

## **Componentes Funcionais Do Computador**

### **O Que É O Computador?**

Um computador é um dispositivo eletrônico controlado por um programa (chamado sistema operacional) , usado para processar dados.

Ele é constituído por componentes eletrônicos, especialmente circuitos integrados, miniaturizados e encaixados em pequeno pedaço de silício, usualmente chamado chip.

Esses circuitos integrados, os chips, são a essência dos computadores modernos, porque são eles que executam todas as operações. Tais operações, que os circuitos integrados executam, são controladas por um programa.

Sem um programa, um computador reduz-se a um conjunto de partes eletrônicas, que nada pode fazer.

Esse programa (o sistema operacional) é um conjunto ordenado de instruções que determina o que o computador deve fazer.

### **Processamento De Dados**

Em informática, e mais especialmente em computadores, a organização básica de um sistema será na forma de:

#### **Entrada > Processamento > Saída**

Dispositivos de entrada são os equipamentos através dos quais podemos introduzir dados no computador. Alguns permitem a intervenção direta do homem, como por exemplo, o teclado.

Processamento pode ser definido como sendo a maneira pela qual os dados de entrada serão organizados, modificados, transformados ou agrupados de alguma forma, gerando-se assim uma informação de saída.

Dispositivos de saída são os equipamentos através dos quais são geradas as informações resultantes do processamento. Por exemplo, o monitor de vídeo e a impressora.

### **Conceitos Fundamentais Da Informática**

É chamado de sistema de computação, o conjunto de hardware e software através do qual executamos um processamento.

O **HARDWARE** é o equipamento físico, representado no computador por suas partes mecânicas, eletrônicas e magnéticas. A máquina em si, tudo o que se pode tocar. Pode ser basicamente formado por: unidade central de processamento, memória e unidades de entrada ou saída de dados.

O **SOFTWARE** é o conjunto de programas (instruções) que faz com que o computador realize o processamento e produza o resultado desejado.

Para facilitar o entendimento, podemos dizer que um toca discos está para o hardware, assim como a música está para o software, ou seja, o seu equipamento (hardware) só tem utilidade com o auxílio de programas (software).

### **Hardware – Componentes Funcionais Do Computador**

#### **Unidade Central De Processamento (UCP Ou CPU)**

A unidade central de processamento ou processador central tem por função executar os programas armazenados na memória principal, buscando cada instrução, interpretando-a e depois a executando. Ela compreende duas grandes subunidades, conhecidas como unidade de controle (UC) e unidade lógica e aritmética (ULA), cujas funções serão mais bem descritas a seguir:

**Unidade de Controle:** Essa unidade supervisiona todas as operações do computador, sob a direção de um programa armazenado. Primeiro ela determina que instrução será executada pelo computador, e depois procura essa instrução na memória interna e a interpreta. A instrução é então executada por outras unidades do computador, sob a sua direção.

**Unidade Lógica e Aritmética:** Essa é unidade que executa as operações aritméticas e lógicas dirigidas pela Unidade de Controle.

Operações lógicas são de forma simples, a habilidade de comparar coisas para tomada de decisão.

Esta habilidade para testar (ou comparar) dois números e ramificar para um dos muitos caminhos alternativos possíveis, dependendo do resultado da comparação, dá ao computador muitas força e habilidade e é uma das razões principais para o uso dos computadores digitais em diferentes aplicações, tanto administrativas como técnicas.

### **Memória**

A memória é um componente que tem por função armazenar internamente toda informação que é manipulada pela máquina: os programas (conjunto de instruções) e os dados. A capacidade de armazenar um programa é uma característica que permite o processamento automático de dados.

A memória é em geral, classificada em dois grandes tipos:

Memória Principal (MP)

Memória Secundária (MS) ou auxiliar ou de massa

### **Memória Principal**

A memória principal é a memória de armazenamento temporário, que armazena os programas e os dados que estão sendo processados, somente durante o processamento. É uma memória volátil (RAM), pois os dados só permanecem nela armazenados enquanto houver energia elétrica. Na falta de energia, quando o computador for desligado, todos os dados são perdidos.

Há alguns conceitos que devem ser conhecidos para que se possa melhor compreender a memória principal nos computadores atuais:

### **RAM – Random Access Memory (Memória de Acesso Aleatório ou Randômico)**

É usada para o armazenamento temporário de dados ou instruções.

Quando escrevemos um texto num computador, as informações são armazenadas na memória RAM, assim como os dados de entrada.

A RAM também é conhecida como memória de escrita e leitura, pois lemos ou escrevemos informações neste tipo de memória.

### **ROM – Read Only Memory (Memória só de Leitura)**

É usada para armazenar instruções e/ou dados permanentes ou raramente alterados. A informação geralmente é colocada no chip de armazenamento quando ele é fabricado e o conteúdo da ROM não pode ser alterado por um programa de usuário. Por esse motivo é uma memória só de leitura.

A ROM se constitui em um chip que possui um software determinado e não apagável pelo usuário. Desta forma a ROM incorpora as idéias de hardware e software (a isto se dá o nome de firmware).

Portanto, firmware, é um hardware que contém um software já determinado, associando assim as duas capacidades. Ex: fita de videogame

Em resumo, a informação armazenada em ROM não é volátil, ou seja, não é perdida quando o fornecimento de energia externa do computador é interrompido. Já a RAM é volátil, pois as

informações armazenadas são perdidas quando a energia é cortada.

### **Memória Secundária**

A memória secundária é a memória de armazenamento permanente, que armazena os dados permanentemente no sistema, sem a necessidade de energia elétrica e, por esse motivo, conhecida como memória não volátil. Ela funciona como complemento da memória principal para guardar dados.

O computador só consegue processar o que está na memória principal, assim como ocorre conosco. Na verdade, só conseguimos processar o que está na nossa memória. Por exemplo, só podemos discar um número telefônico do qual nos lembramos, o qual esteja na nossa memória. Se não lembrarmos, temos que recorrer a uma memória auxiliar, representada neste caso por uma agenda telefônica e só então estaremos em condições de discar.

Como exemplos de memória secundária podemos citar o disquete, o disco rígido e o CD-ROM.

### **Unidades de Entrada e Saída**

Os dispositivos de E/S (Entrada e Saída) servem basicamente para a comunicação do computador com o meio externo. Eles provêm o modo pelo qual as informações são transferidas de fora para dentro da máquina, e vice-versa, além de compatibilizar esta transferência através do equilíbrio de velocidade entre os meios diferentes. Entre estes componentes podemos mencionar o teclado, o vídeo e a impressora.

Teclado (Periférico de Entrada): É sem dúvida o mais importante meio de entrada de dados, no qual estabelece uma relação direta entre o usuário e o equipamento.

Drive (Periférico de Entrada e Saída): Conhecido também como "Unidade de Disco" ou "acionador", o drive, tem como função fazer o disco girar (dentro do envelope) numa velocidade constante e transferir programas ou dados do disco para o computador. Essa operação é feita através de uma cabeça de leitura e gravação que se move para trás e para frente na superfície do disco. Os dados gravados em disco podem ser lidos e utilizados como fonte de consulta em uma operação futura.

Winchester, Disco Rígido ou HD (Periférico de Entrada e Saída): Semelhantemente aos drives em utilização e funcionamento, tem como principal diferença, a inviolabilidade, a maior capacidade de armazenamento e a maior velocidade de operação.

É composto por uma série de discos de material rígido, agrupados em um único eixo, possuindo cada disco um cabeçote. Os cabeçotes flutuam sobre a superfície do disco apoiados num colchão de ar, isso significa que eles devem ser conservados em caixas hermeticamente fechadas para evitar problemas causados pela poeira e outros elementos estranhos.

As unidades winchester devem receber um cuidado maior por guardarem maiores quantidades de informações, pois qualquer trepidação pode fazer com que o cabeçote encoste-se ao disco, danificando os dados.

Vídeo ou Monitor (Periférico de Saída): Utilizado basicamente para a saída de informações, o vídeo é o canal por onde o computador apresenta informações ao operador. Em geral é conectado à placa de sistema por meio de um adaptador monocromático de alta-resolução ou por um adaptador colorido-gráfico.

Caneta Óptica (Periférico de Entrada): A caneta óptica é um instrumento cilíndrico bastante parecido com uma caneta comum (daí seu nome), que tem um fio semelhante ao de um telefone em uma das extremidades. Quando se encosta a caneta óptica na tela, o computador é capaz de detectar exatamente a posição apontada (em alguns sistemas pressiona-se a caneta na tela, para ativar o interruptor existente em seu interior).

A caneta óptica nada mais é do que um sensor óptico, que ao ser apontada na tela do monitor, a coincidência da varredura no ponto onde está a caneta provoca um mapeamento da tela e, portanto, permite até desenhar diretamente na tela.

A caneta óptica é usada mais comumente para escolher um dos itens mostrados na tela. Reconhecendo o ponto indicado pela caneta, o computador reduz o caracter ou símbolo a que o ponto se refere.

**Mouse (Periférico de Entrada):** Há algum tempo atrás, o único modo de fazer um computador funcionar era registrar uma função através do teclado. Por ser esta uma tarefa cansativa que poderia estar fazendo as pessoas deixarem de utilizar os computadores, os fabricantes encontraram a solução brilhante e simples do "mouse".

O mouse é colocado sobre qualquer superfície plana e, quando se move, movimenta também o cursor na tela com extrema agilidade. Assim, uma pessoa pode fazer um movimento para qualquer parte da tela, pressionar o botão e dar andamento à operação desejada. O mouse é utilizado em programas gráficos para traçar linhas ou "pintar" cores na tela e em programas com grande número de menus de opções.

**Joystick (Periférico de Entrada):** Esse tipo de controle manual foi desenvolvido baseado no manche com que o piloto manobra o avião. Geralmente é utilizado para jogos semelhantes aos fliperamas. A espaçonave, ou qualquer outro objeto controlado na tela pelo joystick, move-se na mesma direção que ele. Quando o joystick é movido para frente, a espaçonave avança na tela. O aparelho tem quatro chaves elétricas dispostas de tal forma que, quando o joystick é movimentado apenas um dos contatos se fecha. Cada chave envia sua própria mensagem para o computador: para cima, para baixo, para a esquerda ou para a direita.

Alguns deles são dotados ainda de um botão lateral de disparo (de mísseis, balas, ou eventos, dependendo do programa usado) para ser operado com a mão que estiver desocupada. Em alguns modelos, no entanto, basta que se aperte um botão disparador com o polegar.

**Impressoras (Periférico de Saída):** Existem três tipos principais de impressoras para microcomputador: Matricial (ou de Matriz de Pontos), Jato de Tinta e Laser. São utilizados para a saída de dados.

### **Matricial**

A tecnologia mais comum de impressão é o da matriz de pontos, que funciona por meio de uma cabeça de impressão contendo um grupo de agulhas. Os caracteres são impressos no papel mediante a combinação dessas agulhas. A vantagem da matriz de pontos está na rapidez e no preço. Entretanto, como as letras e números são feitos com série de pontos, a qualidade da impressão deixa a desejar, além disso, essa impressora faz muito barulho.

Algumas impressoras de matriz de pontos resolvem o problema da má qualidade de impressão gravando os pontos duas ou três vezes. Nesse caso, preenchem os espaços deixados na primeira impressão.

### **Jato de Tinta**

As impressoras de jato de tinta são de preço um pouco mais elevado que as matriciais. Injetam gotas de tinta (ou bolhas de tintas aquecidas) que formam o caracter a ser impresso. As gotas passam por um eletrodo e recebem carga elétrica. Esse tipo de impressora trabalha com enorme rapidez, tendo capacidade para imprimir muitos caracteres por segundo. Sua qualidade de impressão é muito boa. São muito adequadas às cores.

### **Laser**

Sistema semelhante ao utilizado nas máquinas de xerox, por sensibilização do papel e uso de toner para impressão. Possui alta velocidade e alta resolução, tanto na escrita quanto em modo gráfico. Se forem coloridas usam toner de 3 ou 4 cores.

**Modem (Periférico de Entrada e Saída):** O modem é um dispositivo de conversão de sinais, que transmite dados através de linhas telefônicas. A palavra MODEM é derivada das palavras MODulação e DEModulação.

Modular significa converter pulsos digitais (dígitos) em sinais analógicos (ondas senoidais), para

que eles possam percorrer numa linha telefônica.

O modem permite que o computador "converse" com qualquer outro computador do mundo; mais isso só pode ocorrer se o outro também tiver um modem. Ele tanto pode ser adaptado a um microcomputador, como ao poderoso equipamento central de uma universidade ou instituição bancária

A ligação de seu micro a um grande equipamento pode lhe dar acesso a grandes bancos de dados, a serviço de informação e as últimas cotações da bolsa de valores. Se ligar o seu micro ao de seu amigo, vocês podem trocar software, enviar cartas eletrônicas (e-mails) , além de praticar jogos bidirecionais.

**Scanner – Digitalizador de imagem – (Periférico de Entrada):** Um digitalizador de imagens é um equipamento de entrada de dados, que permite a leitura de imagens a partir de material impresso (revistas, jornais, cartazes), armazenando na memória toda a tela recebida na leitura.

As telas podem, assim, serem modificadas e reproduzidas novamente por equipamentos adequados de impressão. Dessa forma podemos confeccionar cartazes ou qualquer outro tipo de trabalho utilizando fotografias.

**Multimídia -** Multimídia é uma união de informações, com áudio e vídeo, formando a partir daí um dos mais poderosos recursos digitais utilizados pelo computador.

Também chama-se multimídia aos softwares desenvolvidos especialmente para a utilização destes recursos e podem ser formados a partir de tipos de arquivos diferentes, como: vídeo-clips, músicas digitais, apresentações audiovisuais, animações gráficas, etc.

Para que um microcomputador possa utilizar todas as vantagens que a multimídia oferece, ele precisa de acessórios especiais. Por exemplo, o áudio só será reproduzido pelo computador se o mesmo possuir uma Placa de Som.

Placa de Som é um dispositivo ligado internamente ao computador responsável pela reprodução de sons digitais gerados pelos softwares.

Hoje em dia no mercado, encontramos uma grande variedade de Kits Multimídia, que são pacotes com equipamentos responsáveis pela execução da multimídia no computador. Na maioria deles encontraremos os seguintes itens: uma placa de som, um drive de leitura para CD-ROM, dois cabos para a conexão do drive de

CD-ROM à placa de som, duas caixas amplificadas, disquetes para a instalação dos componentes e manuais de instalação e uso. Como equipamentos opcionais encontraremos: um microfone, títulos em CD-ROM multimídia e talvez até uma câmera digital.

## **Equipamentos De Processamento**

### **Placa Mãe**

O elemento central de um microcomputador é uma placa onde se encontra o microprocessador e vários componentes que fazem a comunicação entre o microprocessador com meios periféricos externos e internos.

No nível físico mais básico, a placa mãe corresponde às fundações do computador. Nela ficam as placas de expansão; nela são feitas as conexões com circuitos externos; e ela é a base de apoio para os componentes eletrônicos fundamentais do computador. No nível elétrico, os circuitos gravados na placa mãe incluem o cérebro do computador e os elementos mais importantes para que esse cérebro possa comandar os seus "membros". Esses circuitos determinam todas as características da personalidade do computador: como ele funciona, como ele reage ao acionamento de cada tela, e o que ele faz.

### **Dois Importantes Componentes Da Placa Mãe São:**

**Microprocessador -** Responsável pelo pensamento do computador. O microprocessador

escolhido, entre as dezenas de microprocessadores disponíveis no mercado, determina a capacidade de processamento do computador e também os sistemas operacionais que ele compreende (e, portanto, os programas que ele é capaz de executar).

Co-processador - Complemento do microprocessador, o co-processador permite que o computador execute determinadas operações com muito mais rapidez. O co-processador pode fazer com que, em certos casos, o computador fique entre cinco e dez vezes mais rápido.

### **Monitores E Vídeos**

Embora os dois termos sejam usados como sinônimos (e às vezes até em conjunto: monitores de vídeo), na realidade há diferenças importantes entre eles. O vídeo é o dispositivo que produz a imagem, a tela que você vê. O monitor é o aparelho completo, a caixa onde o vídeo está alojado, juntamente com vários circuitos de apoio. Esses circuitos convertem os sinais enviados pelo computador (ou por outro equipamento, como um gravador de videocassete) num formato que o vídeo possa utilizar.

Embora a maioria dos monitores funcione segundo princípios semelhantes aos dos aparelhos de televisão (Tubos de Raios Catódicos ou CRT), os vídeos podem ser construídos com base em várias tecnologias, incluindo o cristal líquido (LCD) e o que usa o brilho de alguns gases nobres (painéis eletroluminescentes).

Os vídeos e monitores recorrem a diversas tecnologias para produzir imagens visíveis. A maioria dos computadores de mesa emprega sistemas de vídeo apoiados na mesma tecnologia de tubos de raios catódicos da maioria dos aparelhos de televisão. Os computadores portáteis utilizam principalmente vídeos de cristal líquido.

### **Principais Sistemas Operacionais**

Sistema operacional é um conjunto de programas que têm a função de gerenciar os recursos do sistema e fornecer a interface entre o computador e quem o está utilizando. Os principais e mais usados são: Windows, Mac OS X e Linux.

#### **Principais Sistemas Operacionais**

**WINDOWS:** É o sistema operacional mais usado no mundo todo, atinge cerca de 400 milhões de usuários e foi criado pela Microsoft, empresa de Bill Gates. Seu preço varia para cada uma de suas versões, e a mais atual é o Windows 7 que foi lançado em 2009.

**MAC OS X:** Esse sistema operacional foi criado e é comercializado pela Apple, sua primeira versão foi lançada em 2001 com um preço em torno de \$120,00, e hoje conta com várias versões, que são: Mac OS X 10.1 Puma, Mac OS X 10.2 Jaguar, Mac OS X 10.3 Panther, Mac OS X 10.4 Tiger, Mac OS X 10.5 Leopard, Mac OS X 10.6 Snow Leopard, e por último a Mac OS X 10.7 Lion, que já conta com mais de 22 milhões de usuários.

**LINUX:** Sistema operacional desenvolvido por Linus Torvaldo, finlandês que se inspirou no sistema Minix, esse sistema conta com a colaboração de grandes empresas como Microsoft e Google; foi criado em 1991 e já possui mais de 8 milhões de usuários.

Portanto, todos esses sistemas operacionais são muito usados, mas o Windows ainda se destaca devido à sua praticidade e ao preço.

### **Conheça Todos Os Formatos De Mídia Óptica**

Com a chegada dos equipamentos com capacidade para reproduzir vídeo em alta definição, foi necessário que um novo tipo de mídia óptica fosse inventado, pois quanto maior a definição de um vídeo, mais espaço ele consumirá, demandando discos com maior capacidade. Surgiram assim, as mídias ópticas de grande capacidade e, com elas, uma confusão de nomenclaturas para a qual os usuários não estavam preparados. Para resolver de uma vez por todas as suas dúvidas sobre os tipos diferentes de mídia existentes no mercado, reunimos em um só lugar a definição de todos para você consultar sempre que tiver dúvida.

### **O Bom E Velho CD**



A sigla “CD” foi adotada devido ao fato de, na época do seu lançamento, existirem os discos de vinil, que eram grandes e desengonçados. O nome “Compact Disc” foi criado como uma comparação ao vinil, pois logicamente o CD é extremamente compacto em relação ao seu antecessor. Sem muita demora, surgiram os primeiros CD-R (CD Recordable), que não suportavam mais de uma gravação. Ou seja, assim que você esgotasse a capacidade de armazenamento, seu CD gravável não poderia ser apagado ou receber mais dados.

**CD-R (CD Recordable):** CD gravável. Hoje com capacidade para 700 MB ou 80 minutos de áudio sem compactação. Não permite que nenhum dado seja apagado do CD. Após adicionados, os dados que lá estão são permanentes. Se não for utilizada toda a capacidade na primeira gravação, pode-se gravar outras sessões, até que o CD esteja completamente cheio.

**CD-RW (CD Rewritable):** CD regravável. Também tem a capacidade de 700 MB. Essa mídia permite que você grave, apague os dados e grave novamente. Sua vida útil é de aproximadamente mil ciclos (1 ciclo = gravar uma vez + apagar uma vez).

**Mini-cd:** apesar de pouco popular, é uma boa opção para quem não gosta de carregar os CDs de tamanho normal. Além do tamanho reduzido (8cm de diâmetro, contra os 12cm do CD normal), sua capacidade também é bem menor: 180 MB, ou 23:30 minutos. Os tocadores e gravadores de CD que possuem a “gaveta” são perfeitamente capazes de reproduzir e gravar mini-cds.

### **As Novas Mídias**

A tecnologia foi se desenvolvendo e trazendo novos tipos de mídia. O DVD, que de início era sigla para Digital Video Disc, mas que é chamado por alguns de Digital Versatile Disc, foi lançado a princípio para armazenamento de vídeo, mas assim como o CD, ele foi logo adaptado para ser utilizado para armazenar qualquer tipo de dado. Assim como os CDs, existem os DVDs graváveis e os regraváveis. Porém, os DVDs têm uma particularidade que não existia no CD: existem padrões e capacidades diferentes.

**DVD-R:** com capacidade de 4.7 GB, é o formato mais usado no Brasil. Muitas vezes as pessoas podem se referir a esse tipo de mídia como DVD5, devido ao fato de a sua capacidade estar próxima dos 5 GB. Também existem DVD-Rs com capacidade de 8.5 GB (também chamados de DVD9). Isso é possível porque são usadas duas camadas diferentes no mesmo lado do disco, praticamente dobrando a capacidade de armazenamento.

Também existem os DVDs com capacidade de gravação nos dois lados do disco, mas esse tipo é difícil de ser encontrado, pois não se popularizou no Brasil. Sua capacidade é de até aproximadamente 15 GB.

**DVD-RW:** esse tipo de DVD tem a mesma capacidade do DVD-R, com a possibilidade de apagar os dados e reutilizar o disco, assim como o CD-RW.

**DVD+R e DVD+RW:** esses dois tipos são praticamente idênticos ao DVD-R e o DVD-RW, respectivamente. A diferença básica entre eles é o desempenho na hora de queimá-los, devido ao modo com que os dois tipos realizam a gravação. As mídias com o sinal de menos (-) são gravadas do centro para fora, em uma única linha, formando uma espiral. Já os discos com um sinal de adição (+) são gravados em vários círculos concêntricos. Isso dá uma maior rapidez aos DVD+R e DVD+RW tanto na leitura quanto na gravação. Porém, essa diferença é quase imperceptível.

As mídias com sinal “+” costumam ser um pouco mais caras, mas a diferença é irrisória. Quanto à compatibilidade, no início não era possível executar e gravar discos se o sinal fosse diferente ao suportado pela gravadora. Hoje, a maioria das leitoras e gravadoras já suporta os dois tipos, então você não precisa se preocupar se na loja só tem um dos dois.

### **Saíram Do Forno Agora**

**Blu-ray:** com o surgimento dos equipamentos com capacidade para execução de vídeos e filmes em alta definição, era necessário desenvolver uma mídia de grande capacidade, para possibilitar assim, o armazenamento de imagens em alta definição, que ocupam muito mais espaço. Com a Sony à frente do projeto, foi criado então o Blu-ray, que possui esse nome justamente porque a cor do laser

que faz sua leitura e gravação é azul. A capacidade do Blu-ray é de incríveis 25 GB nas mídias com uma só camada. Nos discos com duas camadas, o tamanho dobra, chegando aos 50 GB.

HD-DVD: similar ao Blu-ray, porém com capacidade menor, o HD-DVD recentemente perdeu a batalha pela hegemonia das mídias de grande capacidade. A empresa Toshiba comandava o desenvolvimento dessa mídia, juntamente com outras gigantes como Microsoft. Porém, há pouco tempo a Toshiba anunciou o abandono do projeto, dando ao Blu-ray e à Sony o título de única mídia de alta capacidade disponível no mercado.

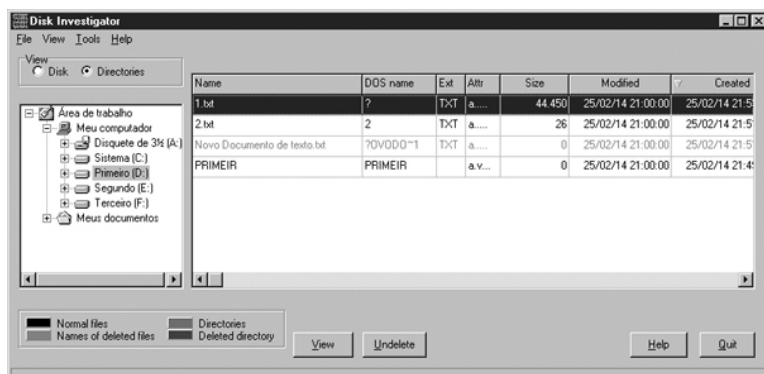
Esses são os tipos de mídia amplamente disponíveis hoje no mercado (exceto pelo HD-DVD). Muitos outros formatos já passaram pelas nossas casas, como o cassete e o MD, mas nem todos foram tão populares quanto os discos ópticos são hoje.

### Ferramentas De Recuperação

Foram analisadas algumas ferramentas de recuperação de arquivos removidos, encontrados pela internet, para verificar os tipos de dados que elas recuperam e qual a sua forma de interface com o usuário. Em algumas delas, não foi possível uma análise mais aprofundada por ser uma versão demo da ferramenta, limitando-se apenas na execução das operações mais simples.

### Ferramenta Disk Investigator

O Disk Investigator é um utilitário que encontra os arquivos ocultos em um disco rígido e ajuda a recuperar dados perdidos. Lista as unidades realmente existentes e diretórios, arquivos, agrupamentos de unidades e setores do sistema. Recupera arquivos previamente apagados. [Absolute, 2004]



### Tela Principal Da Ferramenta Disk Investigator

A versão da ferramenta analisada é v1.31, de Kevin Solway, e apresenta as seguintes características:

Lista os arquivos e diretórios em uma janela semelhante ao do Windows Explorer, sinalizando-os como ativos ou apagados;

Lista as informações do setor de boot, da tabela de alocação de arquivos e do diretório raiz da partição selecionada;

Executa recuperação de arquivos individualmente, onde o procedimento “recupera todos” será adicionado na versão futura;

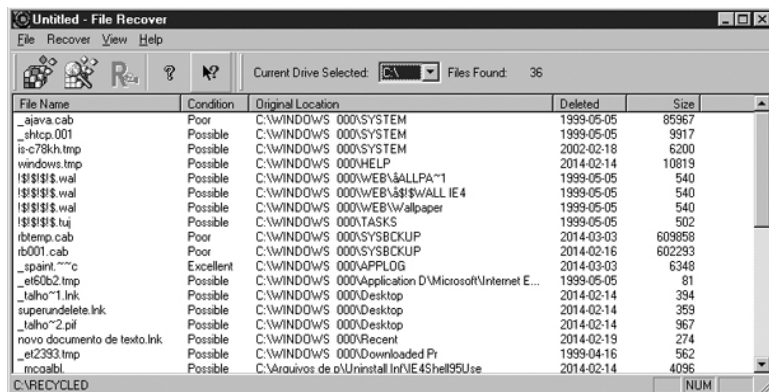
Não consegue recuperar nem listar os arquivos e diretórios de uma partição após uma formatação rápida.

### Ferramenta File Recover

A ferramenta File Recover é um tipo de programa utilitário para recuperação de arquivos removidos. Ele simplesmente identifica se os arquivos estão intactos no disco rígido e lista as opções de recuperação. É de fácil utilização e designado para recuperar arquivos apagados acidentalmente. Suporta disco rígido com sistemas de arquivos de tabela de alocação de arquivos e



NTFS.[Filerecover, 2004]



File Name	Condition	Original Location	Deleted	Size
_ajava.cab	Poor	C:\WINDOWS\000\SYSTEM	1999-05-05	85967
_shcp.001	Possible	C:\WINDOWS\000\SYSTEM	1999-05-05	9917
is-c78h.tmp	Possible	C:\WINDOWS\000\SYSTEM	2002-02-18	6200
windows.tmp	Possible	C:\WINDOWS\000\HELP	2014-02-14	10819
!\$!\$!\$!\$.wial	Possible	C:\WINDOWS\000\WEB\ALLPA~1	1999-05-05	540
!\$!\$!\$!\$.wial	Possible	C:\WINDOWS\000\WEB\ALLPA~1	1999-05-05	540
!\$!\$!\$!\$.wial	Possible	C:\WINDOWS\000\WEB\Wallpaper	1999-05-05	540
!\$!\$!\$!\$.wial	Possible	C:\WINDOWS\000\TASKS	1999-05-05	502
ibtemp.cab	Poor	C:\WINDOWS\000\SYSTEM\BCKUP	2014-03-03	609058
rb001.cab	Poor	C:\WINDOWS\000\SYSTEM\BCKUP	2014-02-16	602293
_tpoint.tmp	Excellent	C:\WINDOWS\000\APPLLOG	2014-03-03	6348
_et60b2.tmp	Possible	C:\WINDOWS\000\Application D\Microsoft\Internet E...	1999-05-05	81
_talho~1.lnk	Possible	C:\WINDOWS\000\Desktop	2014-02-14	394
superdelete.lnk	Possible	C:\WINDOWS\000\Desktop	2014-02-14	359
_talho~2.tif	Possible	C:\WINDOWS\000\Desktop	2014-02-14	967
novo documento de texto.lnk	Possible	C:\WINDOWS\000\Recent	2014-02-19	274
_et2393.tmp	Possible	C:\WINDOWS\000\Downloaded Pr	1999-04-16	562
mcoabtl	Possible	C:\Arquivos de o\Uninstall In\IE45hell95Use	2014-02-14	4096

### Tela Principal Da Ferramenta File Recover

A versão da ferramenta analisada é v2.78\_0\_0d e apresenta as seguintes características:

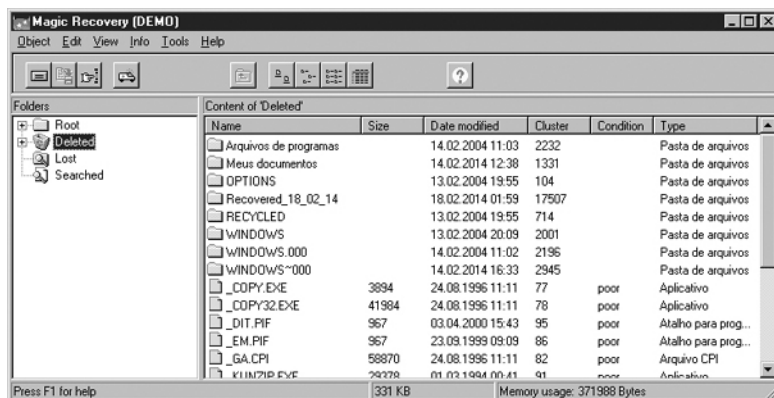
Faz uma varredura para identificar os arquivos apagados na partição selecionada;

Não consegue recuperar nem listar os arquivos e diretórios de uma partição após uma formatação rápida;

Não foi possível executar uma recuperação e uma análise mais detalhada por ser uma versão demo.

### Ferramenta Magic Recovery

A ferramenta Magic Recovery recupera arquivos e diretórios removidos de forma rápida e fácil. Não recupera arquivos afetados por vírus ou por problemas físicos do disco rígido. Funciona em Windows 3.11 / 95 / 98 / Me / NT / 2000. [Ondata, 2004]



Name	Size	Date modified	Cluster	Condition	Type
Arquivos de programas		14.02.2004 11:03	2232		Pasta de arquivos
Meus documentos		14.02.2014 12:38	1331		Pasta de arquivos
OPTIONS		13.02.2004 19:55	104		Pasta de arquivos
Recovered_18_02_14		18.02.2014 01:59	17507		Pasta de arquivos
RECYCLED		13.02.2004 19:55	714		Pasta de arquivos
WINDOWS		13.02.2004 20:09	2001		Pasta de arquivos
WINDOWS.000		14.02.2004 11:02	2196		Pasta de arquivos
WINDOWS~000		14.02.2014 16:33	2945		Pasta de arquivos
_COPY.EXE	3894	24.08.1996 11:11	77	poor	Aplicativo
_COPY32.EXE	41984	24.08.1996 11:11	78	poor	Aplicativo
_DIT.PIF	967	03.04.2000 15:43	95	poor	Atalho para prog...
_EM.PIF	967	23.09.1999 09:09	86	poor	Atalho para prog...
_GA.CPI	58870	24.08.1996 11:11	82	poor	Arquivo CPI
_KUM72P.EVE	29270	01.02.1994 00:41	91	poor	Arquivo

### Tela Principal Da Ferramenta Magic Recovery

A versão da ferramenta analisada é v1.0 e apresenta as seguintes características:

Lista na abertura do programa as opções de “Recuperar arquivos”, “Procurar dados perdidos” e “Procurar partição perdida”;

Lista informações do sistema como quantidade de processadores na máquina avaliada, quantidade de memória, capacidade de resolução do monitor, tamanho de swap, versão do Windows, unidades existentes e as informações da unidade;

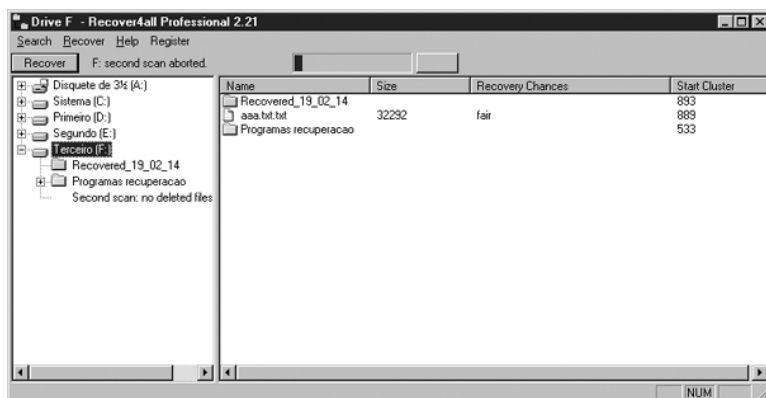
Não consegue recuperar nem listar os arquivos e diretórios de uma partição após uma formatação rápida;

Não foi possível executar uma recuperação e uma análise mais detalhada por ser uma versão

demo.

### Ferramenta Recover4all Professional

A ferramenta Recover4all Professional é um programa que permite recuperar facilmente arquivos apagados acidentalmente do Windows. Para evitar que o arquivo apagado seja sobrescrito, essa ferramenta não requer a instalação podendo funcionar diretamente de um disco flexível. O Recover4all funciona em Windows 95 / 98 / Me / NT / 2000 / XP, ou seja, em sistema de arquivo de tabela de partição de arquivos e NTFS. Suporta drives reconhecidos pelo Windows com IDE, SCSI, USB, PCMCIA e outras interfaces. [Recover4all, 2004]



### Tela Principal Da Ferramenta Recover4all

A versão da ferramenta analisada é v2.21 e apresenta as seguintes características:

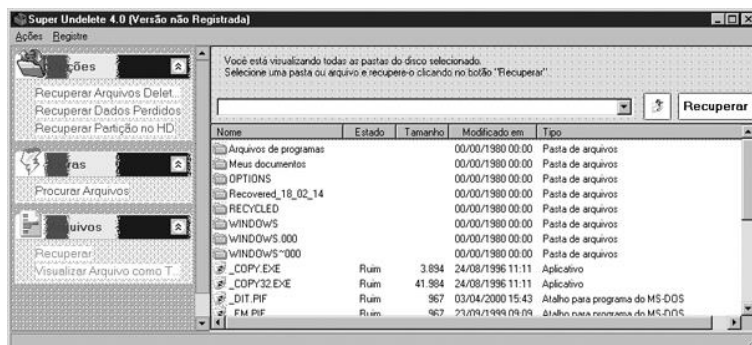
Lista os arquivos apagados da partição selecionada;

Não consegue recuperar nem listar os arquivos e diretórios de uma partição após uma formatação rápida;

Não foi possível executar uma recuperação e uma análise mais detalhada por ser uma versão demo.

### Ferramenta Super Undelete

A ferramenta Super Undelete é um programa de recuperação de arquivos apagados do Windows. Não é possível a recuperação de dados causados por problemas físicos no disco rígido. Em todas as outras situações a recuperação é possível, dependendo apenas da situação e condição específica da integridade de cada arquivo. É possível recuperar arquivos que não estão mais na lixeira, arquivos apagados por ação de vírus, arquivos apagados por problema na tabela de partição de arquivos e por perda de partições e discos lógicos. Funciona em sistemas de arquivos de tabela de partição de arquivos. [Siliconaction, 2004]



### Tela Principal Da Ferramenta Super Undelete

A versão da ferramenta analisada é v4.0 e apresenta as seguintes características:



procedimento.

Montagem da tabela de partição. Com as informações obtidas na varredura, é possível remontar a tabela de partição e obter informações completas dos dados existentes no disco. Se a varredura terminar com o final de disco, conclui-se que só existe uma partição e o endereço armazenado é o setor de boot com o bloco de parâmetros da única partição ativa no disco. Mas, se a varredura terminar ao encontrar o primeiro setor da segunda partição, o vetor conterá o endereço do setor de boot da primeira partição e o endereço contendo uma tabela de partições. A partir desse endereço, contendo a tabela de partições, pode-se calcular os endereços do restante das partições no disco. Com essas informações, tendo o disco uma ou mais partições, é possível montar uma tabela de partições na memória, para uso da ferramenta na recuperação dos arquivos.

Identificação das áreas de controle de cada partição. Com uma tabela de partições montada na memória, é possível vasculhar qualquer informação contida no disco. Para garantir a integridade das informações de controle do disco, a ferramenta poderia listar todas as informações contidas no bloco de parâmetros do setor de boot de cada partição, assim como a tabela de alocação de arquivos e suas cópias. Essa listagem permitiria ao usuário identificar algum problema em outros setores na área de controle, ou se a tabela de partições foi montada corretamente.

Listagem dos arquivos e diretórios. Certificando-se de que a tabela de partições contenha informações coerentes, deve-se listar ao usuário o diretório raiz, mostrando os arquivos e diretórios contidos nas partições, assim como os subdiretórios, para que seja selecionado o conteúdo a ser recuperado.

### A Transferência Dos Dados A Serem Recuperados Para Outra Mídia Será Tratada Na Seção 4.3

#### Danos No Setor De Boot Da Partição

Caso ocorram danos no setor de boot da partição utilizada para inicialização, com a utilização de um disco de inicialização (disquete de boot), geralmente é possível o acesso aos arquivos nessa partição. Transferindo esses arquivos para outra unidade de disco, pode-se formatar a partição para corrigir o setor de boot, sem que seja perdido nenhum arquivo. Se o disco de inicialização não permitir a leitura dessa partição, na tentativa de seu acesso ocorrerá um erro, onde o sistema solicitará a sua formatação. Para recuperar arquivos nessa situação, deve-se executar os seguintes procedimentos:

Obter informações dessa partição. Através do Master Boot Record, a ferramenta pode obter as informações referentes ao início e o fim da partição em questão.

Localizar os setores da área de controle do sistema. A partir do primeiro setor dessa partição, é necessário fazer uma varredura para identificar as seguintes informações:

Setores com os primeiros bytes com os valores "F8 FF FF 0F FF FF FF 07" para sistema TAA 32, "F8 FF FF 7F" para sistema TAA 16, ou "F8 FF FF" para sistema TAA 12. Essa é a configuração do início de uma tabela de alocação de arquivos, onde as duas primeiras entradas são reservadas, conforme as ilustrações a seguir;

0000	F0 FF FF 03-40 00 05 60-00 07 80 00-09 A0 00 0B	- V@ 1' +C oá d
0010	C0 00 0D E0-00 0F 00 01-11 20 01 13-40 01 15 60	L Jo * @- @!!@S'
0020	01 17 80 01-19 A0 01 1B-C0 01 1D E0-01 1F 00 02	0!C0!á@+L@+60V 0
0030	21 20 02 23-40 02 25 60-02 27 80 02-29 A0 02 2B	! @H@%*'@'C@)á@+
0040	60 02 2D 50-02 2F 00 03-31 20 03 33-40 03 35 60	L@-á@/ #1 #30#5'

#### Hexadecimal início TAA 12

0000	F8 FF FF 7F-FF FF FF FF-FF FF 06 00-07 00 08 00	° □ ▲ • ■
0010	09 00 0A 00-0B 00 0C 00-13 00 10 00-FF FF FF FF	○ ◻ ◊ ♀ !! ▶
0020	11 00 61 00-FF FF 65 00-FF FF 3B 00-17 00 18 00	◀ a e ; ! ↑
0030	19 00 1A 00-1B 00 1C 00-1D 00 1E 00-1F 00 20 00	↓ → ← L → ▲ ▼
0040	21 00 22 00-23 00 24 00-25 00 26 00-27 00 28 00	! " # \$ % & ' (

#### Hexadecimal início TAA 16

0000	F8 FF FF 0F-FF FF FF 07-FF FF FF 0F-04 00 00 00	° * • ✦
0010	05 00 00 00-06 00 00 00-07 00 00 00-08 00 00 00	✦ ◻ ◊ ♀
0020	09 00 00 00-0A 00 00 00-0B 00 00 00-0C 00 00 00	◻ ◻ ◻ ◻
0030	0D 00 00 00-0E 00 00 00-0F 00 00 00-10 00 00 00	♪ ♪ ♪ ♪
0040	11 00 00 00-12 00 00 00-13 00 00 00-14 00 00 00	◀ 1    1

### **Hexadecimal início TAA 32**

Em seguida, deve-se localizar o próximo setor contendo essa mesma configuração, para localizar a cópia da tabela de alocação de arquivos. A quantidade de setores entre essas duas tabelas representa o seu tamanho;

Após a quantidade de setores referente às duas tabelas, podem existir mais cópias da tabela de alocação de arquivos. Caso não tiver, a próxima estrutura após as tabelas é o diretório raiz;

Para identificar o tamanho do diretório raiz e o início da área de dados, deve-se executar uma varredura verificando se os setores contém, a cada 32 bytes, a configuração das entradas de diretório. Por exemplo, pode-se verificar se os campos de atributo do arquivo e data de criação contém valores válidos. Caso contrário, o setor representa o início da área de dados.

Listar as informações das áreas de controle. Para garantir a integridade das informações de controle do disco, a ferramenta poderia listar todas as informações encontradas até o momento. Essa listagem permitiria ao usuário identificar se foram encontradas informações coerentes, como por exemplo, se as cópias da tabela de alocação de arquivos são iguais e se o diretório raiz contém informações contendo os nomes dos arquivos.

Listagem dos arquivos e diretórios. Certificando-se de que as informações encontradas são coerentes, deve-se listar ao usuário o diretório raiz, mostrando os arquivos e diretórios contidos nas partições, assim como os subdiretórios, para que seja selecionado o conteúdo a ser recuperado.

A transferência dos dados a serem recuperados para outra mídia será tratada na seção 4.3

### **Danos Na Tabela De Alocação De Arquivos - TAA**

Quando ocorrem problemas na tabela de alocação de arquivos, o próprio sistema tenta se recuperar através das cópias da tabela existente no disco. Caso as cópias também estiverem danificadas, são recuperadas somente as informações que o sistema considerar consistente, ou seja, que estiverem fora da área danificada. Nesse caso, os arquivos que tiverem as informações de seus blocos na área danificada da tabela serão removidos, não sendo possível a sua recuperação.

Geralmente, quando ocorrem danos na tabela de alocação de arquivos, o próprio sistema consegue se recuperar. Quando o sistema não consegue se recuperar, possivelmente houve perda integral da tabela e de suas cópias. Considerando essa situação, não foi possível propor uma metodologia de recuperação de arquivos, pois em todas propostas aqui tratadas, são essenciais as informações da tabela de alocação de arquivos

### **Danos No Diretório Raiz**

Se danos ocorrerem no diretório raiz, provavelmente o sistema não reconhecerá a partição e pedirá uma formatação. Pode acontecer do sistema reconhecer a partição, mas não conseguirá mostrar nenhum conteúdo e não conseguirá manusear corretamente gravações e leituras no diretório raiz. Com a perda das informações do diretório raiz, é possível recuperar somente os arquivos contidos nos sub-diretórios, pois suas entradas de diretório estão localizados na área de dados do disco. Para isso, é preciso executar os seguintes procedimentos:

Identificar o início da área de dados. Para se efetuar a recuperação dos sub- diretórios, é necessário identificar, primeiramente, o início da área de dados. Todas as informações para esse cálculo podem ser encontradas no setor de boot. Somando o tamanho do diretório raiz com o tamanho das tabelas de alocação de arquivos mais os setores reservados, obtém-se o tamanho da área de sistema. Posterior a essa área encontra-se a área de dados.

Localizar as entradas dos sub-diretórios. Após encontrar o início da área de dados, deve-se executar uma varredura procurando todos os setores que contiverem a seguinte configuração:

Primeiro byte com o valor em hexadecimal igual a "2E", e o segundo até o oitavo byte com os valores iguais a "20";

Trigésimo terceiro e o trigésimo quarto byte com o valor igual a "2E", e o trigésimo quinto até o



quadrigésimo byte com o valores iguais a “20”.

Essa é a configuração dos setores contendo as entradas dos sub-diretórios, com as duas primeiras entradas reservadas ponto e ponto-ponto, ilustrado na Figura 4.6. Após encontrar esses setores, deve-se calcular sua localização na tabela de alocação de arquivos, para poder encontrar os blocos que contém sua continuação.

0000	2E	20	20	20-20	20	20	20-20	20	20	10-00	62	B4	A0	.	fDfD	ÁáfD	► b á
0010	66	44	66	44-00	00	B5	AO-66	44	0C	00-00	00	00	00	.	fDfD	ÁáfD	► b á
0020	2E	2E	20	20-20	20	20	20-20	20	20	10-00	62	B4	A0	.	fDfD	ÁáfD	► b á
0030	66	44	66	44-00	00	B5	AO-66	44	00	00-00	00	00	00	.	fDfD	ÁáfD	► b á
0040	42	78	00	74-00	00	00	FF-FF	FF	FF	0F-00	6B	FF	FF	Bx	t	*	k
0050	FF	FF	FF	FF-FF	FF	FF	FF-FF	FF	00	00-FF	FF	FF	FF	Ⓡ	E	A	D
0060	01	52	00	45-00	41	00	44-00	4D	00	0F-00	6B	45	00	Ⓡ	R	A	D
0070	46	00	49	00-52	00	53	00-54	00	00	00-2E	00	74	00	F	I	R	S
															T	.	t

Entrada reservada ponto e ponto-ponto dos sub-diretórios

Listagem dos arquivos e diretórios. Encontrados os setores do passo anterior, é possível a listagem e a obtenção de informações de todos os arquivos e diretórios dos sub-diretórios.

A transferência dos dados a serem recuperados para outra mídia será tratada na seção 4.3.

### Perda De Arquivos Por Remoção Ou Formatação

Em uma remoção, o sistema operacional marca no diretório raiz como arquivo apagado e libera suas entradas na tabela de alocação de arquivos. Sem as informações referentes ao arquivo na tabela de alocação de arquivos, não é possível executar sua recuperação. Uma tentativa, que possivelmente poderia recuperar um arquivo removido, seria da seguinte maneira:

Verificar no diretório raiz, na entrada do arquivo a ser recuperado, qual o primeiro agrupamento de unidades para localizá-lo na tabela de alocação de arquivos;

A partir desse agrupamento, verificar se existe uma sequência de agrupamentos de unidades consecutivas do tamanho do arquivo apagado;

Se não existir, marcar o arquivo como não recuperável. Caso contrário, permitiria sua recuperação. Na tentativa de recuperação, é preciso ativar o arquivo no diretório raiz, mudando o primeiro byte por um caractere válido, e realizar as devidas ligações, consecutivas, nas entradas da tabela de alocação de arquivos a partir do primeiro agrupamento.

Nessa tentativa, existe uma possibilidade do arquivo ser recuperado. Caso o arquivo não ocupe agrupamentos de unidades seqüenciais, ou alguns deles já não tiverem os dados corretos, o arquivo será recuperado e não permitirá sua execução. Se isso acontecer, será emitida uma mensagem de erro de “Arquivo corrompido” ou “Arquivo inválido”. Nessa situação, basta apagá-lo novamente.

Já na formatação, tanto a rápida como a completa, são “zerados” todos os campos do diretório raiz e da tabela de alocação de arquivos. Sem essas duas estruturas de controle, não é possível executar a recuperação de qualquer informação. Talvez exista uma maneira de recuperar esses arquivos, mas até o momento, não foi possível encontrar uma solução para esse problema.

### Transferência Dos Dados Recuperados

Após a listagem e a seleção dos arquivos a serem recuperados, é necessário a sua transferência para outra mídia. Geralmente, não é feita a recuperação de arquivos na mesma mídia para evitar que outros dados removidos sejam sobrescritos. Para a transferência, é necessário executar os seguintes procedimentos:

Verificação de espaço para transferência. Após a seleção, pelo usuário, dos arquivos a serem recuperados e a mídia destino, deve-se verificar se a mídia destino possui espaço suficiente para a gravação. Essa verificação pode ser realizada da seguinte maneira:

Calcular, através das informações de tamanho do arquivo, contido no diretório raiz dos arquivos selecionados, o tamanho total exigido para transferência. Basta, para cada arquivo, verificar sua



entrada de diretório o valor do Byte no offset 1CH, ilustrado na Figura 4.7.

```
0040  44 45 20 20-20 20 20 20-45 58 45 20-00 B2 D2 01  DE  EXE  0000
0050  21 24 44 30-00 00 53 AA-34 30 02 00-C0 4D 03 00  !$D0  S-400  LM?
```

Informação de tamanho do arquivo na entrada de diretório

Verificar, através de operações de alto nível, se a unidade destino possui espaço suficiente para a gravação requerida.

Transferência de dados. Caso haja espaço suficiente na mídia destino, deve-se iniciar a transferência dos arquivos da seguinte maneira:

Localizar o bloco de dados inicial, do arquivo a ser transferido, através do diretório raiz;

Calcular e encontrar, através da tabela de alocação de arquivos, os blocos subsequentes desse arquivo. Caso o arquivo tenha mais de um bloco, devem ser todos armazenados na memória, para a montagem do arquivo;

Gravar na outra unidade, através de operações de escrita de arquivos, da linguagem de programação. Utilizando-se essas operações de alto nível, não é necessário a identificação da estrutura do sistema de arquivos na unidade destino, pois o próprio sistema operacional se encarrega de seu gerenciamento.

### Linguagem De Programação C

A linguagem de programação C foi desenvolvida no início dos anos 70 nos Laboratórios AT&T Bell, nos Estados Unidos. Um dos grandes atrativos dessa linguagem é o balanço atingido entre características próximas da arquitetura de computadores e características de linguagens de programação de alto nível de abstração. A simplicidade da linguagem não restringe, no entanto, a potencialidade de suas aplicações. Blocos de tarefas complexas podem ser criados a partir de blocos elementares, podendo se estender por diversos níveis. Esta habilidade de construir aplicações complexas a partir de elementos simples é uma das principais características da linguagem. [DCA, 2004]

As linguagens de baixo nível são as linguagens que mais se aproximam do código de máquina, ou seja, dos 0 ou 1. Os programas resultantes destas linguagens são pequenos em tamanho e extremamente rápidos. As linguagens de alto nível são orientadas para o problema, necessitando pouca ou nenhuma atenção às características do computador que irá executar o programa, onde facilita a interação da linguagem com o programador. A linguagem C possui boa parte dessas duas características, de alto e de baixo nível. A combinação dos apontadores e operadores a nível de bit, faz do C uma linguagem capaz de substituir o Assembly, com as propriedades e abstrações de uma linguagem de alto nível.

facilidade de utilização de recursos de baixo nível, com operadores similares ao Assembly, é o fator mais importante da linguagem C para a implementação da metodologia proposta. Nela é possível executar operações de baixo nível como as interrupções de hardware, e alocando seus valores em endereços de memória, pode-se tratar facilmente essas informações através de operadores de alto nível. Veja as funções de interrupções da Linguagem Assembly no Apêndice A, que podem ser utilizados similarmente na Linguagem C.

---

---

---

---

---

---

---

---