilégios de administrador, como aplicativos para realizar overclock no celular, *softwares* de backup com muitas opções diferenciadas, programas para economia de energia, software para restauração de arquivos como o Undelete, por exemplo (KARASINSKI, 2012).

Exemplos de *softwares* para “rootar” seu aparelho *smartphone,* são: Unlock Root, SuperOneClick, Z4root – root direto no celular.

5 METODOLOGIA

O propósito das pesquisas exploratórias é proporcionar ao investigador maior familiaridade com o problema, objetivando torná-lo mais explícito ou construir hipótese. Uma pesquisa de cunho exploratório tende a ser bastante flexível, pois leva em consideração os mais variados aspectos relativos ao problema estudado. De modo geral, pesquisas realizadas com propósitos acadêmicos, pelo menos inicialmente, assumem esse caráter exploratório, pois neste momento é pouco provável que o pesquisador tenha uma definição clara do que irá investigar (GIL, 2010).

A produção deste trabalho exibe uma série de etapas que devem ser seguidas até a obtenção dos resultados, que são a recuperação de arquivos deletados. Considerando a natureza delicada de se realizar uma série de operações em *notebooks*, *smartphones* e computadores particulares ou corporativos, um planejamento deve ser realizado e etapas devem ser seguidas para que evidências não sejam perdidas ou invalidadas posteriormente.

Dessa forma, o projeto é inicialmente uma pesquisa exploratória, pois visa estudar técnicas forenses para recuperação de dados em dispositivos de armazenamento e *smartphones*, visando pesquisar e produzir um levantamento de técnicas para análise pericial em *smartphones* Android.

De início, foi produzida uma pesquisa abordando celulares e sua evolução (tópico 4.2), para posteriormente chegar-se aos *smartphones,* a tecnologia mais atual em quesito de telefonia móvel.

Um breve relato (tópicos 4.5, 4.6 e 4.7) sobre os sistemas operacionais Windows, Linux e Android também foi elaborado, demonstrando brevemente o que é cada um. Esta etapa do trabalho visou ressaltar a importância do sistema operacional para a perícia forense, uma vez que o perito deve possuir um bom conhecimento do sistema com que irá trabalhar.

Um tópico 4.10, sobre informação e segurança da informação foi descrito, tendo o propósito de explicar como os ataques a computadores ocorrem e como obter uma politica de segurança eficaz contra os mesmos. Técnicas como criptografia e esteganografia estão presentes para fornecer um conhecimento básico sobre como os textos e arquivos podem ser mascarados.

Visando demonstrar onde a área de perícia forense e suas aplicações em *smartphones* podem estar presentes, um tópico 4.14 sobre seus conceitos e técnicas foi escrito.

Dentro do campo da perícia forense computacional, peritos devem saber como agir, quais os passos a seguir para que nenhum dano ao equipamento utilizado ocorra. Nesse âmbito, o trabalho visa deixar claros os passos para preservar o material encontrado sob suspeita do crime e o que fazer com o mesmo.

Para atingir os objetivos deste trabalho, os seguintes *softwares* foram utilizados neste trabalho: Recuva, DiskDigger e Active@ File Recovery para Windows; para Linux: Foremost, Scalpel e TestDisk. Já para o Android: Remo Recover for Android e Undelete. Os mesmos foram escolhidos por serem gratuitos e de fácil localização em sistemas de buscas, com exceção do Active@ File Recovery, que é pago. O método de análise utilizado foi a busca mais avançada de cada *software*.

O desenvolvimento do tema proposto ocorreu inicialmente em um ambiente planejado, utilizando-se para os testes de recuperação de arquivos, um computador *desktop* com as seguintes configurações:

- MS Windows 7 Ultimate 32-bits
- Intel Pentium Dual CPU E2180 @2.00Ghz
- 3,00GB RAM
- Intel 82945G Express Chipset Family

E um *notebook* com as configurações listadas abaixo:

- MS Windows 7 Ultimate 32-bits
- Intel Core i5-321M CPU @2.50GHZ
- 8,00GB RAM
- Intel HD Graphics 4000

Para a realização dos testes no sistema operacional Linux, o mesmo foi virtualizado no ambiente Windows pelo *software* “VirtualBox 4.3.2 for Windows hosts, x86/amd64”. O sistema Linux utilizado foi o Ubuntu 13.10.

Os testes foram realizados nos três objetos descritos a seguir: *pen drive (32Gb), HD* Externo (200Gb) *e smartphone (32Gb)*, estes por sua vez foram separados para utilização da seguinte maneira:

- Pasta “Músicas”: (30) trinta arquivos de extensão *.mp3*;
- Pasta “Imagens”: (35) trinta e cinco arquivos de extensão *.jpeg*;
- Pasta “Textos”: (20) vinte arquivos de extensão *.doc* e (20) vinte arquivos de extensão *.pdf*;
- Pasta “Vídeos”: (20) vinte arquivos de vídeos no formato *.mp4.*

A quantidade de arquivos utilizada tem como base uma consulta realizada à professora de estatística Sandra Fiorelli De Almeida P. Simeão.

Desse modo, os três dispositivos continham 125 arquivos diversos e 4 pastas. Após os arquivos serem inseridos, o p*en drive* e HD Externo foram formatados na modalidade “Formatação Rápida” para, na sequência, utilizar-se dos *softwares* de recuperação de arquivos.

Os testes no *smartphone* ocorreram com a anexação dos arquivos no cartão de memória do dispositivo móvel. Após essa ação foi dado inicio aos testes, de duas maneiras diferentes. Na primeira, os arquivos foram recuperados por um *software* projetado para computador (*Windows* 7); já na segunda, o *software* foi projetado para rodar diretamente no *smartphone*.

A plataforma Android foi a escolhida para a realização deste trabalho, pois atingiu marcas expressivas como: 700 mil aplicativos desenvolvidos e disponibilizados no Google Play, contando com mais de 1 milhão e 300 mil aparelhos vendidos e ativados de acordo com Android (c2013).

5.1 *Softwares* utilizados para recuperação no Sistema Operacional Windows

5.1.1 DiskDigger

Antes do início dos testes de recuperação, uma imagem foi capturada com todos os arquivos dentro do *pen drive*, conforme demonstra a Figura 5. Esses arquivos foram apagados posteriormente para o teste ser realizado, esta situação foi utilizada para todos os *softwares* em todas as mídias usadas.

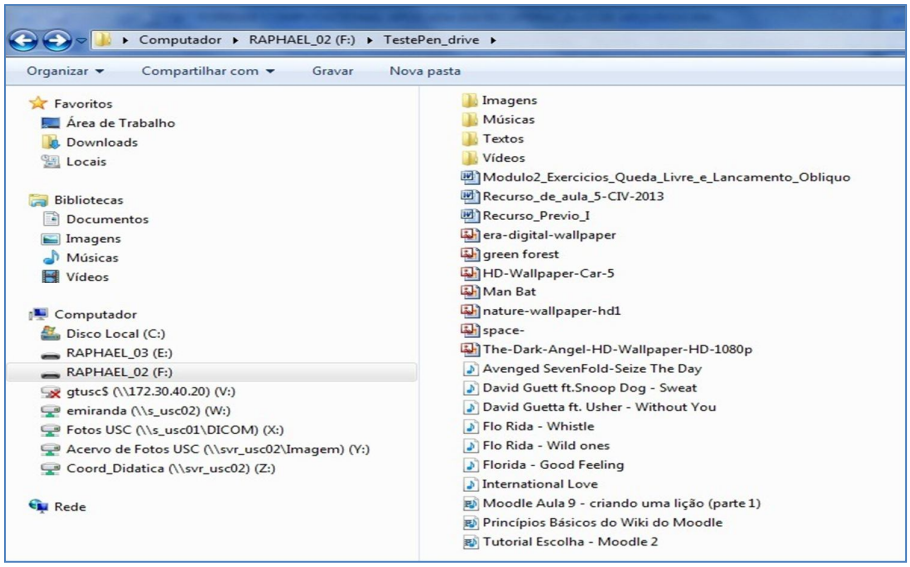

Figura 5 – *Pen Drive* com os arquivos utilizados para os testes de recuperação.
Fonte: Elaborado pelo Autor (2013).

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 6 exibe a *interface* inicial do *software*, denotando os discos físicos, *drives* lógicos, evidenciando também o *pen drive* utilizado no teste, localizado na opção F:.

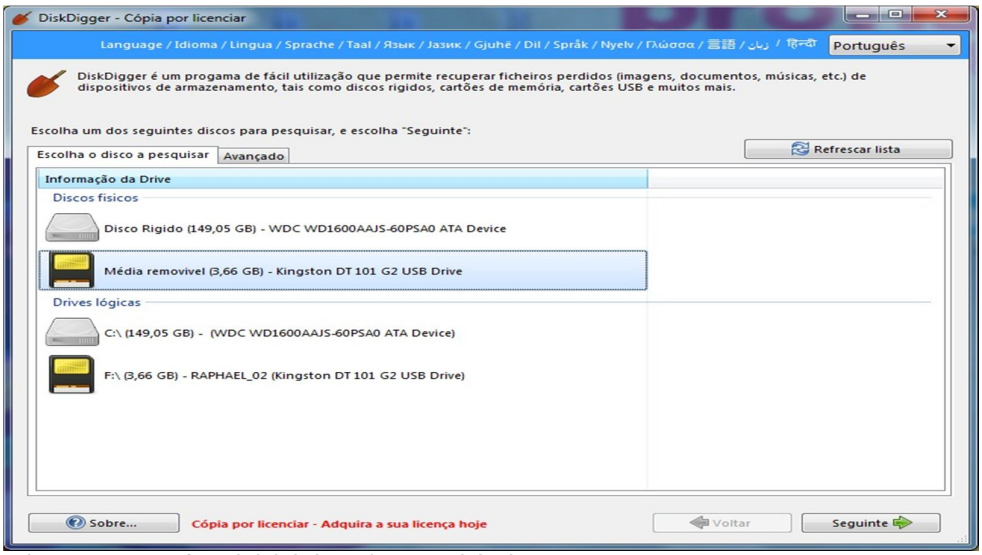

Figura 6 – *Interface* inicial do software DiskDigger.
Fonte: DiskDigger (2013).

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 7.

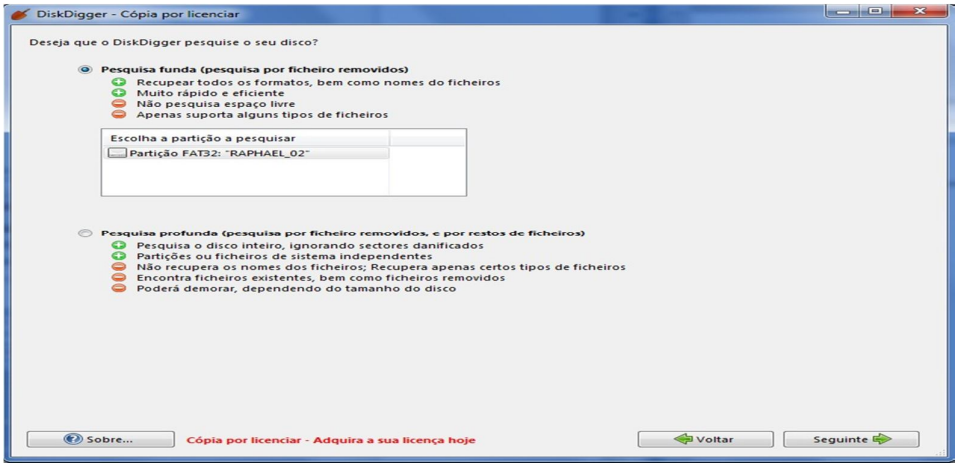

Figura 7 – Tela onde o usuário pode escolher as opções de busca.
Fonte: DiskDigger (2013).

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 8.

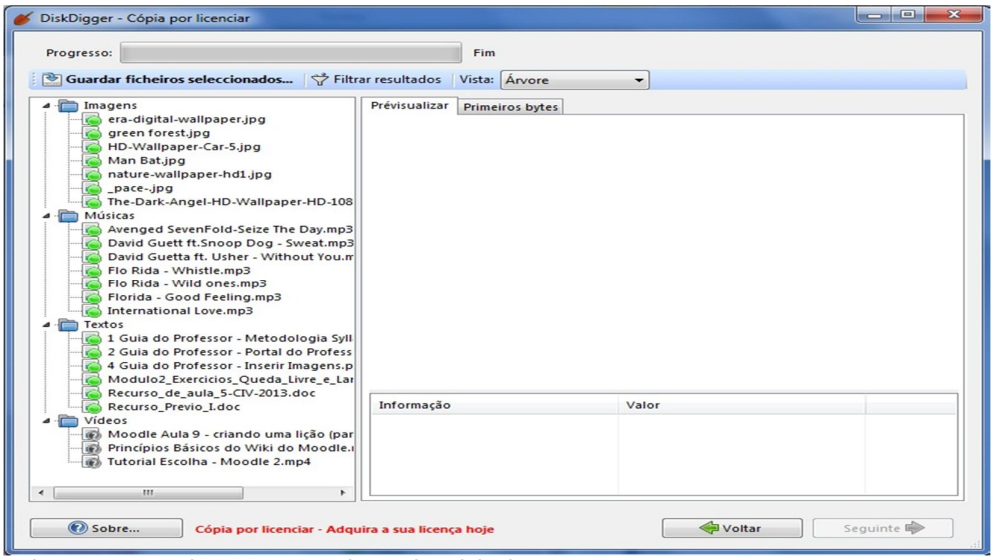

Figura 8 – Arquivos recuperados pelo DiskDigger.
Fonte: DiskDigger (2013).

5.1.2 Recuva

Os testes realizados no *software* Recuva foram idênticos ao DiskDigger, os arquivos do *pen drive* e HD Externo foram apagados e a recuperação dos arquivos foi testada.

Ao apagar um arquivo, o usuário envia a seguinte informação para o computador: “Este espaço do disco rígido poderá ser usado se necessário”. Portanto o arquivo continua ali até que algum outro ocupe seu espaço. 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 9.

Figura 9 – Assistente do *software* Recuva.
Fonte: Recuva (2013).

O próximo passo exibe a sequência do “Assistente do Recuva”. Nessa opção o *software* indica quais tipos de arquivos o usuário está tentando recuperar; de início a opção “documentos” foi escolhida, conforme exibe a Figura 10.

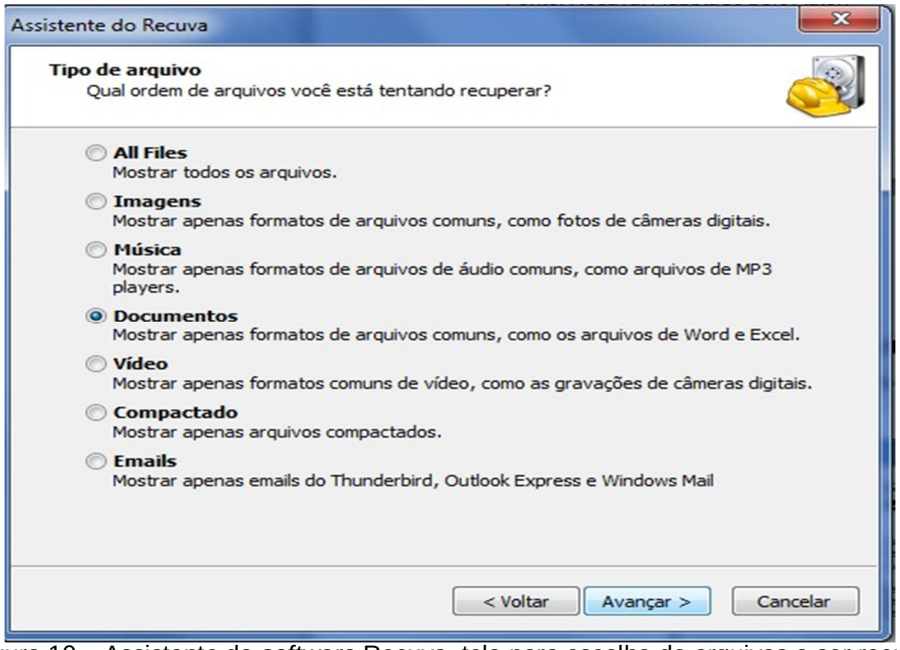

Figura 10 – Assistente do *software* Recuva, tela para escolha de arquivos a ser recuperados.
Fonte: Recuva (2013).

Na sequência o *software* solicitou o local onde os arquivos se encontraram. O usuário pode escolher entre cinco opções; a princípio a opção escolhida foi: “Em um local especifico, “Unidade F:\”. Esta é a unidade onde o *pen drive* está alocado, como demonstra a Figura 11.

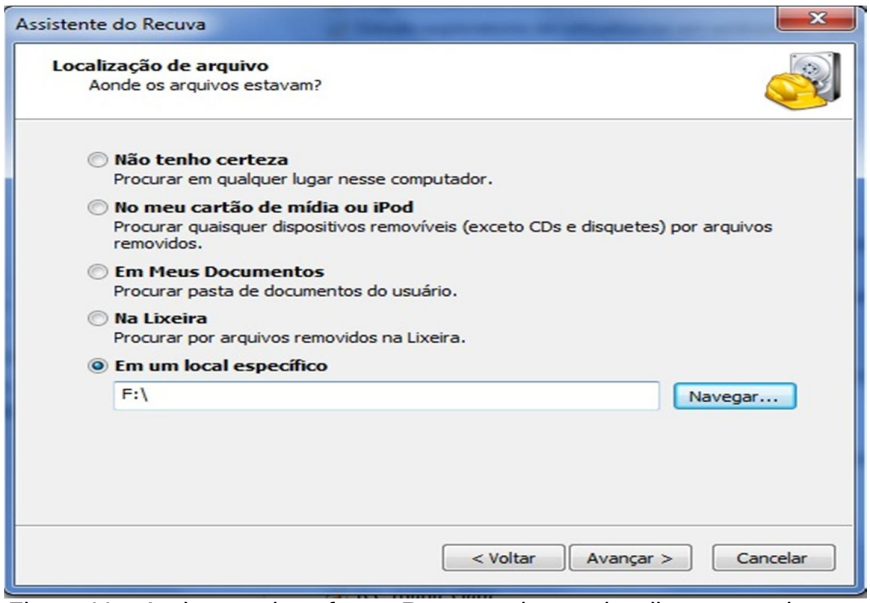

Figura 11 – Assistente do *software* Recuva, tela para localizar os arquivos a serem recuperados.
Fonte: Recuva (2013).

Após a escolha do local onde os arquivos estavam 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 12.

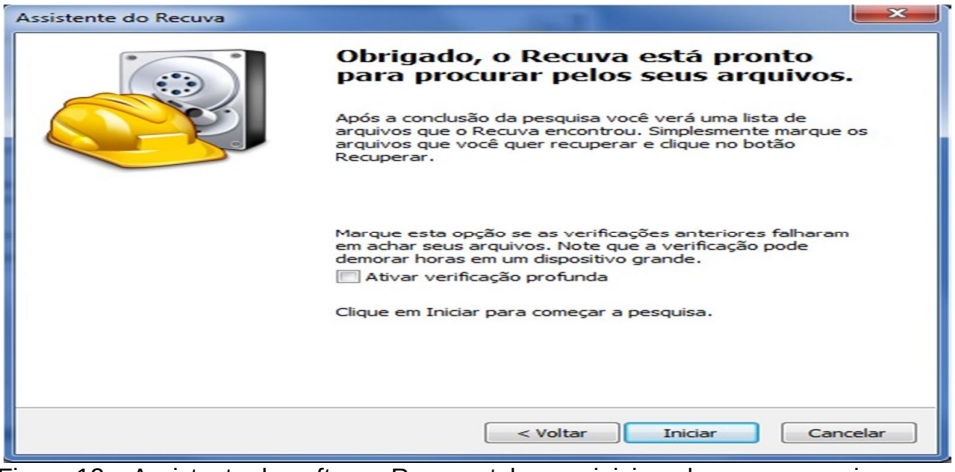

Figura 12 – Assistente do *software* Recuva, tela para iniciar a busca por arquivos apagados.
Fonte: Recuva (2013).

Na sequência, os arquivos com possibilidade de recuperação são demonstrados na Figura 13, ficando a critério do usuário qual recuperar ou não.

Nesta etapa, bastou selecionar o arquivo desejado e clicar em “Recuperar...”, selecionar um local para que o programa possa recuperar esses arquivos e salvá-los.

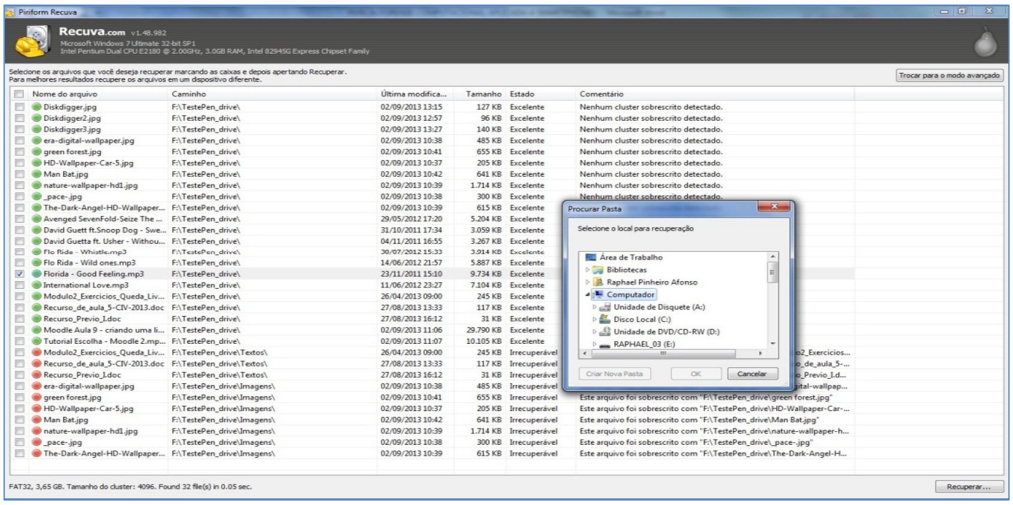

Figura 13 – Arquivos encontrados pelo Recuva.
Fonte: Recuva (2013).

5.1.3 Active@ File Recovery

Depois do *software* instalado e iniciado, o próximo passo foi escolher a opção QuickScan. Essa opção é utilizada para realizar uma varredura rápida no dispositivo escolhido. Após a realização do escaneamento os arquivos com possibilidade de recuperação serão exibidos, conforme Figura 14.

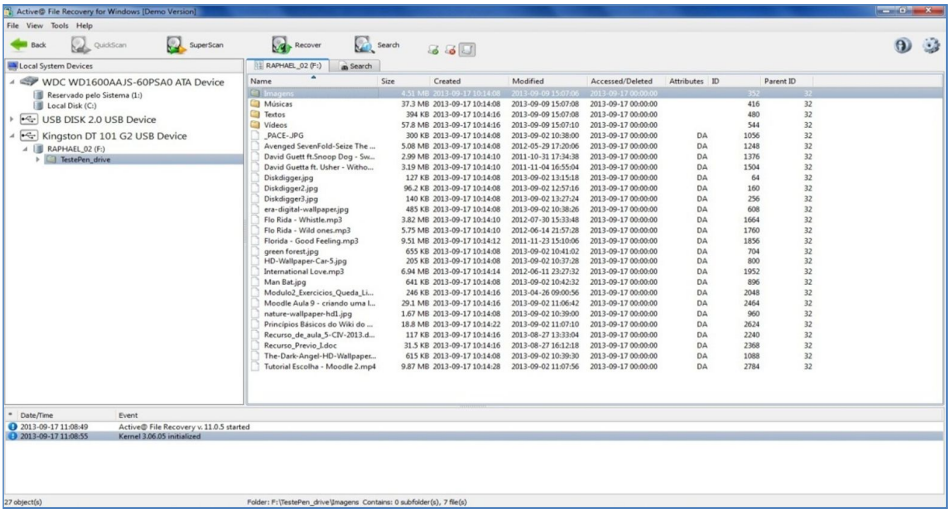

Figura 14 – Arquivos encontrados pelo Active@ File Recovery.
Fonte: Active@ File Recovery (2013).

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 15 demonstra os arquivos que podem ser recuperados, e os locais onde é possível salvar o arquivo desejado.

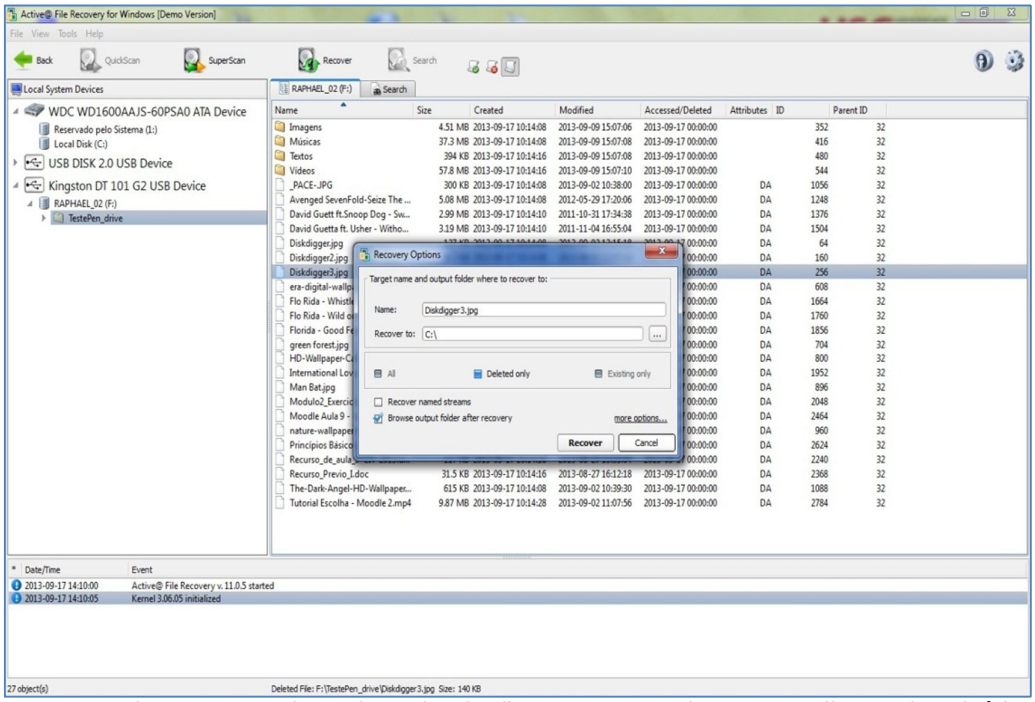

Figura 15 – Arquivos encontrados pelo Active@ File Recovery e tela para escolher onde salvá-los.
Fonte: Active@ File Recovery (2013).

O *software* Active@ File Recovery apresentou, ainda, a opção SuperScan, a qual tem a função de inspecionar volumes existentes mais profundamente. Por exemplo, caso o volume tenha sido formatado, o QuickScan não exibe nenhum arquivo. Já o SuperScan detecta estruturas de dados formatados e reconstrói árvore de dados anterior.

5.2 *Softwares* utilizados para recuperação no Sistema Operacional Android

5.2.1 Remo Recover for Android

A Figura 16 exibe a tela inicial do *software* Remo Recover for Android. Nesta tela existem duas opções para o usuário escolher: Recuperar os Arquivos Apagados ou Recuperar Arquivos Perdidos.

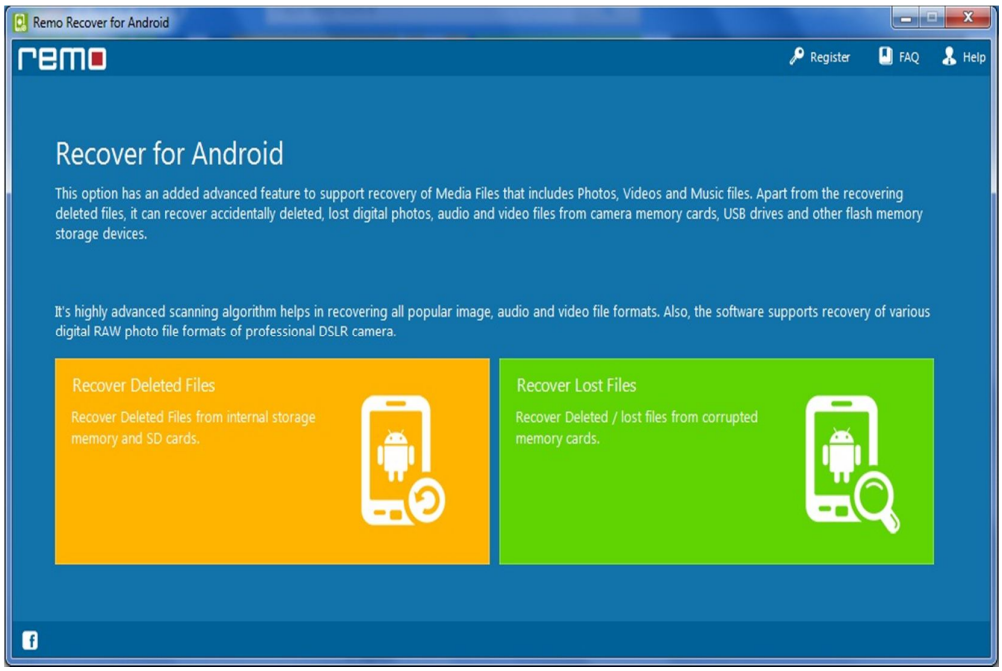

Figura 16 – Tela principal do *software* Remo Recover for Android.
Fonte: Remo Recover for Android (2013).

Já com *smartphone* plugado e reconhecido pelo aplicativo, uma tela foi exibida com as partições do *smartphone*, a Figura 17 demonstra as partições do *smartphone* testado.

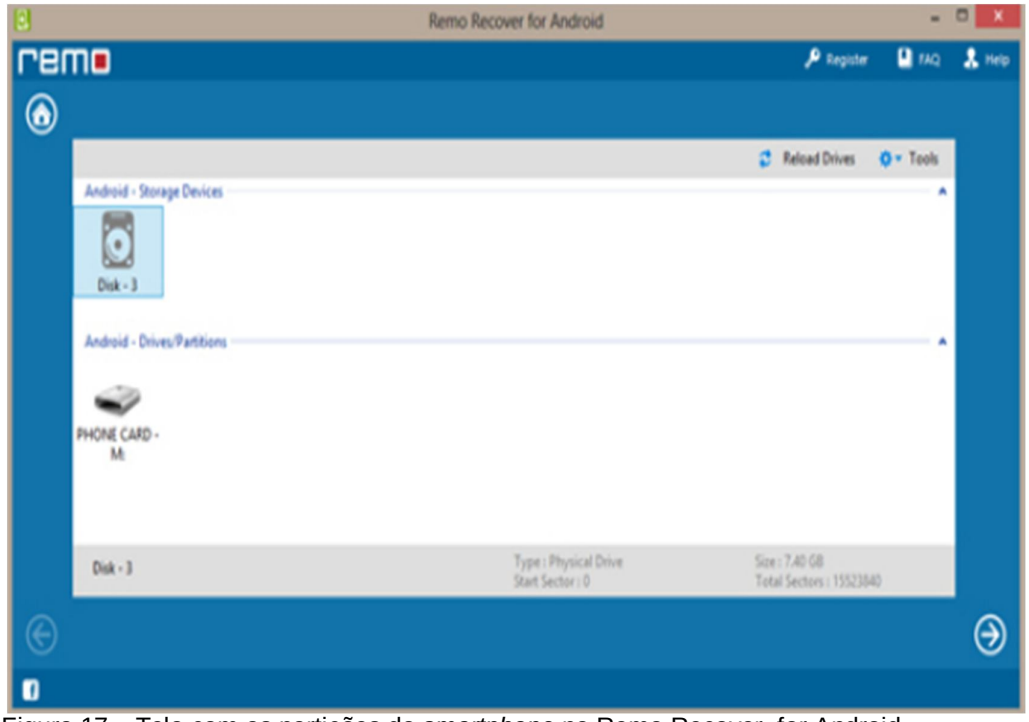

Figura 17 – Tela com as partições do *smartphone* no Remo Recover for Android.
Fonte: Remo Recover for Android (2013).

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 18 exibe estas descrições.

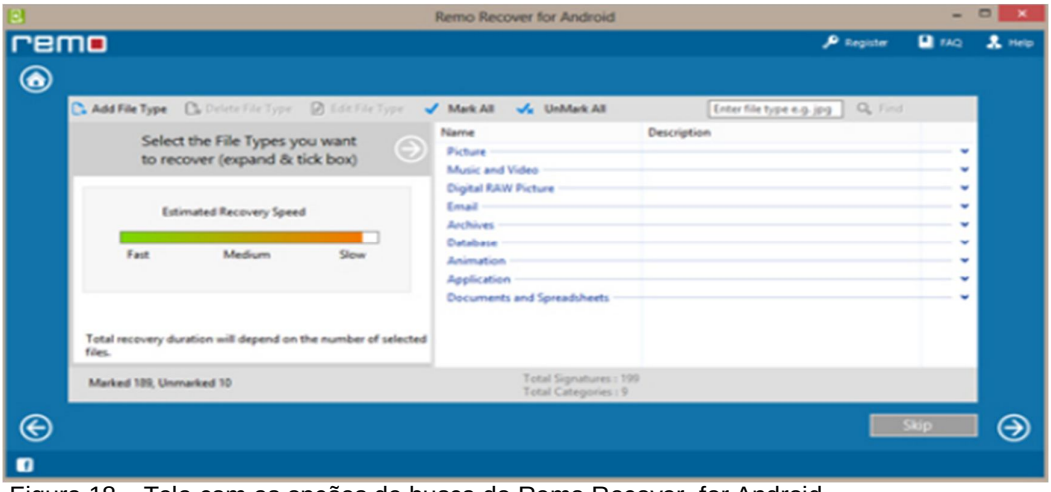

Figura 18 – Tela com as opções de busca do Remo Recover for Android.
Fonte: Remo Recover for Android (2013).

Na sequência, depois de o processo de pesquisa terminar, os arquivos que podem ser recuperados são exibidos, conforme exibe a Figura 19. 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.

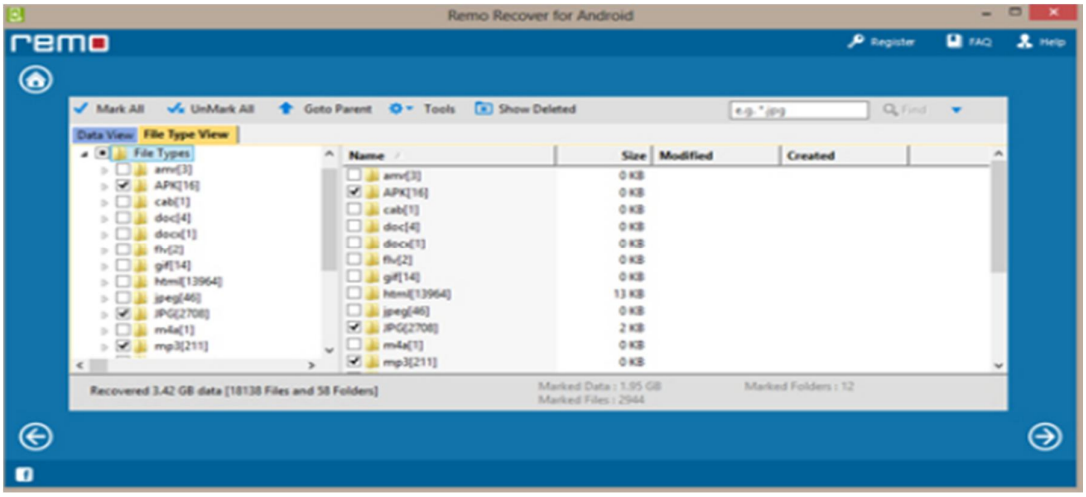

Figura 19 – Tela com os arquivos com possibilidade de recuperação no Remo Recover for Android.
Fonte: Remo Recover for Android (2013).

O programa possui uma *interface* muito interessante, com cores sólidas e chapadas. Além disso, 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, vídeos e apks.

Remo Recover for Android é uma ótima e simples solução para quem precisa recuperar arquivos perdidos e é um bom aliado de pessoas descuidadas que precisam manter o programa sempre por perto.

5.2.2 Undelete

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 20 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 30 segundos. Poderá gastar mais tempo caso o cartão seja maior ou esteja muito carregado de arquivos.

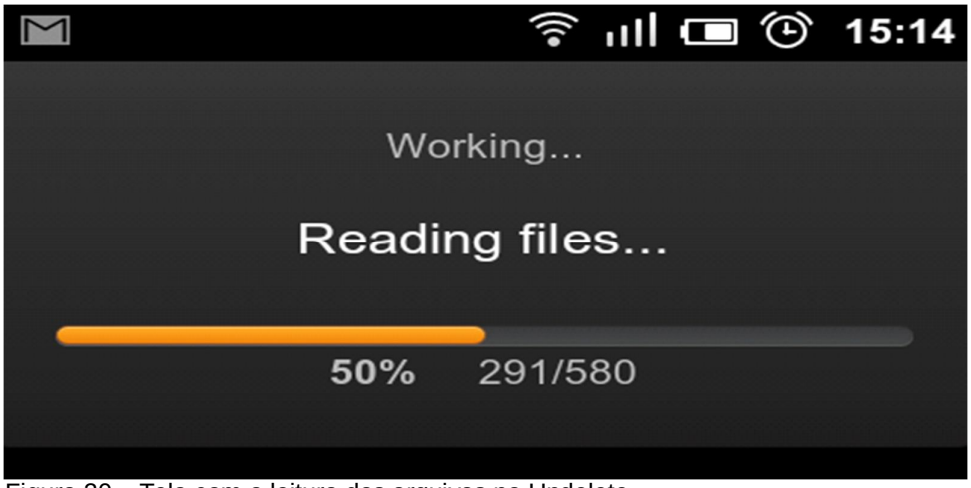

Figura 20 – Tela com a leitura dos arquivos no Undelete.
Fonte: Undelete (2013).

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 na Figura 21 a lista de arquivos encontrados é mostrada, e o tamanho, caminho e onde os arquivos se encontravam antes de serem deletados.

Figura 21 – Tela com os arquivos encontrados no Undelete.
Fonte: Undelete (2013).

Após o usuário escolher qual arquivo será recuperado, basta pressionar o botão “*Restore*” para o aplicativo recuperar o arquivo em questão.

Para que o software funcione o *smartphone* utilizado precisará ter a permissão de Root. Um capítulo sobre este assunto está presente na pagina 40.

5.3 *Softwares* utilizados para recuperação no Sistema Operacional Linux

5.3.1 Scalpel

Para instalar o Scalpel, com o terminal aberto foi necessário pressionar as teclas “Ctrl + Alt + T” e na sequência digitar o seguinte comando:

$ sudo apt-get install scalpel

Com a instalação realizada, a seguinte mensagem é exibida na Figura 22:

```
Lendo listas de pacotes... Feito
Construindo árvore de dependências
Lendo informação de estado ... Feito
Os seguintes pacotes NOVOS serão instalados:
  scalpel
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos e 390 não atualizados.
É preciso obter 0 B/33.9 kB de arquivos.
Após esta operação, serão utilizados 118 kB de espaço em disco adicional.
Selecionando pacote previamente não selecionado scalpel.
(Banco de dados ... 151082 arquivos e diretórios atualmente instalados Leitura).
Desempacotando bisturi (de ... / scalpel_1.60-1build1_i386.deb) ...
Processamento de gatilhos para man-db ...
Criação de scalpel (1,60 1build1) ...
tecmint @ tecmint-Latitude-D630: ~ $
```

Figura 22 – Tela com a Saída de amostra no Scalpel.
Fonte: Scalpel (2013).

Já com Scalpel instalado, foi necessário realizar uma edição de texto. Por utilidade padrão o Scalpel tem seu próprio arquivo de configuração em “**/ etc**” o

caminho do diretório completo é **"/ etc / scalpel / scalpel.conf "** ou "**/ etc / scalpel.conf".**

Pode-se notar que tudo está comentado com (#). Então, é necessário descomentar o arquivo que irá ser recuperado antes do Scalpel ser executado. Entretanto retirar o arquivo inteiro é demorado e irá gerar uma enorme quantidade falsos resultados.

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.

 # GIF e JPG

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.

A saída do comando acima é:

```
Scalpel versão 1.60
Escrito por Golden G. Richard III, com base em Foremost 0,69.
Abertura target " / dev/sda1"
Arquivo de imagem passar ½.
/ Dev/sda1: 6,1% | ***** | 6.6 GB 39:16 ETA
```

Figura 23 – Tela com saída de amostra do Scalpel.
Fonte: Scalpel (2013).

A Figura 23 acima exibi o *software* realizando o processo de recuperação dos arquivos deletados, pode existir certa demora para conclusão do processo, dependendo do espaço em disco utilizado e a velocidade do computador.

5.3.2 Foremost

O *software* Foremost é acima de tudo um programa de console de recuperação de arquivos com base em seus cabeçalhos, rodapés e estruturar de dados internas. O programa permite trabalhar em arquivos de imagem gerados por

softwares de pericia forense, como dd, Safeback, Encase, ou diretamente na unidade. Essa ferramenta pode ser encontrada livremente para qualquer sistema Linux.

O processo de instalação se iniciou a partir da Central de Programas do Linux. Sendo assim, o *software* foi localizado na central do sistema, na barra de atalhos ou pesquisando através do menu de aplicativos do SO.

Já com a Central de Programas aberta, foi pesquisado o nome do Foremost na barra de buscas. Assim que os resultados estiverem compilados, o item foi selecionado “Aplicação forense para recuperar dados” e, em seguida, o programa foi instalado.

Para dar inicio ao processo de recuperação, é necessário digitar o seguinte comando:

sudo fdisk -L

Feito isso, analise a tela exibida no terminal e identifique o disco do qual serão recuperados os arquivos, observando o espaço total de cada um. No caso desta recuperação, o *pen drive* ficou como “/dev/sdc”, conforme ilustra a Figura 23.

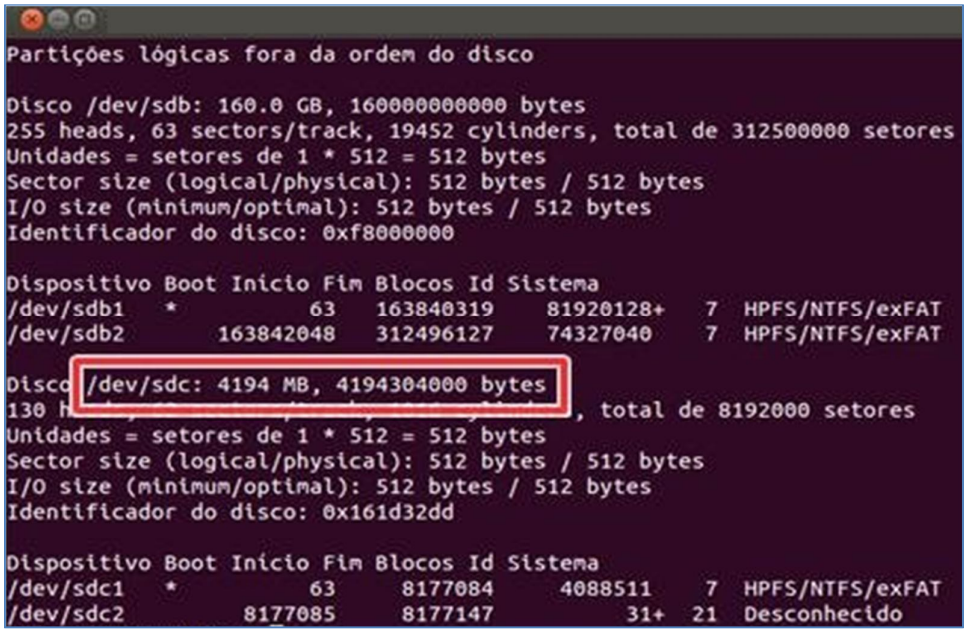

Figura 24 – Pen drive listado no Foremost.
Fonte: Scalpel (2013).

Neste passo, foi necessário criar uma réplica raw do disco. Dependendo do espaço do dispositivo, o procedimento pode ser um pouco demorado. Para tal, digite a linha:

sudo dd if=/dev/sdc/ of=pendrive.raw

Onde estava "**/dev/sdc/**", altere pelo nome do seu disco. Feito isso, entre com a próxima linha de comando:

sudo foremost -t all -i pendrive.raw -o recuperados

Nesta recuperação, foi utilizado o comando "**all**" para selecionar todos os itens para a recuperação. No entanto, pode-se procurar apenas um documento, vídeo, música ou imagem, substituindo esta parte pela extensão do arquivo procurado. Caso seja uma foto, coloque JPG, JPEG, GIF etc.

Desta maneira, os arquivos foram recuperados. Sendo assim, para acessá-los, digite o seguinte comando:

sudo nautilus recuperados

O navegador de arquivos exibiu um diretório com todos os arquivos recuperados separados por pastas que indicam a extensão dos documentos. No entanto, os itens não retornam com os antigos nomes e foi preciso procurar o arquivo desejado dentre as opções.

5.3.2 TestDisk

O programa foi instalado através do terminal com a seguinte sintaxe:

 # apt-get install testdisk

A utilização do programa é todo por linha de comando e exige atenção e conhecimento do conteúdo a ser recuperado. Para começar o trabalho, foi aberto o terminal, pressionando Ctrl+Alt+T e digitado o seguinte comando:

$ sudo testdisk

Com o *pen drive* plugado no computador uma lista de todos os diretórios do pen drive diferentes de (.) e (..) foi feito com o comando **ls –ld*/**.

Desta maneira, a Figura 25 exibe o *software* já apontado para o *pen drive*, restando apenas pressionar a tecla Enter para prosseguir.

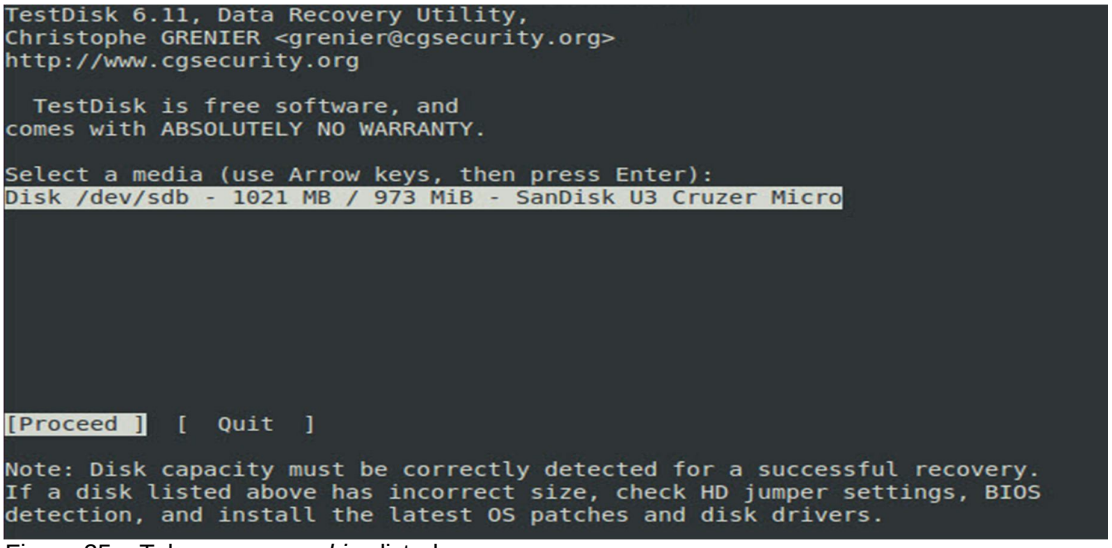

Figura 25 – Tela com o *pen drive* listado.
Fonte: TestDisk (2013).

. No próximo passo, o *software* deseja saber qual tabela de partição de disco está utilizando, no teste realizado foi a Intel, pois a maioria das maquinas atuais seguem a arquitetura X86. A Figura 26 exibe esta representação.

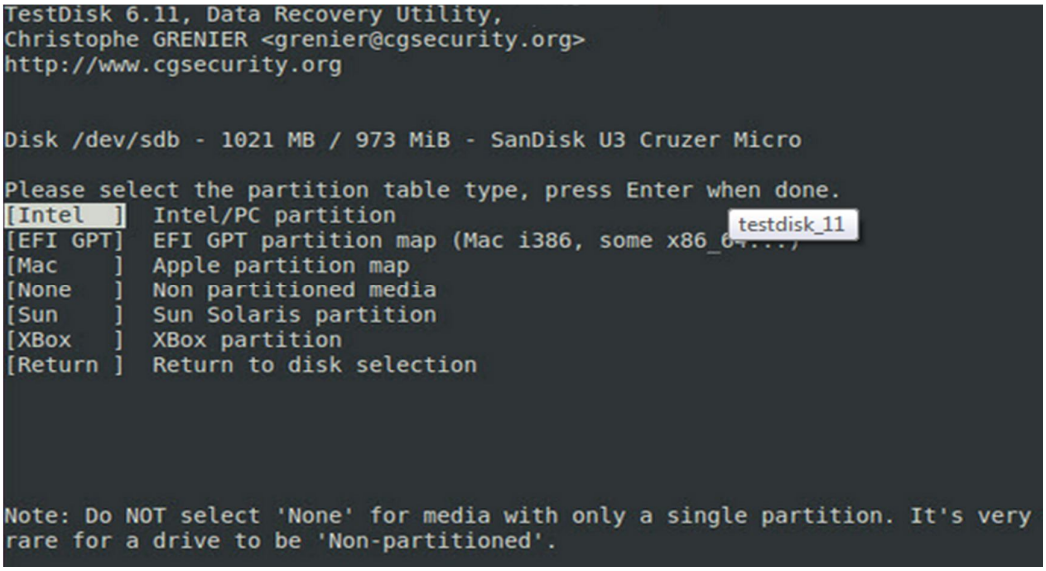

Figura 26 – Tela com a tabela de partições do disco.
Fonte: TestDisk (2013).

Já com a partição escolhida o programa irá listar uma série de opções para realizar o procedimento, a opção utilizada foi: “*Analyse current partition estructure and search for lost partitions”.*

Com a partição encontrada, uma busca é realizada na mesma, isto demanda uma grande quantidade de tempo, pois o software percorreu cilindro por cilindro do disco, esta explicação é exibida na Figura 27**.**

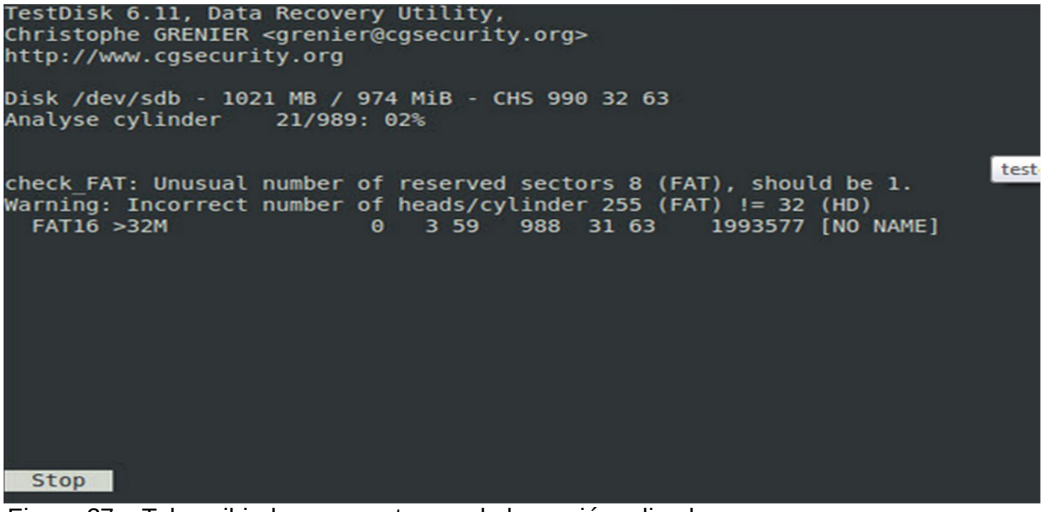

Figura 27 – Tela exibindo a porcentagem da busca já realizada.
Fonte: TestDisk (2013).

Após a realização da busca na partição os arquivos existentes e não existentes do disco estão listados na Figura 28. Todos os arquivos em vermelho “não existem” mais no disco.

Entretanto isto não é totalmente verdade, uma vez que um arquivo existe no disco e é removido, sua referencia ainda permanece até que seja sobrescrita por outro arquivo. No exemplo oferecido somente removendo o diretório junto com os arquivos dentro, e não foi modificado mais nada no *pen drive*. As chances de recuperação são de 95%.

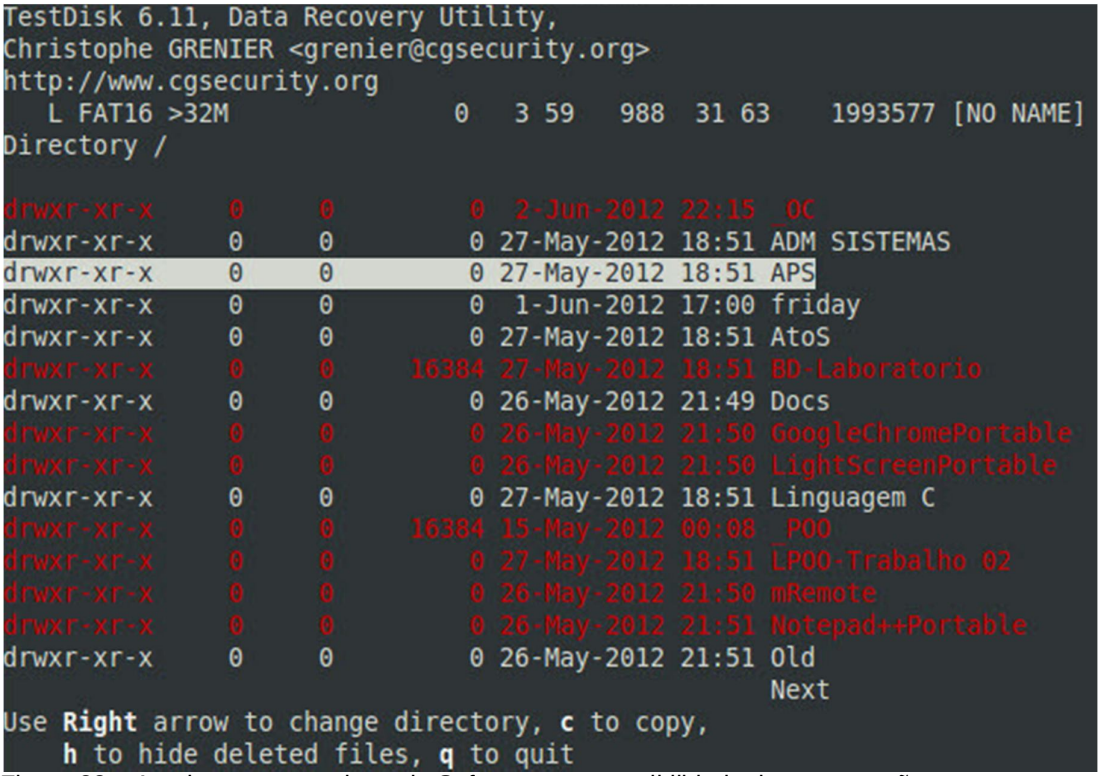

Figura 28 – Arquivos encontrados pelo Software com possibilidade de recuperação.
Fonte: TestDisk (2013).

Para salvar os arquivos basta pressionar c, para copia-los desde que não seja na mesma partição de onde os mesmos vieram.

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 *pen drive,* HD externo e *smartphone* foi de 125 arquivos, divididos entre imagens, músicas, textos e vídeos.

Recuperação de arquivos no Software DiskDigger - Plataforma Windows.

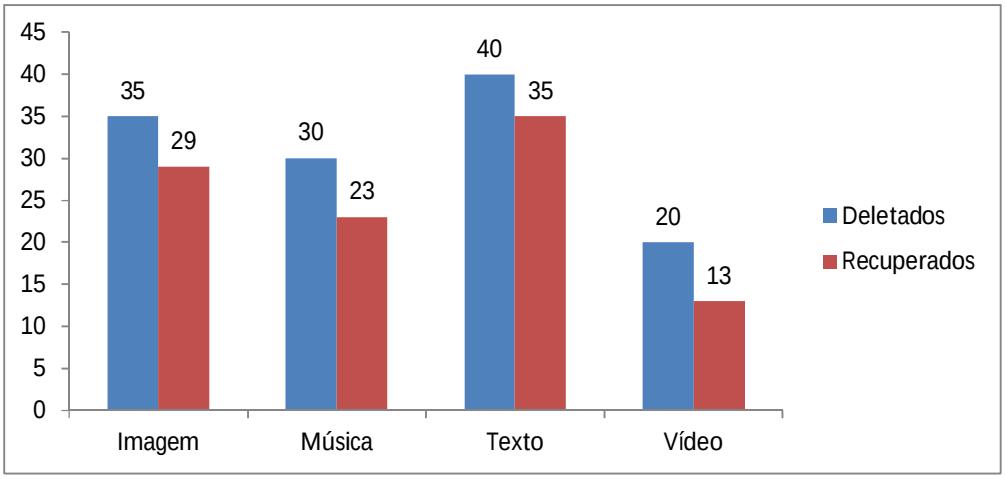

Figura 29 – Resultados obtidos pelo *software*: DiskDigger.
Fonte: Elaborado pelo autor (2013).

Conforme ilustra a Figura 29, (verificar apêndice A), 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 e pdf. com tamanho superior a 5Mb tiveram recuperação parcial, ou seja, faltavam páginas nos arquivos.

Nos testes realizados, o *software* DiskDigger não conseguiu realizar a recuperação dos arquivos, caso o *pen drive* e/ou HD externo fossem formados pelo sistema operacional da máquina testada. O mesmo aconteceu com o cartão de memória do *smartphone*. O programa mostrou um bom desempenho no quesito tempo de recuperação, levando em conta que a busca por arquivos levou cerca de aproximadamente 15 minutos.

Recuperação de arquivos no Software Recuva - Plataforma Windows.

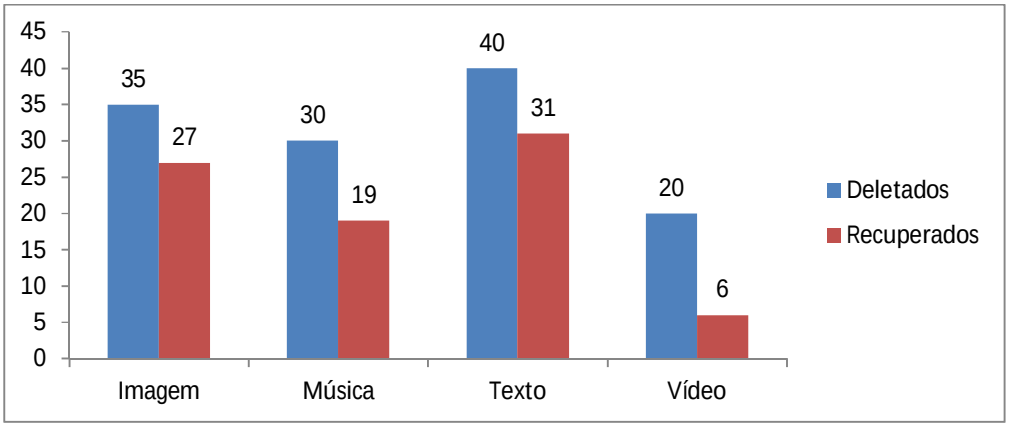

Figura 30 – Resultados obtidos pelo *software*: Recuva.
Fonte: Elaborado pelo autor (2013).

A recuperação pelo *software* Recuva mostrou-se muito eficiente com arquivos nas extensões .jpg, .doc e .pdf. Os arquivos de músicas no formato .mp3 e os de vídeos no formato .mp4, a recuperação pode ser considerada precária.

A quantidade de arquivos recuperados exibida na Figura 30, (verificar apêndice A), 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 9 minutos. O programa pode ser adquirido em sua versão paga, o que aumenta seu poder de recuperação.

Recuperação de arquivos no Software Active@ File Recovery - Plataforma Windows.

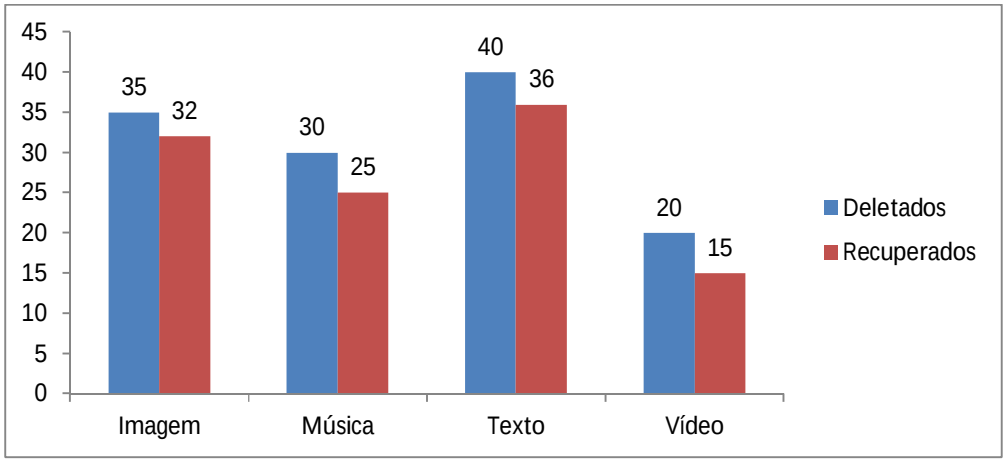

Figura 31 – Resultados obtidos pelo *software*: Active@ File Recovery.
Fonte: Elaborado pelo autor (2013).

O *software* se mostrou muito eficiente na recuperação de qualquer arquivo, em todos os dispositivos testados, conforme demonstra a Figura 31, (verificar apêndice A). O tempo para recuperação foi de aproximadamente 20 minutos, mas compensa por sua eficiência. Embora a qualidade do *software* seja muito boa, arquivos considerados grandes não foram recuperados.

Arquivos .doc e .pdf foram recuperados parcialmente, perdendo páginas, entretanto foram os que demonstraram mais eficiência na recuperação.

Recuperação de arquivos no Software Remo Recover for Android - Plataforma Android.

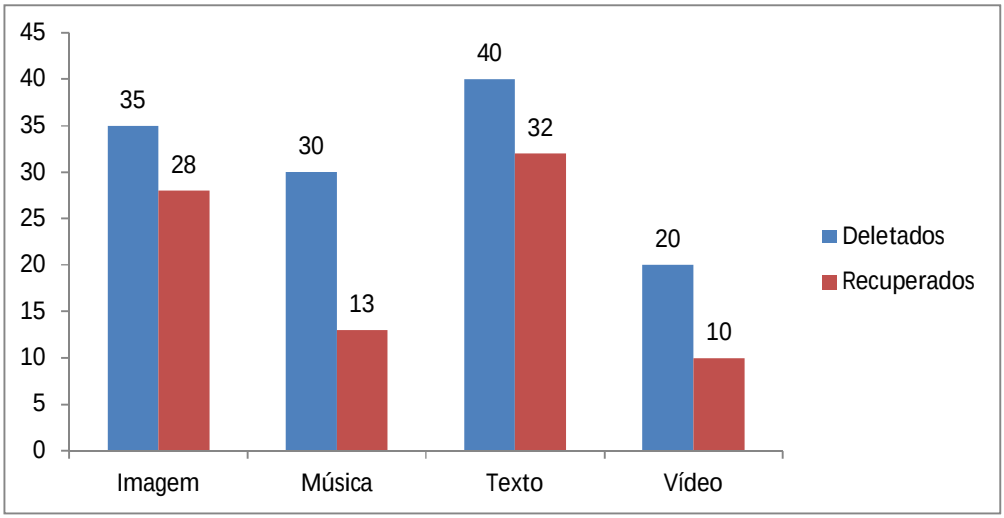

Figura 32 – Resultados obtidos pelo *software*: Remo Recover for Android.
Fonte: Elaborado pelo autor (2013).

O *software* próprio para *smartphones* se mostrou muito eficiente na recuperação de arquivos .pdf, .doc e .jpg, conforme ilustra a Figura 32 (verificar apêndice A). A verificação foi realizada tanto na memória interna do aparelho quanto em seu cartão de memória; a quantidade de arquivos recuperados foi idêntica em ambos os lugares.

Sua capacidade de recuperação deixa a desejar em arquivos de maior tamanho, como músicas e vídeos. O tempo decorrido para a busca por arquivos perdidos foi de aproximadamente 9 minutos. Por se tratar de um *software* próprio para *smartphone* a recuperação foi considerada eficiente.

Recuperação de arquivos no Software Undelete - Plataforma Android.

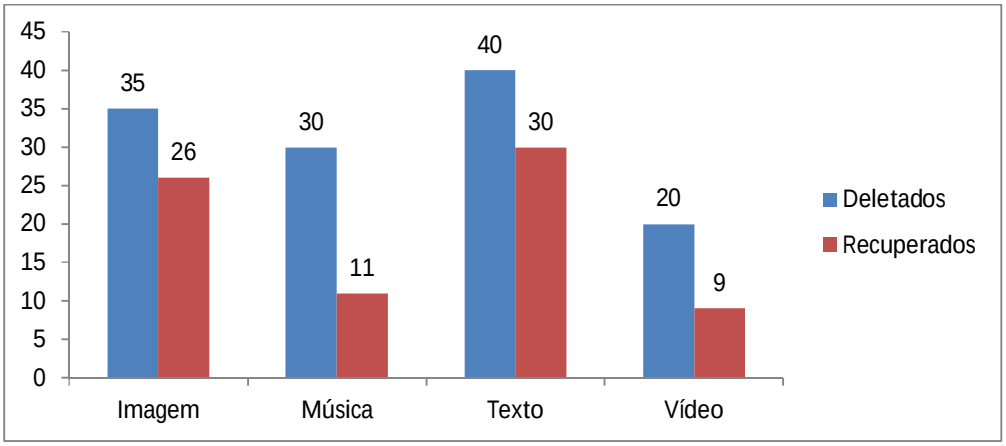

Figura 33 – Resultados obtidos pelo *software*: Undelete.
Fonte: Elaborado pelo autor (2013).

A recuperação no *software* Undelete pode ser considerada muito precária na recuperação de arquivos de grande tamanho, como vídeos ou músicas com até 10 Mbs, mas acima deste tamanho o *software* não consegue nem encontrá-los; o mesmo acontece com músicas. Arquivos .pdf, .doc e .jpg obtiveram uma boa recuperação, como ilustra a Figura 33 (verificar apêndice A).

O tempo de localização dos arquivos deletados foi aproximadamente 8 minutos. No caso específico deste programa o celular do usuário precisa ser "rooteado", caso contrário o programa não funcionará. O software roda diretamente no *smartphone.*

Recuperação de arquivos no Software Scalpel - Plataforma Linux.

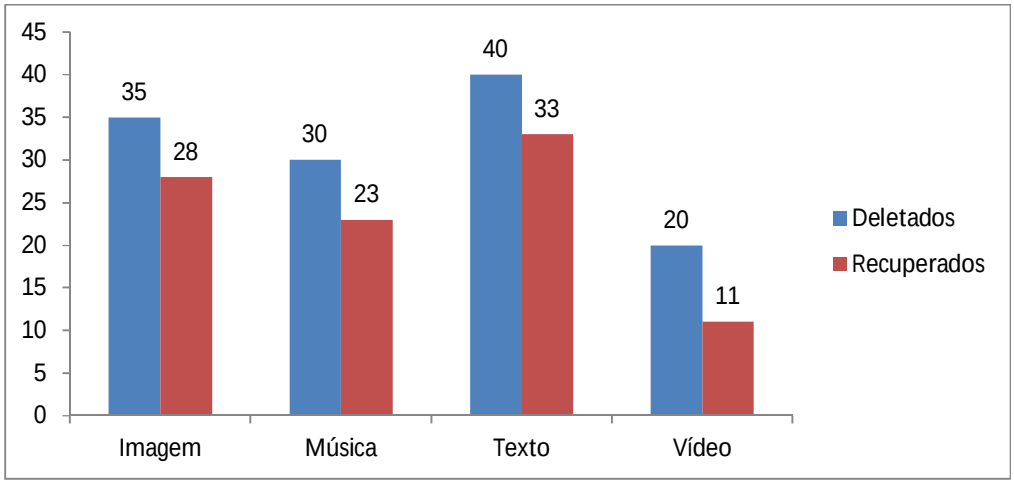

Figura 34 – Resultados obtidos pelo *software*: Scalpel.
Fonte: Elaborado pelo autor (2013).

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 34 (verificar apêndice A).

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

Recuperação de arquivos no Software Foremost - Plataforma Linux.

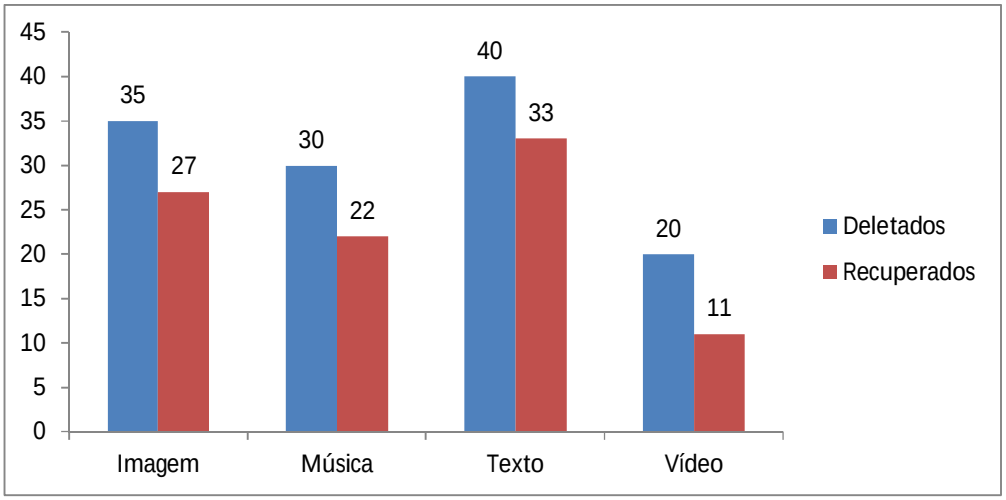

Figura 35 – Resultados obtidos pelo software: Foremost.
Fonte: Elaborado pelo autor (2013).

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

A Figura 35 (verificar apêndice A) ilustra o desempenho do software Foremost, deixando claro que a recuperação de vídeos e texto foi semelhante ao do Scalpel.

O tempo para localização dos arquivos foi aproximadamente 12 minutos.

Recuperação de arquivos no Software TestDisk - Plataforma Linux.

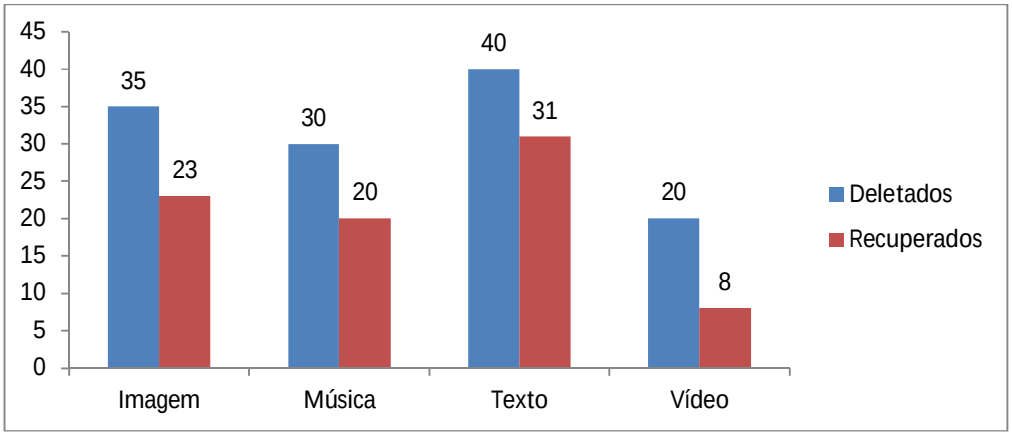

Figura 36 – Resultados obtidos pelo *software*: TestDisk
Fonte: Elaborado pelo autor (2013).

A recuperação no *software* TestDisk se mostrou muito inferior aos seus concorrentes na plataforma Linux, conforme exibe a Figura 36 (verificar apêndice A). O programa recuperou poucos arquivos .jpg, não atingiu nem 50% de recuperação nos arquivos .mp3 (músicas), recuperou arquivos de textos faltando páginas e conseguiu listar algumas músicas em sua busca.

O tempo decorrido para a listagem dos arquivos foi de aproximadamente 9 minutos.

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

Recuperação de Arquivos na Plataforma Windows.

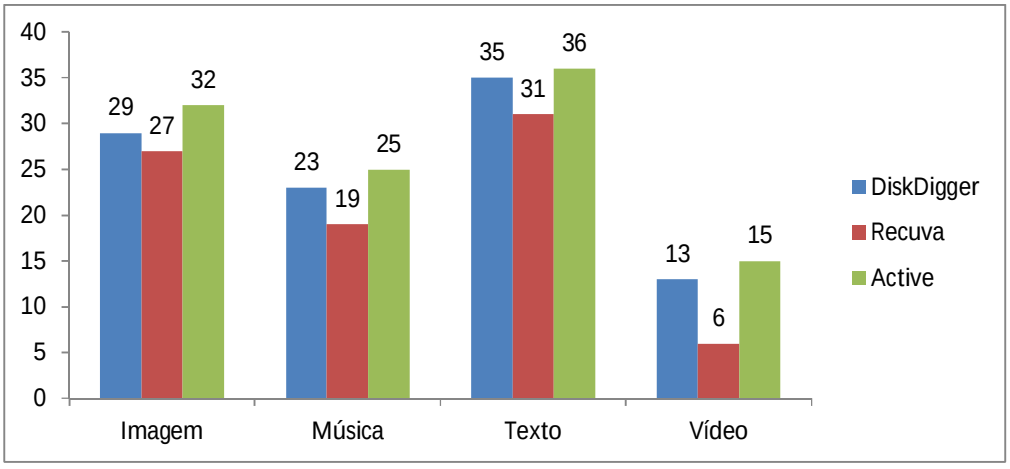

Figura 37 – Resultados comparativos entre os *softwares* na plataforma Windows.
Fonte: Elaborado pelo autor (2013).

Conforme ilustra a Figura 37 (verificar apêndice B), o *software* com maior quantidade de arquivos recuperados foi o Active@ File Recovery, que também obteve a maior recuperação em todos os outros quesitos, como vídeos, imagens e músicas.

Pode-se analisar que o tempo no processo de localização dos arquivos deletados foi maior no Active; isso demonstra que o tempo de recuperação interfere diretamente na recuperação dos arquivos. Todos os *softwares* com maior tempo de localização de arquivos recuperaram mais arquivos que seus concorrentes.

Ficou evidente também que arquivos grandes sejam eles .doc, .pdf, .jpg, .mp3 ou mp4 não são recuperados, ou quando são, ficam incompletos no caso dos arquivos em .pdf e .doc.

O desempenho do *software* Recuva se mostrou abaixo dos outros dois, ficando evidente pelo número de arquivos recuperados. O tempo gasto pelo Recuva para a localização dos arquivos (9 minutos) confirma que, quanto mais rápido o software analisa o *pen drive* e/ou Hd externo, menos arquivos ele consegue recuperar.

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

Recuperação de Arquivos na Plataforma Android.

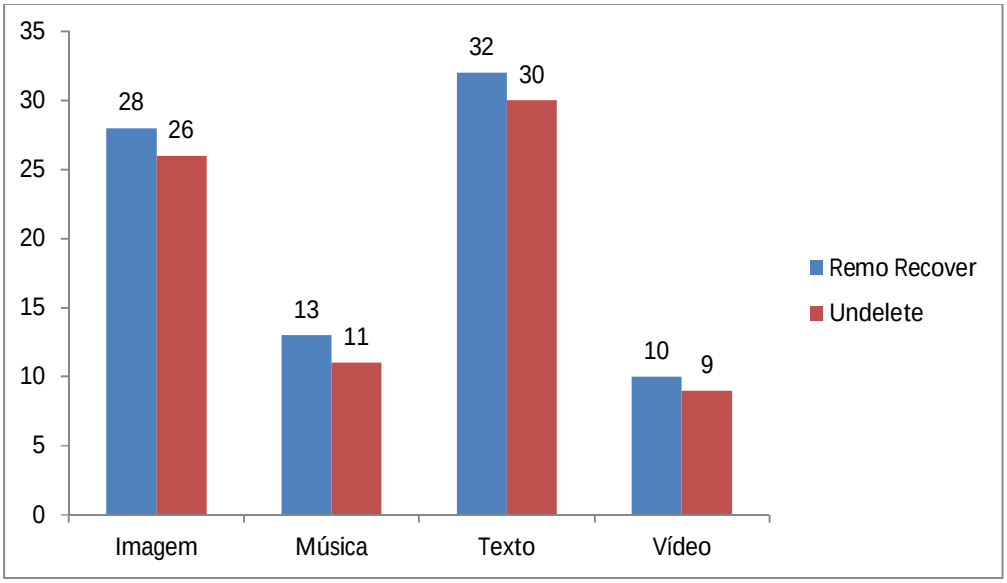

Figura 39 – Resultados comparativos entre os *softwares* na plataforma Android.
Fonte: Elaborado pelo autor (2013).

Através da Figura 39 (verificar apêndice B), ficou evidente que os dois *softwares* de recuperação são muitos semelhantes. Um ponto positivo foi que, caso o usuário não possua “root” em seu *smartphone,* ele poderá utilizar o software Remo Recover for Android, uma vez que o Undelete é específico para celulares e funciona somente no celular. Já o Remo é instalado no Windows.

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 texto foi considerada boa, uma vez que ambos os *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.

Também foi elaborado outro quadro comparativo demonstrando especificamente o número de arquivos recuperados por cada *software* na plataforma Linux.

Recuperação de Arquivos na Plataforma Linux.

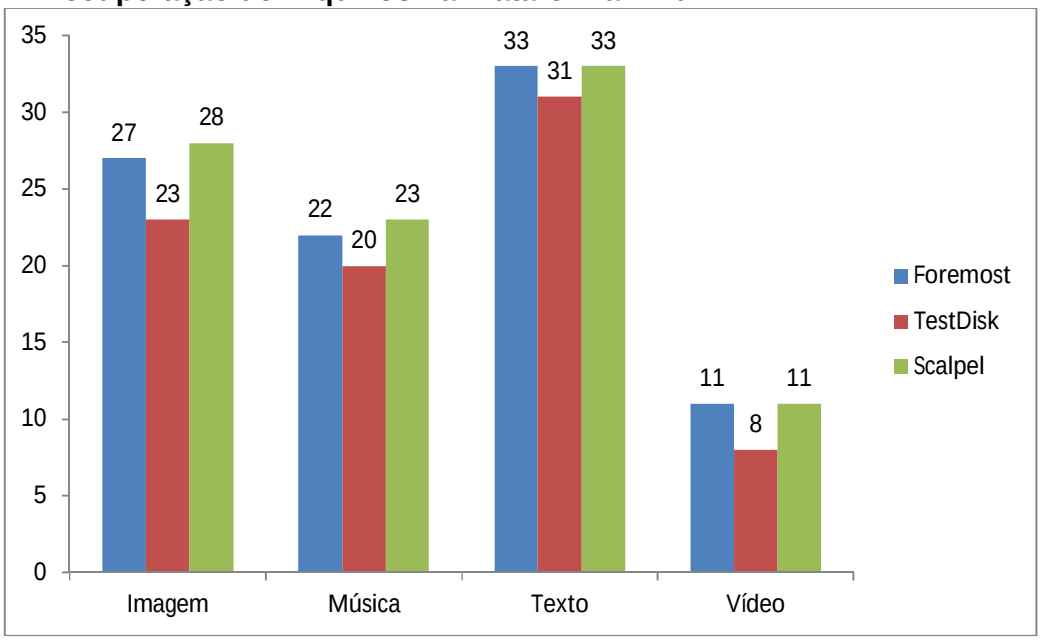

Figura 40 – Resultados comparativos entre os *softwares* na plataforma Linux.
Fonte: Elaborado pelo autor (2013).

Conforme ilustra a Figura 40 (verificar apêndice B), o *software* TestDisk obteve o pior desempenho de recuperação entre os outros programas na plataforma Linux, a recuperação de vídeos foi abaixo do esperado, pois nem existiu a recuperação dos mesmos, com tamanho inferior a 10Mb.

Os softwares TestDisk e Foresmot realizaram uma recuperação parecida. Por se tratar de um *software* derivado do Foremost e mais atualizado, o Scalpel obteve desempenhos melhores na recuperação de imagens e músicas.

O tempo gasto por cada software indica a mesma análise feita nas duas outras plataformas, quanto mais tempo gasto na localização dos arquivos, maior será o número de arquivos recuperados.

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

Comparativo de Recuperação entre as plataformas Windows, Linux e Android.

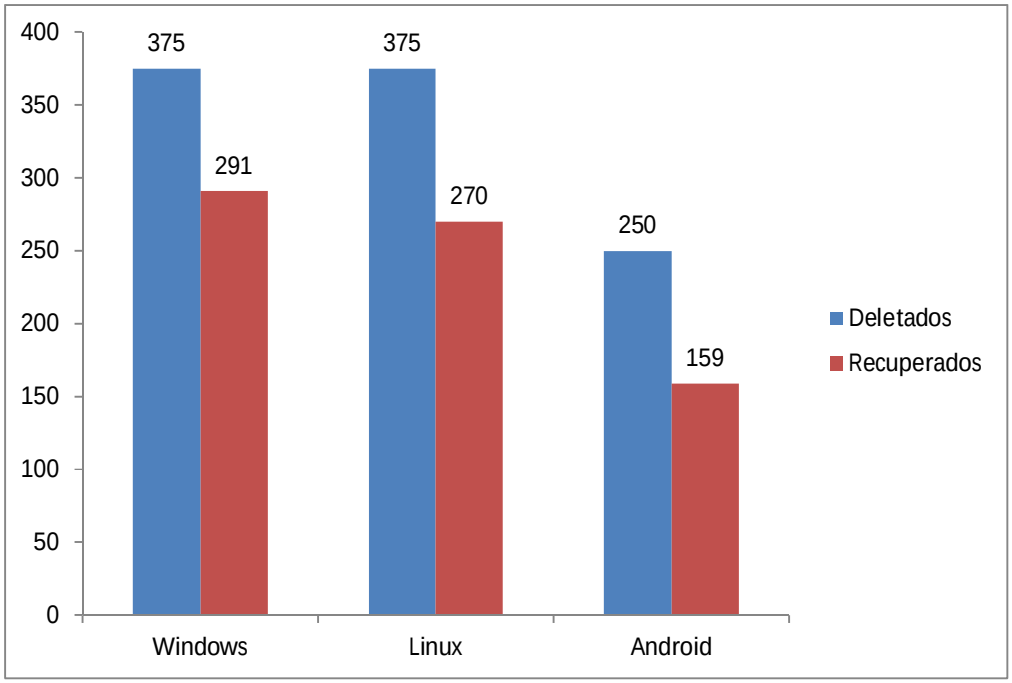

Figura 41 – Resultados comparativos entre os sistemas operacionais.
Fonte: Elaborado pelo autor (2013).

Analisando a Figura 41 (verificar apêndice C), foi constatado que o sistema operacional com mais arquivos recuperados foi o Windows; isso se deve ao fato de que os *softwares* desta plataforma realizam uma busca mais demorada pelos arquivos deletados.

Comparados os S.O. Android e Linux, a diferença na recuperação não foi tão grande, uma vez que a análise no Android utilizou somente dois *softwares* e o Linux utilizou-se de três.

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 por tipo de arquivos.

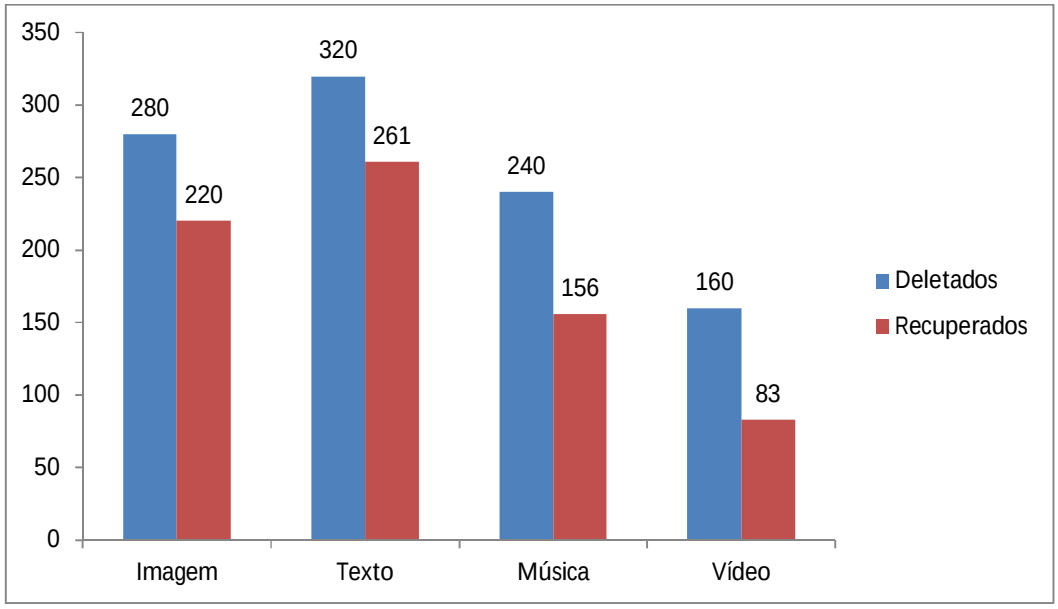

Figura 42 – Resultados comparativos entre os sistemas operacionais.
Fonte: Elaborado pelo autor (2013).

Um último quadro foi elaborado conforme ilustra a Figura 42, (verificar apêndice D) com a intenção de demonstrar 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 texto (.pdf e .doc); isso ocorreu por eles possuírem menos tamanho do que os outros arquivos, embora arquivos que possuam tamanho superior a 10Mb ficam recuperados parcialmente, ou nem mesmo são encontrados para uma possível recuperação.

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 imagens 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 músicas sofrem problemas semelhantes aos de vídeos, músicas muito grandes não são listadas e sua recuperação fica inviável, embora uma quantidade aceitável tenha sido recuperada.

7 CONSIDERAÇÕES FINAIS

Considerando a grande quantidade de arquivos utilizados por uma única pessoa nos dias de hoje, fica indispensável a utilização de técnicas de perícia forense computacional na recuperação de arquivos, uma vez que a possibilidade de roubo ou perda de informações se torna cada vez maior.

Nesse sentido muitas ferramentas são desenvolvidas atualmente com a finalidade de recuperação de arquivos perdidos e/ou deletados, tanto para uso pessoal quanto corporativo. A perícia forense fica cada vez mais evidente no mercado devido a estes fatos, e cada vez mais se precisa de *softwares* com estas funções.

Com esse intuito, foram usadas algumas dessas ferramentas, em três sistemas operacionais utilizados no dia-a-dia de muitas pessoas, sendo Windows, Android e Linux.

As ferramentas foram testadas cada uma em seu sistema operacional. Um detalhe interessante fica para a plataforma Android e os dois *softwares* testados. Um deles, o Remo Recover For Android, deve ser instalado na plataforma Windows para realizar a recuperação de arquivos em *smartphones* com sistemas operacionais Android; entretanto, esta ferramenta só realiza recuperação em celulares, pois um *pen drive* ou Hd externo foi plugado no computador e o *software* nem mesmo reconheceu os dispositivos.

O *software* que apresentou maior desempenho foi o Active@ File Recovery, da plataforma Windows. O mesmo possui funções diferenciadas e uma grande capacidade de recuperação, porém o tempo necessário para a realização por arquivos deletados é grande; nos testes feitos foi de aproximadamente 20 minutos, entretanto o tempo compensa.

Como segunda melhor performance ficou o DiskDigger, o qual de 125 arquivos deletados recuperou 100, confirmando um excelente desempenho. Ficando muito abaixo da média o *software* Recuva recuperou somente 83 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 9 minutos para realizar a checagem por arquivos deletados, confrontando diretamente com o Active@ File Recovery, que demorou 20 minutos e recuperou 108 arquivos.

No caso, as ferramentas utilizadas no ambiente Windows se saíram melhor do que as demais ferramentas. Talvez isso se deve ao fato de que o pen drive e Hd externo utilizados nos testes possuírem seu sistema de arquivos em NTFS, um sistema de arquivos utilizados pelo Windows.

O desempenho 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.

Um ponto observado é a dificuldade que se tem em remover por completo algum arquivo, tornando seu acesso ou recuperação praticamente impossível até mesmo por profissionais nesse quesito, pois existem cada vez mais ferramentas sofisticadas para tal finalidade. Nesse sentido pode-se realizar uma pesquisa futura com possibilidade de análise.

Também em projetos futuros, seria interessante a utilização e pesquisa de técnicas forenses em busca de arquivos deletados em outras plataformas, como Windows Mobile (Phone), Symbian, Mac OSC (iPhones), BlackBerry, Palm webOS, uma vez que a quantidade de plataformas só aumenta.

REFERÊNCIAS

ACTIVE @FILE RECOVERY. Data Recovery Tool, Even if your Sistem is not Bootable. 2013. Disponível em: <h http://www.file-recovery.com/>. Acesso em: 11 set. 2013.

ALMEIDA R. Q. Linhadecódigo. Infra – Linux. 2013. Disponível em: <http://www.linhadecodigo.com.br/artigo/2968/foremost-e-scalpel-recuperacao-de-arquivos.aspx >. Acesso em: 12 set. 2013.

ANDROID, 2013 em: **Wikipédia: a enciclopédia livre**. Disponível em: < http://pt.wikipedia.org/wiki/Android> Acesso em: 01 mai. 2013.

ANDROID (c2013b). **Touch Devices.** Disponível em: <http://source.android.com/tech/input/touch-devices.html>. Acesso em: 18 maio 2013.

ASSOCIANTION OF CHIEF POLICE OFFICERS. **Good Practice Guide for Computer-Based Electronic Evidence**. Versão 4.0. [S.1.]. 2008.

BARBOSA, Alessandro de Sá. **Avaliação Preliminar dos Níveis de Maturidade dos Controles de Segurança da Informação e Comunicação em Organizações Militares do Exército Brasileiro, de acordo com a Norma ABNT NBR ISSO/IEC 27002:2005.** Brasília: UNB, 2009. p.5-17.

BÖGER, D.; JUNIOR, R. B. **Segurança da informação***,* 2008*.* Disponível em: < http://www.das.ufsc.br/~dsboger/aula/07_1/ine5329-administracao_em_processamento_de_dados/transparencias_seguranca.pdf> Acesso em: 10 abr. 2013.

BURNETTE, E. Hello, Android. [S.I.]: Pragmatic Bookshelf, 2008. ISBN 978-1-934356-17-3.

COSTA, Daniel Moraes. **Boas práticas para perícia forense**. 2008. Disponível em: < http://bibdig.poliseducacional.com.br/document/?view=174>. Acesso em: 5 abr. 2013.

COSTA, Marcelo Antonio Sampaio Lemos. **Computação Forense: Curso de Introdução às perícias dos crimes de informática**. 2005.

DISKDIGGER – Undelete and recover photos, documents, music, videos, and more! 2013. Disponível em:< http://diskdigger.org/ >
Acesso em: 10 set. 2013

FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional: teoria e prática aplicada***.* São Paulo: Pearson Prentice Hall, 2007. 190 p.

FERREIRA, Aurélio Buarque de Holanda. **Novo dicionário da língua portuguesa.** 3ed.rev. e atual. São Paulo: Nova Fronteira, 2009.

FONTES, E. **Segurança da Informação; o usuário faz a diferença.** São Paulo: Saraiva, 2006.

FOREMOST. 2013. Disponível em:< http://foremost.sourceforge.net// >
Acesso em: 11 set. 2013

FREITAS, Andrey Rodrigues de. **Perícia forense aplicada à informática: ambiente Microsoft**. Rio de Janeiro: Brasport, 2006.
Disponível em: < http://books.google.com.br/books?hl=pt-BR&lr=&id=HT-MhC3RxR0C&oi=fnd&pg=PA1&dq=pericia+forense+computacional&ots=ZyDVF8Z0LO&sig=aguv2D2jjnhWZXkZzTa6CLsxtzw#v=onepage&q&f=false> Acesso em: 01 mai. 2013.

GIL, A. C. Como Elaborar Projetos de Pesquisa. 5. Ed. São Paulo: Atlas, 2010.

GOOGLE INC. **Android Fundamentals**. Android Developers, 2011. Disponível em: <http://developer.android.com/guide/topisc/fundamentals.html>.Acesso em 10 mai. 2013.

GOOGLE PLAY. Undelete for Root. 2013. Disponível em: <https://play.google.com/store/apps/details?id=fahrbot.apps.undelete&hl=pt_BR>.Acesso em 12 set. 2013.

HAMMERSCHMIDT, R. Remo Recover for Android. 2013. Disponível em: < http://www.baixaki.com.br/download/remo-recover-for-android.htm>. Acesso em 12 set. 2013.

KARASINSKI, L. COMO FAZER ROOT NO SEU CELULAR ANDROID, 2012 em: **Tecmundo**. Disponível em: < http://www.tecmundo.com.br/android/18863-como-fazer-root-no-seu-celular-com-android-video-.htm> Acesso em: 23 out. 2013.

JULIEN, B. **Recuperação de dados forenses.** 2012**.** Disponível em:< http://www.virtualbroker.org/recuperacao-de-dados-forenses.html> Acesso em: 20 de mai. 2013.

LAUDON, Kenneth C., LAUDON, Jane Price. **Sistema da Informação com Internet**. 1999. 4 p.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Informação.** Rio de Janeiro: Ciência Moderna Ltda., 2008. 253 p.

MICROSOSOFT WINDOWS, 2013 em: **Wikipédia: a enciclopédia livre**. Disponível em: < http://pt.wikipedia.org/wiki/Microsoft_Windows> Acesso em: 01 jun. 2013.

MIGUEL, Fabio. **Computadores, Internet e Celular – A Evolução**. 2010. Disponível em: <http://deixapensar.wordpress.com/2010/11/05/computadores-internet-celular-evolucao/>. Acesso em 04 mar. 2013.

MORIMOTO, Carlos E. **Linux: guia prático**. Porto Alegre: Meridional, 2009.

NARDUCI, M. P. Recuva. 2013. Disponível em:< http://www.baixaki.com.br/download/recuva.htm> Acesso em: 10 de set. 2013.

OPEN HANDSET ALLIANCE. **Industry Leaders Announce Open Platform for Mobile Devices.** Disponível em: <http://www.openhandsetalliance.com/press_110507.html>. Acesso em: 18 maio 2013.

PARSONS, J. J.; OJA, D. **Computer Concepts**. 9th ed. Boston: Cengage Learning, 2012. 240 p.

PEIXOTO, M. C. P. **Engenharia social & segurança da informação na gestão corporativa.** Rio de Janeiro: Brasport, 2006.

PIMENTA, Flávio. **Perícia forense computacional baseada em sistema operacional Windows XP Professional**, 2007. Disponível em: < http://pt.scribd.com/doc/53984415/103/CONCLUSAO> Acesso em: 10 abr. 2013.

QUEIROZ, Claudenir; VARGAS, Raffael. **Investigação e Perícia Forense Computacional.** Brasport, 2010.

Represália de ex-funcionário lidera lista de riscos. **Ernest & Young Terco**, 2010. Disponível em: <http://www.ey.com/BR/pt/Issues/Managing-risk/Information-security-and-privacy> Acesso em: 15 mar. 2013.

ROCHA, Anderson de Rezende; GOLDENSTE IN. Siome Klein. **Computação Forense**. Instituto de Computação. UNICAMP. 2008. Disponível em: < http://www.ic.unicamp.br/pos/computacao-forense> Acesso em: 10 mai. 2013.

ROOT – O QUE É, PARA QUE SERVE E COMO FAZER, 2013 em: **Superdownloads**. Disponível em: < http://www.superdownloads.com.br/materias/root-que-que-serve.html> Acesso em: 23 out. 2013.

SIMÃO, A. ***Proposta de método para análise pericial em smartphone com sistema operacional android***. 2011. 110 f. Tese (Mestrado em Engenharia Elétrica) – Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília. 2011.

SISTEMA DE INFORMAÇÃO, 2013 em: **Wikipédia: a enciclopédia livre**. Disponível em: < http://pt.wikipedia.org/wiki/Sistema_de_informa%C3%A7%C3%A3o> Acesso em: 03 jun. 2013.

SERRA, J. Paulo. **Manual de Teoria da Comunicação**. Covilhã: Livros Labcom, 2007.

SMARTPHONE, 2013 em: **Wikipédia: a enciclopédia livre**. Disponível em: < http://pt.wikipedia.org/wiki/Microsoft_Windows> Acesso em: 15 mai. 2013.

TESTDISK, Tesdisk, Data Recovery. Disponível em: <http://www.cgsecurity.org/wiki/TestDisk> Acesso em: 12 set. 2013

VITAL, Guilherme. **Linha do tempo: a evolução dos celulares**. Tecnoinfo. 2012. Disponível em: < http://atecnoinfo.blogspot.com.br/2012/11/a-evolucao-dos-celulares.html> Acesso em: 25 abr. 2013.

ZHANG, Z. **Antenna Design for Mobile Devices**. Singapore: John Wiley & Sons, 2011. 352 p.

ZHENG, P.; NI, L. **Smart Phone and Next Generation Mobile Computing**. San Francisco: Morgan Kaufmann, 2010. 350 p.

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

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

	Deletados		Recuperados	
Tipo de arquivo	**Fa[5]**	**Fr [6](%)**	**Fa**	**Fr (%)**
Imagem	35	28,00	29	29,00
Música	30	24,00	23	23,00
Texto	40	32,00	35	35,00
Vídeo	20	16,00	13	13,00
Total	125	100,00	100	100,00

Fonte: Elaborada pelo Autor (2013).

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

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	35	28,00	27	32,53
Música	30	24,00	19	22,89
Texto	40	32,00	31	37,35
Vídeo	20	16,00	6	7,23
Total	125	100,00	83	100,00

Fonte: Elaborada pelo Autor (2013).

Tabela 3 - Recuperação de arquivos no Software Active@ File Recovery - Plataforma Windows

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	35	28,00	32	29,63
Música	30	24,00	25	23,15
Texto	40	32,00	36	33,33
Vídeo	20	16,00	15	13,89
Total	125	100,00	108	100,00

Fonte: Elaborada pelo Autor (2013).

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

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	35	28,00	28	33,73
Música	30	24,00	13	15,66
Texto	40	32,00	32	38,55
Vídeo	20	16,00	10	12,05
Total	125	100,00	83	100,00

Fonte: Elaborada pelo Autor (2013).

[5] Fa: Frequência absoluta.
[6] Fr: Frequência relativa. Estas notações aplicam-se a todas as tabelas.

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

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	35	28,00	26	34,21
Música	30	24,00	11	14,47
Texto	40	32,00	30	39,47
Vídeo	20	16,00	9	11,84
Total	125	100,00	76	100,00

Fonte: Elaborada pelo Autor (2013).

Tabela 6 - Recuperação de arquivos no Software Foremost - Plataforma Linux

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	35	28,00	27	29,03
Música	30	24,00	22	23,66
Texto	40	32,00	33	35,48
Vídeo	20	16,00	11	11,83
Total	125	100,00	93	100,00

Fonte: Elaborada pelo Autor (2013).

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

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	35	28,00	23	28,05
Música	30	24,00	20	24,39
Texto	40	32,00	31	37,80
Vídeo	20	16,00	8	9,76
Total	125	100,00	82	100,00

Fonte: Elaborada pelo Autor (2013).

Tabela 8 - Recuperação de arquivos no Software Scalpel - Plataforma Linux

	Deletados		Recuperados	
Tipo de arquivo	**Fa**	**Fr (%)**	**Fa**	**Fr (%)**
Imagem	35	28,00	28	29,47
Música	30	24,00	23	24,21
Texto	40	32,00	33	34,74
Vídeo	20	16,00	11	11,58
Total	125	100,00	95	100,00

Fonte: Elaborada pelo Autor (2013).

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

Tabela 9 - Recuperação de Arquivos na Plataforma Windows.

		DiskDigger		Recuva		Active	
	Deletados	Recuperados		Recuperados		Recuperados	
Tipo de arquivo	Fa	Fa	Fr (%)	Fa	Fr(%)	Fa	Fr(%)
Imagem	35	29	82,86	27	77,14	32	91,43
Música	30	23	76,67	19	63,33	25	83,33
Texto	40	35	87,50	31	77,50	36	90,00
Vídeo	20	13	65,00	6	30,00	15	75,00
Total	125	100		83		108	

Fonte: Elaborada pelo Autor (2013).

Tabela 10 - Recuperação de Arquivos na Plataforma Android.

		Remo Recover		Undelete	
	Deletados	Recuperados		Recuperados	
Tipo de arquivo	Fa	Fa	Fr (%)	Fa	Fr (%)
Imagem	35	28	80,00	26	74,29
Música	30	13	43,33	11	36,67
Texto	40	32	80,00	30	75,00
Vídeo	20	10	50,00	9	45,00
Total	125	83		76	

Fonte: Elaborada pelo Autor (2013).

Tabela 11 - Recuperação de Arquivos na Plataforma Linux.

		Foremost		TestDisk		Scalpel	
	Deletados	Recuperados		Recuperados		Recuperados	
Tipo de arquivo	Fa	Fa	Fr (%)	Fa	Fr (%)	Fa	Fr(%)
Imagem	35	27	77,14	23	65,71	28	80,00
Música	30	22	73,33	20	66,67	23	76,67
Texto	40	33	82,50	31	77,50	33	82,50
Vídeo	20	11	55,00	8	40,00	11	55,00
Total	125	93		82		95	

Fonte: Elaborada pelo Autor (2013).

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

Tabela 12 - Comparativo de Recuperação entre as plataformas.

	Deletados	Recuperados	
Plataforma	**Fa**	**Fa**	**Fr(%)**
Windows	375	291	77,60
Linux	375	270	72,00
Android	250	159	63,60
Total	1000	720	

Fonte: Elaborada pelo Autor (2013).

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

Tabela 13 - Recuperação de por tipo de arquivos

	Deletados	Recuperados	
Tipo de arquivo	**Fa**	**Fa**	**Fr (%)**
Imagem	280	220	78,57
Texto	320	261	81,56
Música	240	156	65,00
Vídeo	160	83	51,88
Total	1000	720	

Fonte: Elaborada pelo Autor (2013).

Perícia Forense Computacional Aplicada a Smartphones

Raphael P. Afonso, Elvio G. da Silva, Henrique P. Martins. Patrick P. Silva.

Centro de Ciências Exatas e Sociais Aplicadas - Universidade Sagrado Coração (USC) – Bauru – SP – Brasil

raphael.afonso9@gmail.com, {egsilva, henrique.martins, patrick.silva}@usc.br

Abstract. *Due to the increasing technology development, the Internet has become one of the main communication tools. Besides, there are all kind of services related to it, such as online bill payment, on-line stores, social network communication etc. However, such convenience can bring big problems in the future for both home and corporate users since criminals have been hacking such devices more frequently. One of the threats and major concerns in Information Technology that can put the information security at risk is the data loss or stealing by criminals, putting companies, individuals, and organization security at risk. Along with the Internet expansion, computers and others electronic devices are being used to commit cyber crimes. Thus, digital evidence has been used very often in cybercrimes. Thus, the use of electronic evidence is increasingly involved in cybercrime. Based on this context, this paper analyzed computer forensic software's and techniques to recover deleted files in storage and smartphones with Android operating system devices . The results demonstrated the ability of each software based on tests.*

Resumo. *Com o crescente avanço da tecnologia, a Internet tem se tornado uma das principais ferramentas de comunicação. Vinculada a ela estão todos os tipos de serviços, tais como: pagamentos de contas online, compras em sites, comunicação em redes sociais, entre outros. Para que isso seja possível, faz-se o uso de computadores, tablets e smartphones. Porém, esta facilidade pode gerar grandes complicações futuras, tanto para usuários domésticos ou corporativos, uma vez que tem se tornado frequente a invasão de tais dispositivos por criminosos. Uma das ameaças que podem colocar em risco a segurança da informação, e uma das grandes preocupações em TI, é a perda de dados ou sua subtração por criminosos, colocando em risco a segurança das empresas, organizações e indivíduos. Com a expansão da Internet, computadores e outros dispositivos eletrônicos estão sendo usados para cometer crimes digitais. Com isso, o uso de provas eletrônicas está cada vez mais envolvido em crimes digitais. Com base neste contexto este trabalho analisou técnicas e softwares de perícia forense computacional, para recuperação de arquivos deletados em dispositivos de armazenamento e smartphones, com sistema operacional Android. Os resultados demonstraram a capacidade de cada software com base nos testes realizados.*

1. Introdução

Na década de 1990, os computadores mal ocupavam espaço no âmbito corporativo, porém ninguém imaginaria que um dia teríamos um em casa e muitos menos no bolso. Nessa época, os computadores eram artigos de luxo e só eram utilizados por empreendimentos que podiam bancar o alto investimento. A tecnologia também evoluiu em outros setores e nos últimos 10 anos, os celulares que antes eram verdadeiros itens de luxo tornaram-se mais um item do dia a dia de cada um.

Atualmente, devido ao grande uso dos computadores, cada vez mais o ser humano depende deles. Esta dependência trazida pelas facilidades que os computadores nos trouxeram pode parecer inofensiva, mas basta um simples problema de ordem técnica e uma instituição pode estar arruinada por completo, caso não esteja preparada para a situação.

Uma das ameaças que podem colocar em risco a segurança da informação, e uma das grandes preocupações em TI, é a perda de dados ou sua subtração por criminosos, colocando em risco a segurança das empresas, organizações e indivíduos. Os celulares entraram na lista dos equipamentos utlizados para roubos de informações, invasões, ataque de vírus, entre outros crimes ligados à informática. Atualmente, o mercado de celulares evolui absurdamente e, hoje, têm-se os smartphones.

Assim, a análise pericial nesse tipo de dispositivo pode trazer informações a respeito do seu usuário, devido ao fato de que funcionalidades como: armazenamento de arquivos, histórico de Internet, agenda, contatos, e até mesmo acesso em aplicativos de computação em nuvem, estarão disponíveis no smartphone. Alguns procedimentos devem ser seguidos pelo perito para assegurar que a evidência não seja comprometida, substituída ou perdida.

A Perícia Forense na área computacional inclui análise de mídias, por exemplo, HDs, discos ópticos, *pen drives*, discos SSD, memória RAM etc. Buscando arquivos e conteúdo específico associado a algum tipo de crime digital, tal procedimento utiliza *hardware* e *software* que podem acessar essas mídias sem modificar ou alterar seu conteúdo na procura de evidências para esclarecer um crime digital, podendo ser um roubo, troca de mensagens, alteração de arquivos, cópia não autorizadas de informações sigilosas, compartilhamento de arquivos proibidos (pornografia infantil), acesso não autorizado entre outros.

Os profissionais na área têm regras a seguir, providências definidas a tomar, para que obtenham credibilidade no que fazem; artigos específicos sobre como um capacitado deve proceder em uma investigação para que seu trabalho não tenha sido em vão e desconsiderado em uma audiência judicial, na qual um parecer técnico será necessário.

Com base neste contexto, este estudo tem por finalidade realizar um comparativo entre as ferramentas utilizadas na recuperação de arquivos de um dispositivo de armazenamento e em celulares *smartphones*.

2. Metodologia

O propósito das pesquisas exploratórias é proporcionar ao investigador maior familiaridade com o problema, objetivando torná-lo mais explícito ou construir hipótese. Uma pesquisa de cunho exploratório tende a ser bastante flexível, pois leva em consideração os mais variados aspectos relativos ao problema estudado. De modo geral, pesquisas realizadas com propósitos acadêmicos, pelo menos inicialmente, assumem esse caráter exploratório, pois neste momento

é pouco provável que o pesquisador tenha uma definição clara do que irá investigar (GIL, 2010).

A produção deste trabalho exibe uma série de etapas que devem ser seguidas até a obtenção dos resultados, que são a recuperação de arquivos deletados. Considerando a natureza delicada de se realizar uma série de operações em *notebooks*, *smartphones* e computadores particulares ou corporativos, um planejamento deve ser realizado e etapas devem ser seguidas para que evidências não sejam perdidas ou invalidadas posteriormente.

Dessa forma, o projeto é inicialmente uma pesquisa exploratória, pois visa estudar técnicas forenses para recuperação de dados em dispositivos de armazenamento e *smartphones*, visando pesquisar e produzir um levantamento de técnicas para análise pericial em *smartphones* Android.

De início, foi produzida uma pesquisa abordando celulares e sua evolução, para posteriormente chegar-se aos *smartphones*, a tecnologia mais atual em quesito de telefonia móvel.

Um breve relato sobre os sistemas operacionais Windows, Linux e Android também foi elaborado, demonstrando brevemente o que é cada um. Esta etapa do trabalho visou ressaltar a importância do sistema operacional para a perícia forense, uma vez que o perito deve possuir um bom conhecimento perante o sistema que irá trabalhar.

Um capítulo sobre informação e segurança da informação foi descrito, tendo o propósito de explicar como os ataques a computadores ocorrem e como obter uma politica de segurança eficaz contra os mesmos. Técnicas como criptografia e esteganografia estão presentes para fornecer um conhecimento básico sobre como
s, textos e arquivos podem ser mascarados.

Visando demonstrar onde a área de perícia forense e suas aplicações em *smartphones* podem estar presentes, um capítulo sobre seus conceitos e técnicas foi escrito.

Dentro do campo da perícia forense computacional, peritos devem saber como agir, quais os passos a seguir para que nenhum dano ao equipamento utilizado ocorra. Neste âmbito, o trabalho visa deixar claros os passos para preservar o material encontrado sob suspeita do crime e o que fazer com o mesmo.

Para atingir os objetivos deste trabalho, os seguintes *softwares* foram utilizados neste trabalho: Recuva, DiskDigger e Active@ File Recovery para Windows; para Linux: Foremost, Scalpel e TestDisk. Já para o Android: Remo Recover for Android e Undelete. Os mesmos foram escolhidos por serem gratuitos e de fácil localização em sistemas de buscas, com exceção do Active@ File Recovery, que é pago.

O desenvolvimento do tema proposto ocorreu inicialmente em um ambiente planejado, utilizando-se para os testes de recuperação de arquivos, um computador *desktop* com as seguintes configurações:

- MS Windows 7 Ultimate 32-bits
- Intel Pentium Dual CPU E2180 @2.00Ghz
- 3,00GB RAM
- Intel 82945G Express Chipset Family

E um *notebook* com as configurações listadas abaixo:

- MS Windows 7 Ultimate 32-bits
- Intel Core i5-321M CPU @2.50GHZ
- 8,00GB RAM

- Intel HD Graphics 4000

Para a realização dos testes no sistema operacional Linux, o mesmo foi virtualizado no ambiente Windows pelo *software* "VirtualBox 4.3.2 for Windows hosts, x86/amd64". O sistema Linux utilizado foi o Ubuntu 13.10.

Os testes foram realizados nos três objetos descritos a seguir: *pen drive (32Gb), HD* Externo (200Gb) *e smartphone (32Gb),* estes por sua vez foram separados para utilização conforme ilustra a Figura 1.

Tipo de arquivos	Quantidade	Extensão
Músicas	30	.mp3
Imagens	35	.jpeg
Textos	40	.doc e .pdf
Vídeos	20	.mp4

Figura 1. Arquivos utilizados nos testes.
Fonte: Elaborado pelo autor (2013).

Deste modo os três dispositivos continham 125 arquivos diversos e 4 pastas. Após os arquivos serem inseridos, o p*en drive* e HD Externo foram formatados para na sequência utilizar-se dos *softwares* de recuperação de arquivos.

Os testes no *smartphone* ocorreram com a anexação dos arquivos no cartão de memória do dispositivo móvel, após isto foi dado inicio aos testes, de duas maneiras diferentes. A primeira os arquivos foram recuperados por um *software* projetado para computador (*Windows* 7), já na segunda, o *software* foi projetado para rodar diretamente no *smartphone*.

Neste âmbito, os *softwares* utilizados na recuperação de arquivos foram:

DiskDigger (Windows): *software* gratuito capaz de realizar uma varredura completa em seus discos de armazenamento internos e externos na busca de arquivos excluídos na tentativa de recuperá-los. O aplicativo faz uma busca minuciosa em todos os setores do seu HD, podendo também vasculhar a memória de pen drives, câmeras e outros aparelhos conectados ao PC. A Figura 2 ilustra o processo de recuperação do programa.

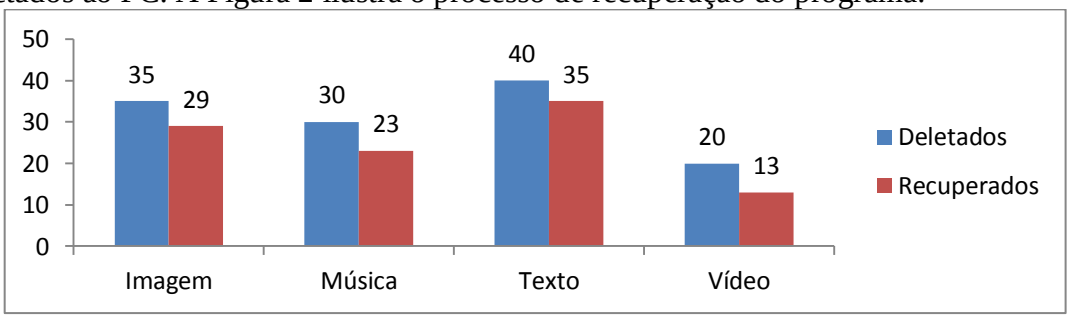

Figura 2. Resultados obtidos pelo software: DiskDigger.
Fonte: Elaborado pelo autor (2013).

Recuva (Windows): *software* gratuito e oferece uma forma fácil de recuperação de arquivos apagados do disco rígido, *pen drive*, câmeras digitais, cartão de memória, HD Externo, entre outros. O Recuva funciona até mesmo com discos rígidos formatados, a Figura 3 ilustra os resultados obtidos pelo Recuva.

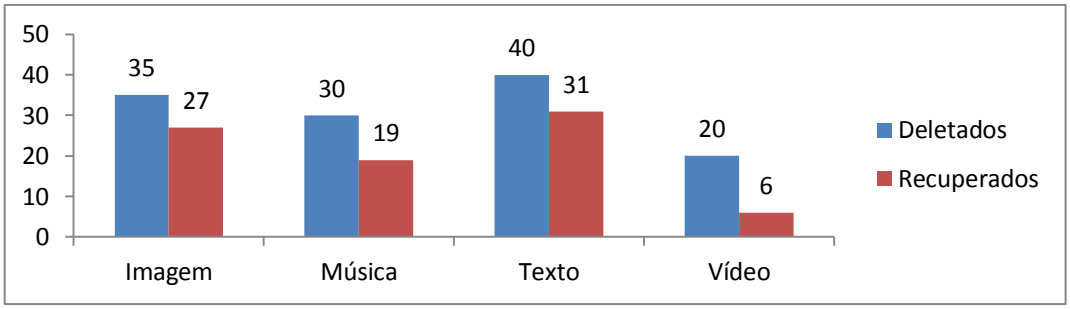

Figura 3. Resultados obtidos pelo *software*: Recuva.
Fonte: Elaborado pelo autor (2013).

Active@ File Recovery (Windows): O *software* pode ser utilizado para recuperar discos rígidos IDE, SATA, SATA II e SCSI, disquetes e outras mídias (CompactFlash, SmartMedia, Sony MemoryStick, USB Hard Drive, USB Flash Memory), ele pesquisa o HD em busca dos arquivos apagados e exibe todos em uma lista. A quantidade de arquivos recuperados pelo *software* é ilustrada na Figura 4.

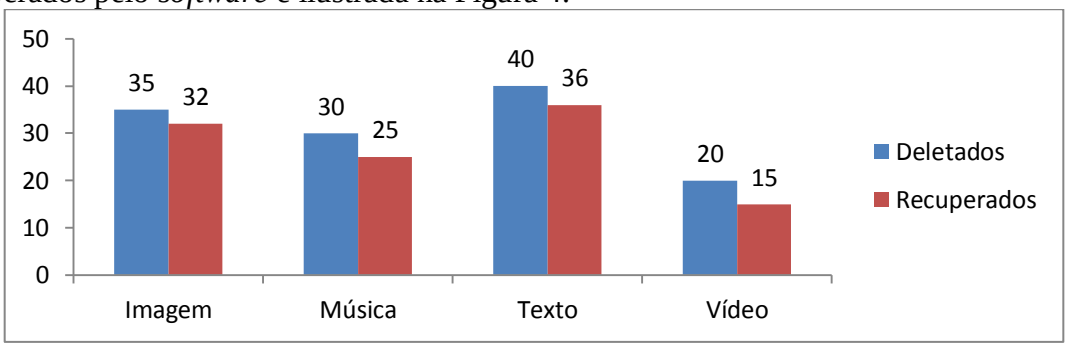

Figura 4. Resultados obtidos pelo *software*: Active@ File Recovery.
Fonte: Elaborado pelo autor (2013).

Remo Recover for Android (Android): Aplicativo cuja função é recuperar arquivos perdidos, que foram apagados acidentalmente em *smartphones* com SO da Google (Android). Além disso, ele restaura os dados após uma formatação de cartão SD, tais como arquivos APK, músicas, vídeos e imagens. A Figura 5 exibe a quantidade de arquivos recuperados.

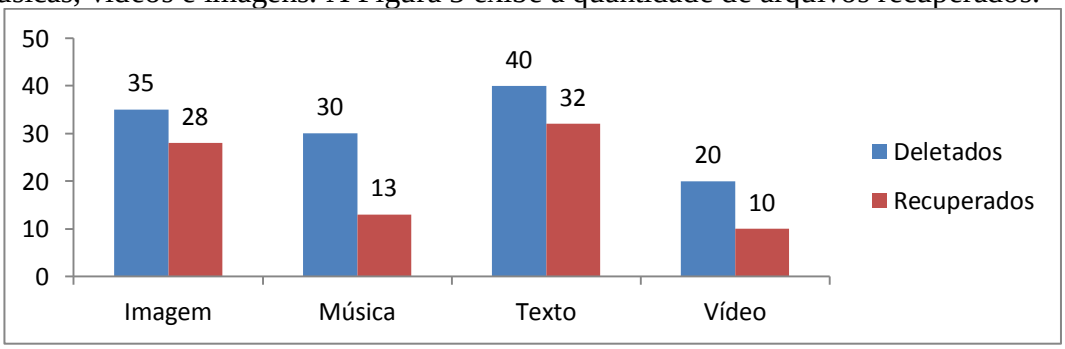

Figura 5. Resultados obtidos pelo *software*: Remo Recover for Android.
Fonte: Elaborado pelo autor (2013).

Undelete (Android): é um aplicativo para a plataforma Android, que permite recuperar qualquer tipo de arquivo que foi excluído do cartão SD ou armazenamento interno do *smartphone*. A quantidade de arquivos recuperados é ilustrada na Figura 6.

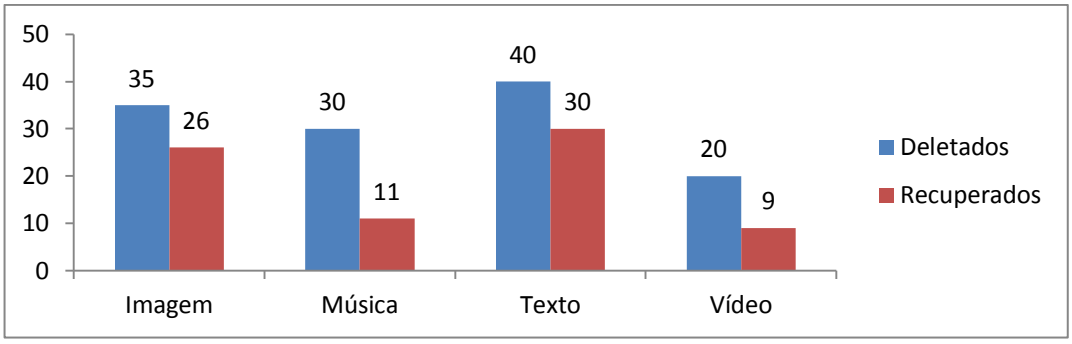

Figura 6. Resultados obtidos pelo *software*: Undelete.
Fonte: Elaborado pelo autor (2013).

Scalpel: é um recuperador de arquivos, de alto desempenho, que lê um banco de dados de definições de cabeçalho e rodapé e extrai os arquivos desejados de um conjunto de arquivos de imagem ou dispositivos raw. A Figura 7 exibe a quantidade de arquivos recuperados no Scalpel.

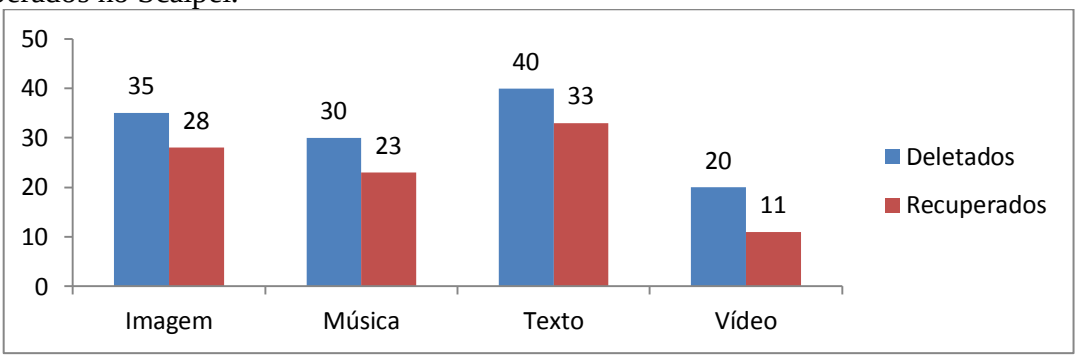

Figura 7. Resultados obtidos pelo *software*: Scalpel.
Fonte: Elaborado pelo autor (2013).

Foremost: *Software* de console utilizado para recuperar arquivos com base em seus cabeçalhos, rodapés e estruturas de dados internas. O *software* permite trabalhar em arquivos de imagem gerados por softwares de pericia forense, como dd, Safeback, Encase, etc. Ferramenta livre para qualquer sistema Linux. A Figura 8 ilustra a recuperação dos arquivos.

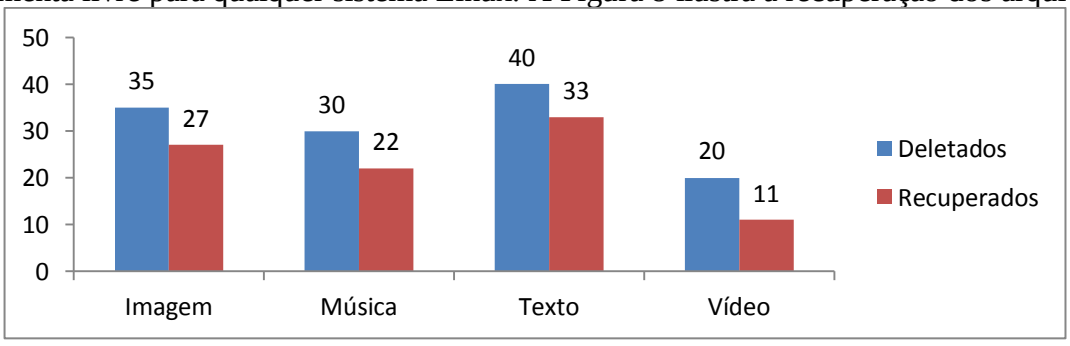

Figura 8. Resultados obtidos pelo *software*: Foremost.
Fonte: Elaborado pelo autor (2013).

TestDisk: utilidades do TestDisk, corrigir a tabela de partição, recuperar partição apagada; recuperar o setor de inicialização FAT32 do seu *backup*; reconstruir o setor de *boot*; corrigir tabelas FAT; restaurar arquivos do FAT, exFAT, NTFS, ext2 *filesystem*, FAT16, FAT32, EXT3, ReiserFS, XFS, LVM e Linux Raid. O desempenho do TestDisk nos testes de recuperação de arquivos, é ilustrado na Figura 9.

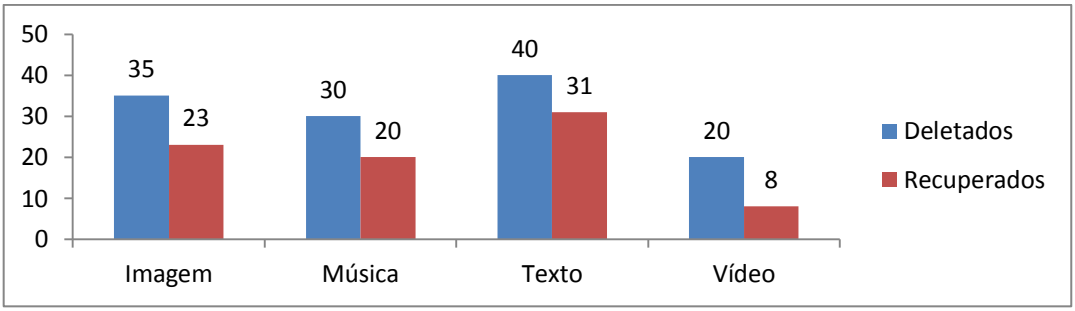

Figura 9. Resultados obtidos pelo *software*: TestDisk.
Fonte: Elaborado pelo autor (2013).

A Figura 10 ilustra a quantidade de arquivos recuperados nas categorias de imagem, texto, música e vídeo.

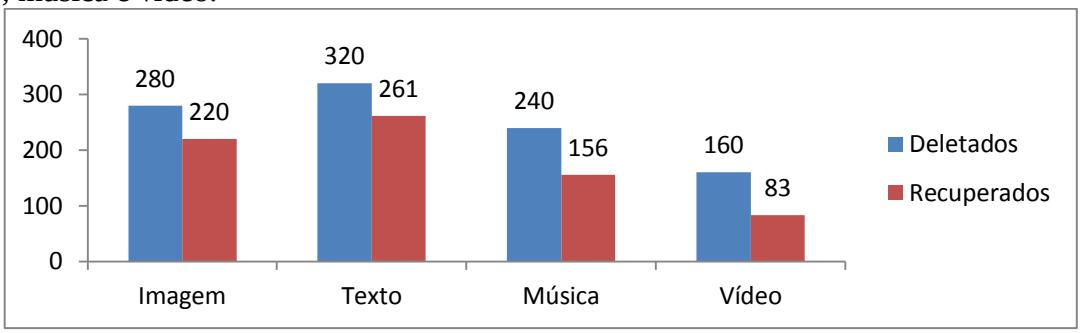

Figura 10. Resultados obtidos pelo *software*: TestDisk.
Fonte: Elaborado pelo autor (2013).

Ficando evidente que os arquivos com mais facilidade para recuperação foram os de texto (.pdf e .doc), isto se deve a eles possuírem menos tamanho do que os outros arquivos, embora arquivos que possuem tamanho superior a 10Mb ficam recuperados parcialmente, ou nem mesmo são encontrados para uma possível recuperação.

Os arquivos de vídeos foram os com 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.

3. Conclusão

Considerando a grande quantidade de arquivos utilizados por uma única pessoa nos dias de hoje, fica indispensável à utilização de técnicas de pericia forense computacional na recuperação de arquivos, uma vez que a possibilidade de roubo ou perda de informações se torna cada vez maior.

Neste sentido muitas ferramentas são desenvolvidas atualmente com a finalidade de recuperação de arquivos perdidos e/ou deletados, tanto para uso pessoal ou corporativo. A perícia forense fica cada vez mais evidente no mercado, devido a estes fatos e cada vez mais precisa de *softwares* com estas funções.

Com este intuito, foram usadas algumas dessas ferramentas, em três sistemas operacionais utilizados no dia-a-dia de muitas pessoas, sendo Windows, Android e Linux.

As ferramentas foram testas cada um em seu sistema operacional, um detalhe interessante fica para a plataforma Android e os dois *softwares* testados, um deles o Remo

Recover For Android deve ser instalado na plataforma Windows para realizar a recuperação de arquivos em *smartphones* com sistemas operacionais Android, entretanto esta ferramenta só realiza recuperação em celulares, um *pen drive* ou Hd externo foi plugado no computador e o *software* nem mesmo reconheceu os dispositivos.

O *software* que apresentou o maior desempenho foi o Active@ File Recovery da plataforma Windows, o mesmo possui funções diferenciadas e uma grande capacidade de recuperação, porém o tempo necessário para a realização por arquivos deletados é grande, nos testes feitos foi de aproximadamente 20 minutos, entretanto o tempo compensa.

Em um segundo momento ficou o DiskDigger, o qual de 125 arquivos deletados recuperou 100, um excelente desempenho, ficando muito a baixo da média o software Recuva recuperou somente 83 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 9 minutos para realizar a checagem por arquivos deletados, confrontando diretamente com o Active@ File Recovery que demorou 20 minutos e recuperou 108 arquivos.

No caso, as ferramentas utilizadas no ambiente Windows se saíram melhor do que as demais ferramentas. Talvez isso se deve ao fato de que o pen drive e Hd externo utilizados nos testes possuírem seu sistema de arquivos em NTFS, um sistema de arquivos utilizados pelo Windows.

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

Um ponto observado é a dificuldade que se tem em remover por completo algum arquivo, tornando seu acesso ou recuperação praticamente impossível até mesmo por profissionais neste quesito, pois existem cada vez mais ferramentas sofisticadas para tal finalidade. Neste sentido pode-se realizar uma pesquisa futura com possibilidade de análise neste sentido.

4. Referências

ANDROID (c2013b). **Touch Devices.** Disponível em: <http://source.android.com/tech/input/touch-devices.html>. Acesso em: 18 maio 2013.

ASSOCIANTION OF CHIEF POLICE OFFICERS. **Good Practice Guide for Computer-Based Electronic Evidence**. Versão 4.0. [S.1.]. 2008.

GIL, A. C. Como Elaborar Projetos de Pesquisa. 5. Ed. São Paulo: Atlas, 2010.

PEIXOTO, M. C. P. **Engenharia social & segurança da informação na gestão corporativa.** Rio de Janeiro: Brasport, 2006.

ROCHA, Anderson de Rezende; GOLDENSTE IN. Siome Klein. **Computação Forense**. Instituto de Computação. UNICAMP. 2008. Disponível em: < http://www.ic.unicamp.br/pos/computacao-forense> Acesso em: 10 mai. 2013.

SIMÃO, A. ***Proposta de método para análise pericial em smartphone com sistema operacional android***. 2011. 110 f. Tese (Mestrado em Engenharia Elétrica) – Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília. 2011.