Capítulo 1

Antiforense Digital: conceitos, técnicas, ferramentas e estudos de caso

Evandro Della Vecchia[†*], Daniel Weber[‡], Avelino Zorzo[†]

[†] Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
{evandro.pereira, avelino.zorzo}@pucrs.br

[*] Instituto-Geral de Perícias (IGP-RS)
evandro-pereira@igp.rs.gov.br

[‡] Universidade Federal do Rio Grande do Sul (UFRGS)
daniel.weber@ufrgs.br

Abstract

Digital anti-forensic can be defined as a set of hiding and removal information methods in storage devices to protect people and institutions privacy. Several papers and police reports often describe situations where sensitive information or images are exposed in public nets, damaging people's reputation or causing losses to institutions. This chapter presents some anti-forensic techniques and resources to protect sensitive data, not to hide proofs or evidences of unlawful acts. The study was conducted through bibliographic review and tests in controlled environments. Our findings indicate that available resources allow, without major investments, an adequate level of protection.

Resumo

A antiforense digital pode ser definida como um conjunto de métodos de ocultação e remoção de informações em dispositivos de armazenamento, para proteger a privacidade de pessoas e empresas. Artigos científicos e relatos policiais registram com freqüência situações onde informações ou imagens sigilosas são divulgadas em redes públicas, prejudicando a reputação de pessoas ou causando perdas financeiras a instituições. Este capítulo apresenta técnicas e recursos antiforense para a proteção de informações sensíveis, não para ocultar provas e evidências de atos ilícitos. O trabalho foi desenvolvido através de consultas bibliográficas e testes em ambientes controlados. As conclusões indicam que os recursos disponíveis possibilitam, sem grandes investimentos, um nível de proteção adequado.

1.1 Introdução

A grande migração de informações para o ambiente digital aumentou o potencial de exposição de dados sensíveis, pessoais ou corporativos, aumentando a possibilidade de seu acesso indevido. Os mesmos recursos tecnológicos desenvolvidos para facilitar a vida de pessoas e empresas de boa índole colaboram para fragilizar a privacidade e podem ser explorados por pessoas de má fé. A busca por informações para obter vantagens pessoais (indivíduos) ou competitivas (empresas) nem sempre é pautada pela legalidade e ética. Alguns dos acontecimentos que motivaram uma grande preocupação com a segurança da informação foram os atentados de 11 de setembro, nos Estados Unidos da América, fazendo com que o governo americano investisse pesado no aparelhamento com instrumentos legais para investigar a vida dos cidadãos, em nome da segurança coletiva. Muitas vezes, estes instrumentos possibilitam a investigação de maneira discutível, por exemplo, em junho de 2013 ocorreu o vazamento de informações relacionadas à espionagem americana que ocorria em diversos países, incluindo o Brasil.

As técnicas que habilitam a invasão de privacidade pela recuperação de dados registrados em mídias de armazenamento são chamadas de **forense digital** [US-CERT 2008] e, em contrapartida, a **antiforense digital** define métodos de remoção, ocultação e subversão de evidências com o objetivo de mitigar os resultados de análises forenses [Garfinkel 2007].

Problemas decorrentes do uso de dados não protegidos de forma eficiente podem ter diversas origens. A queda de preço e conseqüente popularização de *notebooks*, *tablets* e outros dispositivos móveis viabilizaram o seu uso por pessoas que vêem nestes equipamentos apenas uma ferramenta de trabalho adicional, e que não têm discernimento para avaliar o seu potencial de expor informações privadas. Uma pesquisa realizada pelo Ponemon Institute, em maio de 2008, indica o registro de roubo ou perda de mais de 637.000 *notebooks* no período de um ano, exclusivamente nos aeroportos dos Estados Unidos [Shah 2008] e, conseqüentemente, os dados pessoais ou empresariais registrados nas unidades de disco destes equipamentos ficaram expostos.

A criatividade das pessoas com propósitos maliciosos não tem limites. Assim como *notebooks* e eventualmente outros tipos de computadores, uma série de outros recursos tecnológicos tem o potencial de vazar informações privadas, por descuido ou por má intenção. O conteúdo de equipamentos com o acesso lógico restrito por senhas pode ser exposto facilmente, por exemplo, utilizando-se a inicialização por CDs de *boot* para burlar os mecanismos de proteção, ou através do espelhamento do conteúdo de um disco para ser analisado em um outro equipamento [Ulbrich e Valle 2004]. Mídias de armazenamento de grande capacidade ou de tamanho reduzido (*pendrives*, *memory sticks* e dispositivos semelhantes) são adequadas para copiar e transportar arquivos sem muito alarde.

É comum verificar em meios de comunicação notícias relacionadas a situações onde informações ou imagens sigilosas são divulgadas em redes públicas, segredos corporativos são compartilhados com a concorrência e o acesso a informações financeiras privadas facilita negócios muito lucrativos. Um exemplo de vazamento de dados sensíveis ocorrido no Brasil e que resultou em um movimento para aprovação de

lei que trata de crimes cibernéticos (Lei 12737/2012 – [Presidência 2012]) foi o "Caso Carolina Dieckmann". Na verdade, muitos outros casos semelhantes ou com maiores consequências vem ocorrendo há mais tempo, como um caso ocorrido em 2005, relatado em [G1 2013].

Uma regra fundamental dos projetistas de dispositivos de armazenamento é que os dados devem ser protegidos. Uma unidade de disco, principal dispositivo de armazenamento em computadores pessoais, é projetada para evitar perdas e danos acidentais aos dados. Técnicas como um diretório para arquivos reciclados ("lixeira") e comandos *unerase* ou *undelete* estão disponíveis na maioria dos sistemas operacionais para prevenir a perda indesejada de informações. A exclusão de ponteiros (índices) é um padrão para agilizar a exclusão e possibilitar a recuperação de um arquivo em disco, e *drivers* utilizam técnicas de detecção de erros para impedir que uma leitura resulte em valores incorretos [Hughes et al. 2009].

Todo este esforço é realizado com base no pressuposto de que excluir informações de um computador pode ser um evento não usual, entretanto a eficiência destas medidas para proteger e agilizar o acesso de usuários aos dados pode transformar-se em vulnerabilidade, quando exploradas por pessoas não autorizadas.

Quando um equipamento é roubado, perdido ou descartado, os dados continuam armazenados nos discos. Mesmo que um usuário tenha o cuidado de excluir os arquivos com o comando *delete* [James 2006], os dados permanecem no equipamento e podem ser recuperados a partir de diretórios de reciclados ("lixeira") ou utilizando programas específicos desenvolvidos com esta finalidade. O mesmo ocorre com o comando *format*, utilizado para preparar logicamente um disco para o uso, mas que não, necessariamente, realiza destruição alguma de dados.

As técnicas de forense digital utilizam exaustivamente recursos de recuperação de arquivos, fragmentos de arquivos ou fragmentos de texto que o proprietário do equipamento julgava como excluídos. Desta forma, indícios e evidências digitais podem ser obtidos para constituir prova técnica de delitos cometidos. Entretanto, as mesmas técnicas podem ser usadas para atividades criminosas, expondo informações de estratégias corporativas ou dados que possam prejudicar um indivíduo [Garfinkel 2007]. Ou seja, as mesmas técnicas e conhecimentos podem ser utilizados tanto para investigação como para o acesso indevido de dados. O que diferencia um do outro é a ética dos profissionais da área de forense digital.

A necessidade de segurança e privacidade exige procedimentos de exclusão (destruição) confiáveis que possam impedir o acesso de dados em discos descartados. A "esterilização" pode endereçar diferentes níveis dependendo das aplicações (por exemplo, a senha para acesso a um jogo *online* de um indivíduo não tem a mesma importância que o controle de acesso a uma conta bancária), assim mesmo usuários domésticos devem ter acesso a ferramentas que protejam a sua privacidade. Em [Garfinkel e Shelat 2003] são apresentados dados que demonstram que muitas pessoas vendem (ou doam) seus computadores (ou apenas o disco rígido) sem nenhum, ou com pouco cuidado de eliminação de dados sensíveis. Neste artigo, dois estudantes compraram 158 discos usados pela Internet, sendo que apenas 129 funcionaram. Destes, apenas 12 foram "esterilizados" de forma adequada e do restante, foi possível recuperar mais de 5.000 números de cartão de crédito, diversos registros de dados financeiros e

pessoais, inúmeros registros de consultas médicas e *gigabytes* de e-mails pessoais e pornografia.

Desta forma, o objetivo deste capítulo é mostrar um estudo sobre técnicas e recursos antiforense aplicáveis em ambientes privados ou corporativos para a proteção de informações sensíveis. Para atingir este objetivo, primeiramente serão abordados conceitos de forense digital (Seção 1.2), após serão abordados conceitos sobre antiforense digital (Seção 1.3). Na Seção 1.4 serão mostradas técnicas aplicadas em antiforense e exemplos de ferramentas. Para ilustrar os conceitos e técnicas mencionados, a Seção 1.5 mostra estudos de caso, a maioria sendo casos reais adaptados para evitar a identificação dos envolvidos. Por fim, a Seção 1.6 aborda as considerações finais.

1.2 Forense Digital

Forense Digital pode ser conceituado como um conjunto de técnicas e procedimentos que utilizam conhecimento científico para coletar, analisar e apresentar evidências que possam ser utilizadas em um tribunal [Nolan et al. 2005]. O termo forense significa "pertinente à lei". É essencialmente a busca minuciosa de informações relativas a eventos passados específicos para uma investigação criminal, embora Forense Digital (Perícia Digital, além de outros nomes) seja utilizada também em investigações particulares, antes mesmo de se pensar em acionar a polícia ou a justiça.

Diversos crimes são solucionados através da identificação de impressões digitais, pegadas, sangue, cabelo ou amostras de fibras. Análises balísticas são utilizadas para determinar a posição de um atirador, além da arma de fogo utilizada, e resíduos químicos encontrados em uma peça de roupa podem identificar o criminoso. A atividade do perito muitas vezes é fundamental para a coleta de indícios que permitam a prisão e condenação de criminosos, pois as evidências físicas são utilizadas para a reconstrução das circunstâncias em que um crime ocorreu, principalmente quando não houve testemunhas [Dillon 1999]. O exercício da Ciência Forense está sustentado por diferentes áreas do conhecimento, como: Biologia, Química, Psiquiatria, Medicina, Farmacologia, Antropologia, Patologia e, nos últimos anos, na Computação [Eckert 1997].

A prática da Forense Digital surgiu na década de 1980, em resposta aos primeiros casos de vírus de computador que se espalhavam por redes de comunicações [Slade 2004]. Nos anos seguintes, evoluiu para a investigação de casos de distribuição de material contendo pedofilia e posteriormente no combate a crimes cibernéticos, quando a popularização do acesso à Internet e o uso de computador pessoal (além de outros dispositivos eletrônicos) como ferramenta de trabalho e meio de armazenamento criou novas oportunidades para atividades ilegais [Hannan 2004].

Ainda assim a Forense Digital pode ser considerada uma disciplina recente e a consistência de padrões entre a indústria e os tribunais ainda é incipiente. Desta forma, a área ainda busca o reconhecimento como uma atividade científica formal. Uma definição de Forense Digital poderia ser: "Disciplina que combina elementos legais e Ciência da Computação para coletar e analisar dados de sistemas computacionais, redes, comunicações sem fio e dispositivos de armazenamento de modo que possam constituir evidências admissíveis em um tribunal" [US-CERT 2008].

A Forense Digital ganhou notoriedade nos últimos anos devido a várias agências de investigação, oficiais ou privadas, esclarecerem delitos nos quais o computador foi utilizado para a prática de crime ou em situações onde a tecnologia atuou como meio auxiliar para atividades ilegais [Steel 2006].

O ciclo dos procedimentos forenses é ilustrado na Figura 1.1. O processo forense transforma a mídia em evidência, necessária para a aplicação da lei ou para uso interno das empresas. A primeira transformação ocorre quando os dados coletados são examinados e as informações extraídas da mídia são analisadas por ferramentas forenses. A segunda, quando a análise dos dados cria informações que, processadas, resultam em evidências [Kent et al. 2006].

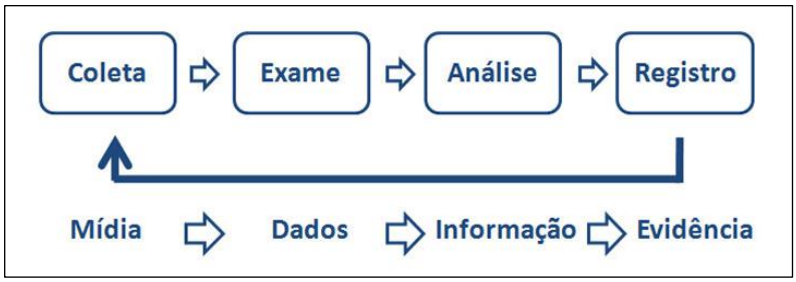


Figura 1.1. Etapas do processo de investigação forense [Kent et al. 2006] (Tradução)

Diferente das provas físicas dos crimes convencionais, comprovações encontradas nas mídias magnéticas são digitais e podem existir de diversas formas. Arquivos, fragmentos de *logs* e outros indícios residentes em uma mídia podem ser relacionados para criar uma evidência que indique a ocorrência de um crime ou auxilie a identificação de um criminoso.

Um dos fatores mais importantes na Forense Digital é a proteção das provas obtidas [Brezinski e Killalea 2002]. Uma das atribuições do perito é garantir que o equipamento sob análise e os processos de coleta sejam administrados com cuidado para garantir que [Lopes et al. 2006], [Mikasey et al. 2001]:

a) Nenhuma evidência seja danificada, destruída ou comprometida pelos procedimentos utilizados para investigar o equipamento;

b) O processo não crie nenhuma condição que possa inviabilizar uma verificação futura;

c) Seja estabelecida (e mantida) uma cadeia de custódia[1];

d) Caso o equipamento esteja em uso (*Live Forensics*), o tempo de intervenção seja o menor possível;

e) Qualquer informação obtida, não pertinente ao escopo da investigação, seja tratada dentro dos limites éticos e legais, e não seja divulgada;

f) Todo o processo deve ser documentado para permitir a sua reprodução.

A Forense Digital pode ser classificada em dois tipos básicos: *Live Forensics* e *Post-Mortem Forensics* [Carvey 2009]. A *Live Forensics* especifica procedimentos de

[1] Cadeia de custódia: Procedimento para assegurar validade legal das atividades enquanto uma evidência estiver sob perícia [Lopes et al. 2006].

investigação não intrusivos, em equipamentos em uso, e analisa informações persistentes (gravadas em dispositivos de armazenamento) e voláteis (com tempo de vida restrito). A *Post-Mortem Forensics* implica na apreensão de equipamentos para análise em laboratório e não inclui a análise de dados voláteis, como os gravados em memória RAM, que são perdidos quando há a falta de energia [Sutherland et al. 2008] [US-CERT 2008].

A análise *Post-Mortem* inclui procedimentos triviais de busca por documentos, *logs*, imagens (fotografias), identificação de data e hora de arquivos, análise de trilhas de uso do computador, recuperação de dados excluídos, entre outros [Carvey 2009].

Um resumo das etapas mostradas na Figura 1, utilizando a nomenclatura adotada por [Kent et al. 2006], será mostrado a seguir, com o enfoque para análise *Post Mortem*, porém pode ser adotada também para *Live Forensics*, com poucas modificações.

Coleta

Nesta etapa há uma mescla de investigação e perícia, pois engloba desde a identificação do material a ser analisado até a cópia integral dos dados. Geralmente o perito não está presente na busca e apreensão do material questionado (esfera criminal), ou em uma empresa em que haja suspeita de algum incidente e deseja-se recolher equipamentos/mídias para serem analisadas. Em muitos casos, o perito recebe o material a ser analisado e não tem conhecimento da cena do crime ou do incidente (a não ser quando se trata de uma análise *Live Forensics*).

Diante disto, é importante que quem realizar a busca e apreensão, tenha conhecimento de equipamentos e mídias de informática, pois atualmente não são apenas os computadores que possuem informação em formato digital. Existem diversos modelos, formatos e tamanhos de equipamentos e mídias (Figura 1.2) e o desconhecimento destes pode resultar em uma busca e apreensão ineficientes (incompletas). É importante registrar com fotografias (ou vídeo), colocar etiquetas de identificação, lacrar o material apreendido e gerar um relatório, reforçando a ideia de uma forte cadeia de custódia. Após, o material deve ser encaminhado ao Instituto/Departamento de Perícia, no caso da esfera criminal, ou aos profissionais designados, no caso de uma perícia particular.

Figura 1.2. Mídias de armazenamento em diversos formatos (Fonte: http://www.insoonia.com/diferentes-modelos-de-pen-drive/)

Seguindo as melhores práticas, diante das mídias o perito deve realizar uma cópia integral das mídias, conhecida também como: cópia *bit a bit*, *raw copy*, duplicação forense, entre outros. Trata-se de uma cópia de todos os *bits* da mídia, inclusive a área não alocada pelo sistema de arquivos. Este tipo de cópia é recomendado

para que seja possível recuperar dados excluídos na cópia, sem nenhum procedimento realizado na mídia questionada, evitando assim a violação da integridade. Ainda para evitar qualquer alteração na mídia questionada, deve-se protegê-la contra escrita, seja através de *hardware* específico ou através de *software*. Um exemplo de *hardware* com este fim é o Tableau Forensic FireWire Bridge, mostrado na Figura 1.3. Com este tipo de equipamento colocado entre a mídia questionada e o computador do perito, há a garantia de apenas leitura.

Figura 1.3. Equipamento de proteção contra escrita Tableau Forensic FireWire Bridge

Através de *software*, a proteção contra escrita pode ocorrer com a utilização de, por exemplo, uma distribuição do sistema operacional Linux conFigurada por padrão para não montar mídias e, quando montar, o perito deve ter o cuidado de montá-la apenas como leitura. Uma das distribuições mais utilizadas e completa para *pentest* e forense digital no momento é a BackTrack. Como pode ser visto na Figura 1.4, esta distribuição possui menus específicos para cada finalidade e em cada uma possui diversas ferramentas.

Figura 1.4. Distribuição forense BackTrack (Fonte: http://www.backtrack-linux.org/screenshots/)

Existem *softwares* que simplesmente habilitam/desabilitam um barramento para escrita. Por exemplo, se uma mídia utilizar uma conexão USB, pode-se desabilitar este barramento para escrita. Na plataforma Windows, pode-se realizar tal controle através do Editor do Registro (RegEdit.exe), da seguinte maneira: adiciona-se uma chave denominada *StorageDevicePolicies* em HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control, nesta chave adiciona-se uma DWord com o nome *WriteProtect*. Para proteger contra escrita basta definir o valor de WriteProtect para 1 (Figura 1.5) e quando desejar-se habilitar a escrita, deve-se definir o valor como 0. Para facilitar existem interfaces gráficas que realizam a operação mencionada de forma simples, com uma interface gráfica, como por exemplo, o Thumbscrew (Figura 1.6).

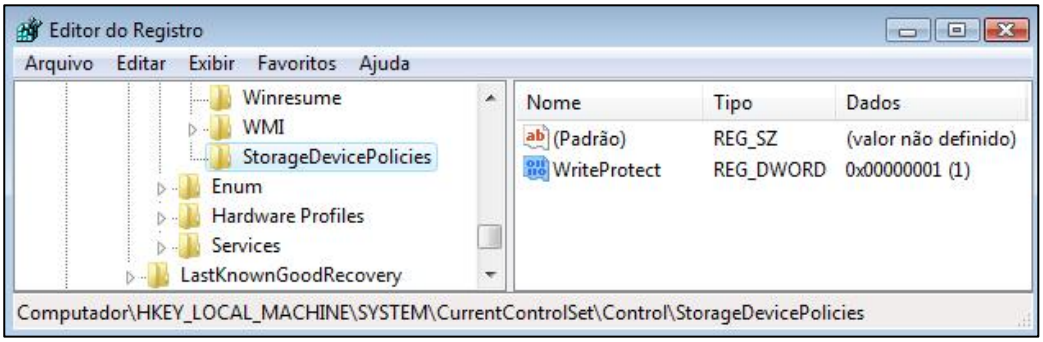


Figura 1.5. Proteção contra escrita no barramento USB – Plataforma Windows

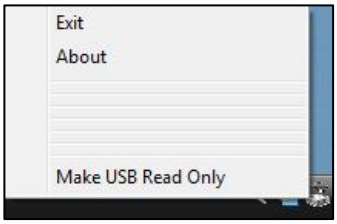


Figura 1.6. Utilização do software Thumbscrew

Para a duplicação forense, o *software* mais conhecido é o *dd*, originário no Linux, mas existente também para a plataforma Windows. Algumas variantes surgiram a partir do *dd*, para facilitar a visualização do andamento da cópia e outras opções que o *dd* não possui. Um exemplo é o *dcfldd*, mostrado na Figura 1.7. Na Figura é possível identificar os parâmetros mínimos necessários para realizar a cópia integral de um *pendrive* com capacidade de 2GiB[2] (if=/dev/sdc), para um arquivo denominado pen2Gib.dd (of=/media/KINGSTON-8G/pen2GiB.dd). A Figura 1.8 mostra o fim da cópia.

[2] GibiByte (GiB) é uma unidade de medida para armazenamento eletrônico de informação, estabelecida pela Comissão Eletrotécnica Internacional (IEC) para designar 2^{30} bytes de informação ou de armazenamento computacional (texto retirado de http://pt.wikipedia.org/wiki/Gibibyte). O GigaByte se refere a 10^9 bytes. Portanto a unidade adequada é GiB, embora os fabricantes ainda não tenham adotado tal nomenclatura. O mesmo ocorre para KiB, MiB, etc.

Figura 1.7. Início da cópia realizada com o dcfldd – Linux

Figura 1.8. Fim da cópia realizada com o dcfldd – Linux

Para verificar a integridade após a cópia, pode-se aplicar um algoritmo de *hash*, como por exemplo, o SHA-1, na mídia questionada e na cópia *bit a bit* gerada (Figura 1.9). No exemplo, a integridade foi mantida (o mesmo *hash* foi gerado).

Figura 1.9. Algoritmo SHA-1 aplicado na mídia questionada e na cópia gerada

Exame

Após realizada a etapa de coleta dos dados, procedimentos de exame podem ser aplicados. Procedimentos comuns nesta etapa englobam: aplicação de filtros, busca de por palavras-chave, recuperação de dados excluídos, entre outros.

Para mostrar tais procedimentos, será utilizada o *software* Autopsy [AUTOPSY 2013], que possui a versão 3 para a plataforma Windows e a versão 2 para Linux e Mac OS X. Uma *cópia bit a bit* utilizada em aulas da disciplina Perícia Digital na PUCRS (copia.dd), criada especificamente para simular um possível crime de estelionato, será examinada no ambiente Windows. Também será mostrado como montar uma cópia integral de um *pendrive* com capacidade de 2GiB no Linux.

Uma das maiores dificuldades para os iniciantes em forense digital ao utilizar o comando *mount* no Linux para montar uma cópia *bia a bit* é saber utilizar corretamente os parâmetros: *loop e offset*. *Loop* deve ser utilizado por se tratar de um arquivo *raw* (cópia integral) e não de uma mídia diretamente e *offset* deve ser utilizado para especificar onde começa a partição, pois *mount* não reconhece a tabela de partições posicionada no começo do disco.

Primeiramente, o usuário deve saber as informações da sua cópia (realizada na etapa de coleta). Uma opção é utilizar o comando *sfdisk*, conforme mostrado na Figura 1.10.

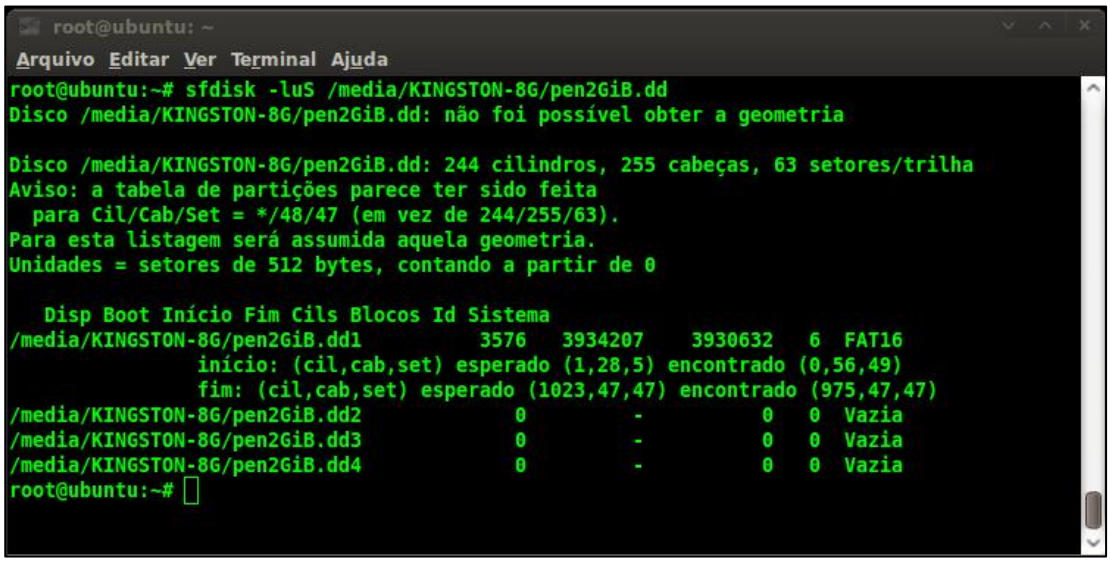


Figura 1.10. Aplicação do comando sfdisk sobre a cópia integral pen2GiB.dd

Conforme mostra a Figura, dos quatro espaços reservados para endereçamento, apenas um foi utilizado, com início no setor 3576 e sistema de arquivos FAT16. Para utilizar o comando *mount*, deve-se primeiro calcular 3576 * 512 (setor de início * tamanho do setor em bytes), obtendo-se um total de 1.830.912. Outros parâmetros importantes são os de não execução e somente leitura, para garantir que não haverá modificação no arquivo *raw*. A Figura 1.11 mostra a execução de *mount* realizada com sucesso e após a navegação e listagem de conteúdo de pen2GiB.dd.

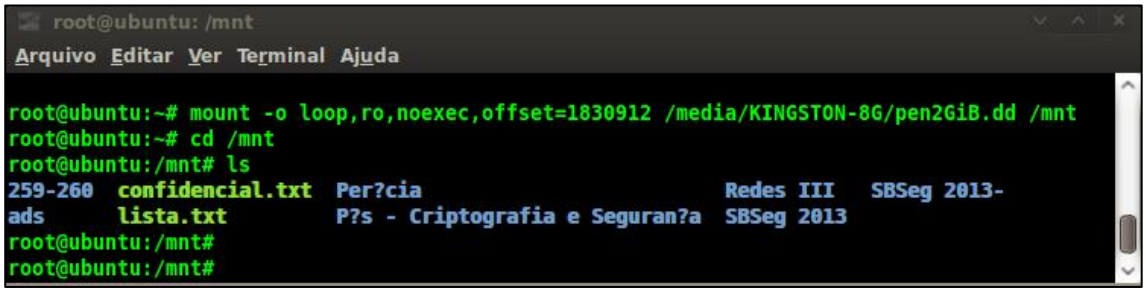


Figura 1.11. Conteúdo de pen2GiB.dd visível pelo sistema de arquivos

O *software* Autopsy (versão utilizada nos experimentos a seguir: 3.0.6) possui um ambiente gráfico, com diversos filtros prontos e possibilita a busca por palavras-chave. Um dos filtros é o de documentos recentes, que mostra doze documentos recentes na Figura 1.12, sendo que o selecionado é um atalho que aponta para o arquivo Areia.bmp (papel de parede do Windows XP). Outro exemplo de filtro é o das buscas realizadas em motores de busca, muito útil para saber o que o suspeito pesquisou na Internet, que mostra na Figura 1.13 pesquisas por "acrobat reader download", "camouflage download", entre outros.

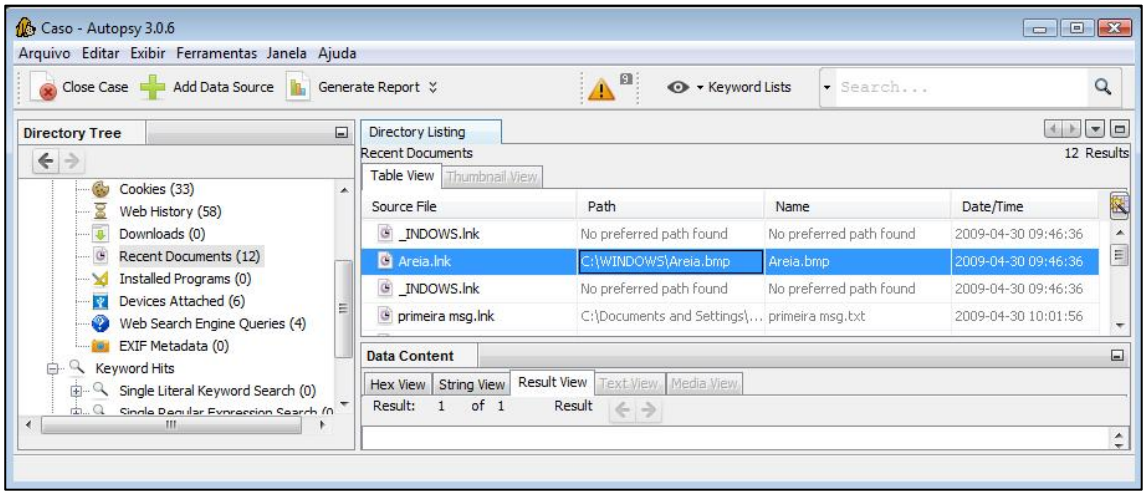


Figura 1.12. Autopsy 3.0.6: Filtro por documentos recentes

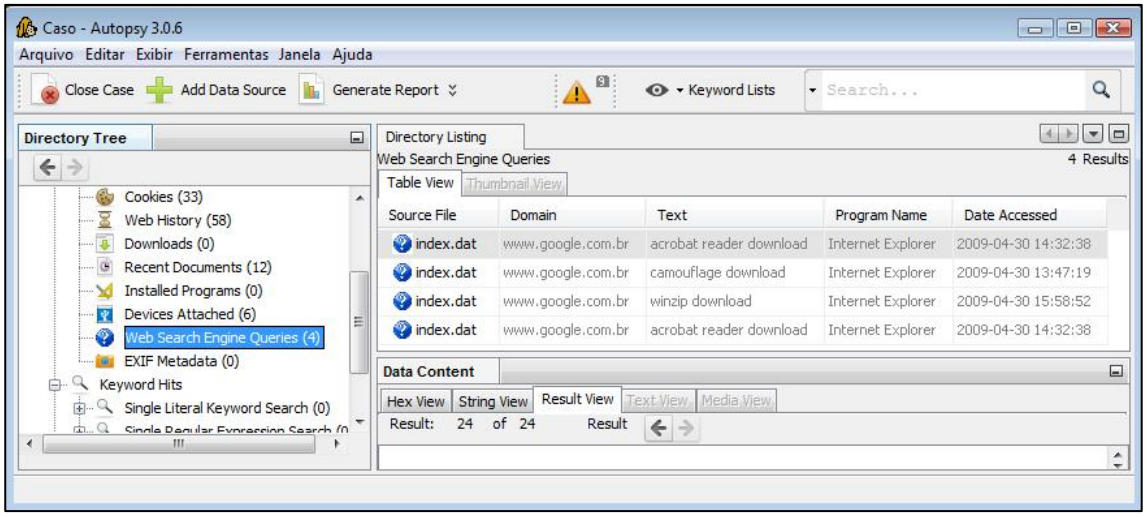


Figura 1.13. Autopsy 3.0.6: Filtro por buscas em motores de busca

Com relação à busca por palavras-chave, o perito pode criar uma lista baseada ao caso investigado (nome do suspeito, da vítima, endereço, telefone, etc.) e em sua experiência (palavras utilizadas em casos semelhantes já analisados pelo perito). A Figura 1.14 mostra uma lista com duas palavras-chave: “Tiburcio” e “falso”. A primeira, por ser o nome do investigado e a segunda por se tratar de estelionato e pela experiência do perito. O resultado da busca por estas duas palavras-chave é mostrado na Figura 1.15.

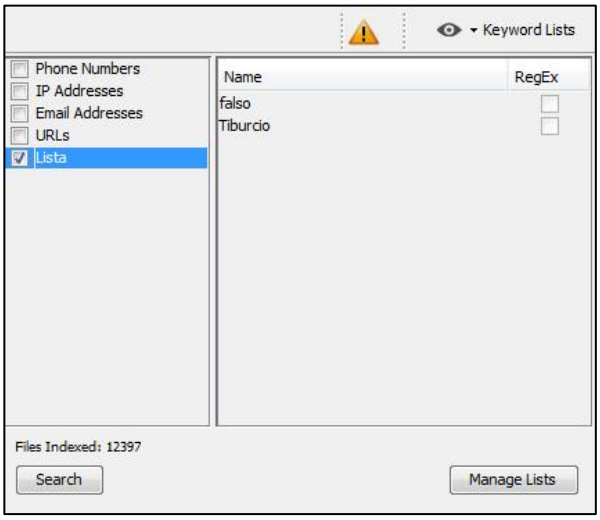


Figura 1.14. Autopsy 3.0.6: Busca por palavras-chave

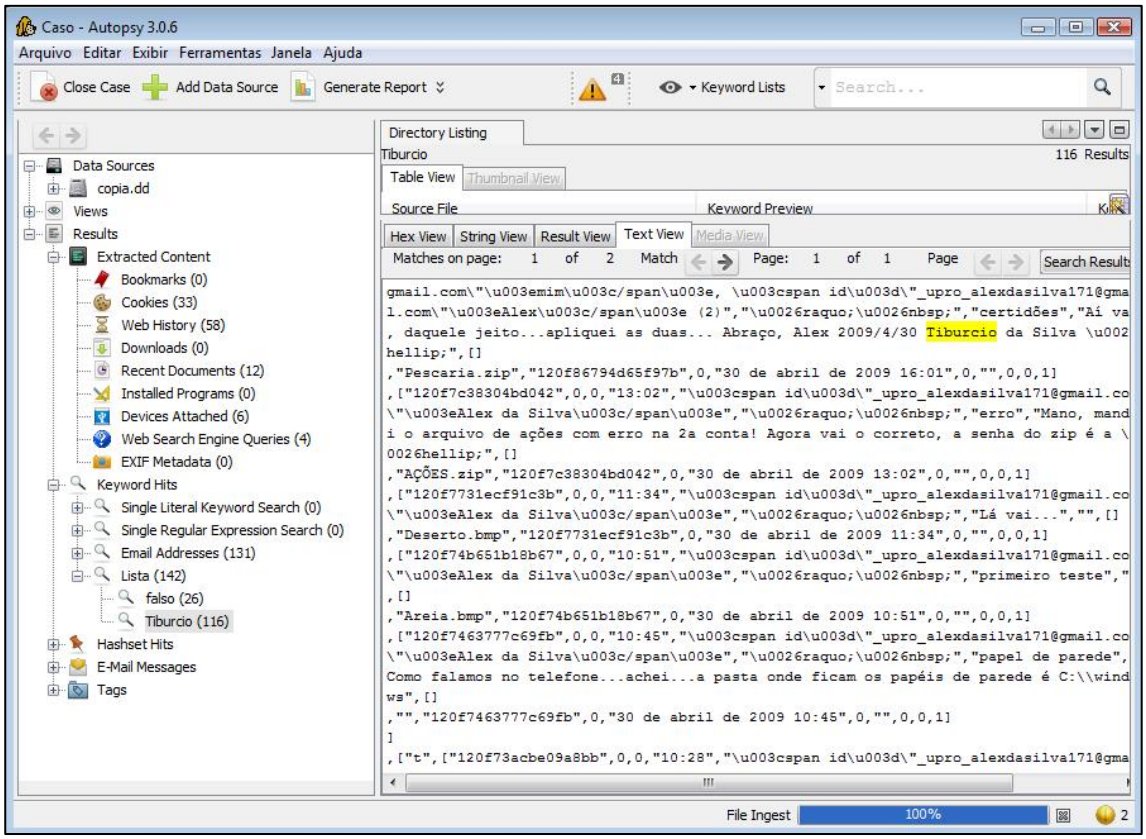


Figura 1.15. Autopsy 3.0.6: Resultado da busca por palavras-chave, com um arquivo contendo uma mensagem eletrônica

Análise

Após aplicação dos procedimentos da fase de exame, o perito deve analisar o que foi retornado. Trata-se de uma etapa manual, difícil de ser automatizada por *scripts* ou ferramentas, pois o perito deve verificar se o arquivo, fragmento de arquivo, trecho de texto e outros, são realmente evidências para o caso em investigação.

Às vezes torna-se necessário a busca de ferramentas para abrir um arquivo encontrado, seja porque ele possui um formato desconhecido ou porque o perito não possui uma ferramenta instalada que consiga visualizá-lo.

Outra situação que exige um trabalho maior é quando um arquivo aparentemente importante não pode ser visualizado diretamente por possuir algum mecanismo de proteção, como por exemplo, senha. Novamente é necessária a busca de uma ferramenta que tente descobrir tal senha ou ignorá-la (quando o mecanismo de proteção não foi bem elaborado).

Registro

O Laudo Pericial é o documento que registra todos os procedimentos realizados e o que foi encontrado como resultado. É a constituição da prova técnica, utilizada por juízes para contribuir no seu convencimento a favor ou contra o réu.

Alguns pontos importantes de um Laudo Pericial são:

- Dados de protocolo: Dados que identifiquem o caso, tais como: ocorrência e inquérito policial (esfera criminal), número do processo (se o solicitante for o juiz), protocolo e/ou requisição (controle da perícia), entre outros;
- Introdução: descreve o caso investigado e define o escopo da perícia;
- Metodologia: define como foi realizada a cópia, que filtros e buscas foram utilizadas, como as evidências foram impressas e/ou copiadas para uma mídia (anexo), entre outros;
- Resultados: mostra o que foi encontrado, quando há muito conteúdo sugere-se explicar o que foi encontrado e colocar os dados em anexo;
- Conclusões: quando for possível realizar uma conclusão, esta deve ser realizada após os resultados;
- Resposta aos Quesitos: podem ser realizadas nas conclusões, mas se não houver, pode haver um item apenas para os quesitos e suas respostas;
- Considerações Finais: informações sobre o que é devolvido após o término da perícia, se há mídias em anexo (e seus *hashes*), entre outras;
- Assinatura do(s) perito(s): devem estar na última página (as demais devem ser rubricadas);
- Anexo do Laudo: impresso ou em meio digital, deve conter as evidências encontradas.

1.3 Antiforense Digital

Não existe uma definição única para Antiforense Digital, o que não é exatamente uma surpresa, visto que é uma ciência relativamente pouco explorada. Algumas definições restringem o termo à descrição de ferramentas que destroem mídias e evitam a captura de informações nelas contidas, outras têm um espectro mais amplo e abrangem sistemas complexos de proteção à privacidade [Berinato 2007].

Talvez o método mais eficiente para obter um significado único para a descrição de Antiforense Digital seja analisar separadamente as palavras que compõem sua definição. O prefixo define "anti" como "oposição ou ação contrária". Da combinação destes termos, Antiforense Digital pode ser definida como "métodos utilizados para

impedir a ação da ciência para a coleta de evidências que resultem na quebra de privacidade individual ou exposição de segredos industriais" [Harris 2006].

Assim como existem várias definições de Antiforense Digital, diversos métodos foram propostos para garantir o sigilo de informações armazenadas. A Tabela 1.1 descreve uma das classificações possíveis para métodos antiforense: destruição, ocultação, eliminação da fonte e falsificação [Harris 2006]. Cada uma destas categorias endereça ações distintas para comprometer a disponibilidade e utilidade da informação para o processo forense. Evidências podem ser destruídas para evitar que sejam encontradas ou que sejam úteis caso sejam localizadas. Podem ser ocultadas para impedir que sejam casualmente expostas ou dificultar a sua identificação por um investigador. Possíveis fontes de evidências podem ser destruídas para garantir que nunca estejam disponíveis, ou mascaradas e manipuladas para distribuir a culpa ou corromper a sua validade, de modo que não possam ser utilizadas em um tribunal [Peron e Legary 2008].

Tabela 1.1. Classificação de categorias antiforense [HARRIS, 2006]

Nome	Destruição	Ocultação	Eliminação da fonte	Falsificação
Alterações MACE[3]	Destruir a informação MACE ou sobrescrever com dados aleatórios.			Reescrever com dados aleatórios para confundir investigadores.
Remover/ esterilizar arquivos	Reescrever o conteúdo com dados aleatórios.	Excluir o arquivo.		
Encapsulamento de dados		Ocultar um arquivo em outro.		
Seqüestro de conta				Criar evidência para culpar outra pessoa por atos irregulares.
Arquivos auto-destrutivos				Criar evidências para comprometer a análise de uma imagem.
Desabilitar *logs*			Não são disponibilizadas informações sobre atividades realizadas.	

Das quatro classificações, a destruição merece uma consideração especial, por ser um processo irreversível. A destruição envolve o processo de tornar a evidência sem utilidade para o processo investigativo, por sua exclusão total ou comprometimento. Destruição implica em ir além da tarefa de tornar uma evidência inacessível (como na ocultação ou eliminação da origem) e é um processo sem possibilidade de recuperação.

Em crimes não digitais, exemplos de destruição podem ser: a eliminação de impressões papilares (digitais, palmares e plantares) de uma arma, de um piso, parede ou vidro; o uso de água sanitária para destruir o DNA de uma amostra de sangue; entre

[3] Acrônimo de *Modfication*, *Access*, *Create* e *Entry Modifying*.

outros [Kemp e Smith 2005]. Como estas ações trabalham sobre evidências existentes, o processo de destruição pode criar novas evidências. Por exemplo, a garrafa utilizada para transportar a água sanitária pode conter impressões papilares que indicam o autor do processo de limpeza.

No mundo digital aplicam-se as mesmas regras: a sobrescrita de um arquivo pode destruir parcialmente ou completamente o seu conteúdo, mas o *software* utilizado para realizar a esterilização pode criar uma trilha de evidências adicionais, de acordo com o corolário de Harlan[4] [Carvey 2009].

1.4 Técnicas e Ferramentas Antiforense

Para dificultar ou impedir que alguém, mesmo que seja um perito forense, tenha acesso às informações presentes em uma mídia de armazenamento, a antiforense digital pode ser aplicada [Peron e Legary 2008]. Segundo a experiência dos autores, as técnicas mais utilizadas são a de destruição e a ocultação de dados. Por este motivo, estas duas serão abordadas nesta seção.

Relacionado à destruição de dados (Seção 1.4.1), serão abordados procedimentos de exclusão segura ou meios para danificar a estrutura física da mídia de armazenamento, fazendo com que os dados não possam ser recuperados nem mesmo pelo proprietário do conteúdo.

Com relação à proteção (ocultação) das informações (Seção 1.4.2), serão abordados procedimentos que garantam a possibilidade de recuperação dos dados. Entretanto, este acesso deve ser limitado exclusivamente ao proprietário ou a alguém que consiga descobrir como foi realizada a proteção e/ou o algoritmo e chave que foram utilizados.

1.4.1 Destruição de dados

O principal objetivo da destruição de dados é impossibilitar que o seu conteúdo seja recuperado e possa expor a privacidade de pessoas ou eventualmente causar algum impacto (positivo ou negativo) no mercado corporativo [EDT 2006]. Como o processo é irreversível, são necessários procedimentos adequados, físicos ou lógicos, que garantam a efetiva destruição das informações e resguardem os responsáveis de possíveis sansões legais (penalidades/responsabilização). A Seção 1.4.1.1 mostrará procedimentos de destruição física e a Seção1.4.1.2 os de destruição lógica.

1.4.1.1 Procedimentos de destruição física

Como o próprio nome sugere, a destruição física consiste em causar danos estruturais ao dispositivo de armazenamento, inviabilizando sua reutilização pelos meios normais para os quais foi projetado [Government of Canada 2006].

[4] A primeira Lei da Forense Digital, proposta por Jesse Kornblum [2002], diz que "Toda a ação gera uma evidência" e o corolário de Harlan complementa especificando "Uma vez compreendida quais condições criam ou alteram um fato, então a completa ausência de fatos é por si mesma um fato" [Carvey 2009], ou seja, a ausência total de informações é um indício de que a unidade de disco possa ter sido esterilizada.

A destruição física pode ser realizada através de procedimentos não muito complexos. Processos mais simples podem ser realizados sem a utilização de ferramentas especiais, acessíveis à maioria das pessoas, inclusive em ambiente doméstico. Os principais processos são descritos nos tópicos seguintes.

Deformação física

Consiste em causar danos que impeçam o funcionamento normal do equipamento após a realização deste procedimento. Pode ser realizado com ferramentas genéricas como martelo, marreta e chaves de fenda, de modo a causar danos internos ou externos à unidade. A utilização de uma furadeira, para criar vários orifícios que atravessem completamente a mídia, pode criar níveis de dificuldade de tal ordem que impeçam técnicos pouco aparelhados de obter êxito na recuperação de qualquer informação [Government of Canada 2006]. Recursos mais avançados, como prensas hidráulicas, também podem ser utilizados com maior eficácia nos resultados.

Desmontar a unidade permite o acesso às superfícies internas e possibilita causar danos diretamente aos discos magnéticos (quando não se tratar de unidades de estado sólido - SSD), potencializando os estragos. Entre as técnicas descritas, esta é a que apresenta menor complexidade e pode ser realizada mesmo em ambiente doméstico.

Abrasivos

Uma variação do item anterior, consiste em desmontar a unidade e remover os discos (também conhecidos como pratos magnéticos) com a utilização de ferramentas comuns. Uma lixa, ou outro material abrasivo, é utilizada para remover a fina camada magnética que reveste os pratos de alumínio [Government of Canada 2006].

Trituradores ou fragmentadores de metais

Em ambientes onde a informação é critica podem ser empregados fragmentadores com capacidade de triturar metais. A indústria americana Security Engineered Machinery produz equipamentos capazes de triturar discos rígidos com a granularidade especificada pelo cliente [SEM 2005].

Exemplos deste tipo de destruição são os procedimentos especificados no documento *Clearing And Declassifying Electronic Data Storage Devices* da Communications Security Establishment[5] (CSE), do governo do Canadá, que limita em 10 mm^2 os fragmentos resultantes para dispositivos que armazenam arquivos classificados como altamente secretos [Government of Canada 2006].

Existem técnicas radicais de recuperação baseadas no princípio de microscopia de força magnética (MFM), que indicam ser possível acessar algumas informações a partir de fragmentos da ordem de milímetros. Nestas condições o custo dos recursos (humanos e equipamentos), associado ao tempo de recuperação, pode inviabilizar economicamente o procedimento [Hughes et al. 2009].

Incineração

O National Institute of Standards and Technology (NIST) lista a utilização de incineradores industriais como uma das técnicas possíveis de destruição física [Kissel et al. 2012]. A perda da capacidade de armazenamento magnético ocorre com a exposição

[5] Agência Nacional de Segurança. Órgão governamental do Canadá.

a altas temperaturas. Para medir qual temperatura seria necessária, foi criada uma medida denominada Ponto Curie, que determina a temperatura na qual todos materiais perdem a capacidade magnética [O'Handley 2000].

A empresa Luftech[6] fabrica equipamentos que alcançam temperaturas de até 1600 graus Celsius [LUFTECH 2013], que atendem as especificações exigidas pela NSA (National Security Agency) para incinerar discos rígidos [NSA 2013]. Esta temperatura supera os aproximados 660 graus Celsius necessários para fundir o alumínio utilizado na construção de algumas partes das unidades (e que podem incluir os próprios pratos magnéticos) ou os 125 graus Celsius necessários para desmagnetizar compostos ferromagnéticos utilizados em partes do disco rígido [Mamun et al. 2007].

Fundição de metais

Reciclagem de metais via fundição de discos rígidos é uma possibilidade de destruição de informações que pode, dependendo da escala, trazer algum retorno financeiro para o processo de descarte. A fundição descaracteriza por completo a mídia de armazenamento magnética, resultando em material seguro para reciclagem [Government of Canada 2006].

Agentes químicos

Uma técnica adicional de destruição do disco rígido é a utilização de produtos químicos (como ácidos) que possam degradar o dispositivo. Entretanto, esse procedimento requer a utilização de equipamentos de proteção individual e sugere-se que seja apenas realizado por profissionais qualificados. Além da necessidade destes cuidados, o armazenamento de reagentes e o descarte adequado dos resíduos, de modo a não causar problemas legais com os órgãos ambientais, podem inviabilizar sua adoção por algumas pessoas ou empresas [Jardim 2013].

1.4.1.2 Procedimentos de destruição lógica

Excluir um arquivo utilizando recursos do sistema operacional (mover para lixeira no ambiente Windows, Mac OS ou o comando *rm* do Linux) e efetivamente eliminar informações de um disco rígido são procedimentos diferentes. O comando *rm* do Linux impede a possibilidade de acesso via recursos dos sistemas operacionais enquanto o recurso de lixeira do Mac OS ou Windows permite a recuperação via operações especiais do sistema operacional. Normalmente, a área que os arquivos ocupavam é marcada pelo sistema de arquivos como disponível para armazenamento de novos dados, todavia as informações continuam gravadas em disco até que um novo dado seja gravado por cima do anterior. Mesmo que um novo dado seja gravado em cima do anterior, ainda é possível recuperar a informação anterior. Usuários especializados estão familiarizados com técnicas de destruição lógica (*wipe*[7]), que emprega a sobrescrita de dados como umas das formas de inviabilizar a sua recuperação [Garfinkel e Shelat, 2003].

A destruição lógica permite a reutilização da mídia e é desenvolvida para possibilitar uma relação de custo/benefício aceitável. Existem diversos procedimentos que permitem a exclusão de um arquivo com pouca ou nenhuma possibilidade de

[6] Disponível em www.luftech.com.br.
[7] Termo em inglês que significa limpar, retirar, apagar, esfregar.

recuperação. Estas técnicas contemplam a sobrescrita do local físico da mídia onde o arquivo está gravado, os registros que identificam a partição ou a sobreposição de informações de todos os setores de um disco [Garfinkel e Shelat 2003]. Outra possibilidade é utilizar desmagnetizadores que permitem praticamente reduzir a zero as informações contidas nos discos rígidos e outras mídias magnéticas. Os procedimentos de sobrescrita e desmagnetização são descritos a seguir.

Sobrescrita (*Overwriting*[8] / *Wipe*)

Um modo comum de inviabilizar que informações gravadas em mídias magnéticas sejam recuperadas é sobrescrever os arquivos com outros dados. Este procedimento, chamado de *wiping* ou *shredding*[9], é considerado um método aceitável de limpeza que não inviabiliza a reutilização dos dispositivos e garante que os dados não possam ser recuperados com o uso de utilitários ou funções dos sistemas operacionais. Segundo Guttmann[10] [Gutmann 1996], os dados ainda podem ser recuperados, mas somente utilizando técnicas e laboratórios especializados.

A sobrescrita intencional é uma proteção para evitar a exposição acidental de informações sensíveis de uma pessoa ou organização. A técnica mais simples consiste em escrever sobre o arquivo ou unidade a ser esterilizada uma sequência padrão de bits. Esta medida impõe dificuldades para que a informação original seja recuperada com utilitários específicos de recuperação de dados [Garfinkel e Shelat 2003].

Para prevenir que técnicas mais avançadas sejam utilizadas para recuperar informações sensíveis, existem padrões de sobrescrita específicos. Estes padrões são utilizados para eliminar a possibilidade de sucesso utilizando ferramentas convencionais. Por exemplo, a reescrita repetida de padrões binários de "0" e "1" é mais eficiente que a simples gravação de "0" uma única vez [DOD 2001].

Uma das fragilidades da sobrescrita é que algumas áreas de discos rígidos podem ficar sem possibilidade de acesso pouco antes da esterilização devido à degradação da mídia ou outros erros, e nestes locais conservar fragmentos dos dados originais. A sobrescrita também é problemática em ambientes que requerem índices de segurança mais efetivos dos usualmente oferecidos por *software* [EDT 2006].

Peter Gutmann estudou a recuperação de dados sobrescritos com padrões convencionais durante a década de 1990 e suas observações indicaram que técnicas de microscopia de força magnética (MFM) poderiam habilitar a recomposição dos dados originais [Gutmann 1996]. Com base em suas descobertas, desenvolveu um método centrado em diversos padrões binários que compensam as fragilidades observadas pela sobrescrita simples, que atualmente é conhecido como Método Gutmann. Daniel Feenberg, por outro lado, um especialista do National Bureau of Economic Research[11] (NBER), classifica como "lenda urbana" as chances de uma informação sobrescrita ser recuperada em um disco rígido atual [Feenberg 2003].

---

[8] Termo em inglês que significa sobrescrita.

[9] Termo em inglês que significa triturar.

[10] Peter Gutmann, profissional de segurança da informação do Departamento de Ciências da Computação da Universidade de Auckland, Nova Zelândia.

[11] NBER é uma organização de pesquisas, sem fins lucrativos, que promove estudos e divulga pesquisas sobre políticas públicas, corporativas, profissionais e acadêmicas em relação ao funcionamento da economia.

O Departamento de Defesa dos Estados Unidos da América (DoD-US) divulgou uma orientação, em novembro de 2007, reconhecendo a sobrescrita como um método eficiente de limpeza de mídias magnéticas, mas a completa esterilização só é aceitável utilizando os métodos de destruição física ou desmagnetização [USAID 1995]. O NIST, na Publicação Especial 800-88 (página 7), editada em 2006, menciona que estudos indicam que a maioria das mídias atuais pode ser efetivamente esterilizada com apenas uma sobrescrita [Kissel et al, 2012].

A sobrescrita pode ser realizada por utilitários residentes em um disco de inicialização (disco de *boot*) especialmente preparado que, dependendo do *software*, permite a conFiguração de processos com diferentes modelos e quantidades (ciclos–repetições), resultando em tempos diferentes para a conclusão [DBAN 2013].

A destruição lógica também pode ser realizada por *softwares* executados pelo próprio sistema operacional, com recursos de excluir apenas arquivos selecionados, pastas ou diretórios, partições ou áreas não alocadas do disco [Heide 2013]. Para esta finalidade, existem *softwares* comerciais, gratuitos (*freewares*) e de código aberto (*opensource*), compatíveis com vários sistemas operacionais. Deve-se observar que estes *softwares* geralmente não eliminam cópias do arquivo aberto mantidas na memória virtual (*swap*) dos sistemas operacionais ou arquivos temporários. Para contornar essa possível vulnerabilidade, pode-se desabilitar o uso da memória virtual (e/ou conFigurar o *software* de destruição lógica para que este realize a sobrescrita da memória virtual no processo de desligamento do computador) e de criação de arquivos temporários [TRUECRYPT 2013]. Um exemplo de aplicação de *wiping* em uma partição de um *pendrive* é mostrado na Figura 1.16, através do *software* Minitool Partition Home Edition. Para visualizar o conteúdo do *pendrive* após a aplicação de *wiping* foi utilizado o software *FTK* Imager (Figura 1.17).

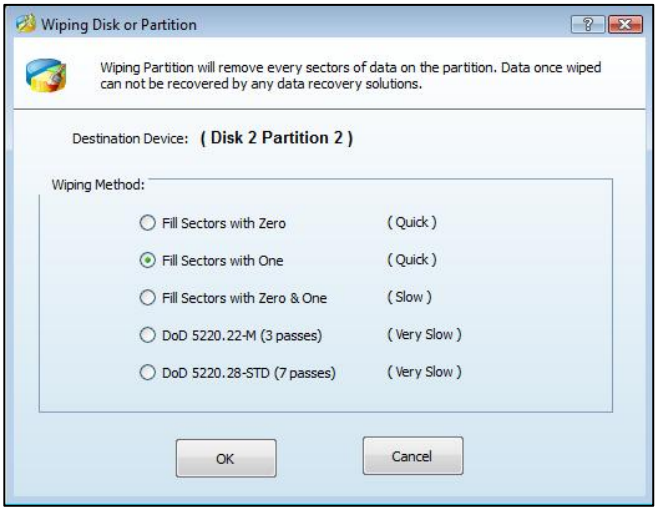


Figura 1.16. Aplicação de wiping com bits “1”

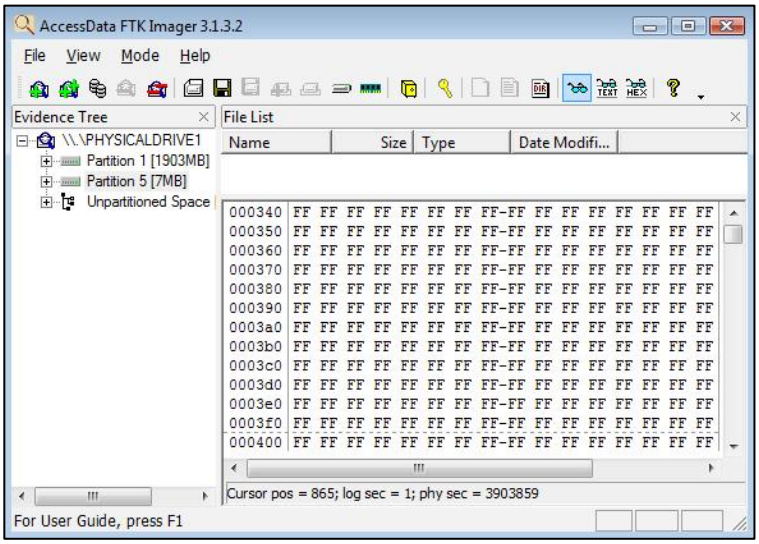


Figura 1.17. Visualização da partição em que foi aplicado wiping

Desmagnetização

Desmagnetização (ou *degaussing*) é o processo de remoção ou redução do campo magnético, que pode esterilizar um disco rígido ou outra mídia com rapidez e eficiência. Este processo usualmente remove a formatação de baixo nível realizada pelo fabricante, causando danos irreversíveis que inutilizam a mídia. Em ambientes de alta segurança, o desmagnetizador deve ser adequado para a mídia a ser esterilizada.

Conforme o documento *Degausser Evaluated Products List* da NSA, a coercividade[12] magnética utilizada nas unidades fabricadas entre os anos de 2000 e 2007 subiu aproximadamente 67%. Um equipamento homologado para esterilizar dispositivos magnéticos no ano de 2000 pode não ter a intensidade magnética necessária para esterilizar um disco rígido de fabricação atual, criando uma vulnerabilidade nos procedimentos de segurança [NSA 2012].

1.4.2 Proteção das informações

A Seção 1.4.2 focou principalmente na destruição de informações, seja de maneira física ou de maneira lógica. A destruição física na maioria das vezes pode não ser desejada devido ao alto custo de algumas mídias. O mesmo pode valer para a destruição lógica, pois pode ser necessário utilizar recursos sofisticados para conseguir eliminar logicamente os dados. Além disto, nem sempre é possível garantir que os dados armazenados não sejam acessados antes que as informações sejam destruídas. Assim é fundamental existir uma forma de proteger informações confidenciais, pessoais ou corporativas, contra exposição indevida por descuido ou por ação de intrusos, independente de motivos reprováveis ou respaldo legal [EDT 2006]. Existem diversas técnicas orientadas para a proteção de dados sensíveis, com diferentes procedimentos de ocultação ou controle. Algumas não escondem a existência da informação, porém impõem dificuldades na interpretação do conteúdo (Criptografia), enquanto outras privilegiam a ocultação da própria existência da informação (Esteganografia) [Cole 2003]. Esta seção apresenta estas duas técnicas e algumas ferramentas que podem ser

[12] Medida de intensidade magnética necessária para modificar um sinal armazenado magneticamente.

utilizadas para que seja possível proteger informações confidenciais através de Criptografia ou Esteganografia.

1.4.2.1 Criptografia

Criptografia pode ser definida como o processo de converter informações (texto) legíveis em um texto (formato) cifrado[13] para serem armazenadas ou transmitidas em um meio potencialmente inseguro. Em Criptografia, uma cifra é definida como um par de algoritmos para criptografar (transformar o texto legível em texto não legível) e descriptografar (transformar o texto cifrado em texto legível). A utilização de cifras permite proteger informações contra organizações criminosas, intrusos maliciosos ou simples curiosos. Em Criptografia a recomendação é que o segredo não esteja nos algoritmos de criptografia e descriptografia, pois caso os mesmos sejam descobertos, então fica mais fácil descobrir qual o texto legível a partir de um texto cifrado. O segredo deve estar na chave utilizada para criptografar e descriptografar.

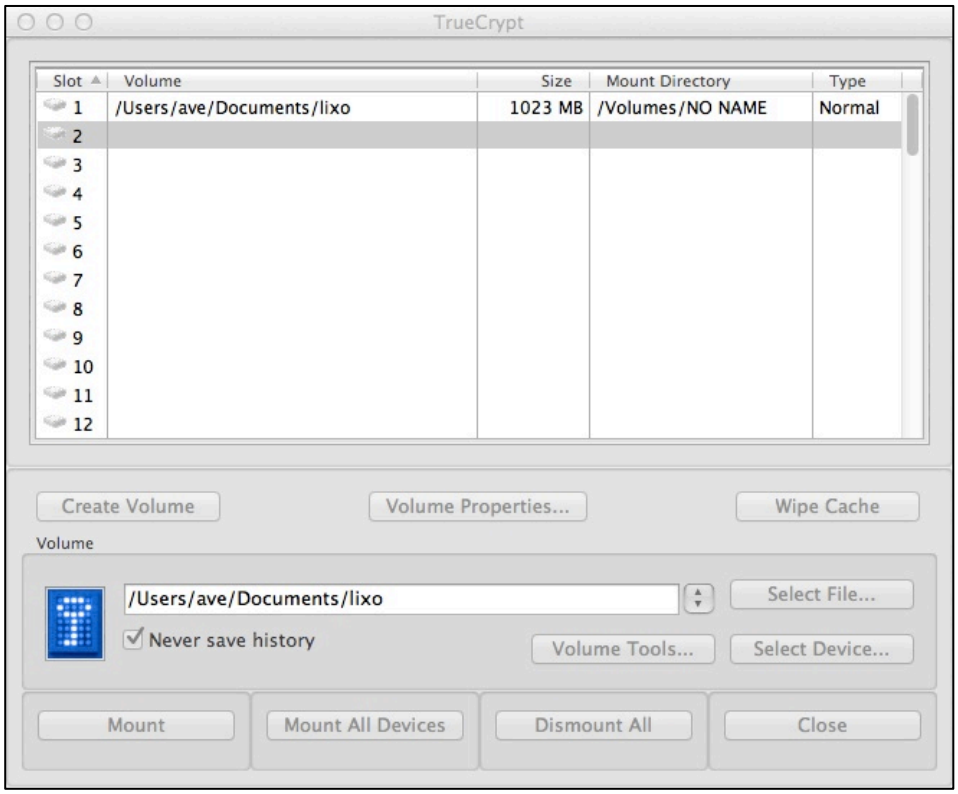
Existem duas formas de utilizar chaves em uma cifra: mesma chave para criptografar e descriptografar (chaves simétricas) e chaves diferentes para criptografar e descriptografar (chaves assimétricas, ou chave pública e chave privada). As cifras que utilizam chaves simétricas possuem operações mais simples e rápidas de serem calculadas. A operação base nas cifras simétricas é a operação *xor* (ou exclusivo), que é muito rápida de ser calculada. Nas cifras assimétricas, utiliza-se Aritmética Modular ou Curvas Elípticas. Em Aritmética Modular, tanto a operação de criptografar quanto a operação de descriptografar utilizam exponenciação (e multiplicação), que para números grandes possui grande tempo para computação. Exemplos de algoritmos de Criptografia de chave simétrica são Blowfish, DES, 3DES, AES, Serpent e Twofish. Exemplos de uso de criptografia assimétrica são: RSA, TLS, ElGammal, PGP e Bitcoin. Para entender um pouco mais sobre Criptografia recomenda-se os seguintes livros: "O livro dos códigos" (*The code book*) de Simon Singh, que apresenta um bom relato sobre o progresso da Criptografia de uma maneira simples e misturado com um pouco de história (um excelente relato sobre como os poloneses e britânicos quebraram a máquina de criptografia Enigma dos alemães); *Handbook of Applied Cryptography* de Alfred Menezes e Paul van Oorschot e *Applied Cryptography* de Bruce Scheneier. Os dois últimos descrevem algoritmos e protocolos, além de recomendações sobre o uso de Criptografia.

Existem diversas soluções para armazenar em disco ou transmitir informações por redes de computadores de maneira segura. Esta proteção pode ser realizada por *hardware* ou por *software*. A criptografia por *software* simplifica os procedimentos de controle e atende às necessidades de segurança [Gutmann 2004]. Para armazenamento de informações de maneira segura por *software*, por exemplo, pode ser realizada através da criação de um arquivo (*container*) em um disco rígido e montar este arquivo em um *drive* virtual. Todas as informações transferidas para o *drive* virtual são armazenados no *container* de forma criptografada. Criptografia por *hardware* pode ser utilizada, por exemplo, por meio de chips da família MAXQ® (DeepCover® Secure Microcontroller) [MAXQ 2013] ou então por *smartcards* como Javacards produzidos pela NXP [NXP 2013]. Ambos exemplos implementam algoritmos de criptografia como 3DES, AES, RSA, ECDSA, SHA, entre outros.

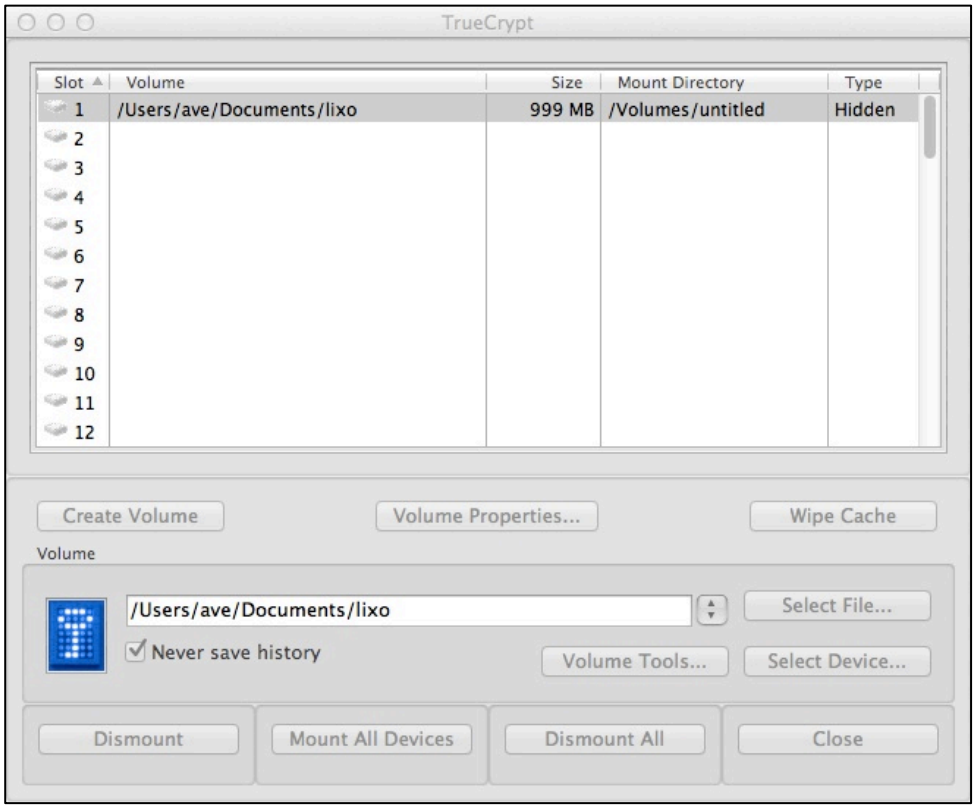
[13] Usaremos o termo "texto legível" para traduzir *plaintext* e "texto cifrado" para *ciphertext*.

Existem diversas soluções em *softwares* para proteger as informações, por exemplo, soluções comerciais: BestCript [JETICO 2008] (para criar um disco criptografado) ou Silent Circle (para criptografar comunicação); ou soluções gratuitas: TrueCrypt [TRUECRYPT 2013] (para criação de disco criptografado), Tails (um sistema operacional completo, com ferramentas de acesso à Internet, para ser usado a partir de um DVD ou *pendrive*), GnuPG (uma ferramenta que disponibiliza diversas soluções de criptografia que pode ser utilizado por outras ferramentas), OTR (Off-The-Record permite a comunicação instantânea com criptografia e autenticação) e AxCrypt (que provê a possibilidade de criptografar arquivos de maneira individual). Os últimos podem ser baixados de maneira gratuita. Na hora da escolha de um *software* para proteção das informações é recomendável a utilização de soluções abertas (com o código disponível), pois assim é possível verificar se possíveis vulnerabilidades ou *backdoors* estão presentes, o que tornaria possível a exploração por pessoas mal-intencionadas.

Entre as soluções apresentadas nos parágrafos anteriores o TrueCrypt provê uma solução para criar um disco criptografado, onde as informações são criptografadas e descriptografadas no momento da leitura ou escrita (*on-the-fly encryption*). TrueCrypt possui a habilidade de criar volumes escondidos que podem ser "negados" (*deniable hidden volumes*). Com o TrueCrypt é possível criar dois tipos de volumes (discos) dentro de um arquivo sobre o sistema de arquivos do sistema operacional (Linux, Mac OS ou Windows): volumes não escondidos (Figura 1.18.a) e volumes escondidos (Figura 1.18.b).



a) Volume não escondido.



b) Volume Escondido.

Figura 1.18. Telas do software TrueCrypt

Por exemplo, volumes não escondidos podem ser criados como um arquivo normal sobre o sistema de arquivos do sistema operacional. O volume poderia ser criado também como uma partição dedicada em um disco. Em ambos casos este volume é considerado um *container* pelo TrueCrypt. Para acessar (montar) este volume é necessário informar uma senha que será utilizada para criptografar os dados do volume utilizando um dos algoritmos mencionados. O TrueCrypt provê também o conceito de Sistema de Arquivo Negável (*Deniable File System*) através do conceito de arquivo escondido. Ao criar um volume do TrueCrypt é possível criar dois volumes, um não escondido, onde o usuário pode colocar informações não sensíveis e outro volume para armazenar informações sensíveis. Assim, se o usuário for constrangido a revelar a senha de acesso ao volume criptografado ele pode revelar a senha de acesso ao volume que possui informações não sensíveis e não a outra. Outras ferramentas apresentadas possuem características similares.

1.4.2.2 Esteganografia

Esteganografia pode ser definida como a arte de esconder informações através de meios que façam com que não se detecte as informações escondidas [Johnson 1998]. Existem diversos métodos de esconder informações de forma que a própria existência delas seja escondida. Estes métodos podem incluir tintas invisíveis, pontos microscópicos, rearranjar caracteres, assinaturas digitais, entre outros. Tratando-se do meio digital, Esteganografia é a técnica de ocultar informações (pode ser arquivos completos) em um arquivo contendo texto, imagem, som, vídeo ou qualquer outro tipo de conteúdo de tal

modo que a presença das informações escondidas não seja percebida. O arquivo que contém as informações escondidas é chamado de hospedeiro ou portador. Criptografia e Esteganografia são duas formas muito próximas de evitar que alguém tenha acesso a informações confidenciais. Todavia, enquanto Criptografia embaralha a mensagem para ela não ser entendida, a Esteganografia esconde a mensagem para ela não ser vista. Uma mensagem cifrada pode levantar a suspeita de que algo importante esteja escondido, enquanto que com a Esteganografia não. Cabe salientar também que em geral pode-se esconder informações criptografadas através de Esteganografia, ou seja, primeiro criptografa-se a mensagem (arquivo) e depois ele é inserido, por exemplo, na imagem.

Várias técnicas de Esteganografia utilizam representação digital de imagens ou áudios como arquivos hospedeiros para ocultar informações. Uma revisão da codificação destes arquivos permite analisar como mensagens podem ser inseridas e retiradas, sem alterar significativamente suas características [Wand e Wang 2004]. Por exemplo, sons podem ter características alteradas de maneira não identificável pelos sentidos humanos, como pequenas alterações no ângulo de fase, cadência da fala e mudanças sutis de frequência, que podem ser utilizadas para ocultar informações. Alterações sutis nos tons de cores de uma fotografia seguramente podem passar despercebidas para um observador e conter informações ocultas. Ainda, imagens e arquivos de áudio são usados frequentemente como hospedeiros de mensagens, pois a existência destes tipos de arquivos é aceita com naturalidade, não levantando muitas suspeitas [Bender et al. 1996]. Além disto, em geral, arquivos de imagens ou áudios podem ter um tamanho elevado. Um filme, por exemplo, pode ter o tamanho de até alguns Gibibytes, assim, esconder mensagens de poucos Kibibytes praticamente não afetaria o tamanho do arquivo e passaria despercebido por alguém que tivesse acesso ao arquivo.

Um exemplo de técnica aplicada a imagens, que encontra-se entre as mais difíceis de ser detectada, é a LSB (*Least Significant Bit*). Como o próprio nome diz, os dados a serem escondidos utilizam o *bit* menos significativo de cada canal de cada *pixel*[14]. Ou seja, se cada *pixel* possui 32 bits (8 bits para o canal de transparência, 8 para o vermelho, 8 para o verde, 8 para o azul), então cada um destes componentes possui 2^8 valores possíveis. Se por exemplo, o componente vermelho for alterado de 11111100 (252 em decimal) para 11111101 (253) e o mesmo ocorrer com os demais componentes do *pixel*, a visão de um ser humano não teria condições de identificar tal alteração. Resumindo, é possível realizar alterações mínimas em cada *pixel*, ou em alguns deles, sem deteriorar a imagem. Um exemplo utilizando a técnica LSB é mostrado na Figura 1.19, com a utilização do *software* Hide & Reveal [HIDE 2010].

[14] *Picture Element* - elemento de imagem, cada ponto que compõe a imagem.

(a) Escolha do hospedeiro, arquivo a ser escondido e arquivo destino.

(b) Escolha da técnica LSB simples.

Figura 1.19. Aplicação da técnica LSB (os botões "Hide" e "Reveal" foram retirados das Figuras para melhor visualização)

Em algumas situações o arquivo gerado possui tamanho diferente do original, mas o ideal é que o tamanho seja o mesmo. Após o exemplo mostrado na Figura 1.19, verificou-se o tamanho dos arquivos (Figura 1.20) e pôde-se verificar que os horários de última modificação estão diferentes, porém o tamanho dos dois arquivos (rosto.bmp e rosto2.bmp) é o mesmo. Ou seja, 25 bytes foram inseridos no arquivo hospedeiro, gerando um novo arquivo com o mesmo tamanho. Os dois arquivos de imagem são mostrados na Figura 1.21 para que seja possível a comparação.

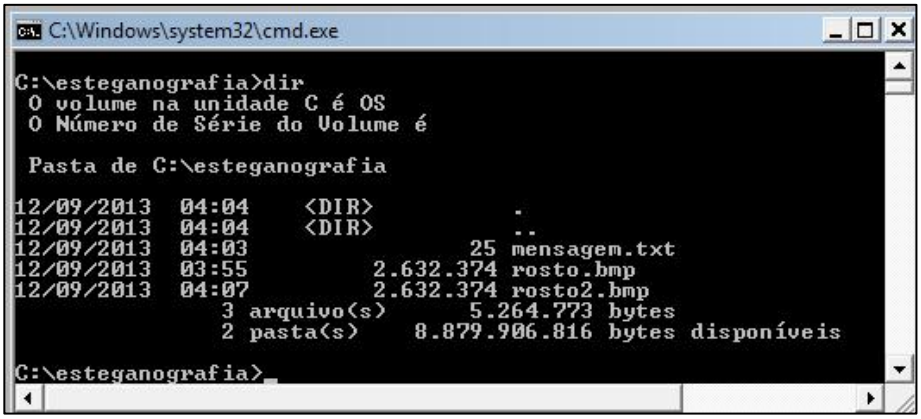
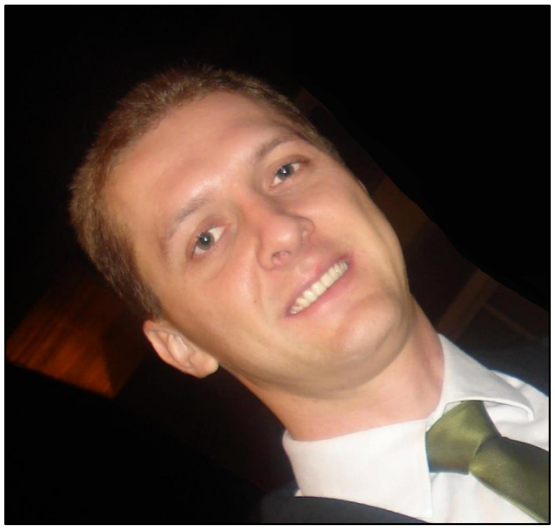
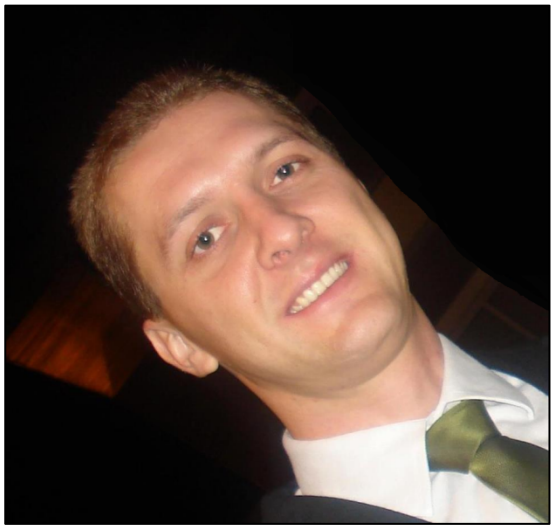


Figura 1.20. Verificação do tamanho dos arquivos



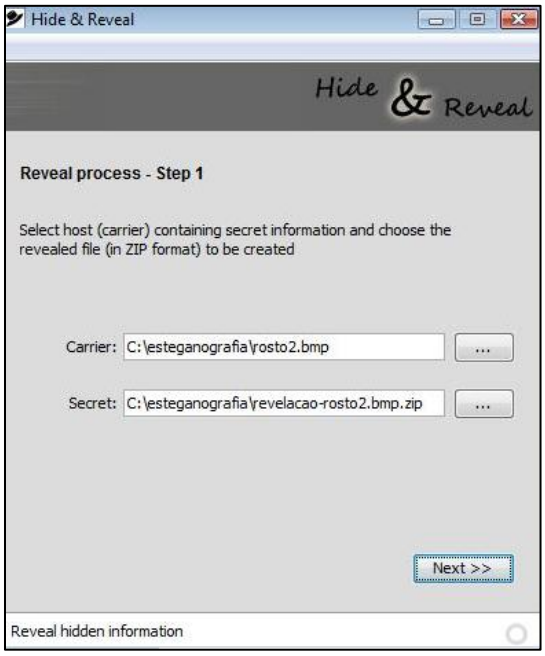
(a) Arquivo rosto.bmp.



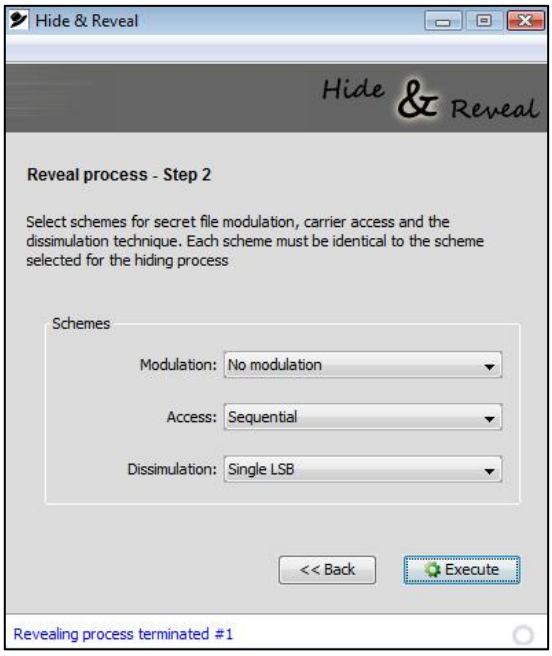
(b) Arquivo rosto2.bmp.

Figura 1.21. Comparação visual dos dois arquivos

Ainda utilizando o *software* Hide & Reveal, para revelar o que foi escondido, o usuário deve clicar no botão "Reveal", escolher o arquivo rosto2.bmp e a técnica utilizada (LSB simples). Este procedimento e o resultado são mostrados nas Figuras 1.22 e 1.23.



(a) Escolha do arquivo que contém dados escondidos e arquivo destino.



(b) Escolha da técnica LSB simples (mesma utilizada para esconder).

Figura 1.22. Revelação da esteganografia (os botões "Hide" e "Reveal" foram retirados das Figuras para melhor visualização)

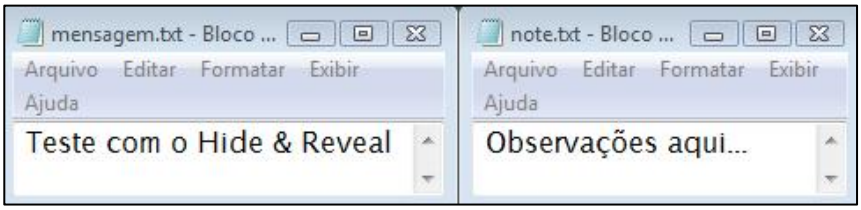
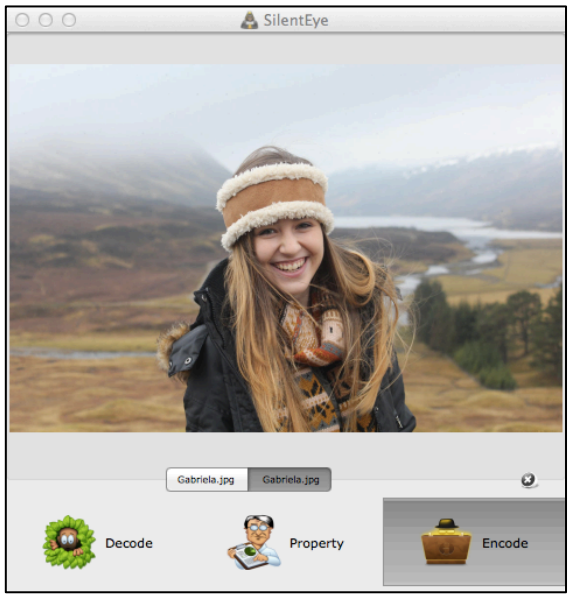


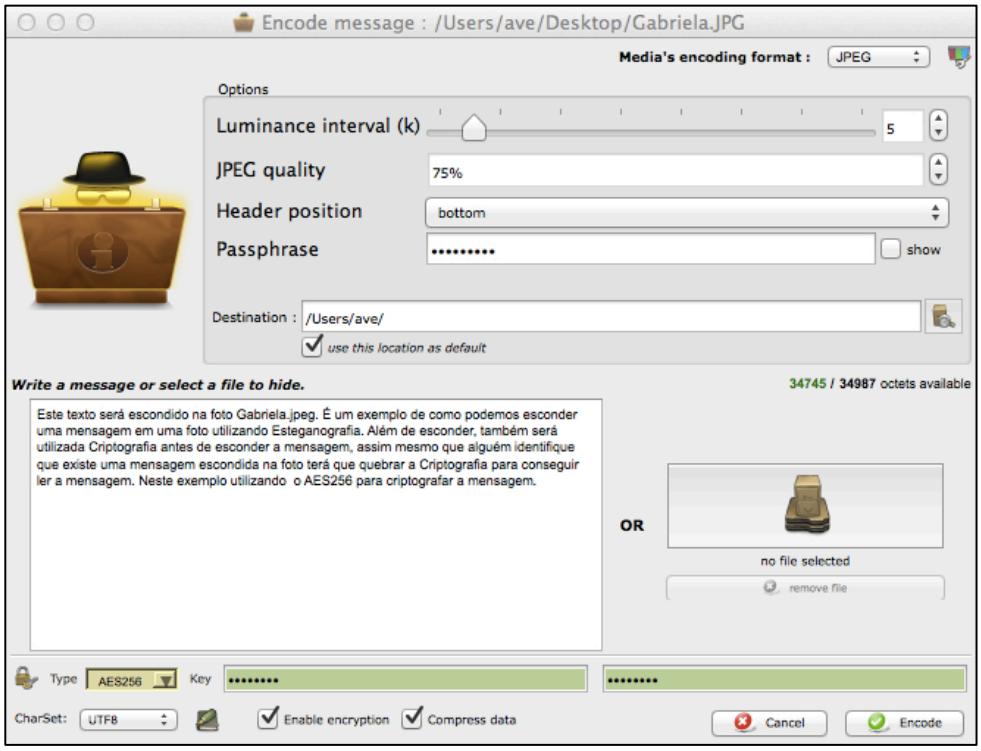
Figura 1.23. Arquivos revelados (o arquivo escondido e o que foi preenchido no campo "Note"), após terem sido descompactados do arquivo revelacao-rosto2.bmp.zip

Além do *software* Hide & Reveal, existem diversos *softwares* que podem ser utilizados para esconder informações dentro de arquivos: SilentEye, OpenPuff ou StegHide. A Figura 1.24 apresenta telas do *software* SilentEye para a versão Mac OS X. A Figura 1.24.a apresenta a foto antes de ter o conteúdo alterado com a mensagem escondida. A Figura 1.24.b mostra a foto já com a mensagem escondida e criptografada. O SilentEye permite que a mensagem criptografe a mensagem (ou arquivo) que será escondida na foto utilizando o algoritmo AES com chave de 128 ou 256 *bits* (não recomenda-se utilizar 128 bits, pois sua quebra pode ser atingida sem muita dificuldade atualmente). A Figura 1.24.c apresenta as opções para esconder uma mensagem (ou arquivo) na foto selecionada. A mensagem pode ser escondida com ou sem Criptografia.

a) Foto que conterá mensagem escondida.



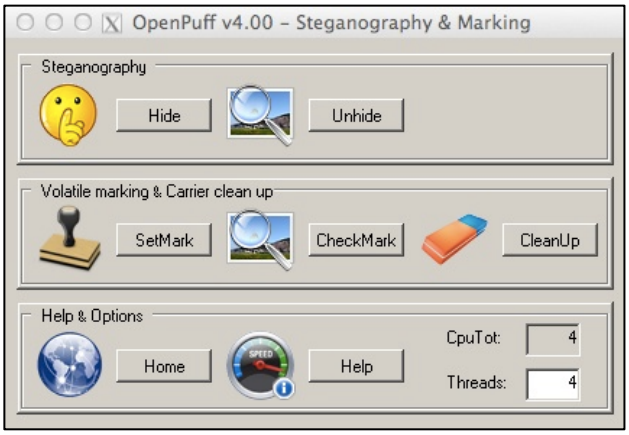
b) Foto com a mensagem escondida.



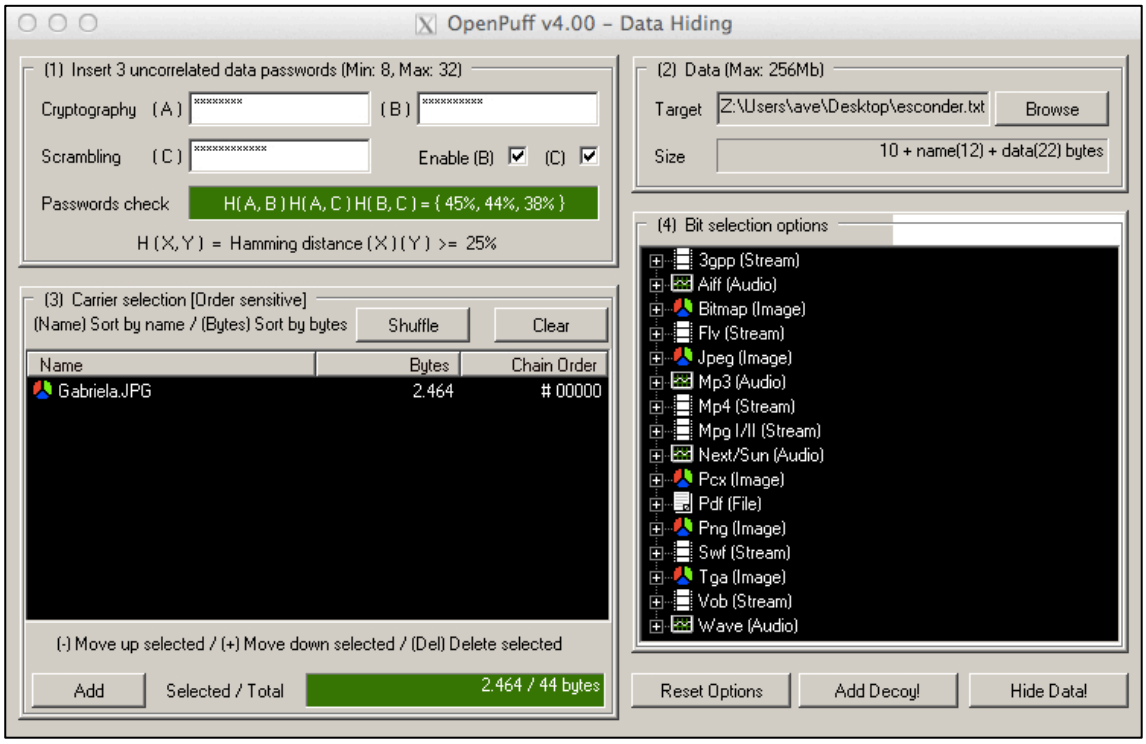
c) Mensagem que será criptografada e escondida na foto

FIGURA 1.24. Telas do software SilentEye

Outro exemplo de *software* para esconder informações é o OpenPuff. A Figura 1.25 mostra duas telas do OpenPuff na versão Windows, mas executado sobre o Mac OS X com o software Wine. A Figura 1.25.a apresenta a tela inicial do OpenPuff e a Figura 1.25.b apresenta a tela com as opções do OpenPuff para esconder informações em um determinado arquivo. O OpenPuff é um exemplo de *software* que além de esconder informações, permite esconder marcas em um determinado arquivo. Assim, se alguém suspeitar que informações estão sendo repassadas para pessoas não autorizadas, o detentor da informação pode utilizar Esteganografia para colocar marcas em diversos arquivos com o mesmo conteúdo e enviar os arquivos (cada um com uma marca diferente, que possa identificar para quem foi enviado o arquivo) para diversas pessoas. Caso algum dos arquivos seja repassado para alguém, então é possível identificar quem foi que repassou a informação ser ter autorização.



a) Tela inicial do OpenPuff.



b) Tela do OpenPuff para ocultar um arquivo (esconder.txt) no arquivo Gabriela.jpg.

Figura 1.25. Telas do software OpenPuff

Slackering

Slack area ou *slack space* são termos ainda sem uma definição apropriada na língua portuguesa e identificam áreas onde é possível ocultar informações com base nas características operacionais dos sistemas de arquivos utilizados em dispositivos de armazenamento [Carrier 2005]. Sistemas de arquivos definem a metodologia de armazenar e organizar arquivos de forma a habilitar o seu acesso quando necessário. Sistemas de arquivos utilizam dispositivos de armazenamento, tais como discos rígidos ou mídias ópticas, e administram a manutenção da localização física dos dados [Berghel et al. 2008].

Os sistemas de arquivos mais comuns são fundamentados em dispositivos que habilitam o acesso a blocos de tamanho fixo, usualmente chamados de setores. O sistema de arquivos é responsável por organizar conjuntos de setores em arquivos e diretórios e controlar quais setores pertencem a um arquivo e quais não estão sendo utilizados. A maioria dos sistemas de arquivos endereça dados em unidades de tamanho fixo, chamadas *clusters* ou *blocks*, que contém um número fixo de setores. O *cluster* (ou bloco) é a menor área em um disco que pode ser alocada para armazenar um arquivo [Carrier 2005].

A seguir é apresentado um estudo realizado em um dos sistemas de arquivos disponíveis, o NTFS (New Tecnology File System), e as suas conclusões podem ser portadas para praticamente todos os sistemas de arquivos. O NTFS é proprietário (Microsoft) e é utilizado por diferentes versões do sistema operacional Windows. Administra setores individuais de 512 bytes, agrupa setores em *clusters* (chamados de unidades de alocação) para reduzir o tamanho da MFT (Master File Table) e para minimizar a fragmentação dos arquivos [TECHNET 2003].

Nas primeiras versões do Windows NT, o NTFS podia definir *clusters* de até 64KiB, entretanto, a partir do Windows 2000, o tamanho pode variar conforme o tamanho da partição até um máximo de 4KiB. Em um sistema de arquivos NTFS com tamanho de cluster de 4KiB, um arquivo de apenas 1KiB ocupa a área de 4KiB na unidade de armazenamento [Carrier 2005].

Esta característica do NTFS, e dos sistemas de arquivos em geral, orienta a definição de *slack area*: o espaço existente entre o fim do arquivo e o fim do *cluster* onde ele está armazenado. Também chamada de *file slack*, a *slack area* é natural porque dificilmente dados armazenados são do tamanho exato do espaço alocado. Em forense digital, a *slack area* é importante porque pode manter dados significativos nas áreas residuais que ocorrem quando um arquivo menor é escrito sobre um arquivo maior [Berghel et al. 2008].

Uma verificação simples foi realizada no disco de um notebook de um dos autores deste capítulo, com o *software* Disk Slack Checker, desenvolvido por Karen Kenworthy[15]. A Figura 1.26 mostra o resultado, onde é possível constatar que em uma partição NTFS com tamanho de *cluster* de 4KiB e capacidade de armazenamento de 132,41GiB, há 257.571 arquivos que alocam o espaço de 122,58GiB, porém utilizam 122,06GiB. Ou seja, a *slack area* representa 533,16MiB, cerca de 0,42% do que foi alocado pelo sistema de arquivos.

[15] Disponível em <http://www.karenware.com>, acesso em Ago. 2013.

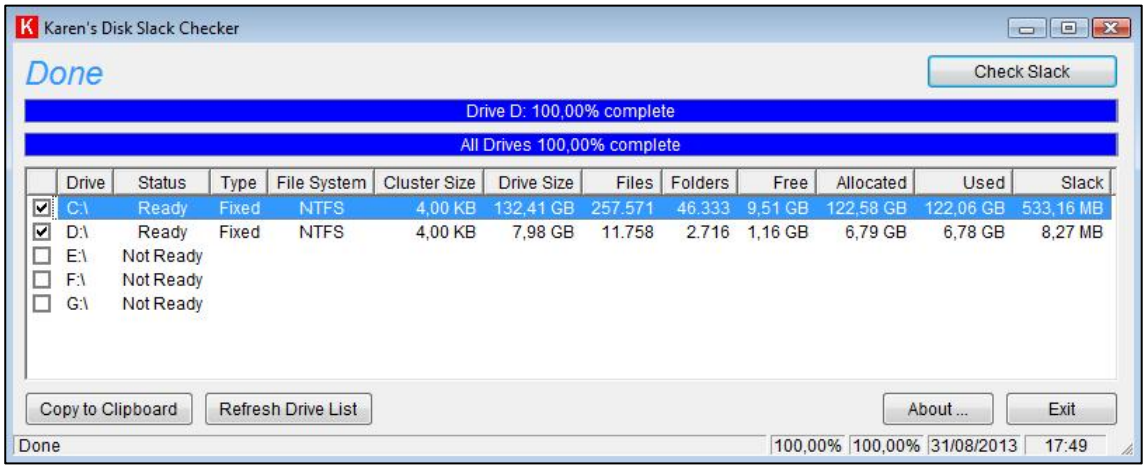


Figura 1.26 Verificação de slack area com o software Disk Slack Checker (diversas colunas foram suprimidas para melhor visualização)

ADS (Alternate Data Stream)

O Alternate Data Stream (ADS) é uma característica do NTFS concebida para permitir a compatibilidade com o sistema de arquivos HFS (Hierarchical File System) utilizado pela Apple [Means 2003]. ADS é a habilidade de distribuir um arquivo de dados entre outros arquivos existentes, sem afetar tamanho, funcionalidade ou maneira com que esses arquivos são tratados por utilitários tradicionais como, por exemplo, o Windows Explorer. O ADS existe em todas as versões do NTFS e é utilizado por inúmeros programas, incluindo alguns nativos do sistema operacional Windows, para armazenar atributos de arquivos ou informações temporárias [Zadjmool 2004].

O uso do ADS é extremamente simples e não requer um perfil técnico avançado. Comandos simples do MS-DOS[16], como o "type", utilizados em conjunto com indicadores de redirecionamento [>] e dois pontos [:] ativam o ADS e ocultam um arquivo em outro.

Um exemplo é mostrado na Figura 1.27, com a ocultação de um arquivo de texto em um arquivo executável (editor de texto WordPad). Como pode ser visualizado, há um arquivo denominado "confidencial.txt" na pasta "C:\dados" com tamanho 7.027 bytes. Na pasta "D:\ADS" existe apenas um arquivo executável (trata-se do editor de textos WordPad - write.exe) com tamanho 10.240 bytes. Antes da ocultação do arquivo havia 1.242.824.704 bytes disponíveis na unidade D: e, após a ocultação, 1.242.624.000 bytes disponíveis. Ou seja, o sistema mostra apenas o arquivo executável, com o seu tamanho original, porém a quantidade de bytes disponíveis na unidade D: diminuiu 200.704 bytes. Após tal experimento, o próprio editor WordPad foi executado para visualizar o arquivo de texto ocultado nele. O resultado da execução é mostrado na Figura 1.28.

[16] Apesar do MS-DOS ser um sistema antigo, ainda existem muitos computadores com o MS-DOS instalado, ou mesmo emuladores de MS-DOS sendo utilizados.

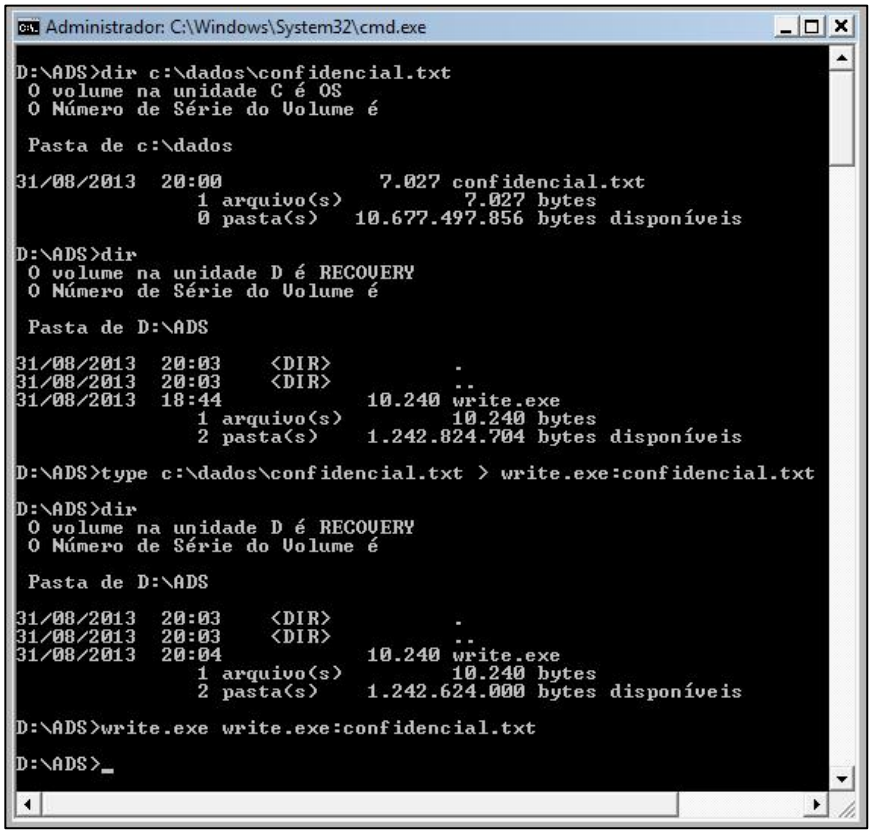


Figura 1.27. Ocultação de um arquivo de texto em um arquivo executável

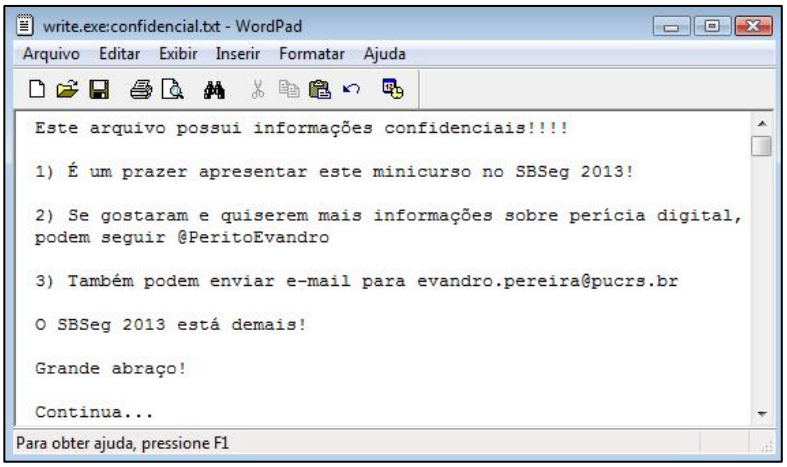


Figura 1.28. Resultado da execução "write.exe write.exe:confidencial.txt"

Arquivos ocultos pelo ADS são muito difíceis de detectar através do gerenciador de arquivos como o Windows Explorer ou por linhas de comando. Como já mencionado, o tamanho arquivo write.exe continua o mesmo e a única indicação visual disponível pelos recursos nativos do sistema operacional é através da análise de modificação de data/hora do arquivo investigado [Zadjmool 2004]. No caso da Figura 1.27, é possível verificar que a ocultação ocorreu no mesmo dia, porém uma hora e vinte minutos depois. Ou seja, o arquivo "write.exe" foi copiado de outro local para a pasta "D:\ADS" às 18h44min e a ocultação ocorreu às 20h04min. Se esta técnica for aplicada em um arquivo do sistema, é possível identificar data/horários suspeitos, porém se for um arquivo comum, não há como ter esse tipo de desconfiança.

Partições Ocultas (HPA e DCO)

Host Protected Area (HPA) e *Device ConFiguration Overlays* (DCO) são áreas de armazenamento em discos rígidos ocultas pelo fabricante que podem ser exploradas por procedimentos antiforense [Gupta et al. 2006]. As especificações do HPA e DCO definem a metodologia e os serviços associados para gravar dados e/ou programas em áreas de discos rígidos, que normalmente não estão disponíveis aos usuários e atende uma demanda dos fabricantes para facilitar o suporte aos seus produtos.

O HPA e o DCO foram desenvolvidos em função do grande número de equipamentos sem defeitos que retornavam à fabrica como inoperantes. Ambos contemplam implementações no *firmware* da BIOS que podem ser utilizadas para executar rotinas de diagnósticos na unidade, cujo objetivo é determinar, com um alto índice de confiabilidade, se o equipamento está funcionando de forma apropriada. Estes diagnósticos estão armazenados em áreas protegidas do disco rígido, para reduzir a possibilidade de contaminação por vírus, corrupção do *software* operacional ou mau uso pelo operador do sistema [Berghel 2007].

O HPA é definido como uma área reservada no disco rígido, projetada para armazenar informações de forma que não possam ser acessadas com os recursos usuais da BIOS, do usuário ou do sistema operacional. Esta área pode conter informações sobre utilitários do disco rígido, ferramentas de diagnóstico e o código de inicialização do equipamento. Uma área adicional disponível nos equipamentos atuais é a DCO que permite, aos fornecedores de sistemas, comprarem unidades de diferentes fabricantes com tamanhos diferentes e conFigurar todos os discos rígidos com o mesmo número de setores para a padronização de procedimentos. Um exemplo de utilização do DCO pode ser um disco de 80GB ser reconhecido como 60GB tanto pela BIOS como pelo sistema operacional [Gupta et al. 2006].

Uma revisão atenta às especificações do padrão ATA (*Advanced Technology Attachment*) e desenvolvimentos recentes da comunidade de *software* livre indicam que estas áreas (HPA e DCO) podem ser acessadas, modificadas e gravadas por utilitários disponíveis sem custo na Internet, possibilitando a ocultação de dados sigilosos [Berghel et al. 2008].

A existência destas áreas também aumenta consideravelmente o risco de que programas de aquisição de imagens não resultem em cópias fidedignas dos discos rígidos de origem e podem conduzir a conclusões incompletas de análises forenses [Gupta et al. 2006]. A proteção de segredos industriais de fabricantes de discos rígidos e montadores de computadores também é um fator adicional de obscuridade para a análise destas áreas como disponíveis para armazenamento de informações.

1.5 Estudos de Caso

Nesta seção serão apresentados quatro estudos de caso, sendo os dois primeiros baseados em casos reais e noticiados na imprensa. Os demais são baseados em casos reais conhecidos pelos autores (com os dados dos envolvidos preservados) ou criados apenas para ilustrar as técnicas abordadas na Seção 1.4. Em todos os quatro foram utilizadas técnicas Antiforense Digital.

Primeiro Caso (Tráfico de drogas)

Este caso será descrito de acordo com as notícias mostradas em [FOLHA 2008], [TERRA 2008] e [INFO 2008]. O traficante de drogas Juan Carlos Ramírez Abadía utilizou a técnica de esteganografia para controlar as rotas do tráfico de drogas e quem deveria ser executado em casos de conflitos.

Agentes da Polícia Federal teriam desconfiado da quantidade de imagens da boneca Hello Kitty que o traficante teria em seu computador. Algumas fontes alegam que havia cerca de duzentas e outras fontes alegam que haveria mais de duzentas imagens e muitas delas foram enviadas por e-mail. Haveria também, fotografias de crianças utilizadas como hospedeiras.

Com a ajuda da Agência Antidrogas dos Estados Unidos, a Polícia Federal teria descoberto o uso da Esteganografia e antes de esconder os arquivos nas imagens de Hello Kitty, estes teriam sido criptografados. Após a quebra da Esteganografia e da Criptografia, foram descobertos arquivos de texto e de áudio com o conteúdo já mencionado.

Pelo que pôde ser observado, houve a desconfiança sobre o uso de esteganografia apenas porque foram utilizadas como hospedeiras imagens da boneca Hello Kitty. Em casos como este, é de extrema importância o papel da investigação que pode ajudar o perito, informando detalhes obtidos durante escutas telefônicas, conversas, depoimentos, etc. Um ofício bem detalhado e uma comunicação mais rica com a perícia podem ser fundamentais em casos como este.

Segundo Caso (Lavagem de dinheiro)

Este caso será descrito de acordo com as notícias mostradas em [G1 2010]. A operação Satiagraha, da Polícia Federal, apreendeu no apartamento do banqueiro Daniel Dantas um computador portátil e seis unidades externas de discos rígidos (HDs). No momento da análise, os peritos constataram que os HDs estavam criptografados.

Segundo a assessoria de Dantas, foram utilizados dois softwares: o PGP e o TrueCrypt, por motivo de suspeita de espionagem. O algoritmo utilizado seria o AES – 256 *bits*. As senhas utilizadas não foram informadas e os peritos da Polícia Federal criaram um dicionário a partir de dados da investigação na tentativa de descoberta da senha através de ataque de dicionário[17].

Após cinco meses de tentativas, foi concedida autorização judicial para envio dos HDs para os Estados Unidos, para que o FBI tentasse quebrar a proteção criptográfica. O FBI teria empregado a mesma técnica de ataque de dicionário e passado um ano informou que não obteve sucesso, devolvendo o material à Polícia Federal.

AES com chave de 256 *bits* é um algoritmo forte, adotado como padrão americano atualmente e, caso não tenha sido utilizada uma senha fraca, levaria dezenas, centenas, milhares ou até mesmo milhões de anos para que se conseguisse descobrir a senha através do ataque de força bruta (já que o ataque do dicionário não obteve êxito). Um detalhe a ser observado é que não existe legislação brasileira que obrigue o réu a informar a senha, nem mesmo há punição caso ele se negue a informá-la.

[17] Técnica de Criptoanálise (quebra de Criptografia) que se baseia na tentativa de busca de senha a partir de um dicionário de palavras conhecidas como possíveis senhas.

Terceiro Caso (Pedofilia)

Sob a acusação de pedofilia, foi cumprido mandado de busca e apreensão na residência de João da Silva Sauro. Foram apreendidos um *notebook* e uma unidade externa de disco rígido (HD). Um detalhe que chamou a atenção é que o HD estava dentro de um guarda-roupa, embaixo de uma pilha de roupas.

Para realizar a análise forense, o perito realizou cópia *bit a bit* do HD encontrado no *notebook* e do HD externo no mesmo caso. Começou a etapa de exame com busca por palavras-chave relacionadas à pedofilia e arquivos excluídos. Diversas ocorrências foram retornadas da busca por palavras-chave, porém, todas fazendo referência a um disco externo, denominado como unidade F: e rótulo "BACKHIDE" (tratava-se de um sistema Windows instalado em um disco com uma única partição, C:, e uma unidade de DVD-RW, D:). Analisando o HD externo, era possível verificar apenas uma partição, com rótulo "BACKUP", porém ocupava apenas cerca de 80% do disco, e o restante era espaço não alocado por partição. O conteúdo binário do espaço não alocado por partição é mostrado na Figura 1.29.

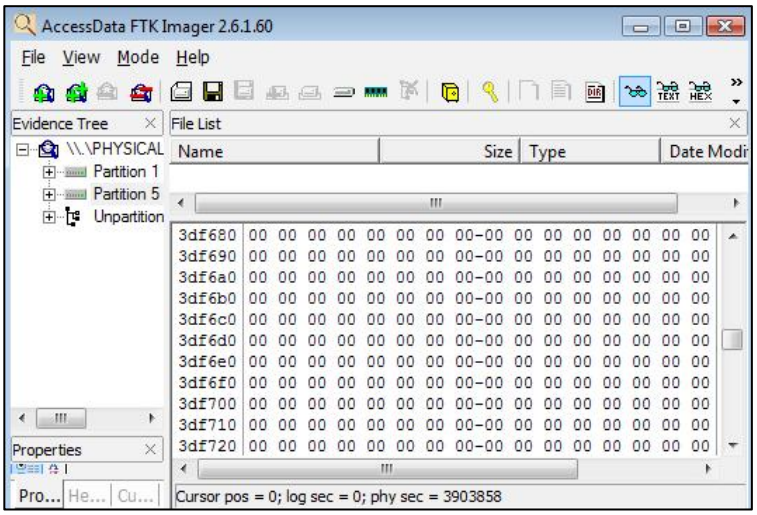


Figura 1.29. Conteúdo binário (notação hexadecimal) da área não alocada pela partição

Não é comum um HD possuir cerca de 20% em área não alocada por partição e totalmente "zerada". Houve suspeita de aplicação de *wiping*, então foi realizada busca pela palavra-chave *wipe* e pelos *softwares* instalados no HD do *notebook*. Foram encontradas diversas buscas no sítio *Google* sobre o assunto e um *download* do software Puran Wipe Disk. Foi realizada busca por *logs* deste *software*, porém sem sucesso. Então foram realizados testes do mesmo para verificar seu funcionamento (Figura 1.30).

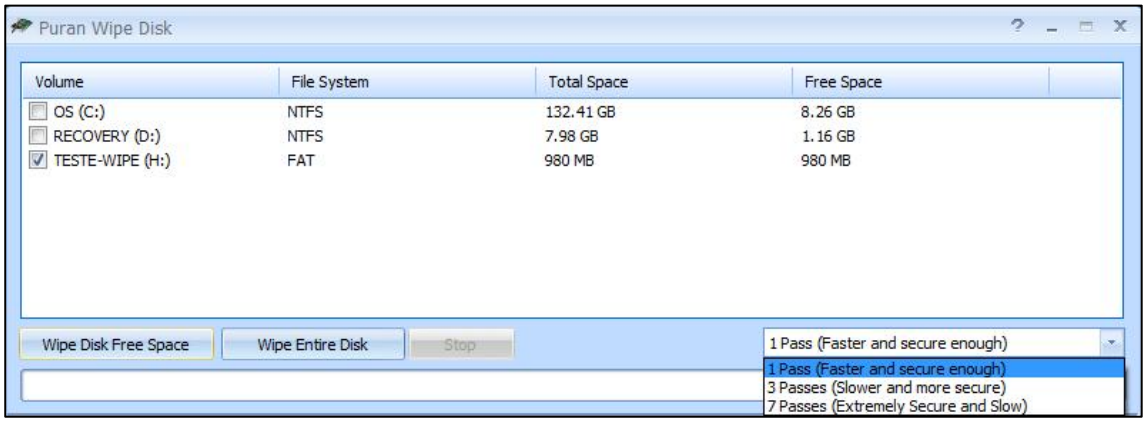
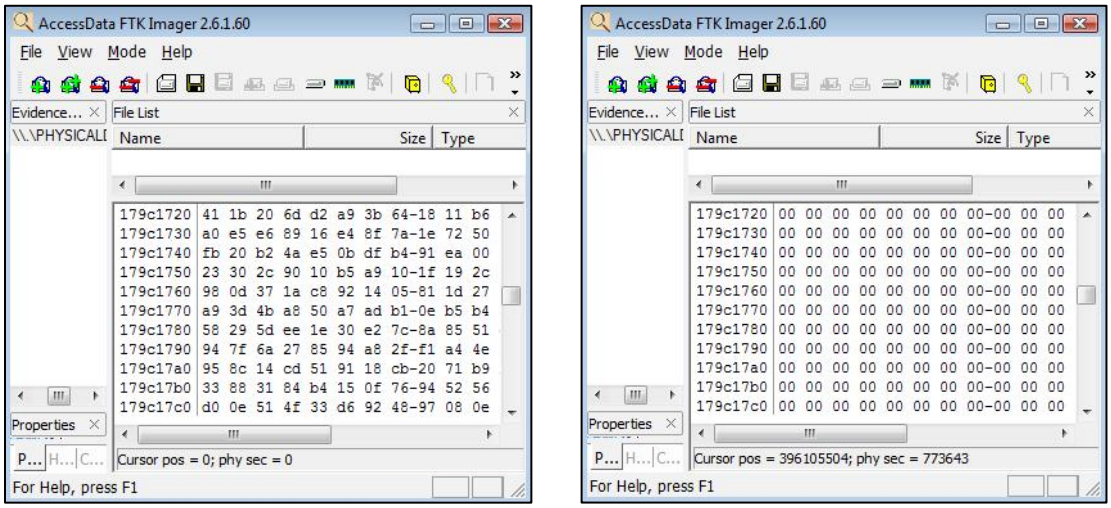


Figura 1.30. Testes do software Puran Wipe Disk

Diante dos testes, foi possível verificar que só havia opção de gravar *bits* zero. A Figura 1.31 mostra o conteúdo do *pendrive* utilizado para teste, antes de depois de aplicado o *wiping*.



(a) Antes de aplicar *Wipe*. (b) Depois de aplicar *Wipe*.

Figura 1.31. Conteúdo do pendrive testado

Diante do que foi exposto, houve indícios da utilização do *software* mostrado para aplicação de *wiping* na área não alocada para partição do HD externo (cerca de 20%). Porém, não foram encontradas evidências. Neste caso, pode-se colocar no Laudo Pericial o experimento realizado e indícios encontrados, mas sem uma conclusão. Para este caso, novas buscas foram realizadas com o foco voltado para a memória virtual (área geralmente esquecida ou de pouco conhecimento de quem aplica *wiping*), onde foram encontrados fragmentos de fotografias relacionados com o objetivo da perícia, os quais foram anexados ao Laudo Pericial.

Quarto Caso (Estelionato)

Sob suspeita de clonagem de cartões de débito e crédito, foi emitido mandado de busca e apreensão para a residência de Floriano Cunha Ambrósio. A polícia civil cumpriu o mandado, recolheu um *notebook*, não encontrando mais nenhuma mídia ou equipamento relacionado com informática no local.

Após realização de cópia *bit a bit*, o perito começou a realizar o exame, através de buscas por palavras-chave e filtros por tipos de arquivos, com a intenção de localizar dados bancários e pessoais (objetivo da perícia), sem sucesso. Então começou a buscar conteúdo de *e-mails*, quando encontrou alguns fragmentos de *e-mail* em unidades de disco não alocadas pelo sistema de arquivos (conteúdo excluído), enviados de xxxxxxxxx@teste.com.br para fca@teste.com.br ("fca" supostamente são as iniciais de Floriano Cunha Ambrósio).

Um dos fragmentos tinha o seguinte trecho: "... os CDs serão enviados por motoboy, um por semana mais ou menos. Copia pro notebook daquele jeito, escondendo...e depois quebra o CD e não coloque no lixo da sua casa! Não deixe rastros!...". Diante deste fragmento de *e-mail*, surgiu a desconfiança de alguma técnica para esconder informações.

Não havia nenhum *software* de Criptografia ou Esteganografia instalado. O sistema de arquivos utilizado nas duas partições era NTFS. Então, o perito começou a analisar os nomes de pastas para ver se alguma poderia ser suspeita. Foi encontrada uma pasta denominada "SDA" contendo oito arquivos de texto pequenos (totalizando apenas 60 bytes), sendo que cinco deles com horário de última modificação às 0h44min e três deles às 1h45min, e mesma data de modificação (Figura 1.32). O conteúdo dos oito arquivos foi visualizado (Figura 1.33) e, pela intuição do perito, havia algo no mínimo estranho.

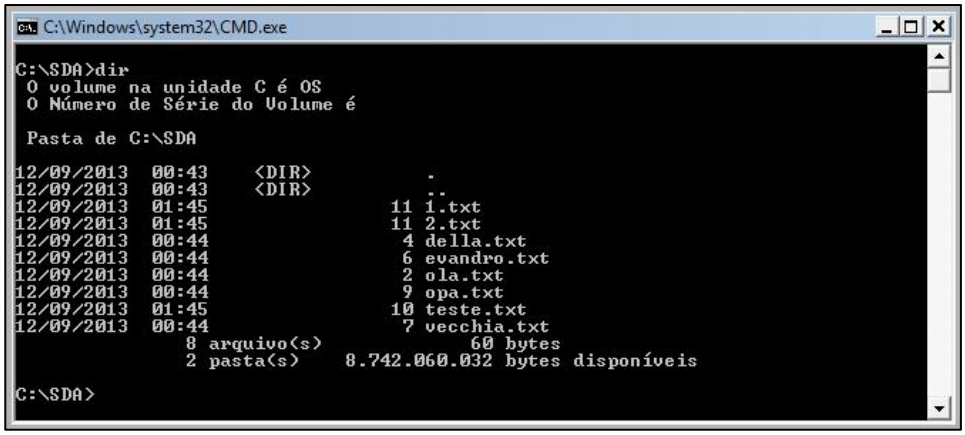


Figura 1.32. Lista dos arquivos localizados em "C:\SDA"

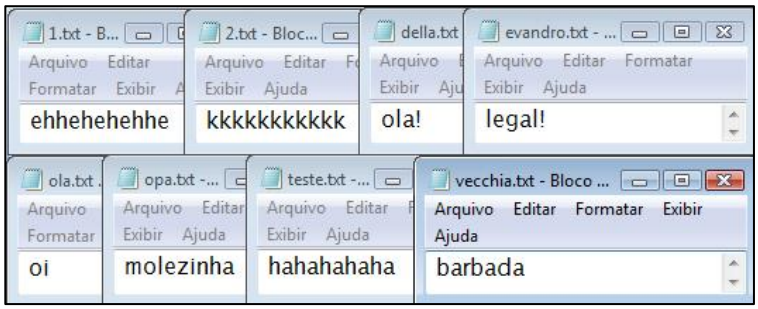


Figura 1.33. Conteúdo dos oito arquivos localizados em "C:\SDA"

A suspeita do perito passou a ser o uso de ADS, por três motivos: o fragmento de *e-mail* já mencionado, os horários de modificação e pouco conteúdo armazenado nos oito arquivos e por fim o nome da pasta (ADS invertido, ou seja, SDA). Há um

parâmetro para o comando DIR que mostra quando foi aplicado ADS, o "/r". Como mostra a Figura 1.34, foram encontrados três arquivos escondidos, totalizando mais de 1,5 MiB. Estes arquivos foram visualizados com o editor de textos *Write* e constatou-se que possuíam dados bancários para utilização em cartões de débito e crédito (Figura 1.35).

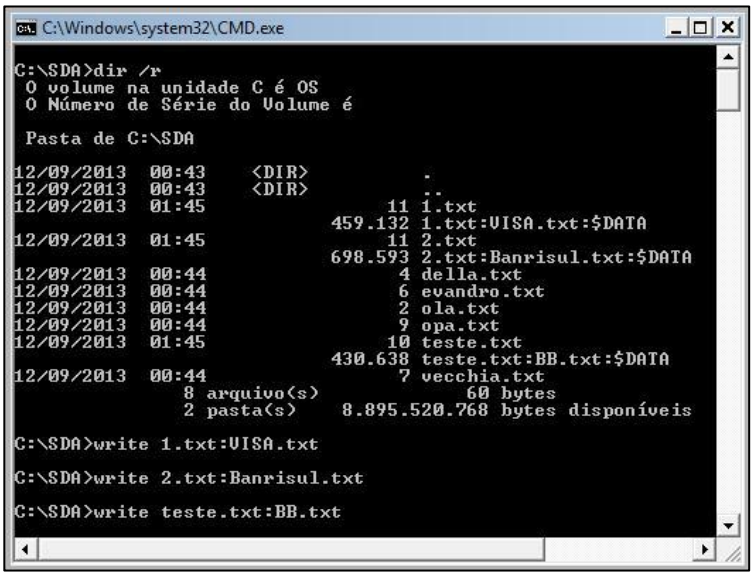


Figura 1.34. Visualização dos arquivos escondidos

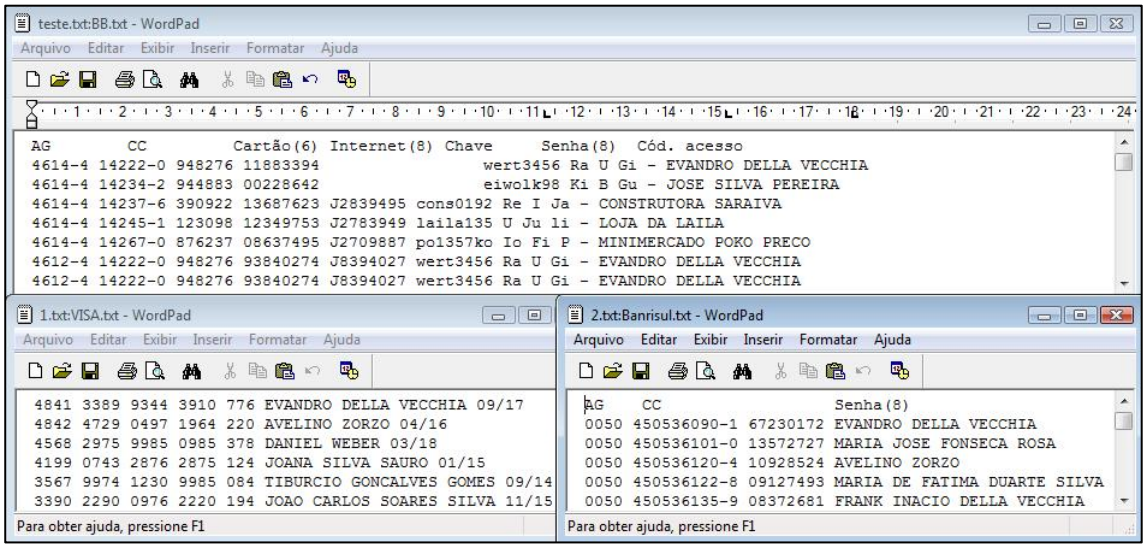


Figura 1.35. Conteúdo dos três arquivos escondidos localizados em "C:\SDA"

1.6 Considerações Finais

Este capítulo apresentou, inicialmente, uma pequena introdução sobre Forense Digital, para após introduzir o assunto principal, a Antiforense Digital. Foram mostrados os conceitos de como é possível buscar garantir a confidencialidade de informações sensíveis, assim como formas que criminosos podem utilizar para esconder, confundir ou destruir informações para dificultar ou impossibilitar a análise pericial.

Após a apresentação de conceitos, foram mostradas técnicas e ferramentas para as principais aplicações de Antiforense Digital: destruição e proteção de dados. Com

relação à destruição, foram abordadas técnicas de destruição físicas e lógicas. As físicas são muito utilizadas em órgãos que possuem informações sensíveis no momento de descarte de mídias, já as lógicas são utilizadas mais por usuários domésticos. Com relação à proteção dos dados, as técnicas mais conhecidas, e abordadas, foram: Criptografia e Esteganografia. As menos conhecidas: ADS, *slackering*, HPA e DCO, mostraram quanta informação pode estar contida em uma mídia e passar despercebida por quem está investigando um incidente. Com exceção de ADS, que possui ferramentas nativas no Windows que permitem sua aplicação, as demais são pouco exploradas e é difícil encontrar algum *software* que aplique essas técnicas.

Por fim, foram mostrados quatro estudos de caso, dois retirados de notícias e dois baseados na experiência dos autores. Estes casos mostram um pouco do trabalho do perito digital, que cada vez mais precisa ter conhecimento de como os infratores estão utilizando técnicas antiforense.

Este capítulo teve como objetivos mostrar as diferentes formas que um usuário pode proteger suas informações de pessoas que não possuem autorização para visualizá-las e também esclarecer peritos que estão iniciando na carreira sobre algumas técnicas utilizadas por criminosos para esconder informações sobre seus crimes.

Nunca é demais salientar que este capítulo apresentou somente alguns exemplos de técnicas e ferramentas e muitas outras existem e estão disponíveis atualmente. Além disto, o acesso a estas ferramentas e técnicas está cada vez mais fácil e portanto cada vez mais pessoas comuns as utilizarão. Desde o início do ano de 2013 quando os jornais e revistas aumentaram a divulgação do acesso de informações de governos e grandes empresas pela NSA dos Estados Unidos da América, muita discussão tem sido gerada em relação a forma como informações podem facilmente ser acessadas. Existe uma tendência de que as pessoas passem a se preocupar mais com o armazenamento de suas informações de maneira protegida, ou seja, se troque a maneira de utilizar o computador de forma despreocupada com a segurança, para uma forma onde as pessoas se preocupem mais em se comunicar ou armazenar suas informações de maneira segura.

Referências

[AUTOPSY 2013] AUTOPSY (2013). *Autopsy: Download*. Disponível em http://www.sleuthkit.org/autopsy/download.php. Acesso em: Set. 2013.

[Bender et al. 1996] Bender, W., Gruhl, D., Morimoto, N. e Lu, A. (1996). *Techniques for data hiding*. IBM Systems Journal, Vol. 35(3-4). Páginas 313–336.

[Berghel 207] Berghel, H. (2007). *Hiding Data, Forensics and Anti-Forensics*. Communications of the ACM, Vol. 50(4). Páginas 15-20.

[Berghel et al. 2008] Berghel, H., Hoelzer, D. e Sthultz, M. (2008). *Data Hiding Tactics for Windows and Unix File Systems*. Advances in Computers. Páginas 1-17.

[Berinato 2007] Berinato, S. (2007). *The Rise of Anti-Forensics*. CSO Security and Risk. Disponível em: http://www.csoonline.com/article/221208/the-rise-of-anti-forensics. Acesso em: Set. 2013.

[Brezinksi e Killalea 2002] Brezinski, D. e Killalea, T. (2002). *Evidence Collection and Archiving*. Disponível em: www.ietf.org/rfc/rfc3227.txt. Acesso em: Set. 2013.

[Carrier 2005] Carrier, B. (2005). *File System Forensic Analysis*. Addison Wesley Professional.

[Carvey 2009] Carvey, H. (2009). *Windows Forensic Analysis. DVD Toolkit*. Syngress. 2nd Edition.

[Cole 2003] Cole, E. (2003). *Hiding in Plain Sight: Steganography and the Art of Covert Communication. "*. John Wiley and Sons.

[DBAN 2013] DBAN (2013). *Darik's Boot And Nuke*. Disponível em: http://www.dban.org. Acesso em: Set. 2013.

[Dillon 1999] Dillon, H. (1999). *Forensic scientists: A career in the crime lab*. Disponível em: http://www.bls.gov/opub/ooq/1999/Fall/art01.pdf. Acesso em: Set. 2013.

[DOD 2001] DOD - Department of Defense (2001). *Disposition of Unclassified DOD Computer Hard Drives*. Disponível em: <http://technology.iusm.iu.edu/index.php/download_ file/view/16/140/&ei=ohEoUvPMCpSC9gTX9YGoCA&usg=AFQjCNEXszLADm DaFzmhY5V0F81OJYYP4Q&sig2=zFGmDM1WvLe0wNthTDZSxw&bvm=bv.517 73540,d.eWU>. Acesso em: Set. 2013.

[Eckert 1997] Eckert, W. (1997). *Introduction to Forensic Sciences*. CRC Press (Originally published: New York: Elsevier, 1992).

[EDT 2006] EDT (Ensconce Data Technology, Inc.) (2006). *Self-Inflicted Security Breaches Through Effective Hard Drive Sanitization*. Disponível em: <http://www.deadondemand.com/assets/documents/whitepapers/avoiding_self_inflic ted_security_breaches.pdf>. Acesso em: Set. 2013.

[Feenberg 2003] Feenberg, D. (2003). *Can Intelligence Agencies Read Overwritten Data? A response to Gutmann*. Disponível em: http://www.nber.org/sys-admin/overwritten-data-guttman.html. Acesso em: Set. 2013.

[Folha 2008] Folha (2008). *Para agência dos EUA, Abadía traficou no Brasil*. Disponível em http://www1.folha.uol.com.br/fsp/cotidian/ff1003200801.htm. Acesso em: Set. 2013.

[G1 2010] G1 (2010). *Nem FBI consegue decifrar arquivos de Daniel Dantas, diz jornal*. Disponível em http://g1.globo.com/politica/noticia/2010/06/nem-fbi-consegue-decifrar-arquivos-de-daniel-dantas-diz-jornal.html. Acesso em: Set. 2013.

[G1 2013] G1 (2013) "Após fotos íntimas pararem na web, mulher diz sofrer preconceito diário". Disponível em <http://g1.globo.com/pr/norte-noroeste/noticia/2013/08/apos-fotos-intimas-pararem-na-web-mulher-diz-sofrer-preconceito-diario.html>. Acesso em: Set. 2013.

[Garfinkel 2007] Garfinkel, S. (2007). *Anti-Forensics: Techniques, Detection and Countermeasures*. 2nd International Conference on i-Warface and Security. Disponível em: http://www.simson.net/clips/academic/2007.ICIW.AntiForensics.pdf. Acesso em: Set. 2013.

[Garfinkel e Shelat 2003] Garfinkel, S. L. e Shelat, A. (2003). *Remembrance of data passed: a study of disk sanitization practices*. IEEE Security & Privacy. Vol. 1(1). Páginas 17-27.

[Government of Canada 2006] Government of Canada (2006). *Clearing And Declassifying Electronic Data Storage Devices*. Communications Security Establishment. Disponível em: http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg06-eng.pdf. Acesso em: Set. 2013.

[Gupta et al. 2006] Gupta, M. R, Hoeschele, M. D. e Rogers M. K. (2006). *Hidden Disk Areas: HPA and DCO*. International Journal of Digital Evidence, Vol. 5, Issue 1. Disponível em: http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE36584-D13F-2962-67BEB146864A2671.pdf. Acesso em: Set. 2013.

[Gutmann 1996] Gutmann, P. (1996). *Secure Deletion of Data from Magnetic and Solid-State Memory*. Sixth USENIX Security Symposium. Disponível em https://www.usenix.org/legacy/publications/library/proceedings/sec96/full_papers/gutmann/. Acesso em: Set. 2013.

[Gutmann 2004] Gutmann, P. (2004). *Cryptographic Security Architecture: Design and Verification*. NewYork: Springer-Verlag.

[Hannan 2004] Hannan, M. (2004). *To Revisit: What is Forensic Computing?* 2nd Australian Computer Network & Information Forensics Conference.

[Harris 2006] Harris, R. (2006). *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem*. Digital Investigation, Vol. 3. Páginas 44–49. Elsevier.

[HEIDE 2013] HEIDI COMPUTERS LIMITED (2013). *About Heidi Computers*. Disponível em: http://heidi.ie/eraser/faq.php. Acesso em: Set. 2013.

[HIDE 2010] HIDE (2010). *Hide & Reveal*. Disponível em http://hidereveal.ncottin.net/. Acesso em: Set. 2013.

[Hughes et al. 2009] Hughes, G., Coughlin, T. e Commins, D. (2009). *Disposal of Disk and Tape Data by Secure Sanitization*. IEEE Security & Privacy. Vol. 7(4). Páginas 29-34.

[INFO 2008] INFO (2008). *Abadía usou e-mail cifrado para traficar*. Disponível em http://info.abril.com.br/aberto/infonews/032008/10032008-3.shl. Acesso em: Set. 2013.

[James 2006] James, D. (2006). *Forensically Unrecoverable Hard Drive Data Destruction*. Infosec Writers. Disponível em: http://www.infosecwriters.com/text_resources /pdf/Hard_Drive_DJames.pdf. Acesso em: Set. 2013.

[Jardim 2013] Jardim, W. F. (2013). Gerenciamento de Resíduos Químicos. Universidade Estadual de Campinas – UNICAMP. Disponível em: http://lqa.iqm.unicamp.br/pdf/ LivroCap11.PDF. Acesso em: Set. 2013.

[JETICO 2013] JETICO (2013). *BestCrypt Container Encryption*. Disponível em: http://www.jetico.com/products/enterprise-data-protection/bestcrypt-container-encryption. Acesso em: Set. 2013.

[Johnson e Jajodia 1998] Jonhson, N. e Jajodia, S. (1998). *Exploring Steganography: Seeing the Unseen*. IEEE *Computer*. Vol. 31(2). Páginas 26-34

[Kemp e Smith 2005] Kemp, B. M. e Smith, D. G. (2005). *Use of bleach to eliminate contaminating DNA from the surface of bones and teeth*. Forensic Science International, Vol. 154. Páginas 53-61. Disponível em: http://public.wsu.edu/~bmkemp/publications/pubs/ Kemp_and_Smith_2005.pdf. Acesso em: Set. 2013.

[Kent et al. 2006] Kent, K., Chevalier, S., Grance, T. e Dand, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response - Recommendations of the National Institute of Standards and Technology*. Disponível em <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>. Acesso em: Set. 2013.

[Kissel et al. 2012] Kissel, R., Scholl, M., Skolochenko, S. e Li, X. (2012). *Guidelines for Media Sanitization Recommendations of the National Institute of Standards and Technology*. Disponível em: <http://permanent.access.gpo.gov/ gpo29126/sp800-88-r1-draft.pdf>. Acesso em: Set. 2013.

[Lopes et al. 2006] Lopes, M., Gabriel, M. e Bareta, G. (2006). Cadeia de Custódia: Uma Abordagem Preliminar. Disponível em: http://ojs.c3sl.ufpr.br/ojs2/index.php/ academica/article/viewFile/9022/6315. Acesso em: Set. 2013.

[LUFTECH 2013] LUFTECH (2013). Incineradores. Disponível em: http://www.luftech.com.br/arquivos/ incinerador.htm. Acesso em: Set. 2013.

[Mamun et al. 2007] Mamun, A., Guo, G. e Bi, C. (2007). *Hard Disk Drive - Mechatronics and Control*. CRC Press.

[MAX@ 2013] MAXQ (2013). *DeepCover Secure Microcontroller with Rapid Zeroization Technology and Cryptography*. Disponível em: http://www.maximintegrated.com/. Acesso em: Set. 2013.

[Means 2003] Means, R. L (2003). *Alternate Data Streams: Out of the Shadows and into the Light*. SANS Institute. Disponível em: http://wwwens.uqac.ca/~flemieux/INF341/ NTFS_Stream.pdf. Acesso em: Set. 2013.

[Mukasey et al. 2001] Mukasey, M. B., Sedgwick, J. L. e Hagy, D. W. (2001). *Electronic Crime Scene Investigation: A Guide for First Responders. U.S. Department of Justice - 2nd Edition*. Disponível em: http://www.ncjrs.gov/pdffiles1/nij/219941.pdf. Acesso em: Set. 2013.

[Nolan et al. 2005] Nolan, R., O'Sullivan, C., Branson, J. e Waits, C. (2005). *First Responders Guide to Computer Forensics*. CERT Training and Education. Disponível em: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf. Acesso em: Set. 2013.

[NSA 2012] NSA - NATIONAL SECURITY AGENCY (2012). *Evaluated Products List - Degausser*. Disponível em: http://www.nsa.gov/ia/_files/Government/MDG/EPL_ Degausser25June2012.pdf. Acesso em: Set. 2013.

[NSA 2013] NSA - National Security Agency (2013). *NSA/CSS Storage Device Declassification Manual*. Disponível em: http://www.nsa.gov/ia/_files/Government/MDG/NSA_ CSS_Storage_Device_Declassification_Manual.pdf. Acesso em: Set. 2013.

[NXP 2013] NXP (2013). *Designed for high-security smart card applications requiring highly reliably solutions*. Disponível em: http://www.nxp.com/products/identification_and_ security/smart_card_ics/smartmx_contact_interface_controllers/. Acesso em: Set. 2013.

[O'Handley 2000] O'Handely, R. C. (2000). *Modern Magnetic Materials: Principles and Applications"*. John Wiley and Sons.

[Peron e Legary 2008] Peron, C. S. J. e Legary, M. (2008). *Digital anti-forensics: emerging trends in data transformation techniques*. Seccuris Labs. Disponível em: http://www.ide.bth.se/~andersc/kurser/DVC013/PDFs/Seccuris-Antiforensics.pdf. Acesso em: Set. 2013.

[Piper e Murphy 2002] Piper, F. e Murphy, S. (2002). *Cryptography: A Very Short Introduction*. Oxford University Press.

[Presidência 2012] Presidência da República (2012) "LEI Nº 12.737, Dispõe sobre a tipificação criminal de delitos informáticos". Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: Set. 2013.

[SEM 205] SEM – Security Engineered Machinery (2005). *Hard Drive Destruction Model 22 HDD SEM*. Disponível em: http://www.semshred.com/stuff/contentmgr/files/ 0/769bebc6af6e4daa2fc2bc4847db9370/folder/Model%2022HDD%200705.pdf. Acesso em: Set. 2013.

[Shah 2008] Shah, A. (2008). *Laptops Lost Like Hot Cakes At US Airports*. CIO Magazine. Disponível em: http://www.cio.com/article/418163/Laptops_Lost_Like _Hot_Cakes_At_US_Airports. Acesso em: Set. 2013.

[Slade 2004] Slade, R. (2004). *Software Forensics: Collecting Evidence from the Scene of a Digital Crime*". McGraw-Hill Professional.

[Steel 2006] Steel, C. (2006). *Windows Forensics: The Field Guide for Corporate Computer Investigations*. John Wiley and Sons.

[Sutherland et al. 2008] Sutherland, I., Evans, J., Tryfonas, T. e Blyth, A. (2008). *Acquiring Volatile Operating System Data Tools and Techniques*. ACM SIGOPS Operating Systems Review. Vol. 42(3). Páginas 65-73.

[TECHNET 2003] TECHNET - Microsoft Corporation (2003). *How NTFS Works*. Disponível em: http://technet.microsoft.com/en-us/library/cc781134.aspx. Acesso em: Set. 2013.

[TERRA 2008] TERRA (2008). *Abadia usava Hello Kitty para enviar ordens*. Disponível em http://noticias.terra.com.br/brasil/noticias/0,,OI2666590-EI5030,00-Abadia+usava+Hello+Kitty+para+enviar+ordens.html. Acesso em: Set. 2013.

[TRUECRYPT 2013] TRUECRYPT (2013). *Truecrypt*. Disponível em: http://www.truecrypt.org. Acesso em: Set. 2013.

[Ulbrich e Valle 2004] Ulbrich, H. C. e Valle, J. D. (2004). Universidade H4ck3r. São Paulo: Digerati, 4th Edition.

[USAID 1995] USAID (1995). *DoD 5220.22-M National Industrial Security Program Operating Manual*. Disponível em: http://transition.usaid.gov/policy/ads/500/d522022m.pdf. Acesso em: Set. 2013.

[US-CERT 2008] US-CERT (2008). *Computer Forensics*. Disponível em: http://www.us-cert.gov/reading_room/forensics.pdf. Acesso em: Set. 2013.

[Wang e Wang 2004] Wang, H. e Wang, S. (2004). *Cyber Warfare: Steganography vs. Steganalysis*. Communications of the ACM - Voting systems, Vol. 47(10). Páginas 76-82.

[Zadjmool 2004] Zadjmool, R. (2004). *Hidden Threat: Alternate Data Streams*. Disponível em: http://www.windowsecurity.com/articles/Alternate_Data_Streams.html. Acesso em: Set. 2013.

