Perícia Forense Computacional: Testes de Softwares, uma Vertente da Perícia Forense Computacional

Cláudia Aline Santana

Prof. Esp. Henrique Pachione Martins

Prof. Dr. Elvio Gilberto da Silva

Prof. Dr. Kelton Augusto Pontara da Costa

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

Claudia._.santana@hotmail.com

henrique.martins@usc.br

egsilva@usc.br

kelton.costa@gmail.com

Abstract. *The computational expertise forense is a relatively new area of research, however its development, is growing given the need to use that expertise in criminal activity involving digital evidence and that become increasingly common. This study aims to describe the main processes of investigation of eletronic crimes of pedophilia, for example, find photos in music files.*

Resumo. *A perícia forense computacional é uma área de pesquisa relativamente nova, no entanto é crescente seu desenvolvimento, haja vista a necessidade de utilização dessa perícia em atividades criminosas que envolvam a prova digital e que se tornam cada vez mais comuns. Essa pesquisa tem como objetivo principal descrever os processos de investigação de crimes eletrônicos através da pericia forense computacional, e identificar, ferramentas forense, para conseguir encontrar crimes de pedofilia, como, por exemplo, recuperar arquivos excluídos.*

1. Introdução

Nos últimos anos a utilização do computador se tornou fundamental na vida das pessoas. Serviços de bancos, compras online, armazenamento de arquivos, desde simples arquivos de músicas e fotos, até documentos confidenciais de empresas.

Lamentavelmente há aqueles que cometem crimes no mundo cibernético. E o número de criminosos vem crescendo junto com o crescimento da tecnologia, esses criminosos fazem o uso de pagers, telefones celulares, computadores e servidores de redes. Essas ferramentas são os meios de consumação dos crimes

computacionais. Por exemplo a Internet pode ser usada para enviar ameaças de sequestros e morte através do correio eletrônico, também pode ocorrer de criminosos guardarem arquivos ocultos em seus computadores, como arquivos de musicas que contém fotos de pedofilia. O correio eletrônico também pode servir para que esses criminosos disseminem vírus de computador ou até mesmo enviem imagens de pornografia infantil.

O aumento considerável de crimes relacionados a computadores, requer que as organizações policiais invistam em novas técnicas de abordagem para o combate aos crimes, com isso eles acabam tendo treinamentos intensivos e parcerias com entidades tecnico-científicas, a fim de ajudar a compreender como obter e utilizar as evidências eletrônicas, armazenadas nos computadores.

2. Conceitos Básicos da Computação Forense

Segundo Medeiros (2009), a perícia forense computacional é a arte de coletar e analisar evidências digitais, reconstruir dados e ataques, e rastrear invasores. Seu objetivo principal é buscar, extrair e examinar dados dos diferentes dispositivos, para que essas informações passem a ser caracterizadas como evidencias e, posteriormente, como provas legais do fato.

De acordo com Vargas (2007), a Forense Computacional é uma ára de pesquisa relativamente recente e são poucos os trabalhos sobre este assunto no Brasil. Entretanto é crescente a necessidade de desenvolvimento nesse sentido, haja visto que a utilização de computadores em atividades criminosas é cada vez mais comum.

Segundo Farmer e Venema (2006), a análise forense de um sistema envolve um ciclo de coleta de dados e processamentos das informações coletadas. Quanto mais preciosos e completos os dados, melhor e mais abrangente a avaliação pode ser. Os dados originais permanecem protegidos em um estado puro; qualquer análise deve ser realizada em uma copia dos dados do computador.

Medeiros (2009) cita que a perícia também pode ser chamada de perícia forense aplicada a informática, forense digital, e investigação eletrônica. A cada dia os dispositivos de armazenamento e acesso à Internet estão se tornando mais baratos, menores e muito mais rápidos, com mais portabilidade e com o uso amplo e difundido.

3. Locais de Crimes de Informática

Segundo Costa (2005), os crimes de informática são nomeados de crimes virtuais, isso é um erro, uma vez que não são ilusórios e deles derivam, efetivamente, danos à vida e ao patrimônio das pessoas, ao contrário de que se possa imaginar os leigos, esse crimes acontecem em um determinado tempo e espaço dando origem a um local.

De acordo com Eleutério e Machado (2011), o local do crime nada mais é do que o lugar onde uma suposta infração penal aconteceu, nesse local pode ser encontrado provas muito importantes a investigação, tentando assim esclarecer, quem foi o autor do delito, como aconteceu o delito e o que aconteceu no local do crime.

Costa (2005), também cita que de forma objetiva pode-se considerar um local de

crime como sendo qualquer área interna, externa ou mista onde tenha sido registrada uma infração penal e que preserve os sinais de seu acontecimento.

4. Atuação do Perito Forense em Locais de Crimes

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), cita 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.

Segundo Espíndula (2011), o perito deve entrevistar as pessoas que moram ou trabalham no local do crime, o perito também crime detêm todas as informações contidas no próprio laudo que emitiram, mas também toda uma série de circunstâncias que tomaram conhecimento por ocasião dos exames, análises periciais e confecção do laudo, que lhes propicia maiores condições de executarem com mais qualidade a respectiva reprodução.

5. Pedofilia

Pontual (2011), cita que a pedofilia é um transtorno de personalidade da preferência sexual que se distingue pela opção sexual por crianças, quer se trate de meninos, meninas ou de crianças de um ou do outro sexo, na maioria das vezes pré-púberes ou no início da puberdade.

Percília (2011), diz que a pedofilia não é uma doença, mas sim uma parafilia, um distúrbio psíquico que se distingue pela obsessão por métodos sexuais não aceitas pela sociedade, como o exibicionismo e o sadomasoquismo. Muitas vezes o pedófilo apresenta uma sexualidade pouco desenvolvida e teme a resistência de um parceiro em iguais condições. Sexualmente inibido, escolhe como parceiro uma pessoa vulnerável. A Figura 12 ilustra dois pedófilos se passando por criança em uma sala de bate-papo na *Internet.*

Figura 1 – Exemplo de pedófilos em sala de bate- papo na Internet. Fonte: Andrey (2011)

Segundo Seabra (1999), o abuso sexual infantil é definido como a exposição de uma criança a estímulos sexuais inadequados para sua idade, seu nível de desenvolvimento psicossocial e seu papel na família. A vítima é obrigada fisicamente ou coagida verbalmente a participar da relação sem ter, necessariamente, a competência emocional ou cognitiva para consentir ou julgar o que está acontecendo.

6. Metodologia

A proposta é descrever o processo de investigação dos crimes computacionais, em especial crimes de pedofilia por meio da perícia forense computacional, esse tipo de perícia está sendo muito utilizada para a comprovação desses crimes, pois ela pode mostrar o caminho para identificar o criminoso virtual.

Como proposta para o presente trabalho de conclusão de curso, a primeira etapa que está acontecendo é a realização de uma pesquisa bibliográfica que de acordo com Domingues; Heubel; (2003), as pesquisas devem conter assuntos gerais e particulares, podendo ser encontradas em diversas fontes de pesquisas como periódicos, livros e materiais digitais.

De acordo com Carvalho, Sartorato (2004), a pesquisa bibliográfica é o primeiro passo na construção efetiva de um protocolo de verificação, quer dizer, que depois da escolha do um assunto é indispensável fazer uma revisão bibliográfica do tema escolhido, essa pesquisa ajuda na escolha de um método mais apropriado, assim como num conhecimento das variáveis e na autenticidade da pesquisa.

A segunda etapa do trabalho de conclusão de curso será realizada em uma pesquisa de vários *softwares* de pericia forense, logo após será feita a instalação dos mesmos para assim poder fazer algumas comparações, como por exemplo, qual dentre os comparados é o mais eficiente, qual entre eles tem uma linguagem mais simples, ou seja, o mais fácil de ser utilizado. Após a pesquisa dos *softwares* e feita a comparação entre eles, será então realizado uma demonstração prática, demonstrando assim como utilizar os *softwares* pesquisados, e explicando como é feito para recuperar arquivos de pedofilia, que foram deletados, logo após será demonstrado em um gráfico quais foram as conclusões sobre os *softwares* pesquisados.

Os materiais utilizados para a elaboração das pesquisas e testes foram: Notebook com o sistema operacional Windows Seven, um computador com o sistema operacional Windows XP, e também foram utilizados os softwares para testes práticos para finalizar a pesquisa, os *softwares* foram: Camouflage a ferramenta é gratuita e é feito para trabalhar no sistema operacional Windows XP, foi utilizado também o Power Data Recovery essa ferramenta é gratuita e é feita para trabalhar em vários sistemas operacionais, o outro programa utilizado foi o undelete 360, é um *software* gratuito e trabalha em vários sistemas operacionais, também foi utilizado para testes o programa Data Recovery Studio, ele é gratuito só para teste e trabalha em vários sistemas operacionais, e por fim também foi testado o software Pc Inspector File Recovery, o programa é gratuito e trabalha em vários sistemas

operacionais.

7. Resultados Obtidos

Foi realizada em uma pesquisa de vários *softwares* de pericia forense, logo após será feita a instalação dos mesmos para assim poder fazer algumas comparações, como por exemplo, qual dentre os comparados é o mais eficiente, qual entre eles tem uma linguagem mais simples, ou seja, o mais fácil de ser utilizado. Após a pesquisa dos *softwares* e feita à comparação entre eles, será então realizado uma demonstração prática, explicando assim como utilizar os *softwares* pesquisados, e esclarecendo como é feito para recuperar arquivos de pedofilia, que foram deletados, logo após será demonstrado em um gráfico quais foram ás conclusões sobre os *softwares* pesquisados.

Os *softwares* foram: Camouflage que é uma ferramenta gratuita e é feito para trabalhar no sistema operacional Windows XP, com o camouflage é possível camuflar um arquivo dentro de outro. Foi utilizado também o Power Data Recovery essa ferramenta é gratuita e é feita para trabalhar em vários sistemas operacionais, a função do programa é recuperar arquivos excluídos. Outro programa utilizado foi o undelete 360, é um *software* gratuito e trabalha em vários sistemas operacionais, o software visa a recuperação de arquivos deletados de diversos dispositivos. Também foi utilizado para testes o programa Data Recovery Studio, a função do software é a recuperação de arquivos deletados, ele é gratuito só para teste e trabalha em vários sistemas operacionais. E por fim também foi testado o software Pc Inspector File Recovery, o papel do programa é recuperar arquivos excluídos, o programa é gratuito e trabalha em vários sistemas operacionais.

Com isso pode-se ser destacado os gráficos com os resultados satisfatórios obtidos com os testes de cada software, é importante destacar que os testes realizados foram bem sucedidos.

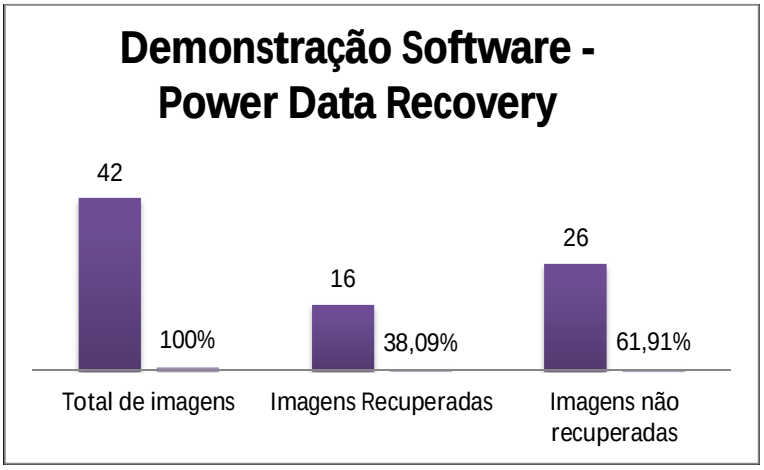

Gráfico 1 - Gráfico de demonstração de Software

O Gráfico 1, mostra a eficiência do software Power Data Recovery, em forma

de um gráfico de Colunas. Como se pode notar ele recupera os arquivos, mais não todos 38,09% dos arquivos foram recuperados com sucesso.

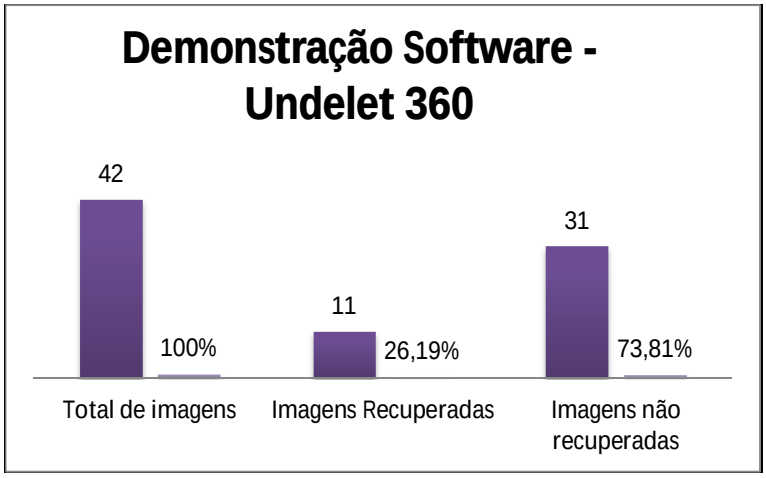

Gráfico 2 - Demonstração do Software Undelet 360

O Gráfico 2 ilustra o desempenho do Software Undelet 360, na forma de gráfico de coluna, o software recupera os arquivos deletados mais não todos, apenas 26,19% dos arquivos deletados foram recuperados com sucesso.

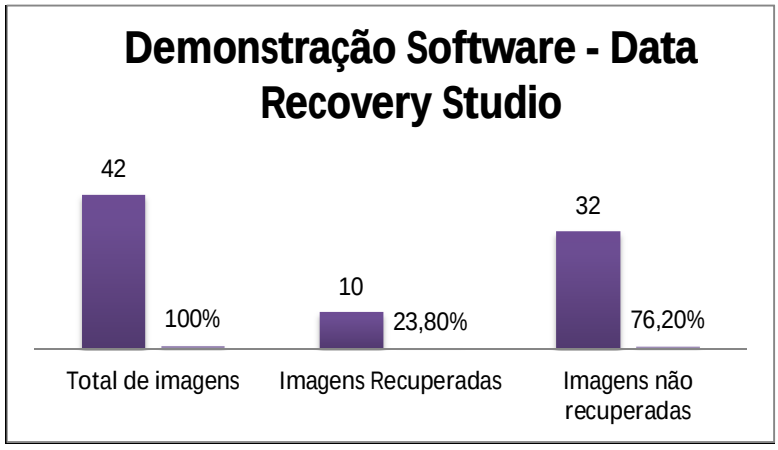

Gráfico 3 - Gráfico de demonstração de software.

O Gráfico 3 ilustra a eficiência do software Data Recovery Studio. Note que o software não recupera todos os arquivos que foram deletados, só recupera 23,80% dos arquivos excluídos.

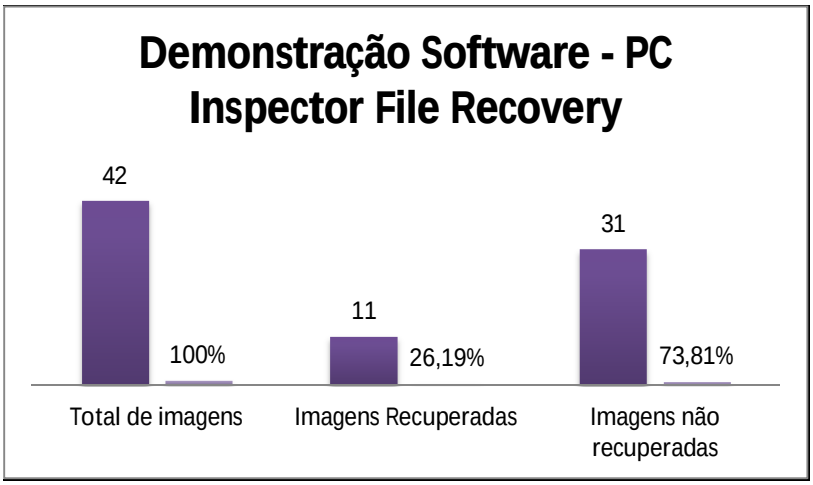

Gráfico 4 - Gráfico de demonstração de software.

O Gráfico 4 é demonstração de desempenho do software Pc Inspector File Recovery, note que não são recuperados todos os arquivos que foram deletados, foram recuperados apenas 26,19% dos arquivos excluídos.

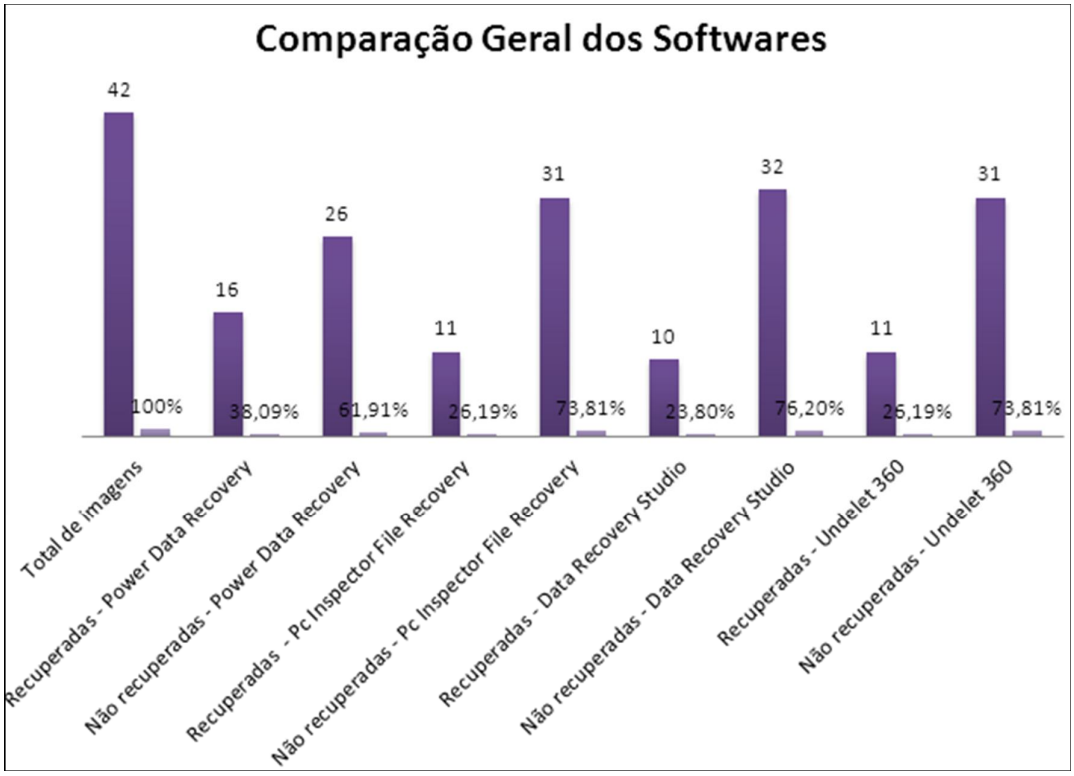

Gráfico 5 - Gráfico comparativo de todos os Softwares Analisados

Está sendo demonstrado no Gráfico 5, um comparativo Geral de todos os softwares analisados. Note que com esse comparativo pode-se definir qual software tem o melhor desempenho em relação aos outros.

8. Conclusões

A proposta que motivou essa pesquisa foi identificar e descrever o processo de investigação de crimes cibernéticos, bem como as ferramentas que podem ser utilizadas para serem feitas tais investigações, e para todos esses processos é dado o nome de perícia forense computacional. Ultimamente vem sendo muito utilizada esse tipo de perícia, para a comprovação de crimes cibernéticos, tais como a pedofilia, pois a perícia pode identificar o criminoso virtual.

Com esse trabalho foi possível identificar ótimas ferramentas para a recuperação de arquivos que foram propositalmente excluídos por um pedófilo, tais ferramentas identificadas foram testadas, para provar que é possível recuperar arquivos. Com esses testes foi identificado que é possível sim recuperar os arquivos excluídos, mas que os softwares testados não recuperam 100% dos arquivos.

Portanto pode se concluir que todos os softwares testados são eficientes, e cumpre o que prometem que é recuperar arquivos excluídos, os softwares testados para essa pesquisa, são extremamente simples, facilitando a utilização para pessoas que não tem um conhecimento técnico, os requisitos que seriam analisados em todos os softwares foram cumpridos, facilidade de uso, agilidade no processo de recuperação.

Se fizermos algumas comparações com os softwares testados, chegaremos em alguns dados: os softwares Pc Inspector File Recovery e o Undelet 360 que cada um tinha 42 arquivos destes 11 foram recuperados, ou seja 26,19 % dos arquivos foram recuperados com sucesso, com esses dados pode- se assegurar que os softwares são eficientes. Já o software Data Recovery Studio conseguiu recuperar 10 arquivos de 42, ou seja 23,80% se formos compararmos com os dois softwares anteriores, podemos afirmar que os Softwares Pc Inspector File Recovery e o Undelet 360 são mais eficientes que o Data Recovery Studio, pois consegue recuperar mais arquivos. Foi testado também o software Power Data Recovery, que entre os demais testados foi o mais eficiente, dessa maneira pode-se afirmar que foi o melhor software entre os testados, por recuperou com sucesso 16 arquivos de 42, ou seja 38,09% dos arquivos foram recuperados, nesse caso então podemos afirmar que o software Power Data Recovery, é o mais eficaz entre os testados.

Acredita-se que o objetivo da pesquisa, foi alcançado com sucesso, testando os softwares e mostrando o resultado de cada um deles, é importante frisar que a perícia forense computacional é uma ciência muito nova, e esta se desenvolvendo rapidamente para cada vez mais ser eficiente e eficaz no combate aos crimes.

Referências

ANDREY. **Pedofilia na internet**. 2011. Disponível em: <http://www.pandorgas.com/2011/04/pedofilia-na-internet.html > Acesso em: 28 de maio de 2011

CARVALHO, D; SARTORATO E; **Pesquisa bibliográfica**. 2004. Disponível em: < http://pesquisabibliografica.helenfernanda.com/2004/06/introduo.html > Acesso em: 02 de maio de 2011

COSTA, M. **Local de Crime de Informática.** 2005. Disponível em: < http://www.dpt.ba.gov.br/arquivos/downloads/provamaterial/prova%20material%205.pdf > Acesso em : 13 de setembro de 2011

DOMINGUES, M.; HEUBEL, M.T.C.D.; ABEL, I.J.; **Base metodológica para o trabalho científico para alunos iniciantes**. Bauru, SP:Edusc, 2003.

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

ESPÍNDULA, A. **Reprodução Simulada. 2011. Disponível em: <** http://www.igp.sc.gov.br/artigos11.html **>** Acesso em: 11 de outubro de 2011

FARMER, D; VENEMA, W. **Perícia Forense Computacional: Teoria e prática aplicada.** Pearson Education do Brasil, 2006

MEDEIROS, A. **Perícia forense computacional: processo de investigação em crimes cibernéticos.** Natal. RN. 2009.

MILAGRE, J**. A profissão do futuro: Como ser um perito digital**. 2011. Disponível em: < http://gilbertomelo.com.br/jurisprudencias-e-noticias/90/2865-a-profissao-do-futuro-como-ser-um-perito-digital > Acesso em: 11 de outubro de 2011

PERCÍLIA, E. **O que é Pedofilia**. 2011. Disponível em: < http://www.oncdp.com.br/site/pedofilia/conceitos/50-o-que-e-pedofilia > Acesso em 16 de novembro de 2011.

PONTUAL, H. D. **O que é Pedofilia.** 2011. Disponível em: < http://www.oncdp.com.br/site/pedofilia/conceitos/50-o-que-e-pedofilia > Acesso em 16 de novembro de 2011.

SEABRA, A. S. **Abuso sexual na infância.** 1999. Disponível em: < http://www.existencialismo.org.br/jornalexistencial/andreseabraabusosexual.htm > Acesso em 16 de novembro de 2011.

VARGAS, R. **Perícia Forense Computacional e metodologias para obtenção de evidências.** 2007. Disponível em: < http://imasters.com.br/artigo/6225 > Acesso em 03 de maio de 2011