UNIVERSIDADE SAGRADO CORAÇÃO
Centro de Ciências Exatas e Sociais Aplicadas
Bacharelado em Ciência da Computação

DOUGLAS DE OLIVEIRA

FORENSE COMPUTACIONAL APLICADA EM RECUPERAÇÃO DE ARQUIVOS EM AMBIENTE WINDOWS, LINUX E MAC OS X

BAURU
2012

DOUGLAS DE OLIVEIRA

FORENSE COMPUTACIONAL APLICADA EM RECUPERAÇÃO DE ARQUIVOS EM AMBIENTE WINDOWS, LINUX E MAC OS X

Monografia apresentada como Trabalho de Conclusão de Curso na Universidade Sagrado Coração, sendo requisito parcial para obtenção do título de bacharel em Ciência da Computação, orientado pelo Prof. Esp. Henrique Pachioni Martins.

BAURU
2012

Oliveira, Douglas de

O482f

Forense computacional aplicada em recuperação de arquivos em ambiente Windows, Linux e Mac OS X / Douglas de Oliveira -- 2012.

50f. : il.

Orientador: Prof. Esp. Henrique Pachioni Martins.

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

1. Arquivos apagados. 2. Forense computacional. 3. Recuperação de dados. I. Martins, Henrique Pachioni. II. Título.

DOUGLAS DE OLIVEIRA

FORENSE COMPUTACIONAL APLICADA EM RECUPERAÇÃO DE ARQUIVOS EM AMBIENTE WINDOWS, LINUX E MAC OS X

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade Sagrado Coração como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Esp. Henrique Pachioni Martins.

Banca examinadora:

_____
Prof. Esp. Henrique Pachioni Martins
Universidade Sagrado Coração

_____
Prof. Dr. Kelton Augusto Pontara da Costa
Universidade Sagrado Coração

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

Bauru, 5 de dezembro de 2012.

AGRADECIMENTOS

Agradeço a Deus acima de tudo, por ter me concedido saúde, força de vontade e perseverança das quais me permitiram estar concluindo uma faculdade.

Aos meus pais e meu irmão pelo amor, carinho e compreensão que me ajudaram a superar mais esta etapa na minha vida.

Ao meu amigo e orientador Henrique Pachioni Martins, me deu conselhos e motivou-me a seguir em frente e também me ajudou a superar as pedras que surgiram no caminho levando à conclusão deste trabalho.

Aos meus amigos que sempre me deram incentivo e me apoiaram em todos os momentos no decorrer deste trabalho, dando ânimo para continuar e faziam sempre com que as horas dedicadas ao trabalho não parecessem tão longas e cansativas assim.

A todos os professores que auxiliaram em minha formação profissional, meus mais sinceros agradecimentos.

RESUMO

A recuperação de dados, comuns ou sigilosos, se faz necessária devido ao crescimento constante do uso de equipamentos de armazenamento de dados. Este procedimento é adotado tanto por usuários comuns, que têm os seus arquivos perdidos por acidente, como por investigadores forenses em busca de evidências de crimes, sejam eles digitais ou não. Este trabalho analisa ferramentas de dados forenses com o objetivo de identificar qual ferramenta e em qual sistema operacional é possível se obter a melhor recuperação de arquivos. Foram selecionadas duas ferramentas para cada sistema operacional, sendo: Recuva e DiskDigger para o Windows; Mac Data Recovery Free e Disk Drill para Mac OS X; Foremost e Scalpel para Linux. Todas essas ferramentas estão disponíveis gratuitamente, porém, algumas delas possuem versão proprietária. Os testes das ferramentas pré-selecionadas foram realizadas com o intuito de recuperar arquivos formatados de um pendrive, cada qual em seu sistema operacional. Após essa bateria de testes, foi possível verificar qual ferramenta é mais eficaz para a recuperação de arquivos deletados.

Palavras-Chave: Arquivos apagados. Forense Computacional. Recuperação de dados.

ABSTRACT

The data recovery, common or sensitive, it is necessary due to the steady growth of the use of data storage equipment. This procedure is adopted by both common users, who have lost their files by accident as by forensic investigators to search for evidence of crimes, be they digital or not. This paper analyzes data forensic tools in order to establish which tool and which operating system you can get the best file recovery. Were selected two tools for each operating system, as follows: DiskDigger and Recuva for Windows, Mac Data Recovery Free and Disk Drill for Mac OS X; Foremost and Scalpel for Linux. All these tools are available for free, but some of them have proprietary version. Testing tools preselected were performed in order to recover files from a formatted flash drive, each in its operating system. After this battery of tests, have been checking which tool is most effective for recovering deleted files.

Keywords: Files deleted. Computational Forensics. Data recovery.

LISTA DE FIGURAS

Figura 1 - Principais informações a serem inseridas no preâmbulo do laudo.....23
Figura 2 - Exemplo de texto contido na seção Histórico.....24
Figura 3 - Exemplo de descrição de um disco rígido em formato tabular. 24
Figura 4 - Exemplo de objetivo de um laudo.....24
Figura 5 - Exemplo de finalização de laudo, incluindo devolução de material lacrado e assinaturas...25
Figura 6 - Assistente do Recuva.....30
Figura 7 - Escolhendo tipo de arquivo a ser recuperado no Assistente do Recuva.....31
Figura 8 - Localizando o local de origem dos arquivos apagados no Recuva.....31
Figura 9 - Iniciando o processo de recuperação de arquivos do “Assiste do Recuva” 32
Figura 10 - Arquivos encontrados pelo "Assistente do Recuva" 33
Figura 11 - Selecionando o local onde os arquivos serão restaurados 33
Figura 12 - Pasta contendo os arquivos recuperados pelo Recuva 34
Figura 13 - Modo de recuperação de arquivos avançado, sem o "Assistente do Recuva" 34
Figura 14 - Tela inicial da ferramenta DiskDigger para escolher a unidade de origem dos arquivos apagados 35
Figura 15 - Tela para escolher as configurações da busca por arquivos no DiskDigger.....36
Figura 16 - Tela para escolher os tipos de arquivos que o DiskDigger deve buscar 36
Figura 17 - Tela mostrando o total de arquivos recuperados pelo DiskDigger 37
Figura 18 - Salvando os arquivos recuperados pelo DiskDigger 37
Figura 19 - Solicitação de licença de uso do DiskDigger 38
Figura 20 - Tela principal do Mac Data Recovery Free.....40
Figura 21 - Escolha da unidade a ser examinada.....41
Figura 22 - Verificação de arquivos pelo Mac Data Recovery Free 41
Figura 23 - Exibição dos arquivos recuperados pelo Mac Data Recovery Free.....42
Figura 24 - Tutorial do Disk Drill 43
Figura 25 - Tutorial de como utilizar o Disk Drill.....43

Figura 26 - Tela principal da ferramenta Disk Drill 44

Figura 27 - Escolha da unidade a ser analisada pelo Disk Drill 44

Figura 28 - Realizando a análise.....45

Figura 29 - Arquivos recuperados com o Disk Drill 45

LISTA DE GRÁFICOS

Gráfico 1 - Comparativo dos resultados entre os softwares 50

LISTA DE TABELAS

Tabela 1 - Resultados obtidos pelo Recuva. 48

Tabela 2 - Resultados obtidos pelo DiskDigger. 48

Tabela 3 - Resultados obtidos pelo Foremost. 48

Tabela 4 - Resultados obtidos pelo Scalpel. 49

Tabela 5 - Resultados obtidos pelo Mac Data Recovery Free. 49

Tabela 6 - Resultados obtidos pelo Disk Drill. 49

LISTA DE QUADROS

Quadro 1 - Dados coletados.....50

LISTA DE ABREVIATURAS E SIGLAS

DOC – formato de documento do Office Word

JPEG/JPG – Joint Photographic Experts Group (tipo de formato de imagem)

MP3 – Moving Picture Experts Group 1 (MPEG) Audio Layer 3 (formato de compactação de áudio)

MP4 – formato de compactação de áudio e vídeo

NTFS – New Technology File System (sistema de arquivos)

PDF – Portable Document Format (formato de arquivo)

SUMÁRIO

RESUMO

ABSTRACT

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

SUMÁRIO **13**

1 INTRODUÇÃO **13**

2 OBJETIVOS **15**

2.1 OBJETIVOS GERAIS 15
2.2 OBJETIVOS ESPECÍFICOS 15

3 JUSTIFICATIVA **16**

4 FUNDAMENTAÇÃO TEÓRICA **17**

4.1 PERÍCIA FORENSE 17
4.2 PERÍCIA FORENSE COMPUTACIONAL 17
4.2.1 Perito Forense Digital *18*
4.2.2 Técnicas da Perícia Computacional *19*
4.2.3 Tipo de Investigação *20*
4.2.4 Coletando Evidências *21*
4.2.5 Laudos *23*
4.3 A ARTE DE RESTAURAR DADOS 25
4.3.1 Fatores que Levam a Perda de Dados *26*
4.3.2 Precauções *27*
4.3.3 Evitando a Recuperação de Arquivos *27*

5 ESTUDO DE CASO **29**

5.1 PREPARAÇÃO DO AMBIENTE 29
5.2 SISTEMAS OPERACIONAIS E SOFTWARES UTILIZADOS 29
5.2.1 Windows *29*
5.2.2 Linux *38*
5.2.3 Mac *40*

6 METODOLOGIA **47**

7 RESULTADOS **48**

8 CONSIDERAÇÕES FINAIS **51**

REFERÊNCIAS **53**

1 INTRODUÇÃO

O avanço constante da informática vem promovendo acesso rápido e prático a rede mundial de computadores, a Internet. Hoje em dia é cada vez mais comum encontrarmos lares com computadores conectados a Internet, fator que evidencia a inclusão digital que se vivencia.

Todavia, tais facilidades promovidas pela Internet abrem espaço para práticas ilícitas e de fundamentação não legal perante a lei, utilizando-se das falhas de segurança de um sistema e da ausência de leis suficientes que definam e tratem de crimes eletrônicos, bem como de tecnologia madura capaz de prover segurança e soluções praticáveis. Assim, aumentam os números de fraudes em transações financeiras pela Rede, invasões de privacidade em organizações, violação de direitos autorais ou destruição de conteúdo privado.

Nesse momento, surge a computação forense – campo da Ciência da Computação responsável pela preservação, identificação, extração e documentação de evidências criminais em sistemas de computador (Marcella e GrennField, 2001). Assim, sua importância é fundamental para toda a sociedade, focando seus esforços em promover um ambiente de informações seguro sob a ótica financeira, além de efetuar um papel investigativo e jurídico, assegurando direitos e punições aos responsáveis de atos ilícitos no âmbito digital.

O processo de análise forense executa uma série de atividades para uma investigação completa. Carrier (2002) cita que, para uma melhor abordagem sobre esse processo, a análise forense computacional pode ser dividida basicamente em três fases: a aquisição, onde são coletadas as evidências, a análise, que examina e analisa as provas adquiridas e a apresentação, que mostra os resultados da investigação.

Buscar vestígios digitais e caracterizá-los como evidências e provas de crime são atividades fundamentais da perícia forense computacional, que requerem cuidados e conhecimentos específicos. É preciso saber onde pesquisar por vestígios, que tipos de vestígios buscarem, dispor de conhecimento técnico para coletar e preservar esses vestígios, e observar a minimização dos riscos de sua deterioração ou invalidação como prova.

Muitas pessoas já pasaram por situações desesperadoras ao perceber que havia perdido algum arquivo ou documento de muita importância do nosso computador, mas

o que muitos não sabem é que quando esses arquivos são “perdidos” ou apagados acidentalmente, eles não são removidos completamente do sistema, e sim, perdem apenas a referência que indica o local de armazenamento daquele arquivo na mídia.

> A recuperação de dados é a ciência que procura reconstruir o sistema de arquivos para que se possam acessar os arquivos apagados. Cada sistema operacional tem um sistema de arquivos, que é um método único de indexar e monitorizar os arquivos. Infelizmente para os que perdem dados, os sistemas de arquivos podem ser muito complexos, razão pela qual pode ser muito difícil localizar arquivos apagados. Por exemplo, os sistemas de arquivos utilizados em meios empresariais requerem detalhes de segurança e dados de operações de acesso. Um bom exemplo disso é um sistema de arquivos baseado em operações, ou um livro-diário, cujo objetivo consiste em registar quando se acessa, modifica ou grava cada arquivo, sendo assim um sistema mais complicado e mais difícil de reconstruir (NÓBREGA, 2010).

Portanto, através de *softwares* específicos e técnicas de recuperação de dados, é possível restaurar quase sempre esses dados apagados.

2 OBJETIVOS

2.1 OBJETIVOS GERAIS

Utilizar técnicas forenses para recuperar arquivos apagados de um pendrive com o auxílio de alguns *softwares*. Considerando que serão testados *softwares* em três sistemas operacionais: Windows, Linux e Mac, realizando assim uma comparação entre os *softwares* utilizados e compararação em qual deles há uma maior margem de restauração dos arquivos.

2.2 OBJETIVOS ESPECÍFICOS

- Estudar técnicas forenses de recuperação de dados e pesquisar *softwares* específicos de recuperação de dados.
- Testar os *softwares* encontrados nos sistemas operacionais propostos.
- Realizar a recuperação de dados com cada *software* em cada Sistema Operacional.
- Coletar resultados e comparar os *softwares*.

3 JUSTIFICATIVA

Devido à perícia forense computacional estar em ascensão na área da tecnologia da informação, faz-se necessário o levantamento de informação bibliográfica a realização de alguns experimentos relacionados com a área para de alguma forma colaborar com a comunidade que tenha interesse no assunto. Ao final desse trabalho teremos uma comparação entre alguns *softwares* que foram testados nos Sistemas Operacionais mais utilizados hoje em dia, visando a recuperação das informações.

4 FUNDAMENTAÇÃO TEÓRICA

4.1 Perícia Forense

Segundo COSTA (2008) o termo Perícia vem do latim e significa destreza, competência e habilidade, e Forense se refere ao foro judicial, relativo aos tribunais. Pode-se dizer então, que a perícia forense é o termo adotado para os métodos científicos da criminalística para se identificar e obter a evidências necessárias para o auxilio da justiça.

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

4.2 Perícia Forense Computacional

Computação forense é o termo usado para designar a ciência de investigação criminal aplicada em sistemas digitais (MELO, 2009). Esta é a ciência usada pelos peritos quando são encontrados vestígios que envolvam equipamentos que possam armazenar algum tipo de dado eletrônico numa cena de crime, mas suas práticas também podem ser utilizadas por administradores de sistemas que suspeitem que a sua rede esteja sendo usada por pessoas ou para finalidades não autorizadas, mas não desejem iniciar um processo judicial propriamente dito.

Segundo Theodoro (2003), o estatuto processual classifica a perícia em:

> 1- Exame: é a perícia propriamente dita, pois consiste no trabalho que o perito faz de inspecionar coisas ou pessoas, procurando desvendar os aspectos técnicos ou científicos que, ocular mente, não se encontram visíveis.
> 2- Vistoria: trata-se da mesma atividade do Exame, mas restrita aos bens imóveis;
> 3- Avaliação: é a atribuição de valores para bens jurídicos (direitos, obrigações, coisas).

Theodoro ressalta ainda, que a perícia possa ser classificada em:

> a) Judicial: a que ocorre dentro do processo, com perito nomeado pelo juiz.
> b) Extrajudicial: parecer técnico apresentado pela parte (autor e/ou réu), instruindo a inicial e a contestação, a fim de se evitar a perícia judicial.
> c) Informal: espécie de perícia judicial, onde o laudo é dispensado. Pode o juiz inquirir o perito e assistentes técnicos acerca do que verificaram, sem o formalismo do laudo.

Da necessidade do avanço científico, e utilizando-se do conceito de perícia forense, surge uma ciência para garantir que a manipulação dessas novas formas de evidências eletrônicas fossem aceitas em juízo: A análise forense computacional (BARROS, 2009). Segundo o mesmo autor, a análise forense computacional:

> compreende a aquisição, preservação, identificação, extração, restauração, análise e documentação de evidências, quer sejam componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais.

As provas "podem ser as mais diversas possíveis como *e-mails*, arquivos de registros (conhecidos como *logs*), arquivos temporários com informações pessoais, conexões abertas, processos em execução" e, além disso, toda e qualquer "evidências que possam existir na máquina, mas para serem aceitas num processo jurídico, devem ter sido obtidas de forma lícita." (TREVENZOLI, 2006, p.11)

As provas de crimes digitais, como quaisquer outras provas, devem ser autênticas, exatas, completas e precisam convencer o júri ou a corporação e estarem em conformidade com a lei. (PIMENTA, 2007, p.15).

Por fim, "uma perícia em um computador suspeito de invasão ou mesmo um computador apreendido em alguma batida policial envolve uma série de conhecimentos técnicos e a utilização de ferramentas adequadas para análise" (BARROS, 2009, p.12):

> Existe a necessidade de se conhecer minúcias do sistema operacional para que se tenha uma noção global de todos os efeitos das ações do perito.
> Quanto à necessidade de se utilizar ferramentas específicas para análise, esta decorre da obrigatoriedade de não se perturbar o sistema que está sendo analisado, perturbações essas que podem ser traduzidas como mudanças nos tempos de acesso aos arquivos anulando, assim, uma das mais poderosas formas de se reconstituir o que aconteceu na máquina em um passado próximo. Ferramentas convencionais não têm a preocupação de manter a integridade dos tempos de acesso. A "Cena do Crime" deve ser preservada para que provas não sejam acidentalmente modificadas ou perdidas.

4.2.1 Perito Forense Digital

É o profissional capacitado e preparado para realizar uma perícia sendo que uma das habilidades necessárias para um perito nesta área é possuir conhecimentos sobre o funcionamento do sistema operacional a ser pesquisado. Com base nesse conhecimento, o perito tem maior capacitação para reconstituir o cenário do passado (procedimento

utilizado para traçar o caminho feito pelo fraudador e facilitar a compreensão do ocorrido) onde há o suspeito crime digital.

O perito forense é o responsável em orientar a equipe quanto à seleção dos equipamentos computacionais, que também faz a preservação e a coleta desses equipamentos para realizar exames forenses posteriormente (Eleutério; Machado, 2011).

De acordo com Milagre (2011), a principal função de um perito forense é reconhecer o local do crime, reconstruir o passado, constatar a materialidade e apurar a autoria de incidentes cometidos com o requinte dos bits.

Eleutério e Machado (2011) citam que depois do reconhecimento do local, deve-se tomar providencias imediatas para a preservação dos dados digitais e isso inclui não deixar que pessoas estranhas à equipe usem os equipamentos computacionais sem a supervisão de um perito, e também não ligar equipamentos computacionais que estejam desligados.

Algumas ações só devem ser realizadas se o perito forense tiver total certeza que isso não ocasionará perdas de evidencias digitais, essas ações podem ser: interromper conexões de rede se existirem, também se pode retirar a fonte de energia dos equipamentos computacionais para desligar, não usar dessas ações se tiver alguma possibilidade de flagrante do delito, como posse de dados ilegais como a pornografia infanto-juvenil, explicam Eleutério e Machado (2011).

O perito, e da mesma forma os assistentes técnicos, não estão, a princípio, nos casos de confecção de laudo escrito, obrigados a comparecer à audiência de instrução, exceto se uma das partes o requerer, perante o juiz, hipótese possível, desde que efetuada no máximo em até cinco dias antes da audiência e apresentando quais as perguntas que deseja que sejam respondidas, sob a forma de quesitos (PAULA, 2003, n.p.).

4.2.2 Técnicas da Perícia Computacional

Independente da área em que será realizada a pericia será necessário utilizar técnicas que possam tornar possível a análise dos elementos de prova. As técnicas empregadas atualmente são de grande auxílio e tornam possível observar a veracidade aos fatos.

Para cada tipo de análise existe uma técnica específica, a qual torna possível identificar e evidenciar a veracidade dos fatos.

Segundo Vargas (2007), com a chegada e a ampliação da tecnologia nos últimos tempos, as violações, invasões, busca, venda e roubo de dados privilegiados, pirataria, emissão de *e-mails* falsos e fraudulentos, tentativas de acessos indevidos a empresas, e até mesmo as pessoas comuns que vêm se modernizando existe a necessidade do auxílio de ferramentas mais atualizadas para encontrar esses infratores.

4.2.3 Tipo de Investigação

Antes de começar a coleta dos dados, deve-se primeiro planejar como a investigação será realizada para que evidências sensíveis e voláteis não sejam perdidas.

Um aspecto a ser considerado dentro de uma investigação é se ela será executada em um sistema desligado ou em uso. Alguns dados críticos somente podem ser obtidos com a máquina ainda ligada e em rede, esta é a chamada análise viva (*Live Analysis*). Quando estes dados não forem necessários ou já tiverem sido coletados, o computador poder ser desligado e seu sistema analisado sem o perigo destes serem alterados. Esta análise é conhecida como *Post Mortem* (MELO, 2009).

A análise *Post Mortem* deve ser escolhida quando o sistema a ser analisado possa ser desligado e o dispositivo de armazenamento recolhido. Para isso, os dados são transferidos bit a bit (ou bloco a bloco) para outro local e esta cópia será analisada enquanto o original é mantido a salvo de modificações em um local adequado. Com o clone da mídia em mãos, o investigador seguirá o planejamento inicial para encontrar dados que servirão de prova para uma determinada hipótese.

No entanto, muitas vezes este tipo de análise não pode ser efetuado por motivos que fogem ao controle do perito. Segundo Melo (2009), o crescimento dos HDs, com alguns chegando a 1TB (um terabyte) de tamanho, faz com que esta cópia bit a bit torne-se cada vez mais complicada e dispendiosa. Outro fator que impede o desligamento de uma máquina para a cópia de sua mídia de armazenamento é de questão econômica. Eventualmente, o computador a ser examinado é um servidor de cujo funcionamento depende toda uma empresa. Cada minuto com um serviço fora do ar pode acarretar perdas de grandes valores em multas e/ou clientes. Mas, mesmo quando os dois motivos anteriores não se enquadrem no momento, alguns dados

periciais simplesmente se perdem ao se desligar o sistema, como, por exemplo, clientes logados na máquina, dados da memória volátil, arquivos abertos no momento, processos ativos etc.

Sendo assim, a técnica chamada Análise Viva *(Live analysis*) é usada. Esta abordagem está sendo cada vez mais seguida quando os dados voláteis do sistema são de suma importância para o caso investigado ou quando o sistema, por algum motivo, não possa ser desligado (MELO, 2009).

Segundo NASCIMENTO (2010) alguns problemas neste tipo de investigação podem ser apontados. Um deles é que, ao se extrair um dado, o estado da máquina e outros dados são modificados. Outro que se pode observar é que os diversos dados dentro de uma máquina, dependendo de como eles são armazenados, têm níveis de volatilidade diferente. Sendo assim, deve-se respeitar a ordem de volatilidade dos dados no momento de extraí-los, sempre observando a relevância dos mesmos dentro do caso.

Outro tipo de investigação é a forense de rede, que é usada quando os dados periciais estão em arquivos e aplicações usadas para fazer computadores se ligarem em rede ou nos dados provenientes desta ligação. Neste tipo de análise, dispositivos de rede são destrinchados e ferramentas apropriadas são usadas para captar tráfego e estado de rede (NASCIMENTO, 2010).

4.2.4 Coletando Evidências

Segundo Aquilina (2003), o ato de coleta de dados ao vivo a partir de um sistema digital provoca mudanças que um investigador terá de explicar no que diz respeito ao seu impacto sobre a prova digital. Por exemplo, executando ferramentas como Helix, a partir de uma mídia removível o dispositivo irá alterar dados voláteis quando é carregado na memória principal, e vai geralmente criar ou modificar arquivos e entradas do Registro no sistema probatório. Da mesma forma, utilizando remotamente as ferramentas forenses, necessariamente se estabelece uma conexão de rede, executa instruções na memória e faz outras alterações no sistema probatório.

Para realizar a análise e coleta de evidências são seguidos procedimentos rígidos para que não exista nenhuma irregularidade durante a investigação do fato, o que pode fazer com que o juiz considere a prova inadmissível.

O processo de coleta de evidências é regido por leis, toda a evidência deve ser autenticada, o que significa que alguma testemunha tem o dever de testemunhar sua autenticidade. No caso da evidência digital esta poderá ser um testemunho pessoal, no qual o individuo tenha conhecimento dos elementos de prova como um perito, por exemplo.

Também existem as evidências as quais não necessitam de testemunho como documentos públicos e publicações oficiais (SHINDER, 2002).

Existem três categorias de provas:

1. Provas físicas: consiste em objetos materiais que podem ser vistos e tocados;
2. Provas de testemunho direto: o depoimento de uma testemunha que pode narrar os fatos de acordo com sua experiência pessoal através dos cinco sentidos;
3. Provas circunstanciais: não baseadas em observação pessoal, mas em observação ou conhecimento de fatos que tendem a apoiar uma conclusão indiretamente, mas não provam isto definitivamente.

Segundo SHINDER (2002), em casos de crimes computacionais as provas são classificadas pelas normas SWGDE (Scientific Working Group on Digital Evidence) / IOCE (The International Organization of Computer Evidence):

1. Provas digitais: informação de valor para um processo penal que está armazenada ou transmitida de forma digital;
2. Dados objetos: consiste em objetos de valor para um processo penal o qual está associado a itens físicos;
3. Itens físicos: consiste nas mídias físicas onde a informação digital é armazenada ou pelo qual é transmitido ou transferido.

Para se iniciar um processo de perícia computacional é necessário seguir procedimentos rigorosos, visando à integridade das provas. São estes requisitos que tornam a prova admissível em um tribunal.

4.2.5 Laudos

Segundo Campos (2011), a fase de Formalização consiste em elaborar um Laudo Pericial, explicando e apresentando as provas digitais coletadas com garantia de integridade.

Carrier (2002) cita que a fase de formalização apresenta as conclusões e as provas correspondentes da investigação. Quando se trata da investigação de uma corporação, a audiência normalmente inclui o conselho geral, recursos humanos e executivos. Em uma definição legal, a audiência é composta, basicamente, de um juiz e o júri, mas os advogados devem primeiro avaliar as provas e aprová-las antes de levar ao tribunal, por isso o trabalho em conjunto com os peritos.

A preparação do laudo pericial, é a ultima parte da fase de formalização, ou seja, o resultado final mostrando assim os resultados da análise, expondo as evidências digitais localizadas nos equipamentos analisados. Nesse laudo é necessário relatar os principais procedimentos efetuados contendo assim as técnicas usadas para preservar, extrair e analisar o conteúdo de equipamentos digitais. Com isso o perito deve saber que o laudo é um documento técnico - cientifico, sendo assim ele deve escrever com clareza e objetividade os métodos e exames feitos (Eleutério; Machado, 2011). Para sua segurança e transparência do processo forense, normalmente existe uma estrutura própria para se realizar um laudo formado geralmente pelas etapas seguintes:

- Preâmbulo: o objetivo é fazer a identificação do laudo, como ilustra a Figura 1.

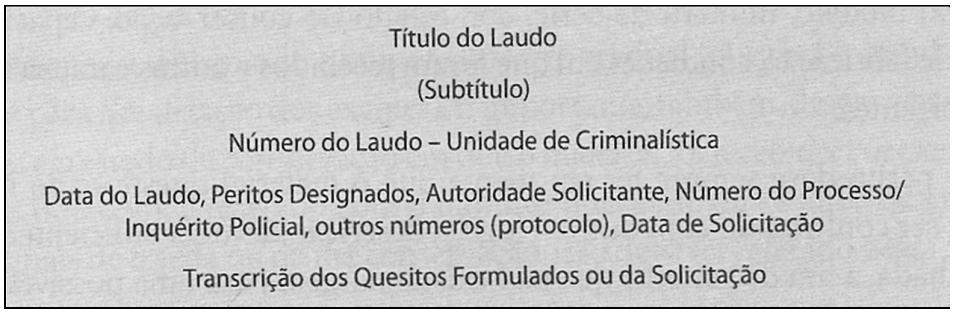
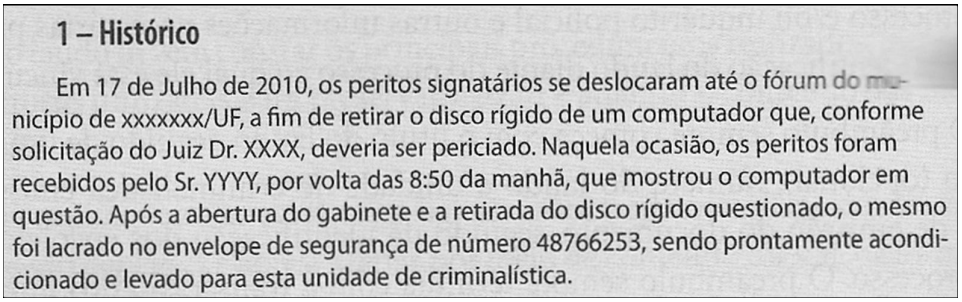


Figura 1 - Principais informações a serem inseridas no preâmbulo do laudo.
Fonte: Machado (2011)

- Histórico: essa etapa é opcional, e tem como objetivo descrever eventos passados relacionados ao laudo (Figura 2).



1 – Histórico

Em 17 de Julho de 2010, os peritos signatários se deslocaram até o fórum do município de xxxxxxx/UF, a fim de retirar o disco rígido de um computador que, conforme solicitação do Juiz Dr. XXXX, deveria ser periciado. Naquela ocasião, os peritos foram recebidos pelo Sr. YYYY, por volta das 8:50 da manhã, que mostrou o computador em questão. Após a abertura do gabinete e a retirada do disco rígido questionado, o mesmo foi lacrado no envelope de segurança de número 48766253, sendo prontamente acondicionado e levado para esta unidade de criminalística.

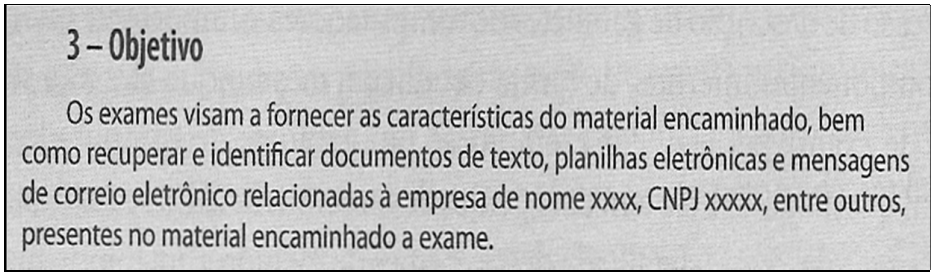
Figura 2 - Exemplo de texto contido na seção Histórico.
Fonte: Machado (2011)

- Material: o objetivo é descrever com detalhes o material analisado no laudo, como está sendo ilustrado na Figura 3.

Referência	Tipo	Características
HDD	Disco Rígido	**Marca:** Samsung **Capacidade Nominal:** 40GB **Modelo:** SP0411N **P/N:** 0881J1BXC35659 **S/N:** S01JJ50XC84329 **País de Fabricação:** Coréia

Figura 3 - Exemplo de descrição de um disco rígido em formato tabular.
Fonte: Machado (2011)

- Objetivo: no objetivo constam dois parágrafos, mostrando os objetivos principais da realização da análise (Figura 4).



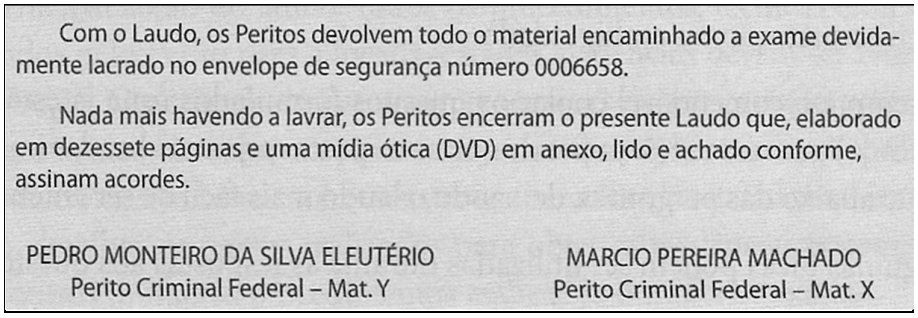
3 – Objetivo

Os exames visam a fornecer as características do material encaminhado, bem como recuperar e identificar documentos de texto, planilhas eletrônicas e mensagens de correio eletrônico relacionadas à empresa de nome xxxx, CNPJ xxxxx, entre outros, presentes no material encaminhado a exame.

Figura 4 - Exemplo de objetivo de um laudo.
Fonte: Machado (2011)

- Considerações técnicas/periciais: essa etapa é opcional, e tem como objetivo explicar os procedimentos, conceitos e a técnicas utilizadas.
- Exames: é a principal etapa do laudo, tem como objetivo relatar os procedimentos, técnicas e métodos usados pelo perito.

- Respostas aos quesitos/ conclusões: nessa ultima etapa é feito um resumo objetivo dos resultados alcançados nas análises, como mostra a Figura 5.



Com o Laudo, os Peritos devolvem todo o material encaminhado a exame devidamente lacrado no envelope de segurança número 0006658.

Nada mais havendo a lavrar, os Peritos encerram o presente Laudo que, elaborado em dezessete páginas e uma mídia ótica (DVD) em anexo, lido e achado conforme, assinam acordes.

PEDRO MONTEIRO DA SILVA ELEUTÉRIO
Perito Criminal Federal – Mat. Y

MARCIO PEREIRA MACHADO
Perito Criminal Federal – Mat. X

Figura 5 - Exemplo de finalização de laudo, incluindo devolução de material lacrado e assinaturas.
Fonte: Machado (2011)

4.3 A Arte de Restaurar Dados

Quando um arquivo é apagado e logo em seguida esvazia-se a lixeira do sistema operacional, esse arquivo ainda existe em seu dispositivo de armazenamento de dados, seja ele um disco rígido, pendrive ou até um cartão de memória.

Isso acontece porque o sistema remove apenas a referência do arquivo apagado na tabela de alocação de arquivos e libera a área do disco que ele usa para gravação de novos dados. Enquanto essa área não é sobrescrita por novos arquivos, existe a possibilidade de recuperação dos arquivos que se estavam gravados nessa área.

Existem diversos programas de recuperação de arquivos, tanto pagos quanto gratuitos, dos quais iremos citar dois para cada sistema operacional, sendo todos disponibilizados gratuitamente.

Os processos para recuperação de arquivos tanto em unidades físicas quanto em unidades removíveis, no caso o pendrive, é exatamente o mesmo.

Policiais usam a recuperação de dados forenses para explorar os computadores dos suspeitos do crime. Se um suspeito tinha excluído arquivos, mídia ou *e-mails* que podem conter elementos de prova de um crime, recuperação de dados forenses pode extrair partes de dados excluídos para uso no Tribunal. Técnicas semelhantes podem ajudar outros usuários de computador que podem ter excluído acidentalmente um importante arquivo ou precisam de acesso aos negócios antigo ou documentos pessoais (JULIEN, 2012).

4.3.1 Fatores que Levam a Perda de Dados

Discos rígidos, pendrives, cartões de memória, entre outras mídias onde podem ser gravados dados, são dispositivos que possuem certa sensibilidade por possuírem uma mecânica um tanto quanto delicada. Por isso, caso essa mídia sofra uma queda ou algum dando físico é possível que os dados gravados na mesma sofram alterações, podendo esses ser apagados ou corrompidos, tais danos também podem se originar de algum erro lógico no sistema.

Abaixo, descrevemos alguns dos principais motivos que geralmente resultam na perda de arquivos:

- Apagamento ou alteração dos dados através do uso de algum programa específico;
- formatação acidental;
- apagamento involuntário de arquivo ou diretório;
- ataque de vírus;
- operação errônea de programa utilitário para discos;
- falha no sistema operacional;
- atuação indevida de programa;
- falta ou grande variação de energia elétrica;
- defeito no hardware do computador;

É comum a prática de recuperação de arquivos por usuários não especializados no assunto por meio de ferramentas disponibilizadas aos montes na Internet, porém, se não houver algumas cautelas pode acabar por comprometer ou até mesmo inviabilizar o resgate dos dados apagados.

Os peritos forenses além de possuírem mais afinidade ao assunto, sabendo exatamente como proceder de forma a resgatar todo, ou parcialmente, o conteúdo, possuem também um conjunto de ferramentas mais poderosas para essa prática.

4.3.2 Precauções

É altamente recomendável que ao realizar a recuperação de arquivos apagados, ou formatados, não grave nenhum arquivo novo na mídia onde o arquivo apagado estava armazenado, pois isso pode fazer com que o novo arquivo gerado pela restauração sobrescreva os antigos arquivos, tornando praticamente impossível uma restauração completa.

Se a unidade a ser restaurada se trata da unidade do sistema (geralmente C:) não se deve instalar nenhum programa, nem mesmo o que será utilizado para a recuperação. O ideal é que se use um *software* de recuperação portátil, caso não tenha nenhum disponível no momento, o indicado é que realize o *download* em outro computador e passe em um pendrive para assim poder utilizar.

Cerifique-se de manter o sistema o mais próximo possível do estado inalterável, pois o simples fato de abrir ou fechar programas pode gerar arquivos temporários que podem vir a substituir os arquivos apagados.

Ao final de uma restauração de dados, grave os arquivos obtidos em um local diferente de onde se originavam anteriormente. Nunca grave esses arquivos na mesma mídia que foi restaurada.

4.3.3 Evitando a Recuperação de Arquivos

Como citado anteriormente, um arquivo apagado não é removido por completo do sistema, possibilitando sua recuperação através de ferramentas e técnicas específicas. Mas existem situações onde pode ser necessário eliminar os arquivos por completo do sistema, evitando a recuperação do mesmo.

Existem técnicas para impossibilitar a recuperação de alguma mídia ou unidade que contenha arquivos que devem ser completamente apagados de uma vez por todas. O fato de sobrescrever os arquivos é um exemplo, mas para que essa técnica seja realmente eficiente e possa garantir que os arquivos não possuem mais acesso, é preciso realizar métodos de sobrescrita mais complexos.

Existem diversos aplicativos que fazem uma formatação diferente daquela que estamos acostumados a realizar quando um sistema operacional é instalado no disco rígido. O chamado *zero fill* é um método de limpeza definitivo do HD, o qual consiste

em preencher cada bit com o valor binário zero, como quando o disco sai de fábrica (MARTINS, 2011).

O *zero fill* pode ser muito útil também quando se adquire um dispositivo de armazenamento usado, pois é uma forma de garantir que não há nenhum vírus ou programa malicioso instalado. Contudo, o fato de utilizar o método *zero fill* garante que pessoas comuns ou até mesmo, em alguns casos, que policiais peritos não consigam recuperar os arquivos apagados, porém existem centenas de programas e soluções desenvolvidas que não estão ao alcance do público geral, uma vez que são utilizados por organizações governamentais poderosas na recuperação de discos, utilizados em espionagens e outros tipos de crimes (MARTINS, 2011).

5 ESTUDO DE CASO

5.1 Preparação do ambiente

Para a realização da ideia proposta inicialmente foi preparado um ambiente para a aplicação dos *softwares* de recuperação de arquivos nos sistemas operacionais escolhidos, mais especificamente, foi preparado um pendrive contendo alguns arquivos, os quais seguem listados abaixo:

- Pasta “Músicas”: dez (10) arquivos de extensão *.mp3*;
- Pasta “Imagens”: dez (10) arquivos de extensão *.jpeg*;
- Pasta “Textos”: cinco (5) arquivos de extensão *.doc* e cinco (5) arquivos de extensão *.pdf*;
- Pasta “Vídeos”: cinco (5) vídeos no formato *.mp4*.

Ao todo, o pendrive continha 35 arquivos diversos e 4 pastas. Após serem colocados esses arquivos no pendrive, o mesmo foi formatado e a partir disso, pode-se fazer uso dos *softwares* de recuperação de arquivos, cada qual em seu sistema operacional.

5.2 Sistemas Operacionais e Softwares Utilizados

5.2.1 Windows

5.2.1.1 Recuva

É um programa gratuito que oferece uma forma fácil de recuperação de arquivos apagados do disco rígido, pendrive, cartão de memória, MP3 Player, iPod, entre outros. Possui também uma versão portátil e é compatível com Windows XP, Vista, Windows 7 e 8. Pode ser encontrado facilmente em *sites* de *download* na Internet como, por exemplo, no endereço: <www.baixaki.com.br>.

A seguir, segue um breve passo a passo de como usar a ferramenta para recuperar arquivos apagados.

Após a instalação, o programa se inicia automaticamente, conforme mostrado na Figura 6, com o seu “Assistente” que vai orientando o usuário por todo o processo de recuperação dos arquivos.

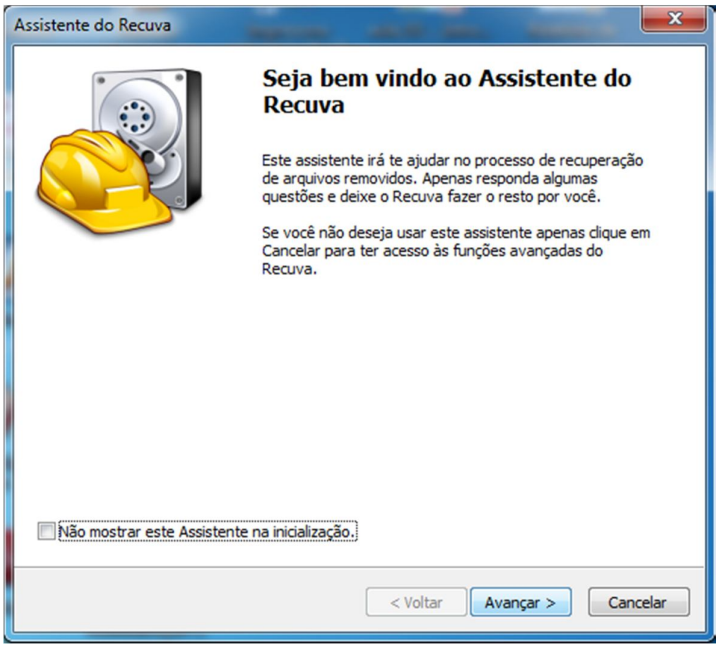


Figura 6 - Assistente do Recuva
Fonte: Recuva

Na Figura 7 é possível observar o próximo passo do “Assistente do Recuva”, o qual nos solicita que seja escolhido o tipo de arquivo que se deseja recuperar, a princípio selecionamos item “Imagens”.

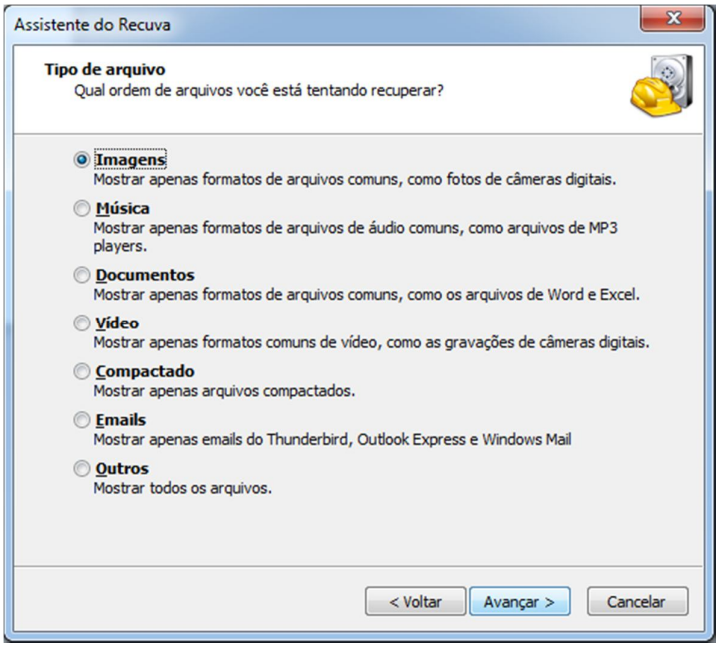


Figura 7 - Escolhendo tipo de arquivo a ser recuperado no Assistente do Recuva
Fonte: Recuva

A seguir, o "Assistente do Recuva" solicita que indiquemos o local de origem dos arquivos apagados, no nosso caso, se tratando de um pendrive, a unidade escolhida foi a E:(Figura 8).

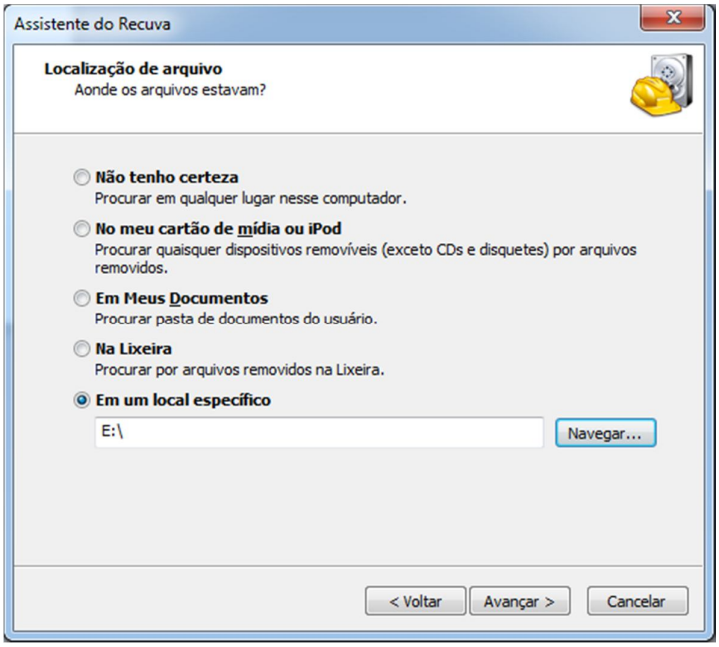


Figura 8 - Localizando o local de origem dos arquivos apagados no Recuva
Fonte: Recuva

Depois de fornecidas as devidas informações ao *software*, basta clicar em “Iniciar” e deixar que ele comece a vasculhar a unidade selecionada em busca de arquivos apagados (Figura 9).

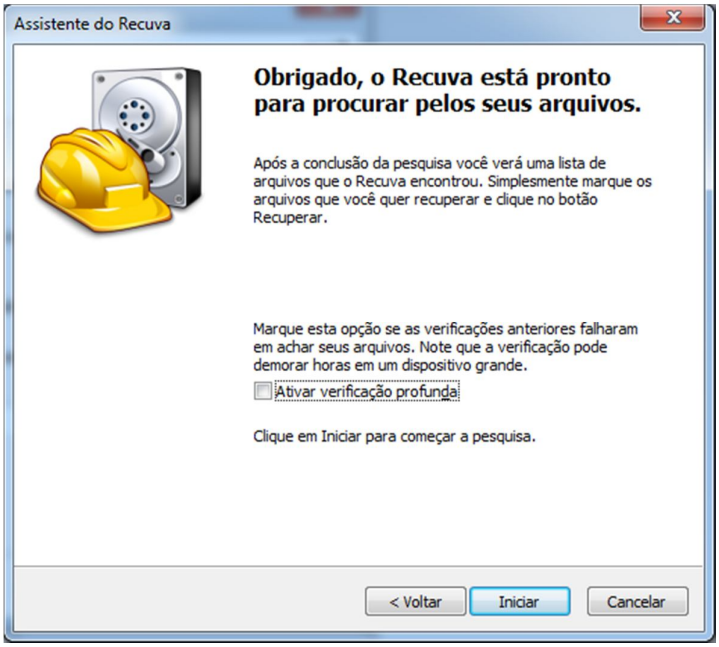


Figura 9 - Iniciando o processo de recuperação de arquivos do “Assiste do Recuva”
Fonte: Recuva

Após o término da verificação, o programa exibe quais os arquivos que foram encontrados e podem ser recuperados. O *software* inclusive exibe uma pré-visualização de alguns dos arquivos encontrados (Figura 10).

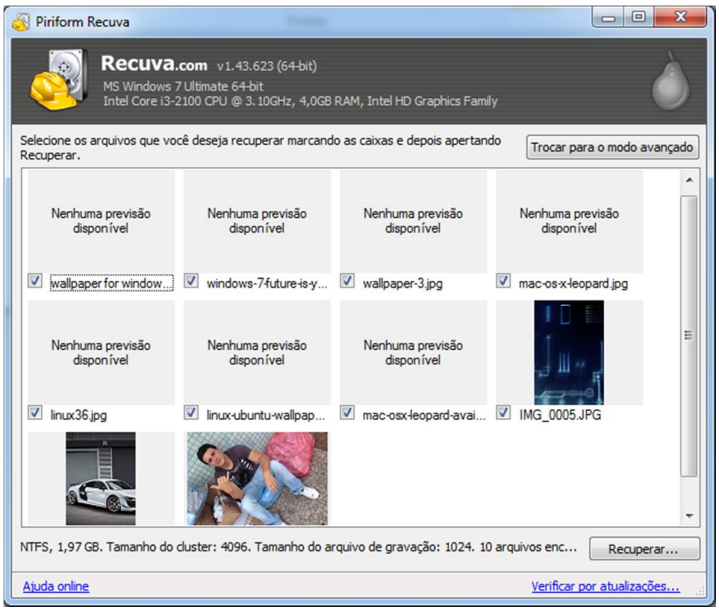


Figura 10 - Arquivos encontrados pelo "Assistente do Recuva"
Fonte: Recuva

Na tela onde são exibidos os arquivos encontrados, é possível selecionar somente aqueles que se deseja recuperar, ou todos os arquivos. Feito isso, basta clicar em “Recuperar...” e selecionar um local para que o programa possa recuperar esses arquivos e salvá-los no local definido, conforme ilustra a Figura 11.

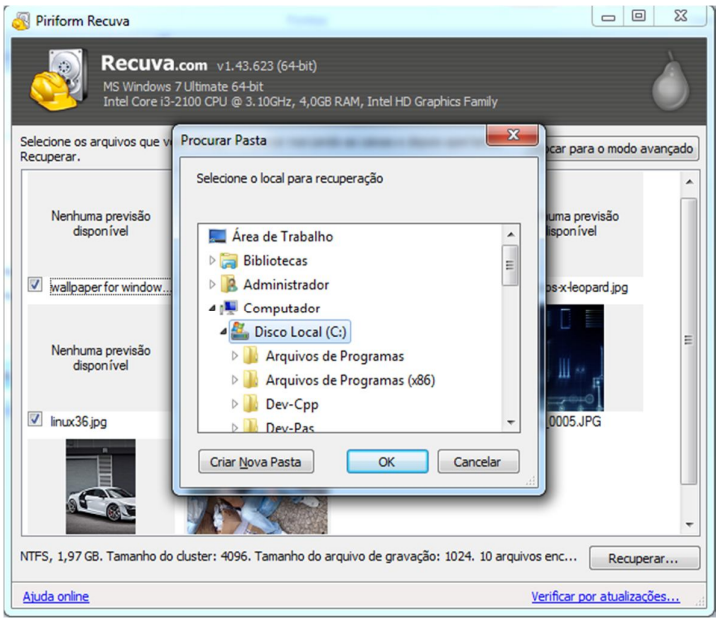


Figura 11 - Selecionando o local onde os arquivos serão restaurados
Fonte: Recuva

Lembre-se de sempre recuperar os arquivos em qualquer outra unidade desde que não seja a mesma unidade de origem dos arquivos.

Na Figura 12 é possível perceber que ao recuperar os arquivos e salvá-los no local escolhido anteriormente, esses arquivos acabam por alterar o próprio nome em algumas vezes, ficando com uma nomenclatura numérica.

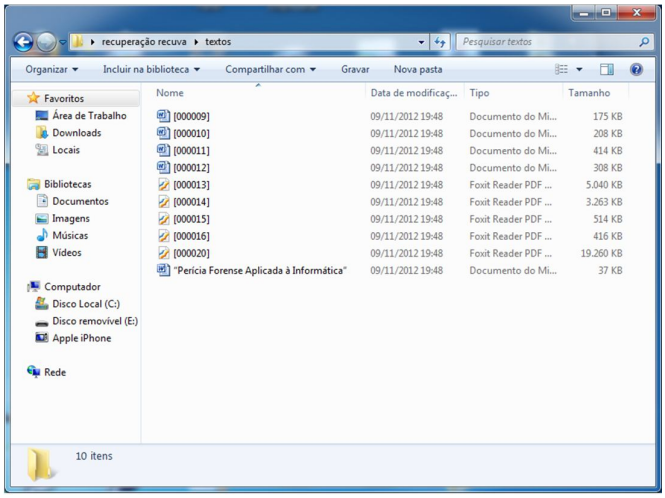


Figura 12 - Pasta contendo os arquivos recuperados pelo Recuva
Fonte: Propriedade do autor

O Recuva também conta com um modo de recuperação de arquivos avançado, com uma tela um pouco mais detalhada que realiza o mesmo processo para recuperar arquivos (Figura 13).

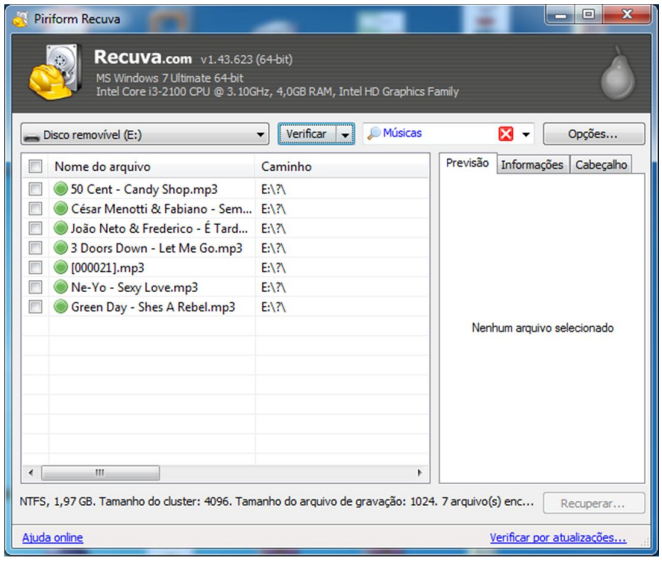


Figura 13 - Modo de recuperação de arquivos avançado, sem o "Assistente do Recuva"
Fonte: Recuva

5.2.1.2 DiskDigger

DiskDigger é uma ferramenta gratuita capaz de vasculhar a fundo seu sistema em busca de arquivos excluídos na tentativa de recuperá-los. O programa pode procurar itens dentro de pendrives, câmeras digitais, cartões de memória e, obviamente, em seu próprio disco rígido. Com uma *interface* intuitiva, bem organizada e fácil de usar, com poucos cliques você pode recuperar vários arquivos apagados de diversas extensões e formatos.

A Figura 14 ilustra como a ferramenta pode ser utilizada para tal recuperação:

Como pode ser obervado na Figura 14 foi selecionada a opção E: onde se encontra o pendrive formatado para a realização da recuperação dos arquivos apagados.

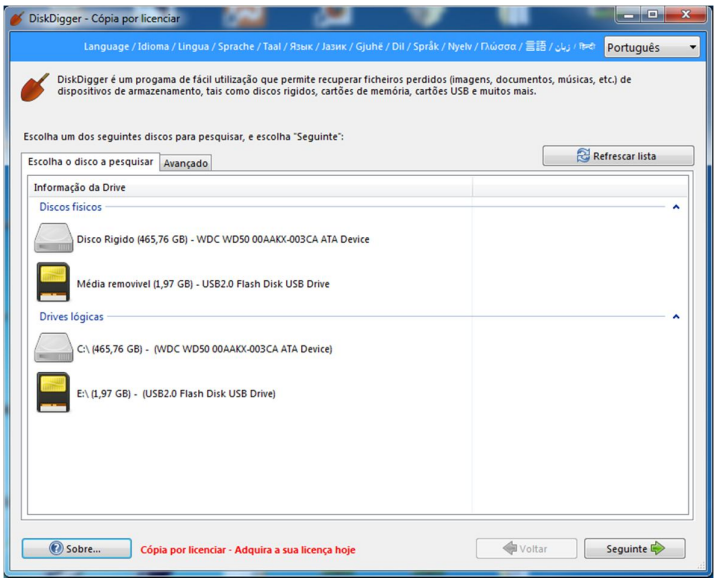


Figura 14 - Tela inicial da ferramenta DiskDigger para escolher a unidade de origem dos arquivos apagados
Fonte: DiskDigger

Na Figura 15, o *software* possibilita o usuário a escolher o tipo de busca que deseja fazer na unidade escolhida.

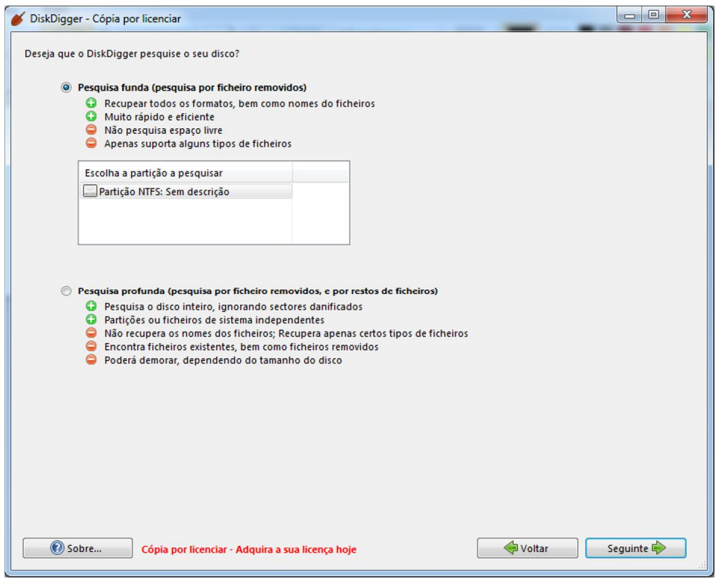


Figura 15 - Tela para escolher as configurações da busca por arquivos no DiskDigger
Fonte: DiskDigger

O DiskDigger oferece a possibilidade do usuário poder selecionar os tipos de arquivos que o programa deve buscar no diretório apontado no início, sendo uma lista muito bem organizada, dividida por categorias e com praticamente todos os tipos de arquivos existentes (Figura 16).

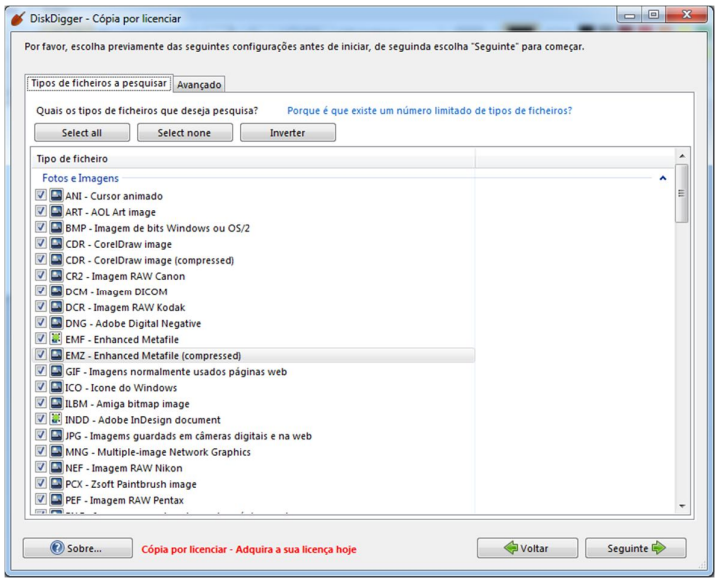


Figura 16 - Tela para escolher os tipos de arquivos que o DiskDigger deve buscar
Fonte: DiskDigger

Após a análise do DiskDigger é exibida uma mensagem em tela dizendo quantos arquivos foram possíveis recuperar, separando-os em categorias por tipo de arquivo assim como é exibido na Figura 17.

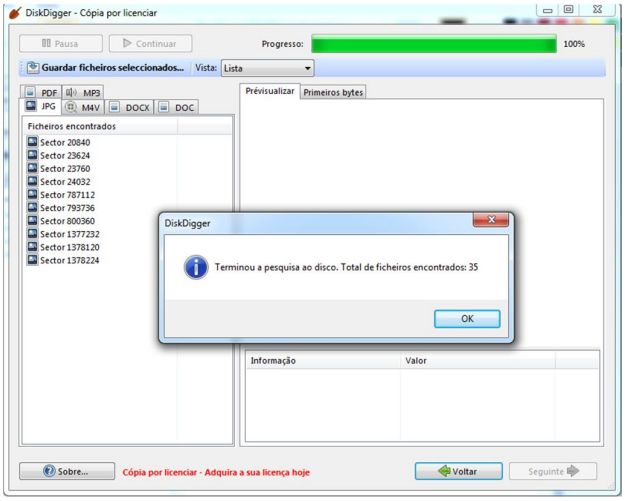


Figura 17 - Tela mostrando o total de arquivos recuperados pelo DiskDigger
Fonte: DiskDigger

Com os dados encontrados já disponíveis para a recuperação, basta selecionar os arquivos desejados e clicar em “Guardar ficheiros selecionados...” e escolher um local para restaurar os arquivos apagados (Figura 18).

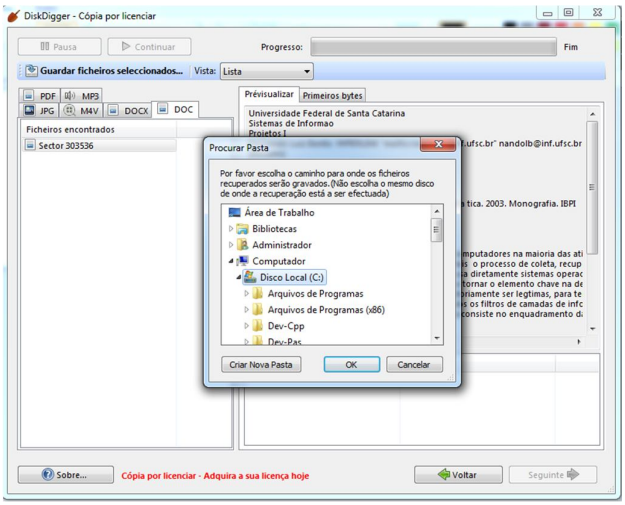


Figura 18 - Salvando os arquivos recuperados pelo DiskDigger
Fonte: DiskDigger

Lembrando novamente que nunca deve se utilizar a mesma unidade de origem dos dados apagados para salvar os arquivos recuperados.

Como o DiskDigger é um *software* gratuito, ele conta com um temporizador de cinco segundos para cada arquivo que se deseja recuperar, isso acaba tornando o processo um pouco inviável quando se deseja recuperar muitos arquivos sem ter a preocupação de ficar clicando em algum botão a todo instante (Figura 19).

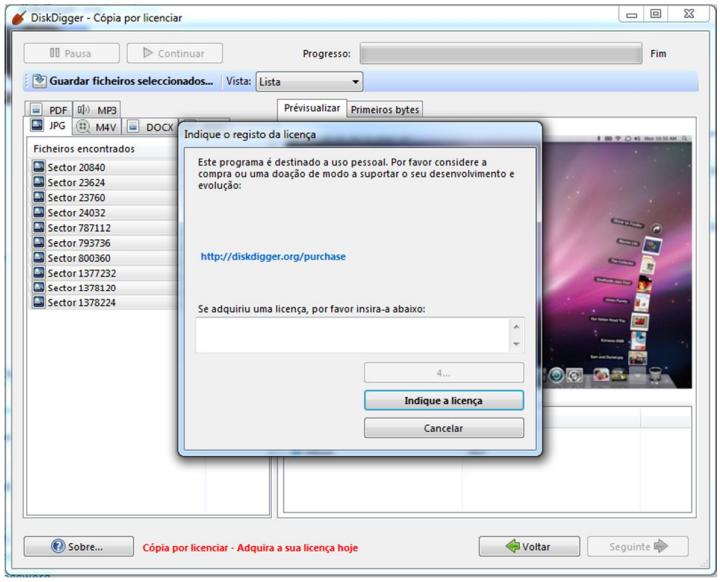


Figura 19 - Solicitação de licença de uso do DiskDigger
Fonte: DiskDigger

5.2.2 Linux

5.2.2.1 Foremost

A ferramenta Foremost, segundo o *site* oficial[1], acima de tudo é um programa de console para recuperar arquivos com base em seus cabeçalhos, rodapés e estruturas de dados internas. O programa permite trabalhar em arquivos de imagem gerados por softwares de perícia forense, como dd, Safeback, Encase, etc, ou diretamente na unidade. Essa ferramenta pode ser adquirida livremente para qualquer sistema Linux.

[1] *http://foremost.sourceforge.net/*

A utilização dessa ferramenta é feita através do terminal do Linux, seguindo a sintaxe:

foremost [-h][-V][-d][-vqwQT][-b<blocksize>][-o<dir>] [-t<type>][-s<num>][-i<file>]

A descrição para as opções acima podem ser obtidas no manual da ferramenta. Segue um exemplo da utilização da ferramenta para buscar todos os tipos de arquivos definidos:

sudo foremost -t all -i image.dd

Ao término da busca, esta ferramenta gera um arquivo em formato de texto com um resumo da operação e uma pasta para cada tipo de arquivo encontrado.

5.2.2.2 Scalpel

O Scalpel, segundo o *site* oficial[2], é um programa *opensource* e tem o Linux como sistema operacional preferencial, mas pode ser utilizado também em ambiente Windows e Mac OS X, para isso basta compilar seu código fonte no sistema desejado.

A utilização desse programa também é através do terminal do Linux, mas antes é preciso acessar o documento *scalpel.conf* e tirar os comentários referentes aos tipos de arquivos que se deseja obter na recuperação dos mesmos, após isso, basta abrir o terminal e utilizar a seguinte sintaxe:

sudo scalpel <device name/Directory name/file name> -o <ouput directory>

Sendo que basicamente passamos o nome do dispositivo, ou diretório do mesmo e informamos o diretório de saída, onde vão ser gravados os dados recuperados. Segue um exemplo de uso do Scalpel:

sudo scalpel imagem_01.dd -c /etc/scalpel/scalpel.conf -o scalpel_01

[2] *http://www.digitalforensicssolutions.com/Scalpel/*

É possível fazer uma busca mais avançada com o Scalpel, para isso existem outras opções de sintaxe na linha de comando de execução do programa, as quais podem ser conferidas no manual da ferramenta.

5.2.3 Mac

5.2.3.1 Mac Data Recovery Free

Foi usada a versão *Free* desse *software* para a realização dos testes. Essa versão conta com um limite de recuperação de dados de apenas 1Gb. É possível comprar uma licença tanto comercial quanto para uso doméstico.

Abaixo um passo a passo de como utilizar esse *software*.

Na Figura 20 é possível ver a *interface* principal do sistema, onde ele oferece as opções de recuperação de dispositivos móveis, arquivos apagados, ou mesmo de partições danificadas. Também apresenta opções para se adquirir um CD de *boot* e um botão para suporte do programa.

Figura 20 - Tela principal do Mac Data Recovery Free
Fonte: Mac Data Recovery Free

Após a escolha da ação que o programa deverá tomar, deve-se escolher a unidade desejada para a recuperação dos arquivos (Figura 21).

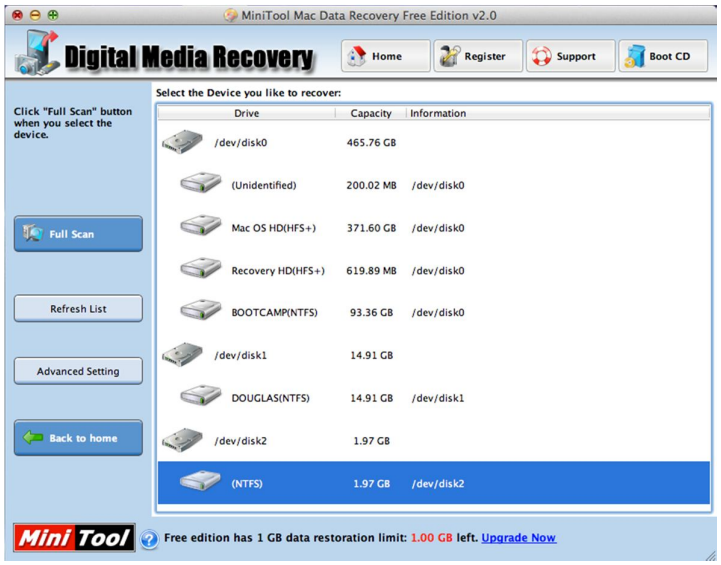


Figura 21 - Escolha da unidade a ser examinada
Fonte: Mac Data Recovery Free

Feita a escolha da unidade a ser recuperada, é só aguardar os resultados do processo de verificação (Figura 22).

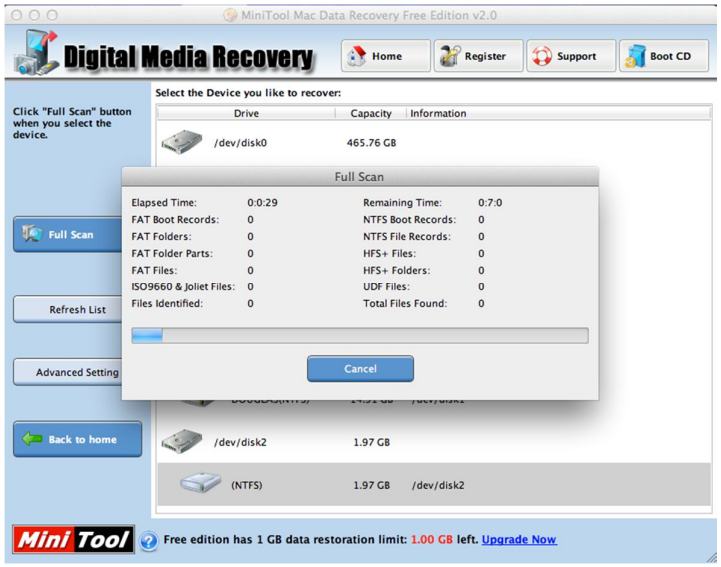


Figura 22 - Verificação de arquivos pelo Mac Data Recovery Free
Fonte: Mac Data Recovery Free

Uma vez a verificação concluída, o *software* trás em tela os arquivos recuperados para que o usuário possa salvar em outra unidade (Figura 23). Com isso é possível recuperar os dados que o *software* conseguiu buscar e recuperar em qual outra unidade diferente da unidade origem dos arquivos apagados.

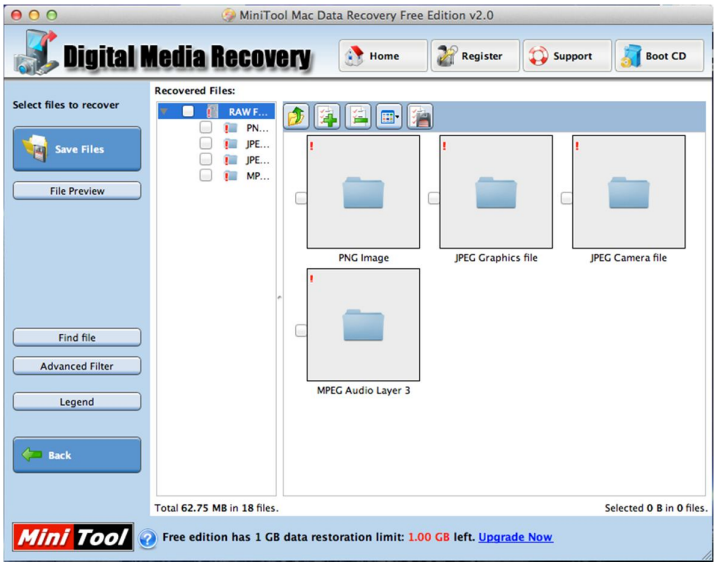


Figura 23 - Exibição dos arquivos recuperados pelo Mac Data Recovery Free
Fonte: Mac Data Recovery Free

5.2.3.2 Disk Drill

Disk Drill, recupera dados do formato de arquivos do tipo HFS/HFS+, FAT, NTFS e outros sistemas de arquivos. O *software* pode trabalhar realizando uma verificação rápida ou profunda da unidade que se deseja recuperar os arquivos. Este programa pode recuperar arquivos dos mais variados formatos e extensões, como também recuperar aplicativos específicos do Mac OS X.

Conforme ilustra a Figura 24, ao término da instalação do programa ele pergunta ao usuário se deseja visualizar um tutorial sobre como o Disk Drill funciona.

Figura 24 - Tutorial do Disk Drill
Fonte: DiskDrill

No tutorial do Disk Drill, ele aponta cada detalhe do programa e qual a sua funcionalidade de uma maneira simples, intuitiva e muito fácil de entender, porém, esse tutorial se encontra em inglês (Figura 25).

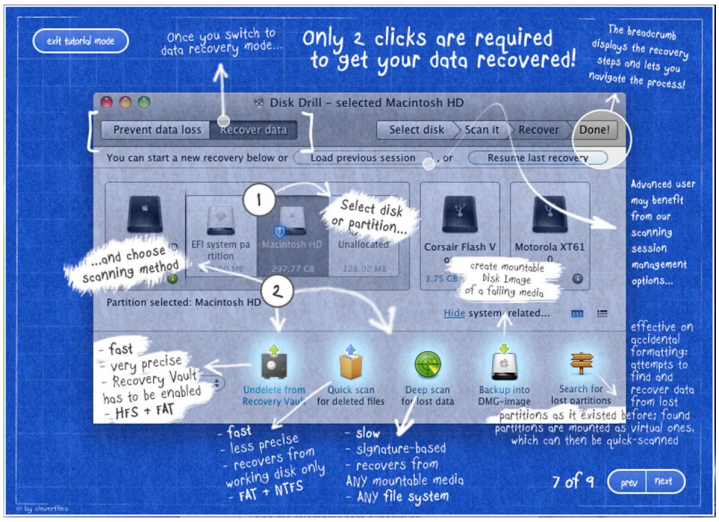


Figura 25 - Tutorial de como utilizar o Disk Drill
Fonte: DiskDrill

Na Figura 26 podemos notar que o sistema é em português, ao contrário do seu tutorial, o que facilita na hora de escolher a opção desejada, no caso a recuperação de arquivos.

Figura 26 - Tela principal da ferramenta Disk Drill
Fonte: DiskDrill

Após ter escolhido a opção de recuperar arquivos na tela principal, o *software* pede que selecione qual a unidade em que ele fará a busca por arquivos apagados (Figura 27).

Figura 27 - Escolha da unidade a ser analisada pelo Disk Drill
Fonte: DiskDrill

Logo em seguida da escolha da unidade, o programa começa a vasculhar a mesma em busca de arquivos apagados, conforme mostrado na Figura 28.

Figura 28 - Realizando a análise
Fonte: DiskDrill

Ao término da busca por arquivos apagados, ele exibe exatamente a estrutura das pastas que estavam contidas no pendrive formatado, porém, não foi capaz de recuperar todos os arquivos como ilustra a Figura 29.

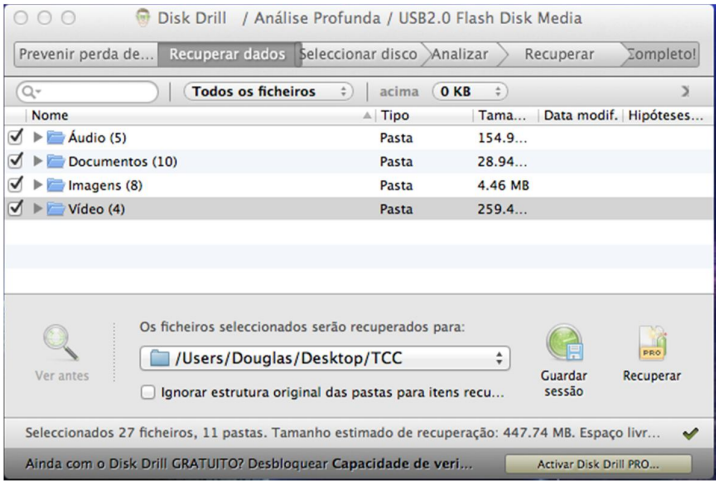


Figura 29 - Arquivos recuperados com o Disk Drill
Fonte: DiskDrill

Como a versão do *software* que utilizamos era de licença *free*, ele não oferece suporte para que possa de fato recuperar os arquivos apagados e salvá-los em outra unidade, isso é possível se adquirir a versão paga do *software*., ou seja, foi possível apenas verificar quais foram os arquivos encontrados e disponíveis para serem recuperados, porém não foi possível recuperá-los.

6 METODOLOGIA

Para Dencker (2002), o início da pesquisa é marcado pela pesquisa bibliográfica por meio de livros, monografias, teses de mestrado e/ou doutorado, e da internet. Através de trabalhos que se adequam ao tema em estudo, a pesquisa se torna mais contundente e rica, pois são diversas opiniões e teorias que entram em conflito para se obter uma ideia em comum.

A princípio foi realizada uma pesquisa e estudo abordando todo o conceito de forense computacional, sobre o que abrange essa área e onde as técnicas forenses se fazem necessárias.

Com relação à perícia forense, o trabalho relata quais os procedimentos que um perito forense deve tomar, quais são os tipos de perícias existentes, métodos para coletas de evidências e também a fase onde o perito gera o laudo, cujo qual deve conter todas as informações obtidas durante a fase de coleta de evidências.

Já em relação à recuperação de arquivos, foi realizada uma rápida pesquisa para verificar quais as ferramentas comumente utilizadas nos três sistemas operacionais, para que depois pudesse ser feita a fase de estudo de caso.

No estudo de caso, foram instalados os *softwares*, cada qual em seu sistema operacional e também foi selecionado um pendrive qualquer para a realização dos testes.

No pendrive, foram colocados alguns arquivos de formatos variados e em seguida esses arquivos foram apagados e o pendrive foi formatado, mantendo seu sistema de arquivos padrão do Windows (NTFS). Com o pendrive preparado, iniciaram-se os testes em busca dos arquivos apagados do pendrive com os *softwares* pré-selecionados nos três diferentes sistemas operacionais.

Os resultados obtidos durante a fase de testes foram tabulados com o auxílio do Excell, colocando o nome do software e a quantia de arquivos recuperados de acordo com seu tipo (música, áudio, vídeo ou texto), para que no fim do trabalho esses resultados pudessem ser comparados, revelando com qual programa e em qual sistema operacional era possível se obter o melhor percentual de restauração dos arquivos apagados.

7 RESULTADOS

Cada resultado obtido por cada software testado foi tabulado no Excell, gerando tabelas com os resultados individuais de cada software. Lembrando que o número de arquivos contidos no pendrive foram 35, divididos entre músicas, imagens, vídeos e textos.

Tabela 1 - Resultados obtidos pelo Recuva.
Fonte: Elaborado pelo autor

Software	Recuva
imagens	10
vídeos	5
músicas	7
textos	10

Tabela 2 - Resultados obtidos pelo DiskDigger.
Fonte: Elaborado pelo autor

Software	DiskDigger
imagens	10
vídeos	5
músicas	10
textos	10

Tabela 3 - Resultados obtidos pelo Foremost.
Fonte: Elaborado pelo autor

Software	Foremost
imagens	6
vídeos	2
músicas	6
textos	0

Tabela 4 - Resultados obtidos pelo Scalpel.
Fonte: Elaborado pelo autor

Software	Scalpel
imagens	3
vídeos	0
músicas	7
textos	10

Tabela 5 - Resultados obtidos pelo Mac Data Recovery Free.
Fonte: Elaborado pelo autor

Software	Mac Data Recovery Free
imagens	8
vídeos	0
músicas	10
textos	0

Tabela 6 - Resultados obtidos pelo Disk Drill.
Fonte: Elaborado pelo autor

Software	Disk Drill
imagens	8
vídeos	4
músicas	5
textos	10

Ao término de todos os testes, pôde-se montar *um quadro* comparando os resultados entre cada *software* em cada sistema operacional, exibindo especificamente o número de arquivos recuperados, conforme mostrado no Quadro 1.

Quadro 1 - Dados coletados

Software	Recuva	DiskDigger	Disk Drill	Mac Data Recovery Free	Foremost	Scalpel
imagens	10	10	8	8	6	3
videos	5	5	4	0	2	0
músicas	7	10	5	10	6	7
textos	10	10	10	0	0	10
	Windows		Mac OS X		Linux	

Fonte: Elaborado pelo autor

Com os dados devidamente coletados e tabulados, foi possível gerar um gráfico (Gráfico 1) que facilitasse a visualização da quantidade de arquivos recuperados entre as diferentes ferramentas utilizadas.

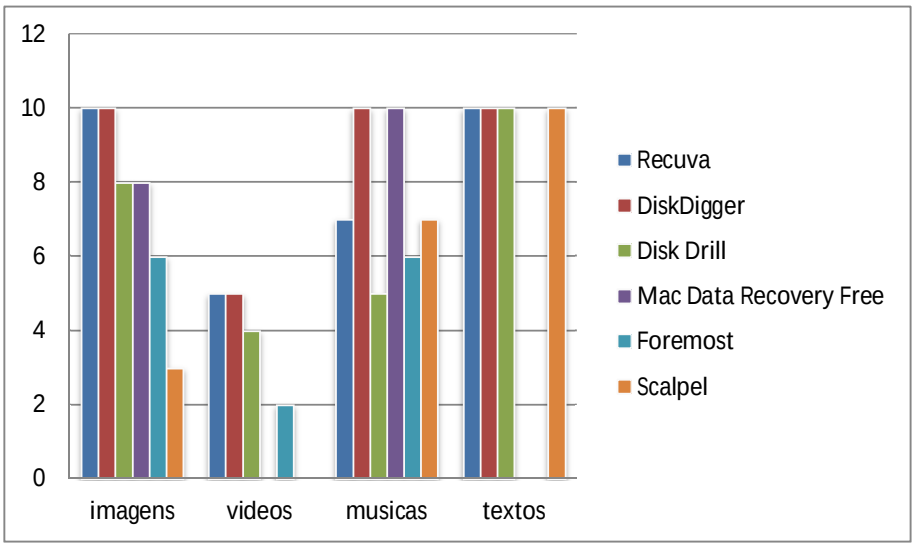


Gráfico 1 - Comparativo dos resultados entre os softwares
Fonte: Elaborado pelo autor

Portanto, percebeu-se com os resultados obtidos que a ferramenta mais eficaz para a recuperação de arquivos apagados em um sistema de arquivos do tipo NTFS é o DiskDigger, utilizado no ambiente Windows.

O fator “tempo” não foi comparado pois ele pode variar de acordo com o computador em que está sendo realizado a recuperação, quanto o tamanho dos arquivos que se deseja recuperar.

8 CONSIDERAÇÕES FINAIS

Com a facilidade na locomoção de dados através de unidades móveis como pendrives e cartões de memória, e os valores dos mesmos cada vez mais acessíveis, a probabilidade de perda de arquivos armazenados nessas mídias se torna cada vez mais comum. Pelo mesmo motivo, os crimes usando estes equipamentos também aumentam na mesma proporção.

Levando isso em consideração, muitas ferramentas são desenvolvidas com o intuito de recuperar esses arquivos, tanto para uso pessoal, em busca de restaurar arquivos perdidos acidentalmente ou mesmo dados importantes, como no uso profissional, no caso de uma perícia forense em busca de vestígios criminais.

Neste trabalho foram usadas algumas dessas ferramentas, todas em sua versão disponibilizadas gratuitamente, e feito o teste nos três sistemas operacionais mais utilizados hoje em dia, sendo Windows, Mac OS X e Linux.

Cada ferramenta, utilizada cada qual em seu sistema operacional, mostraram-se com comportamento diferente quando utilizadas para a recuperação de arquivos de um pendrive formatado, sendo que apenas uma delas mostrou-se totalmente eficaz na recuperação dos arquivos apagados, o DiskDigger. Mas o Recuva também também demonstrou ótimo desempenho, ficando na segunda posição por uma diferença de apenas três arquivos em relação ao DiskDigger.

No caso, as ferramentas utilizadas no ambiente Windows se saíram melhor do que as demais ferramentas de outros sistemas operacionais. Talvez isso se deve ao fato do pendrive utilizados nos testes ter seu sistema de arquivos em NTFS, um sistema de arquivos utilizados pelo Windows. Sendo assim, fica uma sugestão de trabalhos futuros para analisar a recuperação de arquivos levando em consideração cada sistema de arquivos utilizados e não apenas as ferramentas diferenciadas pelos sistemas operacionais.

Outro ponto que pôde ser observado é a dificuldade que se tem em remover por completo algum arquivo, tornando seu acesso ou recuperação praticamente impossível até mesmo por profissionais neste quesito, pois existem cada vez mais ferramentas sofisticadas para tal finalidade. Portanto, pode-se realizar em um estudo futuro, sendo que ao invés de mostrar as técnicas utilizadas na recuperação, mostrar o processo

realizado para evitar a recuperação dos arquivos apagados e inviabilizar seu acesso de uma vez por todas.

REFERÊNCIAS

AQUILINA, James M. **Malware e Forensics: investigating and analyzing malicious code** / James M. Aquilina, Eoghan Casey and Cameron H. Malin. Chicago: Syngress, 2003. 676p.

BARROS, Eduardo Gomes. **Elementos Básicos de Perícia Forense Computacional**, 2009. Disponível em <http://www.mpm.gov.br/mpm/servicos/assessoria-de-comunicacao/anexos/pericia_forense_computacional_conceitos.pdf> Acesso em: 10 mai. 2012.

CAMPOS, G. O que é computação forense. **Portal dos nerds**, 2011. Disponível em: < http://www.portaldosnerds.com.br/?p=445 > Acesso em: 19 mai. 2012.

CARRIER, B. *Open source digital forensics tools*. 2002. Disponível em: <http://www.digital-evidence.org/papers/opensrc_legal.pdf>. Acesso em: 10 mar. 2012.

COSTA, Daniel Moraes. **Boas práticas para perícia forense**. 2008. Disponível em: < http://bibdig.poliseducacional.com.br/document/?view=174>. Acesso em: 24 abr. 2012.

DENCKER, Ada de Freitas Maneti. **Pesquisa e interdisciplinaridade no Ensino Superior:** uma experiência no Curso de Turismo. São Paulo: Aleph, 2002. 111p.

ELEUTÉRIO, P; MACHADO, M. **Desvendando a computação forense**. Novatec. SP, 2011.

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

MARCELLA, A. J.; GRENNFIELD, R. S., (ed.). **Cyber Forensics A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes**. [s. l.] 2001.: Auerbach Publications..

MARTINS, E. **Mito ou Verdade: é preciso sobrescrever um arquivo 7 vezes para ele ser irrecuperável?** 2011. Disponível em:< http://www.tecmundo.com.br/disco-rigido/11381-mito-ou-verdade-e-preciso-sobrescrever-um-arquivo-7-vezes-para-ele-ser-irrecuperavel-.htm> Acesso em: 30 out. 2012.

MELO, Sandro. **Computação Forense com Software Livre:** Conceitos, Técnicas, Ferramentas e Estudos de Casos. 1a ed. Rio de Janeiro: Alta Books, 2009.

MILAGRE, J. **A profissão do futuro: Como ser um perito digital**. Gilberto Melo 2011. Disponível em: < http://gilbertomelo.com.br/jurisprudencias-e-

noticias/90/2865-a-profissao-do-futuro-como-ser-um-perito-digital > Acesso em: 11 mai. 2012.

NASCIMENTO, Josilene dos Santos. **Análise de Ferramentas Forenses de Recuperação de Dados**. 2010. Disponível em:<http://www.fatecjp.com.br/revista/tcc/seginf01.pdf >. Acesso em: 3 nov. 2012.

NÓBREGA, J. **Como funciona a recuperação de dados.** 2010. Disponível em: <http://www.computerworld.com.pt/2010/06/17/como-funciona-a-recuperacao-de-dados/>. Acesso em: 15 out. 2012

PAULA, Alexandre Sturion de. **Epítome da Prova Pericial no Estatuto Processual Civil Brasileiro**. Universo Jurídico, Juiz de Fora, ano XI, 06 de fev. de 2003. Disponivel em: <http://uj.novaprolink.com.br/doutrina/1266/EPITOME_DA_PROVA_PERICIAL_NO_ESTATUTO_PROCESSUAL_CIVIL_BRASILEIR >. Acesso em: 15 de ago. de 2012.

PIMENTA, Flávio. **Perícia forense computacional baseada em sistema operacional Windows XP Professional**, 2007. Disponível em: < http://pt.scribd.com/doc/53984415/103/CONCLUSAO> Acesso em: 11 mai. 2012.

SHINDER, Debra Littlejohn. **Syngress Scene of Cybercrime**: Computer Forensics Handbook. Rockland: Syngress Publishing, Inc, 2002.

THEODORO JÚNIOR, Humberto. **Curso de Direito Processual Civil**. 40ª edição, São Paulo: Forense, 2003.

TREVENZOLI, Ana Cristina. **Perícia Forense Computacional – Ataques, Identificação da Autoria, Leis e Medidas Preventivas**, 2006. Disponivel em < http://pt.scribd.com/doc/62588540/Pericia-Forense-Computacional-Ataques > Acesso em: 10 mai 2012.

VARGAS, R. Perícia Forense Computacional - Ferramentas Periciais. **Imasters**, 2007. Disponível em: <http://imasters.com.br/artigo/6485/forense/pericia_forense_computacional_ferramentas_periciais/> Acesso em: 19 mai. 2012.