UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

WILLIAN ANTUNES CRESCENCIO

MÉTODOS DE RECUPERAÇÃO DE DADOS EM DISCO RÍGIDO COM PARTIÇÃO NTFS

CRICIÚMA

2015

WILLIAN ANTUNES CRESCÊNCIO

MÉTODOS DE RECUPERAÇÃO DE DADOS EM DISCO RÍGIDO COM PARTIÇÃO NTFS

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA

2015

WILLIAN ANTUNES CRESCÊNCIO

MÉTODOS DE RECUPERAÇÃO DE DADOS EM DISCO RÍGIDO COM PARTIÇÃO NTFS

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Sistemas de Computação.

Criciúma, 26 de novembro de 2015

BANCA EXAMINADORA

Prof. Paulo João Martins – MSc. (UNESC) - Orientador

Prof. Sérgio Corrêa - Esp. - (UNESC)

Prof. Valter Blauth Junior - Esp. - (UNESC)

A meus pais que sempre estiveram a meu lado, assim como minha esposa, que sempre me apoiou a estudar.

AGRADECIMENTOS

Aos meus pais que me ensinaram verdadeiros valores da vida, auxiliando-me a traçar o meu caminho, contribuindo assim para minha formação acadêmica.

A meu orientador Prof. MSc. Paulo João Martins que sempre me direcionou de forma correta para que no final meu trabalho saísse da melhor forma possível.

A minha esposa que foi a pessoa que esteve ao meu lado nos últimos semestres dando apoio na conclusão do curso.

Por fim a meus pais, que sempre lutaram por um futuro melhor para mim.

RESUMO

A informação é composta de dados interpretados, dotados de relevância e propósito, sendo o insumo mais importante da produção humana. Mesmo com todos os mecanismos de proteção de dados existentes, podem ocorrer problemas de perda de informação. Desta forma, necessita-se conhecer mecanismos e procedimentos, para recuperação destas informações. Esse trabalho tem por propósito recuperar dados devido à perda de partição, formatação e eliminação de arquivos em discos rígidos com *New Technology Format System* (NTFS). Assim, como compreender sobre o funcionamento de sistemas de arquivos NTFS. Referente aos métodos, foi realizado pesquisa bibliográfica; elaborado um estudo de caso simulando a perda e recuperação de dados devido à perda de partição, formatação e eliminação de arquivos em discos rígidos com NTFS. Os resultados demostraram que o percentual de recuperação de dados devido a partição danificada foi de 93%, partição formatada 98% e eliminação permanente de arquivos foi de 100%. Assim, podemos concluir que foi possível recuperar a maioria dos dados, independente da origem de perda. Ademais, abordamos o funcionamento em baixo nível do sistema de arquivos NTFS e seu envolvimento na recuperação dos dados.

Palavra-chave: Informação; Recuperação de dados; NTFS; MBR; MFT.

ABSTRACT

The information is composed of interpreted data, endowed with relevance and purpose, being the input most important of human production. However, even with all data protection mechanisms existents may occur problems loss of information. Thus, needs to know mechanisms and procedures for recovery of this information. This work has the purpose to recover data due to partition loss, formatting and deleting files on hard disks with New Technology Format System (NTFS). As well as, to understand the functioning of NTFS file systems. Regarding methods, it was carried out bibliographical research; prepared a case study simulating the loss and recovery of data due to partition loss, formatting and deleting files on hard drives with NTFS. The results showed that the data recovery percentage due to damaged partition was 93%, formatted partition was 98% and permanent file deletion was 100%. Therefore, we can conclude that was possible to recover most of the data, regardless of the origin of loss. Furthermore, we approach the operation in low-level file system NTFS and its involvement in data recovery.

Keyword: Information; Data recovery; NTFS; MBR; MFT.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BPB	Bloco de Parâmetro do BIOS
CD	*Compact Disk*
DAS	*Direct Attached Storage*
DVD	*Digital Versatile Disc*
FAT	*File Allocation Table*
HD	*Hard Disk*
HPFS	*High Performance File System*
IDE	*Integrated Drive Electronics*
MBR	*Master Boot Record*
MFT	*Master File Table*
NAS	*Network Attached Storage*
NCQ	*Native Command Queuing*
NTFS	*New Technology Format System*
PBR	*Partition Boot Record*
RAID	*Redundant Array of Independent Disks*
SATA	*Serial Advanced Technology Attachment*
SMART	*Self-Monitoring, Analysis and Reporting Technology*
SSD	*Solid State Drive*
TI	Tecnologia da Informação
USB	*Universal Serial Bus*

SUMÁRIO

1 INTRODUÇÃO

As empresas e pessoas necessitam cada vez mais de informações, estas são fundamentais na descoberta e introdução de novas tecnologias, e se bem utilizadas na exploração de oportunidades e investimentos (BRAGA, 2000). Elas podem ser a combinação e processamento dos dados, gerando assim um significado (CHIAVENATO, 2003). Podem ser audíveis ou visíveis (DRUCKER, 1999).

A informação é de grande importância tanto para as pessoas como empresas, pois acessível, aumenta o conhecimento daquele que recebe, e o capacita no melhor desenvolvimento de determinadas atividades, na tomada de decisão, permitindo um maior desempenho em suas atividades (CARVALHO; PINA; SANTOS, 2000). Para as pessoas, ela pode representar tanto um simples aprendizado em determinadas tarefas do dia a dia, quanto ser um recurso estratégico para a obtenção de vantagem competitiva (BALLONI, 2006).

Elas são armazenadas em meios físicos e magnéticos. Algum tempo atrás o papel era o meio mais utilizado para armazenamento das informações, logo em seguida vieram os meios magnéticos e estes são utilizados até os dias de hoje. O que difere entre eles é a capacidade de armazenamento, velocidade de recuperação da informação e como os mesmos se conectam aos equipamentos (SOUZA et al, 2011).

Nos meios magnéticos, existem problemas como em qualquer outro, os mesmos são inseguros, podendo existir perda do conteúdo armazenado. Assim, para assegurar a não perda de informações, é necessário se ter uma política de segurança, pois, a informação é considerada o principal patrimônio de uma organização (BRASIL, 2012). As políticas de segurança são basicamente regras de conduta onde todos os envolvidos devem adequar-se integramente (MARCIANO; LIMA-MARQUES, 2006).

Mesmo com toda essa política existem perdas. São muitos os motivos que levam isto a acontecer. Perda ou roubo de laptops e dispositivos móveis, transferência não autorizada de dados para dispositivos Universal Serial Bus (USB), roubo de dados por funcionários ou estranhos, impressão e cópia de dados confidenciais, transmissão não intencional de dados confidenciais (EYGM, 2011, tradução nossa).

Estudos relatam que uma empresa que perde seus dados por até dez dias, tem cinquenta por cento de chance de fechar as portas nos próximos cinco anos (SMITH, 2003).

Este trabalho tem por objetivo demonstrar a possibilidade da recuperação de dados perdidos em discos rígidos que utilizam o sistema de arquivos *New Technology File System* (NTFS) a partir da perda da tabela de partição, formatação e exclusão de arquivos. Serão demonstrados por meio de um fluxograma os passos para efetuar o procedimento.

1.1 OBJETIVO GERAL

Recuperar dados devido à perda de partição, formatação e eliminação de arquivos em discos rígidos com NTFS.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa são:

a) compreender sobre segurança da informação;
b) aplicar os conceitos acerca dos tipos de perda de informação;
c) compreender sobre o funcionamento de sistemas de arquivos NTFS;
d) recuperar dados de perda de partição, formatação e eliminação de arquivos, por meio de alguns softwares;
e) documentar os testes realizados.

1.3 JUSTIFICATIVA

A informação em conjunto com recursos tecnológicos é uma necessidade para o funcionamento tático, estratégico e operacional de qualquer empresa. Para vencer no mundo dos negócios, é preciso saber obter a informação como ferramenta estratégica de competitividade. A informação nada mais é do que mensagens com dados que fazem diferença, podendo ser audível ou visível, e onde existe um emitente e um receptor. É o insumo mais importante da produção humana. São dados interpretados, dotados de relevância e propósito (DRUCKER, 1999). Empresas que desenvolvem uma administração da informação de maneira eficaz fazem parte do grupo de empresas de maior desempenho. Estas empresas

dominam a concorrência (LESCA; ALMEIDA, 1994). Assim, pode-se observar o quanto é importante para uma empresa a informação.

Pesquisa recente mostra que cerca de quarenta e três por cento das empresas brasileiras tiveram algum problema relacionado a segurança das suas informações (ULBRICH; VALLE, 2005). De outro lado, existe o usuário doméstico, que tem a necessidade de armazenar fotos, documentos pessoais, contábeis, entre outros. E caso ocorra perda destes dados pode ser prejudicial. Todavia, pode-se proteger as informações com algumas atitudes básicas tais como: *antispyware* e antivírus atualizados, controle de acesso lógico ou físico, criptografia, *firewall*, espelhamento, *backup*, entre outras formas (CONSELHO DA TECNOLOGIA DA INFORMAÇÃO, 2012). Entretanto, mesmo com todas estas providências, podem ocorrer problemas de perda de informação. Desta forma, necessita-se conhecer mecanismos e procedimentos, para recuperação destas informações.

Além de softwares que possam sanar os problemas de quem perdeu seus dados, existem empresas especializadas em recuperação de informações, o problema é o valor a ser pago que ainda não é acessível a todos. Devido a um volume cada vez maior de informações que se perde, este trabalho será executado para fim de auxiliar profissionais da área de tecnologia ou até mesmo pessoas com um nível intermediário de conhecimento em informática a recuperar seus dados perdido da seguinte forma, perda de partição, formatação e eliminação de arquivos. Demonstrando assim que nem sempre o que se perde, está perdido definitivamente. O sistema de arquivo utilizado será o NTFS utilizando Windows 7 em discos rígidos.

1.4 ESTRUTURA DO TRABALHO

A presente pesquisa está estruturada em nove capítulos da seguinte maneira:

O primeiro capítulo é a introdução, onde nela é descrita a definição do problema, objetivo geral, objetivos específicos e a justificativa do trabalho. No segundo capítulo é abordado o assunto acerca da informação, sua segurança e perda. O terceiro capítulo demonstra algumas características, funcionamento e defeitos dos discos rígidos. O capítulo quatro desenvolve o assunto NTFS, definições, e suas características. O quinto introduz sobre Softwares de recuperação de dados para, perda de tabela de partição, formatação e arquivos deletados. O

capítulo seis apresenta sobre trabalhos correlatos, falando de alguns trabalhos que tenha semelhança com este projeto. O sétimo capítulo aborda sobre procedimentos de recuperação de dados, ou seja, os estudos de caso, como ocorrem as perdas, como podem ser recuperados, como se pode proceder para evitar as perdas, tal como backup, ou outras coisas, como computação em nuvem, ou qualquer forma de proteger os dados. O oitavo e penúltimo capítulo emprega a conclusão do projeto. Por fim o nono e último capítulo contém toda a bibliografia relacionada ao trabalho proposto.

2 INFORMAÇÃO E SUA IMPORTÂNCIA

No Brasil, conforme a 23ª Pesquisa Anual do Uso de TI (2012) divulgada existe noventa e nove milhões de computadores em uso, incluindo os utilizados em corporações e residenciais (FGV, 2012). A mesma pesquisa compara o número de computadores por habitantes, e afirma que existe um para cada dois habitantes. Conforme cita, em 2018 o número de computadores deverá ser igual ao de habitantes (GUIMARÃES; SANTOS, 2012). Além dos computadores, os smartphones tiveram um crescimento acima de 47% em 2011 em relação ao mesmo período do ano de 2010 (GARTNER, 2012). Outra pesquisa realizada pelo Instituto Brasileiro de Geografia (2011), relata que entre 2005 e 2011, no Brasil cresceu mais de 100% o uso de celulares, elevando também o uso de internet em todas as faixas etárias (IBGE, 2011). Pode-se incluir também o uso de pen drives, discos rígidos externos, câmeras e todos os demais equipamentos que armazenam ou processam algum tipo de informação.

Somente no ano de 2014 a venda de *smatphones* cresceu 55% em relação ao ano anterior, foi vendido uma média de 104 aparelhos por minuto no Brasil (INTERNATIONAL DATA CORPORATION, 2015). Desse modo, pode-se observar o aumento do uso da tecnologia, que está presente cada vez mais na vida de todos.

2.1 INFORMAÇÃO

Devido ao volume de equipamentos de comunicação existentes atualmente a informação insere-se, de forma intensa na vida de todos (LESCA; ALMEIDA, 1994). Essa tem valor altamente significativo e pode representar grande poder para quem a possui, indivíduos ou instituições. A mesma está presente em todas as atividades que envolvem pessoas, processos, sistemas, recursos e tecnologia (REZENDE; ABREU, 2000). A informação é utilizada nas empresas como um grande trunfo em relação à concorrência. Em pequenas empresas a área de Tecnologia da Informação (TI) é utilizada como suporte à gestão da informação por meio de aspectos como: disponibilidade das informações para uma melhor tomada de decisão e gerenciamento estratégico do negócio. Assim, automatizando as tarefas de rotina, auxiliando no controle interno das operações, amplificando a

capacidade de reconhecimento antecipado dos problemas, sendo aplicada como ferramenta estratégica no processo de planejamento, direção e controle (MORAES; TERENCE; ESCRIVÃO FILHO, 2004).

Toda informação deve ser classificada e tratada conforme seu público-alvo. Cada parte da informação deve ser classificada em uma das seguintes categorias:

a) pessoal: Não pertencente à organização, é de privacidade pessoal;
b) pública: Destinada à distribuição, para visualização do público em geral;
c) confidencial: Para uso dos funcionários, fornecedores e parceiros de negócio;
d) intelectual: Pode ser manuseada exclusivamente por pessoas autorizadas;
e) secreta: Para uso restrito de pessoas designadas com a necessidade de saber (RHODES-OUSLEY, 2013, tradução nossa).

2.2 IMPORTÂNCIA DA INFORMAÇÃO

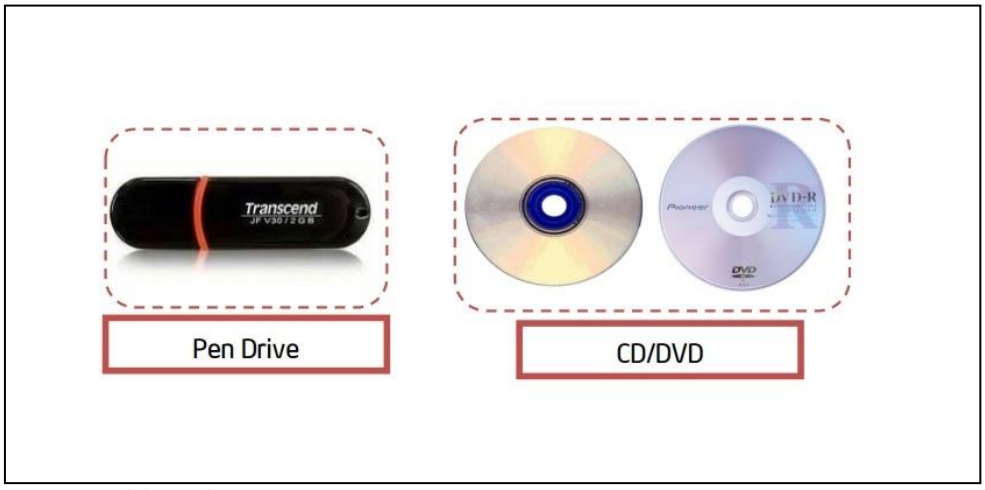
Como observado, a informação tem vários níveis de importância. Uma amostra de como a informação é importante foi a abertura de documentos secretos a respeito da Primeira Guerra Mundial. Pôde-se perceber que a causa da terrível catástrofe que poderia ter sido evitada foi a falta de comunicação entre as partes conflitantes, apesar da vasta quantidade de informação encontrada nesses documentos. Devido ao ocorrido, o mundo científico passou a atentar mais para a informação. Ela também ajuda uma corporação a determinar padrões, comparar o seu desempenho em relação aos padrões pré-estabelecidos (CHIAVENATO, 2003). Gestores estão em contato direto e contínuo com seus empregados, colaborando e compartilhando informações extraordinariamente ricas de forma quase instantânea. Devido ao crescimento dos sistemas de informação nas empresas, os gerentes estão tendo acesso *on-line* ás informações necessárias para as tomadas de decisões precisas e oportunas, compartilhando publicamente as mesmas por meio da Web, blogs e outras ferramentas *on-line* para o crescimento constante da corporação (LAUDON; LAUDON, 2011, tradução nossa). Quanto maior a quantidade de informações e de forma mais rápida elas chegam até as pessoas, maior as

chances de uma empresa conseguir vender seus produtos (RHODES-OUSLEY, 2013, tradução nossa).

2.3 ARMAZENAMENTO

As informações tão vitais para pessoas e empresas têm a necessidade de ser armazenadas em algum lugar. Desde o advento dos computadores, tem havido essa necessidade de armazenamento e/ou transferência permanentemente de dados entre dispositivos. Pode-se necessitar futuramente de arquivos ou imagens criadas hoje. Para isso, esses arquivos devem ser armazenados de forma segura em algum lugar. Da mesma forma, pode-se necessitar transferir um documento ou uma imagem digital para alguém conhecido. Há muitas maneiras de fazer isso *on-line* e *off-line*. Enquanto a transferência ou armazenamento de dados *on-line* requer o uso de Internet, o armazenamento *off-line* pode ser gerenciado com recursos mínimos. O único requisito neste caso seria um dispositivo de armazenamento. Com o desenvolvimento da tecnologia da informação, hoje existem pen drives, CDs, DVDs e outros dispositivos de mídia removível para armazenar e transferir dados. Com estes, é possível guardar, salvar, copiar arquivos e pastas que contêm dados, imagens, vídeos, áudios, entre outros a partir de um computador e até mesmo transferi-los para outro dispositivo. Estes são chamados dispositivos de armazenamento secundário. Para acessar as informações armazenadas nestes dispositivos, deve-se inseri-los em um computador e acessar os dados armazenados (INTEL, 2012).

Figura 1 – Dispositivos de armazenamento portátil

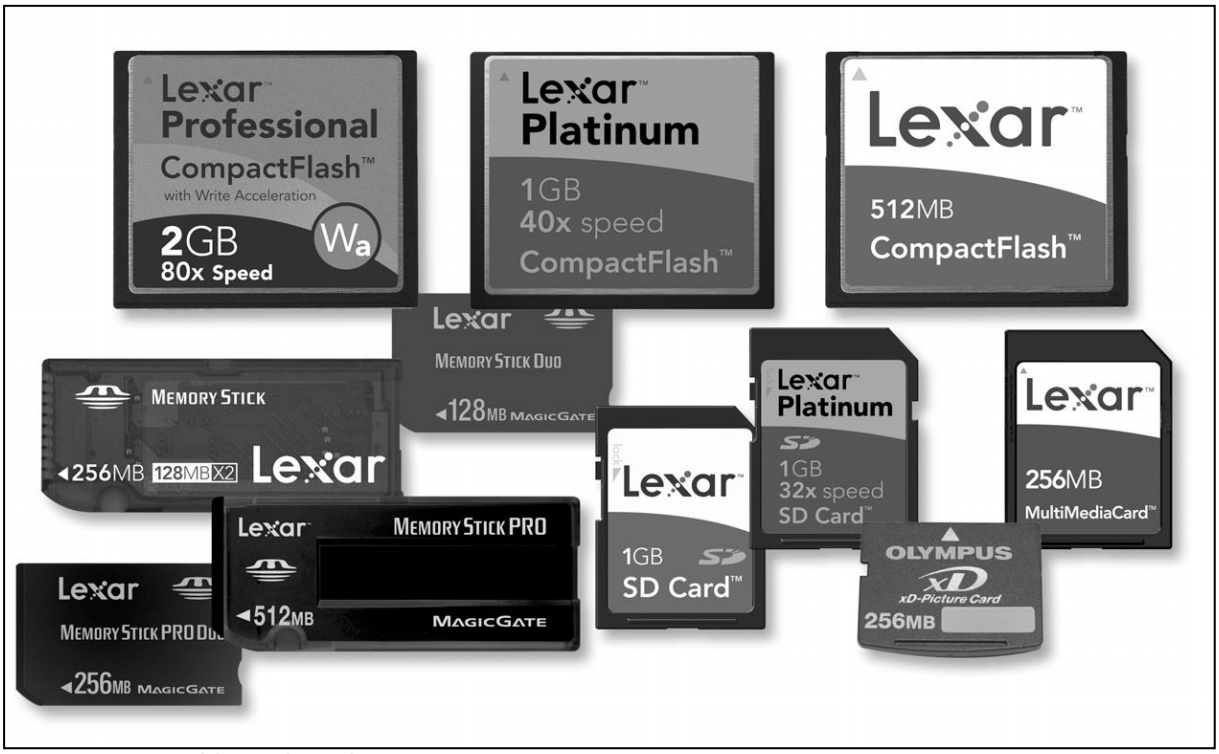


Fonte: Intel (2012).

Existem também o armazenamento conhecido com *Storage* que podem ser do tipo *Direct Attached Storage* (DAS), que são discos externos conectados diretamente em um servidor ou qualquer computador de uma rede (HARDWARE, 2007). *Network Attached Storage* (NAS) que diferentemente do DAS, roda um sistema operacional completo e funciona como um servidor de arquivos, ligado diretamente na rede (HARDWARE, 2007) e *Redundant Array of Independent Disks* (RAID), onde uma das características é o aumento da velocidade de leitura e gravação devido a possibilidade de dividir as tarefas entre vários discos ao mesmo tempo (TECMUNDO, 2009).

Os cartões de memória mais comumente conhecidos como *memory cards* são outros tipos de dispositivos muito utilizados, pois são estes que armazenam informações dentro de inúmeros dispositivos de pequeno porte, por serem de pequenas dimensões, leves e de alta capacidade de transferência (KARP; RATHBONE, 2005).

Figura 2 - Dispositivos de armazenamento de alta velocidade



Fonte: Karp; Rathbone (2005).

De forma similar ao funcionamento dos cartões de memória, porém sendo usados como memória de armazenamento principal, existem os discos sólidos com conexão *Serial Advanced Tecnology Attachment* (SATA), mais conhecidos como *Solid State Drive (SSD)*. Esta é a mais nova tecnologia até o momento. Estão entrando no mercado para a substituição gradativa dos discos rígidos. *Hard Disk* (HD) utilizam discos, e as suas ações mecânicas criam um atraso na leitura ou gravação de dados. SSD são desenvolvidos a partir de chips de memória de silício, não têm partes móveis, por isso não existe atraso de rotação, o tempo de busca é perto de zero, o que reduz drasticamente o tempo de resposta. Os SSD podem ser extremamente valiosos para aplicações que necessitam de alto desempenho. Em relação aos HD, a velocidade de trabalho é muito maior, porém o custo por gigabyte de armazenamento ainda é muito mais caro (DELL, 2011, tradução nossa).

Figura 3 – Dispositivos sólidos de armazenamento principal SSD

Fonte: Sandisk (2012).

Por fim existem os discos rígidos, que são os meios de armazenamento principais mais utilizados por computadores em geral, a popularidade deles continua até hoje, pois o avanço na tecnologia desses dispositivos está em constante crescimento, a capacidade de armazenamento que a tempos atrás era de cerca de 10 Megabytes de dados, o suficiente para armazenar um ou dois arquivos de música, hoje possuem milhares de vezes esta capacidade. Os discos rígidos podem ser encontrados de duas formas. Interno, sendo inserido dentro do gabinete e conectado através da conexão IDE ou SATA, e também externo, quando o disco vem dentro de uma caixa que se conecta no gabinete por meio da porta USB ou

fireware. Uma vez que está fora do gabinete, a unidade externa é muito mais fácil de ser instalada do que a unidade interna (KARP; RATHBONE, 2005). Esse meio de armazenamento é o escolhido a ser utilizado neste projeto.

Figura 4 - Dispositivos de armazenamento principal HDD

Fonte: Seagate (2009).

2.4 SEGURANÇA DA INFORMAÇÃO

Mesmo com toda a tecnologia desenvolvida em torno dos equipamentos de armazenamento, não existe nenhum deles a prova de perda de dados. Dentro das corporações a informação é tratada com muito cuidado e seriedade, independentemente da forma de armazenamento escolhida. Diante disso, ela necessita de segurança. Ela é quem garante a sobrevivência e prosperidade dentro de uma organização (SIQUEIRA, 2005). Já para o indivíduo, ela é importante, pois, é prejudicial perder dados de declaração de imposto de renda, senhas de acesso bancário, arquivos contábeis, comprovantes de pagamento *online,* trabalho de conclusão de curso ou até mesmo fotos de entes queridos que já se foram. Existem arquivos que são inestimáveis a cada indivíduo.

Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

Segurança das informações, nada mais é que a garantia da integridade, confidencialidade, autenticidade e disponibilidade das informações processadas. A integridade consiste na não violação dos dados no intuito de alterar, gravar ou

excluir esta informação acidentalmente ou não. A confidencialidade é a garantia de acesso ás informações somente por pessoas autorizadas. A autenticidade garante a veracidade da informação, pois por meio da autenticação se pode conhecer o autor da mesma. Já a disponibilidade das informações é a garantia de se ter acesso ás mesmas quando necessário, sem a interrupção do fornecimento destas (BRASIL, 2012). Além disso, existem outras características que devem ser respeitados em um sistema para que seja considerado seguro. Não repúdio, que assegura de forma convincente que uma transação ou evento especial tenha ocorrido ou não (LANDWEHR, 2014). Privacidade, quando a informação é utilizada com cuidado em relação às políticas de segurança, é mantida totalmente em sigilo, é a garantia que a informação não será divulgada para outras pessoas, de acordo com a política da empresa (LANDWEHR, 2014).

Em algumas empresas, o gerenciamento de segurança ainda tem muito a crescer, pois ainda nos dias de hoje existem empresas que tratam a segurança das informações como um gasto e não como um investimento, tanto que o envolvimento dentro da empresa em relação a esse assunto fica restrito somente ao setor de tecnologia, deixando de fora todos os outros setores da corporação, onde se quer existe treinamento adequado aos usuários desses setores. Um grande problema de segurança pode começar por uma ameaça de invasão sendo ela acidental ou intencional, com isso um sistema de segurança deve possuir características para prevenir, detectar e recuperar, caso haja alguma inconsistência. A prevenção vem a partir da utilização de proteção de hardware, impedindo acesso físico à infraestrutura da rede por pessoas não autorizadas evitando assim o roubo de dados, desligando os equipamentos em caso de já se estar fisicamente no local, utilizando autenticação, controle de acesso e sistemas de antivírus. Além de ferramentas como *firewall* e roteadores para proteger a rede contra tentativa de invasão sendo ela interna ou externa. A detecção é feita por meio de sistemas que alertam os responsáveis pela segurança a respeito de qualquer anormalidade na rede, outra forma utilizada é a auditoria de componentes críticos buscando mudanças duvidosas. Por fim a recuperação se faz por meio de cópias de segurança em mídias seguras, utilizando-se softwares de *backup* automático onde se é possível restaurar de forma rápida dados perdidos. Por fim podem-se ter equipamentos de reserva para o caso de alguma pane de hardware, substituindo imediatamente o equipamento danificado (PINHEIRO, 2007).

3 INTRODUÇÃO AO DISCO RÍGIDO

Um disco rígido magnético consiste em uma coleção de pratos ou discos que por meio de um motor, giram sobre um mesmo eixo de 5400 a 15000 rotações por minuto (RPM). O disco de metal é coberto por um material de gravação magnética dos dois lados, similar ao material encontrado em fitas cassete ou fita de vídeo. Para ler e gravar informações no disco é usado um braço móvel contendo uma pequena bobina eletromagnética chamada cabeça de leitura e escrita (PATTERSON; HENNESSY, 2013, tradução nossa).

Os braços com as cabeças movem-se em conjunto, de modo que elas são posicionadas sobre o mesmo ponto em cada superfície. Exceto para a parte superior e inferior, cada braço contém duas cabeças de leitura / gravação, que faz o serviço nas superfícies dos dois pratos adjacentes (ENGLANDER, 2009, tradução nossa).

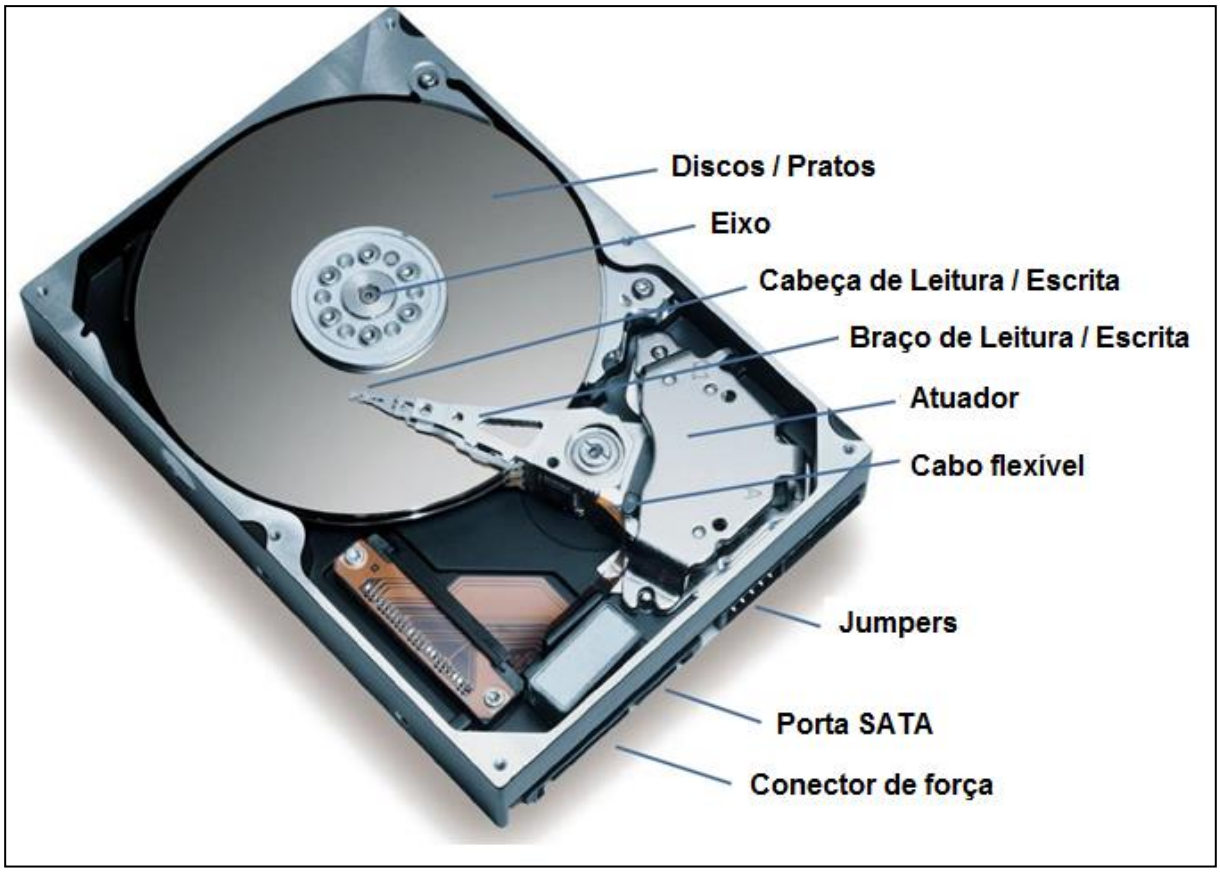
Toda a unidade está permanentemente selada para controlar o ambiente no interior da mesma, o que, por sua vez, permite que as cabeças de leitura e escrita dos discos estejam muito mais perto da superfície da unidade. (PATTERSON; HENNESSY, 2013, tradução nossa). Além disto, existe o atuador, que é quem movimenta o braço móvel de forma magnética para executar a busca ou escrita dos dados (ANDREWS, 2013, tradução nossa).

Com a cabeça em uma posição particular do disco, cria-se um círculo na superfície do disco com a rotação do mesmo, conhecido como trilha. O alinhamento de todas as trilhas onde encontram-se as cabeças de todos os pratos formam um cilindro. Cada trilha contém um ou mais blocos de dados. Na maioria dos discos a superfície é dividida em forma de torta com tamanho igual, essas divisões são conhecidas como setores. Cada setor em uma única faixa contém um bloco de dados, tipicamente de 512 bytes, o que representa a menor unidade que pode ser lida ou escrita de forma independente (ENGLANDER, 2009, tradução nossa).

O sistema operacional não possui a capacidade de operar de forma direta os setores, e sim um grupo sequencial de setores, todos os grupos sequenciais possuem a mesma quantidade de setores. Todas essas estruturas são definidas na formatação do disco, onde o controlador do disco se baseia para se movimentar e se localizar na superfície do disco (YAMAMOTO, 2004).

Na figura 5 está uma imagem interna de um disco rígido com identificação de suas partes mecânicas.

Figura 5 - Disco Rígido, visão interna



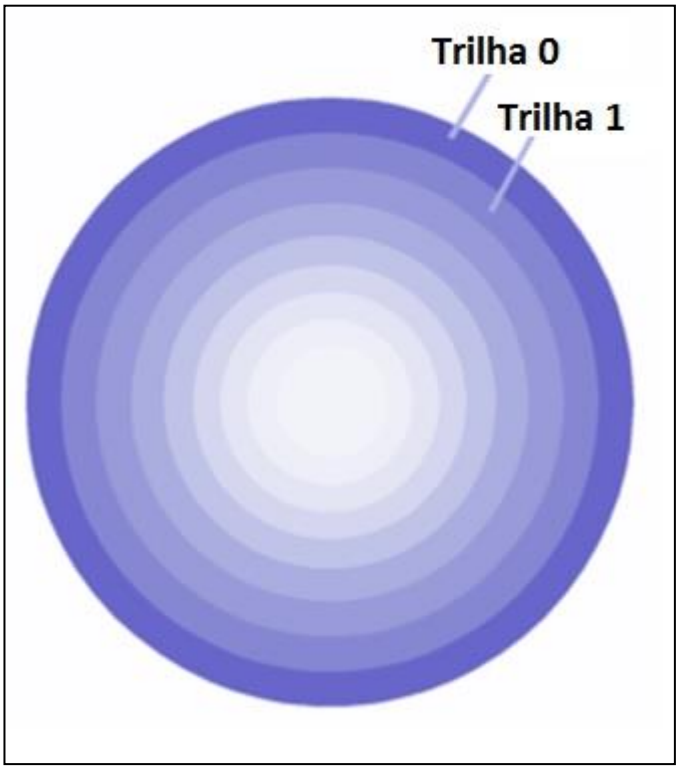
Fonte: Morimoto (2011).

3.1 PARTES DE UM DISCO RÍGIDO

Como dito, todos os discos independentemente da capacidade de armazenamento possuem trilhas, setores e cilindro.

Trilha é um anel circular que gira em torno do disco. É semelhante a uma faixa de pista de corrida de modo que se percorrer todo o circuito, deverá chegar de volta ao mesmo lugar que iniciou. A cada trilha no disco rígido é dado um endereço de fora para dentro, começando com 0. Por exemplo, se há 10.000 trilhas em cada disco, a trilha externa de cada disco será 0, e a trilha interna que é a mais próxima ao centro do círculo será 9.999. Devido ao *layout* de todos os discos ser sempre igual é dado o mesmo endereço a cada faixa (CARRIER, 2005, tradução nossa).

Figura 6 - Identificando as Trilhas

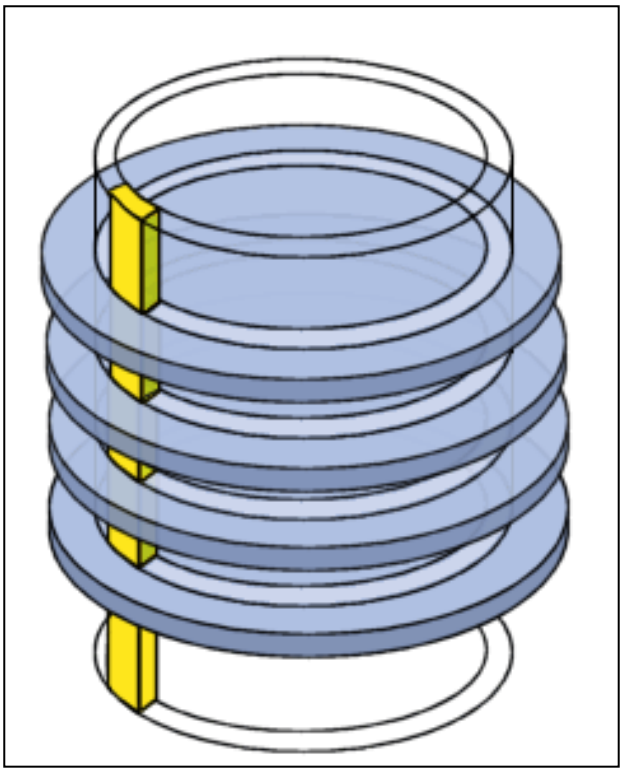


Fonte: Kioskea (2014).

Cada trilha é dividida em setores, que são a menor unidade de armazenamento endereçável no disco rígido e possuem normalmente 512 bytes. Cada setor tem um endereço, iniciando a partir de 1 para cada trilha. Portanto, pode-se encontrar um setor específico usando o endereço do cilindro para obter a trilha, o número da cabeça para obter o disco e lado, e o endereço do setor para obter o setor exato dentro da trilha (CARRIER, 2005, tradução nossa).

Cilindro é o termo usado para descrever todos os dados que se encontram na mesma trilha de todos os discos conforme a figura 7 (CARRIER, 2005, tradução nossa).

Figura 7 - Demonstração de um Cilindro



Fonte: Kioskea (2014).

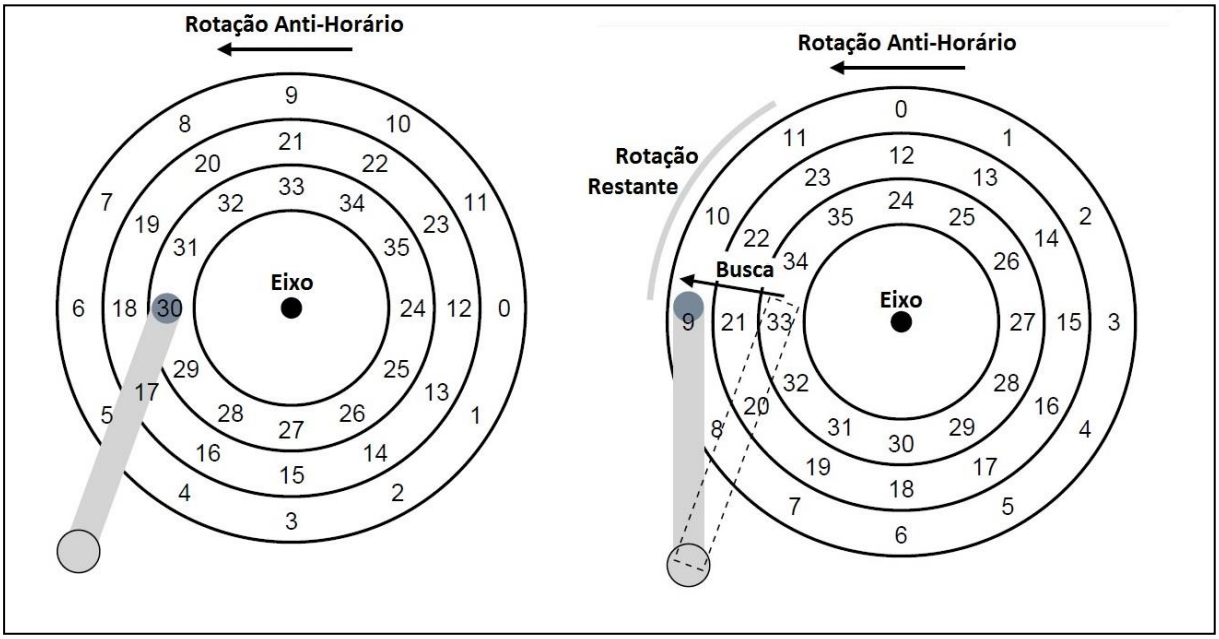
3.2 FUNCIONAMENTO DO DISCO

Em um disco rígido os setores são enumerados de 0 até n-1, onde n é o número total de setores dentro do disco. Muitos sistemas operacionais leem ou escrevem 4 *kilobytes* de cada vez, mesmo cada cluster vindo de fábrica com a capacidade de 512 bytes (ARPACI-DUSSEAU; ARPACI-DUSSEAU, 2014, tradução nossa).

Na sequência está a demonstração dos passos seguidos pelo mecanismo do disco para executar a busca ou escrita de uma informação dentro do mesmo. Conforme a imagem à esquerda na figura 8, a cabeça de leitura/escrita está posicionada na trilha mais interna estando os setores 24 ao 35. A pesquisa neste exemplo será feita no setor 11 que está posicionado na trilha mais externa. Uma busca de dados dentro do disco possui várias fases, primeiro é a fase de aceleração para que o braço de leitura se movimente, até chegar a sua velocidade máxima, então ele desacelera até parar em cima da trilha onde se encontra o cluster a ser lido, conforme a imagem da direita abaixo. Como pode-se observar, durante a busca, o braço foi deslocado para a trilha desejada que neste caso foi cerca de três setores e o disco continua girando. Já na trilha certa o braço espera o setor 11

chegar para fazer a leitura ou escrita no mesmo, concluindo assim um trabalho (ARPACI-DUSSEAU; ARPACI-DUSSEAU, 2014, tradução nossa).

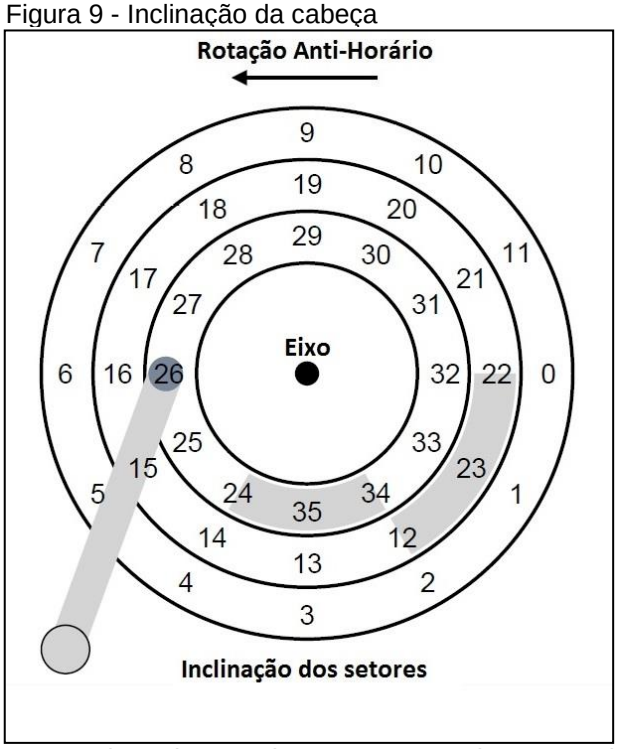
Figura 8 – Executando busca de dados



Fonte: Adaptado Arpaci-Dusseau; Arpaci-Dusseau (2014, tradução nossa).

Existem alguns outros detalhes interessantes sobre como discos rígidos operam. Muitas unidades empregam algum tipo de inclinação dos setores das trilhas para se certificar de que leituras sequenciais podem ser devidamente atendidas, mesmo quando cruzar limites de trilhas (ARPACI-DUSSEAU; ARPACI-DUSSEAU, 2014, tradução nossa). A imagem abaixo mostra esta inclinação, que nada mais é do que o atraso do início dos setores da trilha seguinte em relação ao início dos setores da trilha anterior.

Figura 9 - Inclinação da cabeça



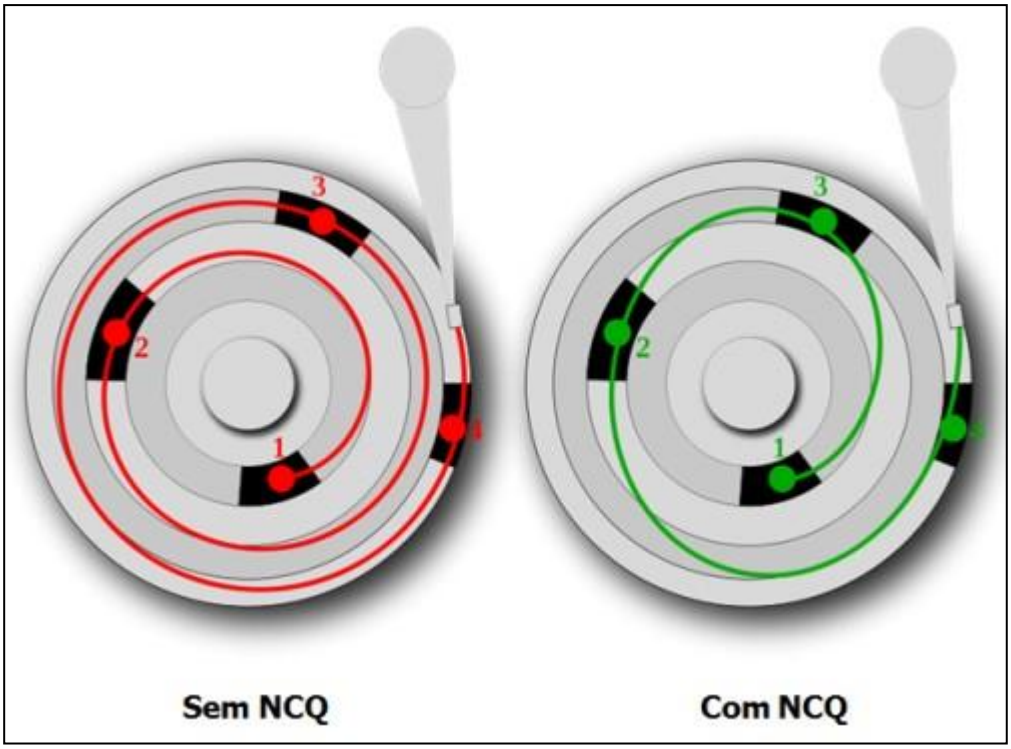
Fonte: Adaptado Arpaci-Dusseau; Arpaci-Dusseau (2014, tradução nossa).

Como se observa na imagem acima, os setores “0”, “12” e “24” são nesse exemplo os setores que iniciam cada trilha, esses setores são frequentemente distorcidos, porque quando se muda de uma faixa para outra, o disco precisa de tempo para reposicionar a cabeça, mesmo com faixas vizinhas. Sem essa inclinação, a cabeça seria transferida para a próxima faixa, mas o próximo bloco desejado já teria rodado sob a cabeça, e, assim, a unidade teria que esperar quase todo o atraso de rotação para acessar o próximo bloco (ARPACI-DUSSEAU; ARPACI-DUSSEAU, 2014, tradução nossa).

Hoje os discos SATA II e III possuem a tecnologia de enfileiramento de comando nativo. Os algoritmos usados nos discos com *Native Command Queuing* (NCQ) agendam o próximo comando a ser executado com base no menor tempo necessário para alcançar o setor de destino associado, em vez de agendar os comandos com base na ordem em que eles foram recebidos. Isto pode resultar em um tempo médio de busca significativamente reduzido, proporcionando um aumento significativo no desempenho do disco, alguns testes informam que o desempenho de uma unidade de 7.200 rpm com NCQ é aproximadamente equivalente ao de uma unidade com padrão de 10.000 rpm (ANDERSON, 2007, tradução nossa).

Pode-se observar o funcionamento da busca em discos que possuem e que não possuem a tecnologia NCQ na figura 10.

Figura 10 - Com e sem NCQ



Fonte: Morimoto (2011).

Porém, não só de boas notícias vive a tecnologia, embora exista o avanço dos discos rígidos, há o outro lado da moeda, as falhas.

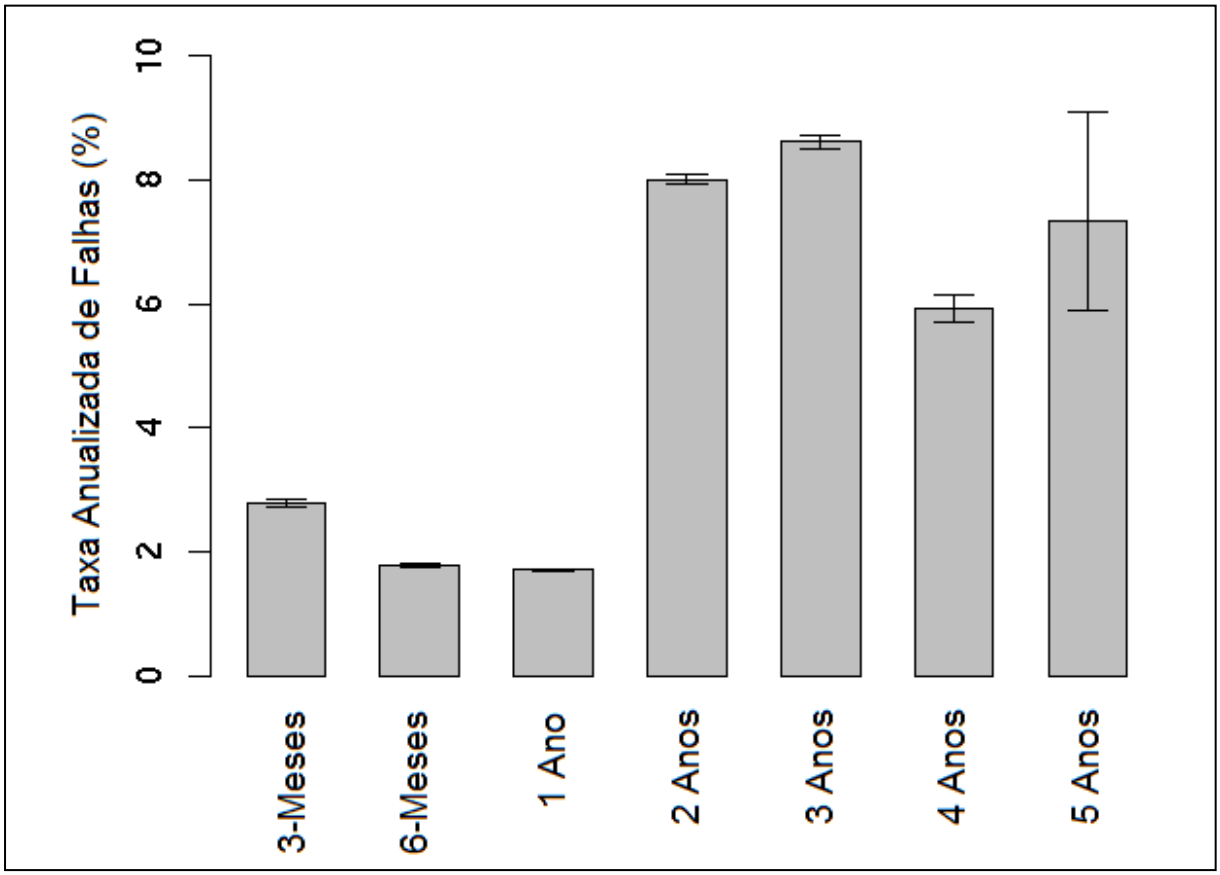
3.3 FALHAS EM DISCOS RÍGIDOS

O grande avanço em discos rígidos de baixo custo e alta capacidade estão entre os principais fatores que ajudam a estabelecer uma sociedade moderna profundamente dependente de tecnologia da informação. Discos rígidos de alta capacidade de armazenamento são produtos tão bem-sucedidos que são utilizados desde computadores pessoais até mesmo em fazendas de servidores. Em 2002, estima-se que mais de 90% de toda a nova informação produzida foi armazenado em mídia magnética, a maioria em unidades de disco rígido. Portanto, é fundamental para melhorar a compreensão de todos o quão robustos esses componentes são e quais os principais fatores estão associados a falhas. Tal entendimento pode ser particularmente útil para orientar no desenvolvimento de sistemas de

armazenamento, bem como elaboração e implantação de estratégias de manutenção (PINHEIRO; WEBER; BARROSO, 2007, tradução nossa).

Apesar da importância dos discos rígidos, há muito poucos estudos publicados sobre as características de falha dos mesmos. A maioria das informações disponíveis vêm dos próprios fabricantes. Um estudo sobre a *Annualized Failure Rates* (AFR) que significa a taxa de falhas no período de um ano, demonstra um gráfico onde pode-se observar em qual momento da vida útil de um disco ocorre uma maior incidência de falhas, independentemente do motivo, marca capacidade de armazenamento ou modelo. O intervalo observado de taxa anualizada de falhas varia de 1,7%, para os discos com menos de um ano de operação, chegando a mais de 8,6%, àqueles que possuem entre 3 e 5 anos (PINHEIRO; WEBER; BARROSO, 2007, tradução nossa).

Figura 11 - Taxa Anualizada de Falhas

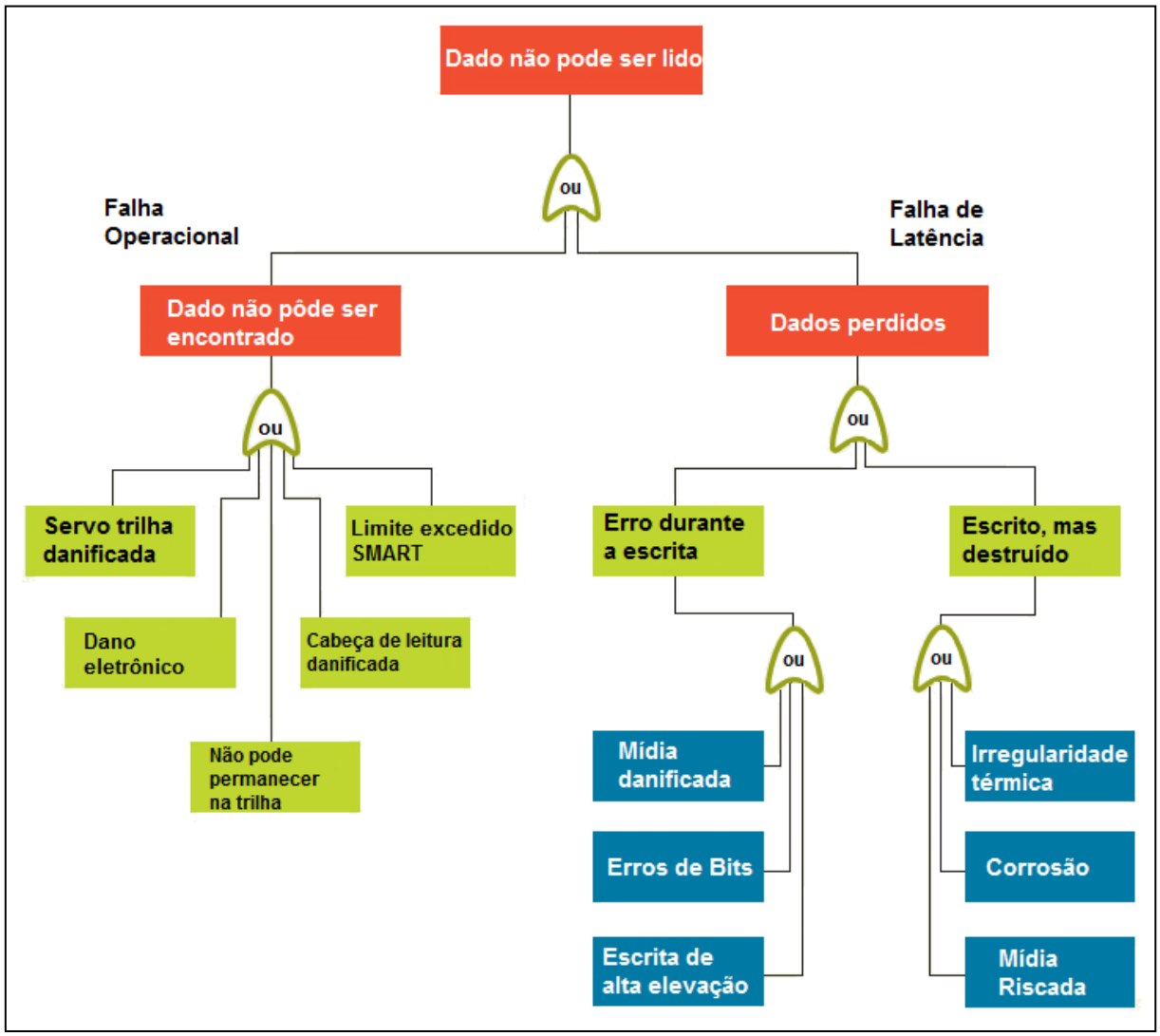


Fonte: Adaptado Pinheiro; Weber; Barroso (2007, tradução nossa).

As falhas em disco podem ser divididas em duas categorias principais. Falha que paralisam o disco e a falha onde o disco permanece em funcionamento,

porém, corrompe os dados. Cada uma dessas categorias tem causas, probabilidades, e efeitos significativamente diferentes. O primeiro tipo é a falha operacional, fácil identificação e baixa ocorrência, já o corrompimento de dados ou defeito oculto não são descobertos até que os dados sejam lidos. A Figura 12 é uma árvore de falhas que demonstra as duas razões básicas pelo qual os dados não podem ser lidos em um disco (ELERATH, 2007).

Figura 12 - Árvore de falhas



Fonte: Adaptado Elerath (2007, tradução nossa).

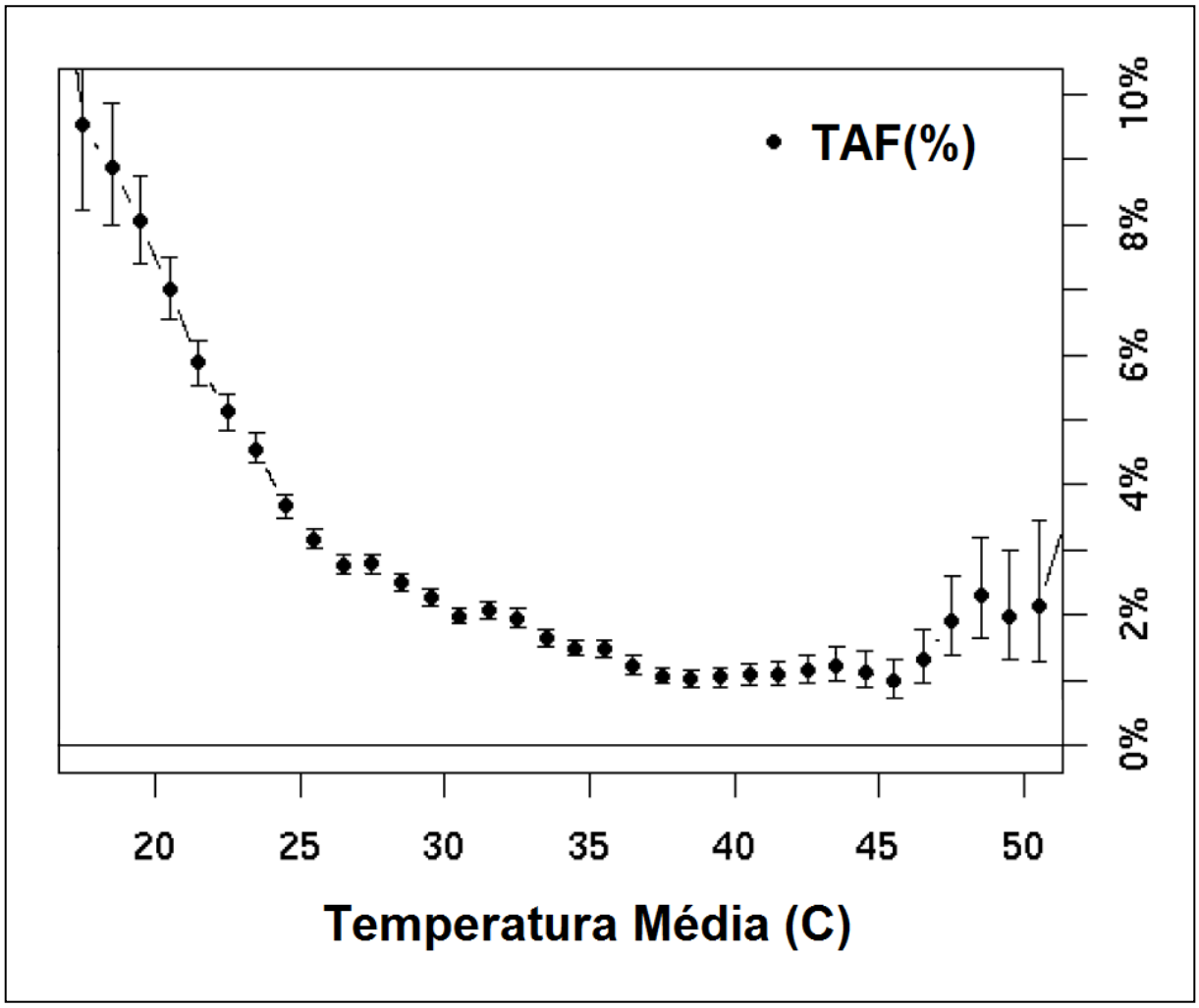
Além de todas as falhas citadas, existe um fato que pesa quanto a longevidade de um disco rígido, a temperatura.

3.3.1 Temperatura

A temperatura é frequentemente citado como o mais importante fator de confiabilidade ambiental que afeta unidade de disco. Um estudo fez leituras de

temperatura a partir dos registros do *Self-Monitoring, Analysis and Reporting Technology* (SMART) minuto a minuto durante um período de nove meses de observação, tentando entender a correlação entre os níveis de temperatura e taxas de insucesso. Foram adicionadas leituras de temperatura em várias maneiras diferentes, incluindo médias, valores máximos, fração de tempo gasto acima de um determinado valor de temperatura, número de vezes que um limite de temperatura é ultrapassado, e última temperatura antes da falha. Foi observado a correlação entre a temperatura média durante o período de observação e fracasso. A Figura 13 mostra a distribuição de unidades com a temperatura média em incrementos de um grau e as taxas de falhas numa base anual correspondentes. A figura mostra que as falhas não aumentam quando a média de temperatura aumenta. Na verdade, há uma tendência clara, mostrando que as temperaturas mais baixas estão associadas com taxas de insucesso mais elevadas. Apenas em temperaturas muito altas há uma ligeira inversão desta tendência.

Figura 13 - Temperatura X Taxa de falhas



Fonte: Adaptado Pinheiro (2007).

4 NEW TECHNOLOGY FORMAT SYSTEM - NTFS

Como proposto no projeto, o Sistema Operacional escolhido para execução será o Windows 7, pelo simples motivo de no momento ser o Sistema Operacional mais utilizado em computadores no mundo (NETMARKETSHARE, 2015, tradução nossa).

O Windows possui vários tipos de formatos de sistemas de arquivo, *File Allocation Table* (FAT)12, FAT16, FAT32 e também o mais utilizado sistema de arquivos até então, o NTFS (COURSE, 2010, tradução nossa).

Um sistema de arquivos é uma parte do sistema operacional que determina como os arquivos são nomeados, armazenados e organizados em um volume. Um sistema de arquivos gerencia arquivos, pastas e as informações necessárias para localizar e acessar esses itens pelos usuários locais e remotos (MICROSOFT, 2003, tradução nossa).

4.1 UMA BREVE HISTÓRIA DO NTFS

Microsoft e IBM uniram forças no início dos anos 1990 em um projeto para que culminava na criação de um poderoso sistema operacional, o OS/2. Eventualmente as empresas divergiram e com isso a Microsoft saiu do projeto, começando naquele momento a trabalhar em outro, o Windows NT. Pegou conceitos chave do sistema de arquivos nativo do OS/2, chamado de *High Performance File System* (HPFS), assim surgiu o sistema de arquivos NTFS (SAMMES; JENKINSON, 2007).

O NTFS foi originalmente criado para resolver as deficiências do sistema de arquivos FAT, especificamente para suportar grandes arquivos e grandes discos, para garantir a segurança de arquivos, reduzir o tempo de acesso, e fornecer capacidade de recuperação (ENGLANDER, 2009, tradução nossa).

O desenvolvimento do NTFS continuou durante toda a sua utilização com o Windows NT. A versão mais comum, originalmente apelidada NTFS 1.1, é mais comumente conhecida como NTFS 4 pelo motivo de seu lançamento ter sido com o Windows NT4. No típico estilo Microsoft, a versão seguinte do NTFS foi lançada com

um novo sistema operacional. Este sistema operacional não foi chamado Windows NT5, mas sim Windows 2000. O novo sistema de arquivo foi nomeado oficialmente de NTFS 5. Possuía alguns novos elementos dentro dele, como o serviço *Active Directory* que facilita o controle e exibição dos recursos de rede, pontos de nova análise, jornais de mudanças, criptografia de pastas e arquivos além de suporte a arquivos esparsos. Com o lançamento do Windows XP, a Microsoft deixou claro sua intenção de dar preferência ao sistema de arquivos NTFS. Os usuários que compraram novos sistemas encontravam-se coagidos a instalar FAT32 no lugar do NTFS, já que o sistema de arquivos padrão do Windows XP é NTFS, sem qualquer escolha aparente. FAT32 pode ser forçado como uma opção apenas se um sistema FAT estiver presente no disco rígido antes da instalação do sistema operacional Windows XP ser iniciada. Os usuários normais não sabem como criar a disposição desta escolha. Como resultado, o uso doméstico do sistema de arquivos NTFS está aumentando exponencialmente (SAMMES; JENKINSON, 2007, tradução nossa).

4.2 ALGUMAS CARACTERÍSTICAS DO NTFS

O NTFS tem uma série de funcionalidades que não estão disponíveis aos usuários de sistema de arquivos FAT. Algumas delas são:

Confiabilidade e resiliência. Embora seja discutível que isto foi conseguido, particularmente entre aqueles que têm sofrido com a perda de dados em um sistema NTFS, a Microsoft tem feito esforços no âmbito do novo sistema para redução na perda de dados e melhorar a capacidade de recuperação quando o sistema falhar ou sofrer com um desligamento repentino (SAMMES; JENKINSON, 2007, tradução nossa).

Comprimento do nome de arquivos e pastas. O *Disk Operating System* - DOS e Windows originais foram restritos a um máximo de 8 caracteres de comprimento, um separador de ponto e uma extensão de até 3 caracteres, tendo como exceção esses especiais entre parênteses (."/\[]:;|=,). O NTFS, por outro lado, permite que se tenha nomes e extensões de arquivos e pastas em um total de 255 caracteres, tendo como exceção os seguintes (?"/\<>*|:) (SAMMES; JENKINSON, 2007, tradução nossa).

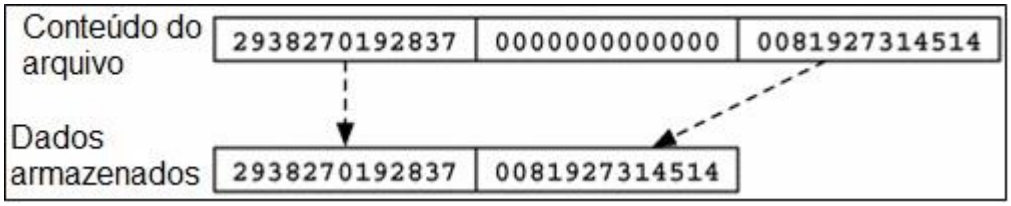
Controle de acesso e segurança. Uma grande falha dos sistemas FAT é a falta de qualquer instalação de segurança em nível de arquivo. Um exemplo, quem

tem e quem não tem acesso a determinados arquivos. NTFS inclui o controle de acesso em nível de arquivo, e também permite a implementação de controle de acesso de nível superior por grupos de usuários (SAMMES; JENKINSON, 2007, tradução nossa).

Rastreamento de link distribuído. Mantém a integridade de atalhos e links *Object Linking and Embedding* (OLE). Pode-se renomear arquivos de origem, movê-los para volumes NTFS em computadores diferentes dentro de um Windows Server 2003 ou domínio do Windows 2000 ou alterar o nome do computador ou nome da pasta que armazena o alvo sem quebrar o atalho ou vínculos OLE (MICROSOFT, 2003, tradução nossa).

Arquivos esparsos. Na maioria das vezes, os aplicativos armazenam arquivos enormes no disco, geralmente compostos por poucos dados e muitos zeros representando o espaço ainda disponível na base de dados. NTFS gerencia arquivos esparsos por rastrear o ponto de início e fim do arquivo esparso, assim como seus dados úteis (não-zero). O espaço não utilizado em um arquivo esparso é disponibilizado como espaço livre no disco (MICROSOFT, 2003, tradução nossa). Na figura 11 é possível visualizar o conteúdo de um arquivo e o que realmente está sendo armazenado, sendo retirado de uso aquele que não possui informação.

Figura 14 - Arquivos esparsos



Fonte: Adaptado Carrier (2005, tradução nossa).

Jornal de Mudanças. Fornece um *log* que possui todas as alterações executadas nos arquivos de um volume. O NTFS mantém o jornal de mudanças sobre arquivos adicionados, excluídos e modificados para cada volume (MICROSOFT, 2003, tradução nossa).

Hard links. Ligações com base NTFS para um arquivo em um volume NTFS. Com a criação de ligações fortes, pode-se ter um único arquivo em várias pastas sem duplicar o arquivo, colocando somente os atalhos. Pode-se também criar várias ligações fortes para um arquivo em uma pasta, se for utilizar nomes de

arquivos diferentes para as ligações fortes. Porque todos as ligações fortes referenciam ao mesmo arquivo, os aplicativos podem abrir qualquer uma das ligações fortes e modificar o arquivo (MICROSOFT, 2003b, tradução nossa).

Sistema de Arquivos Criptografados (EFS). Este sistema de arquivos armazena os arquivos de forma criptografada em NTFS para garantir a confidencialidade dos dados. Funciona como parte complementar do NTFS, a criptografia de chave pública é usada para criptografar os arquivos. Essa criptografia torna praticamente impossível para descriptografar o arquivo sem a chave correta. Arquivos e pastas são criptografados com um atributo. Quando os arquivos são copiados para outro sistema de arquivos, os arquivos criptografados são descriptografados e copiado (COURSE, 2010, tradução nossa).

Compactação de arquivo e pasta: Só está disponível se for escolhido NTFS como sistema de arquivos, essa opção compacta automaticamente todos os arquivos e pastas na unidade. Isso economiza espaço em disco, mas há uma sobrecarga de desempenho mínimo para a compressão / descompressão na unidade utilizada. Ainda pode-se comprimir arquivos e pastas individuais, se for deixado essa opção desmarcada (BOYCE; TIDROW, 2013, tradução nossa).

Networking: A Microsoft observou que a rede de computadores se tornaria uma área muito importante dentro da informática. Devido a isso, esse sistema de arquivos foi desenvolvido para funcionar muito bem em rede, sendo muito funcional para trabalho e fluxo de dados por meio desta.

4.3 FUNCIONAMENTO DO SISTEMA OPERACIONAL

Para minimizar a perda de dados em caso de uma interrupção inesperada do sistema ou falha, um sistema de arquivos deve garantir em todos os momentos a integridade de seus metadados proteger dados confidenciais contra acesso não autorizado. Deve também possuir um modelo de segurança integrada, permissão baseada em software, redundância de dados como uma alternativa de baixo custo para soluções de hardware redundante protegendo assim os dados do usuário (RUSSINOVICH; SOLOMON; IONESCU, 2012, tradução nossa).

NTFS é baseado em um banco de dados relacional. Esta é *a Master File Table* (MFT). Todos os objetos armazenados no volume são considerados arquivos, exceto o *Partition Boot Record* (PBR). Uma MFT contém detalhes de cada arquivo

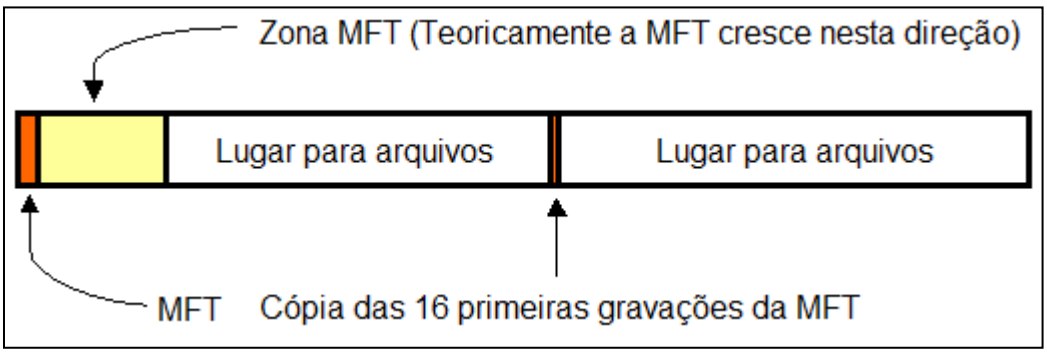
no volume, incluindo os arquivos de gerenciamento que são utilizados para o sistema de arquivo. Uma área considerável do volume está reservada para a MFT para evitar que torne-se fragmentada, uma vez que cresce em tamanho. Esta área, por padrão possui cerca de 12,5% do tamanho do volume e é conhecida como a zona reservada da MFT (SAMMES; JENKINSON, 2007, tradução nossa).

Quando um computador é baseado em BIOS, o primeiro código que ele executa é chamado de BIOS, que é codificado na memória do computador. O BIOS seleciona um dispositivo de boot, lê o *Master Boot Record* (MBR) desse dispositivo na memória e transfere o controle para o código no MBR (RUSSINOVICH; SOLOMON; IONESCU, 2012, tradução nossa).

Em primeiro lugar, o código de um MBR verifica a tabela de partição primária até localizar uma partição que contém um sinalizador setado como Ativo que indica a partição como sendo inicializável. Quando a MBR encontra pelo menos uma sinalizada, ela lê o primeiro setor da partição marcada na memória e transfere o controle para o código dentro da partição. Este tipo de partição é chamado de partição do sistema, e o primeiro setor desta encontra-se o setor de inicialização (RUSSINOVICH; SOLOMON; IONESCU, 2012, tradução nossa).

Para uma maior segurança, o sistema possui em algum lugar na partição o espelho da tabela de arquivos mestre. A MFT tem um número muito grande de entradas. De fato, muitos arquivos pequenos são totalmente armazenados na MFT. A parcela remanescente de grandes arquivos é armazenada na área de dados do sistema de arquivos ou File System Data, que compõe a maior parte da partição. A partir deste esquema, pode-se ver que o NTFS parte do FAT, adaptado ao gigantesco (para os padrões de uma década atrás) tamanhos de disco e volume de dados. Uma cópia da tabela de arquivos mestre armazena as quatro primeiras entradas do sistema (ou da MFT), a fim de reparar o sistema de arquivos, caso um bloco de disco apresentar problema (SCHWARZ, 2007, tradução nossa).

Figura 15 - Tabela de Arquivos Mestre



Fonte: Adaptado EaseUs (2015a)

4.3.1 Arquivos de metadados

O sistema de arquivos propriamente dito depende de uma série de arquivos de gestão, conhecidos como arquivos de metadados, que são arquivos contendo informações sobre o volume em si mesmo. Os metadados são usados para descrever a MFT. Esses arquivos são invisíveis para o usuário e gerenciam a partição em termos de alocação de espaço de armazenamento, identificação de espaço disponível, informações de recuperação e descrições do arquivo disponível, conhecidos como atributos. O NTFS reserva os 16 primeiros bytes da MFT para arquivos de metadados e também a própria MFT que por sua vez armazena as informações necessárias para a recuperação da partição caso ocorra um dano. A MFT é o primeiro arquivo em um volume NTFS e contém informações sobre todos os arquivos e pastas do volume. A primeira informação é sobre o setor de inicialização da partição, que começa no setor zero (MICROSOFT; COURSE, 2003a tradução nossa; 2010, tradução nossa).

A tabela 1 mostra a MFT com a função de cada campo reservado.

Tabela 1 - Tabela de Arquivos Mestre

Sistema de Arquivos	Nome do Arquivo	Registro MFT	Propósito do arquivo
Tabela de Arquivos Mestre – MFT	$Mft	0	Contém um registro de arquivo base para cada arquivo e pasta em um volume NTFS. Se as informações de alocação para um arquivo ou pasta é muito grande para caber dentro de um único registro, outros registros de arquivo são alocados também.
Espelho da Tabela de Arquivos Mestre – MFT	$MftMirr	1	Garante o acesso à MFT no caso de uma falha de um único setor. É uma imagem duplicada dos quatro primeiros registros da MFT.
Arquivo de Log	$LogFile	2	Contém informações usadas pelo NTFS para recuperação mais rápida. O arquivo de log é usado pelo Windows Server 2003 para restaurar a consistência dos metadados para NTFS depois de uma falha do sistema. O tamanho do arquivo de log depende do tamanho do volume, mas você pode aumentar o tamanho do arquivo de log

			usando o comando Chkdsk.
Volume	$Volume	3	Contém informações sobre o volume, tais como o nome do volume e a versão do volume.
Attribute definitions	$AttrDef	4	Listas de atributos. Nomes, números e descrições.
Root file name index	.	5	A pasta raiz.
Cluster bitmap	$Bitmap	6	Representa o volume, mostrando clusters livres e não utilizados.
Boot sector	$Boot	7	É usado para montar o volume NTFS durante o processo de inicialização.
Arquivo de Clusters danificados	$BadClus	8	Contém uma lista dos clusters que têm erros irrecuperáveis.
Arquivos de Segurança	$Secure	9	Contém descritores de segurança exclusivos para todos os arquivos dentro de um volume.
Tabela de Caracteres Maiúsculos	$Upcase	10	É usado para converter todos os caracteres maiúsculos em caracteres Unicode minúsculos.
Extensão de arquivos NTFS	$Extend	11	Extensões opcionais como, citações e identificadores de objetos, são listados aqui.
		12	Reservados para uso futuro
		13	Reservados para uso futuro
		14	Reservados para uso futuro
		15	Reservados para uso futuro

Fonte: Microsoft (2003a, tradução nossa), Course (2010, tradução nossa).

Como já foi mencionado, além da MFT, há uma série de arquivos de metadados que são utilizados pelo NTFS para gerenciar o sistema de arquivamento, e cada um tem seu registro na MFT:

$. É o símbolo do diretório raiz.

$MFT. A primeira entrada na tabela é chamada $MFT, e descreve a localização da MFT no disco. De fato, é o único lugar onde a localização da MFT é descrita; portanto, necessita-se processá-la para determinar o layout e tamanho da MFT. A localização da MFT é dada no setor de inicialização, que está sempre

localizado no primeiro setor do sistema de arquivos (CARRIER, 2005, tradução nossa).

$MFTmirr. Este arquivo está localizado no centro do volume onde se pode, portanto, ser facilmente encontrado em caso de danos ao sistema de arquivos. Ele contém entradas da MFT duplicadas para a $MFT, $MFTMirr, $Logfile e $Volume. É uma cópia das primeiras quatro entradas de arquivos da MFT e pode ser usado em futuras tentativas de recuperação devido alguns problemas no sistema (SAMMES; JENKINSON, 2007, tradução nossa).

$Logfile. Este arquivo é uma base de dados relacional, que registra transações de e para o disco. Ele pode ser usado na recuperação de uma falha do sistema. O NTFS usa um sistema de cache conhecido como escrita lenta, onde os dados não são imediatamente gravados no disco, e ele precisa de mais que uma transação para completar uma tarefa de arquivamento. Por exemplo, duas operações são necessárias para atualizar um arquivo. Uma para atualizar o próprio arquivo e uma segunda para atualizar os detalhes na MFT em relação as datas e horas do arquivo, e assim por diante. No caso de uma falha de energia ocorrida entre as duas operações, a recuperação pode ser efetuada através da conclusão da tarefa perdida, como indicado pelo $Logfile. O tamanho do arquivo do $Logfile depende do tamanho do volume (SAMMES; JENKINSON, 2007, tradução nossa).

$Volume. Este arquivo contém informações sobre o volume, tal como o nome do volume, o número da versão do NTFS, o tempo e data de criação e a "bandeira suja". Este último item é usado para indicar se na última utilização do volume ocorreu ou não um desligamento normal (SAMMES; JENKINSON, 2007, tradução nossa).

$AttrDef. É a tabela que define todos os atributos do sistema dentro do volume (MICROSOFT, 2006, tradução nossa).

$Bitmap. Este é um mapa de bits dos clusters lógicos no volume. Ele é simplesmente composto de bandeiras binárias onde o número um "1" simboliza que um cluster está em uso, e o número zero "0" simboliza que um cluster não está em uso. Em alguns aspectos, é semelhante a uma FAT, mas sem os valores de ponteiro. $Bitmap simplesmente regista a utilização dos blocos de armazenamento no volume (SAMMES; JENKINSON, 2007, tradução nossa).

$Boot. Este é o registro de inicialização do volume. Ele inclui o Bloco de Parâmetros do BIOS (BPB), que é usado para montar o volume, bem como o código

adicional *bootstrap*, que é utilizado caso o volume seja inicializável (SAMMES; JENKINSON, 2007, tradução nossa).

$BadClus. Este é o arquivo que sinaliza dentro de todo o volume quais clusters estão defeituosos. Deve-se notar que este arquivo só se refere a clusters, não aos setores. Se um setor dentro de um cluster estiver danificado, então todo o cluster será marcado como danificado. O cluster também é marcado como "usado" no $Bitmap para garantir que nenhum dado seja armazenado lá. NTFS implementa um recurso em volumes tolerantes a falhas, onde, na identificação de um setor danificado, todos os dados dentro do cluster em questão são movidos para outro local e os detalhes do arquivo são alterados adequadamente (SAMMES; JENKINSON, 2007, tradução nossa).

$Secure. Contém informações sobre a segurança e controle de acesso para os arquivos (CARRIER, 2005, tradução nossa).

$Upcase. Este arquivo armazena uma tabela contendo informações para converter nomes de arquivos para Unicode (COURSE, 2010, tradução nossa).

$Extend. Este é um diretório no qual estão localizados os arquivos de sistema estendidos $Quota, $ObjId, $Reparse e $UsnJrnl (SAMMES; JENKINSON, 2007, tradução nossa).

$ObjId. Este arquivo é usado para rastreamento de links distribuídos. Isto permite que atalhos e links OLE continuem funcionando mesmo depois do arquivo destino ter sido renomeado ou movido. Quando um atalho para um arquivo em um volume NTFS é criado, este sistema coloca um identificador único (ID) para o arquivo de destino. A identificação do objeto também é armazenada no arquivo de ligação e é esta identificação do objeto que é usada para localizar o arquivo de destino. $ObjId usa um arquivo chamado Tracking.log para gestão da informação (SAMMES; JENKINSON, 2007, tradução nossa)

$Reparse. Objetos NTFS como arquivos, pastas entre outros contém um atributo especial, chamado *reparse*. Este atributo especial define uma nova funcionalidade para aquele objeto. As chamadas de sistema podem ser interceptadas e, em seguida, alimentadas através de software adicional (SAMMES; JENKINSON, 2007, tradução nossa).

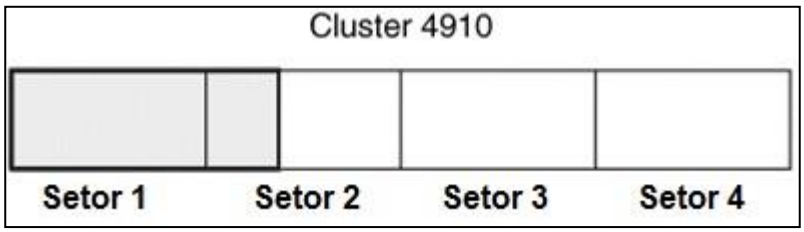
$UsnJrnl. Este é um arquivo esparso em que o NTFS armazena registros de alterações de arquivos e diretórios, assim como seus vários atributos e configurações de segurança. Aplicações como o Windows *File Replication Service*

*(*FRS) e o Windows *Search Service* fazem uso do jornalismo (RUSSINOVICH; SOLOMON; IONESCU, 2012, tradução nossa).

4.3.2 Como é feita a Alocação de dados

Considerando o sistema de arquivos NTFS com um cluster de 2048 bytes e setores de 512 bytes. Tem-se um arquivo de 612 bytes, será alocado todo o primeiro setor e 100 bytes do segundo setor no cluster. O restante de 412 bytes do segundo setor é preenchido com dados da escolha do Sistema Operacional. O terceiro e quarto setores podem ser limpos com “zeros”, forma de identificação de local livre para uso pelo Sistema Operacional, ou ele pode também manter os dados de um arquivo excluído. Na imagem as áreas em cinza são o conteúdo do arquivo e o espaço em branco é o espaço livre (CARRIER, 2005, tradução nossa).

Figura 16 - Armazenando em um cluster



Fonte: Carrier (2005, tradução nossa).

Uma analogia comum para o espaço livre é fita de vídeo VHS. Uma noite grava-se um episódio da mais recente série de TV de investigação criminal contendo 60 minutos. Eventualmente, pega-se de volta a fita para assistir o show, e então rebobina-se a fita. No final da semana, grava-se um programa de TV contendo 30 minutos. Neste ponto, a fita possui o programa de TV de 30 minutos, mas ainda há 30 minutos do show anterior, no final da fita (CARRIER, 2005, tradução nossa). É assim que funciona de forma análoga o armazenamento de dados nas partições NTFS.

O método $Bitmap é uma maneira econômica de manter o controle de espaço livre, uma vez que apenas um bit é necessário para cada bloco no disco. Tem ainda a vantagem de que é fácil para o gerenciador de arquivos localizar blocos contíguos ou blocos que estão nas proximidades dos já alocados para um arquivo. Isso permite que o gerenciador de arquivos os mantenha de uma forma que possa

minimizar buscas em disco durante o acesso aos mesmos, quando o setor está danificado (ENGLANDER, 2009, tradução nossa).

4.4 PARTIÇÃO NTFS

Para que a máquina seja capaz de iniciar o *boot* corretamente, as seguintes condições devem ser aplicadas:

- *Master Boot Record* existir e estar em perfeito estado;
- Tabela de Partição existir e conter ao menos uma partição ativa;

Se assim for, o código executável no MBR seleciona uma partição ativa e passa o controle para ela, com isso ele pode começar a carregar arquivos apropriados (COMMAND.COM, NTLDR, ...), dependendo do tipo de sistema de arquivos nessa partição. No entanto, se esses arquivos estiverem faltando ou corrompidos, então o sistema operacional não iniciará. Um exemplo é o erro "Falta NTLDR". Neste caso, softwares de recuperação acessam a unidade danificada por meio de programação de baixo nível, ignorando a inicialização, permitindo assim a possibilidade de recuperação dos dados (NTFS, 2015).

Para o disco ou partição estarem prontos para o sistema operacional, as seguintes condições devem ser aplicadas:

- Disco ou partição podem ser encontrados através de tabela de partição;
- Setor de inicialização do disco ou partição intacto.

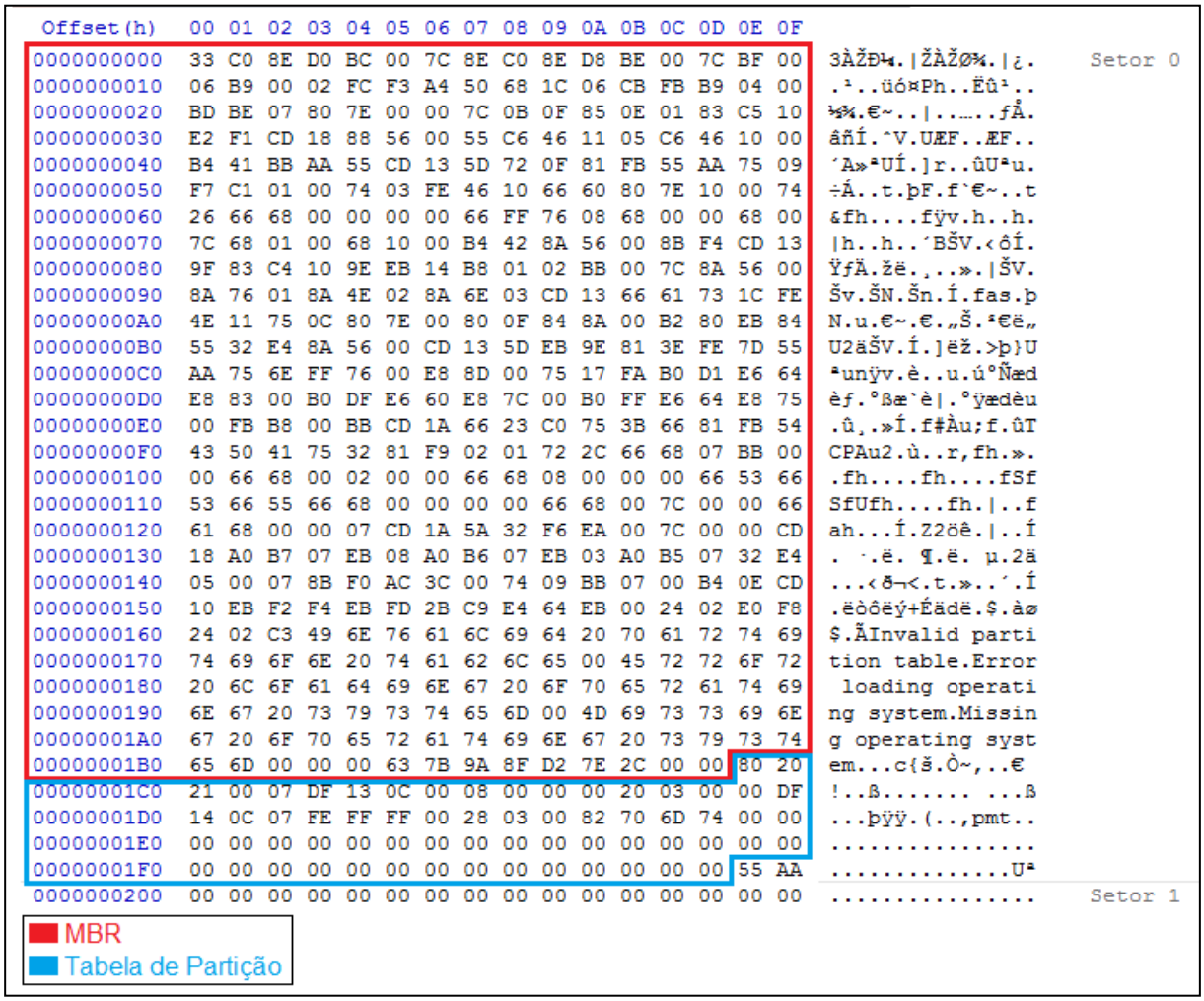
Se assim for, o sistema operacional pode ler parâmetros do disco ou partição e mostrar o drive na lista de unidades disponíveis. No entanto, se o próprio sistema de arquivos estiver danificado o conteúdo do disco pode não ser exibido, mostrando mensagens de erros como "MFT corrompida", "Dispositivo inválido". Neste caso, tem-se menos chances de restaurar dados em comparação ao caso em que o sistema operacional não é inicializável, devido perda ou corrompimento do sistema de arquivos, no entanto softwares de recuperação geralmente usam alguns truques para mostrar talvez não tudo, mas algumas das entradas que ainda estão intactas, permitindo assim salvar os dados para outro local (NTFS, 2015).

4.4.1 MBR Danificada

A *Master Boot Record* é criada juntamente com a primeira partição no disco rígido. É uma estrutura de dados muito importante. Ela contém a tabela de partição e uma pequena quantidade de códigos executáveis para inicialização do mesmo. É localizada sempre no primeiro setor do disco (NTFS, 2015).

Esse setor é subdividido em duas partes, onde a primeira parte possui o *boot loader,* responsável por carregar o sistema operacional na memória. O byte que indica o fim dessa parte é “0x1BE” que se situa na posição 446, porém como o bloco inicia-se no byte 0, a posição 446 encontra-se no byte 445, essa parte é a própria MBR. A segunda parte da estrutura é formada pelos próximos 64 bytes que são as tabelas de partição. A assinatura com dois bytes “0x55AA”, significa o fim desse bloco de bytes, onde no byte de endereço 510 está a sequência “0x55” e no byte 511 encontra-se sequência “0xAA” conforme demonstra a figura 17 (CARRIER, 2005, tradução nossa).

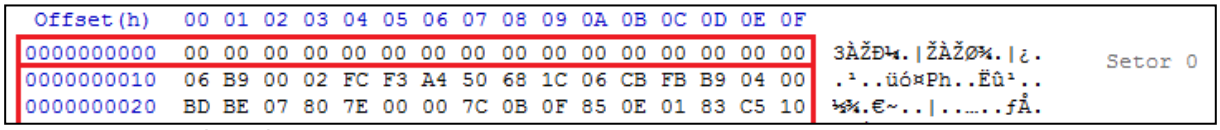
Figura 17 – Identificando MBR e Tabela de Partição



Fonte: Do autor (2015).

Quando o primeiro setor do disco for danificado, como por exemplo um vírus que sobrescreva os 16 primeiros bytes com zeros. Ao tentar inicializar após os procedimentos de teste de hardware executados ao inicializar o computador, é apresentada apenas uma tela em branco sem qualquer informação, isso significa que uma parte do código de inicialização da MBR não pôde ser executada corretamente. No entanto, colocando esse mesmo disco como secundário de outro, os arquivos aparecem intactos, isso ocorre, pois apenas uma parte da MBR foi danificada, sendo mantido intacta a tabela de partição conforme figura 18 (NTFS, 2005, tradução nossa).

Figura 18 - MBR Danificada



Fonte: Do autor (2015).

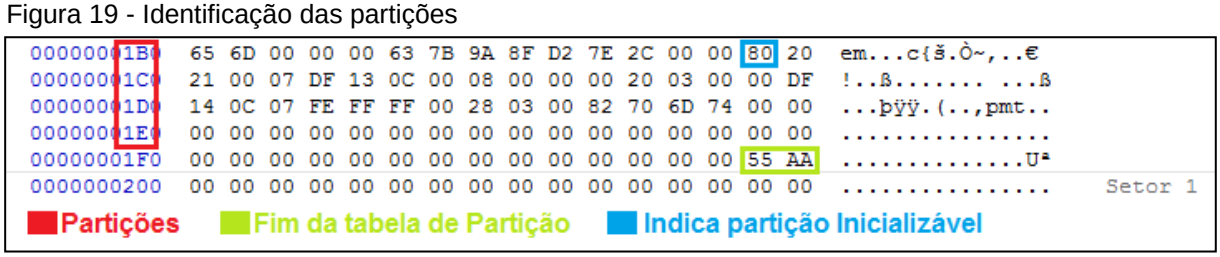
Caso a assinatura que indica o fim do setor, ou seja, os bytes 55AA forem removidos ou danificados, ao efetuar a inicialização do sistema operacional, será apresentado na tela uma mensagem de erro informando “Tabela de partição Inválida”. Assim, a primeira coisa a fazer quando o computador não inicializa, é executar um visualizador de disco que seja capaz de verificar se o primeiro setor físico no disco rígido está apresentando de forma correta a MBR ou não. Uma forma simples de reparar ou recriar a MBR é executando um utilitário padrão do Windows que verifica e repara a partição (NTFS, 2005, tradução nossa).

Quando o primeiro setor estiver danificado ou ilegível, o mais provável é aparecer uma tela preta, similar a tela que todo computador apresenta quando começa a inicializar o carregamento. Colocando o disco como secundário de um outro com sistema operacional e tentando visualizar os dados do mesmo, é apresentada uma mensagem de erro informando que o setor está ilegível, indicando a formatação da partição. Neste caso, somente um software de recuperação de dados é capaz de ajudar por meio de varredura e busca de partições, caso algo seja encontrado, oportuniza ao usuário salvar dados importantes para outro local (NTFS, 2005, tradução nossa).

4.4.2 Tabela de Partição Deletada danificada

As informações sobre as partições primárias e estendidas estão inseridas na tabela de partição, uma estrutura de dados de 64 bytes, localizada no mesmo setor que o *Master Boot Record* ou seja, cilindro 0, cabeça 0, setor 1. A tabela de partição possui um leiaute padrão, que independe de sistema operacional. Os últimos dois bytes do setor sempre serão 0x55AA como visto na figura 19 (NTFS, 2005, tradução nossa).

Figura 19 - Identificação das partições



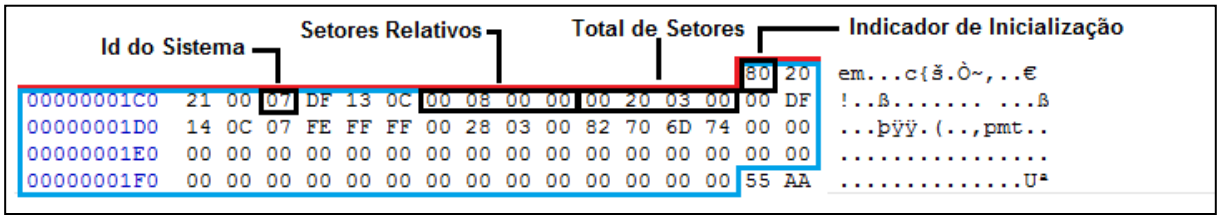
Fonte: Do autor (2005).

Conforme figura 19, pode-se verificar a existência de três partições e uma entrada vazia, pode-se observar também conforme a figura 17 os endereços onde cada partição inicia-se.

- Partição 1, início 0X01BE (446);
- Partição 2, início 0X01CE (462);
- Partição 3, início 0X01DE (478);
- Partição 4, início da partição vazia, 0X01EE (494).

O leitor da MBR pode identificar a localização e tamanho da partição. Ele verifica qual das partições é a ativa, ou seja, a partição que possua o indicador de inicialização igual a 0X80 e passa o controle para o setor de inicialização da partição para posterior carregamento da mesma, além do Indicador de inicialização, existem o ID do sistema, setores relativos e total de setores estão identificados na figura 20 (MICROSOFT, 2003c).

Figura 20 - Entradas na Tabela de Partição



Fonte: Do autor (2015).

A tabela de partição constitui de 4 entradas de 16 bytes no máximo, cada uma das quatro possui os seguintes atributos:

Tabela 2 - Tabela de Partição

CAMPO	TAMANHO
Sinalizador de Inicialização (Id)	1 byte
Lado inicial	1 byte
Cilindro inicial	10 bits
Setor inicial	6 bits
Indicador de Inicialização	1 byte
Lado final	1 byte
Cilindro final	10 bits
Setor final	6 bits
Setores relativos	4 bytes
Total de setores	4 bytes

Fonte: Adaptado Microsoft (2003d).

Sinalizador de Inicialização – Conforme dito anteriormente é quem indica se a partição é ativa ou não, em um disco somente uma partição pode ser ativa, as outras são definidas como 0x00.

Lado inicial e final - O número máximo de Lados representados em 1 byte é de 256.

Cilindro inicial e final - O número máximo de Cilindros com 10 bits é de 1024.

Setor inicial e final - O número máximo de Setores com 6 bits é de 63.

Indicador de inicialização – É quem indica qual o sistema de arquivos está presente na partição, conforme anexo 1.

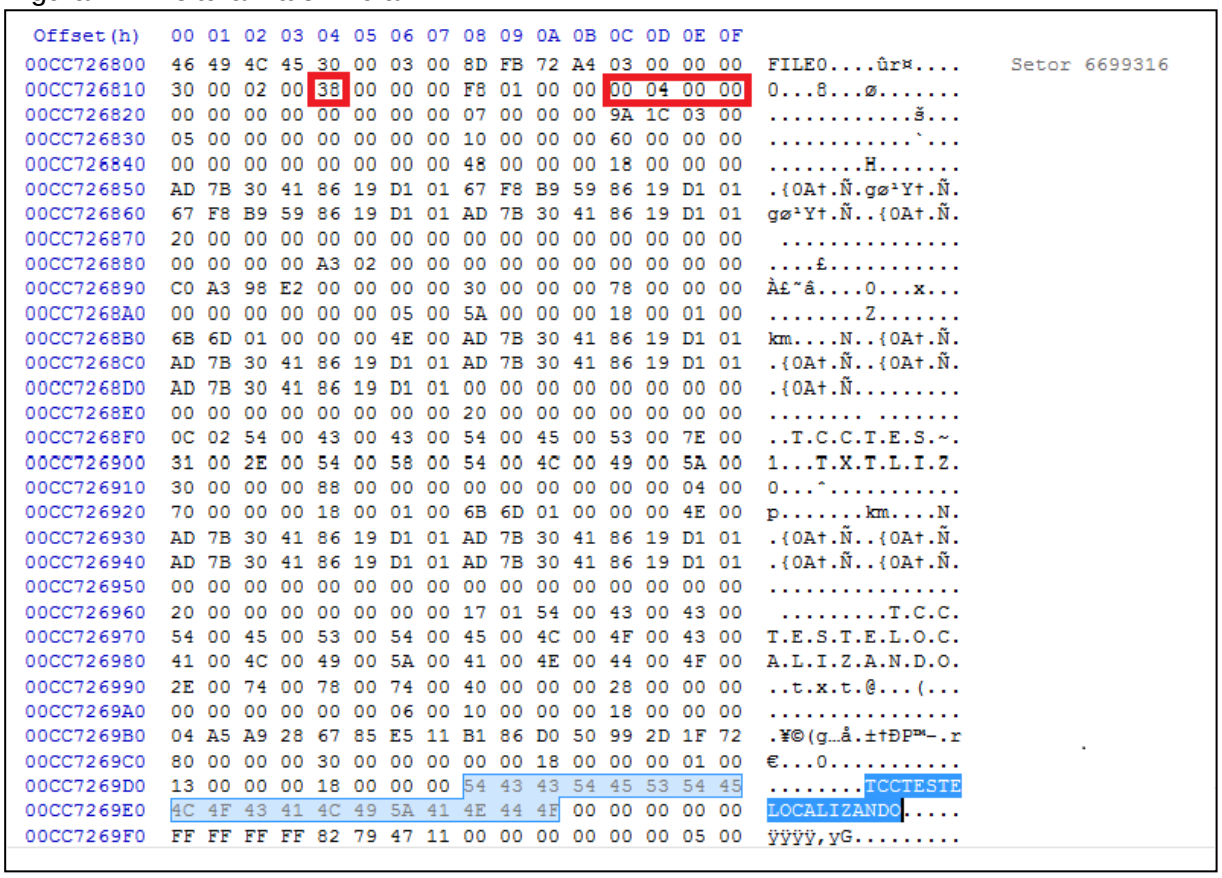
Setores Relativos – Representam o deslocamento do início da tabela de partição até o início da partição.

Total de Setores – Representa o número total de setores contidos na partição.

4.4.3 Arquivos dentro da MFT no formato Litle Endian

O tipo de armazenamento L*ittle Endian* se refere a forma que os arquivos binários com múltiplos bytes são lidos. Esse é o formato utilizado no armazenamento dos arquivos dentro dos setores, esse formato procede com a leitura dos conjuntos de bytes da direita para a esquerda, pois o formato *Little Endian* coloca os dados menos significativos no primeiro byte a ser lido e o mais significativo no ultimo byte a ser lido, esse tipo de leitura é utilizado pelos computadores que possuem sistema operacional Windows, já o *Big Endian* para não deixar de ser citado é utilizado pelos computadores da Apple. Segue na sequencia um exemplo de como os arquivos são armazenados dentro de um setor no disco no modo *Little Endian* (CARRIER, 2005).

Figura 21 - Leitura Little Endian



Fonte: Do autor

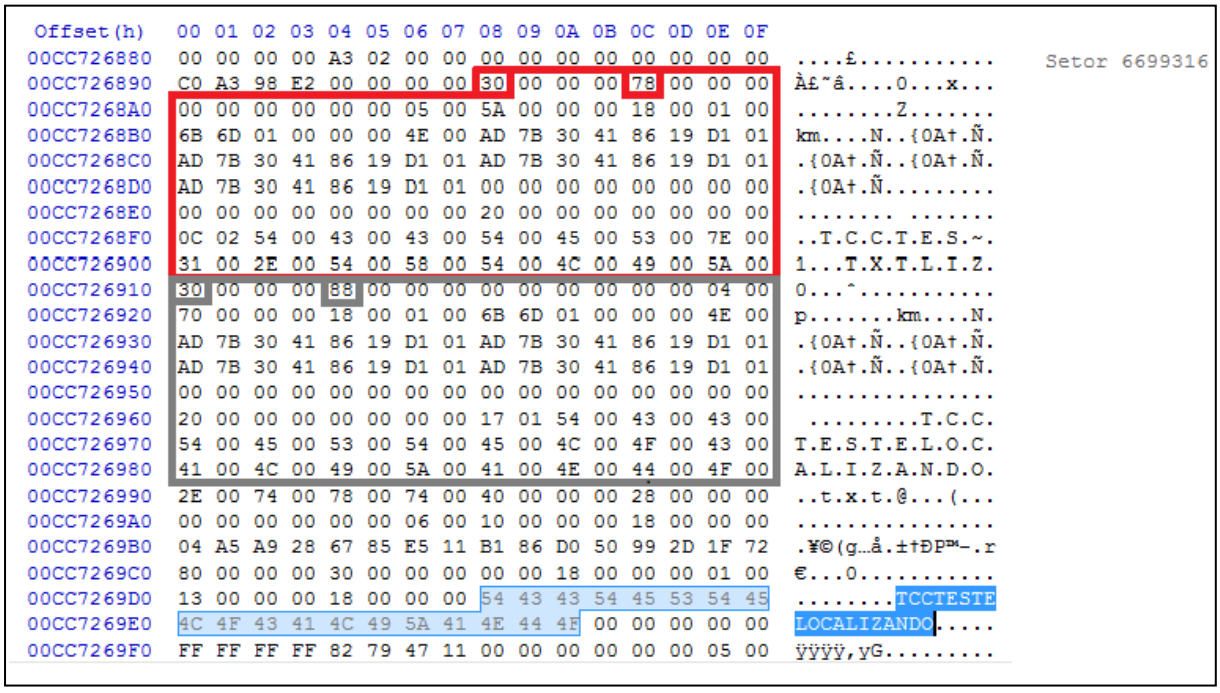
No exemplo da figura 21, o valor no formato *Little Endian* é 00 04 00 00, deve ser convertido para hexadecimal e obtém-se 00000400, ondem todos os zeros a esquerda devem ser ignorados, o valor restante deve ser escrito juntamente com o prefixo 0x, ficando 0x400, transformando para o formato Decimal, o valor informado e 1024, esse e o valor que informa o tamanho gravado na MFT (CARRIER, 2005).

Em continuidade ao exemplo da figura 21, o sistema identifica um arquivo armazenado no disco observando três pontos que são os mais importantes indicando que o mesmo está legível dentro da partição. Primeiramente o arquivo sempre inicia no offset 0x00 com o nome FILE nos quatro primeiros bytes do setor, ou seja, nos 4 primeiros bytes contém as informações 46 49 4C 45 que se referem a cada letra no formato hexadecimal. Posteriormente na posição do offset 0x14 que no valor decimal é 20 e estará presente o comprimento do cabeçalho da MFT, que sempre será 0x38 que convertendo para decimal, obtém-se o valor 56, ou seja os primeiros 56 bytes desse setor é o comprimento do cabeçalho da MFT dentro do arquivo. Por fim o tamanho utilizado para a gravação do arquivo dentro da MFT é identificado entre o offset 0x1C até 0x1F que conforme exposto logo acima sempre

será o valor 00 04 00 00 e por ser *Little Endian* deverá ser transformado para 0x400 que por sua vez transformado para decimal fica 1024, ou seja, esse arquivo ocupa dois setores dentro do disco. No offset 0x39, ou seja, a posição 57 em decimal está o atributo com o padrão de informações da gravação na MFT, nessa posição deverá aparecer o byte 0x10, seguindo o arquivo, na posição offset 0x04 e 05 está o comprimento do atributo 0x10 que são os bytes 60 00 em formato *Little Endian*, transformando para Hexadecimal fica 0x60 e para decimal fica 96, ou seja, os próximos 96 bytes iniciando do byte 0x10 são de atributos do arquivo, onde dentre esses atributos podem ser identificados a data e hora de criação do mesmo, que no exemplo da figura 21 possuem os valores AD 7B 30 41 86 19 D1 01, logo na sequência vem os atributos de data o hora da última modificação, que no exemplo da figura 21 possuem os valores 67 F8 B9 59 86 19 D1 01 posteriormente vem os atributos de data e hora do último acesso feito ao arquivo que no mesmo exemplo possuem os valores 67 F8 B9 59 86 19 D1 01, por último vêm os atributos de data o hora da última atualização das informações dentro do arquivo, que nesse mesmo exemplo traz os bytes AD 7B 30 41 86 19 D1 01 (CARRIER, 2005).

Em relação aos atributos do nome do arquivo pode ser do tipo curto ou longo, onde o tipo curto possui até 8 dígitos antes do ponto e três após o ponto, já quando o arquivo é do tipo longo, o sistema transforma o nome para o tipo curto, reescrevendo o mesmo com os 6 primeiros dígitos, sendo seguidos de um ~ que vem seguido de um número sequencial. Esses atributos são inicializados com o valor hexadecimal 0x30, os offsets 0x04 e 05 possuem o comprimento dos atributos que ao transformar do valor hexadecimal 0x70 para decimal, demonstra o resultado 112, isso nada mais é que a quantidade de bytes que esse atributo possui. Estão inseridos nesse espaço os atributos relacionados ao nome do arquivo, atributos esses que possuem informações como a data e hora de criação do nome, data e hora da última modificação do nome, data e hora do último acesso e data e hora da última atualização feita, sendo similar aos atributos vistos anteriormente com relação ao arquivo. Com relação a este exemplo o nome do arquivo está inserido no tipo longo, sendo assim existe uma diferença dentro dos setores, onde é duplicada a quantidade de atributos, ou seja, haverá dois bytes 0x30, um demonstrando o nome no formato curto e o outro no formato longo. Para um melhor entendimento a figura 22 demonstra esses fatos (CARRIER, 2005).

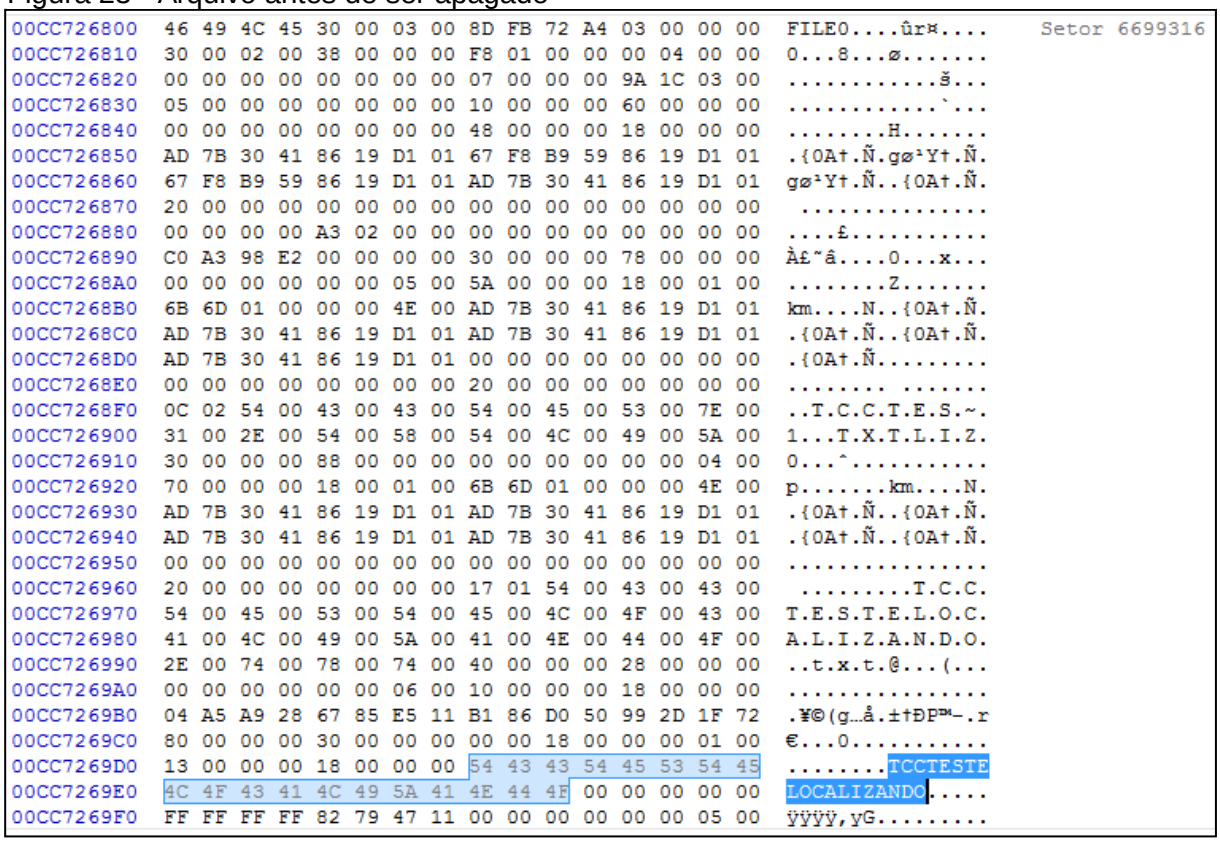
Figura 22 - Atributos de nome de arquivos



Fonte: Do autor

Acima foi demonstrado como se comporta um arquivo dentro de um disco com sistema NTFS. Na sequência será descrito como esse mesmo arquivo se comporta ao ser removido do sistema, ou seja, o que o sistema faz para não demonstrar mais esse arquivo para o usuário. Na figura 23 é demonstrado como um arquivo é armazenado dentro de um setor antes de ser removido permanentemente do computador, deve ser observado que todo o setor que possui um arquivo armazenado nele, inicia com os bytes hexadecimais 46 49 4C 45, que em decimal significam a palavra FILE, como pode ser observado na figura 23 (CARRIER, 2005).

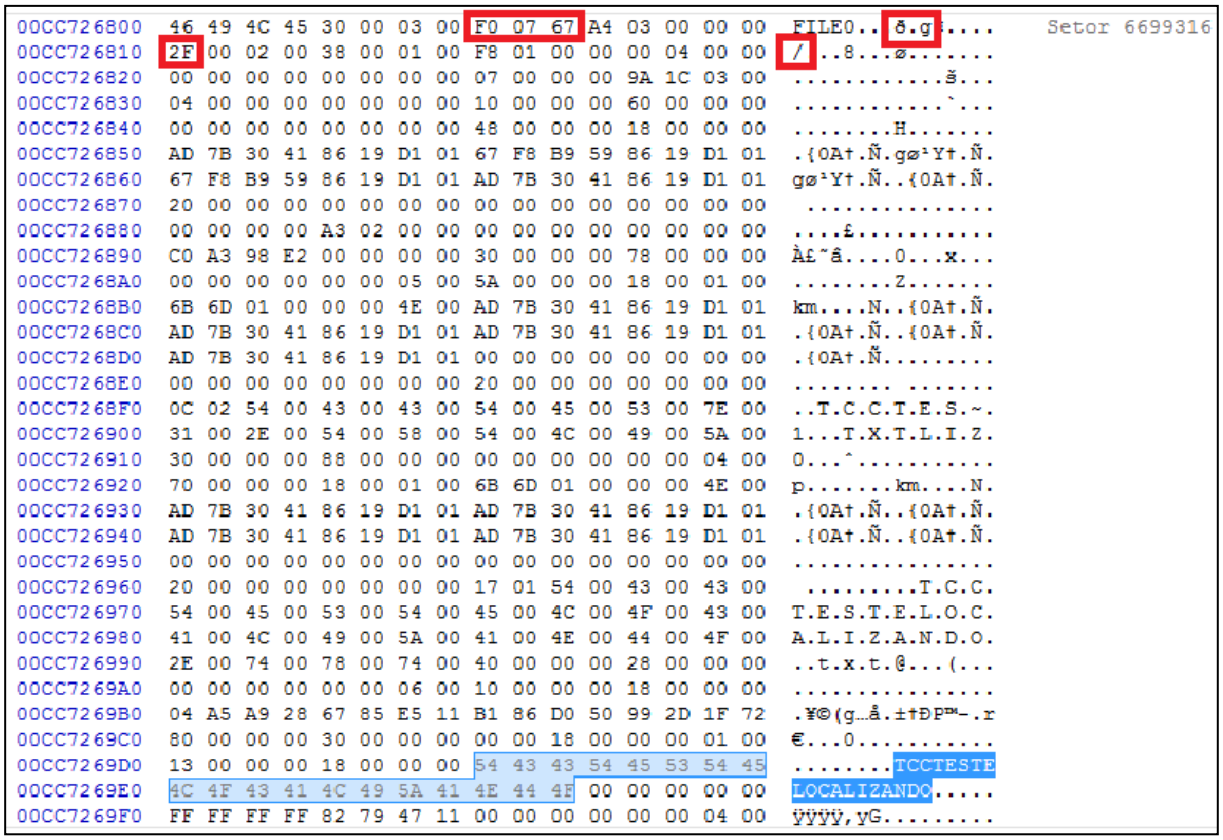
Figura 23 - Arquivo antes de ser apagado



Fonte: Do autor.

Pode-se observar que a figura 24 é praticamente a mesma imagem da figura 23, no entanto existem algumas pequenas diferenças que estão em destaque. Esses bytes em destaque são os bytes que foram modificados após a eliminação permanente do arquivo de dentro do sistema operacional do usuário, ou seja, quando um arquivo é eliminado do computador, ele não tem sua estrutura modificada dentro do setor, o sistema modifica alguns bytes no início, mantendo todo o restante intacto (CARRIER, 2005).

Figura 24 - Arquivo após ser apagado



Fonte: Do autor

5 SOFTWARES DE RECUPERAÇÃO DE DADOS

Neste capítulo foram dispostos alguns softwares de recuperação de dados. Foram descritas algumas características de cada um para que se obtenha um prévio conhecimento dessas ferramentas. Foram descritos um a um e por fim será demonstrado em forma de quadro comparativo algumas de suas características e funcionalidades

5.1 SOFTWARES DE RECUPERAÇÃO E SUAS CARACTERÍSTICAS

Existem muitos softwares na Internet que executam recuperação de dados a partir da perda da tabela de partição. Devido a isso são descriminados a seguir alguns desses com suas características.

Recuva é um software desenvolvido pela Piriform, o site oficial é http://www.piriform.com/. Ele funciona para as versões do Windows 8.1, 8, 7, Vista e XP. Incluindo 32 e 64 bits para todas essas versões. Ele possui uma versão portátil, mais leve e podendo ser executado diretamente de um pendrive. Ao ser executado, aparecem perguntas na tela a respeito da pesquisa a ser feita. Não possui imagens intuitivas para um melhor entendimento do usuário. Possui versão em várias línguas, inclusive o português (PIRIFORM, 2015, tradução nossa).

MiniTool Power Data Recovery é desenvolvido pela empresa Mini Tool, com endereço eletrônico http://www.powerdatarecovery.com/. Esse um software funciona com qualquer versão do Windows 32 e 64 bits e Mac. Recupera arquivos deletados, por meio de partição danificada e disco formatado. Possui layout intuitivo ao usuário, com imagens grandes que auxiliam no entendimento de cada função (MINITOOL, 2015, tradução nossa).

GetDataBack é um sistema desenvolvido pela empresa Runtime Software, o site oficial é http://www.runtime.org/. Existem várias versões deste mesmo software. Roda em todos os sistemas de arquivos FAT12, FAT16, FAT32 e NTFS. É muito fácil de se utilizar, com poucos cliques o sistema já faz a busca. Recupera além dos arquivos, as pastas com seus nomes originais. Possibilidade de rodar a partir de um live cd. Recupera arquivos deletados, de partições danificadas e até mesmo depois de o disco ser formatado. Tem a possibilidade de busca rápida

além a profunda, usada para perda repentina dos dados (RUNTIME, 2015, tradução nossa).

EaseUS Data Recovery Wizard é desenvolvido pela EasyUS, o site oficial é http://www.easeus.com/. Este software possui a capacidade de recuperar arquivos perdidos por exclusão, formatação e partição danificada. Funciona nos sistemas de arquivos FAT12/16/32, NTFS, EXT2/EXT3. Oferece as opções de busca rápida e profunda. Possibilita a busca por tipos específicos de arquivos. Telas iterativas e de fácil uso (EASYUS, 2015, tradução nossa).

Pandora Recovery é produzido pela empresa de mesmo nome. http://www.pandorarecovery.com/. Ele possui a capacidade de recuperar arquivos deletados, por meio de partições danificadas e formatadas. Compatível com FAT16, FAT32, NTFS, NTFS5 e NTFS/EFS. Possui um layout sem muitas imagens, porém o software se parece muito com o Windows Explorer, deixando o ambiente mais familiar ao usuário (PANDORA, 2015).

Puran File Recovery é desenvolvido pela Puran Softwares detentora do site http://www.puransoftware.com/index.html. É compatível aos sistemas de arquivos FAT12 FAT16 FAT32 e NTFS. Possui uma interface muito simples, porém muito rápido nas buscas. Possui vários tipos de busca, dentre eles a busca rápida e a profunda. Recupera arquivos excluídos, por meio de tabela de partição danificada e formatada (PURAN, 2015).

Recover My Files é produzido por GetData Software Department Company. Essa empresa é parceira certificada pela Microsoft. O software possui uma interface com cores agradáveis, se assemelhando com o Windows Explorer. Após a varredura, possui algumas opções de visualização para melhor satisfazer as necessidades do usuário. Como os softwares anteriores, tem a capacidade de recuperar arquivos deletados, por meio de partição danificada e formatada. Suporta todos os tipos de arquivos FAT, NTFS, HFS e HFS+ (GETDATA, 2015).

Free Undelete é produzido pela Recoveronix, uma empresa parceira certificada da Microsoft. Esse sistema é compatível com todas as versões de FAT e NTFS. Funciona nas versões Microsoft Windows XP ou posteriores, não é suportado pelo Windows 98. Possui uma interface extremamente simples, facilitando o uso. Utilizado para ocasião de arquivos deletados (RECOVERONIX, 2015).

PC Inspector File Recovery é produzido pela Convar Repair & Service. O software suporta FAT 12, 16, 32 e NTFS. Esse software possui a capacidade de

recuperar arquivos deletados, assim como a partir de formatação ou perda de tabela de partição. O layout apesar de possuir várias imagens, é pouco intuitivo (CONVAR, 2015).

Tabela 3 - Comparação entre softwares

Nome	Desenvolvido por	S.O. / Versão	Arquivos deletados	Perda de Partição	Partição Formatada
Recuva	Piriform	Windows XP, Vista, 7, 8 e 8.1. Todas versões	X	X	X
MiniTool Power Data Recovery	Mini Tool	Todas versões Windows e Mac	X	X	X
GetDataBack	Runtime	FAT12, 16, 32 e NTFS	X	X	X
EaseUS Data Recovery Wizard	EaseUS	FAT12, 16, 32, NTFS, EXT2 e EXT3	X	X	X
Pandora Recovery	Pandora	FAT16, 32, NTFS, NTFS5 e NTFS/EFS	X	X	X
Puran File Recovery	Puran Softwares	FAT12, 16, 32 e NTFS	X	X	X
Recover My Files	GetData	FAT, NTFS, HFS e HFS+	X	X	X
Free Undelete	Recoveronix	Todas as versões de FAT e NTFS	X		
PC Inspector File Recovery	Convar Repair & Service	FAT 12, 16, 32 e NTFS	X	X	X

Fonte: Adaptado Piriform(2015), Mini Tool(2015), Runtime(2015), EaseUS(2015b), Pandora(2015), Puran(2015), GetData(2015), Recoveronix(2015), Convar (2015)

Os softwares descritos anteriormente foram selecionados se levando em conta alguns critérios de escolha. A busca foi feita na Internet, tendo sido acessado alguns sites conhecidos para download como http://www.baixaki.com.br/, http://www.superdownloads.com.br/, e http://info.abril.com.br/. Dentro deles foi efetuada pesquisa de softwares para recuperação de arquivos na plataforma Windows com sistema de arquivos NTFS. Foram selecionados os mais baixados e com melhor reputação. Preferencialmente sob a licença freeware. Durante a

execução do projeto haverá mais detalhes a respeito dos mesmos, sendo escolhidos alguns desses para executar o projeto.

6 TRABALHOS CORRELATOS

Com uma importância muito grande para o mundo onde a tecnologia e a informação trafegam a todo instante, a perda de dados é algo que acontece, independente da causa, é difícil encontrar alguém que nunca perdeu nenhum arquivo digital em toda sua vida. Serão citados alguns projetos que possuam semelhança com este em execução.

6.1 ANÁLISE DE FERRAMENTAS PARA COMPUTAÇÃO FORENSE EM SISTEMAS NTFS

Esta monografia foi desenvolvida por José Geraldo Popolin da Universidade Federal de Lavras em Minas Gerais, no ano de 2011. O intuito desse trabalho foi mostrar o uso de algumas ferramentas e procedimentos básicos para se realizar análises em caso de incidentes em sistemas operacionais que utilizam NTFS.

O trabalho começa falando sobre os passos utilizados pela forense computacional para se chegar ao objetivo. Na sequência, é falado sobre a coleta de evidências digitais usando a RFC 3227, que nada mais é do que um padrão para a coleta de provas, continuando o assunto falando sobre a volatilidade dos dispositivos, para que se saiba qual dispositivo se deve começar o trabalho de obtenção de provas, entrando em maiores detalhes sobre processadores, memória de periféricos, memória principal, tráfego de rede, estado do sistema operacional e da rede e o sistema de arquivos. Em seguida fala sobre o sistema de arquivos NTFS, sua estrutura e características. Na sequência se utiliza ferramentas para forense em ambiente NTFS para analisar evidências, seguindo com ferramentas para a recuperação de arquivos apagados. Por fim, aplicando ferramentas em demonstração prática.

6.2 UMA ABORDAGEM SOBRE RECUPERAÇÃO DE DADOS EM DISCO RÍGIDO

Esta monografia foi desenvolvida por Edmilson Porto Santos da Universidade Tiradentes em Aracajú no ano de 2002. Este trabalho teve por objetivo divulgar algumas técnicas de recuperação de dados em disco rígido, demonstrar

como são armazenados os dados e cuidados necessários para minimizar as perdas, caso ocorra alguma catástrofe.

O trabalho começa falando sobre o ator principal, o disco rígido. Descreve a respeito de suas especificações uma a uma. Como funciona a leitura e gravação. O avanço da tecnologia e o aumento da capacidade dos discos. Em seguida descreve sobre a MBR, sistemas de arquivos, arquivos, diretórios e métodos de alocação. Descreve logo após sobre partições e alguns comandos utilizados, formatação física e lógica. Indica por meio de figuras onde fica localizado cada elemento do sistema de arquivos FAT. Explica o funcionamento do setor de BOOT e a tabela de alocação de arquivos também conhecida por FAT, a estrutura de diretório no MS DOS, área de dados e finalizando com acesso direto ao disco.

No segundo capítulo foram feitos alguns laboratórios de avaliação dos softwares *Easy Recovery* e o Norton *System Works* 2000. Primeiramente foi criado um ambiente para os experimentos de eliminação indevida de arquivos e posteriormente recuperação dos mesmos apagados ou fragmentados. Depois foi simulado um problema no setor da MBR eliminando assim todos os arquivos já recuperados do primeiro experimento. Todos os dois softwares funcionaram recuperando as informações. O terceiro teste foi efetuado com a formatação da partição. Os dois softwares conseguiram fazer a recuperação dos dados. No quarto experimento foi simulado a recuperação de um disco com danos diversos, o Norton *System Works* conseguiu recuperar, já o *Easy Recovery* não conseguiu recuperar nada.

No último capítulo foi escrito sobre um protótipo utilizado no mesmo ambiente dos outros softwares anteriores. Foi utilizado o compilador Turbo *Assembly* onde todos os testes foram positivos para o funcionamento do mesmo.

6.3 SISTEMAS DE ARQUIVO: ANÁLISE DE DESEMPENHO

Este projeto foi desenvolvido por Théo Rodrigues de Almeida da Universidade São Francisco no ano de 2009. Esta monografia foi escolhida para estar aqui, pois, o estudo central da mesma é um dos pontos mais fortes deste projeto, o sistema de arquivos NTFS.

O projeto tem por objetivo comparar alguns dos sistemas de arquivos mais comuns no mercado e verificar seu desempenho em relação a tempo de

leitura, escrita e reescrita. O trabalho inicia descrevendo sobre os tipos de armazenamento em sistemas de arquivos, demonstrando o funcionamento e comentando as vantagens de cada tipo.

Na sequência aborda os principais sistemas de arquivos existentes no mercado, considerando suas características, história de surgimento, pontos fortes e pontos fracos. São eles NTFS, EXT2, EXT3, EXT4, REISER FS, XFS e JFS. Depois, foi feita uma análise de desempenho entre todos eles. Foi criado um ambiente onde todos foram testados em igualdade de condições pelo software Bonnie++. Foi realizada uma média aritmética com os resultados gerados pelos seis testes consecutivos para que a margem de erro fosse a menor possível.

Os testes foram de escrita por caractere, uso de processador na escrita por caractere, escrita por bloco, uso de processador na escrita por bloco, reescrita, uso de processador na reescrita, leitura por caractere, uso de processador na leitura por caractere, leitura por bloco, uso de processador na leitura por bloco e busca aleatória. No final, foram criadas duas tabelas com todos os resultados para análise.

6.4 FERRAMENTA RECUPERADOR DE ARQUIVOS PERDIDOS

Este projeto é de autoria de Marcos Massao Yamamoto da universidade Estadual de Maringá feito no ano de 2004. Tem-se o objetivo de apresentar propostas de metodologias de recuperação de arquivos para uso futuro. O trabalho inicia descrevendo uma visão geral de discos rígidos, trazendo conceitos e definições, fala também sobre a tabela de alocação de arquivos utilizada, que nesse caso é a FAT, cita o setor de boot demonstrando por meio de figura como identifica-lo. Descreve também como interpretar a tabela de alocação de arquivos, o funcionamento do diretório raiz. Uso de nomes longos pelo DOS. Cita como funciona a organização lógica das partições e volumes no sistema FAT.

O próximo capítulo apresenta informações relacionadas à recuperação de arquivos perdidos, apresentando os principais fatores que levam a uma perda de arquivos, além de citar características e funcionalidades de ferramentas que recuperam dados apagados. São elas: Disk Investigator, File Recover, Magic Recovery, Recover4all Professional, Super Undelete.

No capítulo da metodologia é demonstrado passos para a recuperação de arquivos após dano no *Master Boot Record*, setor de boot da partição, Tabela de

Alocação de Arquivos, diretório raiz, Perda de arquivos por remoção ou formatação. O projeto finaliza descrevendo uma breve história sobre a linguagem de programação “C”.

7 RECUPERAÇÃO DE DADOS EM DISCOS RÍGIDOS

O referido projeto trata-se de recuperação de dados a partir de perda de dados por tabela de partição danificada, perda de dados por formatação da tabela de partição e arquivos permanentemente deletados em discos rígidos por meio de softwares que foram encontrados na Internet. O ambiente onde os softwares foram instalados, situa-se em um dos laboratórios da Universidade do Extremo Sul Catarinense. Foi criado um ambiente de testes controlado, onde se sabe quais arquivos devem ser recuperados. Ao longo do período de utilização dos softwares foram identificadas algumas situações que proporcionaram o uso de algumas variáveis, que por sua vez não foram retiradas de nenhuma métrica padronizada, foram surgindo ao longo do uso dos softwares: Detecção do disco, executou o teste, uso da ferramenta, encontrou os arquivos, recuperação dos arquivos com seus nomes originais, recuperação das pastas com seus nomes originais, quantidade de arquivos recuperados com funcionamento parcial, quantidade de arquivos recuperados não funcionando, quantidade de arquivos não recuperados, quantidade de arquivos recuperados em perfeito estado de conservação, quantidade de arquivos recuperados independentemente da situação, tempo de processo e sistemas operacionais suportados. Ao final foram descritos os resultados, informando qual software apresentou melhor rendimento durante a execução do projeto, além da discussão sobre o projeto.

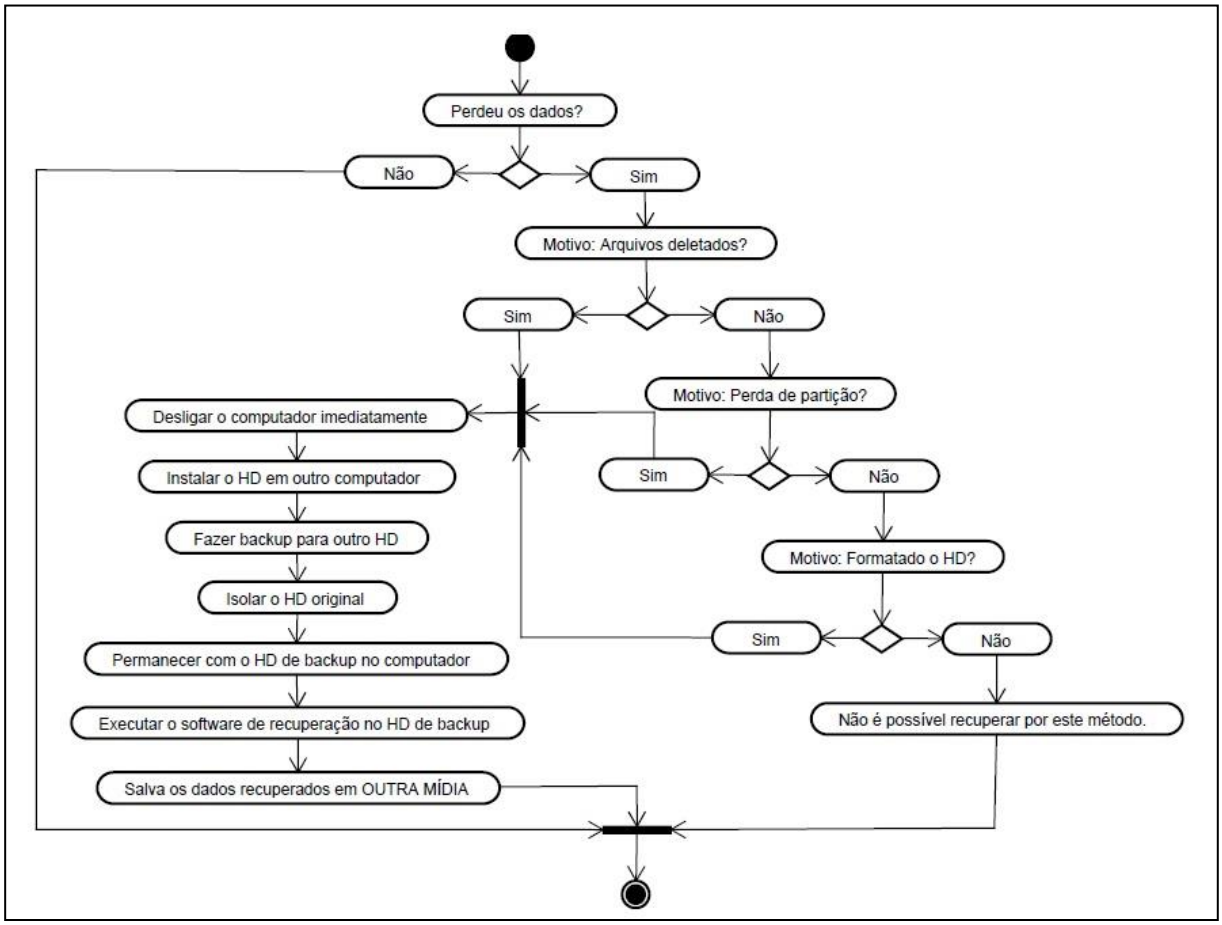
Na sequência estão expostos os procedimentos metodológicos utilizados nesse trabalho.

7.1 METODOLOGIA

Para a execução do trabalho foi efetuado o levantamento bibliográfico sobre os tópicos anteriormente abortados, após foi descrito acerca da informação e sua importância, disco rígido e sistemas de arquivos NTFS. Por fim foi elaborada e realizada a parte prática do projeto com intuito de demonstrar que é possível recuperar uma informação eliminada seja acidentalmente ou não, desde que o disco rígido não esteja com dano físico. Para que se cumpram todos os objetivos deste projeto, definiu-se a metodologia a ser empregada no mesmo.

Primeiramente determinou-se as formas de perda de dados a serem trabalhadas, que para esse projeto foram definidas as seguintes: Perda de dados por tabela de partição danificada, perda de dados por formatação da tabela de partição e arquivos permanentemente deletados. Posteriormente foram definidos os hardwares a serem utilizados na execução deste projeto. Um computador completo contendo um monitor 21”, um processador i7, dezesseis gigabytes de memória, dois discos rígidos de 7200 rpm com capacidade de um terabyte cada, lembrando que essa configuração foi a utilizada para a execução, no entanto qualquer computador com sistema operacional que suporte o tipo de partição NTFS e dois discos rígidos, é capaz de proceder conforme esse projeto sem problemas algum. Posteriormente foram identificados os softwares que seriam utilizados no projeto. O sistema operacional utilizado foi o Windows 7, o software de edição de Tabela de partição foi “HxD” desenvolvido pela empresa alemã Maël Hörz além dos softwares de recuperação de dados utilizados no projeto: Recuva, Minitool Power Data Recovery, GetDataBack, EaseUs Data Recovery Wizard, Pandora Recovery, Puran File Recovery, Recover My Files, Free Undelete e PC Inspector File Recovery. A escolha dos softwares mais utilizados dentre as três formas de perda se deu por meio de pesquisa em sites de download, onde os com maior número de downloads e com melhor reputação foram os escolhidos além da preferência dada aos softwares com licença *freeware*, pois certamente esta característica seria um fator determinante a um usuário no momento da escolha do seu software preferido. Na sequência conforme a figura 25, foram descritas etapas em um fluxograma que podem ser seguidas para o procedimento de recuperação dos dados, esse fluxograma tem a finalidade de direcionar o usuário que não está acostumado com os procedimentos de recuperação de dados.

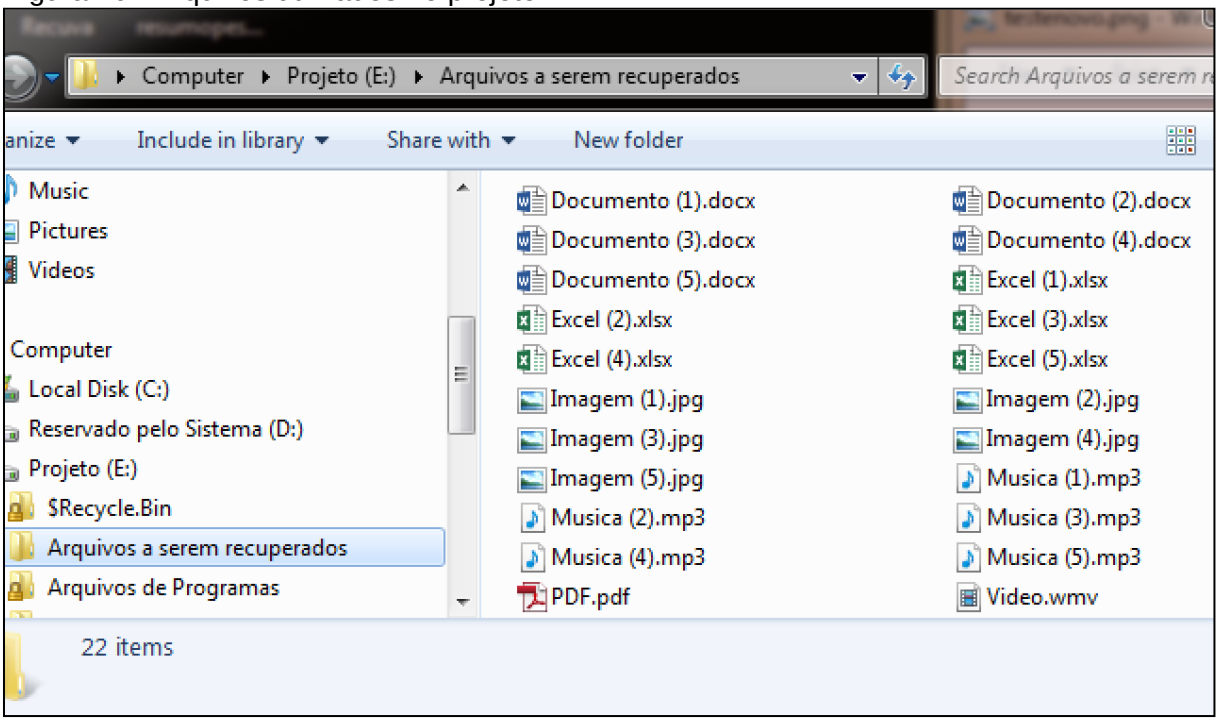
Figura 25 - Fluxograma para recuperação de dados



Fonte: Do autor 2015.

Por fim conforme a figura 26, foram especificados os tipos e quantidades de arquivos utilizados no projeto, tornando assim um ambiente controlado, porém o mais próximo possível da realidade. A escolha desses arquivos se deu por serem os tipos mais comuns de arquivos encontrados e utilizados em computadores pessoais, e dentre os mais utilizados, estão arquivos de imagem, musicas, documentos texto e tabelas, devido a isso foram criados cinco arquivos para cada um desses formatos e todos com tamanhos diferentes, além de um arquivo PDF e um arquivo de vídeo, totalizando 22 arquivos.

Figura 26 - Arquivos utilizados no projeto



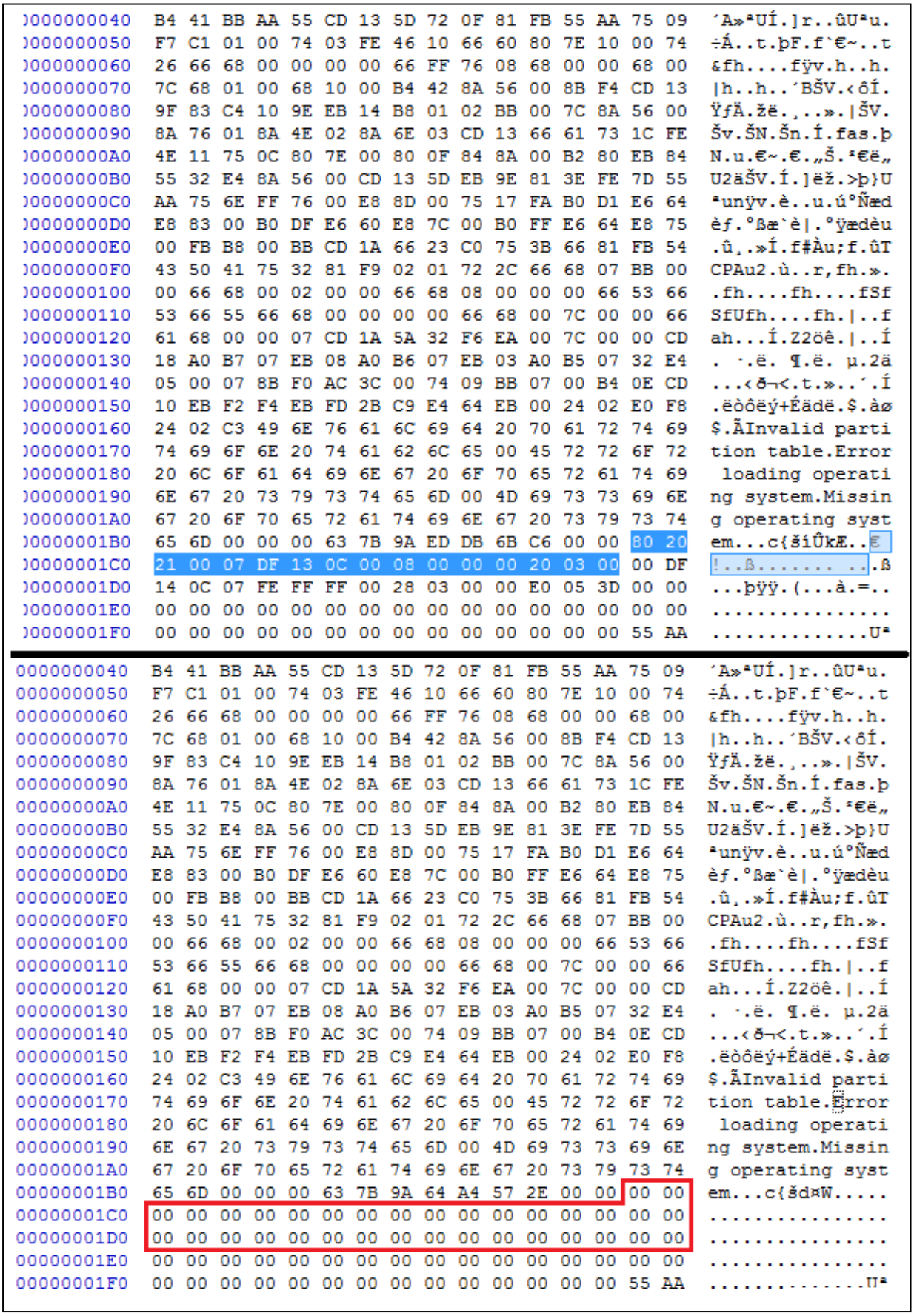
Fonte: Do autor (2015).

Na sequência estão descritos separadamente as três situações do projeto, onde cada uma informa como foi provocada, posteriormente informando o resultado dos testes dos softwares na recuperação dos arquivos relacionados a própria situação.

7.1.1 Perda de dados devido a Tabela de Partição Danificada

Quando ao carregar o Windows, o computador fica processando continuamente sem completar o carregamento, apresenta mensagens que o sistema de arquivos é inválido ou está danificado, está faltando arquivo dentre outras mensagens informando que aquela partição não está de acordo com os parâmetros exigidos. Esses são alguns dos sintomas que a partição do Windows está danificada, tornando inacessível todos os dados que estão inseridos nela.

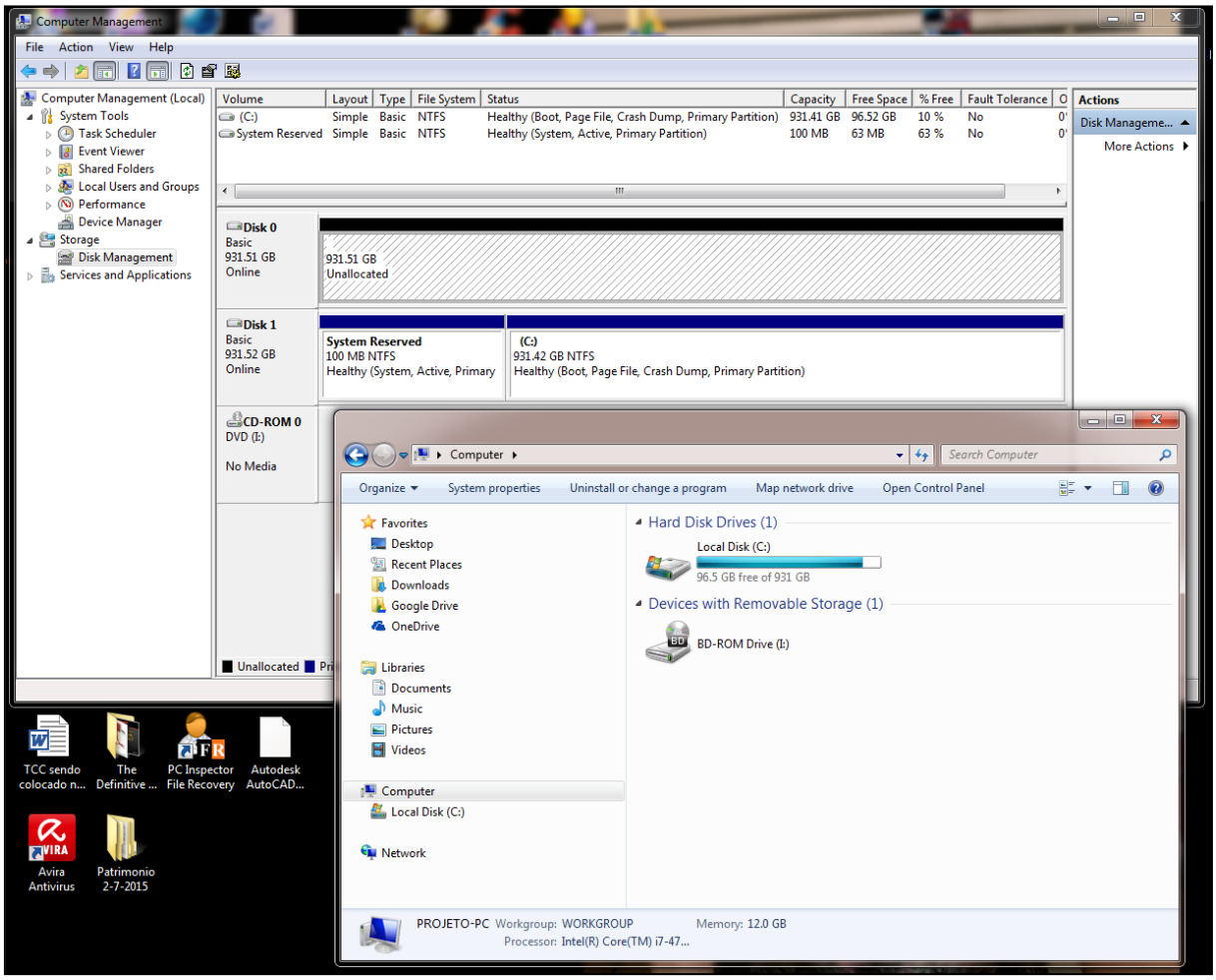
Figura 27 - Danificando a Tabela de Partição



Fonte: Do autor.

Após eliminar todas as informações da partição onde se encontravam os arquivos, a partição ficou inacessível, deixando de ser mostrada ao usuário dentro do sistema operacional. A figura 28 comprova que o disco ainda está instalado, no entanto não aparece dentre os dispositivos de armazenamento no Windows Explorer.

Figura 28 - Partição Corrompida



Fonte: Do autor.

Após provocado o dano na partição, foram executados os softwares de recuperação de dados em partição danificada. Como mencionado nesse projeto, foram executados os softwares Minitool Power Data Recovery, EaseUs Data Recovery Wizard, Puran File Recovery, Recover My Files, já os softwares Recuva, GetDataBack, Pandora Recovery, Free Undelete e PC Inspector File Recovery não encontraram a partição danificada, impossibilitando assim o uso dos mesmos.

Na sequência estão dispostos os resultados obtidos para esse teste. Os resultados encontram-se na tabela 4, onde os testes realizados em um disco com a tabela de partição danificada.

Tabela 4 - Resultados Partição Danificada

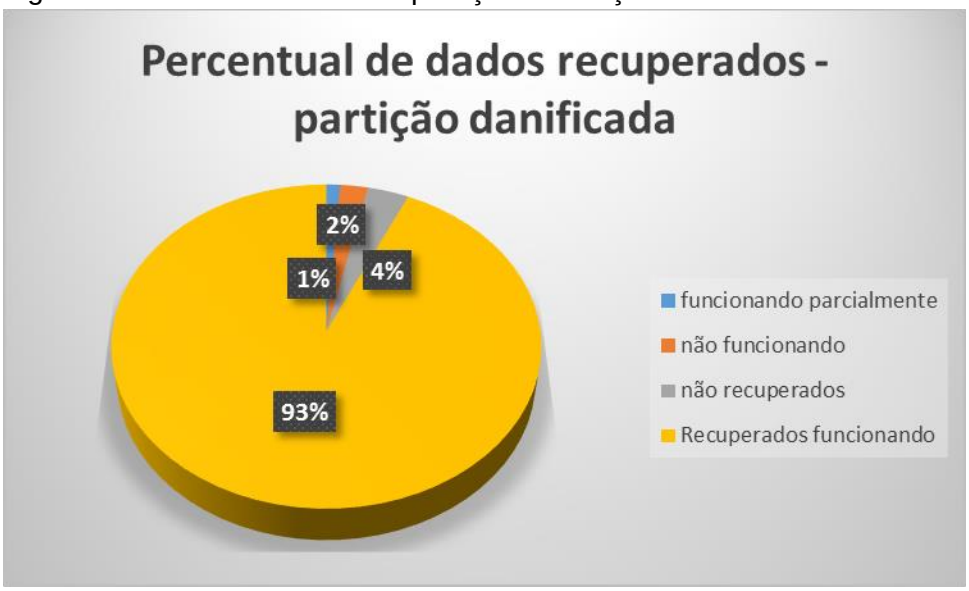
Recuperação de dados por Partição Danificada									
Métricas	EaseUs	Recuva	Minitool	GDB	Pandora	Puran	RMF	Free Undel.	PC Insp.
Detecção do disco	Sim	Não	Sim	Não	Não	Sim	Sim	Não	Não
Executou o teste	Sim	----------	Sim	--------	----------	Sim	Sim	----------	--------
Uso da ferramenta	Fácil	----------	Fácil	--------	----------	Fácil	Fácil	----------	--------
Encontrou os arquivos	Fácil	----------	Difícil	--------	----------	Fácil	Fácil	----------	--------
Recuperação dos arquivos com seus nomes originais	Sim	----------	Não	--------	----------	Sim	Sim	----------	--------
Recuperação das pastas com seus nomes originais	Sim	----------	Não	--------	----------	Sim	Sim	----------	--------
Quantidade de arquivos recuperados com funcionando parcialmente	0	----------	1	--------	----------	0	0	----------	--------
Quantidade de arquivos recuperados não funcionando	0	----------	2	--------	----------	0	0	----------	--------
Quantidade de arquivos não recuperados	0	----------	3	--------	----------	0	0	----------	--------
Tempo de processo	2:47	----------	1:48	--------	----------	1:52	0:46	----------	--------
Quantidade de arquivos recuperados independentemente da situação	22	----------	19	--------	----------	22	22	----------	--------
Quantidade de arquivos recuperados em perfeito estado de conservação	22	----------	16	--------	----------	22	22	----------	--------

Fonte: Do Autor.

O teste com partição danificada, teve um menor índice de recuperação dos dados, onde mais de 50% não foi capaz de identificar a partição danificada. Isso não significa que os softwares que não encontraram a partição, não funcionam,

como existem muitas formas de danificar a mesma, certamente em outras formas de dano estes softwares podem funcionar normalmente, caso contrário eles não seriam anunciados para esta finalidade. Dentre os que conseguiram identificar a partição, o nível de recuperação também não foi tão alto quando os outros testes. Em relação ao tempo de execução, pôde-se observar que existe uma grande diferença entre os softwares, onde alguns chegaram a atingir o triplo do tempo de outros, porém o tempo não foi determinante para indicar o software com melhores resultados, pois tanto o que executou em menor tempo quanto o de maior tempo recuperaram todos os arquivos em perfeito estado. O percentual de recuperação dos dados além de ter sido menor que os outros testes, não decepcionou, como demonstrado na figura 29, possibilitando assim recuperar a grande maioria dos dados de forma íntegra.

Figura 29 - Percentual de Recuperação – Partição Danificada



Fonte: Do autor

Analisando o percentual de 93% de arquivos recuperados, pode ser considerado um nível alto de recuperação e satisfatório a todos aqueles que por ventura tenham perdido seus dados. Como forma de registro, os arquivos que não foram encontrados após a partição ter sido danificada, foram um arquivo de música, um arquivo de tabela, e um arquivo de vídeo. Esse resultado demonstra que é possível recuperar dados mesmo após um dano lógico na partição onde os mesmos se encontram.

7.1.2 Perda de dados devido a Tabela de Partição Formatada

Neste caso por algum motivo qualquer a partição foi reinicializada com a formatação, e assim houve perda dos dados. Os testes que foram executados e seus resultados estão descritos abaixo.

Para esse teste foi criada uma pasta no disco de teste nomeada por “Arquivos a serem recuperados de formatação”, onde dentro desta foram inseridos os mesmos 22 arquivos encontrados na figura 26. Após, foi executado o procedimento de formatação desta partição, ocasionando a perda de todos os arquivos inseridos nela.

Após a formatação, utilizou-se os seguintes softwares: Recuva, EaseUS Data Recovery, MiniTool Power data recovery, GetDataBack, Puran File Recovery e Recover My Files, e assim tentar recuperar os dados, por algum motivo os softwares Free Undelete e PC Inspector não conseguiram encontrar a partição formatada, o software Recovery não funcionou, demonstrando erro ao iniciar a execução, foi efetuado a reinstalação do mesmo por várias vezes, porém sem solução impossibilitando assim o uso do mesmo.

Os resultados demonstrados na tabela 5 foram colhidos a partir de testes feitos em um disco com a tabela de partição formatada onde foram executados os programas para a recuperação dos dados.

Tabela 5 – Resultados Partição Formatada

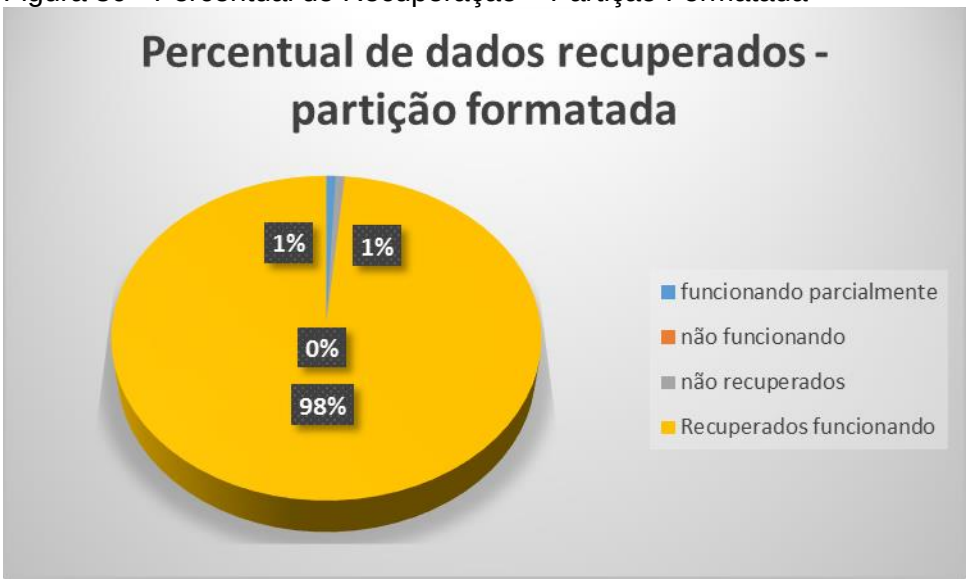
Recuperação de dados por Partição Formatada									
Métricas	EaseUs	Recuva	Minitool	GDB	Pandora	Puran	RMF	Free Undel	PC Insp.
Detecção do disco	Sim	Sim	Sim	Sim	--------	Sim	Sim	Sim	Sim
Executou o teste	Sim	Sim	Sim	Sim	--------	Sim	Sim	Não	Não
Uso da ferramenta	Fácil	Moderado	Fácil	Difícil	--------	Fácil	Fácil	--------	----------
Encontrou os arquivos	Fácil	Difícil	Fácil	Fácil	--------	Moderado	Moderado	--------	----------
Recuperação dos arquivos com seus nomes originais	Sim	Sim	Sim	Sim	--------	Não	Sim	--------	----------
Recuperação das pastas com seus nomes originais	Sim	Não	Sim	Sim	--------	Não	Não	--------	----------

Quantidade de arquivos recuperados com funcionando parcialmente	0	0	0	0	--------	1	0	--------	----------
Quantidade de arquivos recuperados não funcionando	0	0	0	0	--------	0	0	--------	----------
Quantidade de arquivos não recuperados	0	0	0	0	--------	1	0	--------	----------
Tempo de processo	1:23	01:07	1:41	1:23	--------	00:56	1:47	--------	----------
Quantidade de arquivos recuperados independente mente da situação	22	22	22	22	--------	21	22	--------	----------
Quantidade de arquivos recuperados em perfeito estado de conservação	22	22	22	22	--------	20	22	--------	----------

Fonte: Do Autor.

Nos testes efetuados pelo método de recuperação de dados em partição formatada, pôde-se observar que nem todos os softwares foram capazes de identificar partições perdidas por formatação, e dentre os outros que conseguiram rodar seus testes, observou-se que a grande maioria dos dados foi recuperada de forma íntegra. Pôde-se observar também que a varredura em discos formatados é mais rápida que em discos com a partição danificada, pois a média de tempo entre a primeira e a segunda situação demonstra isso. A demora parece estar ligada diretamente a dificuldade de encontrar os dados no disco, pois o processo mais demorado foi também o que obteve o menor percentual de recuperação. O software que procedeu de forma mais rápida foi o único que não conseguiu recuperar 100% dos dados, não encontrando um arquivo texto ou seja nesse caso a maior velocidade não necessariamente é um aliado. A figura 30 demonstra o percentual de recuperação dos dados para esse método.

Figura 30 - Percentual de Recuperação – Partição Formatada



Fonte: Do autor

Mais uma vez o gráfico demonstra um resultado muito satisfatório, com um percentual de 98% de todos os dados perdidos sendo recuperados de forma íntegra. Demonstrando assim que mesmo após a formatação de uma partição é possível recuperar dados inseridos na mesma.

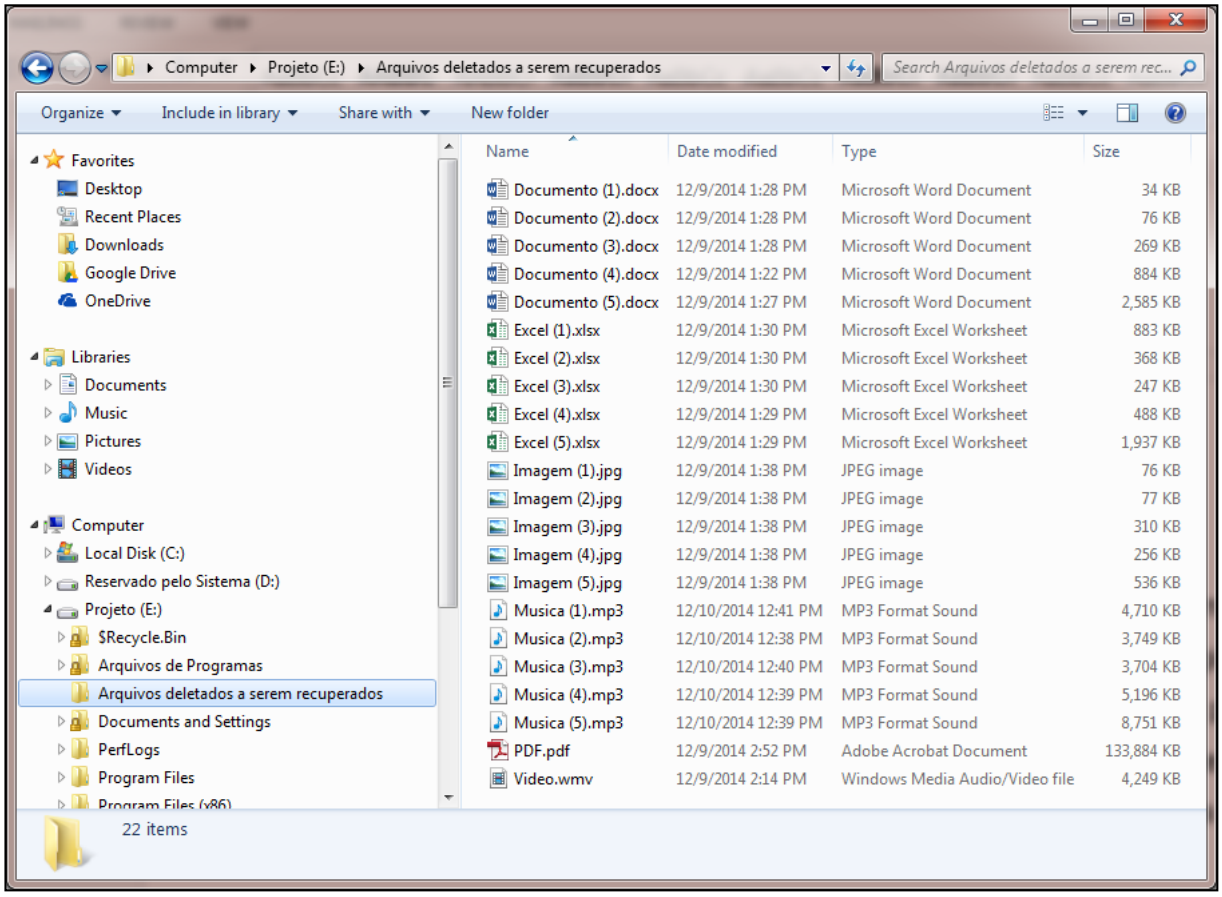
7.1.3 Perda de dados devido a Eliminação Permanente

Os arquivos quando removidos pelo usuário, geralmente param na lixeira do computador, que por muitas vezes acaba por auxiliar na recuperação de arquivos removidos acidentalmente. Mas existem usuários que tem certeza da não necessidade do arquivo, que apertam a tecla “Delete” com o “Shift” pressionado, ocasionando a eliminação permanente do arquivo, assim como aqueles que limpam a lixeira, removendo permanentemente todos os arquivos da mesma. Ao executar uma dessas ações, o usuário acredita que os arquivos foram eliminados permanentemente. O problema começa neste momento, quando os arquivos, são necessários e não mais facilmente ao alcance. Os testes que foram executados e seus resultados estão descritos abaixo.

No disco de teste foram inseridos os mesmos arquivos da figura 26, dentro de uma pasta nomeada por “Arquivos deletados a serem recuperados”

conforme demostra a figura 31. Posteriormente foi executada a eliminação permanente dos arquivos.

Figura 31 - Arquivos a serem deletados



Fonte: Do autor.

Após a eliminação dos arquivos utilizou-se os softwares: Minitool Power Data Recovery, EaseUs Data Recovery Wizard, Puran File Recovery, Recover My Files, Recuva, GetDataBack, Free Undelete e PC Inspector File Recovery já o software Pandora Recovery não funcionou, demonstrando erro ao iniciar a execução, foi efetuado a reinstalação do mesmo por várias vezes, porém sem solução, impossibilitando assim o uso do mesmo.

Os resultados demonstrados na tabela 6 foram colhidos a partir de testes feitos em um disco onde foram executados os programas para a recuperação dos dados deletados permanentemente.

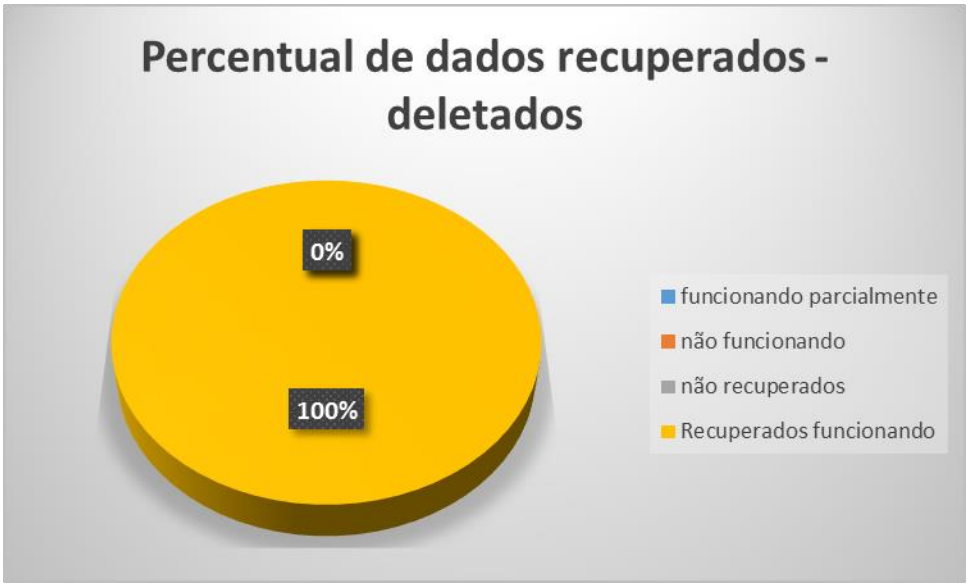
Tabela 6 - Resultados Arquivos Deletados

Métricas	EaseUs	Recuva	Minitool	GDB	Pandora	Puran	RMF	Free Undel	PC Insp
Detecção do disco	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Executou o teste	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim
Uso da ferramenta	Fácil	Moderado	Fácil	Difícil	----------	Fácil	Fácil	Fácil	Difícil
Encontrou os arquivos	Fácil	Difícil	Fácil	Difícil	----------	Fácil	Fácil	Fácil	Muito difícil
Recuperação dos arquivos com seus nomes originais	Sim	Sim	Sim	Sim	----------	Sim	Sim	Sim	Não
Recuperação das pastas com seus nomes originais	Sim	Não	Sim	Sim	----------	Sim	Sim	Sim	Não
Quantidade de arquivos recuperados com funcionando parcialmente	0	0	0	0	----------	0	0	0	0
Quantidade de arquivos recuperados não funcionando	0	0	0	0	----------	0	0	0	0
Quantidade de arquivos não recuperados	0	0	0	0	----------	0	0	0	0
Tempo de processo	0:01	0:01	0:01	0:01	----------	0:01	0:01	0:01	01:07
Quantidade de arquivos recuperados independentemente da situação	22	22	22	22	----------	22	22	22	22
Quantidade de arquivos recuperados em perfeito estado de conservação	22	22	22	22	----------	22	22	22	22

Fonte: Do Autor

No teste com deleção de arquivos, pôde-se observar que todos os softwares foram capazes de identificar a partição onde os arquivos se encontravam antes de terem sido deletados, e a grande maioria dos softwares foi capaz de executar a varredura em busca dos dados perdidos. Pôde-se observar que todos os softwares que executaram a varredura conseguiram recuperar todos os dados excluídos de forma permanente, onde todos os arquivos se mantiveram íntegros, sem qualquer dano em sua estrutura. Pôde-se observar também que o tempo de execução de praticamente todos os softwares foi extremamente rápido identificando os dados com menos de um minuto, tendo como exceção um software que demorou aproximadamente uma hora, levando a entender que os softwares com tempos parecidos trabalham de forma similar na busca das informações. Nesse caso pode-se observar que os softwares acessam de forma direta a tabela de partição e posteriormente o local de cada arquivo, que fisicamente ainda estão alocados no disco até que uma nova informação sobreponha esses dados. A figura 32 demonstra o percentual de dados recuperados após terem sido eliminados de forma permanente de dentro da partição.

Figura 32 - Percentual de Recuperação – Arquivos Deletados



Fonte: Do autor

O resultado demonstrado na figura 32 é a prova de que mesmo após a remoção permanente de um arquivo, existe a possibilidade de recuperação do mesmo. De certa forma esse processo é o mais tranquilo dentre os três métodos apresentados nesse projeto devido a tabela de partição estar intacta.

7.2 DISCUSSÃO

Os resultados desse projeto por meio dos softwares utilizados demonstraram claramente que é possível recuperar arquivos independente da maneira em que os dados foram perdidos, partição danificada ou formatada e/ou eliminação permanente. Semelhante aos achados, Santos (2002) demonstrou que os softwares *Easy Recovery* e o Norton *System Works* 2000 conseguiram recuperar os dados a partir da formatação da partição.

Yamamoto (2004) relatou a recuperação de arquivos após dano no *Master Boot Record*, setor de boot da partição, tabela de alocação de arquivos, diretório raiz, perda de arquivos por remoção ou formatação. Neste estudo, acredita-se que a recuperação de arquivos no caso de partição danificada ou formatada, ocorra através de cópia do *Bootloader,* MBR e MFT encontrados dentro do disco. Essas mesmas cópias são utilizadas pelo sistema operacional Windows quando ocorre algum problema de inicialização, ocorrendo então a restauração do sistema de forma automática. No caso de arquivos deletados de forma permanente, acredita-se que os softwares de recuperação executem uma busca por meio da palavra "File" e posteriormente avaliam os atributos desse arquivo, recuperando assim aqueles arquivos que não foram sobrepostos por outras informações.

Nesse contexto, o estudo é inovador e de extrema relevância, pois realizou-se uma descrição lógica e de fácil entendimento a respeito do funcionamento em baixo nível do sistema de arquivos NTFS, algo pouco abordado no meio acadêmico. Agrupou-se muitas informações importantes que são dificilmente encontradas em documentos científicos. Além disso, nesse trabalho foram executados diferentes testes de recuperação de dados com uma quantidade expressiva de softwares em relação aos projetos correlatos.

CONCLUSÃO

Com a popularização de equipamentos eletrônicos como computadores, notebooks, tablets, celulares entre outros, houve também um crescimento muito grande na quantidade de dados gerados pelos usuários desses equipamentos. Muitos desses dados são de suma importância para quem o possui, devido a isso, surgiu uma necessidade cada vez maior de protegê-los. Existem várias formas de proteção para esses dados, como senhas para acesso aos dispositivos, softwares sempre atualizados, uso de criptografia, e uma das formas mais seguras e utilizadas tanto por usuários domésticos como por corporações, o *backup,* porém quando a proteção não se faz suficiente e a perda dos dados ocorre, a última chance de reaver os dados perdidos é a restauração por meio de mecanismos de recuperação de dados.

Hoje no mercado existem dezenas ou até centenas de softwares para recuperação de dados, devido a isso a decisão de qual software utilizar no momento da perda, se torna uma tarefa nada fácil. Nesse momento deve-se filtrar por meio das características mais relevantes ao usuário.

Nesse estudo, pode-se concluir que os softwares EaseUs e Recover My Files, utilizados nesse trabalho, foram capazes de recuperar os diferentes arquivos deletados, independente da origem de perda, partição danificada e/ou formatada e eliminação permanente. Ademais, abordou-se sobre o funcionamento em baixo nível do sistema de arquivos NTFS e seu envolvimento na recuperação dos dados.

Com relação as dificuldades encontradas nesse projeto, a maior delas foi encontrar materiais científicos relacionados com o funcionamento dos sistemas de arquivos em baixo nível, em especifico o NTFS, e quando achados esses materiais eram muito superficiais, sem aprofundamento do assunto ou de difícil entendimento, principalmente com relação ao funcionamento da tabela de partição, MFT e armazenamento dos arquivos em baixo nível. A dificuldade no entendimento do funcionamento do sistema de arquivos foi amenizada devido a testes executados diretamente no disco rígido do computador deste projeto, onde pôde-se entender melhor os pontos chave devido a testes de criação e eliminação de arquivos e partições, observando as modificações nos mesmos.

Como proposta de trabalhos futuros, sugere-se a investigação com os mesmos softwares desse projeto no novo sistema de arquivos *Resilient Format*

System (ReFS), assim como em novos dispositivos de armazenamento SSD, para que possa ter um melhor entendimento dos mecanismos envolvidos e consequentemente um aprimoramento dos softwares utilizados com o intuito de recuperação de dados. Outra proposta para trabalhos futuros é o desenvolvimento de um software de recuperação de dados utilizando as informações contidas nesse projeto.

REFERÊNCIAS

ALMEIDA, T.H. **SISTEMAS DE ARQUIVO: ANÁLISE DE DESEMPENHO.** 2009. 26 f. Monografia (Trabalho de Conclusão de Curso em Engenharia da Computação) - Universidade São Francisco, Itatiba, 2009.

ANDERSON, D. **SATA Storage Technology:** Serial ATA. 1. ed. Colorado Springs: MindShare, 2007. 464 p.

ANDREWS, J. **A+ Guide to Hardware:** Managing, Maintaning, and Troubleshooting. 6. ed. Boston: CompTIA Certified, 2013. 754 p.

ARPACI-DUSSEAU, R.H.; ARPACI-DUSSEAU, A.C. **Operating Systems:** Three Easy Pieces. 1. ed. New York: Arpaci-Dusseau Books, 2014. 605 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Norma Brasileira **ABNT NBR ISO/IEC 17799:** Tecnologia da informação, Técnicas de segurança, Código de prática para a gestão da segurança da informação. 2 ed. Rio de Janeiro: ABNT, 2005. 120 p.

BALLONI, A.J. **Por que GESITI:** por que gestão em sistemas e tecnologias de informação? 1. ed. São Paulo: Komedi, 2006. 320 p.

BOYCE, J; TIDROW, R. **Windows® 8 Bible:** The Comprehensive Tutorial Resource. 1 ed. New York: John Wiley & Sons, Inc, 2013. 1179 p.

BRAGA, A. **A gestão da informação.** Millenium, v.19, p. 1-10, 2000.

BRASIL. Tribunal de Contas da União. **Guia de boas práticas em contratação de soluções de tecnologia da informação:** riscos e controles para o planejamento da contratação. Ed. 4. Brasília: TCU, 2012. 527 p.

BRITZ, M.T. **Computer Forensics and Cyber Crime:** An introduction. 3 ed. United States: Prentice Hall, 2013. 408 p.

CARRIER, B. **File System Forensic Analysis**. 1 ed. Upper Saddle River: Pearson Education, 2005. 382 p.

CARVALHO, M.S.; PINA, M.F.; SANTOS, S.M. **Conceitos Básicos de Sistemas de Informação Geográfica e Cartografia Aplicados à Saúde.** 1 ed. Brasília: Organização Panamericana de Saúde/Ministério da Saúde, 2000. 39 p.

CHIAVENATO, I. **Introdução à teoria geral da administraçã**o: uma visão abrangente da moderna administração das organizações. 7 ed. Rio de Janeiro: Elsevier, 2003. 633 p.

CONSELHO DA TECNOLOGIA DA INFORMAÇÃO – FECOMERCIO-SP. **Segurança da Informação para Empresas:** Soluções simples Grandes resultados. 1 ed. São Paulo: Fischer 2, 2012. 45 p.

CONVAR. 2015. Info. Disponível em:< http://www.pcinspector.de/default.htm?language=1>. Acesso em: 19 junho 2015.

COURSE TECHNOLOGY - CENGAGE LEARNING. **Computer Forensics:** Investigating Hard Disks, Files & Operating Systems. 1 ed. Clifton Park: EC-Council, 2010. 240 p.

DELL Inc. **Solid State Drive vs. Hard Disk Drive Price and Performance Study.** Mai 2011.

DRUCKER, P. **Desafios gerenciais para o século XXI**. 1 ed. São Paulo: Pioneira, 1999. 176 p.

EASEUS. 2015a. EaseUS NTFS physical structure – Feactures. Disponível em: < http://www.easeus.com/resource/ntfs-disk-structure.htm>. Acesso em: 10 abril 2015.

EASEUS. 2015b. EaseUS Data Recovery Wizard Free – Feactures. Disponível em: < http://www.easeus.com/spec/drw-free.html >. Acesso em: 19 junho 2015.

ELERATH, J. Hard Disk Drives: The Good, The Bad, and The Ugly. **ACM QUEUE**, v.5, 28-37. Set./Out. 2007.

ENGLANDER, I. **The Architecture of Computer Hardware, Systems Software, & Networking:** An Information Technology Approach. 4 ed. United States: John Wiley & Sons, 2009. 708 p.

EYGM. **Data Loss Prevention:** Keeping your sensitive data out of the public domain. Insights on governance, risk and compliance. Ernst & Young, 1-22. 2011.

FUNDACAO GETULIO VARGAS – FGV. **Tecnologia da Informação** - 23ª Pesquisa Anual do Uso de TI. São Paulo, 2012.

GARTNER. Gartner Says Worldwide Sales of Mobile Phones Declined 3 Percent in Third Quarter of 2012; Smartphone Sales Increased 47 Percent. **Newsroom.** Egham, 2012.

GETDATA. **Need File Recovery or Hard Drive Data Recovery software?** 2015. Disponível em: < http://www.recovermyfiles.com/>. Acesso em 20 junho 2015.

GUIMARÃES, R.; SANTOS, A.L. dos. Mais computadores entre os brasileiros. **GV-executivo**, v. 11, n. 2, p. 72-73, julho-dezembro, 2012.

HARDWARE**. Armazenamento de rede: DAS, NAS e SAN.** 2007. Disponível em: < http://www.hardware.com.br/tutoriais/das-nas-san/>. Acesso em 01 dezembro 2015.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Pesquisa Nacional por Amostra de Domicílios:** Acesso à Internet e Posse de Telefone Móvel Celular para Uso Pessoal. 1 ed. Rio de Janeiro: IBGE, 2011. 157 p.

INTERNATIONAL DATA CORPORATION – **IDC**. Disponível em: <http://br.idclatin.com/releases/news.aspx?id=1801>. Acesso em: 10 maio 2015.

INTEL Easy Steps. **Using external storage devices like Pen Drive, CDs and DVDs.** 2012. Disponível em: <http://download.intel.com/education/easysteps/UseExternalStorageDevices.pdf>. Acesso em: 15 maio 2015.

JANSEN W; AYERS R. **Guidelines on PDA Forensics:** Computer Security. National Institute of Standards and Technology. Special Publication 800-72. 2004. p. 67.

KARP, D.A.; RATHBONE, A. **PCs:** The Missing Manual. 1 ed. New York: O'Reilly Media, 2005. 600 p.

KIOSKEA. 2014. Disponível em: <http://ccm.net/contents/385-hard-drive>. Acesso em: 20 maio 2015.

LANDWEHR, C. E. Computer security. **International Journal of Information Security**, v. 1, n. 1, p. 3–13, 31 jan. 2014.

LAUDON, K.C; LAUDON, J.P. Management Information Systems: Managing the Digital Firm. ed 12. United States: Pearson, 2011. 672 p.

LESCA, H.; ALMEIDA, F. Administração estratégica da informação. **Revista de Administração**, v. 29, n. 3, p. 66-75, 1994.

MARCIANO, J.L.; LIMA-MARQUES, M. O enfoque social da segurança da informação. **Ciência da Informação**, v. 35, n. 3, p. 89-98, Dez 2006.

MICROSOFT. 2003a. **How NTFS Works.** Disponível em: <http://technet.microsoft.com/en-us/library/cc781134%28WS.10%29.aspx#w2k3tr_ntfs_how_rxtc>. Acesso em: 29 maio 2015.

MICROSOFT. 2003b. **What Is NTFS?** Disponível em: <https://technet.microsoft.com/en-us/library/cc778410.aspx>. Acesso em: 27 maio 2015.

MICROSOFT. 2003c. **How Basic Disks and Volumes Work.** Disponível em: <https://technet.microsoft.com/en-us/library/cc739412(v=ws.10).aspx>. Acessado em: 20 set. 2015.

MICROSOFT. 2003d. **Windows NT Boot Process and Hard Disk Constraints.** Disponível < https://support.microsoft.com/en-us/kb/114841>. Acessado em 28 set. 2015.

MICROSOFT. 2006. Disponível em: <http://support.microsoft.com/kb/103657/en-us>. Acesso em: 25 maio 2015.

MIDDLETON, B. **Cyber crime investigator's field guide.** 2 ed. Boca Raton: Auerbach, 2005. 296 p.

MINITOOL. 2015. About MiniTool® Partition Wizard. Disponível em: < http://www.powerdatarecovery.com/about.html> Acesso em: 19 junho 2015.

MORAES, G.D. de A.; TERENCE, A.C.F.; ESCRIVAO FILHO, E. A tecnologia da informação como suporte à gestão estratégica da informação na pequena empresa. **Revista de Gestão da Tecnologia e Sistemas de Informação,** v.1, n.1, p. 27-43, 2004.

MORIMOTO, C.E. 2011. Tudo sobre os HDs, flash e armazenamento. Disponível em: <http://www.hardware.com.br/guias/hds/>. Acesso em: 22 maio 2015.

NETMARKETSHARE. 2015. Disponível em: <http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>. Acesso em: 01 junho 2015.

PATTERSON, D.A.; HENNESSY, J.L. **Computer Organization and Design:** The Hardware / Software Interface. 5 ed. San Mateo: Morgan Kaufmann, 2013. p. 912.

PANDORA. 2015. Pandora Recovery Feature Overview:. Disponível em: < http://www.pandorarecovery.com/features/>. Acesso em: 19 junho 2015.

PINHEIRO, E; WEBER, W.D.; BARROSO, L.A. **Failure Trends in a Large Disk Drive Population.** USENIX Association. 5 ed USENIX Conference on File and Storage Technologies 2007.

PINHEIRO, J.M. dos S. Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar. **Cadernos UniFOA,** Volta Redonda, n. 5, p. 11-21, dez. 2007.

PIRIFORM. 2015. Recuva – Features. Disponível em: <https://www.piriform.com/recuva/features>. Acesso em: 19 junho 2015.

POPOLIN, J.G. **Análise de ferramentas para computação forense em sistemas NTFS**. 2011. 65 f. Monografia (Trabalho de Conclusão de Curso em Ciência da Computação) - Universidade Federal de Lavras, Lavras, 2011.

PURAN. 2015. Puran File Recovery Description. Disponível em: < http://www.puransoftware.com/File-Recovery.html >. Acesso em 19 junho 2015.

RECOVERONIX. 2015. File undelete software. Free for personal use. Disponível em: < http://www.officerecovery.com/freeundelete/>. Acesso em: 19 junho 2015.

REZENDE, D.A.; ABREU, A.F. **Tecnologia da Informação:** Aplicada a Sistemas de Informação Empresariais. São Paulo: Atlas, 2000.

RHODES-OUSLEY, M. **Information Security:** The Complete Reference. 2 ed. New York: Mcgraw-Hill, 2013. p. 854.

RUNTIME. 2015. GetDataBack. Disponível em: < http://www.runtime.org/data-recovery-software.htm >. Acesso em: 18 junho 2015.

RUSSINOVICH, M.; SOLOMON, D.A.; IONESCU, A. **Windows Internals:** Part 2. 6 ed. United States: Microsoft, 2012. p. 672.

SAMMES, T; JENKINSON, B. **Forensic Computing:** A practitioner's guide. 2 ed. Shrivenham: Springer, 2007. 464 p.

SANDISK. **SanDisk Ultra® Plus Solid State Drive (SSD**). Datasheet. 2012.

SANTOS, E.P. **Uma abordagem sobre recuperação de dados em disco rígido.** 2012. 82 f. Monografia (Trabalho de Conclusão de Curso em Tecnologia em Processamento de Dados) - Universidade Tiradentes, Aracaju, 2012.

SCHWARZ, T. **COEN 252 Computer Forensics NTFS.** 2007. Disponível em: <http://www.cse.scu.edu/~tschwarz/coen252_07Fall/Lectures/NTFS.html> Acesso em: 05 junho 2015.

SEAGATE. **Seagate® Barracuda® 3.5" Internal Drive Instant Add-on Storage.** 2009. Disponível em: <http://www.seagate.com/docs/pdf/datasheet/disc/ds_internal_sata.pdf>. Acesso em: 10 junho 2015.

SIQUEIRA, M.C. **Gestão estratégica da informação:** Como transformar o conteúdo informacional em conhecimento valioso. 1 ed. Rio de Janeiro: Brasport, 2005. p. 157.

SMITH, D.M. The Cost of Lost Data: The importance of investing in that "ounce of prevention" **Graziadio Business Review**, v. 6, n.3, p. 1-10, 2003.

SOUZA, A.A.; PEREIRA, F.S.; RAMOS, G.H.O.; PINTO, M.R.P.; DA SILVA, P.B.; CHAVES, S.M.F.; BARROS, V.B. **Armazenamento de Dados.** Belo Horizonte: UNIBH, 2011.

TECMUNDO. **O que é RAID?** 2009. Disponível em: <http://www.tecmundo.com.br/aumentar-desempenho/2367-o-que-e-raid-.htm> Acesso em: 01 dezembro 2015.

ULBRICH, H.C.; VALLE, J.D. **Universidade H4CK3R:** Desvendando todos os segredos do submundo dos hackers. 4. ed. São Paulo: Digerati Books, 2005. 348 p.

YAMAMOTO, M.M. **Ferramenta Recuperador de Arquivos Perdidos.** 2004. 64 f. Trabalho de Conclusão de Curso (Monografia) – Curso de Informática, Universidade Estadual de Maringá, Paraná, 2004.

Apêndice

Métodos de recuperação de dados em disco rígido com partição NTFS

Willian Antunes Crescencio[1], Paulo João Martins[1]

[1]Departamento de Ciências da Computação

Universidade do Extremo Sul Catarinense (UNESC) – Criciúma, SC - Brazil

willianantunes1980@hotmail.com, pjm@unesc.net

Abstract. *The information is composed of interpreted data, endowed with relevance and purpose, being the input most important of human production. However, even with all data protection mechanisms existents may occur problems loss of information. Thus, needs to know mechanisms and procedures for recovery of this information. This work has the purpose to recover data due to partition loss, formatting and deleting files on hard disks with New Technology Format System (NTFS). As well as, to understand the functioning of NTFS file systems. Regarding methods, it was carried out bibliographical research; prepared a case study simulating the loss and recovery of data due to partition loss, formatting and deleting files on hard drives with NTFS. The results showed that the data recovery percentage due to damaged partition was 93%, formatted partition was 98% and permanent file deletion was 100%. Therefore, we can conclude that was possible to recover most of the data, regardless of the origin of loss. Furthermore, we approach the operation in low-level file system NTFS and its involvement in data recovery.*

Keyword: Information; Data recovery; NTFS; MBR; MFT.

Resumo. *A informação é composta de dados interpretados, dotados de relevância e propósito, sendo o insumo mais importante da produção humana. Entretanto, mesmo com todos os mecanismos de proteção de dados existentes, podem ocorrer problemas de perda de informação. Desta forma, necessita-se conhecer mecanismos e procedimentos, para recuperação destas informações. Esse trabalho tem por propósito recuperar dados devido à perda de partição, formatação e eliminação de arquivos em discos rígidos com New Technology Format System (NTFS). Assim, como compreender sobre o funcionamento de sistemas de arquivos NTFS. Referente aos métodos, foi realizado pesquisa bibliográfica; elaborado um estudo de caso simulando a perda e recuperação de dados devido à perda de partição, formatação e eliminação de arquivos em discos rígidos com NTFS. Os resultados demostraram que o percentual de recuperação de*

dados devido a partição danificada foi de 93%, partição formatada 98% e eliminação permanente de arquivos foi de 100%. Assim, podemos concluir que foi possível recuperar a maioria dos dados, independente da origem de perda. Ademais, abordamos o funcionamento em baixo nível do sistema de arquivos NTFS e seu envolvimento na recuperação dos dados.

Palavra-chave: Informação; Recuperação de dados; NTFS; MBR; MFT.

1. Introdução

A informação nada mais é que dados com relevância a quem o possui [Chiavenato, 2003]. A informação é de grande importância tanto para as pessoas como empresas [Carvalho; Pina; Santos, 2000]. Ela pode ser armazenada em meios magnéticos, que por sua vez, são suscetíveis a defeito [Souza et al, 2011]. Assim, para assegurar a não perda de informações, é necessário se ter uma política de segurança, pois, a informação é considerada o principal patrimônio de uma organização [Brasil, 2012].

Mesmo com toda proteção, existem muitos motivos que levam a perda, dentre eles, perda ou roubo de laptops e dispositivos móveis, transferência não autorizada de dados para dispositivos Universal Serial Bus (USB), roubo de dados por funcionários ou estranhos, impressão e cópia de dados confidenciais, transmissão não intencional de dados confidenciais [EYGM, 2011].

Devido ao exposto, o objetivo geral consiste em recuperar dados devido à perda de partição, formatação e eliminação de arquivos em discos rígidos com NTFS. Os objetivos específicos consistem em compreender sobre segurança da informação, aplicar os conceitos acerca dos tipos de perda de informação compreender sobre o funcionamento de sistemas de arquivos NTFS, recuperar dados de perda de partição, formatação e eliminação de arquivos, por meio de alguns softwares e documentar os testes realizados.

2. Justificativa

A informação é o insumo mais importante da produção humana [Drucker, 1999]. Uma pesquisa mostra que cerca de quarenta e três por cento das empresas brasileiras tiveram algum problema relacionado a segurança das suas informações [Ulbrich and Valle, 2005]. De outro lado, existe o usuário doméstico, que tem a necessidade de armazenar fotos, documentos pessoais, contábeis, entre outros. E caso ocorra perda destes dados pode ser prejudicial. Todavia, pode-se proteger as informações com algumas atitudes básicas tais como: antispyware e antivírus atualizados, controle de acesso lógico ou físico, criptografia, firewall, espelhamento, backup, entre outras formas [Fecomercio-SP, 2012]. Entretanto, mesmo com

todas estas providências, podem ocorrer problemas de perda de informação. Desta forma, necessita-se conhecer mecanismos e procedimentos, para recuperação destas informações.

3. Metodologia

Para a execução do projeto, determinou-se as formas de perda de dados a serem trabalhadas, que para esse projeto foram definidas as seguintes: Perda de dados por tabela de partição danificada, perda de dados por formatação da tabela de partição e arquivos permanentemente deletados. Posteriormente foram definidos os hardwares a serem utilizados na execução deste projeto. Um computador completo com sistema operacional que suporte o tipo de partição NTFS e dois discos rígidos. Posteriormente foram identificados os softwares que seriam utilizados no projeto. O sistema operacional utilizado foi o Windows 7, o software de edição de Tabela de partição foi "HxD" desenvolvido pela empresa alemã Maël Hörz além dos softwares de recuperação de dados utilizados no projeto: Recuva, Minitool Power Data Recovery, GetDataBack, EaseUs Data Recovery Wizard, Pandora Recovery, Puran File Recovery, Recover My Files, Free Undelete e PC Inspector File Recovery.

Por fim, foram especificados os tipos e quantidades de arquivos utilizados no projeto, tornando assim um ambiente controlado, porém o mais próximo possível da realidade. A escolha desses arquivos se deu por serem os tipos mais comuns de arquivos encontrados e utilizados em computadores pessoais, e dentre os mais utilizados, estão arquivos de imagem, musicas, documentos texto e tabelas, devido a isso foram criados cinco arquivos para cada um desses formatos e todos com tamanhos diferentes, além de um arquivo PDF e um arquivo de vídeo, totalizando 22 arquivos.

3.1. Perda de dados devido a Tabela de Partição Danificada

Quando ao carregar o Windows, o computador fica processando continuamente sem completar o carregamento, apresenta mensagens que o sistema de arquivos é inválido ou está danificado, está faltando arquivo dentre outras mensagens informando que aquela partição não está de acordo com os parâmetros exigidos. Esses são alguns dos sintomas que a partição do Windows está danificada, tornando inacessível todos os dados que estão inseridos nela.

Para provocar o dano na partição foi efetuado um procedimento por meio do software HxD, onde foi colocado 00 em todos os 16 bytes da tabela de partição onde se encontrava a partição inicializável.

Após eliminar todas as informações da partição onde se encontravam os arquivos, a partição ficou inacessível, deixando de ser mostrada ao usuário dentro do sistema operacional.

Após provocado o dano na partição, foram executados os softwares de recuperação de dados em partição danificada. Como mencionado nesse projeto, foram executados os softwares Minitool Power Data Recovery, EaseUs Data Recovery Wizard, Puran File Recovery, Recover My Files, já os softwares Recuva, GetDataBack, Pandora Recovery, Free Undelete e PC Inspector File Recovery não encontraram a partição danificada, impossibilitando assim o uso dos mesmos.

Na sequência estão dispostos os resultados obtidos para esse teste. Os resultados encontram-se na figura 1, onde os testes realizados em um disco com a tabela de partição danificada.

Recuperação de dados por Partição Danificada

Métricas	EaseUs	Recuva	Minitool	GDB	Pandora	Puran	RMF	Free Undel.	PC Insp.
Detecção do disco	Sim	Não	Sim	Não	Não	Sim	Sim	Não	Não
Executou o teste	Sim	----------	Sim	-------	----------	Sim	Sim	----------	-------
Uso da ferramenta	Fácil	----------	Fácil	-------	----------	Fácil	Fácil	----------	-------
Encontrou os arquivos	Fácil	----------	Difícil	-------	----------	Fácil	Fácil	----------	-------
Recuperação dos arquivos com seus nomes originais	Sim	----------	Não	-------	----------	Sim	Sim	----------	-------
Recuperação das pastas com seus nomes originais	Sim	----------	Não	-------	----------	Sim	Sim	----------	-------
QTD arquivos recup. com funcionando parcialmente	0	----------	1	-------	----------	0	0	----------	-------
QTD arquivos recup. não funcionando	0	----------	2	-------	----------	0	0	----------	-------
QTD arquivos não recuperados	0	----------	3	-------	----------	0	0	----------	-------
Tempo de processo	**2:47**	----------	1:48	-------	----------	1:52	**0:46**	----------	-------
QTD arquivos recup. independentemente da situação	**22**	----------	19	-------	----------	**22**	**22**	----------	-------
QTD arquivos recup. em perfeito estado de conservação	**22**	----------	16	-------	----------	**22**	**22**	----------	-------

Figura 1 - Resultados Partição Danificada

O teste com partição danificada, teve um menor índice de recuperação dos dados, onde mais de 50% não foi capaz de identificar a partição danificada. Isso não significa que os softwares que não encontraram a partição, não funcionam, como existem muitas formas de danificar a mesma, certamente em outras formas de dano estes softwares podem funcionar normalmente, caso contrário eles não seriam anunciados para esta finalidade. Dentre os que conseguiram identificar a partição, o nível de recuperação também não foi tão alto quando os outros testes. Em relação ao tempo de execução, pôde-se observar que existe uma grande diferença entre os softwares, onde alguns chegaram a atingir o triplo do tempo de outros, porém o tempo não foi determinante para indicar o software com melhores resultados, pois tanto o que executou em menor tempo quanto o de maior tempo recuperaram todos os arquivos em perfeito estado. O percentual de recuperação dos dados além de ter sido menor que os outros testes, não decepcionou, como demonstrado na figura 2, possibilitando assim recuperar a grande maioria dos dados de forma íntegra.

Figura 2 - Percentual de Recuperação – Partição Danificada

Analisando o percentual de 93% de arquivos recuperados, pode ser considerado um nível alto de recuperação e satisfatório a todos aqueles que por ventura tenham perdido seus dados. Como forma de registro, os arquivos que não foram encontrados após a partição ter sido danificada, foram um arquivo de música, um arquivo de tabela, e um arquivo de vídeo. Esse resultado demonstra que é possível recuperar dados mesmo após um dano lógico na partição onde os mesmos se encontram.

3.2. Perda de dados devido a Tabela de Partição Formatada

Este caso ocorre quando por algum motivo a partição é formatação, havendo assim perda dos dados. Os testes que foram executados e seus resultados estão descritos abaixo.

Para esse teste foi criada uma pasta no disco de teste, onde dentro foram inseridos os mesmos 22 arquivos descritos na metodologia. Após, foi executado o procedimento de formatação desta partição, ocasionando a perda de todos os arquivos inseridos nela.

Após a formatação, utilizou-se os seguintes softwares: Recuva, EaseUS Data Recovery, MiniTool Power data recovery, GetDataBack, Puran File Recovery e Recover My Files, e assim tentar recuperar os dados, por algum motivo os softwares Free Undelete e PC Inspector não conseguiram encontrar a partição formatada, o software Recovery não funcionou, demonstrando erro ao iniciar a execução, foi efetuado a reinstalação do mesmo por várias vezes, porém sem solução impossibilitando assim o uso do mesmo.

Os resultados demonstrados na figura 3 foram colhidos a partir de testes feitos em um disco com a tabela de partição formatada onde foram executados os programas para a recuperação dos dados.

Recuperação de dados por Partição Formatada									
Métricas	**EaseUs**	**Recuva**	**Minitool**	**GDB**	**Pandora**	**Puran**	**RMF**	**Free Undel**	**PC Insp.**
Detecção do disco	Sim	Sim	Sim	Sim	--------	Sim	Sim	Sim	Sim
Executou o teste	Sim	Sim	Sim	Sim	--------	Sim	Sim	Não	Não
Uso da ferramenta	Fácil	Moderado	Fácil	Difícil	--------	Fácil	Fácil	--------	----------
Encontrou os arquivos	Fácil	Difícil	Fácil	Fácil	--------	Moderado	Moderado	--------	----------
Recuperação dos arquivos com seus nomes originais	Sim	Sim	Sim	Sim	--------	Não	Sim	--------	----------
Recuperação das pastas com seus nomes originais	Sim	Não	Sim	Sim	--------	Não	Não	--------	----------
QTD arquivos recup. com funcionando parcialmente	0	0	0	0	--------	1	0	--------	----------
QTD arquivos recup. não funcionando	0	0	0	0	--------	0	0	--------	----------
QTD arquivos não recuperados	0	0	0	0	--------	1	0	--------	----------
Tempo de processo	1:23	1:07	1:41	1:23	--------	0:56	1:47	--------	----------
QTD arquivos recup. independentemente da situação	22	22	22	22	--------	21	22	--------	----------
QTD arquivos recup. em perfeito estado de conservação	22	22	22	22	--------	20	22	--------	----------

Figura 3 – Resultados Partição Formatada

Nos testes efetuados pelo método de recuperação de dados em partição formatada, pôde-se observar que nem todos os softwares foram capazes de identificar partições perdidas por formatação, e dentre os outros que conseguiram rodar seus testes, observou-se que a grande maioria dos dados foi recuperada de forma íntegra. Pôde-se observar também que a varredura em discos formatados é mais rápida que em discos com a partição danificada, pois a média de tempo entre a primeira e a segunda situação demonstra isso. A demora parece estar ligada diretamente a dificuldade de encontrar os dados no disco, pois o processo mais demorado foi também o que obteve o menor percentual de recuperação. O software que procedeu de forma mais rápida foi o único que não conseguiu recuperar 100% dos dados, não encontrando um arquivo texto ou seja nesse caso a maior velocidade não necessariamente é um aliado. A figura 4 demonstra o percentual de recuperação dos dados para esse método.

Figura 4 - Percentual de Recuperação – Partição Formatada

Mais uma vez o gráfico demonstra um resultado muito satisfatório, com um percentual de 98% de todos os dados perdidos sendo recuperados de forma íntegra. Demonstrando assim

que mesmo após a formatação de uma partição é possível recuperar dados inseridos na mesma.

3.3. Perda de dados devido a Eliminação Permanente

Os arquivos quando removidos pelo usuário, geralmente param na lixeira do computador, que por muitas vezes acaba por auxiliar na recuperação de arquivos removidos acidentalmente. Mas existem usuários que tem certeza da não necessidade do arquivo, que apertam a tecla “Delete” com o “Shift” pressionado, ocasionando a eliminação permanente do arquivo, assim como aqueles que limpam a lixeira, removendo permanentemente todos os arquivos da mesma. Ao executar uma dessas ações, o usuário acredita que os arquivos foram eliminados permanentemente. O problema começa neste momento, quando os arquivos, são necessários e não mais facilmente ao alcance. Os testes que foram executados e seus resultados estão descritos abaixo.

No disco de teste foram inseridos os mesmos 22 arquivos dos testes anteriores, dentro de uma pasta. Posteriormente foi executada a eliminação permanente dos arquivos.

Após a eliminação dos arquivos utilizou-se os softwares: Minitool Power Data Recovery, EaseUs Data Recovery Wizard, Puran File Recovery, Recover My Files, Recuva, GetDataBack, Free Undelete e PC Inspector File Recovery já o software Pandora Recovery não funcionou, demonstrando erro ao iniciar a execução, foi efetuado a reinstalação do mesmo por várias vezes, porém sem solução, impossibilitando assim o uso do mesmo.

Os resultados demonstrados na figura 5 foram colhidos a partir de testes feitos em um disco onde foram executados os programas para a recuperação dos dados deletados permanentemente.

Recuperação de dados Deletados									
Métricas	EaseUs	Recuva	Minitool	GDB	Pandora	Puran	RMF	Free Undel	PC Insp
Detecção do disco	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Executou o teste	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim
Uso da ferramenta	Fácil	Moderado	Fácil	Difícil	----------	Fácil	Fácil	Fácil	Difícil
Encontrou os arquivos	Fácil	Difícil	Fácil	Difícil	----------	Fácil	Fácil	Fácil	Muito difícil
Recuperação dos arquivos com seus nomes originais	Sim	Sim	Sim	Sim	----------	Sim	Sim	Sim	Não
Recuperação das pastas com seus nomes originais	Sim	Não	Sim	Sim	----------	Sim	Sim	Sim	Não
QTD arquivos recup. com funcionando parcialmente	0	0	0	0	----------	0	0	0	0
QTD arquivos recup. não funcionando	0	0	0	0	----------	0	0	0	0
QTD arquivos não recuperados	0	0	0	0	----------	0	0	0	0
Tempo de processo	0:01	0:01	0:01	0:01	----------	0:01	0:01	0:01	1:07
QTD arquivos recup. independentemente da situação	22	22	22	22	----------	22	22	22	22
QTD arquivos recup. em perfeito estado de conservação	22	22	22	22	----------	22	22	22	22

Figura 5 - Resultados Arquivos Deletados

No teste com deleção de arquivos, pôde-se observar que todos os softwares foram capazes de identificar a partição onde os arquivos se encontravam antes de terem sido deletados, e a grande maioria dos softwares foi capaz de executar a varredura em busca dos

dados perdidos. Pôde-se observar que todos os softwares que executaram a varredura conseguiram recuperar todos os dados excluídos de forma permanente, onde todos os arquivos se mantiveram íntegros, sem qualquer dano em sua estrutura. Pôde-se observar também que o tempo de execução de praticamente todos os softwares foi extremamente rápido identificando os dados com menos de um minuto, tendo como exceção um software que demorou aproximadamente uma hora, levando a entender que os softwares com tempos parecidos trabalham de forma similar na busca das informações. Nesse caso pode-se observar que os softwares acessam de forma direta a tabela de partição e posteriormente o local de cada arquivo, que fisicamente ainda estão alocados no disco até que uma nova informação sobreponha esses dados. A figura 6 demonstra o percentual de dados recuperados após terem sido eliminados de forma permanente de dentro da partição.

Figura 6 - Percentual de Recuperação – Arquivos Deletados

O resultado demonstrado na figura 32 é a prova de que mesmo após a remoção permanente de um arquivo, existe a possibilidade de recuperação do mesmo. De certa forma esse processo é o mais tranquilo dentre os três métodos apresentados nesse projeto devido a tabela de partição estar intacta.

4. Discussão

Os resultados desse projeto por meio dos softwares utilizados demonstraram claramente que é possível recuperar arquivos independente da maneira em que os dados foram perdidos, partição danificada ou formatada e/ou eliminação permanente. Semelhante aos achados, Santos (2012) demonstrou que os softwares Easy Recovery e o Norton System Works 2000 conseguiram recuperar os dados a partir da formatação da partição.

Yamamoto (2004) relatou a recuperação de arquivos após dano no Master Boot Record, setor de boot da partição, tabela de alocação de arquivos, diretório raiz, perda de arquivos por remoção ou formatação. Neste estudo, acredita-se que a recuperação de arquivos no caso de partição danificada ou formatada, ocorra através de cópia do Bootloader, MBR e MFT encontrados dentro do disco. Essas mesmas cópias são utilizadas pelo sistema operacional Windows quando ocorre algum problema de inicialização, ocorrendo então a restauração do sistema de forma automática. No caso de arquivos deletados de forma permanente, acredita-se que os softwares de recuperação executem uma busca por meio da palavra "File" e posteriormente avaliam os atributos desse arquivo, recuperando assim aqueles arquivos que não foram sobrepostos por outras informações.

Nesse contexto, o estudo é inovador e de extrema relevância, pois realizou-se uma descrição lógica e de fácil entendimento a respeito do funcionamento em baixo nível do sistema de arquivos NTFS, algo pouco abordado no meio acadêmico. Agrupou-se muitas informações importantes que são dificilmente encontradas em documentos científicos. Além disso, nesse trabalho foram executados diferentes testes de recuperação de dados com uma quantidade expressiva de softwares em relação aos projetos correlatos.

5. Conclusão

Com a popularização de equipamentos eletrônicos como computadores, notebooks, tablets, celulares entre outros, houve também um crescimento muito grande na quantidade de dados gerados pelos usuários desses equipamentos. Muitos desses dados são de suma importância para quem o possui, devido a isso, surgiu uma necessidade cada vez maior de protegê-los. Existem várias formas de proteção para esses dados, como senhas para acesso aos dispositivos, softwares sempre atualizados, uso de criptografia, e uma das formas mais seguras e utilizadas tanto por usuários domésticos como por corporações, o backup, porém quando a proteção não se faz suficiente e a perda dos dados ocorre, a última chance de reaver os dados perdidos é a restauração por meio de mecanismos de recuperação de dados.

Hoje no mercado existem dezenas ou até centenas de softwares para recuperação de dados, devido a isso a decisão de qual software utilizar no momento da perda, se torna uma tarefa nada fácil. Nesse momento deve-se filtrar por meio das características mais relevantes ao usuário.

Nesse estudo, pode-se concluir que os softwares EaseUs e Recover My Files, utilizados nesse trabalho, foram capazes de recuperar os diferentes arquivos deletados, independente da origem de perda, partição danificada e/ou formatada e eliminação permanente. Ademais,

abordou-se sobre o funcionamento em baixo nível do sistema de arquivos NTFS e seu envolvimento na recuperação dos dados.

Com relação as dificuldades encontradas nesse projeto, a maior delas foi encontrar materiais científicos relacionados com o funcionamento dos sistemas de arquivos em baixo nível, em especifico o NTFS, e quando achados esses materiais eram muito superficiais, sem aprofundamento do assunto ou de difícil entendimento, principalmente com relação ao funcionamento da tabela de partição, MFT e armazenamento dos arquivos em baixo nível. A dificuldade no entendimento do funcionamento do sistema de arquivos foi amenizada devido a testes executados diretamente no disco rígido do computador deste projeto, onde pôde-se entender melhor os pontos chave devido a testes de criação e eliminação de arquivos e partições, observando as modificações nos mesmos.

Como proposta de trabalhos futuros, sugere-se a investigação com os mesmos softwares desse projeto no novo sistema de arquivos Resilient Format System (ReFS), assim como em novos dispositivos de armazenamento SSD, para que possa ter um melhor entendimento dos mecanismos envolvidos e consequentemente um aprimoramento dos softwares utilizados com o intuito de recuperação de dados. Outra proposta para trabalhos futuros é o desenvolvimento de um software de recuperação de dados utilizando as informações contidas nesse projeto.

Referências

Brasil. Tribunal de Contas da União (2012). “Guia de boas práticas em contratação de soluções de tecnologia da informação: riscos e controles para o planejamento da contratação. ” 4ª Edição. Brasília: TCU, 2012. Página 527.

Carvalho, M.S.; Pina, M.F.; Santos, S.M. (2000) “Conceitos Básicos de Sistemas de Informação Geográfica e Cartografia Aplicados à Saúde.” 1 ed. Brasília: Organização Panamericana de Saúde/Ministério da Saúde. Página 39.

Chiavenato, I. (2003) “Introdução à teoria geral da administração: uma visão abrangente da moderna administração das organizações. ” 7a edição. Rio de Janeiro: Elsevier. Página 633.

EYGM. (2011) “Data Loss Prevention: Keeping your sensitive data out of the public domain. Insights on governance, risk and compliance.” Ernst & Young, Páginas 1-22.

Fecomercio-SP - Conselho da Tecnologia da Informação. (2012) “Segurança da Informação para Empresas: Soluções simples Grandes resultados. ” 1a edição. São Paulo: Fischer 2. Página 45.

Santos, E.P. (2012) “Uma abordagem sobre recuperação de dados em disco rígido. 82 f. Monografia (Trabalho de Conclusão de Curso em Tecnologia em Processamento de Dados) ” - Universidade Tiradentes, Aracaju.

Souza, A.A.; Pereira, F.S.; Ramos, G.H.O.; Pinto, M.R.P.; Da Silva, P.B.; Chaves, S.M.F.; Barros, V.B. (2011) “Armazenamento de Dados. ” Belo Horizonte: UNIBH.

Ulbrich, H.C.; Valle, J.D. (2005) “Universidade H4CK3R: Desvendando todos os segredos do submundo dos hackers. ” 4a edição. São Paulo: Digerati Books. Página 348.

Yamamoto, M.M. (2004) “Ferramenta Recuperador de Arquivos Perdidos. ”, Trabalho de Conclusão de Curso (Monografia) – Curso de Informática, Universidade Estadual de Maringá, Paraná.