FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

INSEGURANÇA NO DESCARTE DE DISCOS RÍGIDOS

Cleberton Moreno Matoso

Americana, SP

2017

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

INSEGURANÇA NO DESCARTE DE DISCOS RÍGIDOS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso em Segurança da Informação, sob a orientação do Prof.Esp. Marcus Vinicius Lahr

Americana, SP

2017

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

M383i MATOSO, Cleberton Moreno

Insegurança no descarte de discos rígidos./ Cleberton Moreno Matoso. – Americana: 2017.

57f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp.Marcus Vinícius Lahr Giraldi

1. Hardware I. GIRALDI, Marcus Vinícius LahrII. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.31

Cleberton Moreno Matoso

INSEGURANÇA NO DESCARTE DE DISCOS RÍGIDOS

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

Americana, 26 de junho de 2017.

Banca Examinadora:

Marcus Vinicius Lahr Giraldi (Presidente)
Especialista
Fatec Americana

Wagner Siqueira Cavalcante (Membro)
Mestre
Fatec Americana

Paula da Fonte Sanches (Membro)
Mestre
Fatec Americana

RESUMO

Este trabalho tem como finalidade o estudo de recuperação lógica dos dados após a formatação do disco rígido, sendo utilizadas formas diferentes para a exclusão dos dados no disco rígido e utilizando se de ferramentas existentes no mercado para recuperação dos dados, sendo gerada ao fim do trabalho uma matriz de comparação entre softwares e métodos de exclusão.

Palavras Chave: Dados; Recuperação; Formatação

ABSTRACT

This work aims to study the logical recovery of data after formatting the hard disk, using different ways to delete data on the hard disk and using existing tools in the market for data recovery, being generated at the end of the work a comparison matrix between software's and exclusion methods.

Keywords: Data; Recovery; Formatting

SUMÁRIO

LISTA DE FIGURAS E DE TABELAS

INTRODUÇÃO

A Segurança da Informação sustenta-se sobre três pilares: Confidencialidade, Autenticidade e Disponibilidade. A renovação periódica do parque tecnológico garante a alta disponibilidade da informação, porém causam dúvidas quanto ao descarte de equipamentos como: servidores, *laptops, desktops*, pois estes dispositivos guardam em seus discos rígidos informações importantes, as quais, se não forem tratadas corretamente, podem gerar problemas à empresa. No que diz respeito à confidencialidade da informação, isso tem feito com que as empresas destruam os equipamentos que ainda podem ser reutilizados e aumentam a quantidade de lixo eletrônico e os problemas ambientais do planeta.

Esses equipamentos, se tratados corretamente, garantem a confidencialidade das informações. Com base nas normas ISO 27002:2005, em seus itens 9.2.6, "reutilização e alienação segura de equipamentos", e 10.7.2, "descarte de mídias", podem descrever os métodos aplicáveis para esses equipamentos.

Esse trabalho tem como intenção apresentar técnicas disponíveis para o descarte de discos rígidos, tornando possível ou não a reutilização desses equipamentos, determinando métodos de descarte sem comprometer a confidencialidade dos dados que foram armazenados anteriormente. A destruição do disco rígido do computador é eficaz, porém existem outras formas as quais podemos garantir que a informação não seja recuperada e se mantenha a confidencialidade da informação. O reaproveitamento dos equipamentos nas empresas pode gerar lucros financeiros, e uma imagem positiva da empresa.

O autor tentará demonstrar métodos para eliminação dos dados garantindo a confidencialidade, baseando-se nos conhecimentos adquiridos durante o curso de Segurança da Informação.

A pesquisa será baseada em estudo de caso e de procedimentos técnicos comparativos, sendo feita de modo experimental, a fim de exibir com exemplos reais, os resultados dos experimentos, provindos de um laboratório, que simula um ambiente corporativo e que alimentará uma base de dados que irá gerar o conteúdo da pesquisa. Ferramentas existentes foram utilizadas para destruição dos dados e efetuar tentativas de recuperação dos mesmos.

1. SEGURANÇA DA INFORMAÇÃO

Sabe-se que uma empresa bem informada tem vantagens competitivas no mercado e que, como é um ativo precioso, essas informações devem ser bem guardadas, independentemente de onde esta armazenadas, escrita em papel ou digitalmente, com isso a NBR 27002(2005, p. X) complementa, “a informação é um ativo que, como qualquer outro ativo importante é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida”.

Com o avanço tecnológico, as informações se tornam cada vez mais acessíveis, o que gera novas informações, as quais são cada vez mais necessárias para o crescimento e a sustentabilidade de uma empresa, com isso é necessário a preocupação com a sua segurança, como complementam Geus e Nakamura (2007, p. 50): “neste mundo globalizado, onde as informações atravessam fronteiras com velocidade espantosa, a proteção do conhecimento é de vital importância para a sobrevivência das organizações”. Assim também diz a NBR 27002(2005, p. X) “é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio”.

A segurança da informação é formada por três principais pilares, que são:

- Confidencialidade: Garantir que a informação seja acessada somente por aquele que possui autorização para acesso;
- Disponibilidade: a informação deve estar disponível para todos que precisarem dela;
- Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida.
- Além destes três aspectos principais, tem-se:
- Autenticação: garantir que um usuário é de fato quem alega ser;
- Não Repúdio: capacidade do sistema de provar que um usuário executou uma determinada ação;
- Legalidade: garantir que o sistema esteja aderente a legislação pertinente;
- Privacidade: capacidade de um sistema manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações;

- Auditoria: capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque.

1.1 O que é informação

É chamado de informação o processo resultante da analise e manipulação de dados, que, de alguma forma significativa represente, uma modificação ou aumento no conhecimento do sistema na qual esta informação foi inserida.

1.2 Como a informação é armazenada

Conforme a descrição, a informação pode ser armazenada de diversas formas. O cérebro humano pode armazenar informação na forma de conexões de neurônios. Um dos métodos mais efetivos de armazenamento da informação é a escrita, e a partir deste advento, o homem pode registrar seu conhecimento e passá-lo às gerações seguintes.

Com o surgimento da tecnologia e o avento dos computadores, armazenar informação tornou-se um processo essencial para esta ciência, e logo diversos modos foram desenvolvidos e aprimorados, mas todos eles tem como principio o *bit* (*Binary Digit)* a unidade básica de informação que consiste em Zero (0) ou 1 (Um), onde a partir deste principio a informação passou a ser codificada e armazenada digitalmente.

1.3 Discos rígido

A finalidade desse tópico é abordar conceitos sobre discos rígidos, informando a sua origem, história e como é o seu funcionamento físico e lógico, a fim de contribuir para entendimento da pesquisa e dos testes realizados posteriormente.

1.3.1 O que é um disco rígido?

O Disco Rígido é conhecido por vários nomes como: Disco Rígido, HD, *Hard Disk, e Winchester* (termo em desuso), tendo a função de armazenar programas e dados em computadores, como: músicas, vídeos, fotos, textos, além de armazenar o sistema operacional, e aplicativos. Este periférico, diferente da memória *RAM (Random Access Memory),* memória principal do computador, mais rápida, porém volátil, ou seja, suas informações são apagadas quando o computador é desligado, guarda e mantém suas informações gravadas por um longo período, pois a memória do disco rígido é não-volátil, ou seja, mesmo que o computador seja desligado, suas informações permanecem gravadas.

1.3.2 História do Disco Rígido

O disco rígido que é a tecnologia de armazenamentos de dados teve sua produção no inicio dos anos 50. A primeira unidade de armazenamento de grandes quantidades de informação foi criada por engenheiros da IBM, e deram a esta mídia o nome de disquete,conforme figura 1.

Figura 1: Disquete

fonte: http://www.techtudo.com.br/platb/hardware/2011/01/06/evolucao-discos-rigidos-hd/04l/2016

Porém, este dispositivo possuía uma capacidade de armazenamento extremamente limitada pela tecnologia, a não mais que alguns *Megabytes*, sendo necessárias muitas destas unidades para armazenar arquivos grandes

Pensando em como resolver este problema, a IBM, no ano de 1956, criou o computador 305 RAMAC,conforme mostra a figura 2, que vinha com disco interno composto por 50 discos de 24 polegadas, armazenando 5 MB.

Figura 2: Computador 305 RAMAC

fonte: http://www.techtudo.com.br/platb/hardware/2011/01/06/evolucao-discos-rigidos-hd/04/2017

Continuando no processo de desenvolvimento, na década seguinte, a IBM lançou o IBM 3340, com dois discos internos com capacidade de 30 MB cada, o que era revolucionário em termos de tamanho para a época. Este design, de dois discos de 30 MB, foi atribuído, o mesmo nome de um popular rifle, o Winchester 30-30, em sua homenagem, tornando os futuros HDs, também conhecidos por este nome.

Nas décadas seguintes, ainda que os HDs tenham se tornados portáteis, eles ainda eram grandes e desajeitado, mas, apesar disto, cabiam dentro dos gabinetes, exatamente com o mesmo tamanho das baias reservadas aos drives de disquetes de 8”, e 5,25”.

A tendência de mercado incentivou a pesquisa e desenvolvimento de equipamentos que fossem menores e gastassem menos, então empresas como Toshiba, Samsung e ainda IBM atualmente tem discos ultra compactos de ate 0,85”.

As capacidades de armazenamento dos discos chamados convencionais, que usam sistemas de discos, estão na ordem dos 4 TB de armazenamento, porém as

mídias *SSD (Solid-State DiskDrive)* ou disco de estado sólido já ultrapassam com folga esta margem, com cerca de 16 TB de armazenamento.

O principal ponto fraco dos discos rígidos é a utilização de motores e sistema eletromecânicos para realizar o armazenamento e leitura dos dados, fazendo com que o tempo de acesso a eles seja muito maior do que o de mídias *Flash,* por exemplo.

O desempenho dos computadores atuais é limitado principalmente pelo uso de dispositivos eletromecânicos, como motores, por exemplo. O principal exemplo disso é a demora na leitura de uma mídia em *CD (Compact Disc)*. Por este motivo percebeu-se a tendência da eliminação dos dispositivos que contenham estes componentes, e o principal deles é o HDD.

A pesquisa com Disco de estado solida vem com a intenção de substituir permanentemente os HDs convencionais, garantindo menor tempo de acesso aos dados, maior capacidade, menos peso e menor consumo de energia. Tirando o problema de custo que deve ser solucionado com a produção em larga escala, as unidades SSD prometem aposentar os antigos HDs.

1.3.3 Gravação e Leitura dos Dados nos Discos Rígidos

Em um Disco Rígido, os dados são gravados em superfícies magnéticas que recebem o nome de *Platter*, que é composta por uma camada magnética fina. A espessura desta camada determina a sensibilidade e a densidade de dados gravados.

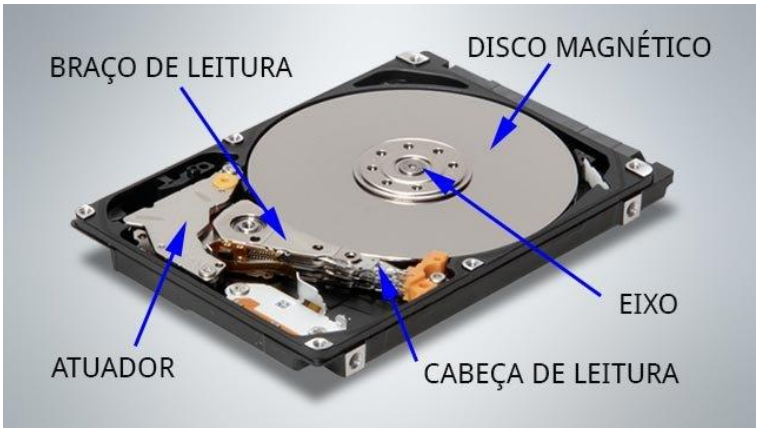
A gravação dos dados é feita pela cabeça de gravação e leitura, que consiste em um eletroímã minúsculo controlado eletronicamente. Esta cabeça grava os dados organizando as moléculas de óxido de ferro presentes na camada de magnetização dos *Platters*, criando trilhas com centésimos de milímetros de espessura. Com a alteração dos pólos, a cabeça de gravação, magnetiza a trilha criando polos positivos ou negativos, que correspondeu aos do tipo 0 (Zero) ou 1 (Um).

Como o sistema de arquivos trabalha com sequência de *bits*, a cabeça de gravação e leitura pode alterar sua polaridade milhões de vez por segundo, de forma definida e com grande precisão.

No processo de leitura, a cabeça detecta a polaridade das moléculas alinhadas, a variação no campo magnético induz uma corrente que é captada pela cabeça de gravação, e levada até a placa lógica do disco rígido e determina qual o *bit* desejado. Quanto maior for a densidade de gravação do disco, menos moléculas precisarão ser magnetizadas, permitindo a criação de mais trilhas e mais setores, mas consequentemente demandam uma cabeça de leitura e gravação mais precisa e sensível.

Esses discos, conforme figura 3, geralmente são fabricados de alumínio cobertos por um material magnético. Os HDDs possuem um ou mais discos magnéticos onde suas informações são gravadas. Podemos encontrar discos rígidos com apenas um disco magnético e outros de alta capacidade com até 8 discos. Os discos rígidos mais comuns em micros *desktop* possuem entre1 e 4 discos internos.

Figura 3: Disco rígido



FONTE: http://www.baboo.com.br/wp-content/uploads/2003/10/HD.jpg 04/2017

A superfície dos discos é dividida em trilhas e setores para organizar o processo de gravação e leitura dos dados gravados no disco rígido. As trilhas são círculos concêntricos, que começam no final do disco e vão se tornando menores conforme se aproximam do centro. Cada trilha recebe um número de

endereçamento, que permite sua localização. A trilha mais externa recebe o número 0 e as seguintes recebem os números 1, 2, 3, e assim por diante. As trilhas se dividem em setores para facilitar ainda mais o acesso aos dados, que são pequenos trechos onde são armazenados os dados, cada setor guarda 512 *bytes* de informações. Um disco rígido atual possui até 900 setores em cada trilha o número varia de acordo com a marca e modelo, possuindo sempre mais de 3000 trilhas.

Para definir onde termina um setor e onde começa o próximo, e o limite entre uma trilha e outra, são usadas marcas de endereçamento, pequenas áreas com um sinal magnético especial, que orientam a cabeça de leitura, permitindo à controladora do disco localizar os dados desejados.

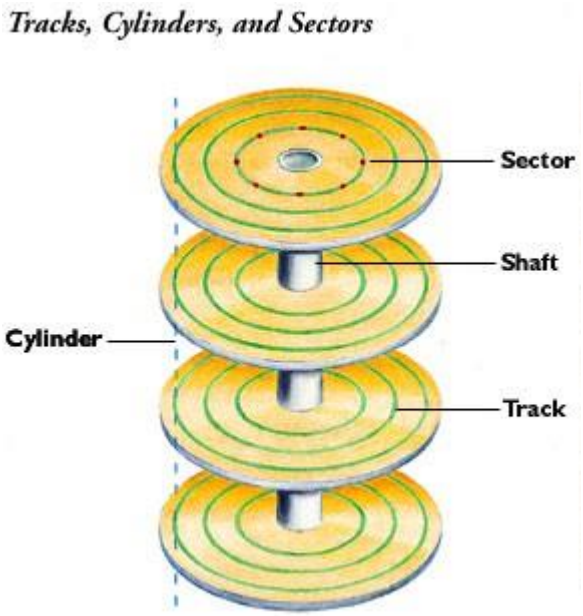
Estas marcas são feitas apenas uma vez em HDs, que é durante a fabricação do disco, e não podendo ser apagadas via software. Existem alguns programas como o Zero Fill, que são utilizados por usuários para regravar as marcas de orientação o que melhoraria a confiabilidade dos discos. Entretanto, a grande maioria dos discos atuais não permite este tipo de regravação, também por que ela não é necessária. Ao rodar estes programas, apesar de ser mostrado um indicador de progresso as trilhas e setores não são regravados, esses softwares servem apenas para identificar onde a setores danificados e demarcarem este setor.

Há também as faces de disco, um HD é formado internamente por vários discos empilhados, sendo o mais comum o uso de 2 ou 3 discos. Em geral, apenas HDs de grande capacidade utilizam 4 ou mais discos, podemos usar os dois lados do disco para gravar dados, cada lado passa então a ser chamado de face. Como uma face é isolada da outra, temos num disco rígido, várias cabeças de leitura, uma para cada face.

As várias cabeças de leitura num disco rígido não se movimentam independentemente, pois são todas presas à mesma peça metálica, chamada braço de leitura que é uma peça triangular, que pode se mover horizontalmente. Para acessar um dado contido na trilha 820 da face de disco 3, por exemplo, a controladora do disco ativa a cabeça de leitura responsável pelo disco 3 e a seguir, ordena ao braço de leitura que se dirija à trilha correspondente. E por esse motivo não é possível que uma cabeça de leitura esteja na trilha 820, ao mesmo tempo em que outra esteja na trilha 2042, por exemplo. Já que todas as cabeças de leitura sempre estarão na mesma trilha de seus respectivos discos, deixamos de chamá-las

de trilhas e passamos a usar o termo "cilindro". Que é o conjunto de trilhas com o mesmo número nos vários discos. Por exemplo, o cilindro 1 é formado pela trilha 1 de cada face de disco, o cilindro 2 é formado pela trilha 2 de cada face, e assim por diante, conforme figura 4.

Figura 4: Trilhas, Cilindros e Setores



Trilhas, setores e cilindros (Cortesia da Quantum)

Fonte: http://www.hardware.com.br/livros/hardware-manual/trilhas-setores-cilindros.html 04/2017

2. FORMATAÇÃO DO DISCO RÍGIDO E FORMAS DE RECUPERAÇÃO DE DADOS.

Para utilizar o disco rígido, primeiro é necessário submetê-lo ao processo de formatação. Formatar significa dividir logicamente o disco em setores endereçáveis, permitindo que os dados possam ser gravados e posteriormente lidos de maneira organizada.

A formatação do disco é um assunto relativamente complicado, tanto que muitas vezes, mesmo profissionais da área têm dúvidas sobre este assunto. A primeira coisa a se compreender sobre isto, é que existem dois tipos de formatação: a formatação física, ou formatação de baixo nível, e a formatação lógica.

2.1 Formatação física

A organização do disco em trilhas, setores e cilindros é necessária para que se possa ler e gravar dados no disco.

Uma formatação de baixo nível, ou formatação física, é a divisão do disco em trilhas, setores e cilindros. Os discos mais antigos, padrão ST-506 e ST-412 que deixaram de ser usados há mais de uma década, sendo substituídos pelos discos padrão *IDE (Integrated Development Environment)* e *SCSI (Small Computer System Interface)*, permitiam que a formatação física fosse feita pelo próprio usuário através do *Setup* da *Bios (Basic Input Output System)*. Estes discos precisavam ser periodicamente reformatados fisicamente. Isso acontecia devido a um problema simples: quando lidos pela cabeça de leitura, os setores do disco esquentavam e se expandiam, esfriando e contraindo-se logo em seguida. Isto alterava a posição das trilhas, causando desalinhamento e dificultando a leitura dos dados pela cabeça magnética, sendo necessária uma nova formatação física para que as trilhas, setores e cilindros, voltassem às suas posições iniciais. Era utilizado um motor de passo para movimentar as cabeças eletromagnéticas que, por não serem completamente precisos, sempre acabavam causando algum desalinhamento.

Os HDs *IDE* e *SCSI*, usados atualmente, já são muito mais complexos que os discos antigos, sendo quase impossível determinar sua disposição de trilhas, setores

e cilindros, impossibilitando uma segunda formatação física. Eles também não possuem o problema de desalinhamento, de modo que, neles, a formatação física é feita somente uma vez na fábrica.

Tentativa indevida de formatar fisicamente um disco moderno simplesmente não surtirá efeito, podendo em alguns casos raros, até mesmo inutilizar o disco. Concluindo, todos os HDs do padrão *IDE* ou *SCSI* não precisam ser formatados fisicamente, não sendo aconselhada qualquer tentativa.

Programas, como *o Es-Tool, Ontrack Disk Manager ou o Maxtor Low Level Format,* são usados por alguns usuários como formatadores físicos. Estes programas são simplesmente ferramentas de diagnóstico e correção de erros, na mesma linha do *Scandisk*, apenas com alguns recursos a mais, que verificam o disco, marcando setores defeituosos, permitindo também visualizar muitos outros erros lógicos no disco e corrigi-los. De qualquer maneira, a ação destes programas é apenas a nível lógico.

Programas antigos, assim como a opção de *Low Level Forma* encontrada no Setup de placas mãe antigas, são destinados a formatar fisicamente os antigos *HDs* padrão *MFM* (*Modified Frequency Modulation*) e *RLL* (*Run Length Limited*). Quando usado em um *HD IDE* ou *SCSI*, este tipo de formatação simplesmente não funciona, quando muito é apagado o *Defect Map que é* o setor de *Boot* do *HD*, desfazendo a formatação lógica do disco e fazendo com que os dados gravados fiquem inacessíveis pelo sistema operacional, no entanto, não é alterada a formatação física.

Um setor danificado é uma pequena falha na superfície magnética do disco rígido, onde não se pode gravar dados com segurança. Estes danos na superfície do *HD* podem surgir devido a algum impacto forte, ou mesmo devido ao desgaste da mídia magnética, o que costuma ocorrer em *HDs* com muito uso. Quando executa-se algum utilitário de diagnóstico do disco rígido, como o *Scandisk*, ou outros softwares de analise de discos, são testados todos os setores do disco rígido, e aqueles que estão danificados são marcados como defeituosos numa área reservada do disco chamada de *Defect Map*, para que não sejam mais utilizados. Os setores danificados são comumente chamados de *bad-blocks*.

Por apresentarem tendência à corrupção dos dados gravados, estes setores são marcados como defeituosos. Tentar apagar o *Defect Map*, faria apenas com que

estes setores fossem novamente vistos como bons pelo sistema operacional. Esta tentativa desesperada não soluciona o problema, simplesmente faria com que as áreas danificadas do disco, antes marcadas, voltem a ser utilizadas, diminuindo a confiabilidade do disco.

2.2 Formatação lógica

A formatação lógica adiciona as estruturas utilizadas pelo sistema operacional. Diferentemente da formatação física, a formatação lógica é feita via software e pode ser refeita quantas vezes forem necessárias, porém deve-se observar que ao se fazer a reformatação das unidades, os dados ficam inacessíveis, mas podem ser recuperados através de ferramentas especificas como pode-se ver mais adiante.

A formatação lógica consiste em duas etapas, sendo a primeira o particionamento do disco, ou seja, a definição do tamanho de cada volume em seu *HD*. Exemplo: Se um *HD* possui 100 GB de espaço pode-se dividi-lo em duas partições de 50 GB, deixando uma para o sistema operacional e outra para armazenamento de dados.

A segunda etapa é a escolha do sistema de arquivos que pode ser definido como o conjunto de estruturas lógicas que permitem ao sistema operacional organizar e otimizar o acesso ao HD. A cada dia a tecnologia avança aumentando a capacidade dos discos e dos volumes de arquivos acessados, esta tarefa torna-se cada vez mais complicada, exigindo o uso de sistemas de arquivos cada vez mais complexos e robustos.

No ambiente Microsoft Windows, há apenas três sistemas de arquivos: *FAT16*, *FAT32* e *NTFS*. O *FAT16* é o mais antigo, usado desde os tempos do *MS-DOS*, enquanto o *NTFS* é o mais complexo e atual. Apesar disso, há uma variedade muito grande de sistemas de arquivos diferentes no *Linux* e outros sistemas *Unix*, que incluem o *EXT2, EXT3, ReiserFS, XFS, JFS* e muitos outros.

Com a partição definida formata-se a partição com o sistema de arquivos escolhido de acordo com a necessidade e ambiente. Assim que formatado consegue-se salvar arquivos e visualizá-los dentro das partições.

O comando *Format* do Windows 7, é utilizado para fazer formatação em um disco preenchendo todos os setores do disco com *bits* 0, tornando a recuperação dos dados anteriormente gravados no disco irrecuperáveis por vias normais. Porém, empresas de recuperação de dados como *KrollOntrack, Sagate ou Sert Datarecovery*, possuem aparelhos capazes de ler a carga residual das mídias.Como todo o HD passa a armazenar *bits* zero, um resquício de carga positiva sob a superfície indicaria que lá estava antes armazenado um bit 1. Isto seria um processo caro e demorado, mas ainda assim seria possível recuperar grande parte dos dados. Um método para eliminar qualquer forma de recuperação seria a gravação aleatórias de bits 1 e 0, tornando impossível a recuperação da informações antes armazenadas ali. Um *software* disponível para fazer esse tipo de formatação seria o *HP Disk Sanitizer* que se utiliza do método *Department Of Defense (DoD*), o qual faz as seguintes operações: Primeiro: escreve zero e verifica a escrita; Segundo: Escreve um e verifica a escrita; Terceiro: Grava um caractere aleatório zero ou um e verifica a escrita. O caractere aleatório garante que nenhum software consiga identificar o que estava ali anteriormente, garantindo assim que os dados não sejam recuperados.

2.3 Formatação rápida

Na formatação rápida, apesar dos dados não aparecerem disponíveis no HD após a formatação eles continuam lá, todas as informações contidas no HD tem um endereçamento registrado na tabela da partição, assim o computador sabe onde pode gravar novos arquivos e onde esta os arquivos quando solicitado pelo usuário, porém ao executamos o comando “formatação rápida” esse tabela é apagada informando o HD que não há arquivos nesse disco e ele pode gravar em qualquer endereço, sobrescrevendo assim as novas informações sobre as informações antigas. O mesmo se aplica a arquivos apagados do HD, é somente apagado o endereçamento do arquivo, ou seja enquanto o arquivo não for sobrescrito no HD é possível recuperá-lo.

2.4 Formatação completa

Diferente da formatação rápida, a formatação completa varre setor a setor sobrescrevendo todos os bit no HD por 0, assim qualquer informação no HD é sobrescrita, além disso ele verifica se há setor danificado, fazendo marcação para a inutilização desse setor. A formatação completa tem um tempo razoável e é variada conforme o tamanho do HD, quanto maior o HD maior o tempo. Após essa formatação, a recuperação dos dados torna-se inviável através de softwares convencionais e deve se procurar empresas especializadas na recuperação dos dados, pois se precisa de equipamentos de leitura de precisão, onde será verificado oscilação no disco magnético e identificação de bits 0 que antes era 1, essa oscilação é precisa por isso deve se ter equipamentos como placa controladoras especificas.

2.5 Recuperações físicas

A recuperação física de um HD destina-se a recuperação dos dados substituindo componentes eletrônicos ou mecânicos, que podem ser ocasionados por queda do dispositivo, alterações na corrente elétrica, desgaste por tempo de uso, alta temperatura entre outros fatores.

Essa recuperação deve ser feita por profissionais em um ambiente preparado para essa manutenção, pois a sala onde esse dispositivo é aberto deve estar sem nenhuma poeira e o manuseio deve ser correto para não ocasionar problemas na leitura do(s) disco(s).

Se os discos do HD não sofrerem grandes danos muita informação pode ser recuperada, pois toda a estrutura de um HD pode ser substituída para se obter os dados antes gravados nesse(s) disco(s). Os dados somente não serão recuperados se houver comprometimento do disco(s) onde os dados são armazenados, ou seja, não adianta quebrar a placa lógica do HD e achar que seus dados não possam ser recuperados. As principais falhas físicas são: Queima de circuitos eletrônicos,

quebra de cabeças de leitura, danos a superfície dos discos, Setores defeituosos, desgaste natural do disco, travamento do motor, queima do motor.

2.6 Recuperações lógicas

A recuperação lógica de um HD destina-se a recuperação dos dados via *softwares*, dependendo do nível em que o HD foi formatado ou se os arquivos foram apenas apagados, o próprio usuário pode efetuar a recuperação, porém aconselha-se sempre procurar especialistas para a recuperação dos dados, pois se os dados forem sobrescritos por novos dados pode se perder os dados antigos nesse HD.

Se houve uma formatação completa do HD, seus dados não serão recuperados sem softwares e placa controladora especifica. A recuperação lógica torna-se mais difícil quanto mais houver alterações de dados do HD, por isso executar algumas ferramentas pode comprometer os dados antes armazenados ali. A recuperação lógica pode ser feita conforme será mostrado posteriormente nos testes.

3. TESTES COM SOFTWARES PARA FORMATAÇÃO E RECUPERAÇÃO DE DADOS EM DISCO RÍGIDO

Serão realizados testes em três métodos de formatação: formatação rápida, formatação completa e formatação DoD. Após formatação de cada método, serão realizados testes de recuperação de dados e informado o resultado de cada teste.

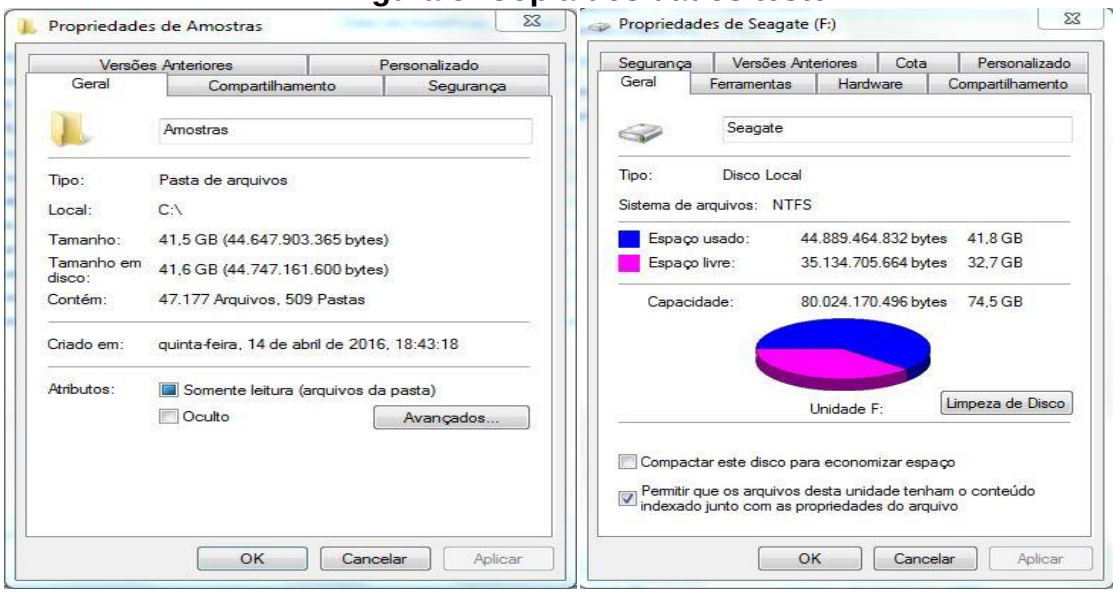
3.1 Formatação rápida e tentativa de recuperação

Nesta etapa foi realizado teste no método de formatação rápida utilizando-se o sistema operacional Microsoft Windows 7. Posteriormente a esse método de formatação foram realizadas tentativas de recuperação dos dados através de softwares de recuperação lógica de dados.

Para esses testes foram utilizados os seguintes itens: um disco rígido de 80 GB da marca *Seagate* modelo ST980811AS, um microcomputador com sistema operacional *Microsoft Windows 7 Ultimate* e dois softwares de recuperação de dados "*GetDataback for NTFS* Version 4.33" e "*Recuva V1.43.623*"

1º Teste: Foi copiado para esse disco rígido uma pasta chamada "Amostras" com tamanho de 41,5 GB contendo 47.177 arquivos e 509 pastas. Contendo arquivos com diversas extensões como: JPG, JPEG, PNG, MP3, VOB, XLS, PDF, ZIP, DOC, DOCX, PPT.

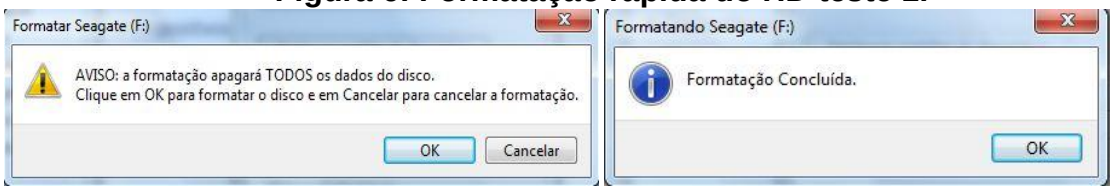
Figura 5: Cópia dos dados teste 1.



Fonte: Print Screen – Fonte do autor 04/2017

Após a cópia dos dados, conforme figura 5, foi executado a Formatação Rápida do Windows, conforme figura 6.

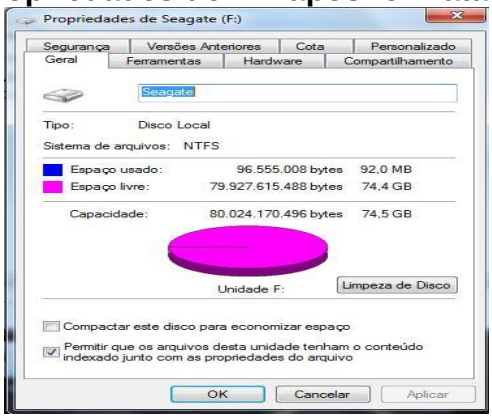
Figura 6: Formatação rápida do HD teste 1.



Fonte: Print Screen – Fonte do autor 04/2017

A figura 7 demonstra o estado do disco após sua formatação.

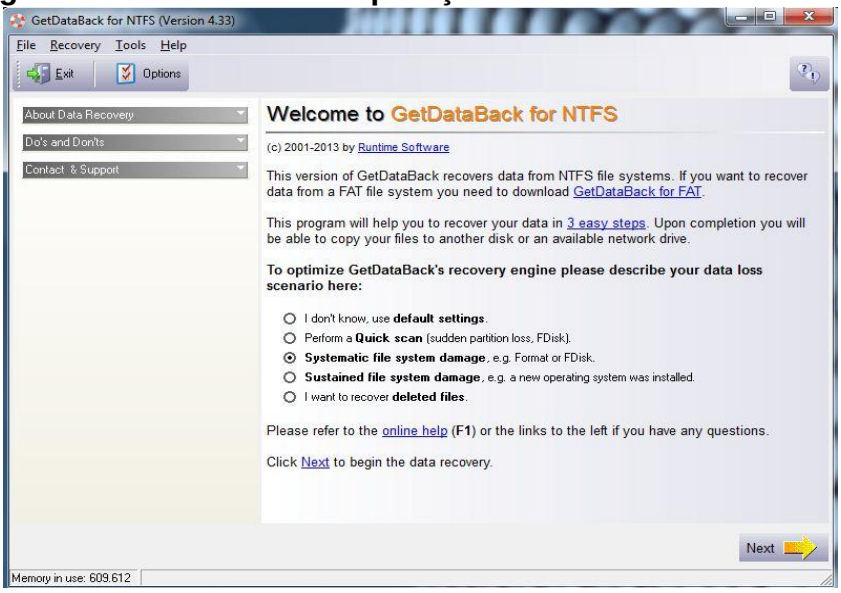
Figura 7: Propriedades do HD após formatação teste 1.



Fonte: Print Screen – Fonte do autor 04/2017

Após concluir a formatação em modo rápido, iniciou-se a tentativa de recuperação de dados por meio do *software GatDataBack.* Selecionou-se a opção “ *Systematic file system damage , e.g Format or FDisk”*, conforme figura 8.

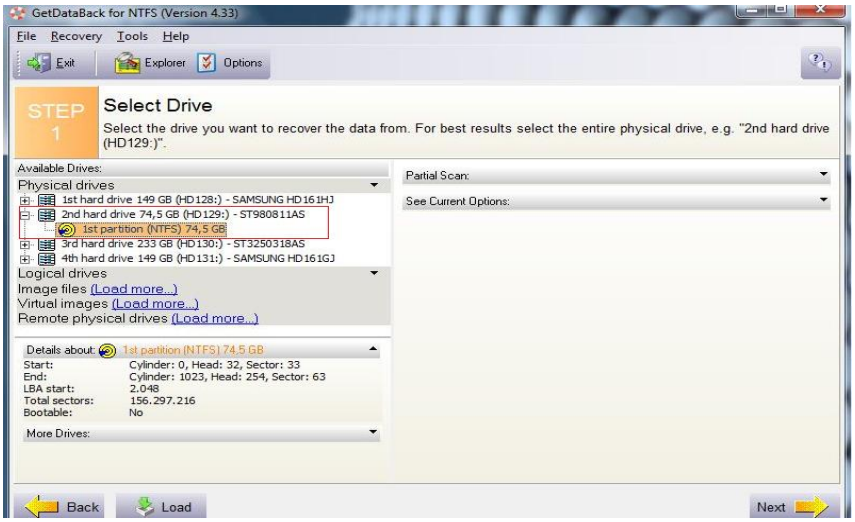
Figura 8: Interface de recuperação do GetDataBack teste 1.



Fonte: Print Screen – Fonte do autor 04/2017

Foi selecionado o disco rígido a ser recuperado e iniciado o processo de recuperação, conforme figura 9.

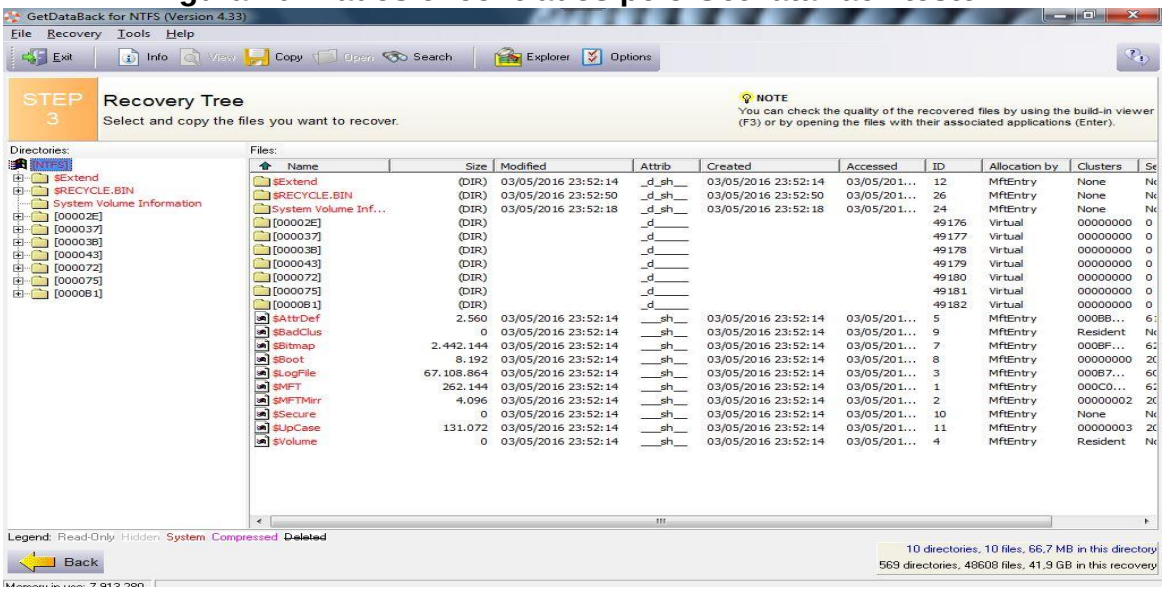
Figura 9: Seleção do disco a ser recuperado pelo GetDataBack teste 1.



Fonte: Print Screen – Fonte do autor 04/2017

Após 32 minutos, o *software GatDataBack* concluiu o processo de recuperação. Ele recuperou 41,9 GB, sendo 569 diretórios e 48.608 arquivos. Recuperou inclusive pastas e arquivos da partição os quais ficam ocultos, sendo a diferença apresentada da pasta “Amostras”, conforme figura 10.

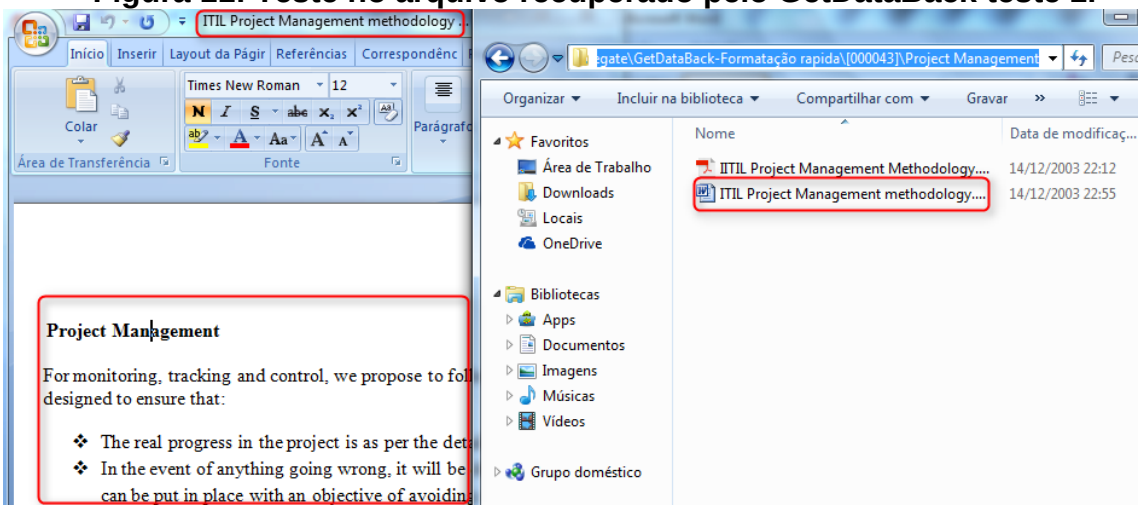
Figura 10: Dados encontrados pelo GetDataBack teste 1.



Fonte: Print Screen – Fonte do autor 04/2017

Foi realizado um teste para verificar se o arquivo, depois de recuperado, ficaria legível,e o resultado foi positivo, conforme figura 11.

Figura 11: Teste no arquivo recuperado pelo GetDataBack teste 1.

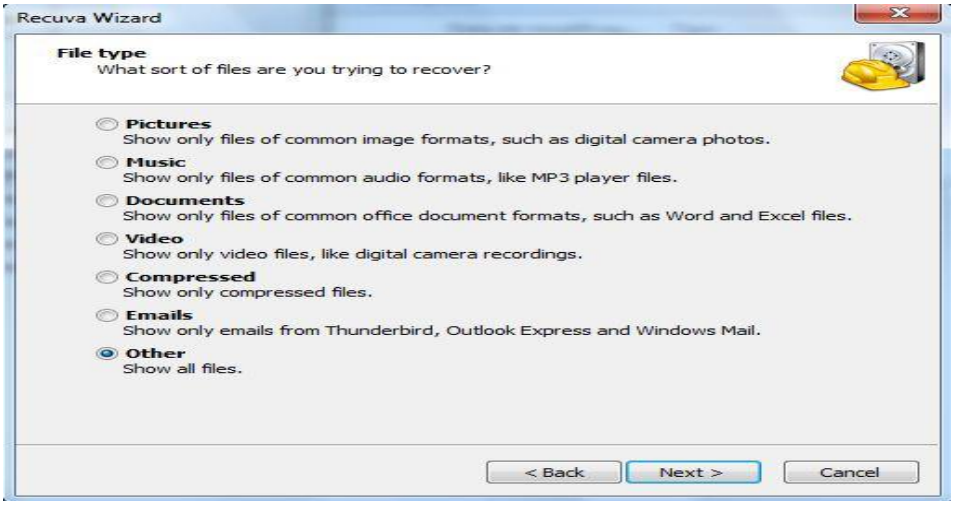


Fonte: Print Screen – Fonte do autor 04/2017

Após concluir os testes com o *software GetDataBack,* iniciou-se o teste com o software Recuva utilizando o mesmo disco rígido, o qual não sofreu alterações pois a recuperação dos dados efetuada pelo *GetDataBack* foi restaurada para outro disco rígido “C:”.

Selecionou-se a opção “*Other*” e clicamos em “*Next*”, conforme figura 12.

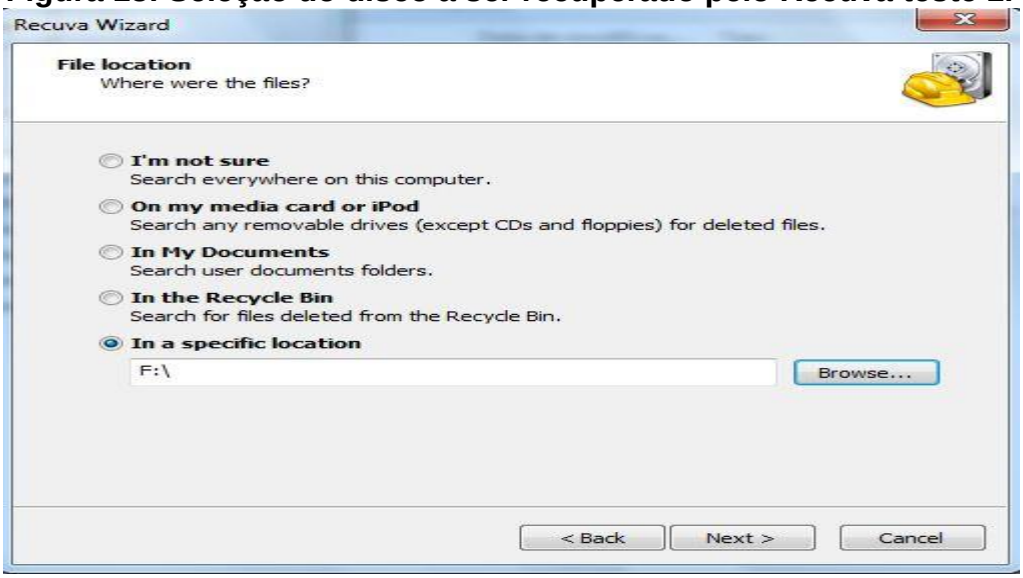
Figura 12: Interface de recuperação do Recuva teste 1.



Fonte: Print Screen – Fonte do autor 04/2017

Então é necessário selecionar a partição da qual deseja-se recuperar dados, nesse caso é a unidade F:, conforme figura 13.

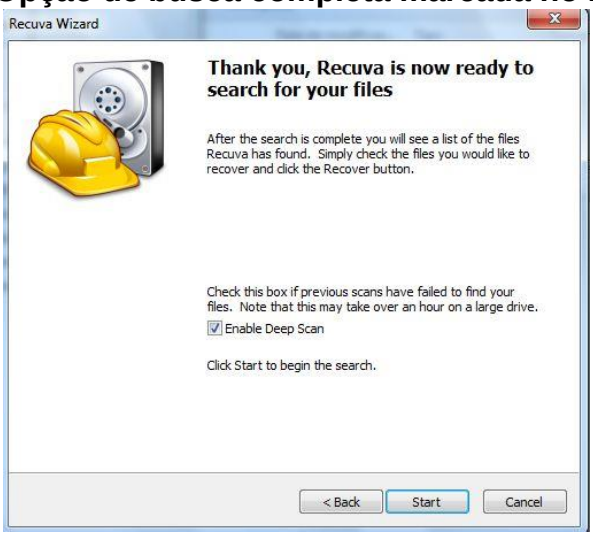
Figura 13: Seleção do disco a ser recuperado pelo Recuva teste 1.



Fonte: Print Screen – Fonte do autor 04/2017

Foi marcado a opção “Enable Deep Scan”,conforme figura 14, essa opção faz uma busca completa no disco rígido.

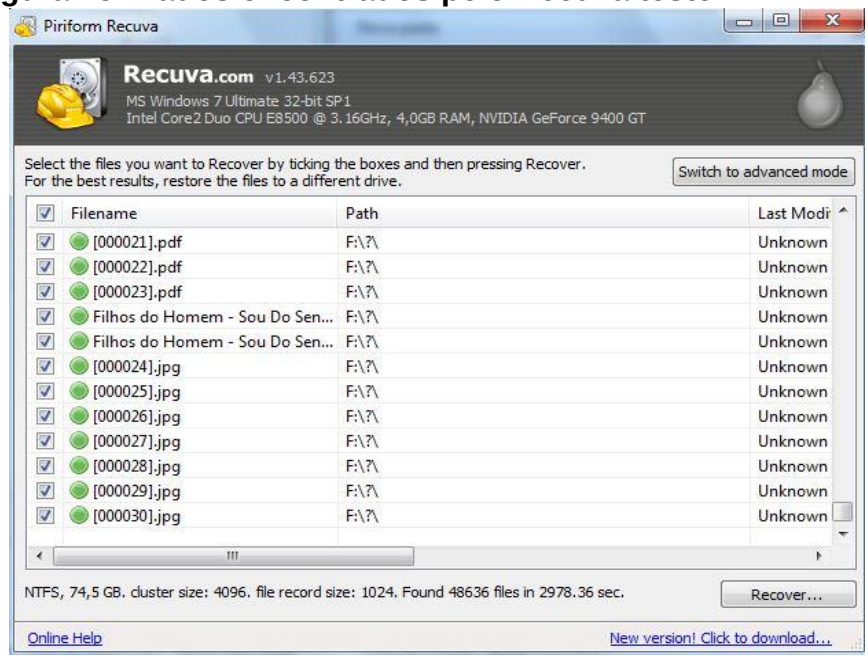
Figura 14: Opção de busca completa marcada no Recuva teste 1.



Fonte: Print Screen – Fonte do autor 04/2017

Após iniciar o processo, o *Recuva* demorou cerca de 50 minutos para finalizar a busca por arquivos nesse disco rígido. Ele encontrou 48636 arquivos, conforme figura 15.

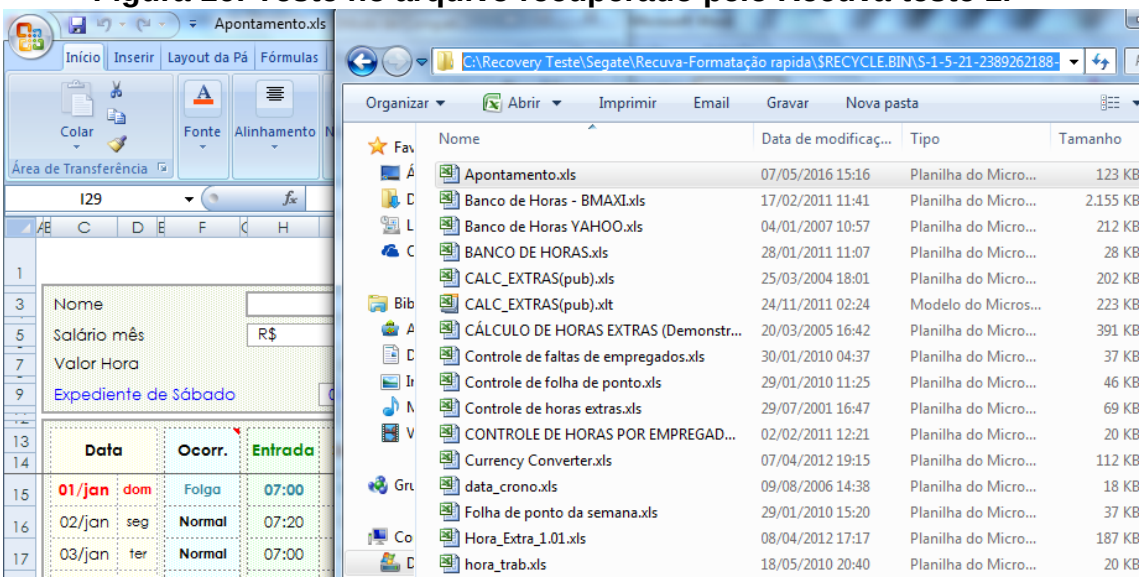
Figura 15: Dados encontrados pelo Recuva teste1.



Fonte: Print Screen – Fonte do autor 04/2017

Foi realizado um teste para verificar se o arquivo, depois de recuperado, ficaria legível, e o resultado foi positivo, conforme figura 16.

Figura 16: Teste no arquivo recuperado pelo Recuva teste 1.



Fonte: Print Screen – Fonte do autor 04/2017

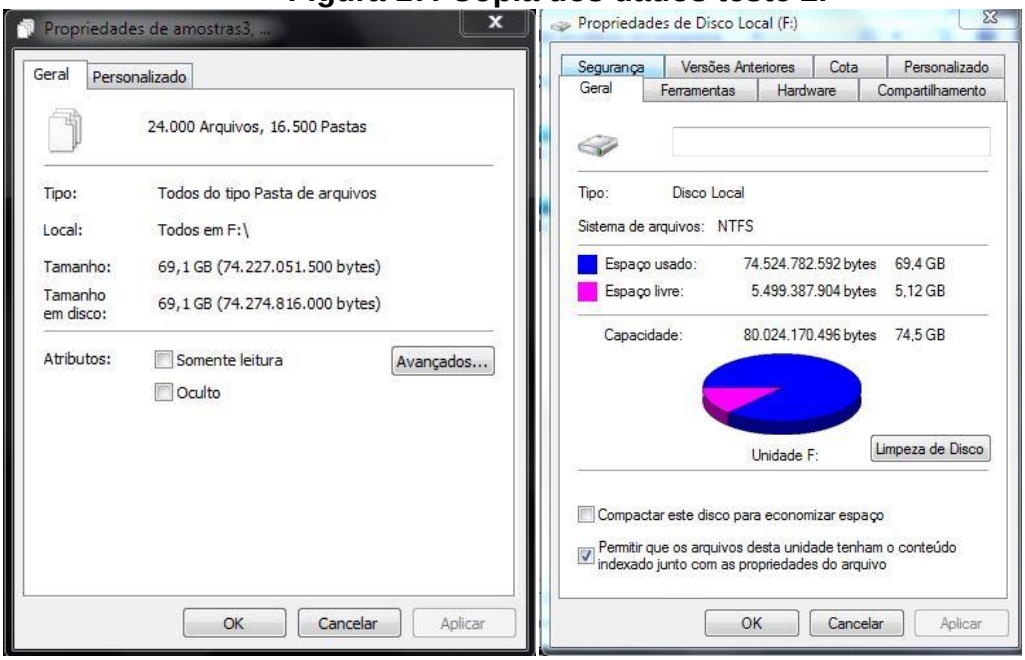
3.2 Formatação completa e tentativa de recuperação

Nesta etapa foram realizados testes no método de formatação completa utilizando-se o sistema operacional Microsoft Windows 7. Posteriormente a esse método de formatação, foram realizadas tentativas de recuperação dos dados através de softwares de recuperação lógica de dados.

Para esses testes foram utilizados os seguintes itens: um disco rígido de 80 GB da marca Fujitsu modelo MHY2080BH, um microcomputador com sistema operacional Microsoft Windows 7 *Ultimate* e três softwares de recuperação de dados "*GetDataback for NTFS Version* 4.33" , *"Recuva V1*.52.1086" e "*Wondershare Data Recovery"*

2º Teste: Foi copiado para esse disco rígido uma pastas chamada "Amostras3" com tamanho de 69,1 GB, contendo 24.000 arquivos e 16.500 pastas, conforme figura 17. Contendo arquivos com diversas extensões como: JPG, JPEG, PNG, MP3, VOB, XLS, PDF, ZIP, DOC, DOCX, PPT.

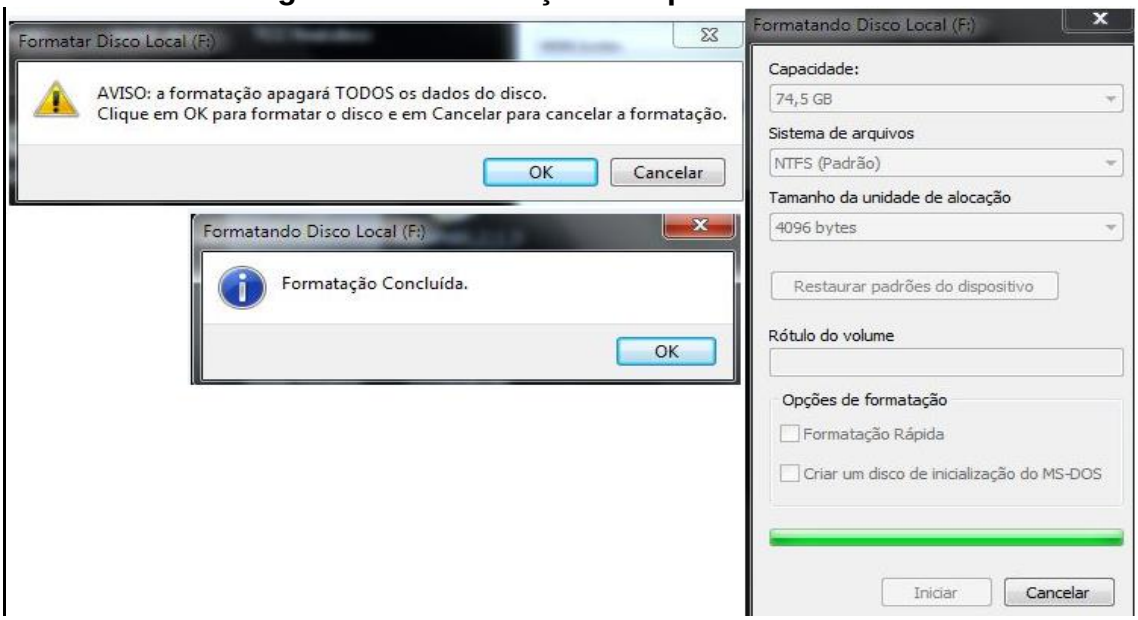
Figura 17: Cópia dos dados teste 2.



Fonte: Print Screen – Fonte do autor 04/2017

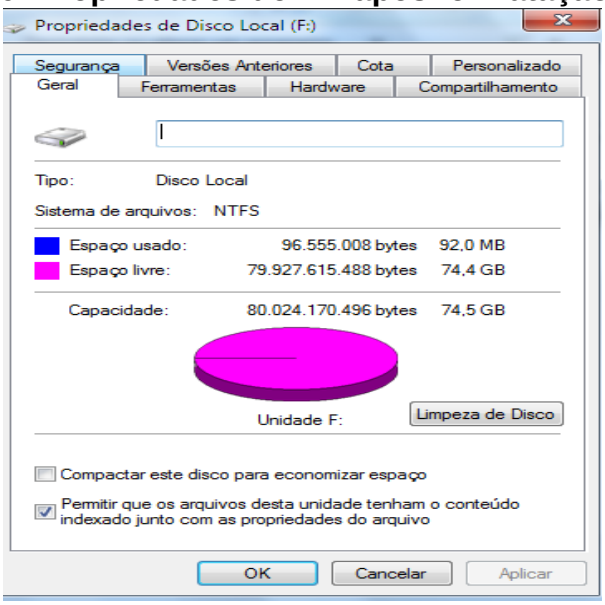
Após a copia dos dados foi executado a Formatação Completa do Windows, conforme figura 18.

Figura 18: Formatação completa do HD teste 2.



Fonte: Print Screen – Fonte do autor 04/2017

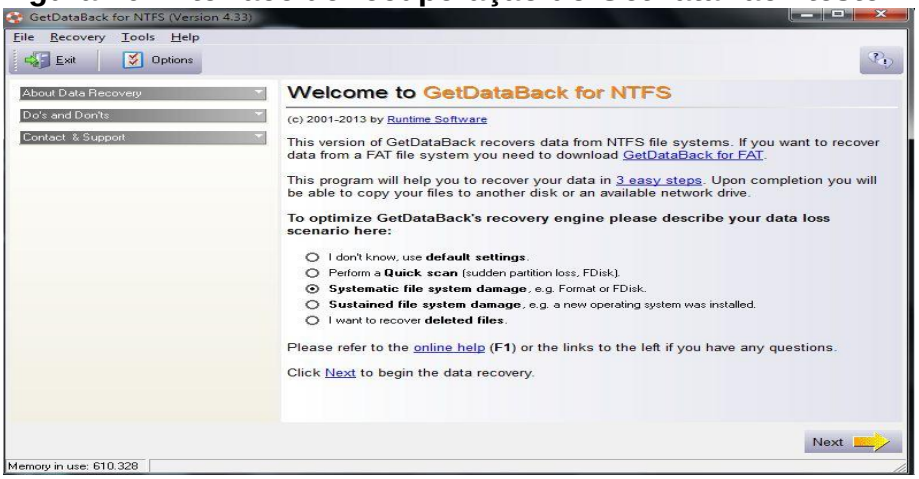
Figura 19: Propriedades do HD após formatação teste 2.



Fonte: Print Screen – Fonte do autor 04/2017

Após concluir a formatação em modo completo, conforme figura 19, iniciou-se a tentativa de recuperação de dados por meio do *software GatDataBack.* Selecionamos a opção " *Systematic file system damage , e.g Format or FDisk",* conforme figura 20.

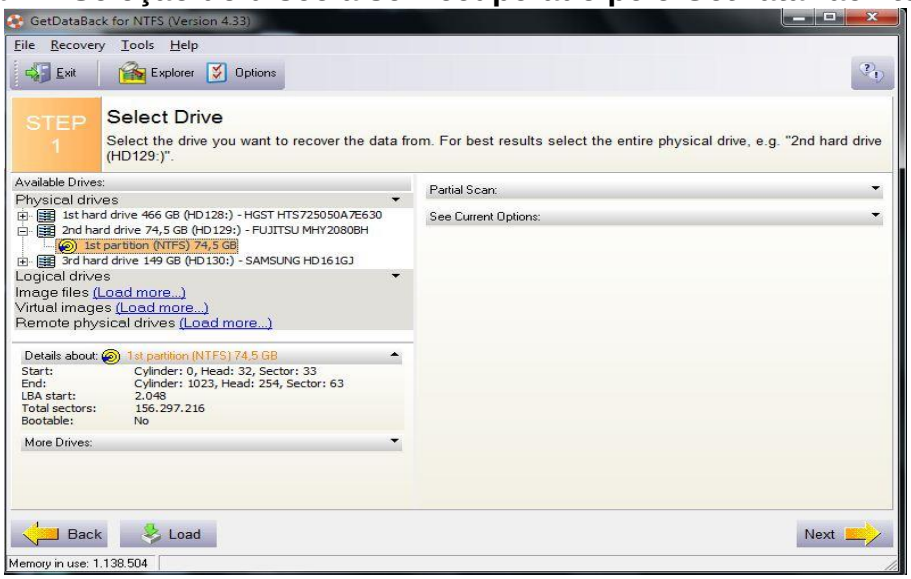
Figura 20: Interface de recuperação do GetDataBack teste 2.



Fonte: Print Screen – Fonte do autor 04/2017

Foi selecionado o disco rígido a ser recuperado e iniciado o processo de recuperação, conforme figura 21.

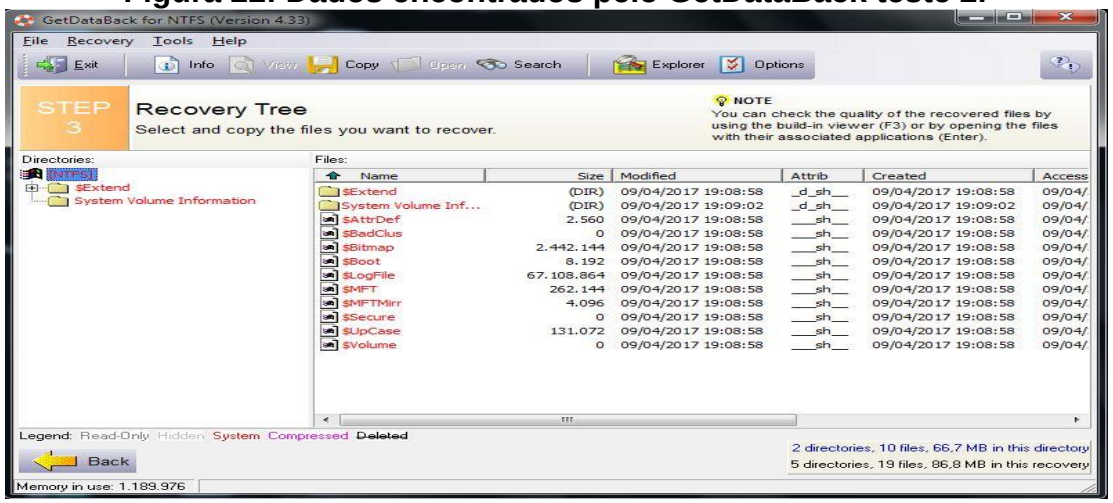
Figura 21: Seleção do disco a ser recuperado pelo GetDataBack teste 2.



Fonte: Print Screen – Fonte do autor 04/2017

Após 42 minutos o *software GatDataBack* concluiu o processo de recuperação. Encontrando apenas pastas e arquivos da partição os quais ficam ocultos, não encontrando nenhum arquivo que possa ser utilizado, ou importante para o usuário. Nenhum arquivo da pasta “Amostras3”foi recuperado, conforme figura 22.

Figura 22: Dados encontrados pelo GetDataBack teste 2.



Fonte: Print Screen – Fonte do autor 04/2017

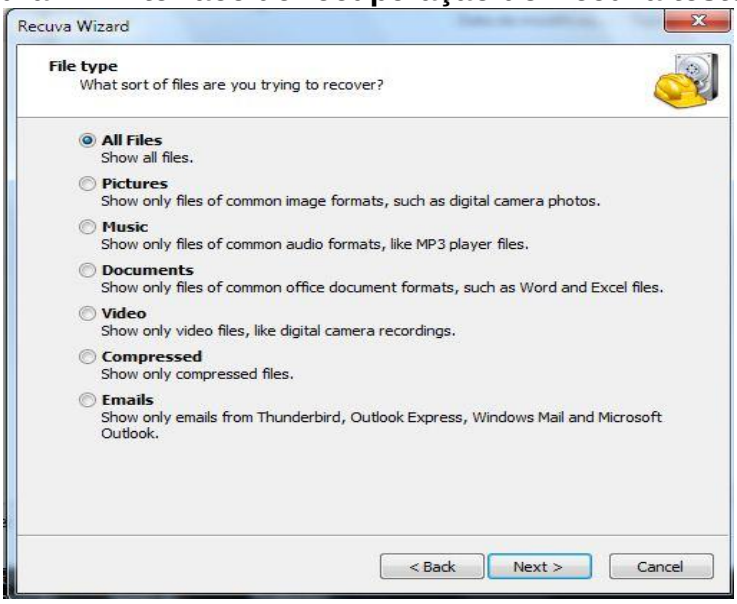
Após concluir os testes com o *software GetDataBack*, iniciou-se o teste com o *software Recuva* utilizando o mesmo disco rígido, conforme figura 23, o qual não sofreu alterações.

Figura 23: Interface inicial do Recuva teste 2.

Fonte: Print Screen – Fonte do autor 04/2017

Selecionamos a opção *"All Files*" e clicamos em "*Next*", conforme figura 24.

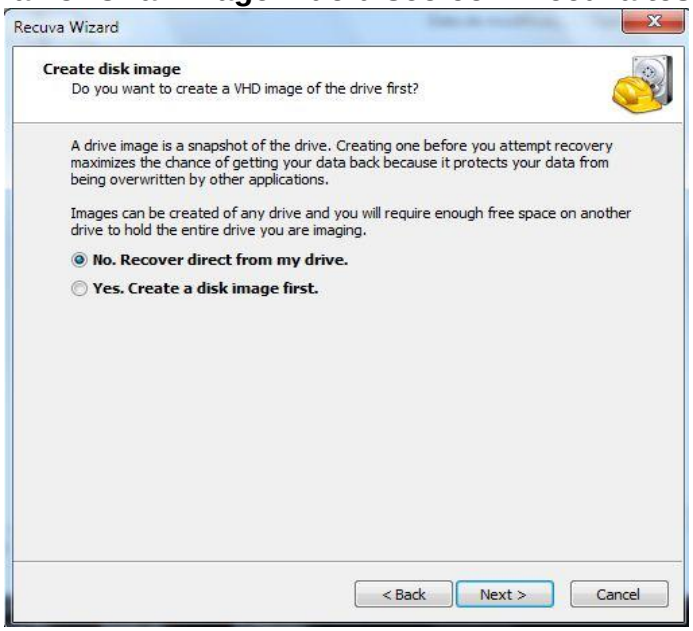
Figura 24: Interface de recuperação do Recuva teste 2.



Fonte: Print Screen – Fonte do autor 04/2017

Nessa etapa pode-se criar uma imagem do disco para não comprometer os dados por aplicativos sobrescrevendo os dados no HD, conforme figura 24, porém como é um disco de teste não há necessidade desse processo.

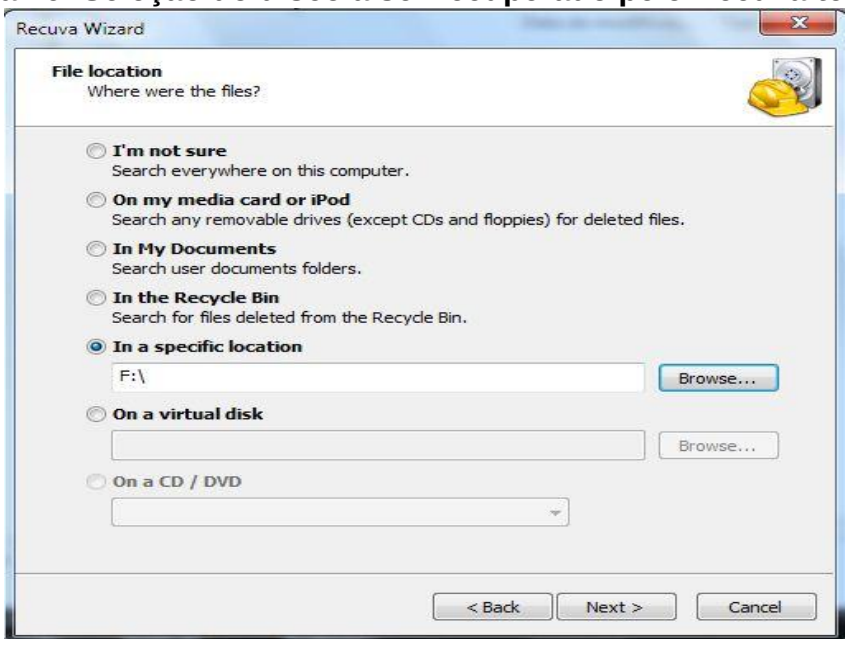
Figura 25: Criar imagem do disco com Recuva teste 2.



Fonte: Print Screen – Fonte do autor 04/2017

Então é necessário selecionar a partição a qual deseja recuperar dados, nesse caso é a unidade F:, conforme figura 26.

Figura 26: Seleção do disco a ser recuperado pelo Recuva teste 2.



Fonte: Print Screen – Fonte do autor 04/2017

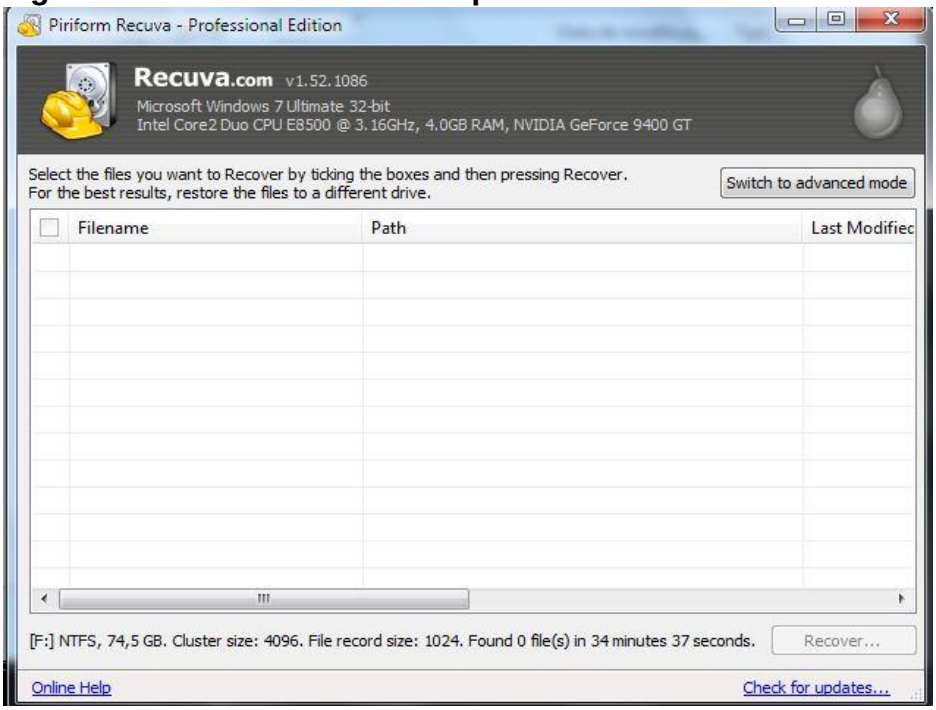
Marcou-se a opção “*Enable Deep Scan*”, conforme figura 27, essa opção faz uma busca completa no disco rígido.

Figura 27: Opção de busca completa marcada no Recuva teste 2.

Fonte: Print Screen – Fonte do autor 04/2017

Após iniciar o processo o Recuva demorou cerca de 34 minutos para finalizar a busca por arquivos nesse disco rígido. Ele não encontrou nenhum arquivo para ser recuperado, conforme figura 28.

Figura 28: Dados encontrados pelo Recuva teste2.



Fonte: Print Screen – Fonte do autor 04/2017

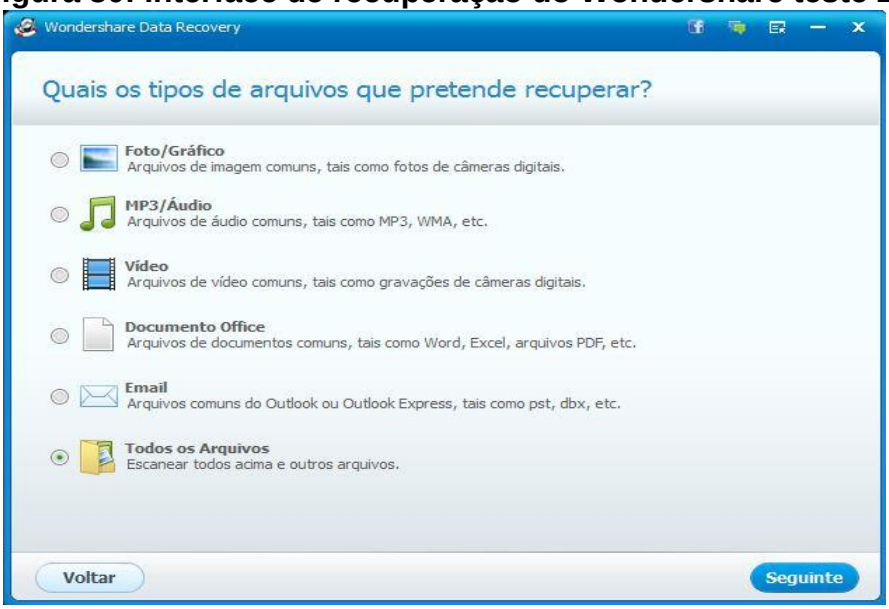
Após concluir os testes com o software Recuva, iniciou-se o teste com o *software* Wondershare Data Recovery, conforme figura 29, utilizando o mesmo disco rígido, o qual não sofreu alterações.

Figura 29: Interface inicial do Wondershare teste 2.

Fonte: Print Screen – Fonte do autor 04/2017

Selecionou-se a opção “Todos os Arquivos” e “Seguinte”, conforme figura 30.

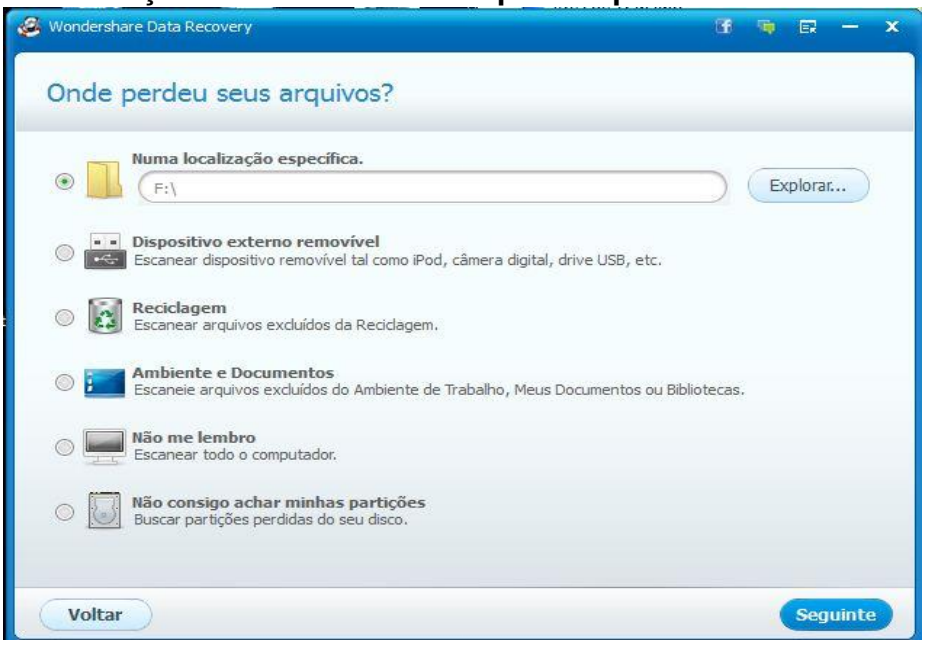
Figura 30: Interface de recuperação do Wondershare teste 2.



Fonte: Print Screen – Fonte do autor 04/2017

Então é necessário selecionar a partição a qual deseja recuperar dados, nesse caso é a unidade F:, conforme figura 31.

Figura 31: Seleção do disco a ser recuperado pelo Wondershare teste 2.



Fonte: Print Screen – Fonte do autor 04/2017

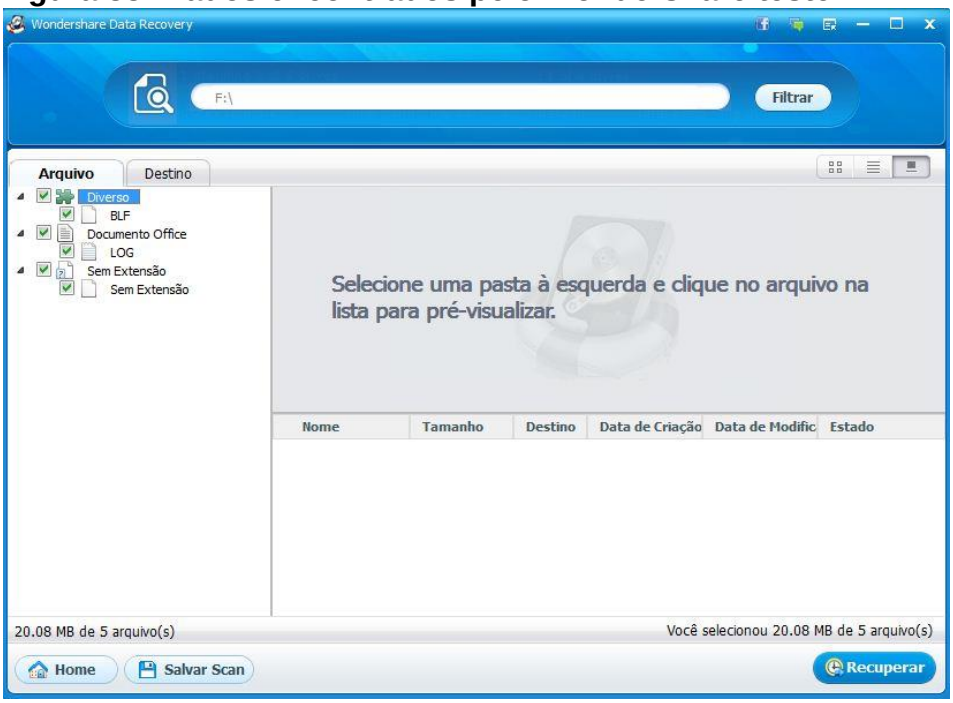
Marcou-se a opção “Permitir Scan Profundo”, conforme figura 32, essa opção faz uma busca completa no disco rígido.

Figura 32: Opção de busca completa marcada no Wondershare teste 2.

Fonte: Print Screen – Fonte do autor 04/2017

Após iniciar, o processo o *Wondershare* demorou cerca de 40 minutos para concluir o processo de recuperação. Encontrando apenas pastas e arquivos da partição os quais ficam ocultos, conforme figura 33, não encontrando nenhum arquivo que possa ser utilizado, ou importante para o usuário. Nenhum arquivo da pasta “Amostras3” foi recuperado.

Figura 33: Dados encontrados pelo Wondershare teste2.



Fonte: Print Screen – Fonte do autor 04/2017

Após conclusão dos testes sem sucesso, foram realizados novos testes com outros softwares conforme figura 34, os quais obtiveram os mesmos resultados, sem sucesso de recuperação.

Figura 34: Softwares de recuperação de dados

Fonte: Print Screen – Fonte do autor 04/2017

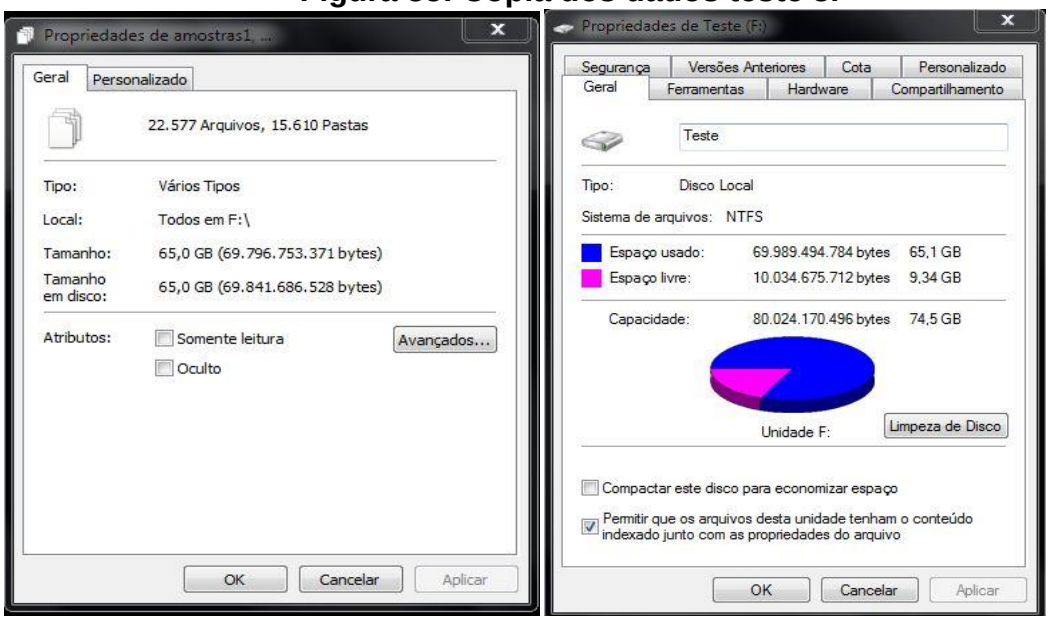
3.3 Formatação utilizando método dod 5220.22-m e tentativa de recuperação

Nesta etapa foram realizados testes utilizando-se o método de eliminação de dados DoD 5220.22-M, para esse método foi utilizado o software Disk Wipe v1.7. Posteriormente a esse método de formatação foram realizadas tentativas de recuperação dos dados através de softwares de recuperação lógica de dados.

Para esses testes foram utilizados os seguintes itens: um disco rígido de 80 GB da marca Fujitsu modelo MHY2080BH, um microcomputador com sistema operacional Microsoft Windows 7 *Ultimate* e três softwares de recuperação de dados "*GetDataback for NTFS Version* 4.33" , *"Recuva V1*.52.1086" e "*Wondershare Data Recovery"*

3º Teste: Foi copiado para esse disco rígido 22.577 arquivos e 15.610 pastas, conforme figura 35. Contendo arquivos com diversas extensões como: JPG, JPEG, PNG, MP3, VOB, XLS, PDF, ZIP, DOC, DOCX, PPT.

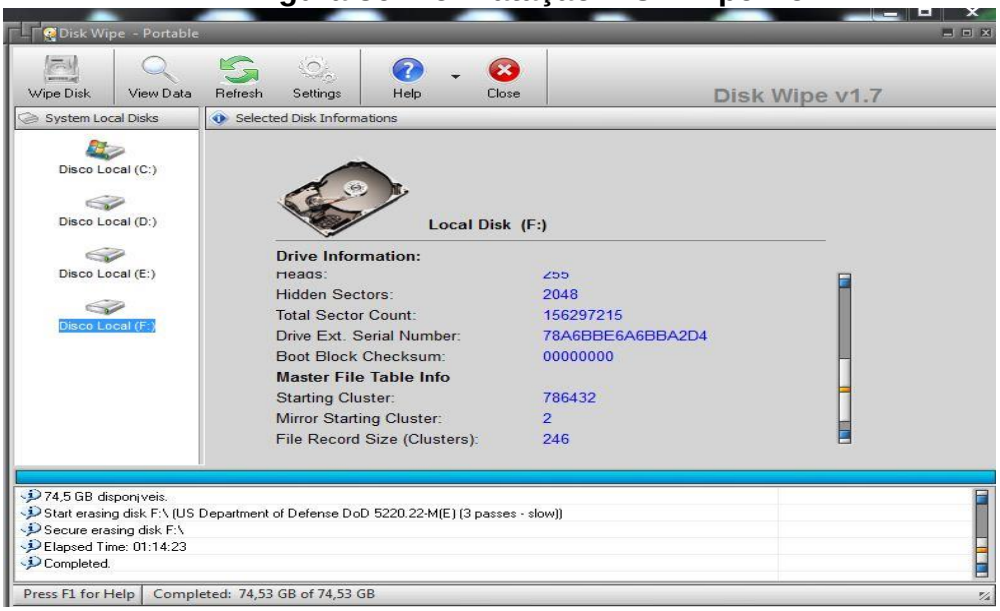
Figura 35: Cópia dos dados teste 3.



Fonte: Print Screen – Fonte do autor 05/2017

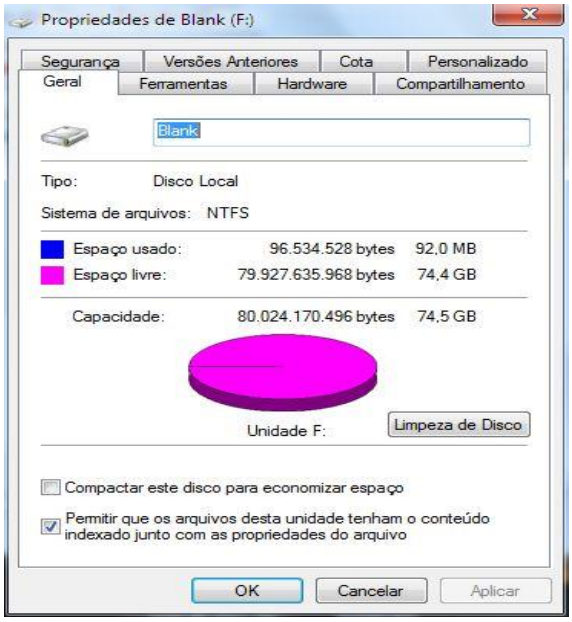
Após a cópia dos dados foi executado o *software* Disk Wipe, conforme figura 36, efetuando a eliminação dos dados utilizando-se o método DoD , conforme figura 37.

Figura 36: Formatação Disk Wipe DoD.



Fonte: Print Screen – Fonte do autor 05/2017

Figura 37: Propriedades do HD após executar o Disk Wipe teste 3.



Fonte: Print Screen – Fonte do autor 05/2017

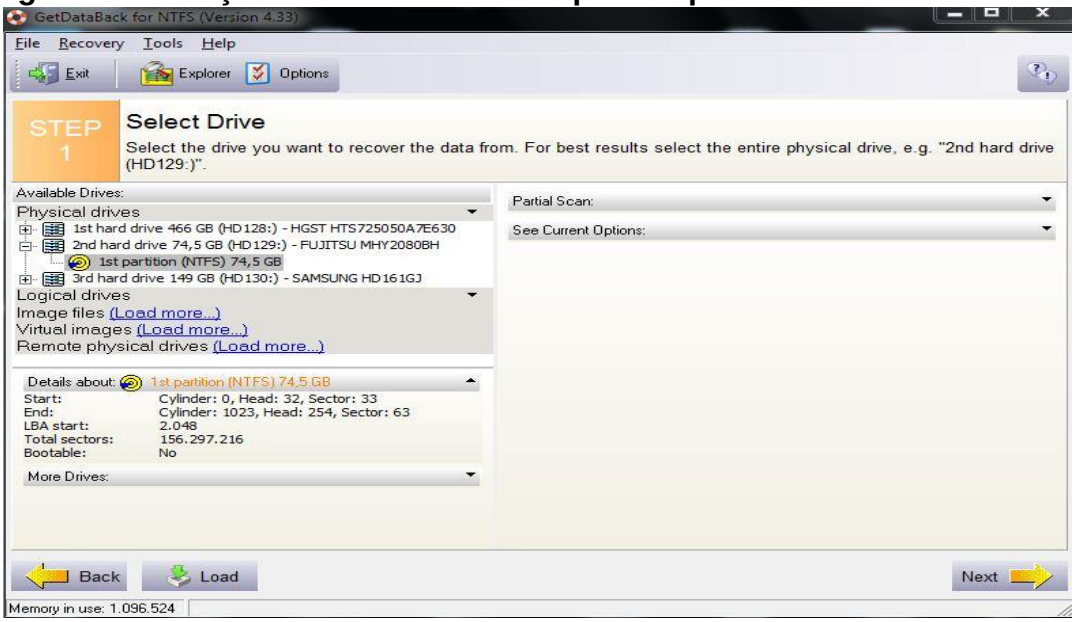
Após concluir a formatação em modo completo, iniciou-se a tentativa de recuperação de dados por meio do *software GatDataBack.* Selecionamos a opção “ *Systematic file system damage , e.g Format or FDisk”,* conforme figura 38.

Figura 38: Interface de recuperação do GetDataBack teste 3.

Fonte: Print Screen – Fonte do autor 05/2017

Foi selecionado o disco rígido a ser recuperado e iniciado o processo de recuperação, conforme figura 39.

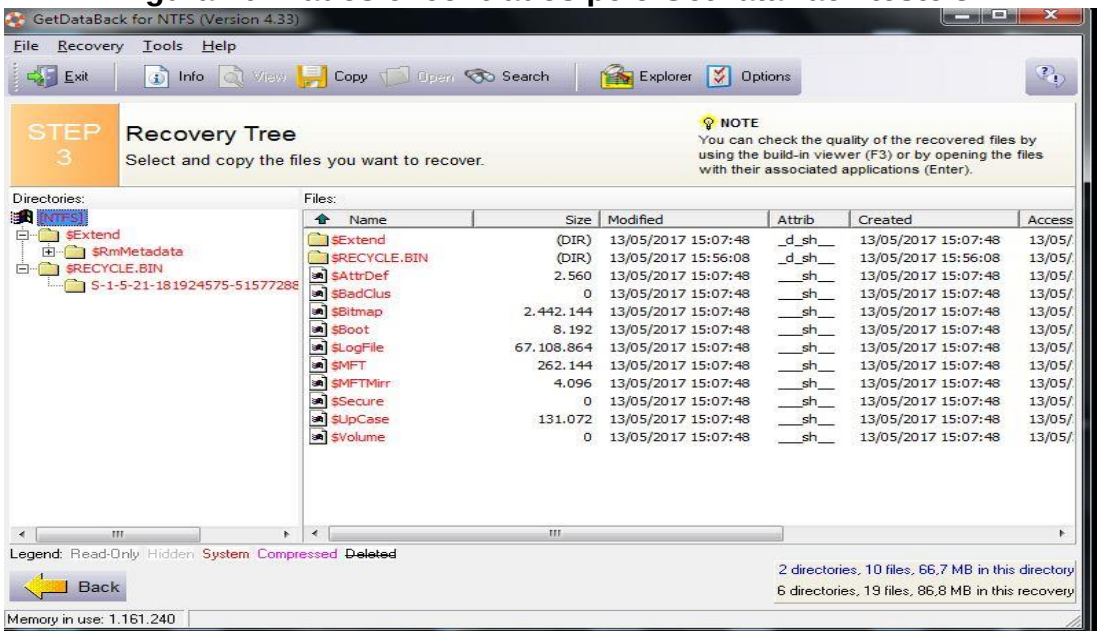
Figura 39: Seleção do disco a ser recuperado pelo GetDataBack teste 3.



Fonte: Print Screen – Fonte do autor 05/2017

Após 47 minutos, o software *GatDataBack* concluiu o processo de recuperação, econtrando apenas pastas e arquivos da partição os quais ficam ocultos, conforme figura 40, não encontrando nenhum arquivo que possa ser utilizado ou importante para o usuário. Nenhum arquivo foi recuperado.

Figura 40: Dados encontrados pelo GetDataBack teste 3.



Fonte: Print Screen – Fonte do autor 05/2017

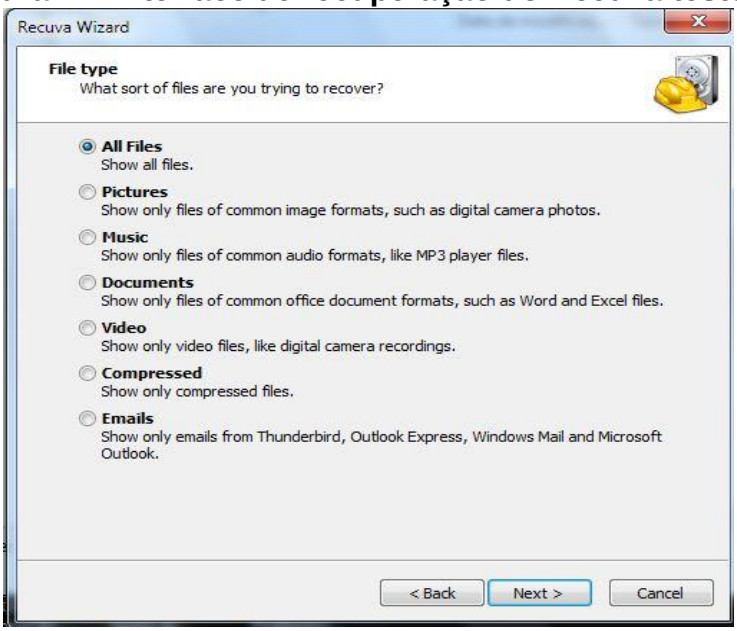
Após concluir os testes com o *software GetDataBack*, iniciou-se o teste com o software Recuva, conforme figura 41, utilizando o mesmo disco rígido, o qual não sofreu alterações.

Figura 41: Interface inicial do Recuva teste 3.

Fonte: Print Screen – Fonte do autor 05/2017

Selecionou-se a opção *"All Files*" e clicamos em "*Next*", conforme figura 42.

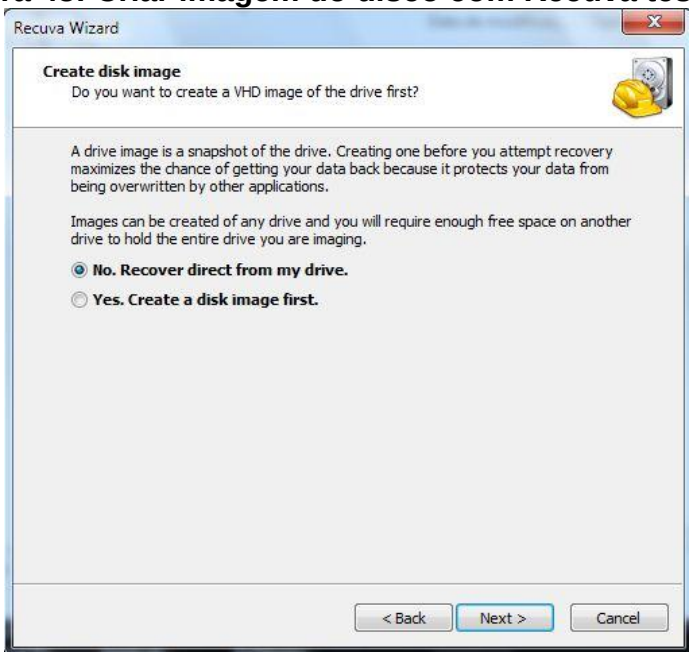
Figura 42: Interface de recuperação do Recuva teste 3.



Fonte: Print Screen – Fonte do autor 05/2017

Nessa etapa pode-se criar uma imagem do disco para não comprometer os dados por aplicativos sobrescrevendo os dados no HD, conforme figura 43, porém como é um disco de teste não há necessidade desse processo.

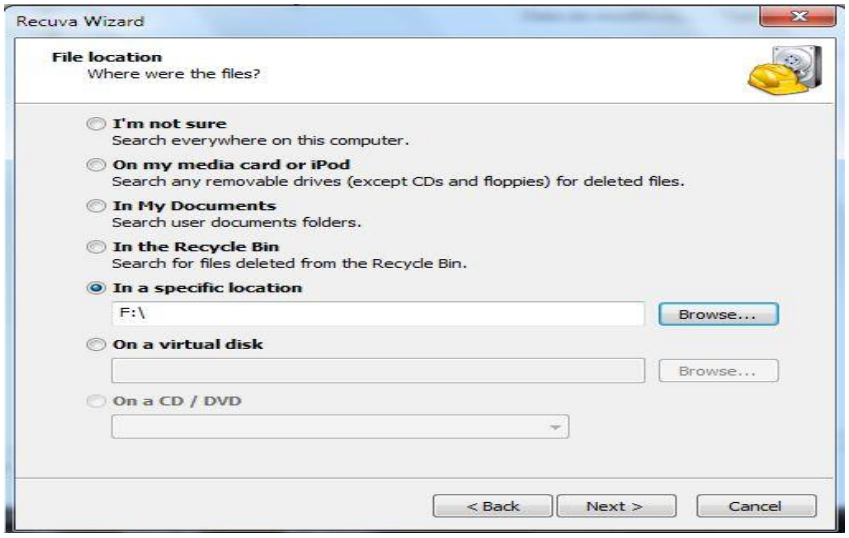
Figura 43: Criar imagem do disco com Recuva teste 3.



Fonte: Print Screen – Fonte do autor 05/2017

Então é necessário selecionar a partição a qual deseja recuperar dados, nesse caso é a unidade F:, conforme figura 44.

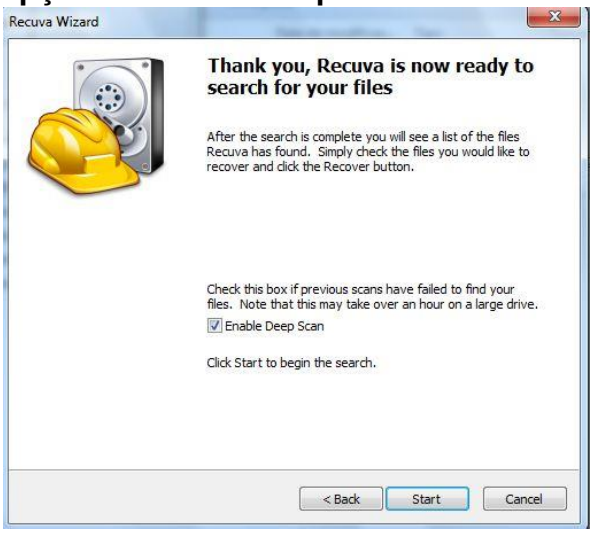
Figura 44: Seleção do disco a ser recuperado pelo Recuva teste 3.



Fonte: Print Screen – Fonte do autor 05/2017

Marcou-se a opção “*Enable Deep Scan*”, conforme figura 45, essa opção faz uma busca completa no disco rígido.

Figura 45: Opção de busca completa marcada no Recuva teste 3.

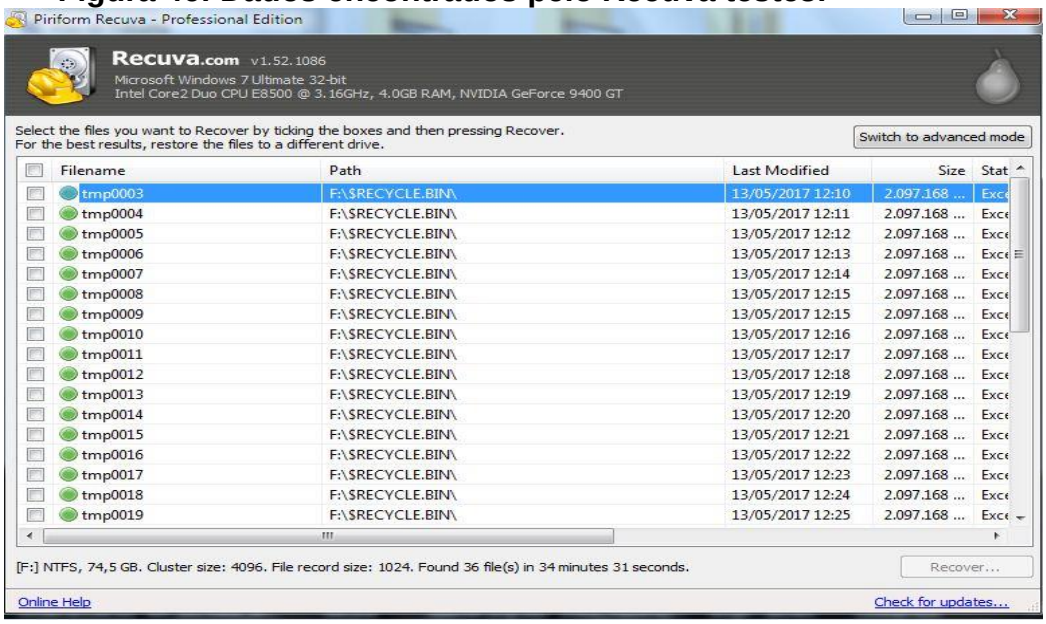


Fonte: Print Screen – Fonte do autor 05/2017

Após iniciar o processo o *Recuva* demorou cerca de 34 minutos para finalizar a busca por arquivos nesse disco rígido. Ele encontrou arquivos temporários com que foram escritos pelo *Disk Wipe* na sobrescrita dos dados anteriores, conforme figura 46. Foram recuperados esses temporários, porém não continham

nenhuma informação válida. Esses arquivos foram criados apenas pra sobrescrever os dados antes armazenados.

Figura 46: Dados encontrados pelo Recuva teste3.



Fonte: Print Screen – Fonte do autor 05/2017

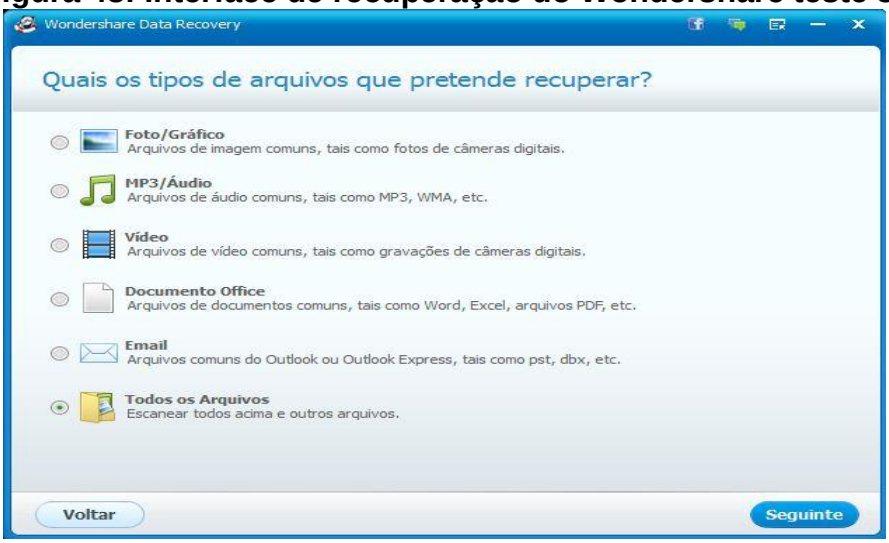
Após concluir os testes com o software Recuva, iniciou-se o teste com o software Wondershare Data Recovery utilizando o mesmo disco rígido, o qual não sofreu alterações, conforme figura 47.

Figura 47: Interface inicial do Wondershare teste 3.

Fonte: Print Screen – Fonte do autor 05/2017

Selecionou-se a opção “Todos os Arquivos” e clicamos em “Seguinte”, conforme figura 48.

Figura 48: Interface de recuperação do Wondershare teste 3.



Fonte: Print Screen – Fonte do autor 05/2017

Então é necessário selecionar a partição a qual deseja recuperar dados, nesse caso é a unidade F:, conforme figura 49.

Figura 49: Seleção do disco a ser recuperado pelo Wondershare teste 3.

Fonte: Print Screen – Fonte do autor 05/2017

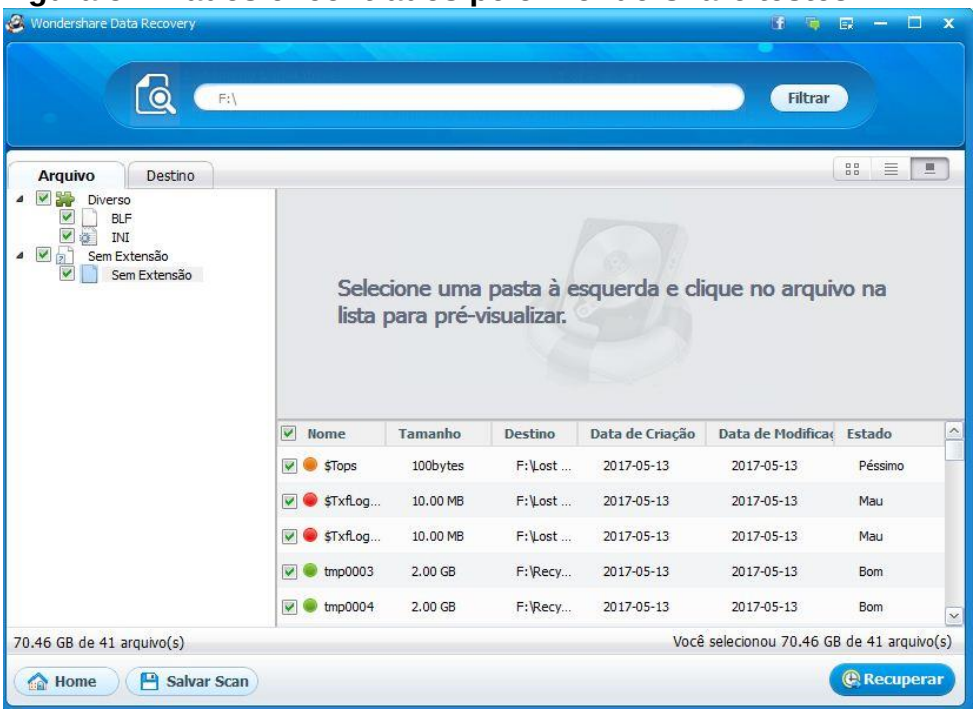
Marcou-se a opção “Permitir Scan Profundo”, conforme figura 50, essa opção faz uma busca completa no disco rígido.

Figura 50: Opção de busca completa marcada no Wondershare teste 3.

Fonte: Print Screen – Fonte do autor 05/2017

Após iniciar o processo, o *Wondershare* demorou cerca de 42 minutos para concluir o processo de recuperação. Ele encontrou arquivos temporários com que foram escritos pelo Disk Wipe na sobrescrita dos dados anteriores, conforme figura 51. Foram recuperados esses temporários, porém não continham nenhuma informação válida. Esses arquivos foram criados apenas pra sobrescrever os dados antes armazenados.

Figura 51: Dados encontrados pelo Wondershare teste3.



Fonte: Print Screen – Fonte do autor 05/2017

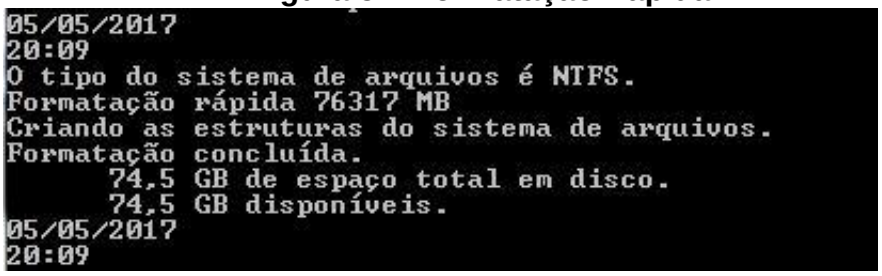
Após conclusão dos testes sem sucesso, foram realizados novos testes com outros softwares conforme figura 34, os quais obtiveram os mesmos resultados, sem sucesso de recuperação.

4. TEMPO DE FORMATAÇÃO PARA CADA MÉTODO E MATRIZ DE RESULTADOS DOS SOFTWARES UTILIZADOS

Para essa analise foi utilizado um disco rígido de 80 GB da marca *Fujitsu*, sendo que o tempo de formatação pode variar de acordo com o tamanho do disco rígido e configuração do computador.

Formatação rápida: Concluiu o processo em menos de um minuto, conforme figura 52.

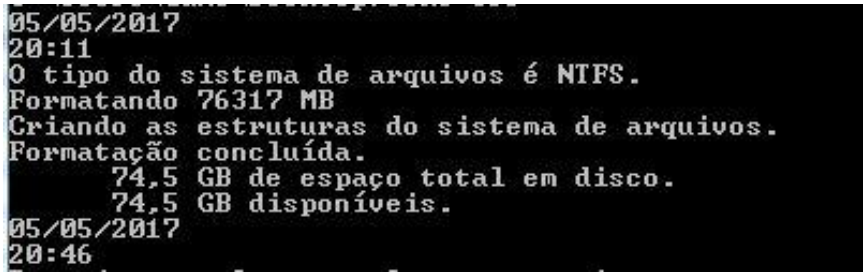
Figura 52: Formatação Rápida.



Fonte: Print Screen – Fonte do autor 05/2017

Formatação completa: Concluiu o processo em trinta e cinco minutos, conforme figura 53.

Figura 53: Formatação Completa.

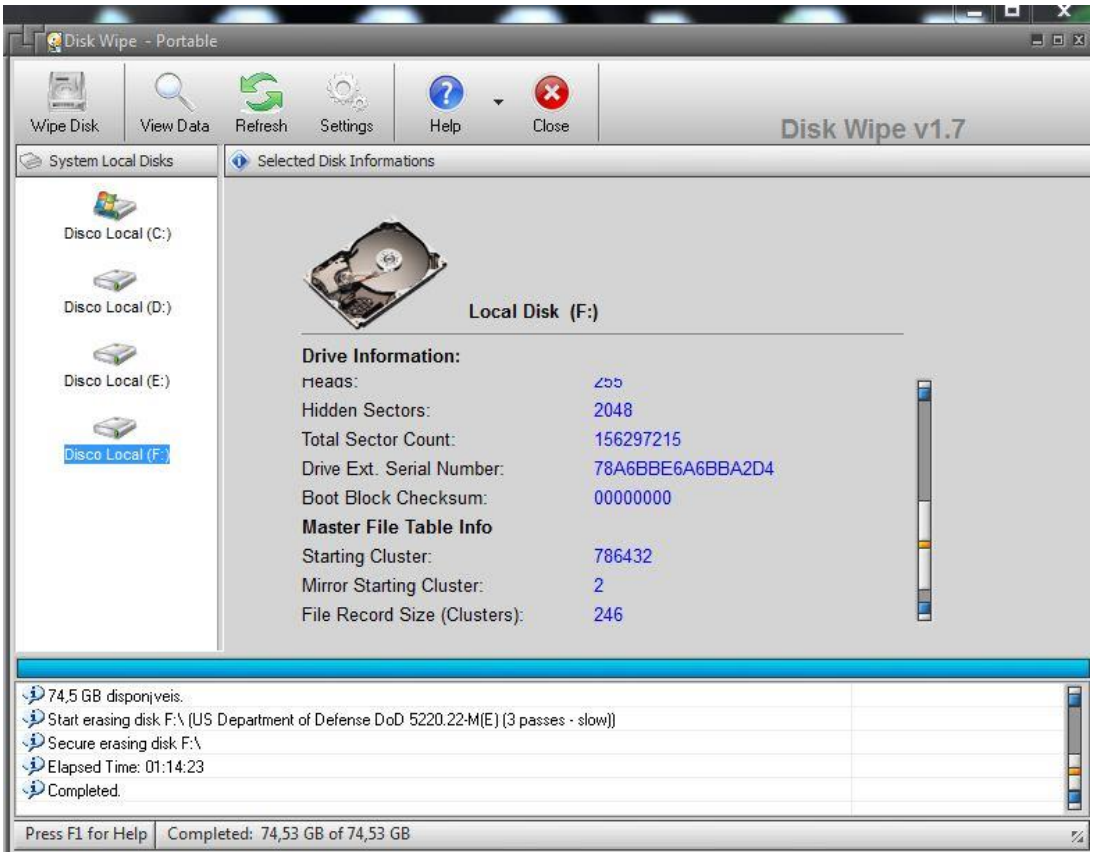


Fonte: Print Screen – Fonte do autor 05/2017

Formatação DoD (US Department of Defense): Para esse processo foram utilizados dois *softwares*, afim de comparações de tempo.

Primeiro *software* utilizado: Disk Wipe v1.7, usando método DoD 5220.22-M[E] 3 passos, concluiu o processo em uma hora e quatorze minutos, conforme figura 54

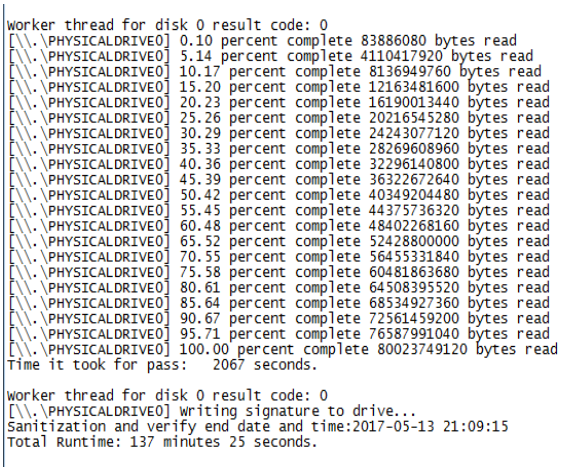
Figura 54: Formatação Disk Wipe DoD 5220.22-M[E].



Fonte: Print Screen – Fonte do autor 05/2017

Segundo *software* utilizado: HP Disk Sanitizer 2.3.0.1 usando método DoD 5220.22-M[E] 3 passos, concluiu o processo em duas horas e dezessete minutos, conforme figura 55.

Figura 55: Formatação HP Disk Sanitizer DoD 5220.22-M[E].



Fonte: Print Screen – Fonte do autor 05/2017

A tabela 1 demonstra os resultados obtidos nos testes.

Tabela 1- Resultados dos testes realizados

Método de Formatação	Tempo de Formatação HH:MM:SS	Recuperação GetDataBack	Tempo de Recuperação GetDataBack HH:MM:SS	Recuperação Recuva	Tempo de Recuperação Recuva HH:MM:SS	Recuperação Wondershare	Tempo de Recuperação Wondershare
Rápida	00:00:15	Sim	00:32:00	Sim	00:50:00	N/A	N/A
Completa	00:35:37	Não	00:42:00	Não	00:34:37	Não	00:40:00
Disk Wipe DoD 5220.22-M[E]	01:14:23	Não	00:47:00	Não	00:34:31	Não	00:42:15
HP Disk Sanitizer DoD 5220.22-M[E]	02:17:25	Não	00:46:00	Não	00:35:12	Não	00:42:17

Fonte: Arquivo pessoal do Autor 05/2017

CONSIDERAÇÕES FINAIS

Após a realização dos testes, a recuperação de dados mostrou-se possível quando um disco rígido não é tratado da maneira correta, ou seja, para que a informação não seja recuperada, deve-se realizar os procedimentos corretos com as ferramentas corretas.

A formatação rápida do Microsoft Windows 7, mostrou-se ineficaz para a exclusão dos dados, mostrando que até um simples usuário consegue realizar a recuperação dos dados utilizando-se de ferramentas encontradas na internet.

A recuperação de dados, após uma formatação completa, torna-se difícil de ser realizada por pessoas sem conhecimento ou sem as ferramentas adequadas, conforme mostrado nos testes. Essa recuperação não foi bem sucedida utilizando-se apenas de *softwares* de recuperação, devido a informação ser sobrescrita com bits zero após uma formatação completa do Windows, mas não a torna impossível, com equipamentos e ferramentas como grandes empresas de recuperação possuem. É possível fazer a recuperação dos dados, analisando resquícios de bits, porém isso exige muito tempo e equipamentos de valores altos, o que torna o custo dessa recuperação alto, além de que a informação possa não vir completa e obter apenas fragmentos da informação.

A formatação, utilizando o método *DoD (US Department of Defense)* é eficiente e deixa a informação impossível de ser recuperada, isso devido ao seu sistema de sobrescrita dos *bits* com valores aleatórios, o que impossibilita análise da existência anterior do BIT 1 ou 0 naquele setor. Esse método foi desenvolvido pela força militar dos Estados Unidos, e é utilizada por empresas para eliminação dos dados no descarte de seus computadores.Este é o método mais seguro para a eliminação completa dos dados.

A destruição do disco rígido, se não for completa, pode deixar vulneráveis os dados. Ao destruir apenas a parte eletrônica do disco rígido ou a parte mecânica sem danificar o disco (*platter*) é possível realizar a recuperação, ou seja, quando um disco apresenta problemas de leitura, se for descartado sem a destruição do *platter* pode ser recuperado.

As informações de uma empresa são vitais para sua existência, e devem ser protegidas. Às vezes há a preocupação no descarte de discos rígidos funcionando e não há preocupação com os que não estão funcionando, isso é uma falha no processo da empresa, pois como visto, é possível a recuperação dos dados partindo de um disco rígido inoperante.

A reutilização dos computadores com seus discos rígidos são viáveis desde que tratadas corretamente. Como analisado o tempo para o processo correto de limpeza dos dados não é exorbitante e, se adotados, podem gerar lucros e uma imagem positiva da empresa em relação ao meio ambiente e a solidariedade, isso com a garantia de que suas informações continuem protegidas, garantido-se a confidencialidade da informação para empresa.

REFERÊNCIAS

DESTRUCTDATA - **Department Of Defense (DoD) Media Sanitization Guidelines 5220.22M -** http://www.destructdata.com/dod-standard/ acessado em: 09/04/2017

GUANABARA, Gustavo - **A Evolução dos Discos Rígidos** - http://www.techtudo.com.br/platb/hardware/2011/01/06/evolucao-discos-rigidos-hd/- Acessado em:09/04/2017

HP - **HP Disk Sanitizer, External Edition -** http://h20564.www2.hp.com/hpsc/swd/public/detail?swItemId=vc_64697_1&swEnvOid=2096 - acessado em:09/04/2017

IBM –**IBM 350 disk storage init** - http://www-03.ibm.com/ibm/history/exhibits/storage/storage_350.html - Acessado em:09/04/2017

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício de; **Segurança de Redes em Ambientes Cooperativos - Fundamentos, Técnicas, Tecnologias, Estratégias**. Novatec Editora, 2007

MORIMOTO, Carlos E. - **Hardware, o Guia Definitivo**- http://www.hardware.com.br/livros/hardware/eliminando-dados-com-seguranca.html

NBR 27002:2005

PIRIFORM – **Recuva -** https://www.piriform.com/recuva - acessado em:13/05/2017

VASCONCELOS, Laércio. **Hardware na Prática**. 4a Edição, 2014, Laércio Vasconcelos Computação.

WONDERSHARE – **Wondershare Data Recovery -** https://www.wondershare.com.br/ad/data-recovery - acessado em:13/05/2017