UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

RAMIRO WEBBER DIMER

PERÍCIA FORENSE COMPUTACIONAL APLICADA A AMBIENTES NEW TECHNOLOGIES FILE SYSTEM (NTFS)

CRICIÚMA, DEZEMBRO DE 2007.

RAMIRO WEBBER DIMER

PERÍCIA FORENSE COMPUTACIONAL APLICADA A AMBIENTES NEW TECHNOLOGIES FILE SYSTEM (NTFS)

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA, DEZEMBRO DE 2007.

RAMIRO WEBBER DIMER

PERÍCIA FORENSE COMPUTACIONAL APLICADA A AMBIENTES NEW TECHNOLOGIES FILE SYSTEM (NTFS)

Submetido ao corpo docente do Departamento de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de bacharel em Ciência da Computação.

Prof[a] MSc. Ana Cláudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

Prof. MSc. Paulo João Martins (UNESC)
Orientador

Prof. M.Sc. Alfredo Engelmann Filho (UNESC)

Prof. MSc. Rogério Antônio Casagrande (UNESC)

Dedico esta conquista a meus pais, que estiveram sempre presentes incentivando na busca dos meus ideais.

AGRADECIMENTOS

Agradeço essa conquista aos meus pais, Édna Dimer Webber Dimer e Silvio Maia Dimer, que sempre presentes, me incentivaram a lutar por meus objetivos. Aos meus irmãos mais novos, Nádia Webber Dimer e Douglas Webber Dimer, pela alegria e carinho dedicados. Que eu seja um bom exemplo para eles e agradeço a toda família pelo apoio incondicional.

Agradeço também aos meus amigos, que sempre apoiaram e deram a força para continuar na caminhada sem desanimar, em especial ao Pedro Paulo Alexandrino e ao Ânderson Willian Zanelatto, companheiros, quase irmãos. À minha namorada, pela compreensão e por estar sempre presente nos momentos mais difíceis, acolhendo e incentivando-me.

Ao orientador Paulo João Martins por ter me direcionado e mostrado o caminho para desenvolver esse trabalho e ao amigo e incentivador Marco Antonio Torrez Rojas, presente desde o início do trabalho, auxiliando sempre que possível.

À todos os meus professores, pela educação e por me mostrarem o caminho da busca pelo saber e a todos da comunidade cientifica que me proporcionaram, a obtenção de uma enorme gama de conhecimento.

Agradeço também a todas as pessoas que não mencionei, mas que direta ou indiretamente estiveram envolvidas nessa conquista.

RESUMO

O aumento dos crimes praticados por meio do computador torna cada vez mais importante a busca de métodos para combate aos chamados: crimes digitais. Com a adaptação dos criminosos ao ambiente digital, as evidências digitais ganham importância por meio da perícia forense computacional. A manipulação e o tratamento correto dessas evidências são de extrema importância para que o resultado da perícia seja aceito e utilizado de forma segura em um tribunal de justiça. Neste trabalho, serão apresentados métodos para a preservação, busca e a análise das evidências em ambientes New Technologies File System, assim como ferramentas que podem ser utilizadas com segurança na perícia forense, proporcionando clareza e transparência para que a mesma seja considerada válida.

Palavras Chaves: Perícia Forense Computacional, Segurança da informação, Crimes Digitais, Sistema de arquivos NTFS.

ABSTRACT

The increase of crimes practiced by computer means makes more and more important the search of methods against the so called: digital crimes. Due to the adaptation of criminals into the digital environment, the digital evidences earn importance through the computational forensic techniques. The correct manipulation and handling of those evidences are of extreme importance so that the result of the investigation can be accepted and utilized securely in a court of justice. On this assignment, preservation approaches, search and analysis of the evidences in New Technologies File System environments will be presented, as well as tools which can be utilized securely in the forensic techniques, providing explicitness and rectitude for the same be considered valid.

Keywords: Computer Forensic, Security of information, Cybercrime, NTFS File System.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

ACE	Access Control Entry
ACL	Access Control List
ADS	Alternate Data Streams
CPU	Central Processing Unit
CUI	Console User Interface
DLL	Dynamic-Link Library
DOS	Disk Operating System
EFS	Encrypting File System
FAT	File Allocation Table
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Identification
IP	Internet Protocol
KB	Kilobyte
MFT	Master File Table
NTFS	New Technologies File System
NTRK	NT Resource Kit
RAM	Random Access Memory
SID	Security Identifier
TCP	Transmission Control Protocol

SUMÁRIO

1 INTRODUÇÃO

Com o aumento substancial do uso da Internet, vários serviços passaram a ser disponibilizados em meio eletrônico. Bancos, escolas, órgãos públicos têm seus sites na Internet, oferecendo ao usuário a comodidade de efetuar transações e fazer consultas às informações de qualquer ponto de acesso à Internet.

Comumente as pessoas armazenam arquivos pessoais em computadores, fazem negócios pela Internet e utilizam a tecnologia disponível no trabalho profissional. Todas essas questões fazem com que os criminosos se adaptem à uma forma de crime mais recente, os crimes digitais. Esses têm o objetivo de extrair informações sigilosas, causando: roubo de informações proprietárias, infiltrações em sistemas, fraudes financeiras, aumento de privilégios indevidos ao sistema, instalação de programas maliciosos.

Amplamente conhecido e utilizado (CHOFFNES; DEITEL; DEITEL, 2005), o sistema de arquivos NTFS é um dos sistemas alvo dos criminosos. Esses interceptam informações que trafegam na rede, disseminam vírus e pesquisam dados contidos em máquinas vulneráveis. Muitas vezes, esses criminosos utilizam-se de técnicas para impedir a sua identificação, com o objetivo de ficarem impunes perante a lei. Independentemente do cuidado do criminoso, inevitavelmente ele deixará algumas evidências sobre as suas atividades. Essas evidências podem ser examinadas e serem usadas contra o suspeito, por exemplo, em um tribunal de justiça.

O processo de coleta, preservação, análise e apresentação dessas evidências é denominado perícia forense computacional.

Dessa forma, esse trabalho faz uma explanação sobre o método de busca, preservação e análise de evidências em sistemas de arquivos NTFS, tendo em vista a identificação e possível punição do invasor.

1.1 OBJETIVO GERAL

Aplicar técnicas computacionais forenses de duplicação pericial, recuperação de dados para a busca e análise de evidências em ambientes baseados em sistemas de arquivo New Technologies File System (NTFS).

1.2 OBJETIVOS ESPECÍFICOS

São objetivos específicos deste trabalho:

a) compreender aspectos básicos sobre o sistema de arquivos NTFS;
b) entender os principais passos na perícia forense computacional em ambientes NTFS;
c) identificar os principais aspectos de segurança em ambientes NTFS que serão relevantes ao enfoque da pesquisa;
d) abordar a busca, preservação e análise de evidências no sistema de arquivos NTFS;
e) analisar os vários aspectos que envolvem a análise de evidências na perícia forense em ambientes NTFS de maneira geral;
f) enumerar possíveis evidências da memória secundária (*Hard Disk*), de ambientes NTFS;

g) realizar estudo de caso, aplicando as técnicas computacionais forense estudadas, na memória secundária (*Hard Disk*), em ambiente NTFS.

1.3 JUSTIFICATIVA

Ainda alguns crimes são resolvidos usando evidências como: impressões digitais, pegadas, documentos de papel e outros itens tangíveis extraídos da cena do crime. Com a popularização da tecnologia, a evidência digital também pode ser utilizada para este fim. Essa, muitas vezes, pode ser mais proveitosa que uma impressão digital (SCHWEITZER, 2003).

Ainda segundo Schweitzer (2003) os profissionais da lei estão reconhecendo evidências providas do computador e que podem ser incluídas como ponto chave na solução de certos crimes. Com o aumento da importância da evidência digital, cresce ainda mais a importância de que a evidência seja corretamente tratada e examinada.

Tendo como base, o sistema de arquivos NTFS, que é amplamente utilizado (CHOFFNES; DEITEL; DEITEL, 2005), porém, carente de estudos que abordam as técnicas forenses corretas, este trabalho vem a contribuir e suprir essa carência, por meio da pesquisa e aplicação das técnicas de busca, preservação e análise das evidências no ambiente NTFS.

1.4 ESTRUTURA DO TRABALHO

A presente pesquisa tem como meta demonstrar de maneira prática a análise das evidências em um ambiente NTFS. Para tanto, o trabalho é dividido em duas

grandes partes: a primeira abordando a base teórica dos objetos de estudo e a segunda a parte prática, que é baseada na fundamentação teórica apresentada, simulando um ambiente real.

O primeiro capítulo aborda a perícia forense computacional de modo geral, explanando sobre evidências digitais, o modo como encontrar e preservá-las. O capítulo seguinte apresenta o sistema de arquivos NTFS, sua estrutura e questões sobre a segurança nesse ambiente. O terceiro capítulo mostra a teoria sobre o modo de conduzir uma perícia forense em um ambiente NTFS, locais onde as evidências são encontradas, cuidados necessários e resultados que podem ser obtidos. E completando o trabalho, a parte prática, que utiliza um computador pessoal para a prática da fundamentação teórica apresentada no decorrer da pesquisa.

2 PERÍCIA FORENSE COMPUTACIONAL

Os incidentes de segurança estão presentes em muitas organizações, ocorrem até mesmo com usuários domésticos, por meio do roubo de senhas, número de cartões de crédito e violação de informações sigilosas.

Segundo Vacca (2002) a perícia forense computacional é a coleta, preservação, análise e apresentação de evidências. Consiste, portanto, no uso de métodos científicos e ferramentas apropriadas para desenvolver corretamente a pesquisa, que trará como resultado, conclusões sobre o incidente investigado, apresentando os fatos e as evidências.

Em relação ao objetivo final da forense computacional, existem duas abordagens. Na primeira, a perícia forense busca por evidências com valor jurídico com o objetivo de serem utilizadas em um processo criminal. Na segunda abordagem, a perícia forense é aplicada dentro da organização com o objetivo de determinar a causa de um incidente e suprir as deficiências para que ele não ocorra novamente. Esta segunda abordagem não se preocupa com as formalidades legais, é apenas um procedimento interno da organização para aperfeiçoar-se.

Mesmo a perícia enquadrando-se na segunda abordagem, sem a intenção de se lançar um processo criminal, a investigação deve abranger a utilização de metodologias padrões, para garantir a possível aceitação em uma corte de justiça.

Os aspectos que devem ser observados quanto ao processo de perícia forense em um sistema operacional (CASEY, 2004):

a) coleta de informações;

b) reconhecimento das evidências;

c) coleta, restauração, documentação e preservação das evidências encontradas;

d) correlação das evidências;

e) reconstrução dos eventos.

As informações referentes ao incidente, devem ser coletadas, as evidências devem ser identificadas, extraídas, documentadas e preservadas. Assim, as evidências podem ser correlacionadas para a reconstrução dos acontecimentos relacionados ao incidente em questão (CASEY, 2004).

2.1 EVIDÊNCIAS DIGITAIS

Em um ambiente computacional, um criminoso sempre deixará vestígios de sua passagem. Mesmo os mais cuidadosos, que tratam de apagar ou despistar seus rastros, deixam seus vestígios. Nesse caso os vestígios podem ser muito difíceis ou impossíveis de serem encontrados.

A evidência digital é definida como qualquer dado armazenado ou transmitido utilizando-se um computador, que pode provar ou negar a teoria de como ocorreu um crime, intenção ou álibi (CASEY, 2004). Estabelecendo uma relação entre o crime e a vítima e a vitima ou um crime e um criminoso.

A evidência digital é formada por campos magnéticos e pulsos eletrônicos que podem ser coletados e analisados utilizando-se das técnicas e ferramentas corretas. Contudo, a evidência possui características que são próprias das “provas” digitais e que remetem confiabilidade ao trabalho do perito (CASEY, 2004):

a) podem ser duplicadas com precisão, permitindo a integridade da evidência original durante o processo de análise;

b) é possível identificar se uma evidência foi modificada;

c) mesmo quando o arquivo é “excluído” ou o disco rígido é formatado, a informação ainda permanece no local, podendo facilmente ser recuperada;

d) cópias de evidências destruídas podem estar presentes em outros locais, como em cópias de segurança.

Em um sistema operacional, a busca pelas evidências, é o ato de examinar minuciosamente os dados que nele se encontram. São analisados os dispositivos de armazenagem, como o disco rígido e a memória principal, entre outros, como o tráfego de rede.

Uma característica dos sistemas computacionais que deve ser observada antes de se iniciar a busca por evidências é a ordem de volatilidade dos meios onde se encontram. A análise deve seguir uma ordem de busca, sempre iniciando-se pelos meios mais voláteis, caso contrário, informações importantes ao caso estudado poderão ser perdidas. Mohay, et al. conceituam a ordem de volatilidade, que é apresentada na ordem descendente:

a) dispositivos de armazenagem da Central Processing Unit (CPU) (registradores e *caches*);

b) memória do sistema (virtual e física);

c) tráfego de rede;

d) estado do sistema operacional (como, por exemplo, estado das conexões de rede e dos processos em execução, usuários identificados no sistema);

e) sistema lógico de arquivos;

f) dispositivos de armazenagem secundária (um deles, o disco rígido);

g) CD-ROMs e páginas impressas.

Mesmo essa ordem sendo rigorosamente seguida, não garante a integridade das informações, pois a simples análise em um meio extremamente volátil, como dos registradores da CPU, pode sobrescrever os dados contidos nesse, tornando-os irrelevantes.

2.1.2 Dispositivos de Armazenagem da CPU

Os dados contidos nos registradores da CPU são de pouca utilidade na investigação, pois nem sempre remetem às informações relacionadas ao caso, sua recuperação torna-se quase que impossível. A memória *cache*[1] pode incluir dados que ainda não tenham sidos atualizados na memória principal e sejam relevantes à perícia (MOHAY, 2003).

2.1.3 Memória de Periféricos

Diversos dispositivos periféricos como *modems*[2], *pagers*[3], aparelhos de fax e impressoras, possuem memórias que podem ser lidas e gravadas. Essas memórias podem conter dados que não mais se encontram no sistema operacional. Um exemplo é que, em uma análise da memória de uma impressora, é possível encontrar documentos, ou parte deles, que poderão não ser encontrados no sistema analisado (SHINDER, 2002).

---

[1] Seção de memória de alta velocidade que armazena dados que o computador pode acessar rapidamente (MICHAELIS, 1998).

[2] Modulador/Demodulador. Dispositivo que permite que dados sejam enviados via telefone por meio da conversão de sinais binários de um computador em sinais analógicos de som que podem ser transmitidos via uma linha telefônica (MICHAELIS, 1998).

[3] Dispositivo pequeno transportado por alguém, que permite ser chamado de um escritório central, por meio de um sinal de rádio (MICHAELIS, 1998).

2.1.4 Memória Principal do Sistema

A memória principal do sistema contém dados importantes à perícia. Segundo Mohay, et al. ela contém todo o tipo de dados voláteis, como exemplo, dados dos processos que estão sendo executados, dados que estão sendo manipulados e que possivelmente ainda não foram salvos no disco, além das informações do sistema operacional. Agregando essas informações à outras coletadas no sistema, a análise torna-se mais confiável e menos sujeita a falhas.

2.1.5 Tráfego de Rede

A captura do tráfego de rede se dá no momento em que os dados estão circulando pela mesma. Com os pacotes capturados, é possível fazer a reconstituição da comunicação do atacante com a máquina alvo, trazendo uma seqüência de eventos ocorridos, que podem ser utilizados juntamente com outras evidências para formular uma "prova" mais completa e confiável. No tráfego de rede pode-se encontrar muitas evidências, como (CASEY, 2004):

a) pacotes com endereço de Internet Protocol (IP) inválido ou suspeito;
b) pacotes relacionados a portas suspeitas;
c) tráfego Transmission Control Protocol (TCP) sem estabelecimento de conexão, sem *flags*[4] ou números de seqüência inválidos;
d) tráfego intenso de pacotes incomuns à rede, ou que deveriam estar desabilitados;

[4] Sinalizador, indicador (MICHAELIS, 1998)

e) pacotes Internet Control Message Protocol (ICMP) *echo reply* sem correspondente *echo request* anterior;
f) pacotes contendo comandos Unix na área de dados;
g) tráfego intenso de pacotes para um determinado serviço ou máquina;
h) requisições HyperText Transfer Protocol (HTTP) suspeitas.

2.1.6 Estado do Sistema Operacional

Dados providos do estado do sistema operacional podem trazer informações importantes sobre a existência, tipo e origem de um ataque em andamento. Essas informações representam um estado do sistema operacional em um determinado momento e que, normalmente são perdidas quando o sistema é desligado. As informações mais comuns abstraídas nesse momento são os processos em execução, as conexões de rede ativas, os usuários autenticados, as tabelas e *caches* mantidas (CASEY, 2004).

2.1.6.1 Processos em Execução

A busca por informações sobre os processos em execução do sistema analisado é de grande valia para a perícia, pois pode revelar a ação de atividades suspeitas, indicando processos não autorizados mas, que mesmo assim, estão sendo executados (MANDIA; PROSISE, 2001).

Os processos são executados individualmente em um ambiente com privilégios específicos que determinam quais recursos do sistema, programas e arquivos de dados podem ser acessados e de que modo. Um invasor pode causar uma parada na

execução de um determinado processo, deixando uma "brecha" no sistema, por exemplo, pela parada de um *firewal*[5]*l*, vindo a poder executar processos maliciosos como *rootkits*[6], *back door* e Cavalos-de-Tróia.

Muitos utilitários permitem acessar as informações relacionadas aos processos em execução do sistema operacional. Vários permitem, por exemplo, capturar uma lista de todos os processos do sistema, com data e hora de início do processo, comando executado, arquivos abertos e o consumo de recursos de cada um deles.

Com as informações coletadas, pode-se identificar possíveis intrusões. As situações abaixo são comumente consideradas suspeitas, pois ferem o funcionamento normal e racional do sistema:

a) existência de processos com nomes suspeitos (comandos não identificados ou conhecidamente maliciosos);
b) ausência de processos que deveriam estar executando (principalmente relacionados aos mecanismos de segurança, como por exemplo, *software* antivírus e *firewall*);
c) processos com consumo de recursos acima do normal.

2.1.6.2 Conexões de Rede

Verificar o estado da rede traz informações úteis sobre as conexões de rede em andamento ou finalizadas e dos processos aguardando uma conexão. Com essas informações é possível identificar se a máquina foi invadida, observando se existe

[5] Software ou hardware que protege uma rede de área local contra pacotes enviados por usuários mal-intensionados de uma rede externa (CHOFFNES; DEITEL; DEITEL, 2005)
[6] Mecanismos e técnicas usadas por vírus, *malware*, *spyware* e *trojans* na tentativa de esconder sua presença de antivírus, antispyware e utilitários (FREITAS, 2006).

alguma conexão suspeita em andamento. Alguns dos vestígios comumente encontrados em tráfegos de rede são (MANDIA; PROSISE, 2001):

a) endereços de IP suspeitos;
b) serviços suspeitos aguardando conexão ou com conexões estabelecidas;
c) serviços que deveriam estar desabilitados;
d) ausência de servidores que deveriam estar em execução.

2.1.6.3 Usuários Logados

Simples de serem identificados, a busca pelos usuários nos leva a identificar uma possível intrusão no sistema. Nomes suspeitos ou desconhecidos, autenticação de origem ou horários suspeitos, executando comandos indevidos ou não autorizados, nos remetem à uma provável intrusão.

2.1.6.4 Dispositivos de Armazenagem Secundária

Segundo Mandia e Prosise (2001) o disco rígido possui a maior fonte de dados para a pesquisa forense. Isso, pois não é uma memória volátil e sua capacidade é muito maior que à dos dispositivos até agora mencionados. Arquivos de todas as espécies são mantidos no disco rígido e podem ser facilmente abstraídas. Existem partes do disco que não estão acessíveis por meio do sistema operacional, mas que também podem conter dados importantes a respeito do caso estudado. Para analisar essas partes do disco rígido, deve-se utilizar ferramentas e métodos apropriados, com cautela para que os dados contidos não sejam danificados.

2.2 LEGISLAÇÃO

O aumento do uso da Internet trouxe para o meio computacional os problemas do mundo real. Ataques a instituições financeiras, apropriação indébita, violação de direitos autorais, pornografia infantil, que outrora somente existiam por meio de contato físico entre pessoas e instituições, atualmente ocorre também por meio do mundo virtual no qual a sociedade atual está incluída.

Assim como no mundo real, o virtual também carece de medidas de contenção dos crimes por meio da punição dos criminosos, trazendo a necessidade de tipificação dos delitos que violam uma política ou moral, ou mais especificamente, quando violam uma lei criminal.

Segundo Bitencourt (2006), crime é toda ação ou omissão proibida por lei, sob ameaça de pena, contrariando valores ou interesses do corpo social. Para Caricatti e Rodrigues (2004), o crime digital é qualquer incidente ligado à tecnologia do computador, no qual a vítima sofreu, ou poderia ter sofrido, um prejuízo, e um agente teve, ou poderia ter tido, vantagens.

Segundo Trevenzoli (2006) não há uma lei específica que aborde os crimes digitais, mas as leis vigentes podem ser interpretadas para aplicação em casos que têm por meio o ambiente computacional. A legislação brasileira vem sendo aplicada para solução e punição dos criminosos que se utilizam deste ambiente para cometer delitos. O exemplo pode ser uma transação bancária ilegal na Internet, que é considerado crime e já é previsto no atual Código Penal brasileiro. A diferença está apenas no meio utilizado pelo criminoso para cometer o furto.

A seguir são apresentadas algumas leis do Código Penal utilizadas pelo poder judiciário para punir os criminosos digitais:

a) **D. Lei nº. 2848/40 no artigo 153, *caput*:** "Divulgar alguém, sem justa causa, conteúdo de documento particular, ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem" (L2848/40).

   Certos vírus de computador são disseminados com o objetivo de capturar arquivos confidenciais alheios para a obtenção de informações. Essas informações são coletadas e enviadas, por exemplo, aos contatos da lista de e-mails ou a um remetente específico. Assim o criminoso poderia ser punido com base nesse artigo, por estar divulgando informações confidenciais, sigilosas ou simplesmente pessoais.

b) **D. Lei nº. 2848/40 no artigo 155, *caput*:** "Subtrair, para si ou para outrem, coisa alheia móvel" (L2848/40).

   Fraudes que obtêm de forma ilícita, os dados de usuários, como os dados de autenticação deste em algum sistema de informação, sendo os mesmos utilizados, por exemplo, para efetuar desvio de dinheiro de contas bancárias, podem ser enquadradas nesse artigo, pois trata-se de um furto.

c) **D. Lei nº. 2848/40 no artigo 163, *caput***: "Destruir, inutilizar ou deteriorar coisa alheia" (L2848/40).

   O criminoso que criar ou propagar um programa de computador que danifique arquivos pessoais ou que apague todos os dados contidos no disco rígido do computador de outra pessoa ou instituição, pode ser enquadrado nesse artigo.

d) **D. Lei nº. 2848/40 no artigo 171, *caput***: “Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento" (L2848/40).

   Os crimes que visam o beneficiamento financeiro do criminoso, podem ser enquadrados nesse artigo. Os casos de roubo de senha pessoal, de informações de cartão de crédito e de documentos pessoais são comuns e os devidos criminosos podem sofrer a punição prevista nesse artigo.

   Geralmente essas informações são adquiridas por meio da criação de uma página de Internet visualmente idêntica à original, mas as informações inseridas pelo usuário, não tem o destino previsto por este. Elas são enviadas para o criminoso que a criou, com o intuito de serem ilicitamente utilizadas.

e) **D. Lei nº. 2848/40 no artigo 307, *caput*:** “Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem" (L2848/40).

   Após apropriar-se das informações alheias, o criminoso as utiliza para fins ilícitos, como transferência bancária, envio de e-mails em nome da vitima, acesso a informações sigilosas mediante autenticação do usuário. Como o criminoso está utilizando de artifícios para se passar por uma pessoa que realmente não é, ele pode ser enquadrado nesse artigo da lei.

f) **D. Lei nº. 2848/40 no artigo 313-A, *caput*:** “Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de

dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano" (L2848/40).

Podem ser enquadrados nesse artigo, funcionários autorizados, que inserem dados falsos, ou modificam ou excluem indevidamente dados da base de dados da Administração Pública.

g) **D. Lei nº. 9296/96 no artigo 10, *caput*:** "Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei" (L9296/96).

Muitos criminosos poderiam ser enquadrados nessa lei, já que para conseguirem as informações, a maioria das vezes a conexão de Internet deve ser monitorada e o tráfego da rede coletado, deixando evidentes as informações sigilosas do usuário, que trafegam na rede.

À medida que os crimes digitais aumentam, cresce a necessidade da utilização da perícia forense no combate a esses tipos de crime e criminosos. As evidências digitais encontradas, documentadas e apresentadas pelos peritos em sistemas analisados, estão sendo utilizadas cada vez mais em processos criminais na busca pelo correto julgamento do acusado. Muitas vezes, essas evidências têm maior valor, do que provas encontradas utilizando-se a perícia tradicional.

Esse contexto mostra a necessidade de que o perito esteja ciente da legislação e de estar em conformidade com as leis que amparam seu trabalho. Além disso, o perito forense deve possuir ainda, os conhecimentos técnicos necessários sobre o ambiente no qual a perícia será aplicada e a metodologia utilizada deve estar baseada em um método científico comprovado, para que seu parecer seja relevante e aceito para os mais diversos fins.

3 SISTEMA DE ARQUIVOS NEW TECHNOLOGIES FILE SYSTEM

O sistema de arquivos NTFS foi desenvolvido pela Microsoft, sendo o padrão para os sistemas operacionais Microsoft Windows (NT, 2000, XP e Server). Com a saída do Windows 98 e ME do mercado, o Windows XP tornou-se o padrão entre os sistemas para consumo, tornando o NTFS popular. Esse é o sistema de arquivos mais apropriado para a aplicação da perícia forense computacional em um sistema Windows, pois possui suporte a auditoria, assim como um controle de acesso aos arquivos de um modo diferenciado, gerando *logs* sobre diversas operações do sistema (CARRIER, 2005).

Ele foi desenvolvido com a intenção de aumentar a confiabilidade, permitindo que o sistema operacional se recupere de problemas sem perder informações, tornando-o tolerante a falhas. A segurança é um dos pontos chaves do sistema de arquivos, onde é possível obter um controle de acesso preciso e ter aplicações que executem em rede local, fazendo com que seja possível o gerenciamento de usuários, incluindo suas permissões de acesso e alteração de dados. Também foi aprimorado, o suporte aos dispositivos de armazenamento de grande capacidade (CHOFFNES; DEITEL; DEITEL, 2005).

Um dos conceitos mais importantes sobre este sistema de arquivos, é o modo como os dados são alocados nos arquivos. Ele inclui dados administrativos do sistema de arquivos básicos que são normalmente ocultos por outros sistemas de arquivos.

3.1 ESTRUTURA DO NTFS

Segundo Carrier (2005) a formatação de uma partição de sistema de arquivos NTFS, resulta na criação da Master File Table (MFT) e num conjunto de arquivos que contém informações utilizadas para implementar a estrutura do sistema de arquivos. A MFT possui informações sobre todos os arquivos e diretórios de uma partição NTFS.

A Figura 1 ilustra um registro na MFT para um arquivo.

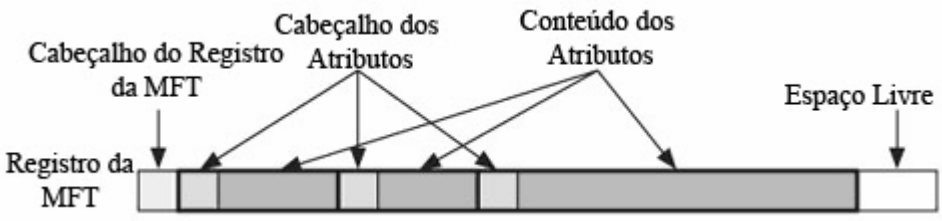

Figura 1. Exemplo de um registro de arquivo ou diretório na MFT.
Fonte: CARRIER, B. (2005).

Uma entrada na MFT é comumente chamada de um arquivo de registro. Na primeira parte, a MFT *Entry Header* traz a informação padrão do sistema. A segunda coluna especifica o nome do arquivo ou do diretório. Na terceira coluna estão armazenadas as informações sobre segurança. Na quarta coluna, encontramos dados ou índices de arquivos. A última coluna não é utilizada.

Segundo Carrier (2005), cada arquivo e diretório do sistema possui pelo menos um registro na tabela. Esses registros são simples e possuem o tamanho de 1 *Kilobyte* (KB), mas apenas 42 *bytes* são utilizados para a definição do arquivo. O espaço que sobra na tabela é utilizado para armazenar atributos, como o nome do arquivo.

3.2 MASTER FILE TABLE

Contendo informações sobre todos os arquivos e diretórios do disco, a MFT é considerada a parte principal do sistema de arquivos NTFS (CHOFFNES; DEITEL; DEITEL, 2005).

Uma entrada na MFT é uma pequena estrutura interna e é utilizada comumente para armazenar atributos, como são estruturas de dados, podem armazenar um tipo específico de dado. Existem muitos tipos de atributos, e cada um possui um tipo de estrutura interna. Como exemplo, temos os atributos para nomes de arquivos, data e hora, entre outros. Esse é um dos motivos pelo qual o NTFS se diferencia de outros sistemas de arquivos. Na maioria dos sistemas, existe a leitura e agravação do conteúdo dos arquivos, mas no NTFS existe a leitura e a gravação de atributos (CARRIER, 2005).

Enquanto cada tipo de atributo armazenado tem um diferente tipo de dado, todos os atributos possuem as mesmas partes: o cabeçalho e o conteúdo. O cabeçalho é genérico e padrão para todos os atributos. O conteúdo do atributo é específico para seu tipo e o tamanho é variável.

3.2.1 Cabeçalho do Atributo

Este local contém as seguintes informações (RUSSON; FLEDEL, 2005):

a) números de seqüência, usados para verificação de integridade;

b) ponteiro para o primeiro atributo do registro;

c) ponteiro para o primeiro *byte* livre no registro;

d) número do registro em relação ao registro base da MFT, caso não seja o primeiro.

3.2.2 Conteúdo do Atributo

O conteúdo do atributo possui um formato e muitos tamanhos. Por exemplo, um deles é utilizado para armazenar o conteúdo de um arquivo, mas este arquivo pode conter Megabytes ou Gigabytes de dados. Isso torna impraticável o armazenamento de todo o conteúdo do arquivo na MFT, já que são suportados apenas 1.024 *bytes*.

Segundo Russon e Fledel (2005) para resolver este problema, o NTFS disponibiliza dois locais onde o conteúdo dos atributos pode ser armazenado. O atributo residente armazena seu conteúdo na MFT e o atributo não-residente armazena em um *cluster* externo no sistema de arquivos. No cabeçalho está a identificação do atributo como residente ou não-residente. Caso a primeira opção seja atendida, o conteúdo é enviado imediatamente para o cabeçalho, caso contrário, o cabeçalho armazena o endereço do *cluster*.

Atributos não-residentes são armazenados em *clusters* consecutivos, e a execução é documentada utilizando o endereço do *cluster* de inicio e a quantidade deles. Por exemplo, um atributo é armazenado nos *clusters* 80, 81, 82, 83 e 84, a leitura começará no 80 com o número de 5 *clusters*, ou seja, segue pelos próximos em seqüência até chegar ao 84.

3.2.3 Tipos de Atributos Padrão

Cada atributo da MFT é subdivido em dois componentes: um cabeçalho que armazena o tipo do atributo, nome, *flags* e a localização da parte de dados do registro, e local onde é armazenada a informação do registro.

Os principais atributos são (CARRIER, 2005):

a) **Standard Information Attribute ou Atributo Padrão de informações:** consta as datas de criação, modificação e último acesso, assim como a identificação do arquivo como sendo de somente leitura ou oculto.

b) **File Name Attribute ou Atributo de Nome do Arquivo:** armazena os nomes dos arquivos.

c) **Data Attribute ou Atributo de dados:** armazena o conteúdo do arquivo, pequenos arquivos e diretórios podem caber totalmente neste atributo, mas para arquivos maiores, apenas uma parte fica armazenada, e um indicador é posto apontando para o restante dos dados localizados em outra parte do disco rígido (fora da MFT).

d) **Security Descriptor Atribute ou Atributo Descriyor de Segurança:** contém as diretivas de segurança dos arquivos.

A seguir, é exibida a Tabela de registros padrões da MFT, no primeiro campo está o nome do arquivo precedido pelo caractere $, que indica um arquivo da MFT, na segunda coluna está o código do registro, na terceira, encontra-se a descrição do tipo de registro.

Tabela 1. Tabela de registro padrões da MFT.

Nome do Arquivo	Registro na MFT	Descrição
$MFT	0	Master File Table
$MftMirr	1	Cópia dos primeiros registros da MFT
$LogFile	2	Arquivo de *log* das transações efetuadas no disco
$Volume	3	Informação sobre o volume, com rótulo, identificador e versão
$AttrDef	4	Definição dos atributos
.	5	Diretório raiz do volume
$Bitmap	6	Representação do disco indicando quais *clusters* estão sendo utilizados
$Boot	7	Setor de *boot* do volume
$BadClus	8	*Clusters* defeituosos
$Secure	9	Contém informações sobre a segurança e o controle de acesso dos arquivos (Somente Windows 2000 e XP)
$Upcase	10	Mapeia caracteres minúsculos em seus correspondentes maiúsculos
$Extend	11	Usado por extensões opcionais

Fonte: CARRIER, B. (2005).

3.3 ENTRADAS DE ENDEREÇO NA MASTER FILE TABLE

Cada entrada é sequencialmente endereçada usando um valor de 48-*bit*, e a primeira entrada começa no endereço 0. A quantidade máxima de endereços da MFT muda conforme a MFT aumenta e é determinada pela divisão do tamanho do $MFT pelo tamanho de cada entrada. A Microsoft chama esse endereçamento seqüencial de "*file number*", ou, número do arquivo (CARRIER, 2005).

O NTFS utiliza o endereço de referência do arquivo para se referir as entradas da MFT pelo fato de que o número seqüencial produzido facilita a determinação quando o arquivo de sistema está corrompido.

3.4 SEGURANÇA EM NTFS

O NTFS admite definir permissões de acesso para arquivos e diretórios individualmente, ou seja, pode-se ter arquivos diferentes em um mesmo diretório, com permissões diferentes para usuários diferentes. As permissões NTFS têm efeito localmente, ou seja, mesmo que o usuário efetue autenticação no computador onde um determinado arquivo está alocado, se ele não possuir as permissões necessárias, não poderá acessar o arquivo. Isso traz um certo grau de segurança, desde que as permissões NTFS sejam configuradas corretamente (CARRIER, 2005).

O NTFS possui várias características relacionadas à segurança, algumas delas são citadas a seguir (CARRIER, 2005):

a) criptografia de arquivos e diretórios, traz um aumento na segurança, pois os arquivos não podem ter seu conteúdo exibido, se o usuário não possuir a chave para descriptografar o arquivo ou diretório em questão;
b) cotas de usuário, fazendo com que seja possível limitar o espaço em disco que cada usuário pode utilizar;
c) gerenciamento e otimização melhorados.

3.4.1 Permissões Em NTFS

São um conjunto de permissões que possibilitam conceder ou negar acesso aos diretórios e arquivos para cada usuário ou grupo. A segurança NTFS é efetiva nos acessos locais ou em acessos por meio da rede.

O NTFS armazena uma Access Control List (ACL), ou seja, uma lista de controle de acesso, com cada arquivo e pasta em uma partição do sistema de arquivos.

A ACL contém uma lista de todas as contas de usuários, grupos e computadores aos quais está concedido acesso para o arquivo ou diretório e o tipo de acesso permitido (RUSSON; FLEDEL, 2005). Para que um usuário acesse um diretório, deve estar contido na ACL um registro, chamado de Access Control Entry (ACE), ou entrada de controle de acesso, para a cada conta de usuário, grupo ou computador ao qual o usuário pertence. Para que o usuário tenha acesso ao arquivo ou diretório solicitado, a ACL deve conter uma ACE que permita o tipo de acesso ao qual o usuário está solicitando. Caso contrário, o sistema operacional negará acesso do usuário ao recurso.

As permissões NTFS, além de indicar os usuários, grupos e computadores que têm acesso a arquivos e diretórios específicos no sistema de arquivos, indicam as operações que os usuários poderão executar sobre esses arquivos ou diretórios.

3.4.2 Permissões De Diretório

A Tabela 2 lista as permissões padrão do NTFS para os diretórios e o tipo de acesso que pode ser fornecido por cada uma delas:

Tabela 2. Permissões padrão no NTFS.

Permissão NTFS	Descrição
Read	Permite visualizar os arquivos e os subdiretórios da pasta, os atributos, a propriedade e as permissões deste diretório
Write	Permite criar novos arquivos e subdiretórios, alterar os atributos e visualizar as permissões e as propriedades desta pasta.
List Folder Contents	Permite Visualizar os nomes dos arquivos e dos subdiretórios.
Read & Execute	Permite percorrer as pastas e executar ações autorizadas pelas permissões *Read* e *List Folder Contents*
Modify	Permite Excluir um diretório e executar as ações autorizadas pelas permissões *Write* e *Read & Execute*
Full Control	Permite alterar as permissões, copiar, mover ou excluir pastas e arquivos. Permite também, executar as ações autorizadas por todas as permissões NTFS de pasta.

Fonte: CARRIER, B. (2005).

3.4.3 Permissões NTFS de Arquivo

A Tabela 3 informa as permissões para os arquivos e o tipo de acesso provido por cada uma delas.

Tabela 3. Permissões de arquivos no sistema NTFS.

Permissão NTFS	Descrição
Read	Permite ler o arquivo e visualizar os atributos, as propriedades e as permissões deste arquivo.
Write	Permite Substituir o arquivo, alterar seus atributos e visualizar as propriedades e as permissões deste arquivo.
Read & Execute	Permite executar aplicativos e executar ações autorizadas pelas permissões *Read*
Modify	Permite Excluir um o arquivo e executar as ações autorizadas pelas permissões *Write* e *Read & Execute*
Full Control	Permite alterar as permissões, copiar, mover ou excluir arquivos. Permite também, executar as ações autorizadas por todas as permissões NTFS de arquivo.

Fonte: CARRIER, B. (2005).

3.4.4 Arquivos Criptografados

O Encrypting File System (EFS) permite a criptografia de arquivos para armazenamento no Sistema de arquivos NTFS (CHOFFNES; DEITEL; DEITEL, 2005).

Os usuários trabalham com arquivos criptografados assim como trabalham com arquivos e diretórios comuns, pois para o usuário, esse proesso é transparente, sendo o arquivo descriptografado automaticamente quando o usuário que está tentando acessá-lo possui permissão de leitura ou escrita sobre o arquivo. Quando o arquivo é salvo, a criptografia é reaplicada. Usuários sem autorização para o acesso ao arquivo criptografado, recebem uma mensagem do sistema informando que o acesso ao arquivo não está autorizado, quando tentarem abrir, copiar, mover ou renomear o arquivo ou diretório (CARRIER, 2005).

Algumas características do EFS (BIDWELL; CROSS; RUSSEL, 2002):

a) se mostra transparente ao usuário e para as aplicações. Não é necessária a digitação de uma senha especial para descriptografar o arquivo, pois esse processo é feito automaticamente quando o usuário autorizado acessa o arquivo criptografado;
b) chave de segurança confiável. Diferentemente de outros tipos de criptografia, onde a mesma depende da senha digitada pelo usuário, o EFS gera chaves mais seguras que são utilizadas para criptografar e descriptografar arquivos e diretórios;
c) todos os processos de criptografia e descriptografia são executados no modo *Kernel*, excluindo o risco de se deixar resíduos de chaves em arquivos paginados, lugares de onde podem ser extraídos;
d) EFS possui um mecanismo de recuperação de dados, o qual é muito útil no meio organizacional, tornando possível a recuperação de dados criptografados.

3.4.5 Alternate Data Streams

Segundo Shinder (2002) todo arquivo NTFS possui um outro arquivo sem nome embutido, chamado *default stream* ou *unnamed stream*, onde dados convencionais são armazenados.

Esse arquivo embutido pode conter outros arquivos quaisquer, como programas executáveis. Esses arquivos representam um sério risco de segurança, pois são quase que invisíveis para as ferramentas tradicionais instaladas nos sistemas

operacionais, tornando-os locais ideais para alojar arquivos maliciosos como vírus e “cavalos de tróia”.

Essa característica pode ser facilmente utilizada, e pode ser apenas detectada com softwares especializados para este fim. Programas como o “Explorer” do Windows somente visualiza arquivos tradicionais não mostrando os arquivos “escondidos” nem mostra o espaço utilizado por estes.

3.4.6 Slack Space

Segundo Oliveira, Guimarães e Geus (2001) o sistema NTFS armazena seus arquivos em disco utilizando blocos de dados de tamanho fixo, chamados de *clusters*. Porém os arquivos armazenados raramente possuem o tamanho exato do *cluster*, tornando inevitável a sobra de espaços não utilizados nos *clusters*.

Esse espaço remanescente pode ser utilizado para o alojamento de diversos dados, assim como para programas maliciosos. Visto que os arquivos serão armazenados em blocos inutilizados, o atacante consegue despistar muitos softwares de análise forense.

O espaço disponível em cada um destes blocos inutilizados é minúsculo, por esse motivo, o atacante necessita de um software especializado para unir todos os pequenos espaços disponíveis em cada bloco, de forma a conseguir um único fluxo de informação suficientemente grande para armazenar seus arquivos, quer seja um pequeno arquivo executável, ou um arquivo de *log* suficientemente grande, por armazenar inúmeras informações sobre o sistema no qual está alojado.

3.4.7 Arquivos de Log

Estes arquivos representam a fonte de informação mais valiosa sobre as atividades do sistema. Eles podem registrar, entre outras informações, as atividades dos usuários, dos processos e do sistema, as conexões e atividades da rede e informações específicas de aplicativos e serviços. A maioria dos arquivos de *log* está localizada em um diretório comum dentro do sistema.

Durante a análise do sistema invadido, algumas informações sobre os arquivos de *log* devem ser consideradas (OLIVEIRA; GUIMARÃES; GEUS, 2001):

a) nem todos os programas registram uma entrada nos *logs*;
b) os arquivos de *log* podem ter nomes diferentes do padrão conhecido, ou podem estar localizados em outras partes do sistema, em outras máquinas ou em cópias de segurança;
c) a capacidade de *log* de alguns aplicativos pode estar desabilitada, ou configurada para um baixo nível de detalhes, que torna-o inviável para a análise;
d) a falta de autenticação nos *logs*, permite que qualquer usuário insira informações neste arquivo, deixando informações falsas para o analista;
e) a ordem dos eventos registrados em um arquivo de *log* pode não representar a linha de tempo real dos acontecimentos, pois sistemas diferentes com data e hora diferentes podem gravar informações num mesmo arquivo de *log*.

Algumas questões referentes aos arquivos de *logs* que remetem a uma intrusão do sistema são (SHINDER, 2002):

a) a exclusão de um arquivo de *log* tradicional;

b) a evidência de modificação nos arquivos de *log*, como a inexistência de um registro de um aplicativo ou serviço que deveria ter sua inicialização armazenada no arquivo, desorganização no que se refere ao tempo cronológico de execução;
c) atividades em horários ou datas incomuns, como um registro no *log* em um horário posterior ao término do expediente;
d) atividades incomuns;
e) tentativas mal sucedidas de autenticação no sistema;
f) erros provenientes de serviços de rede;
g) desligamento ou reinicialização em horário suspeito;
h) alterações não autorizadas na data e hora do sistema;
i) entradas de *log* contendo caracteres não usuais, fora do padrão normal;
j) conexões de rede provenientes de origem desconhecidas;
k) transmissões de arquivos suspeitos via File Transfer Protocol (FTP).

A análise manual de arquivos de *log* torna-se impraticável quando estamos nos referindo a um sistema com grande volume de transações documentadas nesses tipos de arquivos. Para essa análise existem soluções especializadas, como ferramentas que varrem os arquivos em busca de padrões definidos em seu arquivo de configuração.

Na Tabela 4, é exibida uma lista de *logs* que são armazenados no sistema e seus respectivos conteúdos.

Tabela 4. Arquivos de log

Arquivo de Log	Descrição e características
utmp	Registra os usuários atualmente "logados" no sistema. Apresenta-se no formato binário e pode ser acessado pelos comandos w, who, users, e finger. Encontra-se no diretório /var/run.
wtmp	Registra todos os *logins, logouts, shutdowns* e mudanças no tempo do sistema. Apresenta-se no formato binário e pode ser acessado pelos comando *last* e *ca*.
btmp	Registra as tentativas mal sucedidas de *login*. Apresenta-se no formato binário e pode ser acessado pelo comando *lastb*
lastlog	Registra o momento e a origem do *login* mais recente de cada usuário. Apresenta-se no formato binário e pode ser acessado pelo comando *latlog*
boot.log e dmesg	Registram as mensagens relativas ao processo de inicialização do sistema. Apresentam-se no formato texto.
messages ou syslog	Registra vários eventos e informações do sistema e aplicativos. Representa o principal arquivo de *log* do sistema e geralmente contém informações encontradas também em outros arquivos de *log*, como, por exemplo, tentativas mal sucedidas de *login.*
Secure	Registra mensagens privadas de programas relativos a autorização de usuários. Apresenta-se no formato texto.
Sulog	Registra o uso do comando *su*.
acess_log	Registra os acessos ao servidor HTTP. Apresenta-se no formato texto.
Xferlog	Registra os acessos ao servidor FTP. Apresenta-se no formato texto.
cron	Registra a execução das tarefas agendadas. Apresenta-se no formato texto.
maillog	Registra mensagens relativas ao serviço de correio eletrônico. Apresenta-se no formato texto.
aculog	Registra o uso de conexões *dial-out*.
pacct ou acct	Registram os processos executados por cada usuário. Apresentam-se no formato binário e podem ser acessados pelos comandos *lastcomm*, *acctcom* e *sa*.
history files (.history, .sh_history, .bash_history)	Registram os comandos recentemente usados por cada usuário. Apresentam-se no formato texto e encontram-se nos diretórios de cada usuário.
logs de *firewalls* e sistemas de detecção de intrusão	Registram conexões permitidas e eventos caracterizados como possíveis intrusões.

Fonte: REIS, M.; GEUS, P. (2002)

4 BUSCA E PRESERVAÇÃO DE EVIDÊNCIAS EM UM AMBIENTE NTFS

No momento em que a busca por evidência começar, pode-se optar por um dos dois métodos de investigação. Um é realizar as etapas investigativas na própria mídia com as provas. O outro deve-se realizar a duplicação pericial da mídia e realizar a investigação por meio da imagem criada.

Segundo Mandia e Prosise (2001) se a análise for efetuada na própria mídia que contém os vestígios, as evidências serão alteradas e não terá como provar posteriormente a integridade e a veracidade das informações coletadas. Do outro lado está a opção por efetuar uma duplicação pericial da mídia a ser analisada. Se for utilizada a cópia como base da investigação, e alguma evidência vier a ser danificada, ainda temos a mídia original com os dados inalterados. A utilização da cópia facilita a posterior comprovação da evidência encontrada, já que pode-se comprovar a veracidade das informações por meio da original. Por outro lado, se a duplicação pericial falhar, o risco de danificação da mídia original deve ser levado em consideração.

O Simples fato do computador ter o sistema operacional inicializado, implica em alterações de arquivos de extrema importância para a perícia forense, causando a possível alteração da evidência digital (CASEY, 2004). Devido a esse fato, é imprescindível que a busca de evidências em uma ambiente NTFS seja conduzida por meio de um ambiente controlado, utilizando-se ferramentas confiáveis e de preferência um outro sistema operacional, para que as evidências não sejam alteradas. (OLIVEIRA; GUIMARÃES; GEUS, 2001).

Para se ter certeza de que as ferramentas utilizadas são confiáveis, deve-se criar um kit contendo os utilitários que são necessários à perícia, e utilizá-los para não correr o risco de danificar possíveis evidências.

4.1 CRIAÇÃO DE UM KIT DE FERRAMENTAS

O sistema operacional Windows, possui dois tipos de aplicativos, os baseados em Graphical User Interface (GUI) e os com base em Console User Interface (CUI). Os aplicativos em GUI criam a parte gráfica para a interação com o usuário e executam rotinas que não podem ser totalmente identificadas e visualizadas pelo usuário. Devido à esse fato, é aconselhável o uso de ferramentas CUI no processo de aplicação da perícia forense (MANDIA; PROSISE, 2001).

A Tabela 5 lista as ferramentas que podem estar contidas no Kit.

Tabela 5. Ferramenta do kit de resposta.

Ferramenta do Kit de resposta	**Descrição**
cmd.exe	O *prompt* de comando para Windows
loggedon	Um utilitário que mostra todos os usuários conectados localmente e remotamente
rasusers	Um comando do NT Resource Kit (NTRK) que mostra quais usuários possuem privilégios de acesso remoto no sistema-alvo.
netstat	Uma ferramenta de sistema embutida que enumera todas as portas à escuta e todas as conexões atuais a essa porta.
fport	Um utilitário que enumera todos os processos que abriram as portas TCP/IP em um sistema Windows NT/2000.
pslist	Um utilitário que enumera todos os processos em execução no sistema-alvo.
listdlls	Um utilitário que lista todos os processos em execução, os argumentos de linha de comando e as bibliotecas vinculadas dinamicamente das quais cada processo depende.
nbstat	Uma ferramenta de sistema embutida que lista as conexões NetBIOS recentes por aproximadamente 10 minutos.
arp	Uma ferramenta de sistema embutida que mostra os endereços MAC de sistema com os quais o sistema-alvo tem se comunicado, durante o ultimo minuto.
kill	Um comando NTRK que finaliza o processo.
md5sum	Um utilitário que cria verificações *md5* por um certo arquivo
rmtshare	Um comando NTRK que exibe os compartilhamentos acessíveis em uma máquina remota.
netcat (cryptcat)	Um utilitário usado para criar um canal de comunicação entre dois sistemas diferentes. O Cryptcat é usado para criar um canal criptografado de comunicações. O Netcat oferece uma maneira simples de transferir informações entre os sistemas de rede.
doskey	Uma ferramenta de sistema embutida que exibe o histórico de comandos para um *shell* aberto CMD.EXE

Fonte: MANDIA, K.; PROSISE, C. (2001).

Ao final da investigação, o Kit de Ferramentas deve estar no mesmo estado, com as ferramentas inalteradas desde o começo da investigação. Para isso, é utilizado o comando *md5sum* para gerar um arquivo texto contendo a soma de verificação de cada ferramenta do Kit. Essa soma pode ser considerada uma assinatura digital, pois cada arquivo possui um valor exclusivo. Se o arquivo em questão for alterado, o valor da soma, também será alterado (FREITAS, 2006).

4.2 ONDE RESIDE A EVIDÊNCIA

Antes de iniciar a busca pela evidência, deve ser identificado o local onde as mesmas serão coletadas. O local pode depender do caso em estudo, mas de modo geral pode-se listar os locais citados a seguir (MANDIA; PROSISE, 2001):

a) em dados voláteis nas estruturas do *Kernel*;
b) espaço sem atividade, onde se pode obter informações de arquivos que foram excluídos e irrecuperáveis;
c) espaço livre ou não alocado, onde pode obter arquivos excluídos anteriormente;
d) *clusters* inacessíveis ou danificados.

No sistema de arquivos lógicos:

a) nos *logs* de eventos;
b) no Registro, que pode ser considerado um enorme arquivo de *log*;
c) nos *logs* dos aplicativos de terceiros, que não são gerenciados pelo Windows;
d) no arquivo de troca, que inclui informações alocadas recentemente na memória RAM (chamadas *pagefiles.sys* na partição ativa);

e) arquivos específicos em nível de aplicativo, como o cache do navegador de Internet e os arquivos temporários;

f) a Lixeira (uma estrutura de arquivos lógicos ocultos onde itens recentemente excluídos podem ser encontrados);

g) o s*pool* de impressão;

h) e-mails enviados e recebidos, armazenados por um gerenciador de e-mails como o Outlook Express.

4.3 OBTENDO DADOS VOLÁTEIS

Os dados voláteis devem ser coletados antes do sistema ser desativado, caso contrário, esses dados serão perdidos.

Para comprovar oficialmente o momento em que foi dado inicio à investigação, deve-se primeiramente, capturar a data e a hora atual do sistema e salvá-los em um arquivo texto. Para efetuar a captura, é possível utilizar os comandos *date* e *time*, os quais estão presentes nos sistemas operacionais Windows 2000, 2003 e XP (FREITAS, 2006).

A próxima etapa é definir quais usuários possuem conexões ativas no sistema. Para buscar essas informações devem ser utilizados os comandos *arp*, *nbtstat* e *netstat*. A descrição dessas ferramentas estão disponíveis na Tabela 5.

Para aumentar a confiabilidade da perícia, deve-se registrar as portas que estão abertas no sistema. Para isso, pode-se utilizar o programa chamado *fport*. O *fport* é uma ferramenta desenvolvida pela Foundstone que enumera todas as portas de processos a escuta em um sistema Windows baseado em NTFS. O *fport* é capaz de exibir as portas de processos, mas não as portas que são servidas a sistemas remotos.

Para obter essa informação, deve-se utilizar o *netstat*, um comando padrão do Windows que lista todas as portas à escuta e todas as conexões atuais a essas portas.

Segundo Freitas (2006) uma questão muito importante a ser verificada é o registro de todos os processos que estão em execução no sistema. Um processo pode ser um programa executável, um serviço ou um subsistema. Para listar todos os processos em execução é utilizada a ferramenta *pslist*, de Mark Russinovich. Para analisar e verificar algum processo malicioso no sistema, o perito deve ter alguma experiência com os processos do sistema em questão, observando que a ferramenta apenas lista os processos em execução com informações básicas de cada um deles.

Para documentar a análise, é sugerido criar um arquivo contendo todos os comandos executados no *prompt*. Utilizando da ferramenta *doskey*, é possível armazenar em um documento de texto simples, todos os comandos executados no *prompt*, de forma seqüencial.

Ao analisar um sistema suspeito, a busca por arquivos de *log* é de fundamental importância para a perícia forense. Muitos utilitários do sistema Windows e aplicativos de terceiros criam arquivos de *logs* específicos.

Os sistemas operacionais Windows NT/2000/XP e 2003 armazenam três arquivos de *log* separados (CASEY, 2004):

a) *log* de Sistema (sysevent.evt): constam os eventos do sistema que não são auditados, como *drivers* de dispositivos, falhas de *hardware* e o inicio, pausa e parada de serviços;

b) *log* de Aplicativo (appevent.evt): contém os eventos auditados pelo "*Performance Monitor*" do Windows, como o número de *logon*, a quantidade de uso de disco entre outros;

c) *log* de Segurança (secevent.evt): armazena informações acerca dos eventos de segurança que são auditados, como mudanças no privilégio do usuário, mudança na diretiva de auditoria, acessos a diretórios e arquivos, assim como o *login* e *logoff* do sistema.

O Registro do Windows armazena várias informações úteis sobre o sistema analisado. Uma opção para a recuperação inicial do arquivo de registro do sistema, é a utilização da ferramenta *reg query*, a qual extrai apenas os valores-chave de interesse no Registro (MANDIA; PROSISE, 2001).

O próximo passo para a análise inicial do sistema em questão, é capturar os dados de data e hora dos arquivos armazenados. Esse procedimento é de fundamental importância, pois ao final da análise podemos garantir a integridade de um arquivo, assim como auxiliar na análise, pois se o intervalo de tempo em que ocorreu o incidente for conhecido, a busca por esse intervalo será feita de modo mais eficaz e eficiente.

Para efetuar o registro dos dados de data e hora de todos os arquivos e diretórios do sistema, pode-se utilizar o comando dir que está presente nas versões do Windows NT/2000/XP e 2003. A Tabela 6 exemplifica o comando dir:

Tabela 6. Exemplos do comando *dir*.

Comando	Descrição
dir /t:a /a /s /o:d c	Oferece uma listagem recursiva de diretórios de todas as horas de acesso no drive C
dir /t:w /a /s /o:d d	Oferece uma listagem recursiva de diretórios de todas as horas de modificação no drive D
dir /t:c /a /s /o:d e	Oferece uma listagem recursiva de diretórios de todas as horas de criação no drive E

Fonte: MANDIA, K.; PROSISE, C. (2001).

Pode ser importante para o desenvolvimento da perícia, o esvaziamento do conteúdo da memória Random Access Memory (RAM) do sistema. Esse procedimento pode revelar senhas, textos criptografados que tenham sido digitados recentemente ou programas abertos momentos antes do início da análise (MANDIA; PROSISE, 2001).

4.4 MANIPULANDO SENHAS

Durante a investigação, provavelmente chegará ao ponto de ser necessário o conhecimento da senha do sistema analisado para o acesso com as devidas permissões aos arquivos. Se não for possível obter a senha por meios comuns, como em uma entrevista com o usuário, tem-se quatro opções para decifrá-la (MANDIA; PROSISE, 2001):

a) obter o banco de dados SAM na investigação inicial ao vivo para posteriormente decifrar as senhas utilizadas;
b) obter o banco de dados SAM durante a análise *off-line* e decifrar as senhas obtidas;
c) desviando a autenticação solicitada pelo Windows alterando o Registro;
d) mudar as senhas no SAM.

Para manipular as senhas dos usuários, pode-se utilizar a ferramenta *chntpw*. O *chnptw* é uma ferramenta do Linux que permite visualizar e modificar as senhas de usuários em um arquivo do banco de dados SAM do Windows. Além de alterar senhas, ele contém um editor simples do Registro e editor hexadecimal para a edição no baixo nível do Registro do Windows.

4.5 PROCURANDO POR LOGS DE APLICATIVOS

Um dos passos fundamentais na busca aprofundada por evidências, é analisar minuciosamente os arquivos de *logs* criados pelo sistema operacional e por programas de terceiros. Pode-se encontrar nesses arquivos, informações como:

a) determinar quais usuários acessaram determinados arquivos;

b) identificar os usuários que tiveram autenticação reconhecida no sistema;
c) obter informações sobre usuários que não tiveram a autenticação bem sucedida no sistema;
d) rastrear o uso de aplicativos específicos;
e) perceber alterações nas diretivas de auditoria;
f) identificar mudanças nas permissões de acesso de usuários.

Para obter essas informações dos arquivos de *log* do sistema, deve-se obter uma cópia dos arquivos *secevent.evt, appevent.evt, sysevent.evt* que estão contidos na imagem pericial. É possível obter esses arquivos por meio de um disco de inicialização do Disk Operating System (DOS) ou por meio de um disco de inicialização Linux com o *Kernel* apropriado para montar *drives* NTFS.

Após o procedimento para recuperar os arquivos, pode-se visualizar os *logs* em sua estação de trabalho pericial. Para isso se utiliza a ferramenta *psloglist*, capaz de gerar relatórios acerca dos *logs*, ou a ferramenta "*Event Viewer*" (Visualizador de Eventos), que é disponibilizada juntamente com os sistemas Windows NT/2000/XP e 2003.

Uma questão que pode vir a prejudicar a análise dos *logs* do sistema é o fato de que o Windows NT/2000 possuem por padrão, a configuração de não gerar *log* de auditoria. Isso faz com que *logs* de autenticação de usuários, acessos à arquivos, desligamentos e muitos outros eventos essenciais não sejam registrados pelo sistema. Essa questão se torna um grande obstáculo para a perícia forense em um sistema NT/2000 (MANDIA; PROSISE, 2001).

Uma desvantagem de analisar sistema NT/2000 *off-line* é que os *logs* podem perder as descrições das entradas referentes aos programas de terceiros. Isso ocorre pois o campo *Decription* do registro do *log*, é preenchido com valores de diversos arquivos

Dynamic-Link Library (DLL), ou seja, bibliotecas vinculadas dinamicamente. Essa questão não deveria ocorrer já que os *logs* são gravados com atributos padrão, mas os *logs* de aplicativos podem não possuir descrição apropriada que corresponda ao Identification (ID) do evento que o aplicativo gerou. A estação de trabalho pericial deve conter os mesmos aplicativos instalados na máquina analisada, para não estar sujeito à perda de informações acerca de importantes eventos.

4.6 REALIZANDO BUSCAS POR PALAVRA-CHAVE

A busca por palavras-chave se faz necessária para encontrar as evidências no sistema em questão. Devido aos modernos discos rígidos com grande capacidade de armazenamento, torna-se impraticável a busca manual por arquivos de texto que contenham informações relevantes ao caso. Para sanar essa deficiência, utiliza-se ferramentas que varrem o disco rígido ou disquetes em busca de palavras-chave que podem remeter a arquivos importantes para a perícia (VACCA, 2002).

A maioria das ferramentas para a busca de palavras-chave são vendidas como ferramentas periciais e efetuam leituras simples no disco rígido, realizando uma busca por *string* retornando informações armazenadas. Para executar esse tipo de ferramenta, é necessário que se inicialize o sistema por meio de um ambiente controlado, pois não é possível ler fisicamente um disco rígido que esteja executando um sistema operacional Windows. As ferramentas mais utilizadas para esse tipo de pesquisa são o DS2 da NTI e o *dtsearch* (MANDIA; PROSISE, 2001).

4.7 EXAMINANDO ARQUIVOS RELEVANTES

No decorrer da perícia forense, faz-se necessário pesquisar por arquivos que possam conter informações relevantes a mesma. A questão é, como descobrí-los.

Os sistemas Windows NT/2000 gravam entradas e saídas de tantos arquivos de uma só vez que quase todas as operações realizadas no sistema deixam um vestígio de sua ocorrência. O NT/2000 possui arquivos temporários, arquivos de *cache*, um Registro que armazena a lista dos arquivos utilizados recentemente, uma Lixeira que mantém os arquivos excluídos e inúmeros outros locais onde os dados são armazenados em tempo de execução do sistema operacional (MANDIA; PROSISE, 2001).

4.8 REVISANDO OS REGISTROS DE DATA/HORA

Para determinar os arquivos que foram alterados pelo incidente é indispensável que o período em que o sistema esteve exposto seja de conhecimento do perito. Segundo Vacca (2002) para a reconstrução dos eventos ocorridos no sistema é necessário que seja criada uma linha de tempo das intrusões. Mas essa reconstrução é complicada, devido ao fato do relógio do sistema operacional poder ser alterado sem qualquer ressalva, também pelo fato de existirem vários fusos horários distribuídos pelo Planeta.

Arquivos de *logs* utilizam o horário do sistema para indicar o momento em que uma entrada foi adicionada no arquivo, a partir desse princípio pode-se efetuar a reconstituição do incidente.

4.9 E-MAIL

Os clientes de e-mail contêm as mensagens enviadas e recebidas por um sistema. Clientes de e-mail como o Eudora e Netscape, armazenam as mensagens em um arquivo de texto simples, já o Outlook, Outlook Express, e AOL, utilizam formatos proprietários que necessitam de ferramentas adequadas para serem exibidas (CASEY, 2004).

4.10 RECUPERANDO DADOS EXCLUÍDOS

Para o sucesso da perícia forense, é imprescindível que seja feita a busca por arquivos excluídos. Esses arquivos podem revelar importantes informações acerca do caso estudado, pois normalmente, quando alguém infringe as normas, tenta esconder os fatos.

Existem em geral, quatro maneiras de recuperação de dados (MANDIA; PROSISE, 2001):

a) utilizando ferramentas de recuperação;
b) restaurando arquivos armazenados na Lixeira;
c) recuperando arquivos temporários (.tmp);
d) utilizando ferramentas de baixo nível para recuperar dados diretamente do sistema de arquivos.

No momento em que são excluídos pelo sistema operacional, os arquivos não são apagados fisicamente, apenas são marcados como espaço não utilizado e até o momento em que outras informações forem armazenadas neste local, os arquivos continuam intactos e passíveis de recuperação (FREITAS, 2006).

4.10.1 Investigando Arquivos na Lixeira

A Lixeira é um recurso do Windows 9x/NT/2000/XP e 2003, foi desenvolvida para evitar a exclusão acidental de arquivos. Os arquivos excluídos por meio do Explorer são armazenados na Lixeira e podem ser recuperados posteriormente. Exclusões efetuadas por meio de linha de comando de *software* de terceiro não são armazenadas na Lixeira, assim como exclusões em unidades de rede (MANDIA; PROSISE, 2001).

A Lixeira cria um subdiretório para cada usuário do sistema. Por padrão, o diretório tem o nome de Recycler e o subdiretório do usuário é rotulado pelo *Security Identifier* (SID) (FREITAS, 2006).

O diretório Recycler não é criado quando o sistema operacional é instalado, mas sim, no momento em que algum arquivo é excluído pelo usuário. O diretório da Lixeira é criado na raiz da unidade, portanto, se o usuário excluir um arquivo de uma partição C:, o caminho para ela será: C:\RECYCLER, se for excluído algum arquivo da unidade d:, o caminho para a Lixeira será: d:\RECYCLER (MANDIA; PROSISE, 2001).

4.10.2 Investigando Arquivos Temporários

Os aplicativos como o Microsoft Word criam arquivos temporários no sistema para fins de segurança, se o aplicativo for vítima de alguma anomalia e necessitar ter sua execução finalizada, as informações que estavam contidas neste podem ser recuperadas.

Normalmente o Microsoft Word cria dezenas de arquivos temporários para um documento comum. Por padrão, os arquivos são criados no diretório onde o arquivo original está contido. Quando o documento é salvo e a aplicação é finalizada corretamente, os arquivos temporários são excluídos, mas na prática muitas questões podem fazer com que eles não sejam apagados. Mesmo quando eles são excluídos corretamente pelo sistema, podem ser recuperados utilizando-se ferramentas para esse fim (VACCA, 2002).

Outros arquivos também podem gerar arquivos temporários no sistema, como, a visualização de anexos em mensagens de correio eletrônico, o *download* de arquivos. Esses arquivos são criados no diretório principal do sistema. No Windows 2000/XP e 2003, eles se encontram no caminho (FREITAS, 2006):

<Drive>:\Documents and Settings\<usuário>Configurações Locais\Temp

Os arquivos temporários podem ser excluídos quando o sistema é desligado ou reiniciado, por isso, pode ser importante fazer a duplicação pericial sem desligar o sistema.

4.10.3 Recuperando Arquivos de *Backup*

Uma das maneiras mais confiáveis de se encontrar os dados necessários à perícia forense, que não estão disponíveis no sistema, é por meio dos *backup's* do sistema.

Eles armazenam informações de muitos tipos e tamanhos, podendo ser algum documento pessoal do usuário, arquivos de instalação de programas, entre outros.

4.11 INVESTIGANDO O REGISTRO DO SISTEMA

O Registro do Sistema Operacional Windows, é um banco de dados hierárquico e centralizado que armazena informações de configuração dos usuários e do sistema. Ele contém dados sobre cada usuário individualmente, informando suas configurações gravadas assim como dados de aplicativos instalados no sistema. É formado por chaves e subchaves, seções e entradas de valores.

As informações armazenadas no Registro são fontes importantes para revelar os softwares utilizados e arquivos do Disco Rígido que foram acessados.

As principais chaves do Registro são (FREITAS, 2006):

a) **HKEY_CLASSES_ROOT (HKCR):** contém as associações dos arquivos aos seus respectivos *softwares*;

b) **HKEY_CURRENT_USER (HKCU):** armazena informações relativas à conta do usuário autenticado no sistema. A subchave Software, detêm a lista dos programas utilizados no sistema;

c) **HKEY_LOCAL_MACHINE (HKLM):** detêm informações sobre a parte de *hardware* e a de *software*, instalados no computador;

d) **HKEY_USERS (HKU):** essa chave armazena informações sobre todos os usuários do sistema e suas respectivas configurações;

e) **HKEY_CURENT_CONFIG (HKCC):** contém informações sobre as configurações atuais da parte de *hardware*. Se o usuário não possuir perfis de *hardware* ativados, essa chave conterá informações padrão do Windows.

O Registro do Windows faz parte de um grupo de arquivos chamado de *hives*. *Hives* são arquivos binários, ocultos, somente leitura ou de sistema. *Hives* do

sistema estão armazenados no diretório: *<Drive>:\Winnt\system32\config*, já os arquivos específicos de usuário estão gravados em: *<Drive>:\documents and settings*\<*usuário*>. Na Tabela 7, estão especificadas as entradas do registro e seus devidos arquivos no sistema.

Tabela 7. Entradas no Registro do Windows.

Chave/Subchave	Arquivo
HKEY_LOCAL_MACHINE\SAM	SAM e SAM.LOG
HKEY_LOCAL_MACHINE\SECURITY	SECURITY e SECURITY.LOG
HKEY_LOCAL_MACHINE\SOFTWARE	SOFTWARE e SOFTWARE.LOG
HKEY_LOCAL_MACHINE\SYSTEM	SYSTEM e SYSTEM.LOG
HKEY_USERS\DEFAULT	DEFAULT e DEFAULT.LOG
HKEY_USERS\Security ID	NTUSER.DAT
HKEY_CURRENT_USER	NTUSER.DAT
HKEY_CLASSES_ROOT	Criada no momento da inicialização

Fonte: FREITAS, A. (2006).

Tabela 8. Arquivo do Registro no sistema.

Arquivo	Descrição
SAM	Armazena o banco de dados de usuários
SECURITY	Complementa o arquivo SAM.
SOFTWARE	Contém informações de configuração de softwares, informações que não variam de usuários para usuários.
SYSTEM	Contem informações de configuração (drives, programas, parâmetros etc.)
NTUSER	Cada usuário tem o seu NTUSER.DAT contendo suas preferências específicas para os aplicativos.

Fonte: FREITAS, A. (2006).

Para investigar o Registro do Windows em modo *off-line*, ou seja, sem inicializar o sistema operacional, basta localizar os arquivos *hive* do Registro do local padrão e utilizar uma ferramenta para visualizar as informações contidas.

4.12 ANALISANDO VÍNCULOS

Uma etapa importante da perícia é a busca por vínculos interrompidos, ou seja, algum arquivo ou atalho que aponte para um arquivo não mais existente. Quando os softwares são desinstalados incorretamente, muitos atalhos ficam com seus vínculos interrompidos, pois seus arquivos de destino não são mais encontrados no sistema. Esse

procedimento auxilia na identificação de softwares e arquivos que estavam presentes anteriormente no sistema.

O diretório *\%system-root%\Profiles\<usuário>\Desktop* armazena todos os vínculos (**.lnk*) dos aplicativos da área de trabalho do usuário.

4.13 INVESTIGANDO ARQUIVOS DO NAVEGADOR DE INTERNET

A Internet é acessada por meio de navegadores desenvolvidos para este fim. Esses navegadores armazenam algumas informações e arquivos sobre a páginas visitadas, como imagens e textos, assim como grava o endereço da página em um histórico.

O Internet Explorer é o navegador padrão do Windows a partir da versão 95. Este navegador armazena as informações das páginas em (FREITAS, 2006):

Windows NT: *<Drive>:\WINNT\Profiles\<usuário>\Temporary Internet Files*

Windows 2000/XP/2003: *<Drive>:\Documents and settings\<usuário>\ Configurações locais\ Temporary Internet Files.*

4.13.1 Investigando o Histórico do Navegador

O Histórico é um utilitário padrão do Windows que lista as páginas ou arquivos do computador que o usuário acessou, organizados de forma cronológica. O Histórico cria uma trilha de auditoria exibindo qual o arquivo e em que momento o usuário acessou tal arquivo.

No Windows NT, o Histórico é armazenado no diretório: : *<Drive>:\WINNT\Profiles\<usuário>\Histórico*, já no Windows 2000\XP\2003, as informações estão contidas no diretório *<Drive>:\Documents and settings\<usuário>\Configurações locais\Histórico*.

O Windows XP armazena mais informações sobre as páginas visitadas no arquivo *index.dat*. Para exibir as informações contidas nesse arquivo, é necessária a utilização de uma ferramenta apropriada, já que este é um arquivo binário.

4.13.2 Analisando o Menu Favoritos do Navegador

O menu Favoritos contém os endereços armazenados pelo usuário, ou seja, suas páginas preferidas na Internet. Esse menu permite observar o assunto predileto do usuário, assim como identificar páginas que têm correlação com o crime estudado.

4.13.3 Obtendo Informações em *Cookies*

São arquivos armazenados no sistema pelos *sites* e associados ao navegador de Internet. Eles armazenam informações acerca da navegação do usuário pelas páginas do *site* como, o endereço da última página visitada, informações sobre serviços utilizados e os passos do usuário pelo *site* (VACCA, 2002).

Devidamente analisados, eles podem trazer boas evidências ao investigador.

4.14 PROCURANDO POR ARQUIVOS INCOMUNS OU OCULTOS

Conforme estudado no Capítulo 4, o NTFS permite vários fluxos de dados, viabilizando a ocultação de informações.

Para a identificação desses arquivos, pode ser utilizada a ferramenta *sfind*.

A ferramenta *hfind* pode ser utilizada para listar os arquivos ocultos no sistema. Ela informa quais os arquivos ocultos e a data do seu último acesso.

4.15 DESCOBRINDO ARQUIVOS COM INICIALIZAÇÃO AUTOMÁTICA

Segundo Freitas (2006) utilizando a ferramenta *Autoruns*, é possível identificar quais os programas têm sua execução iniciada logo após a inicialização do sistema operacional Windows. Utilizando esta ferramenta, é possível localizar o programa suspeito e visualizar suas propriedades para a obtenção de evidências acerca do acontecimento estudado.

4.16 IDENTIFICANDO *ROOTKITS* NO SISTEMA

O termo *rootkit* faz referência as técnicas e métodos usados por programas maliciosos, *spyware*, *trojans* e vírus para dificultar a sua identificação pelos softwares antivírus e outros. Para a identificação de um *rootkit*, utiliza-se a ferramenta *RootkitRevealer* (FREITAS, 2006). Considerando a atualização constante destes, essa ferramenta pode não identificar alguns *rootkits* instalados no sistema.

Esses programas maliciosos também são utilizados para manter um ponto de acesso remoto à maquina alvo por meio da rede, para aumentar os privilégios do

atacante, como obter permissões de administrador do sistema, posição que não possui nenhuma restrição de operação no sistema (MOHAY, 2003).

5 TRABALHOS CORRELATOS

Durante os estudos objetivando o desenvolvimento da pesquisa, foram estudados alguns trabalhos semelhantes, mas com outro enfoque. Abaixo, está a descrição de alguns trabalhos envolvendo a perícia forense computacional.

O trabalho com o título: “Perícia Forense Em Software Livre”, do autor Thiago Figueiredo Marques Leite, objetivando *Lato Sensu* pela UNIDESC, tem como objetivo apresentar um estudo sobre perícia forense utilizando Software Livre, bem como criar um documento de base para servir como uma primeira recorrência por peritos, da polícia ou não, em casos em que uma perícia forense computacional deve ser utilizada. É demonstrada a análise de evidências em logs de acesso do sistema operacional, logs de servidores web, mensagens eletrônicas e como ocultar rastros utilizando técnicas anti-forenses.

O trabalho com o título: “Técnicas computacionais no auxílio à perícia forense na análise de evidências coletadas em servidores GNU/LINUX”, do autor Adauto de Souza Bernardo, objetivando o *Lato Sensu* pela Universidade do Extremo Sul Catarinense, tem como objetivo aplicar técnicas computacionais forenses na análise dos resultados gerados pela etapa de busca de evidências na memória principal, memória secundária (*Hard Disk*), processos e módulos do *kernel* em servidores GNU/Linux. Nesse trabalho, são apresentadas algumas formas publicamente conhecidas na análise das evidências em ambientes GNU/Linux. Analisando basicamente a memória, módulos do *kernel* e sistema de arquivos de maneira prática, a pesquisa não tem como objetivo esgotar o assunto e faz uso do embasamento teórico presente na literatura e a utilização de ferramentas livres.

6 PERÍCIA FORENSE APLICADA A AMBIENTES NTFS

Neste capítulo, será apresentada a parte prática da pesquisa, demonstrando a utilização das ferramentas forenses e o conhecimento adquirido na teoria, para a busca, preservação e análise das evidências em um ambiente NTFS.

A parte prática está dividida em três grandes partes: a simulação do ambiente, a duplicação pericial e a busca e análise das evidências. A simulação do ambiente, busca a estruturação de um ambiente computacional no qual a prática forense possa ser aplicada de um modo geral. A seguir será descrito o modo como o ambiente foi preparado.

6.1 SIMULAÇÃO DO AMBIENTE

O ambiente proposto é de um usuário doméstico tradicional, que possui acesso à Internet e possui diversos arquivos pessoais de texto e imagem. Para isso, foi utilizado um computador doméstico, o qual possui dois discos rígidos, o primeiro disco foi utilizado como ambiente dos acontecimentos e o segundo, utilizado como ferramenta da perícia forense.

O primeiro disco rígido, de tamanho 10,2Gb, possui duas partições, uma com 6,14Gb e outra com 4.09Gb (valores obtidos por meio da ferramenta dd, com a opção “--list"), mas para fins da pesquisa, somente o primeiro será utilizado. O segundo disco rígido possui capacidade de armazenamento de 20Gb. Todas as partições possuem o sistema de arquivos NTFS. Em ambos os discos rígidos foi instalado o sistema operacional Windows XP Profissional, versão 2002 com *Service Pack* 2.

Com essas características, este computador pôde ser utilizado tanto para a simulação do ambiente, quanto como ferramenta para a perícia forense.

Para idealizar o ambiente, foi criada uma nova conta de usuário, com o nome fictício de: João da Silva, e uma senha. Os eventos de auditoria foram ativados e operações típicas de um usuário doméstico, foram efetuadas, como: acesso, armazenamento e exclusão de arquivos do disco rígido, acesso à Internet, e envio e recebimento de *e-mails.*

Para demonstrar um quesito de segurança, conforme descrito no capítulo 3, foi utilizado o Alternate Data Streams para “esconder” um arquivo de texto num arquivo de imagem.

A Figura 2 mostra o comando utilizado para tal fato:

Figura 2. Aplicação de técnica para “esconder” um arquivo.

O comando *type* escreve o arquivo *NTFSdoc.txt* no arquivo *Pedido.jpg*, mas os dois pontos indicam um novo fluxo de dados, ou seja, não será identificado pelos métodos normais de operação do sistema operacional.

Observa-se na Figura 3, que o tamanho do arquivo não foi alterado após a aplicação da técnica, impossibilitando ao usuário a identificação da alteração do arquivo.

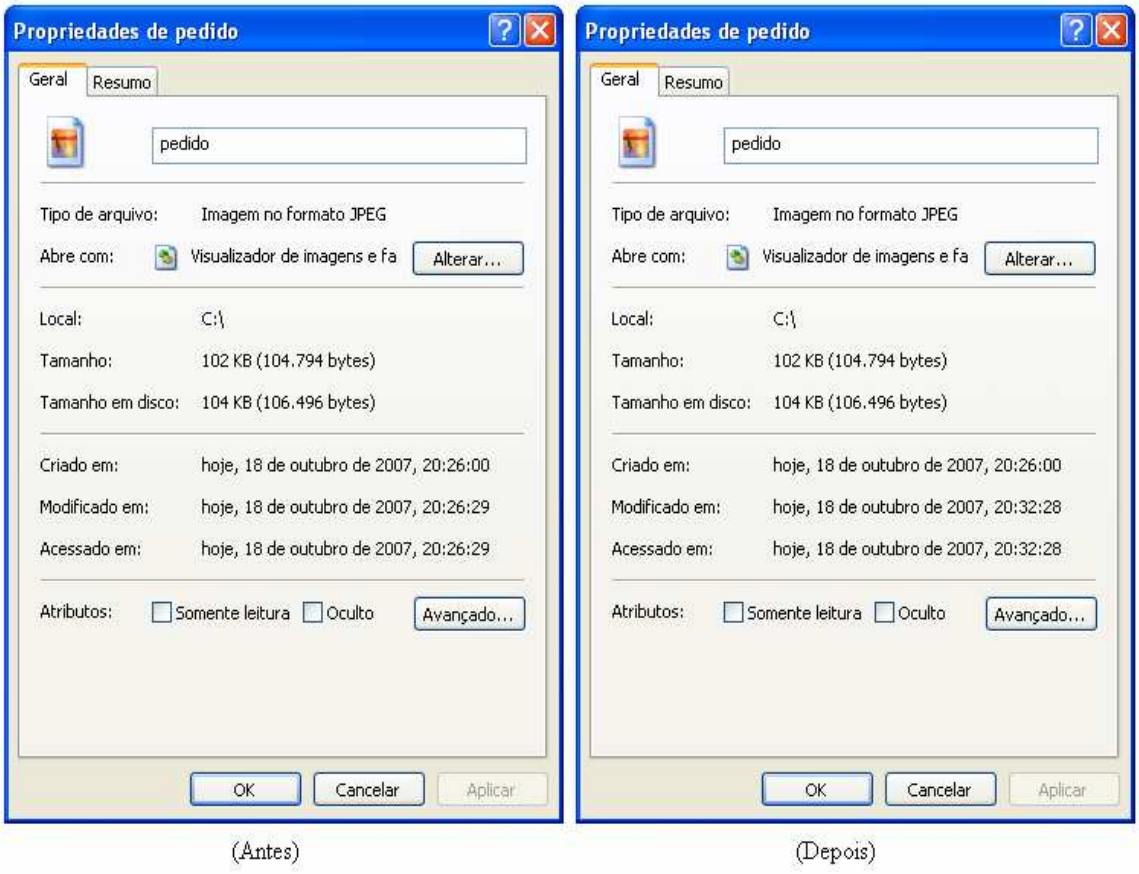

Figura 3. Propriedades do arquivo *Pedido.jpg* antes e depois de ser alterado.

A tela da esquerda (Antes) mostra as propriedades do arquivo original, a tela da direita (Depois) indica as propriedades do mesmo arquivo após a aplicação da técnica para criar um novo fluxo de dados.

6.2 DUPLICAÇÃO PERICIAL

Conforme o estudado na fundamentação teórica, os métodos utilizados para a obtenção de evidências, não podem de forma alguma, danificar ou alterar as mesmas. Para que todo o processo seja feito de forma segura, as ferramentas utilizadas devem ser de confiança do perito, para isso deve-se criar um kit contendo as ferramentas que serão utilizadas.

As ferramentas *open source*, ou seja, de código fonte aberto, tiveram a preferência neste trabalho, devido ao fato de que seu código fonte pode ser analisado, atribuindo transparência e confiabilidade à perícia forense.

De acordo com os propósitos deste trabalho, e as características do ambiente criado, o primeiro passo a ser dado após a criação do kit, é a obtenção dos dados contidos no disco rígido. Essa etapa consiste na duplicação do disco por meio de uma ferramenta confiável. Segundo Freitas, 2006 essa duplicação é chamada de duplicação pericial.

A duplicação pericial deve utilizar uma ferramenta que faça a cópia do disco rígido em sua totalidade, copiando desde arquivos comuns, até arquivos ocultos e do sistema de arquivos. Essa cópia feita *bit* a *bit* é chamada de *bitstream*.

A ferramenta escolhida para essa etapa, foi a ferramenta dd, que faz a cópia *bitstream* do disco. Ela é um *software* livre, ou seja, pode ser utilizado gratuitamente por qualquer pessoa. A Figura 4, mostra a ferramenta sendo executada para armazenar o conteúdo do disco em um arquivo do tipo imagem.

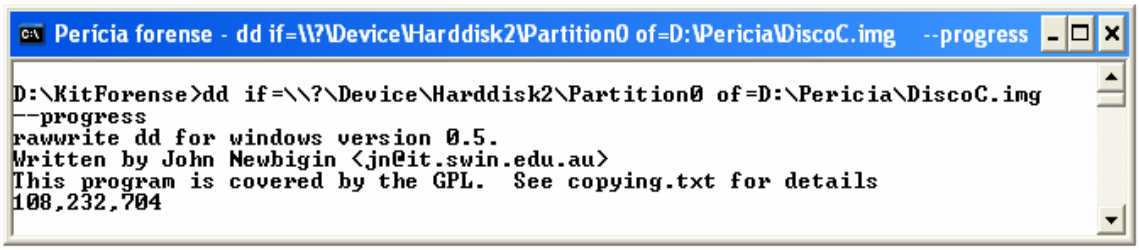

Figura 4. Ferramenta dd sendo executada.

Após a duplicação pericial do disco, deve ser criado um *hash*[7] para a verificação da integridade da imagem. A Figura 5 mostra a ferramenta *md5summer* sendo executada para a geração do *hash* do disco de modo recursivo.

[7] Soma de verificação de um determinado arquivo (FREITAS, 2006).

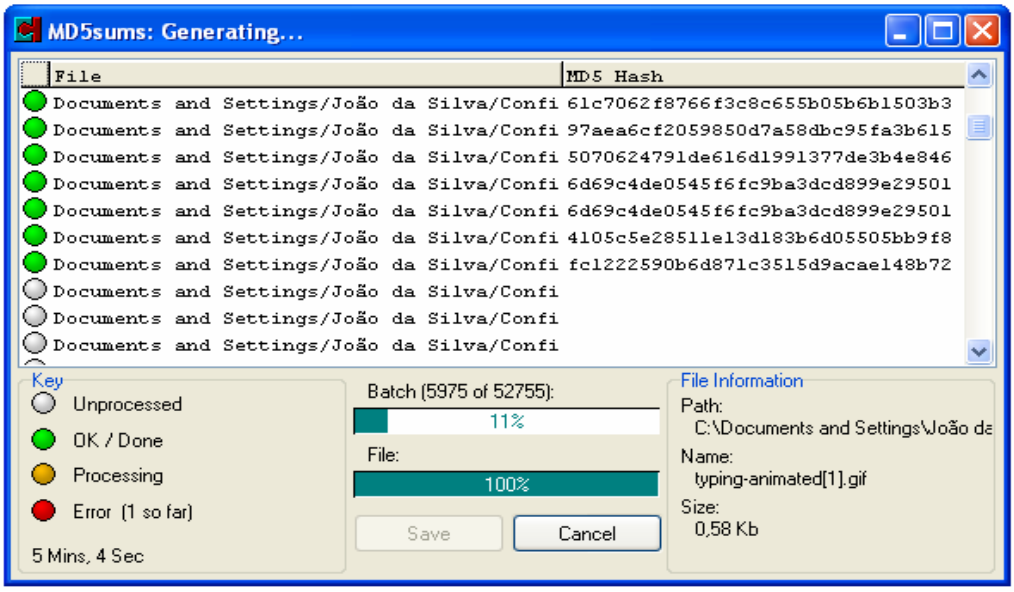

Figura 5. Utilização da ferramenta *md5summer* para geração do arquivo *hash* do disco rígido.

Com os dados coletados, pode-se aplicar as técnicas forenses para a busca e análise das evidências.

6.3 BUSCA E ANÁLISE DAS EVIDÊNCIAS

Agora com a imagem do disco rígido original criada, pode-se utilizá-la para a busca e análise de evidências, mas antes desse procedimento ser efetuado, a imagem deve ser analisada para que se tenha certeza e consiga provar que os dados contidos nela, são idênticos ao disco original.

6.3.1 Preservação e validação das evidências

Antes de começar a investigação da imagem obtida, o acesso ao disco rígido original é desabilitado por meio do painel gerenciador de dispositivos do Windows. Esse procedimento impossibilita o acesso ao disco, removendo a possibilidade do mesmo ser acessado acidentalmente e ter alguma evidência alterada.

O próximo passo é montar a imagem obtida para servir como base para a aplicação das ferramentas forenses. A imagem deve ser montada como uma unidade de somente leitura, ou seja, de forma que a mesma não possa ser alterada. Todas as requisições do sistema operacional para escrita na imagem, devem ser negadas, garantindo a integridade das evidências.

Para montar a imagem foi utilizada a ferramenta VDK (Virtual Disk Driver) conforme mostrado na Figura 6.

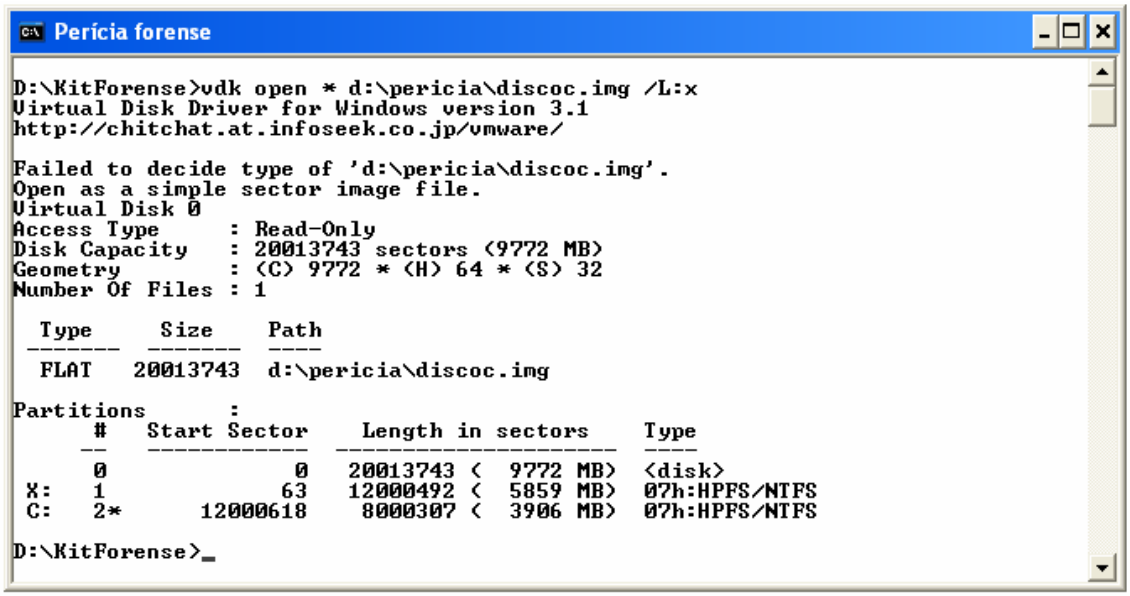

Figura 6. Utilização da ferramenta VDK para montar a imagem.

O comando para a montar a imagem, especifica que ela seja montada como unidade “X:”, como o disco rígido original possuía duas partições, a segunda partição foi montada na unidade “C:” (lembrando que o disco original que estava em “C:” foi desabilitado, deixando essa unidade disponível). Nota-se que o método de acesso à imagem é do tipo *read-only* (somente leitura), sendo assim, nenhum dado contido na mesma será alterado.

Para dar continuidade a perícia, deve-se ter certeza que o conteúdo da imagem criada pela duplicação pericial reflete exatamente os dados do disco original,

assim, deve ser efetuada a comparação entre o *hash* do disco original e da imegem. A Figura 7 mostra o resultado da comparação utilizando a ferramenta *md5summer*.

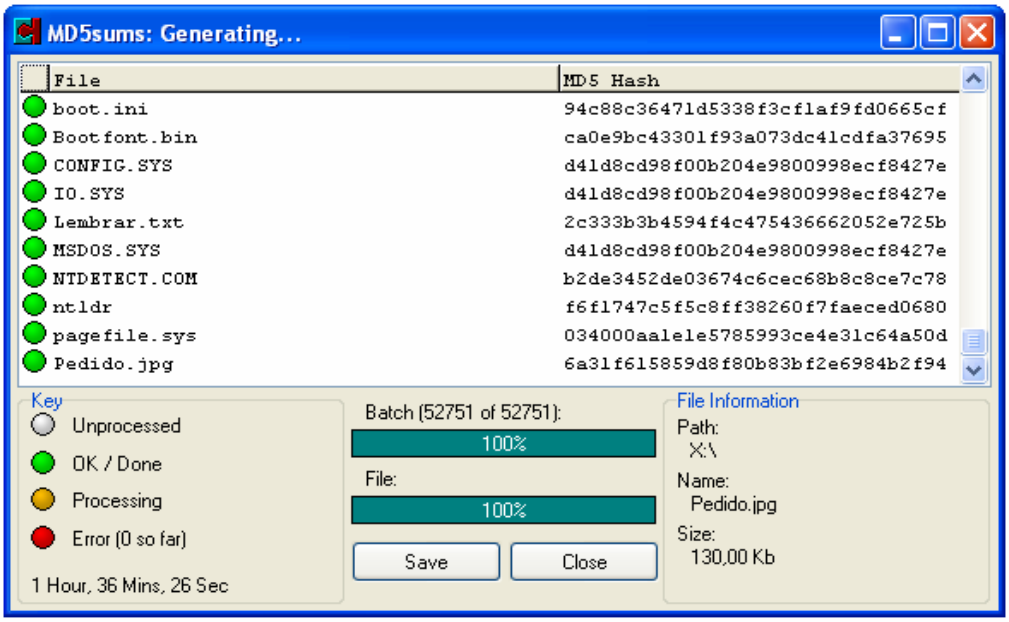

Figura 7. Comparação entre os *hashes* utilizando a ferramenta *md5summer*.

Observe que nenhum erro foi detectado no processo de comparação, indicando que os *hashes* de todos os arquivos se equivalem, garantindo assim a veridicidade da imagem a ser utilizada.

6.3.2 Listagem de arquivos

Um dos passos importantes na perícia forense é obter a lista de arquivos, organizados por data de modificação, criação e acesso. Se o perito souber o intervalo cronológico em que ocorreu o incidente, essas listas serão utilizadas para identificar os arquivos modificados, criados e acessados pelo invasor.

Para obter essa lista, utiliza-se o comando *dir* conforme as figuras abaixo:

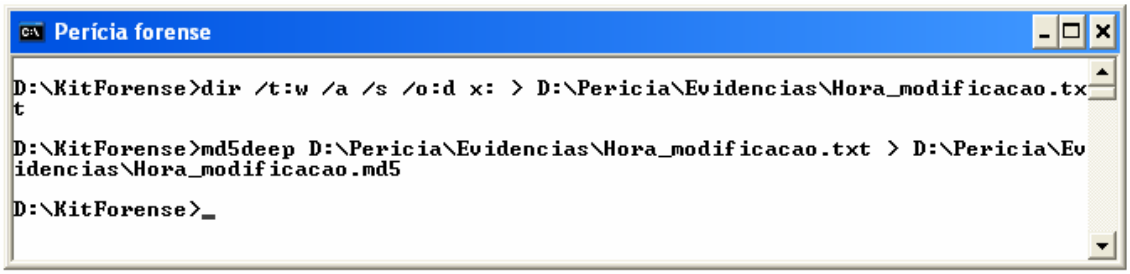

Figura 8. Comando para listagem dos arquivos em ordem cronológica de modificação.

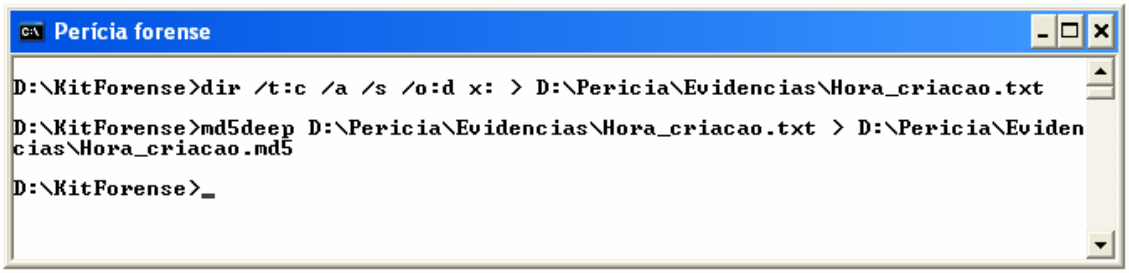

Figura 9. Comando para listagem dos arquivos em ordem cronológica de criação.

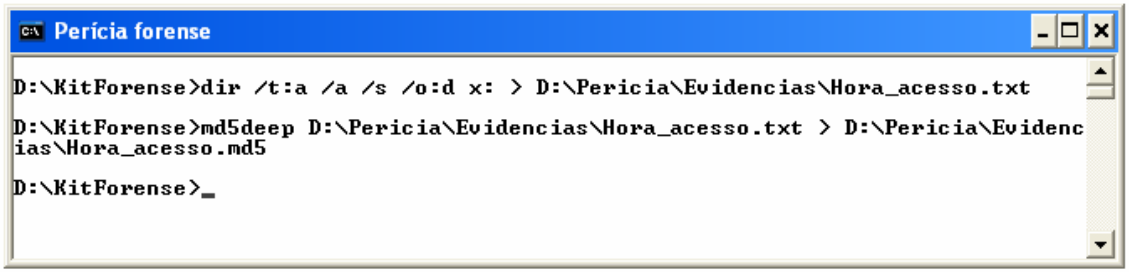

Figura 10. Comando para listagem dos arquivos em ordem cronológica de acesso.

6.3.3 Analisando *logs*

Revisando os *logs* do sistema, pode-se determinar quais usuários têm acessado arquivos específicos, rastrear o uso de aplicativos e identificar alterações nas configurações do usuário no sistema operacional.

Para analisar os *logs* contidos no sistema analisando, os arquivos com extensão ".evt", contidos em: */Windows/System32/Config*, foram copiados para a estação pericial. As diretivas de auditoria na estação foram desabilitadas para não inserir no *log* informações sobre a própria estação de trabalho pericial.

Com os *logs* copiados, a ferramenta *psloglist* pôde ser utilizada para gerar relatórios dos *logs* de aplicativo, de sistema e de segurança. A Figura 11 mostra o *log* de segurança gerado pela ferramenta.

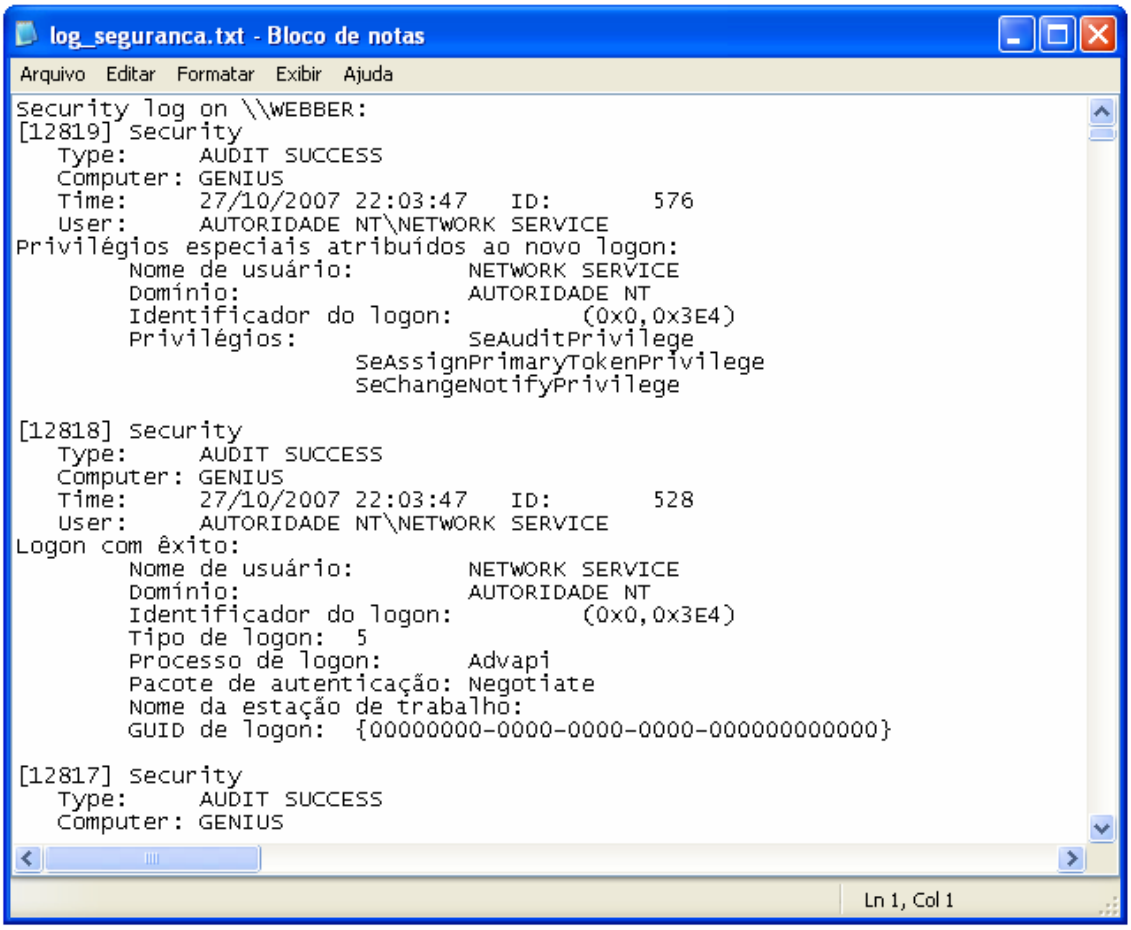

Figura 11. Relatório gerado pela ferramenta *psloglist*.

Por meio dos arquivos de *log* é possível identificar os usuários que foram autenticados ou que tiveram autenticação negada no sistema. A Ferramenta *ntlast* permite visualizar essas tentativas de *login*. Podem ser visualizadas todas as tentativas, as que tiverem êxito ou apenas as tentativas que falharam. A Figura 12 mostra a ferramenta sendo aplicada selecionando apenas as tentativas que não tiveram êxito.

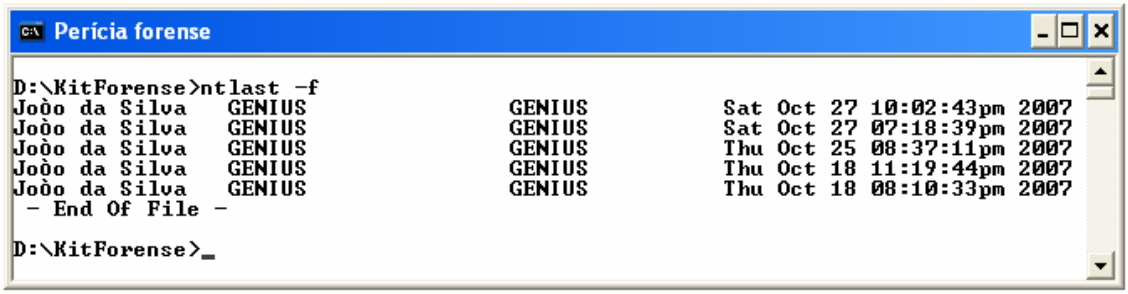

Figura 12. Utilização da ferramenta ntlast.

Observa-se na Figura 12, que por volta das oito horas, em dez dias, três tentativas de *login* fracassaram. Dependendo das outras evidências encontradas no sistema, esse fato pode remeter à uma tentativa de intrusão.

6.3.4 Alternate Data Streams

Para identificar os Alternate Data Streams, foi utilizada a ferramenta *lads*. Ela possui diversos recursos, entre eles a busca recursiva dos diretórios, indispensável para uma para a perícia em um disco rígido com muitos diretórios.

A Figura 13, mostra a ferramenta sendo utilizada para exibir os arquivos que possuem ADS.

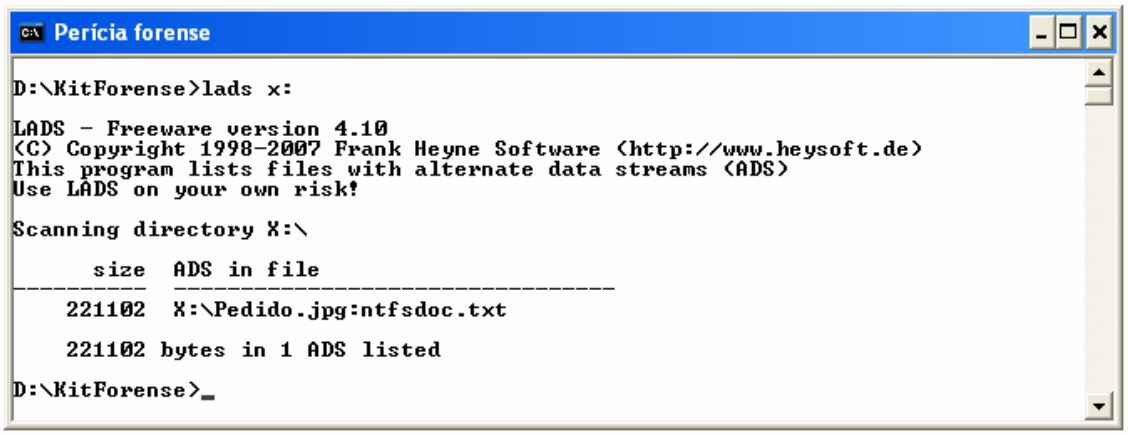

Figura 13. Identificação do ADS no arquivo.

Conforme visualizado na imagem, o arquivo *Pedido.jpg* possui um fluxo de dados com o arquivo *ntfsdoc.txt*. Sabemos que a extensão *txt* faz referencia à um

arquivo de texto, assim podemos visualizar o arquivo escondido no fluxo de dados. A Figura 14 mostra o comando para abrir o arquivo de texto.

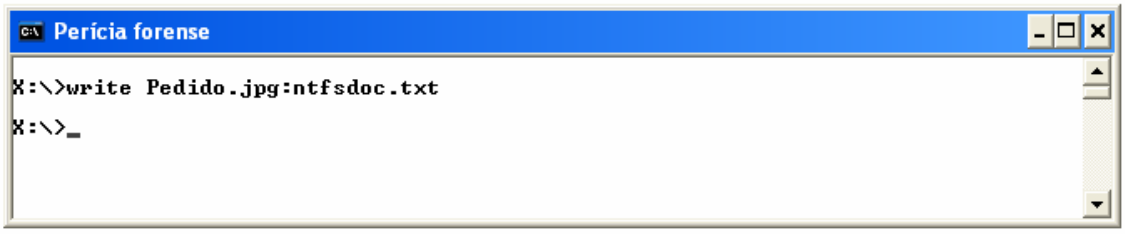

Figura 14. Comando para abrir um ADS de texto.

O comando *write* invoca o programa WordPad para abrir o arquivo *ntfsdoc.txt* que está em um fluxo de dados do arquivo *Pedido.jpg*. A Figura 15 mostra o arquivo de texto exibido quando o comando acima visto, é executado.

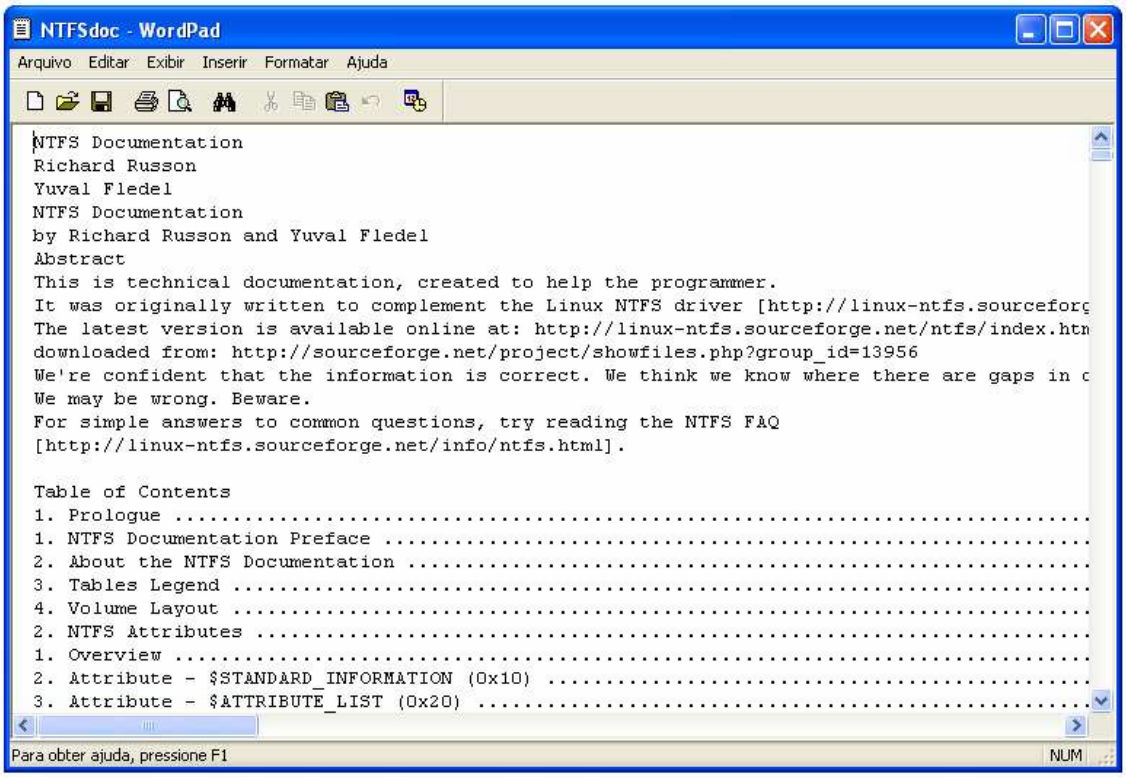

Figura 15. Texto contido no arquivo *Pedido.jpg*.

Estava escondido um arquivo de texto, mas poderiam ser outros tipos de arquivos, como um executável.ou outro arquivo de imagem. Por esses motivos a análise dos ADS em NTFS são de extrema importância para o sucesso da perícia forense.

6.3.5 Identificando permissões do arquivo

Para descobrir quem tem acesso a determinado arquivo, utiliza-se o comando *cacls*. A Figura 16 mostra a lista de controle de acesso (ACL), os usuários que tem acesso ao arquivo com ADS e seus direitos de acesso.

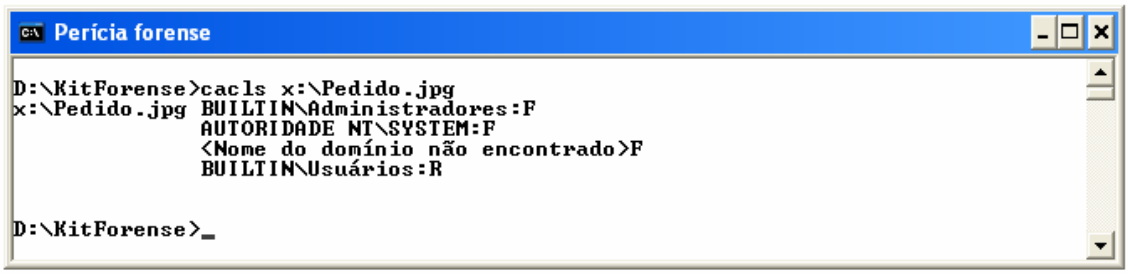

Figura 16. Lista de Controle de Acesso (ACL) do arquivo *Pedido.jpg*.

Nota-se que é exibido um domínio não encontrado, esse fato ocorre pois o ID do usuário não está contido no sistema da estação de trabalho. Essa questão torna-se um problema para a perícia, pois não é possível identificar com clareza o usuário que tem acesso ao arquivo em questão.

Os tipos de acesso são classificados:

Tipo de Acesso	Descrição
R	Ler
W	Gravar
C	Alterar
F	Controle Total

Fonte: Freitas, A. (2006).

6.3.6 Investigando o Registro

Para analisar o Registro do sistema por meio da imagem obtida, utiliza-se a ferramenta Windows Registry File Viewer (RFV). Com ela é possível selecionar o arquivo de registro que deve ser analisado.

Utilizando a ferramenta, é possível analisar a chave do Registro: *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs*. Essa chave contém a lista dos últimos arquivos utilizados pelo usuário. A Figura 17 mostra a ferramenta RFV sendo utilizada para visualizar o conteúdo da chave anteriormente citada.

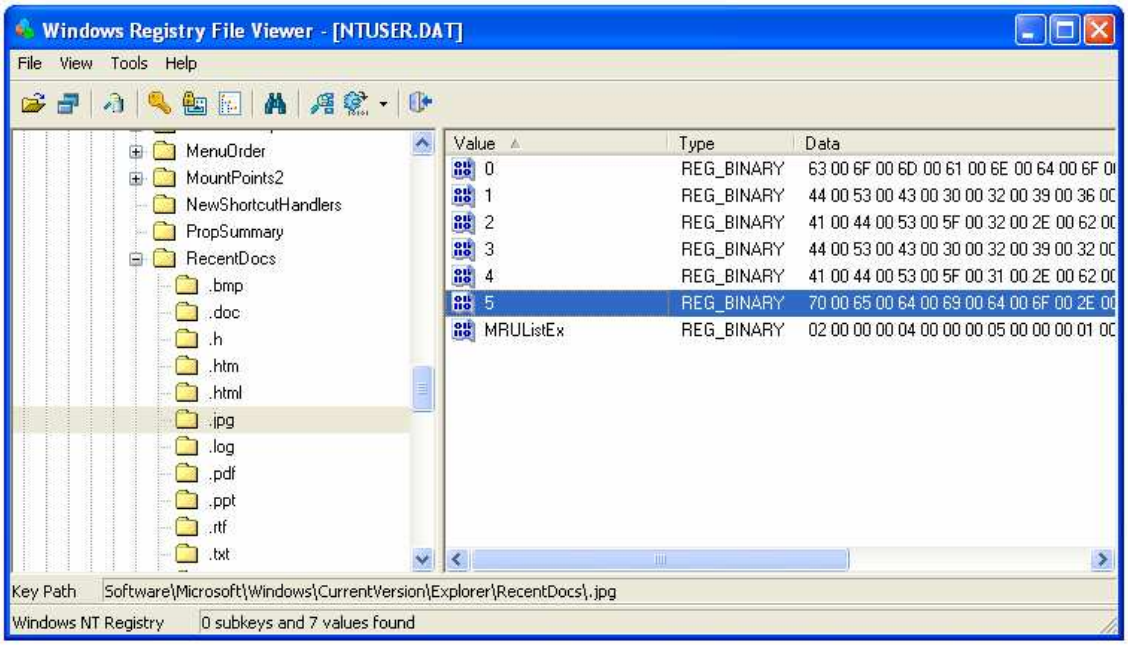

Figura 17. Análise dos arquivos utilizados recentemente.

Observando, à esquerda tem-se a estrutura dos arquivos recentes organizados por tipo. À direita, os arquivos que foram acessados e que pertencem ao tipo selecionado. Como valores de cada chave são visualizados em hexadecimal, deve-se usar o utilitário de visualização dos dados para que os mesmos sejam compreendidos.

A Figura 18 mostra as informações contidas no registro de número 5 do tipo *.jpg*.

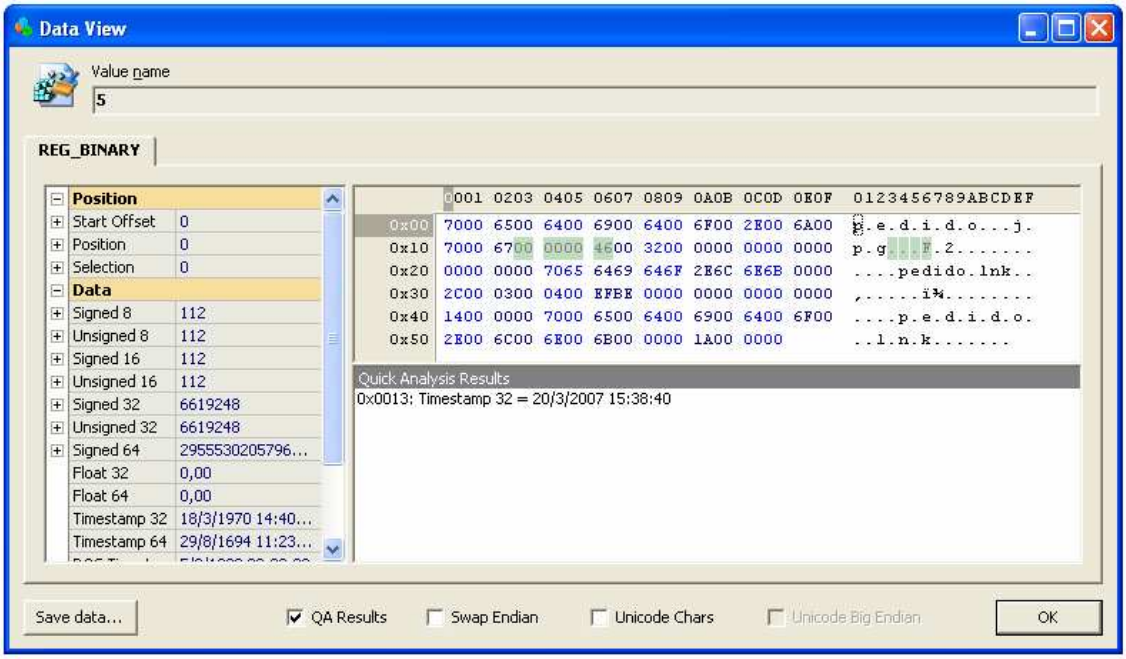

Figura 18. Visualização das informações do registro.

Nas informações geradas pela ferramenta, observa-se que o arquivo utilizado em questão, é o arquivo *Pedido.jpg*. Como o local onde se encontra o arquivo não é informado, esse pode não ser o mesmo *Pedido.jpg* anteriormente identificado e que possui o ADS. Esse fato ocorre pois outro diretório do sistema pode conter esse arquivo cujo nome é idêntico ao anterior, mas de conteúdo diferente.

6.3.7 Lixeira

Os arquivos excluídos por meio do sistema operacional são enviados para um diretório padrão chamado de Recycler. Para visualizar os arquivos contidos na Lixeira, utiliza-se o comando *dir* conforme a Figura 19.

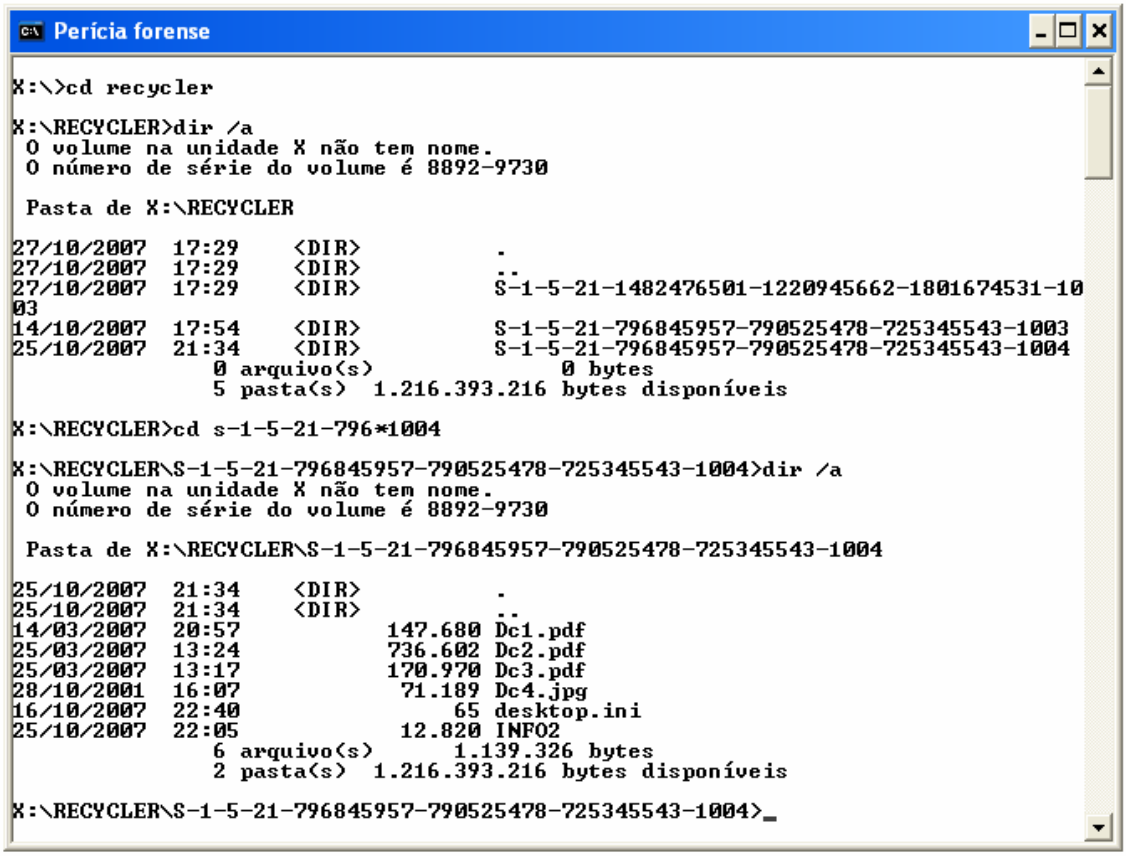

Figura 19. Conteúdo da Lixeira.

O comando *dir /a* tem como resultado a exibição dos arquivos contidos no diretório. No primeiro momento, são exibidos os subdiretórios da Lixeira, onde cada um faz referência a um usuário diferente. Depois que o diretório do usuário é selecionado, são exibidos os arquivos, mas os mesmos não estão com os nomes corretos.

As informações corretas sobre os arquivos excluídos, estão contidas no arquivo *INFO2*, e para visualizá-las é utilizada a ferramenta *rifiuti*. A Figura 20 mostra como a ferramenta é utilizada para a análise.

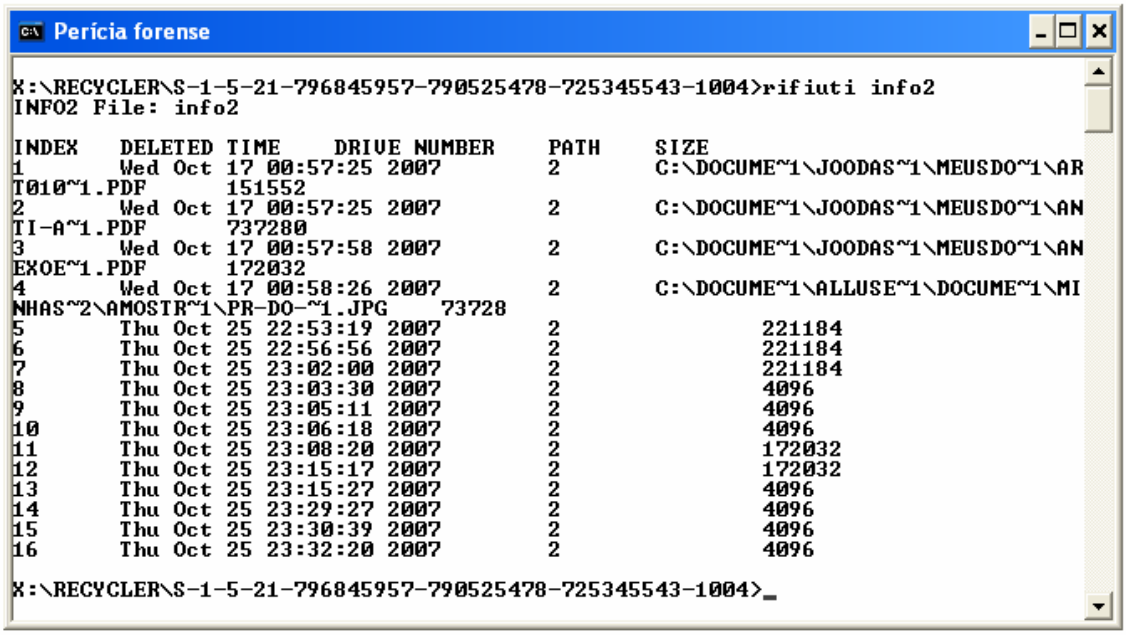

Figura 20. Utilização da ferramenta *rifiuti*.

Com a utilização da ferramenta as informações são corretamente exibidas. Pelo fato de não possuírem os caminhos dos arquivos, os índices 5 ao 16 fazem referência a arquivos que já foram apagados da Lixeira.

6.3.8 Recuperando arquivos excluídos

Para recuperar os arquivos que foram excluídos da lixeira ou possivelmente apagados com uma formatação rápida do disco, utilizou-se a ferramenta File Recovery. A Figura 21 mostra a ferramenta sendo utilizada para recuperação de informações.

Vários *clusters* foram restaurados e tiveram seu conteúdo analisado. Eles continham arquivos de texto, fotos pessoais entre outros.

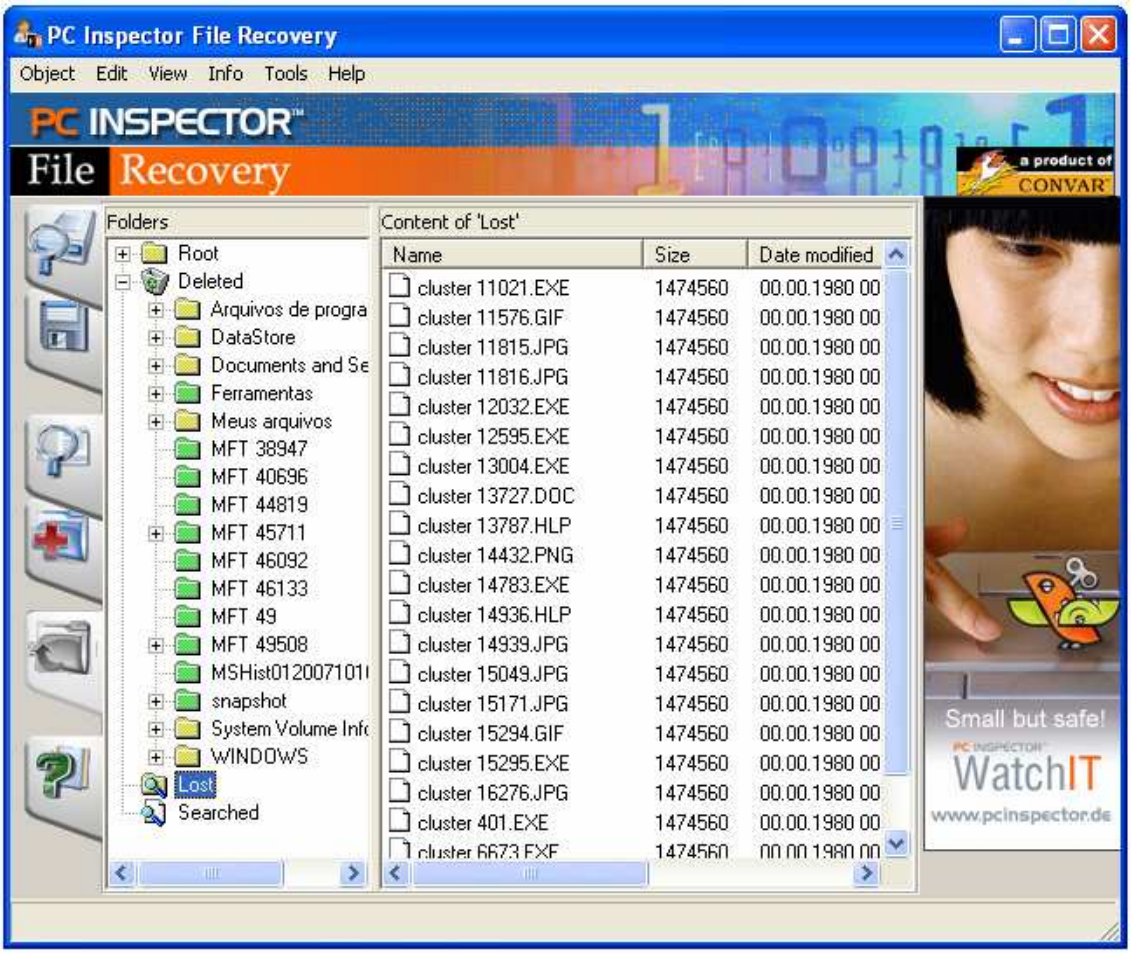

Figura 21. Dados recuperados com a ferramenta File Recovery.

6.3.9 Busca por palavras-chave

A ferramenta Disk Investigator é utilizada para a busca de palavras-chave na imagem. Essa ferramenta exibe todos os resultados possíveis, não considerando os atributos do sistema operacional, como arquivo oculto ou excluído.

A Figura 22 mostra o resultado de uma busca pela expressão “Senha pessoal” na imagem do disco utilizada para a perícia.

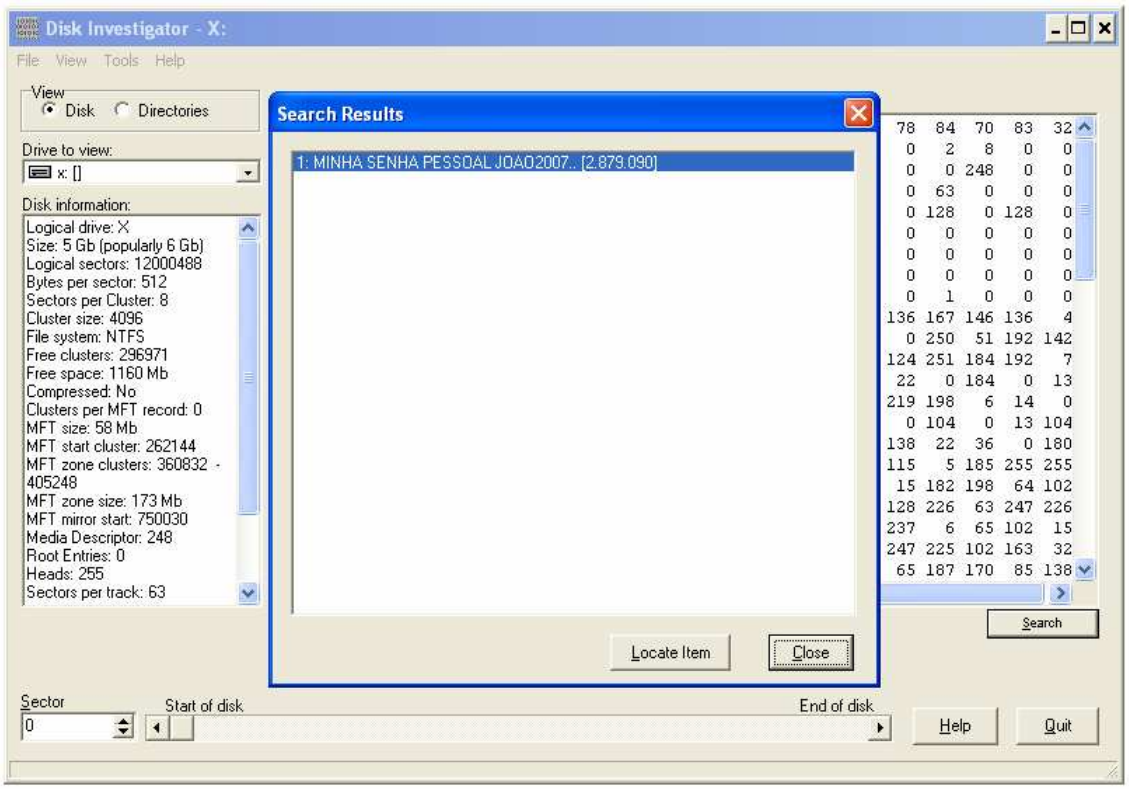

Figura 22. Ferramenta Disk Investigator.

A tela exibida traz o resultado da busca com o número do *cluster* em que a palavra foi encontrada. A Figura 23 demonstra a exibição do conteúdo do *cluster* localizado.

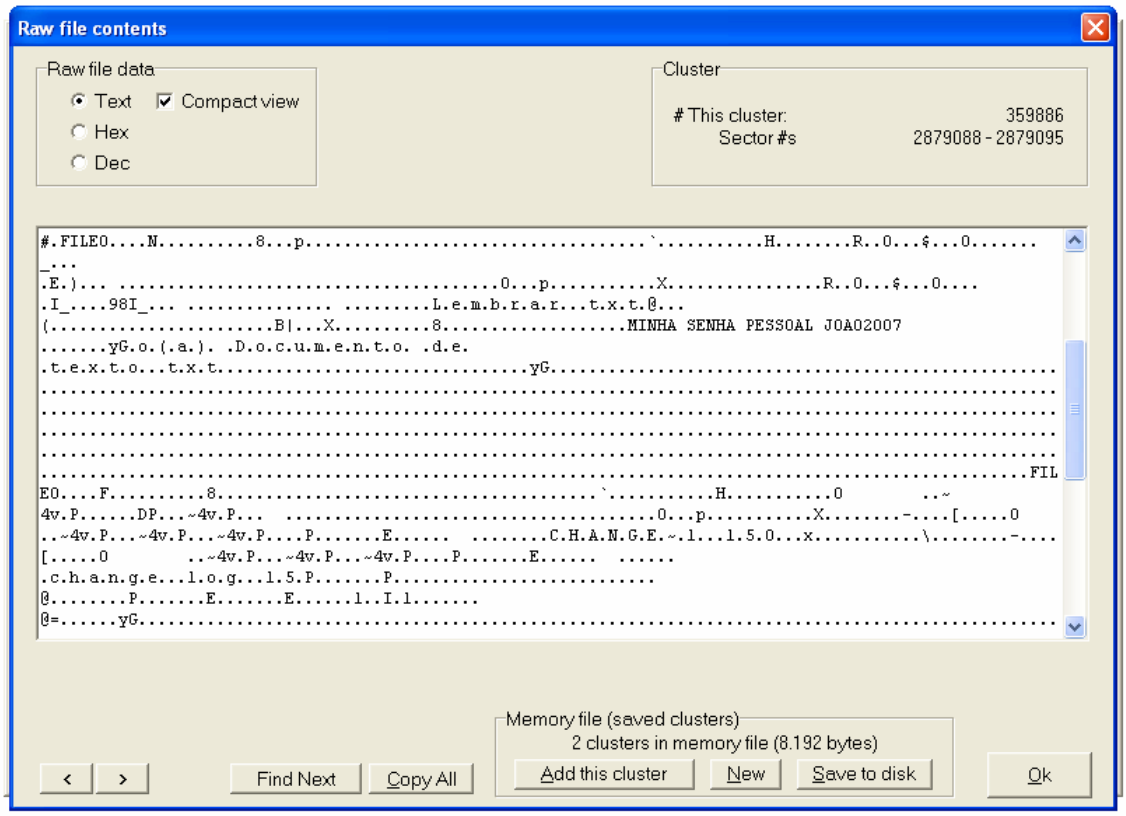

Figura 23. Conteúdo do *cluster* localizado.

No conteúdo do *cluster*, uma frase chama a atenção: “minha senha pessoal joao2007”. Essa deve ser a senha padrão do usuário João da Silva, e provavelmente é utilizada em várias ocasiões.

6.3.10 Analisando e-mails

A busca por *e-mails* recebidos e enviados é de extrema importância para a perícia forense. No sistema analisado, foram encontrados os arquivos do gerenciador de *e-mails* Outlook Express, contendo as caixas de mensagens de entrada, saída e enviados. A Figura 24 mostra os arquivos e o local onde os mesmos foram encontrados.

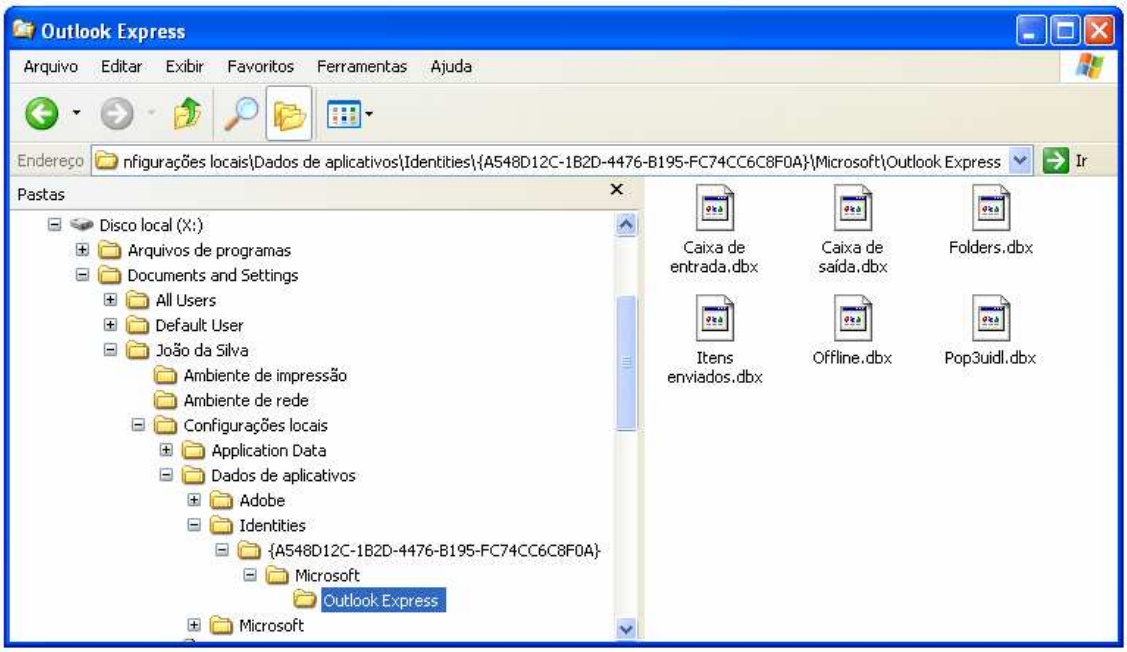

Figura 24. Arquivos do Outlook Express encontrados.

Para serem analisados, esses arquivos foram copiados para a estação de trabalho pericial. Uma vez importadas as caixas de mensagens, as mesmas podem ser visualizadas por meio do próprio Outlook Express instalado na estação.

Observando as mensagens contidas, uma chamou a atenção. A Figura 25 mostra o conteúdo dessa mensagem.

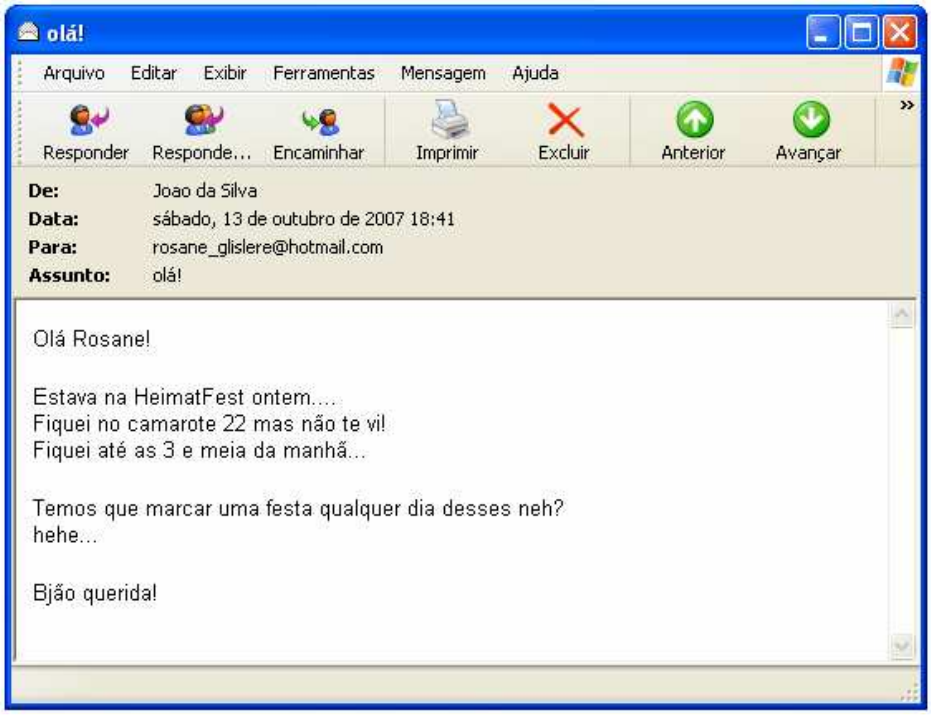

Figura 25. *E-mail* enviado.

Foi observado que a mensagem possui no texto, a informação do local e do horário onde o suspeito estava no dia anterior ao envio do *e-mail*. Conforme a figura, a data de envio do *e-mail* foi dia 13 de outubro de 2007, portanto a festa foi no dia 12.

Essa mensagem poderia ser o álibi do suspeito caso ele fosse acusado de algum crime ocorrido no dia 12 de outubro de 2007.

6.3.11 Investigando o navegador de Internet

O navegador utilizado no sistema periciado é o Internet Explorer, o navegador padrão para o sistema operacional Windows XP. Foram feitas buscas pelos *sites* acessados recentemente, *sites* favoritos, e arquivos temporários do navegador.

A Figura 26 mostra os sites que estão no menu Favoritos do navegador. Esses *sites* informam o tipo de conteúdo preferido pelo usuário na Internet, ajudando a definir o perfil do mesmo.

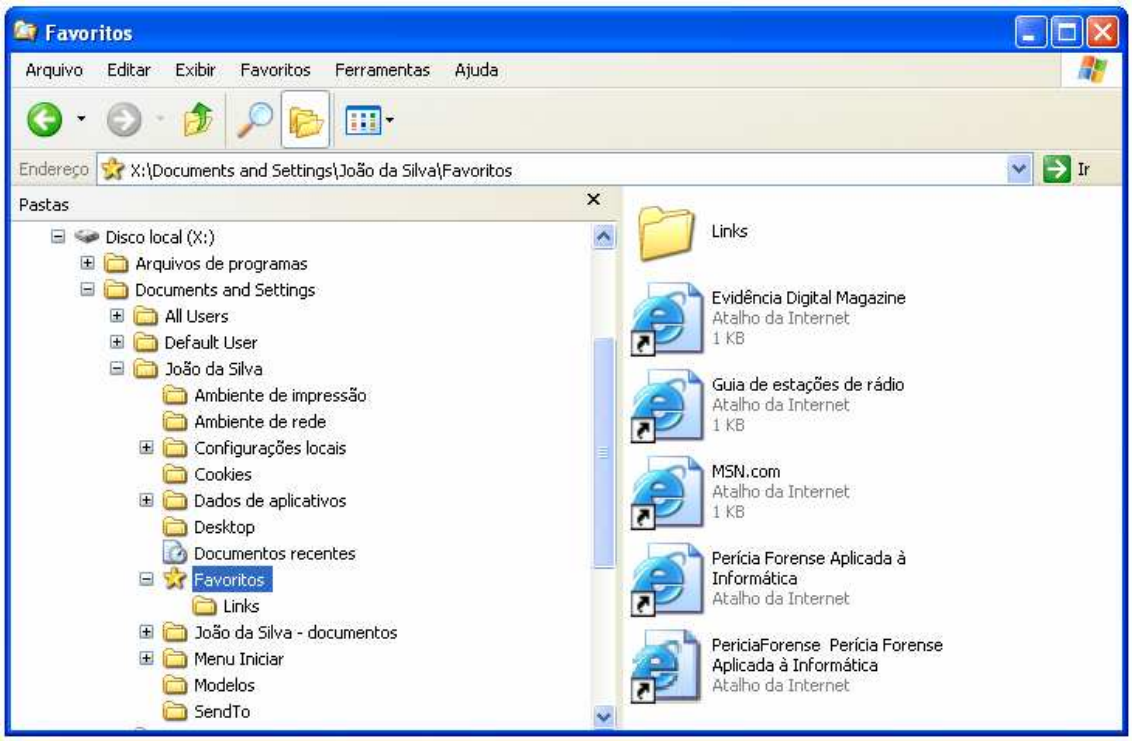

Figura 26. *Sites* favoritos do Internet Explorer.

A Figura 27 mostra os arquivos temporários do navegador e o local onde os mesmos foram encontrados.

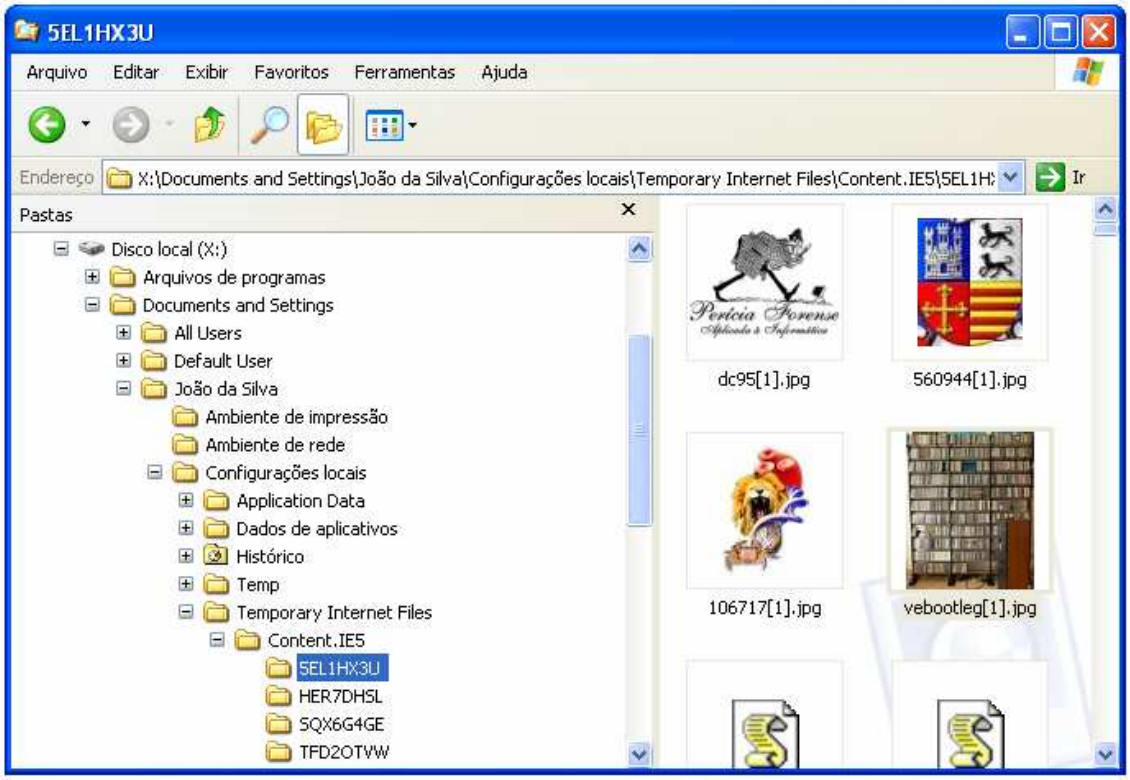

Figura 27. Arquivos temporários do Intenet Explorer.

Para analisar o histórico de Internet, foi utilizada a ferramenta *IEHistoryView*. Essa ferramenta permite visualizar as informações contidas nos arquivos *index.dat* que armazenam os dados das páginas de Internet acessadas. Esses arquivos são encontrados em: *x:\Documents and Settings\João da Silva\Configurações Locais\Histórico\History.IE5*.

A Figura 28 mostra as informações do histórico do navegador, são exibidos: o endereço da página, o título da página, a quantidade de cliques do *mouse* na página, a data de modificação, data de expiração e nome do usuário que acessou a página.

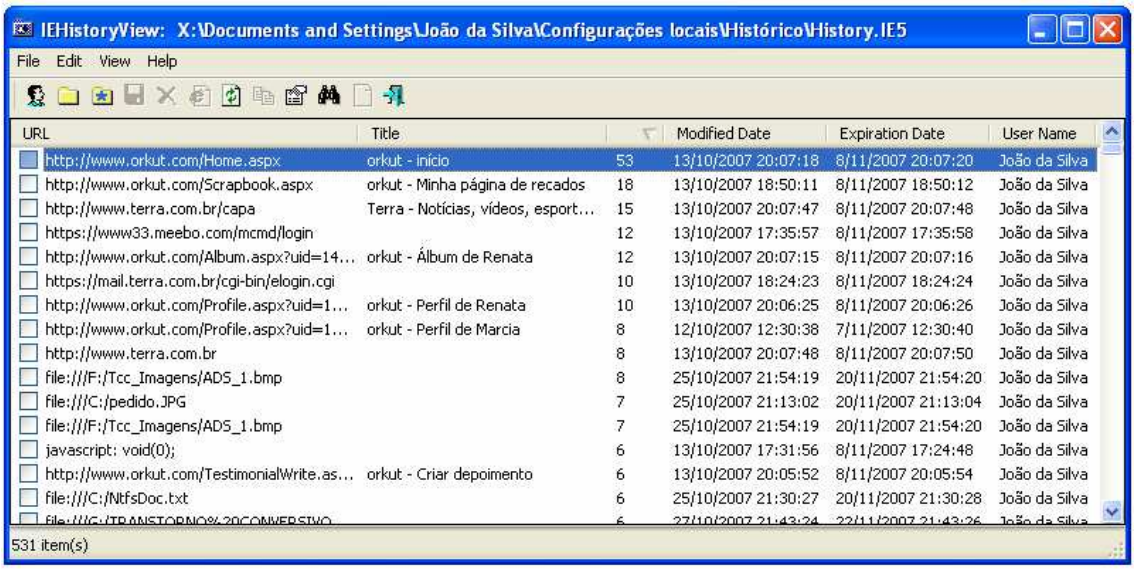

Figura 28. Histórico do Internet Explorer.

A exibição dos históricos está organizada pela ordem descendente do número de cliques. Observa-se que um dos *sites* preferidos do usuário é o *www.orkut.com*, um site de relacionamentos na Internet. Nota-se também, pela quantidade relevante de cliques, que o usuário navegou pelo álbum de Renata e de Márcia, mostrando um provável interesse do usuário nessas duas pessoas.

Para organizar e apresentar as evidências da perícia, foram gerados relatórios das informações obtidas do histórico de Internet. A Figura 29 mostra o relatório gerado pela própria ferramenta *IEHistoryView*.

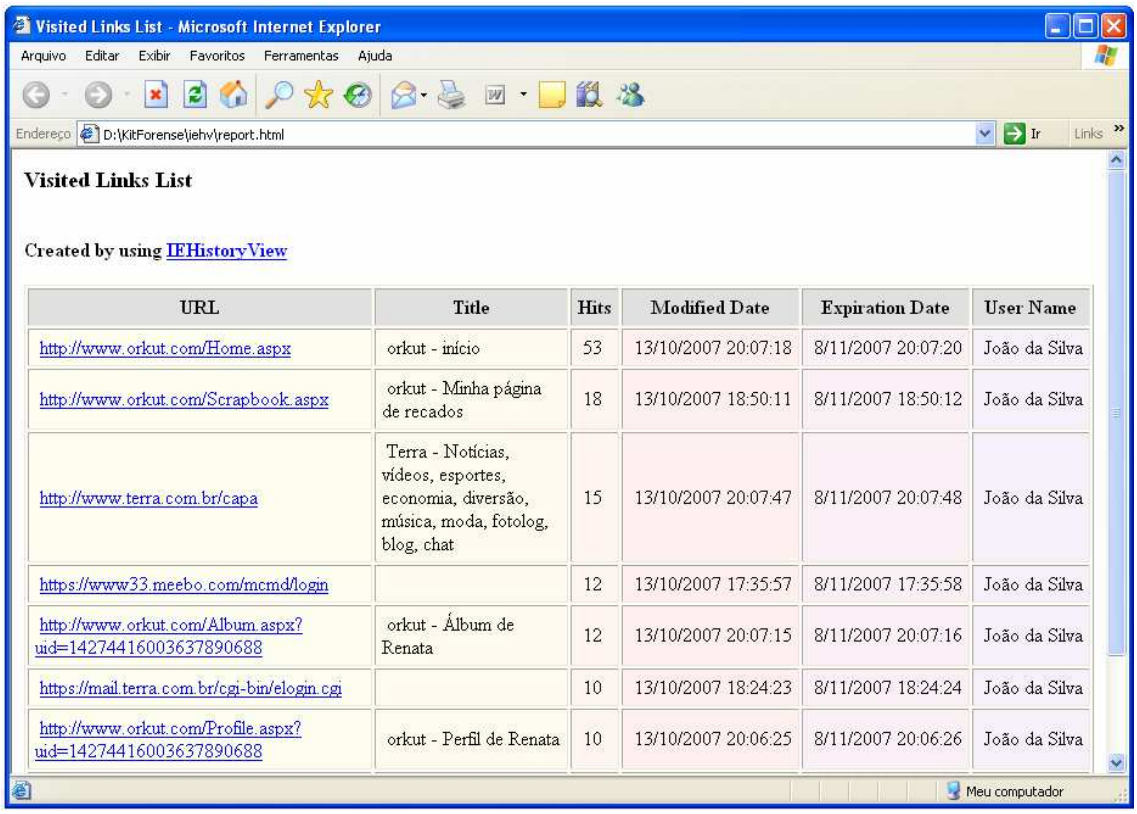

Figura 29. Relatório do histórico de Internet.

6.3.12 Documentando comandos

Antes do *prompt* de comando ser finalizado, foram documentados os comandos executados.. Esse procedimento aumenta a confiabilidade na perícia, pois todos os comandos utilizados podem ser analisados e verificado se algum deles pode ter danificado alguma evidência. A Figura 30 mostra o comando que armazena em um arquivo de texto, os comandos utilizados no *prompt*. Em seguida é gerado o *hash* para garantir a integridade do arquivo de texto gerado.

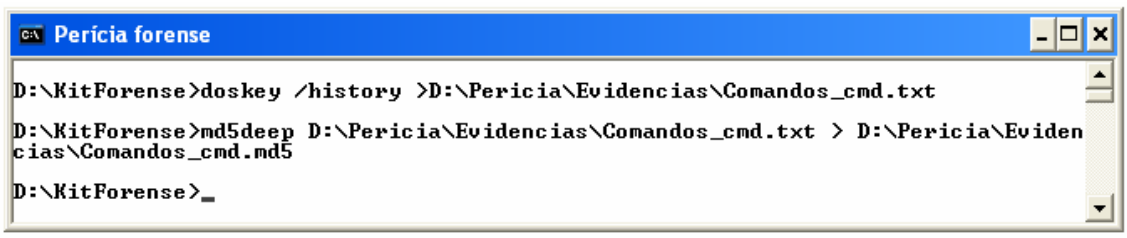

Figura 30. Utilização do comando *doskey* para documentação dos comandos executados.

6.4 ANÁLISE FINAL

Após as etapas de coleta e análise das evidências, o perito tem a capacidade de desenvolver um relatório sobre o sistema periciado, enumerando as evidências encontradas, como o ADS no arquivo *Pedido.jpg* e correlacionar as evidências aos fatos de modo geral, atingindo o objetivo da perícia em questão.

CONCLUSÃO

À medida que os crimes digitais aumentam, cresce a necessidade da utilização da perícia forense no combate a esses tipos de crime e criminosos. As evidências digitais encontradas, documentadas e apresentadas pelos peritos em sistemas analisados, estão sendo utilizadas cada vez mais em processos criminais na busca pelo correto julgamento do acusado. Muitas vezes, essas evidências têm maior valor, do que provas encontradas utilizando-se a perícia tradicional.

Por esse motivo, os procedimentos adotados durante a perícia devem ser claros, transparentes e objetivando sempre a busca pela verdade, sem distorção ou omissão de informações relevantes ao resultado da perícia. A utilização de técnicas avançadas e inovadoras por parte dos criminosos, faz necessária a capacitação do perito nos diversos ambientes computacionais. Todos os dados levantados durante o processo devem ser cientificamente autênticos para que o resultado reflita a realidade e para que o júri possa utilizar a perícia como uma ferramenta para a punição do criminoso.

A perícia forense em ambientes New Technologies File System, traz excelentes resultados na investigação de crimes que têm por meio o ambiente computacional. As evidências digitais encontradas, na sua maioria podem ser comprovadas e utilizadas de modo seguro, mas para isso, deve ser utilizada uma metodologia comprovada para a busca, preservação e análise das evidências. A complexidade do sistema de arquivos NTFS exige experiência, capacitação e um apurado raciocínio lógico do perito, para que se obtenha ótimos resultados da perícia forense.

Um dos pontos negativos do NTFS é a falta de documentação. Como este é um sistema de arquivos “fechado”, o fabricante não disponibiliza toda a literatura

necessária para a compreensão detalhada sobre o sistema. Em contra partida, grupos de *software* livre estudam esse sistema de arquivos e divulgam os resultados obtidos para a comunidade científica, dando as condições básicas ao perito para decidir quais as técnicas forenses serão adotadas em cada caso.

A metodologia e as técnicas a serem aplicadas na perícia, dependem do tipo de crime e do ambiente encontrado, por esse motivo algumas técnicas abordadas durante esse trabalho podem ser inaplicáveis enquanto outras se enquadram perfeitamente no ambiente analisado. De maneira geral, a parte prática mostrou que é possível gerar bons resultados aplicando-se as ferramentas forenses utilizadas, em um ambiente NTFS. A documentação das evidências e a metodologia aplicada agregaram autenticidade às evidências, podendo estas, serem utilizadas para diversos fins.

Para encerrar, o presente trabalho abre as portas para os trabalhos futuros, que podem ser aprofundados em áreas específicas como aplicação da perícia forense computacional na memória principal e nos arquivos de paginação do sistema operacional. A constante inovação das formas de crimes digitais, torna necessária a atualização dos procedimentos forenses adotados neste trabalho.

REFERÊNCIAS

BERNARDO, Adauto de Souza. **Técnicas Computacionais no Auxílio à Perícia Forense na análise de evidências coletadas em servidores GNU/LINUX**. 2006. 106 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade do Extremo Sul Catarinense, Criciúma.

BIDWELL, Teri; CROSS, Michael; RUSSEL, Ryan. **Hack Proofing Your Identity in the Information Age**. Massachusetts: Syngress Publishing, Inc., 2002.

BITENCOURT, Cezar R. **Tratado de Direito Penal: parte geral.** 11.ed. São Paulo: Saraiva, 2006.

Brasil, Decreto lei nº. 2.848, de 7 de outubro de 1940. **Institui o Código Penal.** Diário Oficial (da República Federativa do Brasil) Rio de Janeiro, p. 2391, 31 dez. 1940.

Brasil, Lei no 9.296, de 24 de julho de 1996. **Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.** Diário Oficial (da República Federativa do Brasil) Brasília, p. 13757, 25 jul. 1996.

CARICATTI, André Machado; RODRIGUES, Jorilson da Silva: **Criminalística Computacional - Alguns Procedimentos Legais.** VI Simpósio de Segurança em Informática. 2004.

CARRIER, Brian. **File System Forensic Analysis.** Indiana: Addison Wesley. Professional, 2005.

CASEY, Eoghan. **Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.** 2d. Londres: Academic Press, 2004.

CHOFFNES, David; DEITEL, Harvey; DEITEL, Paul. **Sistemas Operacionais.** 3. ed**.** São Paulo: Pearson Prentice Hall, 2005.

FERREIRA, Aurélio Buarque de Holanda. **Novo Aurélio Século XXI: o dicionário da língua portuguesa.** 3.ed. Rio de Janeiro: Nova Fronteira, 1999. 2128 p.

FREITAS, Andrei Rodrigues de. **Perícia Forense Aplicada à Informática.** Rio de Janeiro: Brasport 2006.

LEITE, Thiago F. M. **Perícia Forense em Software Livre.** 2006. 155 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – UNIDESC.

MICHAELIS: moderno dicionário da língua portuguesa.. São Paulo: Ed. Melhoramentos, 1998. 2259 p

MOHAY, George M. et al. **Computer and Intrusion Forensics.** Massachusetts: Artech House, 2003.

OLIVEIRA, F. de S. (Discente-Autor /Mest.Acadêmico); Cardoso Guimarães, C. (Docente); de Geus, P. L. (Docente): **Metodologias de análise forense para ambientes baseados em NTFS**; III Simpósio de Segurança em Informática; 2001; 1; 1; 1; 1; 83; 90; SSI'2001 - Simpósio de Segurança em Informática; São José dos Campos, SP, Brasil; BRASIL; Português; ; Impresso; ; .

PROSISE, Chris; MANDIA, Kevin. **Hackers: resposta e contra-ataque.** Rio de Janeiro: Campus, 2002.

PROSISE, Chris; MANDIA, Kevin. **Incident Response & Computer Forensics.** 2.d. [S.I.]: McGraw-Hill/Osborne, 2003.

RUSSON, Richard; FLEDEL, Yuval**. NTFS Documentation.** Versão 0.5, 2005. Linux-NTFS Project [http://linux-ntfs.sourceforge.net/]

SCHWEITZER, Douglas. **Incident Response: Computer Forensics Toolkit.** Indiana: Wiley Publishing, 2003.

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

TREVENZOLI, Ana Cristina. **Perícia forense computacional – ataques, identificação da autoria, leis e medidas preventivas.** 2006. 89f. Trabalho de Conclusão de Curso (Especialista em Segurança de Redes e Sistemas) - Faculdades Senac – Sorocaba, Sorocaba.

VACCA, John R. **Computer Forensics-Computer Crime Scene Investigation.** Massachusetts: Charles River Media, 2002.

ANEXO A – Eventos de auditoria

Evento	Descrição
528	O usuário fez logon com sucesso
529	Tentativa de logon feita com um nome de usuário desconhecido ou com um nome de usuário correto mas com uma senha incorreta.
530	Usuário tentou fazer logon fora do horário especificado.
531	Tentativa de logon utilizando uma conta desativada.
532	Tentativa de logon usando uma conta expirada.
533	Usuário não tem permissão para fazer logon nesse computador.
534	Usuário tentou fazer um logon com um tipo de logon que não é permitido, como rede, interativo, serviço, lote ou interativo remoto.
535	A senha para a conta especificada expirou.
536	O serviço Net Logon não está ativo.
537	Tentativa de logon falhou por outros motivos.
538	Usuário fez logoff.
539	A conta estava bloqueada no momento em que a tentativa de logon foi feita.
540	Logon realizado com sucesso.
624	Conta de usuário criada.
625	Tipo de conta do usuário alterado.
626	Conta de usuário ativada.
627	Tentativa de alteração de senha.
629	Conta de usuário desativada.
628	Senha de usuário foi definida
630	Conta de usuário excluída.
631	Grupo global que permite segurança foi criado.
632	Membro do grupo global que permite segurança foi adicionado.
633	Membro do grupo global que permite segurança foi removido.
634	Grupo global que permite segurança foi excluído.
635	Grupo local que não permite segurança foi criado.
636	Membro do grupo local que permite segurança foi adicionado.
637	Membro do grupo local que permite segurança foi removido.
638	Grupo local que permite segurança foi excluído.
639	Grupo local que permite segurança foi alterado.
641	Grupo global que permite segurança foi alterado.
642	A conta de usuário foi alterada.
643	A política de domínio foi alterada.
644	A conta de usuário foi bloqueada.
672	Um ticket de serviço de autenticação foi emitido e validado com sucesso.
673	Um ticket de serviço de concessão de ticket foi concedido.
674	A segurança principal renovou um ticket.
675	A pré-autenticação falhou.
676	A solicitação de ticket de autenticação falhou.
677	Um ticket não foi concedido.
678	Uma conta foi mapeada com sucesso para uma conta de domínio.
680	Identifica a conta utilizada na tentativa de logon bem sucedido.
681	Foi tentado um loggon de conta de domínio.
682	O usuário reconectou a uma sessão do Terminal Services que estava desconectada.
683	O usuário desconectou uma sessão do Terminal Services sem fazer o logof

Fonte: Freitas, A. (2006).

ANEXO B – IDs de evento do log de segurança

Evento	Descrição
516	Alguns registros de evento de auditoria descartados.
517	Log de auditoria limpo.
528	Logon bem-sucedido.
529	Logon falhou.
531	Logon falhou, bloqueado.
538	Logoff bem sucedido.
576	Atribuição e uso dos direitos.
578	Uso de serviço privilegiado.
595	Acesso indireto a objeto.
608	Mudança nas diretivas de direitos.
610	Novo domínio confiável.
612	Mudança na diretiva de auditoria.
624	Nova conta adicionada.
626	Conta de usuário ativada.
630	Conta de usuário excluída.
636	Mudança no grupo de contas.
642	Mudança na conta de usuário.
643	Mudança na diretiva de domínio.

Fonte: Mandia, K.; Prosise, C. (2001).