

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN**

Cinthia Meire de Azevedo Silva

FORENSE COMPUTACIONAL COM FERRAMENTAS WINDOWS

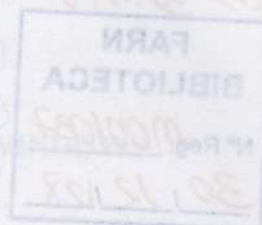
FORENSE COMPUTACIONAL COM FERRAMENTAS WINDOWS

Orientador:

Ricardo Kleber Martins Galvão, M. Sc.

**NATAL / RN
2006**

CINTHIA MEIRE DE AZEVEDO SILVA



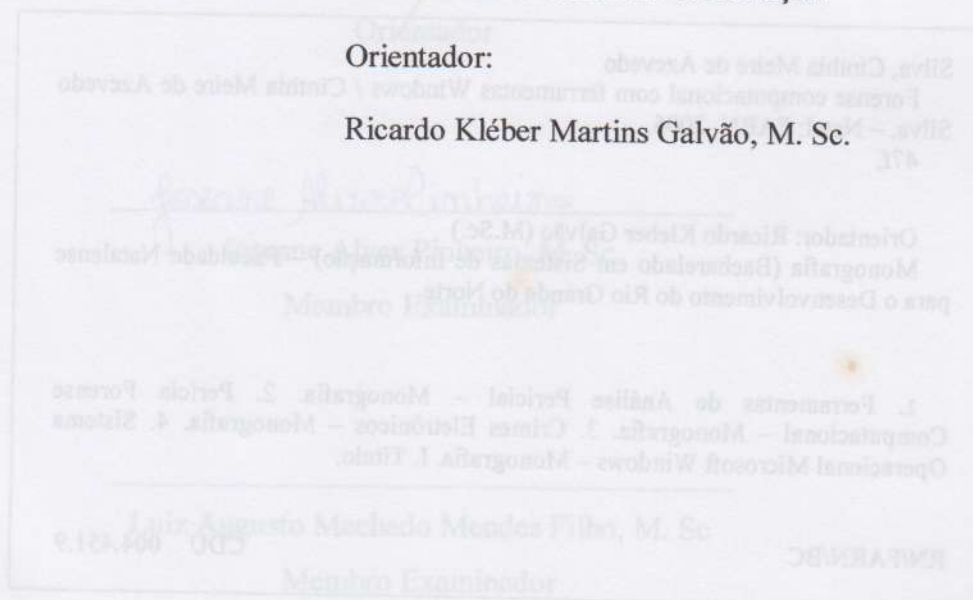
FORENSE COMPUTACIONAL COM FERRAMENTAS WINDOWS

Monografia apresentada ao Curso de Bacharelado em Sistemas de Informação da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte e aprovada em 19 de dezembro de 2006 pela banca examinadora composta pelos seguintes membros:

Monografia apresentada ao curso Bacharelado em Sistemas de Informação da Faculdade Natalense para o desenvolvimento do Rio Grande do Norte, como requisito obrigatório para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador:

Ricardo Kléber Martins Galvão, M. Sc.



NATAL / RN

2006

RB- 31.748

M



004.451.9

e5794

2006

ex 01

Catalogação na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Silva, Cinthia Meire de Azevedo

Forense computacional com ferramentas Windows / Cinthia Meire de Azevedo

Silva. – Natal: FARN, 2006.

47f.

Orientador: Ricardo Kleber Galvão (M.Sc.)

Monografia (Bacharelado em Sistemas de Informação) – Faculdade Natalense
para o Desenvolvimento do Rio Grande do Norte.

1. Ferramentas de Análise Pericial – Monografia. 2. Perícia Forense
Computacional – Monografia. 3. Crimes Eletrônicos – Monografia. 4. Sistema
Operacional Microsoft Windows – Monografia. I. Título.

RN/FARN/BC

CDU 004.451.9

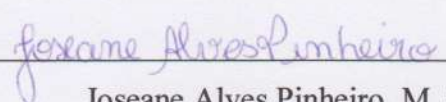
CINTHIA MEIRE DE AZEVEDO SILVA

FORENSE COMPUTACIONAL COM FERRAMENTAS WINDOWS

Monografia apresentada ao Curso de Bacharelado em Sistemas de Informação da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte e aprovada em 19 de dezembro de 2006 pela banca examinadora composta pelos seguintes membros:



Ricardo Kléber Martins Galvão, M. Sc
Orientador



Joseane Alves Pinheiro, M. Sc.
Membro Examinador

Luiz Augusto Machado Mendes Filho, M. Sc
Membro Examinador

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus por mais uma vitória alcançada, guiando e iluminando sempre os meus passos em todos os momentos de minha vida. A minha mãe, um exemplo de mulher guerreira, que com todas as dificuldades encontradas na vida, conseguiu me educar, mostrando-me sempre o melhor caminho a ser percorrido, pelo amor incondicional, suportando a distância durante todo esse tempo de minha vida acadêmica. A você, padrinho, que surgiu em minha vida para preencher um espaço tão importante que eu não conhecia, desempenhando brilhantemente o papel de um verdadeiro pai, meu muito obrigada. Essa vitória não é minha, é de vocês, que sempre acreditaram em mim. A toda minha família, em especial a Sara Cassiano, que sempre esteve ao meu lado me encorajando, e mostrando que valia a pena seguir em frente, principalmente nos momentos em que pensei em desistir, obrigada Sarinha. Aos amigos, que já existiam em minha vida e aos que fiz, pela amizade e companheirismo, a todos os mestres que me ensinaram coisas novas durante esses quatros anos, e ao meu orientador, pelas sugestões, críticas e conselhos, mestre SCARDUSKLEBS, obrigada. E fica aqui, a esperança de que um novo e brilhante caminho está por vir.

RESUMO

ABSTRACT

Os computadores estão cada vez mais presentes na vida das pessoas. Os últimos anos foram de grandes avanços tecnológicos, com isso, surgiram diversos tipos de crimes, principalmente os crimes eletrônicos. É possível fazer desde pagamentos, transferências bancárias, compras, tudo isso utilizando a Internet e o computador. Dados importantes são jogados na rede, como número de conta bancária, número de cartão de crédito, número de documentos pessoais, endereços, fotografias, e a qualquer momento um desses dados pode cair em mãos de pessoas ilícitas. Para se chegar ao acusado de atos ilícitos, utilizando o computador, é preciso que seja feita a perícia na máquina suspeita. Tal procedimento pode ser feito com a ajuda de diversos tipos de ferramentas que auxiliam ao perito a encontrar, de forma rápida e segura, provas que possam ser usadas contra o usuário da máquina investigada. Surge assim, a necessidade de investigar crimes cometidos através do uso do computador. O presente trabalho tem por objetivo apresentar as principais ferramentas baseadas no Sistema Operacional Microsoft Windows utilizadas na Perícia Forense Computacional, no qual foram pesquisadas diversos tipos de ferramentas que podem auxiliar na perícia forense. Entre elas existem desde ferramentas auxiliares até ferramentas completas, onde podem ser usadas como fonte de apoio para os peritos (investigadores).

Keywords: Electronic crimes. Tools of it Analysis Pericial, Forensic Computational.

Palavras-chave: Crimes Eletrônicos. Ferramentas de Analise Pericial. Forense Computacional. Perícia Forense.

ABSTRACT

The computers are more and more presents in the people's life. The last years were of great technological progresses, with that, several types of crimes, mainly the electronic crimes appeared. It is possible to do from payments, bank transfers, purchases, all this using the Internet and the computer. Important data are played in the net, as number of bank bill, credit card number, number of personal documents, addresses, pictures, and to any moment one of those data can drop in illicit people's hands. To arrive to the accused of illicit acts, using the computer, it is necessary that is made the know-how in the machine he/she suspects. Such procedure can be made with the help of several types of tools that you/they aid to the expert to find, in a fast way and it holds, tests that can be used against the user of the investigated machine. It appears like this, the need to investigate crimes made through the use of the computer. The present work has for objective to present the main tools based on the operating system Microsoft Windows used in the Forensic Know-how Computational, in which you/they were researched several types of tools that can aid in the forensic know-how. Among them they exist from auxiliary tools to complete tools, where they can be used as support source for the experts (investigators).

Keywords: Electronic crimes, Tools of it Analyzes Pericial, Forensic Computacional, Forensic Know-how.

LISTA DE FIGURAS

FIGURA 01 – Tela inicial do Software Norton Ghost Básico.....	20
FIGURA 02 – Tela inicial do Software Norton Ghost Avançado.....	21
FIGURA 03 – Tela mostrando qual mídia será duplicada e qual o seu destino.....	22
FIGURA 04 – Tela inicial do Software Power Quest Drive Image.....	23
FIGURA 05 – Tela do Software Power Quest Drive Image com visualização de mídia para ser feita imagem.....	24
FIGURA 06 – Tela inicial do Software Easy Recovery.....	25
FIGURA 07 – Tela do Software Easy Recovery Data Recovery.....	26
FIGURA 08 – Tela selecionar partição para recuperação de dados.....	27
FIGURA 09 – Tela destino dos arquivos recuperados.....	28
FIGURA 10 – Tela informando qual partição escolhida e a quantidade de arquivos recuperados.....	29
FIGURA 11 – Tela inicial do Software GetDataBack.....	30
FIGURA 12 – Tela do Software GetDataBack para escolher mídia para recuperação de arquivos.....	31
FIGURA 13 – Tela inicial do Software Forensic Toolkit (FTK).....	32
FIGURA 14 – Tela do Software Forensic Toolkit (FTK) para adicionar tipo de mídia.....	33
FIGURA 15 – Tela do Software Forensic Toolkit (FTK) mostrando as opções de mídia.....	34
FIGURA 16 – Tela do Software Forensic Toolkit (FTK) mostrando qual tipo de mídia foi incluindo.....	35
FIGURA 17 – Tela do Software Forensic Toolkit (FTK) analisando unidade.....	36
FIGURA 18 – Tela do Software Forensic Toolkit (FTK) arquivos analisados.....	37
FIGURA 19 – Tela do Software Forensic Toolkit (FTK) mostrando os gráficos.....	38
FIGURA 20 – Tela inicial do Software Encase.....	39
FIGURA 21 – Tela do Software Encase analisando unidade A:.....	40

LISTA DE SIGLAS

CAIS – <i>Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pesquisa</i>	09
FTK – <i>Forensic Toolkit</i>	10
IHCFC – <i>International Hi-Tech Crime and Forensics Conference</i>	10
IOCE – <i>International Organization on Computer Evidence</i>	10
RNP – <i>Rede Nacional de Pesquisa</i>	11
SOPs – <i>Standard Operating Procedures</i>	11
SWGDE – <i>Scientific Working Group on Digital Evidence</i>	11

2.1.1 COMO AGEM OS ATACANTES	12
2.1.2 CARACTERÍSTICAS E DESAFIOS NA FORENSE EM SISTEMAS WINDOWS	12
2.1.3 FERRAMENTAS FORENSES	13
2.1.4 PRINCÍPIOS FORENSES BÁSICOS	14
2.1.5 MANIPULAÇÃO DE EVIDÊNCIAS DIGITAIS	15
2.1.6 FONTES DE INFORMAÇÃO	15
2.1.7 SISTEMAS DE ARQUIVOS	16
2.1.8 ARQUIVOS DE LOG	16
2.1.9 ESPAÇOS NÃO UTILIZADOS NO DISPOSITIVO DE ARMAZENAGEM	16
2.2 ASPECTOS LEGAIS	17
3 METODOLOGIA	18
4 ANÁLISE DE RESULTADOS	19
5 FERRAMENTAS DE DUPLICAÇÃO PERICIAL	19
6 FERRAMENTAS DE RECUPERAÇÃO DE ARQUIVOS APAGADOS	24
7 FERRAMENTAS DE ANÁLISE PERICIAL	32
8 CONCLUSÃO	43
9 REFERÊNCIAS	46

1 INTRODUÇÃO	09
1.1 OBJETIVOS	10
1.1.1 Geral	10
1.1.2 Específicos	10
1.2 JUSTIFICATIVA	10
2 REFERENCIAL TEÓRICO	11
2.1 PERÍCIA FORENSE	11
2.2 O PAPEL DA ANÁLISE FORENSE COMPUTACIONAL NO TRATAMENTO DE INCIDENTES	11
2.2.1 COMO AGEM OS ATACANTES	12
2.3 CARACTERÍSTICAS E DESAFIOS NA FORENSE EM SISTEMAS WINDOWS	12
2.4 FERRAMENTAS FORENSES	13
2.5 PRINCÍPIOS FORENSES BÁSICOS	14
2.6 MANIPULAÇÃO DE EVIDÊNCIAS DIGITAIS	15
2.7 FONTES DE INFORMAÇÃO	15
2.7.1 SISTEMAS DE ARQUIVOS	16
2.7.2 ARQUIVOS DE LOG	16
2.7.3 ESPAÇOS NÃO UTILIZADOS NO DISPOSITIVO DE ARMAZENAGEM	16
2.8 ASPECTOS LEGAIS	17
3 METODOLOGIA	18
4 ANÁLISE DE RESULTADOS	19
4.1 FERRAMENTAS DE DUPLICAÇÃO PERICIAL	19
4.2 FERRAMENTAS DE RECUPERAÇÃO DE ARQUIVOS APAGADOS	24
4.3 FERRAMENTAS DE ANÁLISE PERICIAL	32
5 CONCLUSÃO	43
REFERÊNCIAS	46

1 INTRODUÇÃO

Conforme Lim-Apo (2004, p. 8) os últimos anos foram marcados por mudanças tecnológicas revolucionárias no uso de computadores pelos cidadãos de todo o mundo. A Internet trouxe uma capacidade de comunicação e integração de computadores que há alguns anos seria difícil de se prever. Tudo isso de forma bastante rápida. Inúmeras relações humanas são espelhadas na Internet, a ponto de se dizer que se trata de um mundo virtual. Mas, não existe mundo virtual, e sim o mesmo mundo real só que com diferentes ferramentas e novos paradigmas de relacionamento humano.

As comunicações, as relações de poder, os governos, as religiões, a política, as atividades culturais e o comércio acontecem na Internet. Na mesma Internet, vê-se também o crescimento das guerras, o terrorismo, os furtos, as chantagens, difamações, extorsões, corrupção, pedofilia, quebra de direitos autorais, pichações, furto de informações, estelionatos, falsidade ideológica, brigas pessoais, guerras internacionais e praticamente qualquer outra prática indevida, inadequada e muitas vezes criminosa. É o mundo real, e sujeito às leis reais já existentes, e às novas leis que vêm sendo criadas.

Mesmo crimes que não sejam cometidos na Internet, como terrorismo em massa, um estupro ou homicídio, podem ser cometidos deixando evidências em um computador. Sendo assim, é crescente a necessidade dos estudos na área de forense computacional que auxiliem o desenvolvimento de metodologias e a acumulação de conhecimentos para a descoberta, manipulação e análise de evidências digitais.

Ainda segundo Lim-Apo (2004, p. 8), para entender a aplicação de técnicas de forense computacional basta familiarizar-se com os conceitos e objetivos desta prática. A analogia com a prática forense e pericial de uma forma geral é comum e bastante esclarecedora.

Por exemplo, o ambiente computacional é tratado como uma cena de crime, e um host pode ser tratado como um cadáver sendo dissecado em autópsia. Em outros casos pode-se ter um ativo de rede sendo analisado como um paciente que ouve do médico que não é nada, pois o sintoma está dentro de padrões normais. Claro que a necessidade de legalidade jurídica e a ética são partes da prática de forense computacional, pois de nada valem as ações de um perito investigador se as suas ações apagam ou invalidam provas cruciais desnecessariamente.

A perícia computacional é um processo que passa pela coleta, recuperação, análise e correlacionamento de dados visando reconstruir ações e cenários, estabelecer causa e efeito,

autoria, local e testemunhas, que, depois poderão vir a se transformar em um laudo e/ou ação judicial. Para isso é necessário o uso de ferramentas e técnicas específicas.

Na perícia forense aplicada a informática, existem vários tipos de ferramentas, que podem ser usadas no auxílio à investigação de crimes envolvendo computadores. Dentre estas ferramentas, existe uma divisão natural entre as que fazem uso do sistema operacional Microsoft Windows e as que utilizam Sistema Operacional UNIX. Este estudo visa responder à questão: **Quais as melhores ferramentas para a realização de perícia forense utilizando o ambiente Microsoft Windows?**

1.1 OBJETIVOS

1.1.1 Geral

Apresentar os tipos de ferramentas baseados no Sistema Operacional Microsoft Windows, que possam auxiliar na perícia forense, facilitando assim, a aquisição, preservação, restauração e análise de evidências computacionais.

1.1.2 Específicos

- * Verificar requisitos para a escolha de ferramentas adequadas à análise de evidências computacionais;

- * Apresentar ferramentas baseadas no Sistema Operacional Windows para a prática da Perícia Forense Computacional.

1.2 JUSTIFICATIVA

Com o advento da Internet e a sua popularização entre usuários com os mais diferentes perfis, delitos tradicionais passaram a ser cometidos também utilizando o “mundo virtual”. Surgiu então a necessidade de investigar a prática de crimes via computador (Internet), passou a existir então a necessidade de uma ciência que investigasse esse tipo de crime, dando origem a Forense Computacional, que é descrita como: “a ciência que estuda a aquisição, preservação, recuperação e análise de dados que estão em formato eletrônico e armazenados em algum tipo de mídia computacional”. (OLIVEIRA, GUIMARÃES, GEUS, 2002, p. 2).

Por se tratar de um assunto que no Brasil ainda é pouco explorado, e que falta material na língua portuguesa para servir de base de pesquisa nessa área, foi escolhido o tema citado.

2 REFERENCIAL TEÓRICO

Uma das áreas mais complexas para a coleta de evidências em um processo investigativo é, sem dúvida, o “mundo virtual”. A volatilidade dos dados e a condição de evidência digital necessitam de perícia na condução deste tipo de investigação. Segundo Rocha (2005, p. 1), “A posterior análise destas evidências irá permitir desde a criação de novos e melhores procedimentos de segurança para prevenir ou minimizar tais incidentes até a indenização e responsabilização dos envolvidos”.

2.1. PERÍCIA FORENSE

De acordo com Reis; Geus (2001, p. 2) a perícia forense tem por objetivo levantar evidências que contam a história do fato ocorrido, como por exemplo: Quando? Como? Porquê? E onde? Se a perícia é feita em uma máquina (computador) suspeita, podem ser encontrados arquivos incriminadores. Nesse caso a prova é direta. A análise forense inicia imediatamente após a chegada dos policiais ao local, começando pelo isolamento eficiente do perímetro, evitando assim, a exposição excessiva e possível contaminação das evidências. Passe-se então para a fase de identificação e coleta de todo tipo de dado e material que possa ter alguma relevância na resolução do caso em questão.

Enquanto não existe uma padronização das metodologias de análise forense, é feito um paralelo com métodos tradicionais, a fim de se garantir o valor judicial de uma prova eletrônica. É fundamental ao perito a compreensão do Código de Processo Penal.

2.2 O PAPEL DA ANÁLISE FORENSE COMPUTACIONAL NO TRATAMENTO DE INCIDENTES

Conforme Rocha (2005, p. 1), o profissional de Segurança da Informação precisa ter em mente que a análise forense é a segunda etapa no tratamento de incidentes.

É uma atividade posterior, que ocorre sempre em razão do recebimento de uma notificação de incidente de segurança ou em função de alertas gerados por mecanismos de detecção como, por exemplo, um IDS. No entanto, sua realização é uma atividade extremamente custosa, principalmente em razão do tempo necessário

para a análise. Vale a pena ressaltar que a sua realização deve ser amparada por instrumentos legais.

Um detalhe fundamental são os procedimentos adotados pelo analista, que evitam a ocorrência de erros que comprometam o trabalho.

Ou seja, é importante salientar a necessidade de existirem procedimentos para as diversas etapas da atividade e que estes procedimentos já tenham sido validados tecnicamente e juridicamente. Durante uma análise não é recomendável a tomada de decisões técnicas. A atividade deve estar sempre embasada em procedimentos. (ROCHA, 2005).

Ainda de acordo com Rocha (2005, p. 2), o processo da análise forense pode acontecer de duas formas: a “educacional”, realizada somente com fins de coletar informações relacionadas com a atividade maliciosa sem que se busquem ações legais, e a conhecida como “pericial”, utilizada no ambiente judicial e policial. Nesses tipos de análise, o analista terá os subsídios para traçar as características das ações realizadas por invasores.

De uma forma geral, estas atividades estão ligadas ao comprometimento de sistema, instalação de ferramentas, remoção de evidências e manutenção do controle sobre o sistema comprometido. Tanto os métodos utilizados como os sistemas alvo dos ataques mudam constantemente, da mesma forma que um processo de comprometimento de um sistema Linux possui diferenças quando comparado a de um sistema Windows. É aqui que a atividade de análise forense ‘educacional’ mostra seu valor, pois permite o acesso a informações vitais para os grupos de segurança. (ROCHA, 2005, p. 2).

2.2.1 COMO AGEM OS ATACANTES

Para Jacomo Piccolini apud Rocha (2005, p.2), o analista deve traçar as ações realizadas por invasores, como por exemplo:

- Identificação do alvo;
- Coleta de informação sobre o alvo;
- Identificação das vulnerabilidades;
- Comprometimento do sistema;
- Controle do sistema;
- Instalação de ferramentas;
- Remoção de rastros;
- Manutenção do sistema comprometido;
- Abuso do sistema.

2.3 CARACTERÍSTICAS E DESAFIOS NA FORENSE EM SISTEMAS WINDOWS

Os ataques cujo alvo seja sistemas Windows diferem dos ataques voltados contra sistemas Linux. Dessa forma, o processo de forense em ambiente Windows apresentará

algumas particularidades. A primeira delas é não negligenciar o processo de custódia legal. “Esta etapa refere-se aos controles relacionados com a manutenção segura e controlada de todas as informações e equipamentos coletados” (ROCHA 2005, p. 2). Uma outra característica envolve a coleta das informações. Segundo o especialista Jacomo apud Rocha (2005), a experiência do CAIS (Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa), tem mostrado que, em plataformas Windows, a preferência é que o sistema ainda esteja vivo (com a energia ligada, processos executando, disco sendo acessado, tráfego na rede e conteúdo na tela).

Uma das informações mais interessantes nesta etapa é o conteúdo de memória, que pode ser utilizada para mostrar que um determinado programa foi executado ou que uma informação específica foi acessada. A única oportunidade de coletar estas informações é antes de desligar o sistema. Mais uma vez este procedimento somente é válido se sua política e procedimentos indicarem que um sistema comprometido deve ser mantido ligado até a coleta das informações, orienta o especialista. (ROCHA, 2005, p. 2).

Terceira particularidade relaciona-se com o aumento da capacidade de armazenamento disponível nas estações de trabalho. “É muito comum encontrar computadores pessoais com discos de 120 gigas, sendo que já existem no mercado discos de 500 gigas. Se for necessária a preservação de uma imagem do disco rígido, o desafio atual é conseguir espaço de armazenamento. Uma coisa é gerar uma imagem de um disco de 80 gigas e armazená-la, mas isto se torna um problema muito sério quando o número de máquinas é 40”, afirma Jacomo apud (ROCHA, 2006, p. 1).

2.4 FERRAMENTAS FORENSES

É preciso ter em mente que o uso de uma ferramenta não substitui o conhecimento científico da tecnologia que está sendo analisada. Indiscutivelmente pode poupar muito tempo do examinador, contudo é sempre necessário interpretar os resultados. Em relação às ferramentas disponíveis para realização de uma forense em ambiente Windows, o especialista do CAIS, Piccolini (apud ROCHA, 2005, p. 3), diz que existe uma variedade de ferramentas: muitas gratuitas, outras comerciais e algumas de uso exclusivo e que não são disponibilizadas. A recomendação que o grupo dele faz, é que seja utilizado um pacote de ferramentas, composto por ferramentas gratuitas e que foram desenvolvidas exclusivamente para o ambiente Windows e ferramentas gratuitas que foram portadas do ambiente Unix para o Windows.

A utilização de aplicativos Unix portados para Windows é muito interessante, pois permite que um analista forense que tem sólidos conhecimentos nas ferramentas Unix as utilize no ambiente Windows. Outro ponto favorável é que estas ferramentas já foram testadas e avaliadas e são consideradas como confiáveis para a realização do trabalho, relata o mesmo.

Mas nem só de desafios e ferramentas vive um processo de análise forense. Para que o trabalho seja bem feito, é fundamental que o profissional se mantenha em dia sobre os aspectos que envolvem a aplicação de tal ciência.

Conforme Hannemann (apud ROCHA, 2005, p. 3), como princípios técnicos ele indica um vasto conhecimento de sistemas operacionais e aplicativos, bom conhecimento de aspectos operacionais de sistemas de informação nas empresas, domínio de tecnologias de rede e Internet e, acima de tudo, conhecimento dos procedimentos corretos de levantamento e preservação das evidências. Se as evidências não forem corretamente preservadas e manipuladas durante a análise, elas podem perder o valor jurídico.

Já o perito criminal federal Rodrigues (apud ROCHA 2005, p. 3) aponta outras características fundamentais.

O profissional deve ser objetivo, célere, ter capacidade de sintetizar em alguns parágrafos o resultado das análises que realizou, redigindo de maneira clara e direcionada para público leigo em informática. Deve ser sempre imparcial, relatando os seus achados de maneira específica. Nunca especular sobre elementos que não sejam materiais e não encontrados nos equipamentos recebidos para análise.

Para que isso aconteça, o essencial é buscar treinamento e formação técnica específica. “Porém, tão importante quanto isto, é que o profissional possua um padrão ético que lhe permita ter acesso a informações sigilosas e/ou confidenciais”, informa Jacomo.

2.5 PRINCÍPIOS FORENSES BÁSICOS

Entre as informações mais interessantes segundo o especialista Jacomo apud Rocha (2005, p. 2), foi que em plataformas Windows, a preferência é que o sistema ainda esteja vivo (com a energia ligada, processos executando, disco sendo acessado, tráfego na rede e conteúdo na tela), para isso ele cita os seis princípios forenses básicos que são eles:

- Minimizar a perda de dados;
- Evitar a contaminação de dados;

- Registrar, documentar TUDO;
- Analisar, impreterivelmente, dados em cópias;
- Reportar as informações coletadas;
- Se manter imparcial;

2.6 MANIPULAÇÃO DE EVIDÊNCIAS DIGITAIS

Existe hoje um grande esforço para se conseguir chegar à padronização da forense computacional. A importância de tal esforço reside na necessidade de se garantir a integridade das evidências apresentadas em um tribunal, dado que, uma vez padronizados os procedimentos, torna-se juridicamente inviável o questionamento dos fatos apresentados tomando como tese a metodologia utilizada na manipulação das provas, desde que esta tenha sido aplicada corretamente. (OLIVEIRA; GUIMARÃES; GEUS, 2002, p. 2).

Ainda segundo Oliveira; Guimarães; Geus (2002, p. 4), atualmente já existem padrões internacionais definidos e sendo aplicados de forma experimental. Eles foram desenvolvidos pelo SWGDE (*Scientific Working Group on Digital Evidence*), que é o representante norte-americano na *International Organization on Computer Evidence* (IOCE). Tais padrões foram apresentados durante a *International Hi-Tech Crime and Forensics Conference* (IHCFC), realizada em Londres, de 4 a 7 de outubro de 1999. Os padrões desenvolvidos pelo SWGDE seguem um único princípio:

O de que todas as organizações que lidam com a investigação forense devem manter um alto nível de qualidade a fim de assegurar a confiabilidade e a precisão das evidências. Esse nível de qualidade pode ser atingido através da elaboração de SOPs (*Standard Operating Procedures*), que devem conter os procedimentos para todo tipo de análise conhecida e prever a utilização de técnicas, equipamentos e materiais largamente aceitos na comunidade científica internacional.

No Brasil ainda não existe padronização em andamento, apenas trabalhos feitos a pedido da polícia federal, trabalhos esses direcionados para público leigo composto por promotores e juizes federais, informa Flávio de Souza Oliveira. (OLIVEIRA, 2002, p. 3).

2.7 FONTES DE INFORMAÇÃO

A busca por vestígio em um sistema computacional é feita por meio de uma varredura minuciosa nas informações que nele residam, sejam eles dados em arquivos ou em memória, apagados ou não, cifrados ou possivelmente danificados. Tais vestígios variam de acordo com o tipo de infração a que estão relacionados, determinando diferentes abordagens,

no que diz respeito ao objetivo da busca, para o processo de análise forense. (REIS; GEUS, 2001, p. 3).

Muitas são as fontes de informação para uma análise forense em um sistema computacional, podendo ser citadas as seguintes:

2.7.1 SISTEMA DE ARQUIVOS

O sistema de arquivo é considerado a maior fonte de informação para o exame forense. Os arquivos de dados e executáveis são analisados para se determinar seu conteúdo e funcionalidade no sistema computacional. Os vestígios podem ser encontrados por meio de palavras-chave, tipo: datas, nomes, números de telefone e vocábulos específicos da linguagem criminal, imagens, dados específicos (registros em arquivos log e informações roubadas), por exemplo, ou programas utilizados para práticas ilícitas. (REIS, GEUS, 2001, p. 3).

2.7.2 ARQUIVOS DE LOG

Ainda segundo (REIS, GEUS, 2001, p. 3), os sistemas de log representam um papel importante na análise do sistema de arquivos, pois permitem a reconstituição de fatos que ocorreram no sistema computacional.

Os arquivos de log variam de acordo com o sistema operacional, os aplicativos e serviços executando no sistema, e as configurações determinadas pelo administrador.

2.7.3 ESPAÇOS NÃO UTILIZADOS NO DISPOSITIVO DE ARMAZENAGEM

Para Reis e Geus (2001, p. 4) os espaços no dispositivo de armazenagem não utilizados pelo sistema de arquivos podem conter indícios que o usuário tentou apagar dados. A “remoção” de arquivos e diretórios não apaga os dados do dispositivo de armazenagem, apenas disponibiliza o espaço ocupado para ser sobrescrito por novos arquivos. Esses espaços podem ser caracterizados por espaços não alocados dentro do sistema de arquivos, espaços alocados a arquivos mas não totalmente utilizados, e áreas de dispositivo de armazenagem que não constituem uma partição de disco ou que não contém um sistema de arquivos (é possível ler e escrever dados no dispositivo de armazenagem sem a abstração de arquivos, o que é chamado de raw I/O).

2.8 ASPECTOS LEGAIS

Os aspectos legais constituem-se das formalidades e enquadramentos judiciais a que estão sujeitos os peritos e a função pericial. Tais exigências legais estão dispostas no Código de Processo Penal Brasileiro, no entanto, a legislação processual data de 1941 e, atualmente, o universo de perícias que nela deveria estar regulamentado é bem maior.

Enquanto não existe uma padronização das metodologias de análise forense, é feito um paralelo com métodos tradicionais, a fim de se garantir o valor judicial de uma prova eletrônica. (GALVÃO, 2005, p. 2).

As exigências legais devem obedecer princípios que permitam a utilização de evidências digitais por jurisdição com diferentes legislações. Alguns tipos de princípios adotados: (REIS; GEUS, 2001, p. 4).

- * a função pericial deve ser exercida por pessoa portadora de nível superior, forensicamente capacitada, com habilitação técnica relacionada à natureza do exame e sem antecedentes que levantem suspeitas acerca de seu caráter e ética;

- * o exame pericial deve produzir um laudo pericial segundo algum modelo preestabelecido;

- * o perito deve ser judicialmente responsável pelos resultados da perícia e pelas evidências, enquanto em sua posse;

- * os casos de suspeição dos peritos devem ser predispostos;

- * o exame pericial deve ser realizado por mais de um perito, permitindo conclusões livres de interpretações pessoais;

- * o exame pericial deve ser obrigatório caso haja vestígios a serem analisados.

3 METODOLOGIA

Trata-se de uma pesquisa exploratória-descritiva, pois, de acordo com Lakatos e Marconi (2001, p. 188), “são estudos exploratórios que têm por objetivo descrever completamente determinado fenômeno, como por exemplo, o estudo de um caso para o qual são realizadas análises empíricas e teóricas”.

Tendo por finalidade gerar conhecimentos sobre ferramentas utilizadas na perícia forense, de modo que estas possam auxiliar na descoberta de crimes praticados utilizando computadores.

O trabalho foi realizado através de uma pesquisa bibliográfica, com base na leitura de livros, artigos, reportagens e todo material pertinente ao tema mencionado, já publicado. Tendo como finalidade a descrição das principais ferramentas para perícia forense no Sistema Operacional Microsoft Windows.

De acordo com Dantas (2005, p. 184), a pesquisa exploratória buscar identificar e definir problemas, identificar variáveis relevantes e definir hipóteses. Para realizá-la, procuram-se pontos de informação secundária, como bibliotecas, museus, universidades, material impresso (livros, apostilas, fascículos, teses, anuários e mensários, etc.), faz-se consulta a entendidos no assunto, utilizam-se estudos comparativos de situações análogas e estudo de grupo. A pesquisa exploratória tem uma carga qualitativa muito grande, uma vez que é à base para uma investigação mais detalhada de fenômenos diversos.

4 ANÁLISE DE RESULTADOS

4.1 FERRAMENTAS DE DUPLICAÇÃO PERICIAL

É de extrema importância manter intactas e preservadas as provas materiais, para que no decorrer da perícia as mesmas possam ser analisadas. Por isso a duplicação pericial é tão importante na hora da investigação, para que as provas originais não venham a ser comprometidas.

A duplicação pericial consiste em criar uma imagem, ou seja, uma cópia fiel da mídia ou de um sistema que será investigado. Através dessa cópia o perito poderá realizar suas análises, preservando assim as provas originais. Para que essa cópia seja feita é necessário que o perito use ferramentas adequadas para tal execução. Os principais itens que uma ferramenta precisa para se tornar confiável são:

- * Ter a capacidade de criar uma imagem da mídia de armazenamento (HD, disquete, CD, DVD, Pen drive, etc);
- * Não alterar os arquivos originais;
- * Ser capaz de tratar os erros de leitura com segurança.

A seguir alguns tipos de ferramentas (para sistema operacional Microsoft Windows) usadas na duplicação pericial:

NORTON GHOST

O Norton Ghost da Symantec (www.symantec.com) é uma ferramenta bastante popular usada para essa finalidade, sendo ela desenvolvida em um ambiente completamente gráfico, possibilitando ao usuário a realização de imagens de dispositivos em análise com bastante facilidade. Suporta/reconhece uma variedade de dispositivos de mídia e busca recuperar todo o seu sistema em etapas rápidas e simples. Na maioria dos casos, recupera o sistema e dados, mesmo quando não se consegue reiniciar o sistema operacional. Pode realizar, ainda, o backup de todo o conteúdo da mídia, copiando qualquer tipo de arquivo.

A figura 01 mostra a tela inicial do Norton Ghost, onde o usuário pode fazer um backup de todos os seus arquivos, como também fazer a restauração de um arquivo utilizando uma imagem feita pelo Ghost.

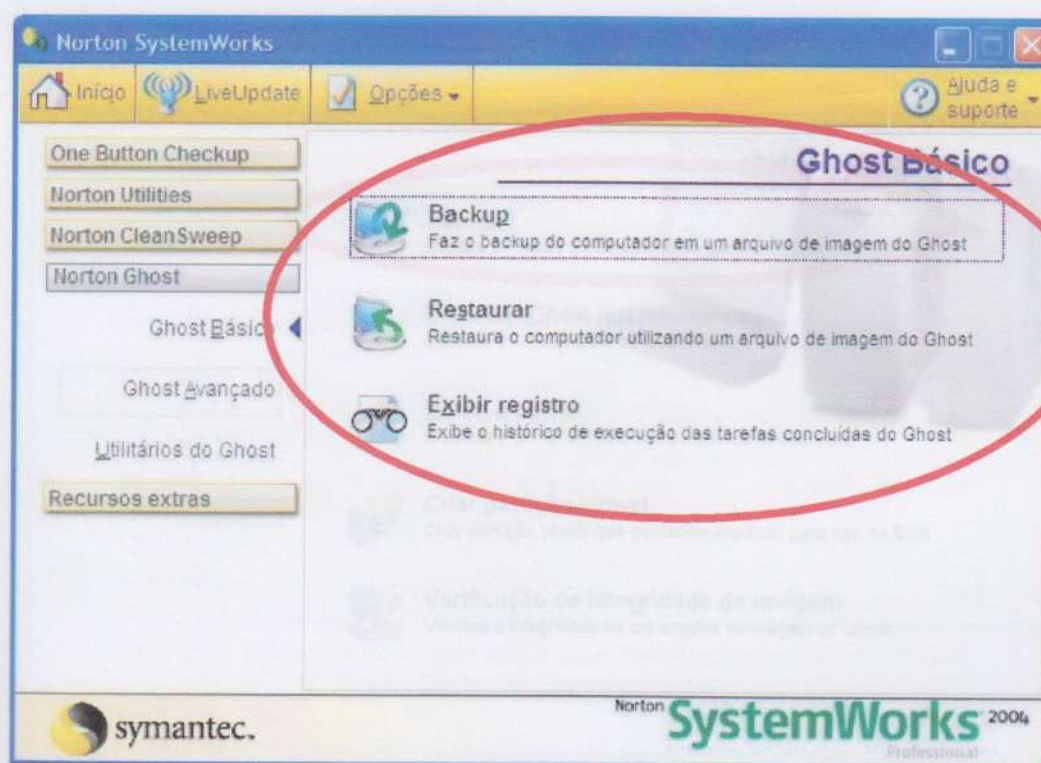


Figura 01 – Tela inicial do Norton Ghost Básico
Fonte: Dados da Pesquisa (2006)

A figura 02 mostra a tela do Ghost Avançado apresentando as opções para o usuário, onde ele poderá escolher o procedimento que irá utilizar, seja a realização de uma duplicação da partição, ou a geração de uma imagem do dispositivo que será periciado. Esta versão também permite a execução interativa do Ghost, cópia remota e verificação de integridade.

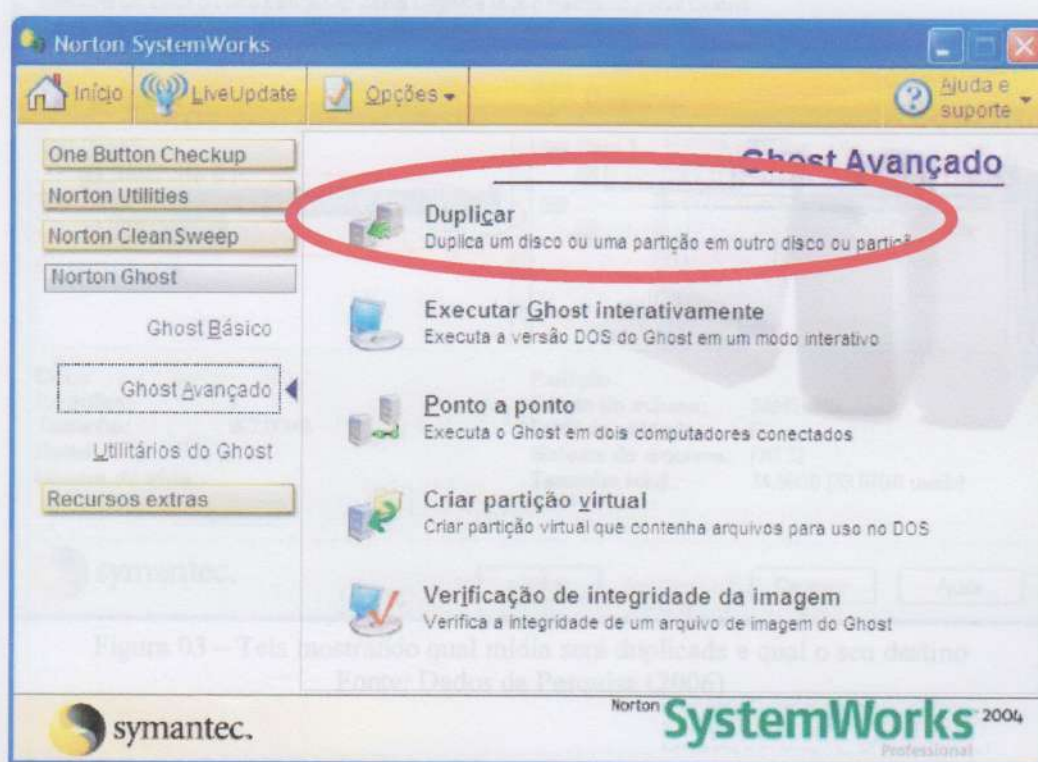


Figura 02 – Tela inicial do Norton Ghost Avançado

Fonte: Dados da Pesquisa (2006)

A figura 03 mostra as opções de dispositivos que o usuário tem para fazer a imagem. Neste exemplo existia o disco rígido e uma unidade removível. O usuário seleciona a mídia que irá ser duplicada, escolhe o destino no qual ela será salva, e em seguida seleciona o botão avançar.

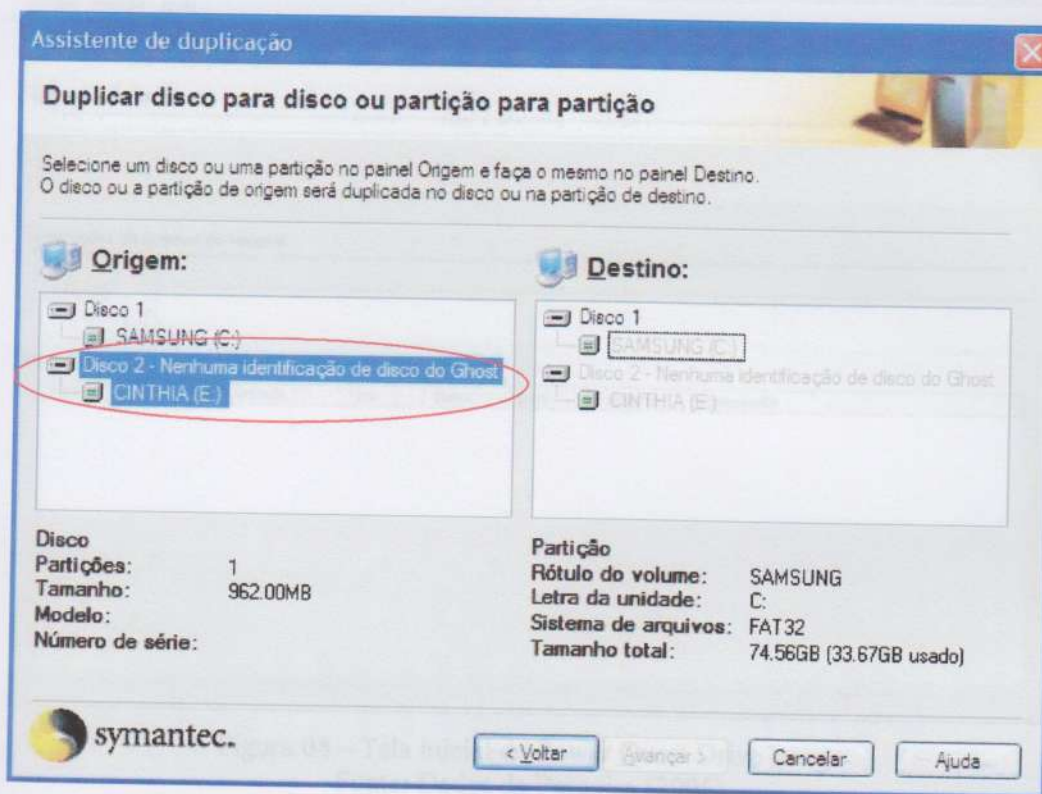


Figura 03 – Tela mostrando qual mídia será duplicada e qual o seu destino
Fonte: Dados da Pesquisa (2006)

POWER QUEST DRIVE IMAGE

A ferramenta Power Quest Drive Image da PowerQuest (www.powerquest.com), também é uma ferramenta de duplicação pericial, além das funcionalidades de recuperação de arquivos e clonagem de partições. Essa ferramenta possibilita que seja armazenada em um arquivo, compactado ou não, todas as informações físicas de uma instalação de sistema operacional, permitindo assim, que o perito tenha em mãos uma cópia fiel da mídia. O Power Quest suporta rede, como também vários tipos de partições (FAT 32 e 16, HPFS, NTFS, etc).

A figura 04 mostra a tela inicial do Power Quest Drive Image onde o perito fará a escolha de qual tipo de mídia será feita a imagem.

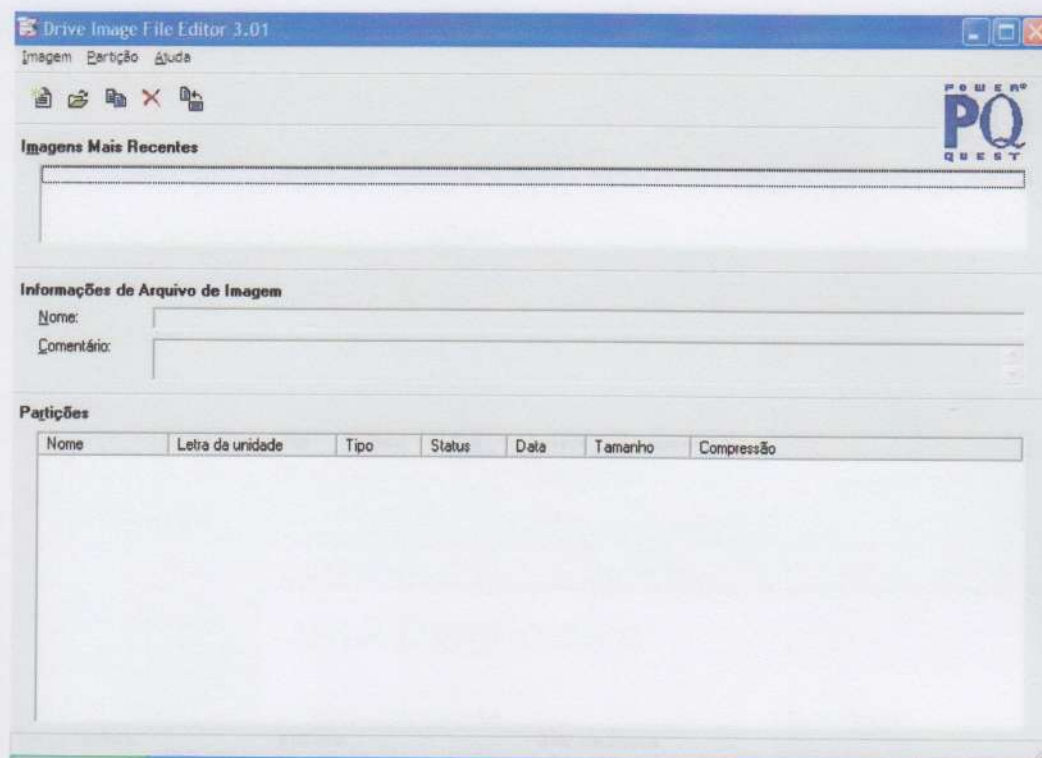


Figura 04 – Tela inicial do Power Quest Drive Image
Fonte: Dados da Pesquisa (2006)

4.2 FERRAMENTAS DE RECUPERAÇÃO DE ARQUIVOS APAGADOS

Quando um usuário realiza a exclusão de arquivos, na verdade estes não são excluídos do disco, mas somente marcados para exclusão. O que realmente acontece é que os arquivos tornam-se inacessíveis e na medida em que outros arquivos vão sendo criados, sobrescrevem a área onde estão se encontrando. Então, quanto mais rápido o perito tentar recuperar o arquivo, mais chances terá.

Existem vários tipos de ferramentas que podem ser usadas na recuperação de arquivos, alguns exemplos são apresentados a seguir.

A figura 05 mostra qual tipo de mídia foi escolhida pelo perito, na qual será feita uma cópia fiel, ou seja, será feita uma imagem da mídia.

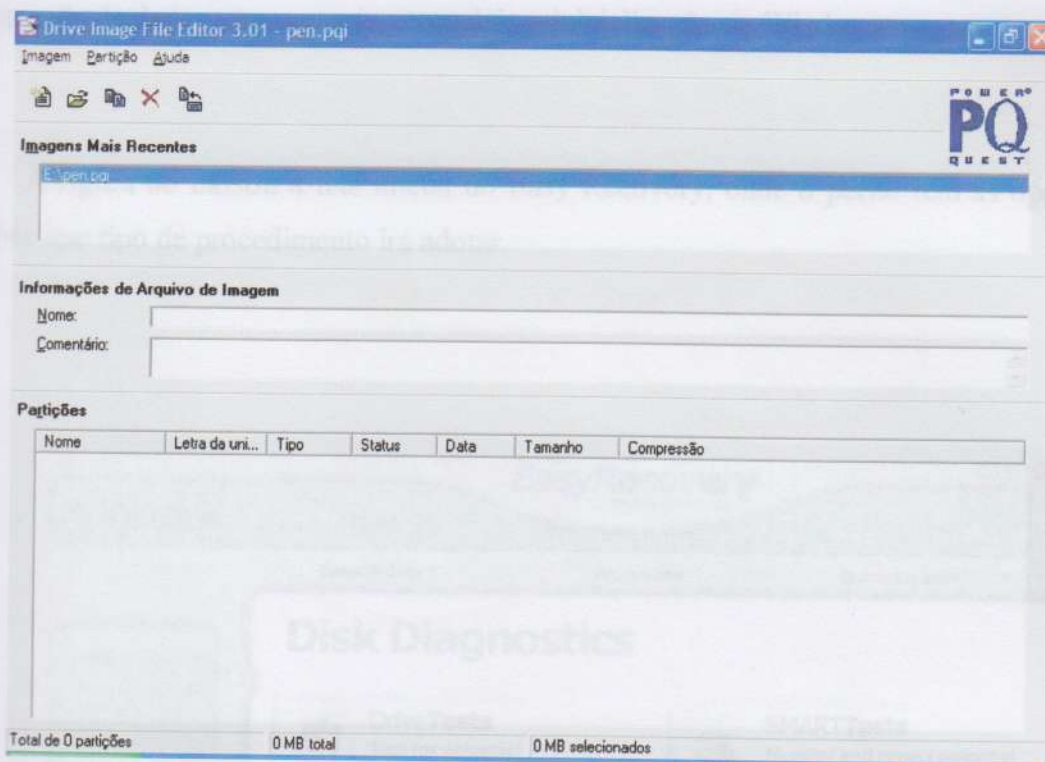


Figura 05 – Tela do Power Quest Drive Image com visualização de mídia para ser feita imagem
Fonte: Dados da Pesquisa (2006)

4.2 FERRAMENTAS DE RECUPERAÇÃO DE ARQUIVOS APAGADOS

Quando um usuário realiza a exclusão de arquivos, na verdade estes não são excluídos de fato, mas, somente marcados para exclusão. O que realmente acontece é que os arquivos continuam intactos e na medida em que outros arquivos vão sendo criados, sobrescrevem a área física onde se encontram. Então, quanto mais rápido o perito tentar recuperar o arquivo, mais chance terá.

Existem vários tipos de ferramentas que podem ser usadas na recuperação de arquivos, alguns exemplos são apresentados a seguir.

EASY RECOVERY

O Easy Recovery (www.ontrack.com) é uma ferramenta profissional que auxilia o perito na recuperação de arquivos perdidos. Recuperando dados apagados, ou até mesmo partições corrompidas. Tem, ainda, a capacidade de gerar um disco de inicialização para recuperação de dados sem que seja necessário a inicialização do Windows.

A figura 06 mostra a tela inicial do Easy Recovery, onde o perito tem as opções de escolher que tipo de procedimento irá adotar.



Figura 06 – Tela inicial do Easy Recovery
Fonte: Dados da Pesquisa (2006)

A figura 07 mostra a tela do Easy Recovery mostrando em destaque as opções que o perito tem de recuperação de dados, onde os mesmos tenham sido apagados intencionalmente ou não, ou até mesmo tenham sido formatados.

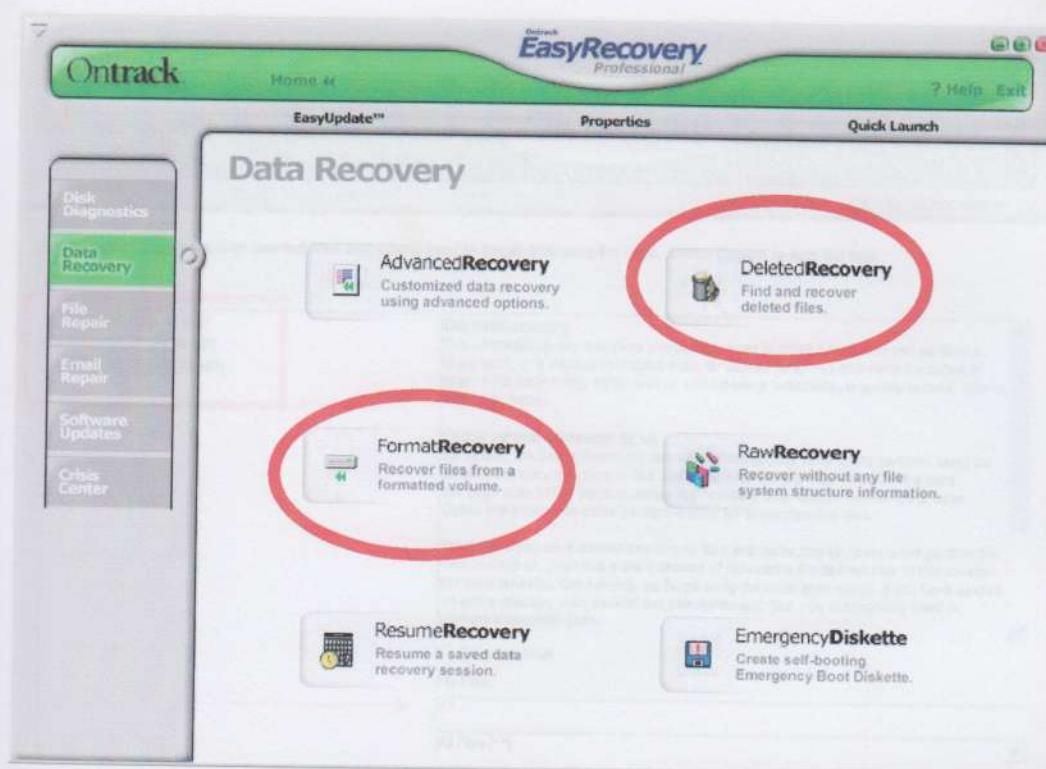


Figura 07 – Tela do Easy Recovery Data Recovery
Fonte: Dados da Pesquisa (2006)

A figura 08 mostra a tela do EasyRecovery onde o perito tem a opção de escolher qual mídia irá recuperar, como também escolher tipos de arquivos específicos para recuperar, escolhendo a mídia e colocando o tipo de extensão específica.

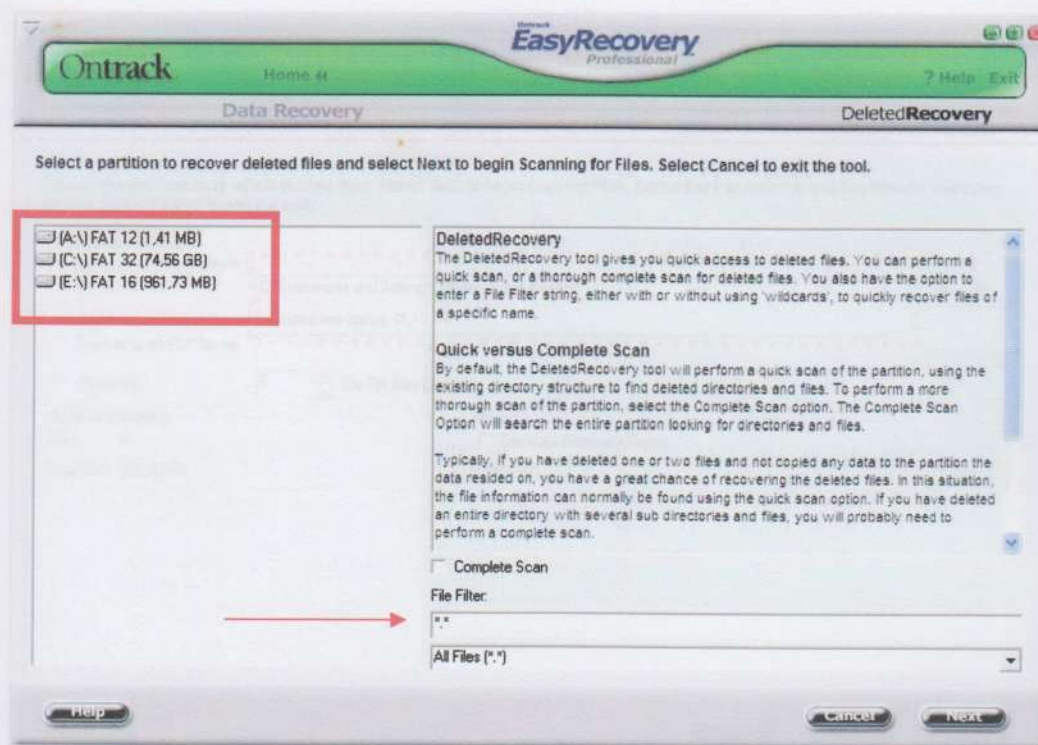


Figura 08 – Tela selecionar partição para recuperação de dados
Fonte: Dados da Pesquisa (2006)

A figura 09 mostra a tela do EasyRecovery onde o perito pode escolher qual o destino dos arquivos recuperados, colocando assim, os arquivos recuperados em uma local específico.

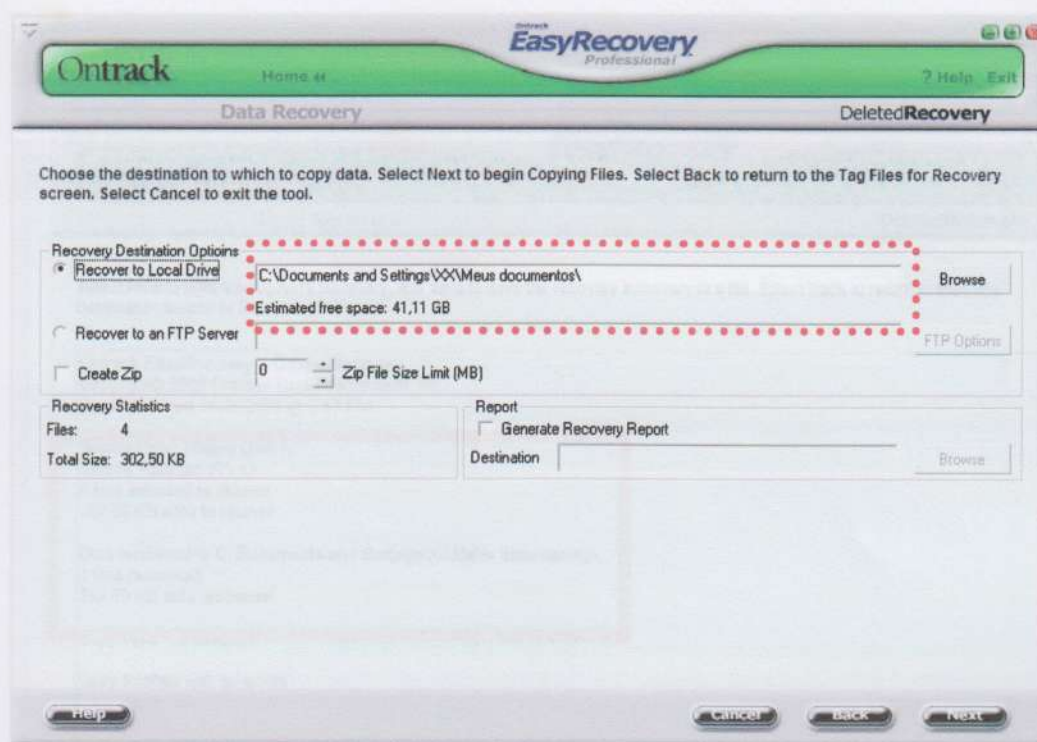


Figura 09 – Tela destino dos arquivos recuperados
Fonte: Dados da Pesquisa (2006)

GETDATARACK

A ferramenta GetDataBack da Runtime Software (www.runtime.org), permite ao usuário localizar arquivos que através de métodos normais não eram possíveis de se localizar.

A figura 10 mostra a tela do Easy recovery informando qual a mídia escolhida para recuperação de dados, o local para onde foram destinados os arquivos recuperados, como também a quantidade de arquivos recuperados.

A figura 11 mostra a Tela inicial do GetDataBack, informando ao usuário as opções que

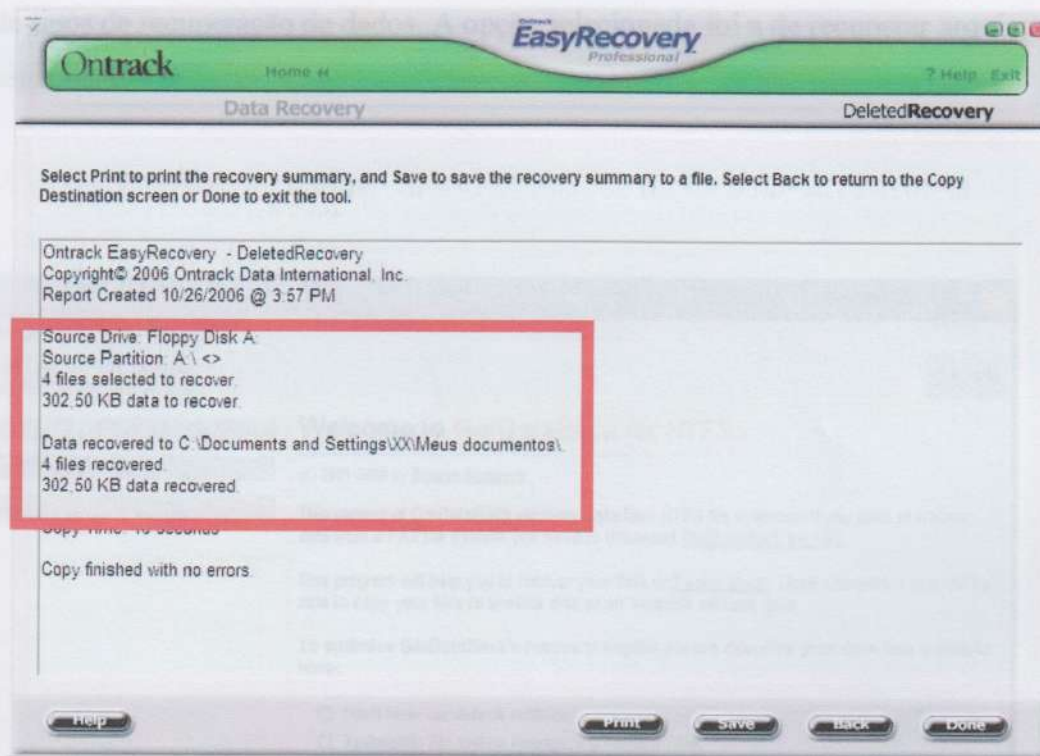


Figura 10 – Tela informando qual partição escolhida e a quantidade de arquivos recuperados
Fonte: Dados da Pesquisa (2006)

Figura 11 – Tela inicial do GetDataBack
Fonte: Dados da Pesquisa (2006)

GETDATABACK

A ferramenta GetDataBack da Runtime Software (www.runtime.org), permite ao perito localizar provas que através de métodos normais não eram possíveis de se localizar. Mas é preciso que o perito tenha um pouco de conhecimento sobre ela. Com esta ferramenta é possível descobrir se em um HD ou qualquer outro tipo de mídia contém informações sigilosas. É uma ferramenta que recupera dados apagados em sistemas FAT e NTFS, mesmo quando o sistema de arquivos foi formatado com fdisk.

A figura 11 mostra a Tela inicial do GetDataBack, informando ao perito as opções que ele tem de tipos de recuperação de dados. A opção selecionada foi a de recuperar arquivos que foram apagados.

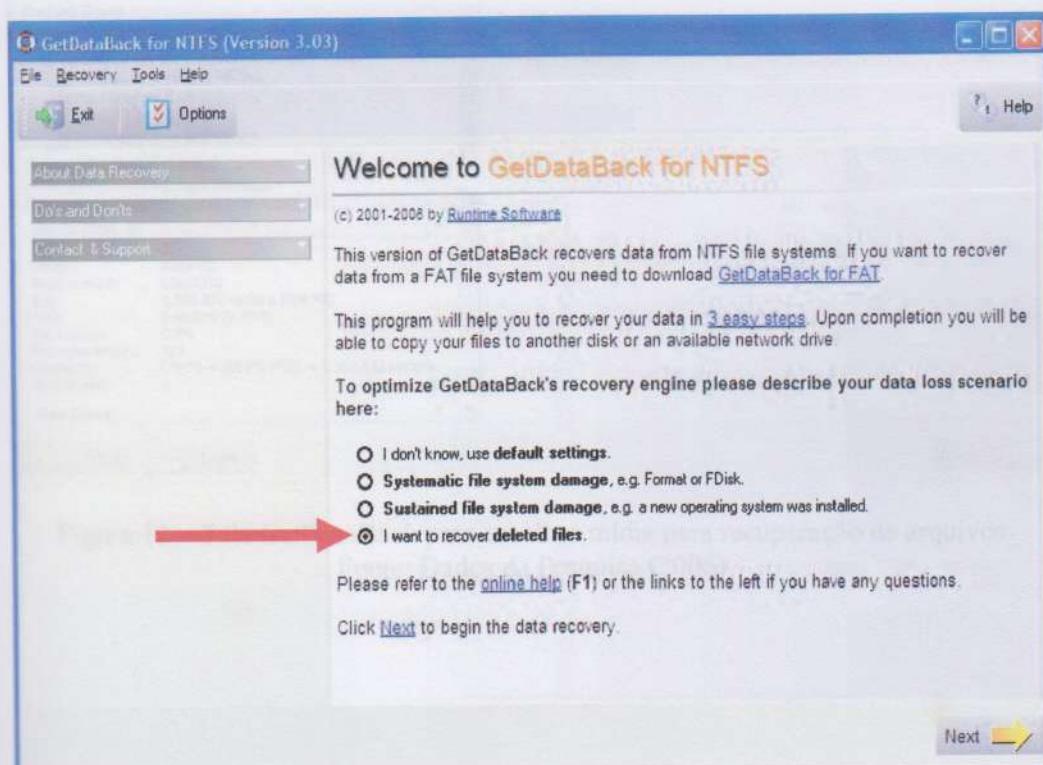


Figura 11 – Tela inicial do GetDataBack
Fonte: Dados da Pesquisa (2006)

4.3 FERRAMENTAS DE ANÁLISE PERICIAL

No mercado atual existem vários tipos de ferramentas que permitem que o usuário realize uma investigação detalhada no sistema ou mídia investigados. Para o ambiente Windows as opções são excelentes, embora o fator custo representa geralmente um problema.

A figura 12 mostra a tela do GetDataBack, onde o examinador pode escolher qual o tipo de mídia para recuperar os dados removidos.

recuperação de dados apagados, geração de imagens de discos, pesquisas de arquivos utilizando palavras-chave, suporte a e-mail, visualização rápida de todos os arquivos de imagem (BMP, JPG, GIF e TIFF), dentre outros.

A seguir são apresentadas as principais ferramentas desse tipo.

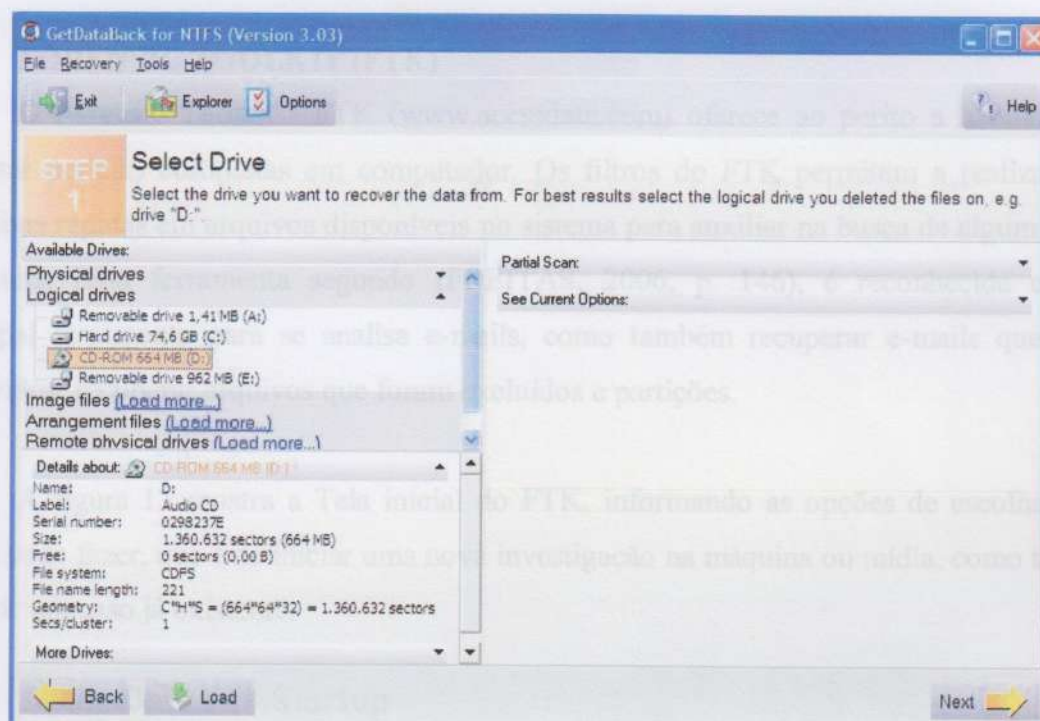


Figura 12 – Tela GetDataBack para escolher mídia para recuperação de arquivos
Fonte: Dados da Pesquisa (2006)

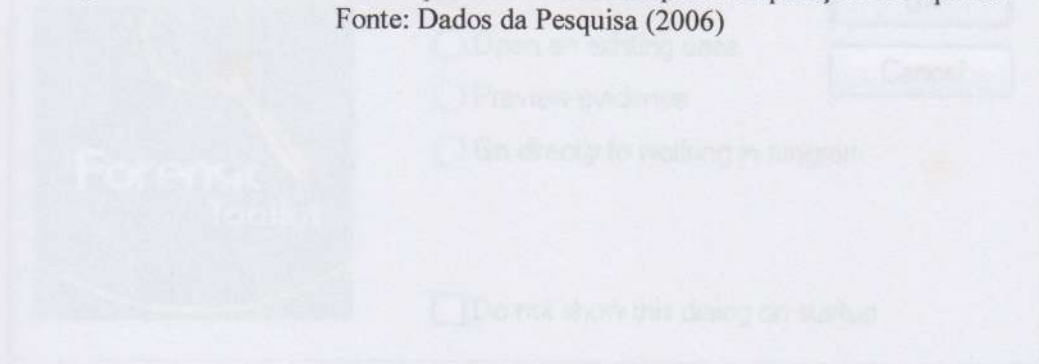


Figura 13 – Tela inicial do Forensic Toolkit (FTK)
Fonte: Dados da Pesquisa (2006)

4.3 FERRAMENTAS DE ANÁLISE PERICIAL

No mercado atual existem vários tipos de ferramentas que permitem que o usuário realize uma investigação detalhada no sistema ou mídia investigados. Para o ambiente Windows as opções são excelentes, embora o fator custo represente geralmente um problema. São ferramentas que podem ser consideradas completas, porque atendem todas as necessidades do perito, como por exemplo: recuperação de dados apagados, geração de imagens de discos, pesquisas de arquivos utilizando palavras-chaves, suporte a e-mail, visualização rápida de todos os arquivos de imagem (BMP, JPG, GIF e TIFF), dentre outras.

A seguir são apresentadas as principais ferramentas deste tipo.

FORENSIC TOOLKIT (FTK)

O Forensic Toolkit - FTK (www.accessdata.com) oferece ao perito a habilidade de executar perícias completas em computador. Os filtros do FTK permitem a realização de pesquisas rápidas em arquivos disponíveis no sistema para auxiliar na busca de algum tipo de evidência. Essa ferramenta segundo (FREITAS, 2006, p. 146), é reconhecida como a principal ferramenta para se analisa e-mails, como também recuperar e-mails que foram removidos, recuperar arquivos que foram excluídos e partições.

A figura 13 mostra a Tela inicial do FTK, informando as opções de escolha que o perito pode fazer, que é de iniciar uma nova investigação na máquina ou mídia, como também de abrir um caso já existente.

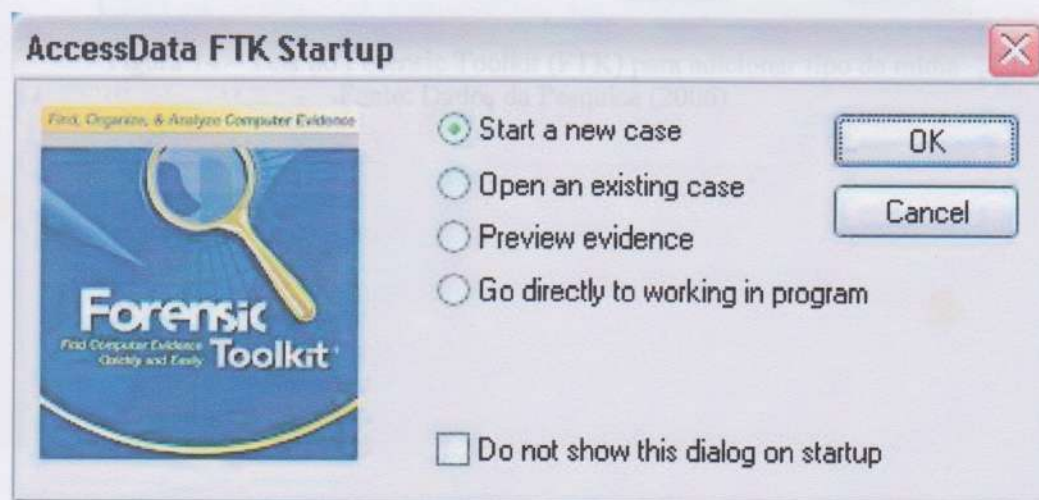


Figura 13 – Tela inicial do Forensic Toolkit (FTK)
Fonte: Dados da Pesquisa (2006)

A figura 14 mostra a tela do FTK, onde o perito tem as opções de adicionar qual tipo de mídia será periciado, editar, remover, ou até mesmo redefinir qual tipo de mídia irá ser analisado.

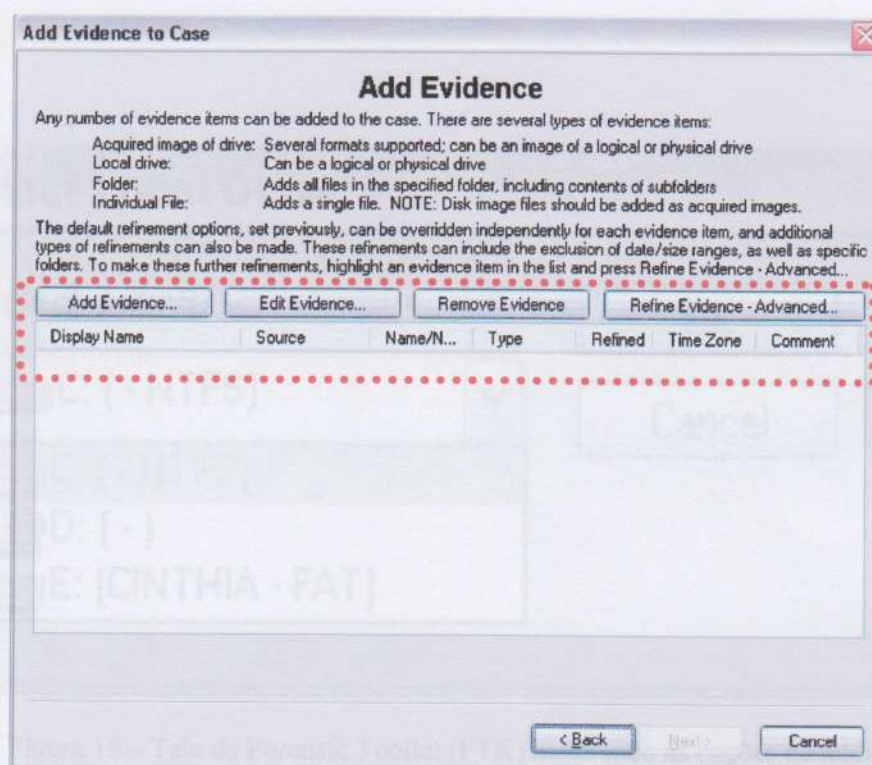


Figura 14 – Tela do Forensic Toolkit (FTK) para adicionar tipo de mídia
Fonte: Dados da Pesquisa (2006)

A figura 15 mostra quais as opções de mídia o perito tem para fazer a análise pericial, podendo o mesmo escolher, o próprio disco rígido da máquina, como também a unidade de Cd Rom ou até mesmo a partição E:, que no exemplo acima se trata de uma pen drive.

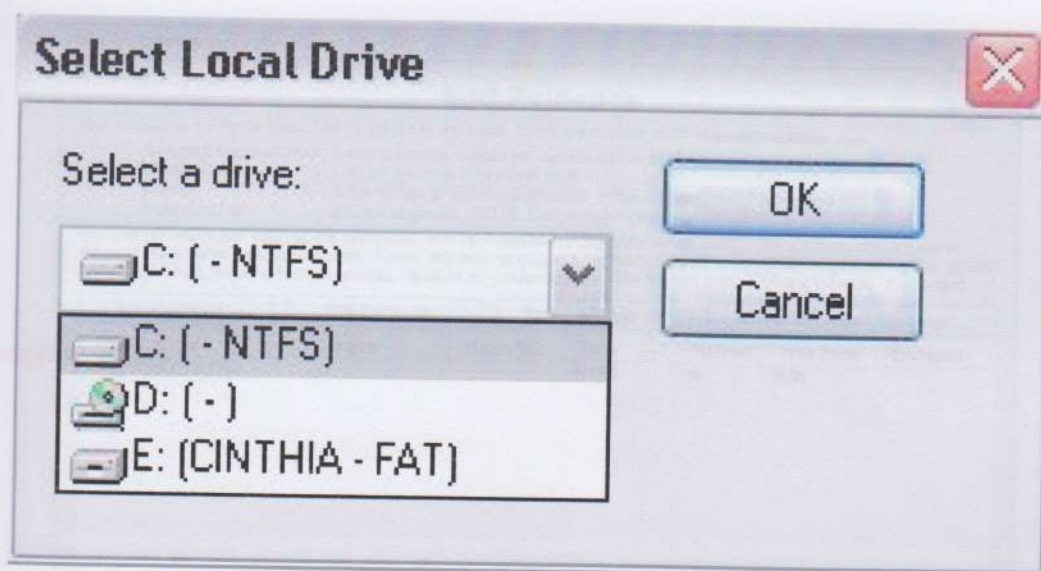


Figura 15 – Tela do Forensic Toolkit (FTK) mostrando as opções de mídia
Fonte: Dados da Pesquisa (2006)

Figura 16 – Tela do Forensic Toolkit (FTK) mostrando qual tipo de mídia
Fonte: Dados da Pesquisa (2006)

A figura 16 mostra qual tipo de mídia foi escolhida e adicionada pelo investigador, onde o mesmo tem a opção de clicar no botão Next, e começar a investigação na mídia escolhida.

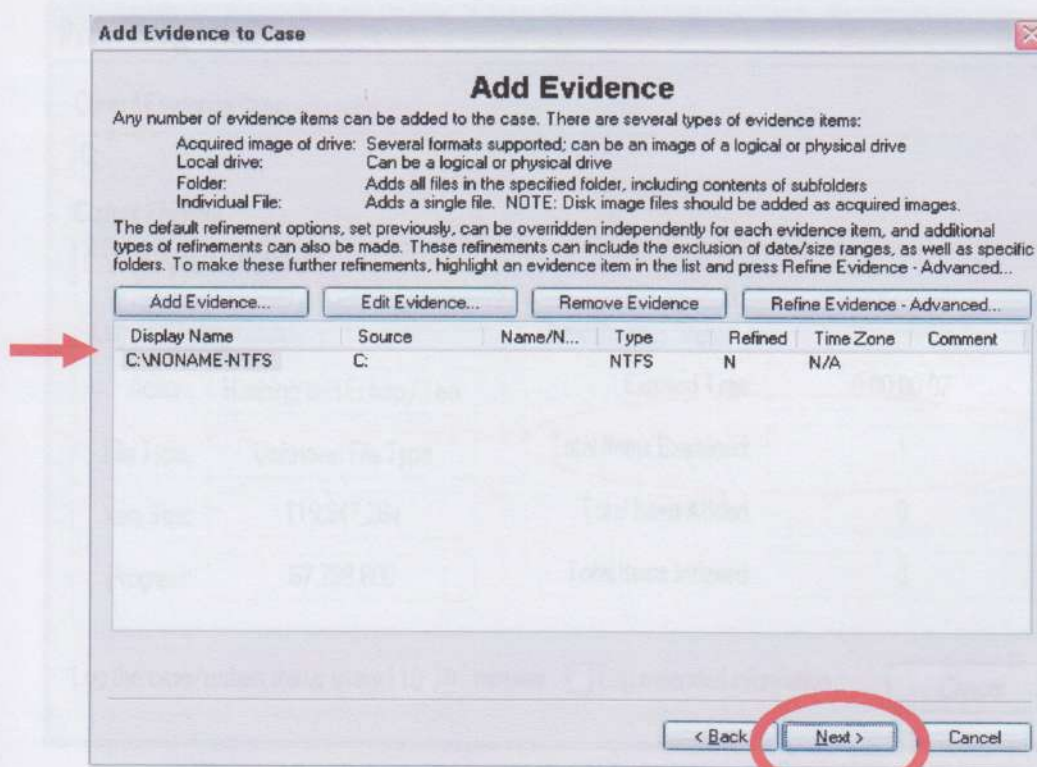


Figura 16 – Tela do Forensic Toolkit (FTK) mostrando qual tipo de mídia
Fonte: Dados da Pesquisa (2006)

A figura 18 mostra a quantidade de arquivos que foram examinados, os tipos de arquivos analisados, os arquivos que foram apagados, os arquivos que tem duplicação, como

A figura 17 informa qual mídia está sendo periciada, como também quantos arquivos já foram examinados.

Processing Files...

Current Evidence Item:
C:

Current File Item:
C:\NONAME-NTFS\\$.MFT

Current File Item Status		Total Process Status	
Action:	Hashing and Entropy Test	Elapsed Time:	0.00:00:07
File Type:	Unknown File Type	Total Items Examined:	1
Item Size:	119,947,264	Total Items Added:	0
Progress:	67,788,800	Total Items Indexed:	0

Log the case/system status every 10 minutes ☐ Log extended information Cancel

Figura 17 – Tela do Forensic Toolkit (FTK) analisando unidade
Fonte: Dados da Pesquisa (2006)

A figura 18 mostra a quantidade de arquivos que foram examinados, os tipos de extensões analisadas, os arquivos que foram apagados, os arquivos que tem duplicação, como também vários tipos de gráficos, ou seja, fotos, e etc.

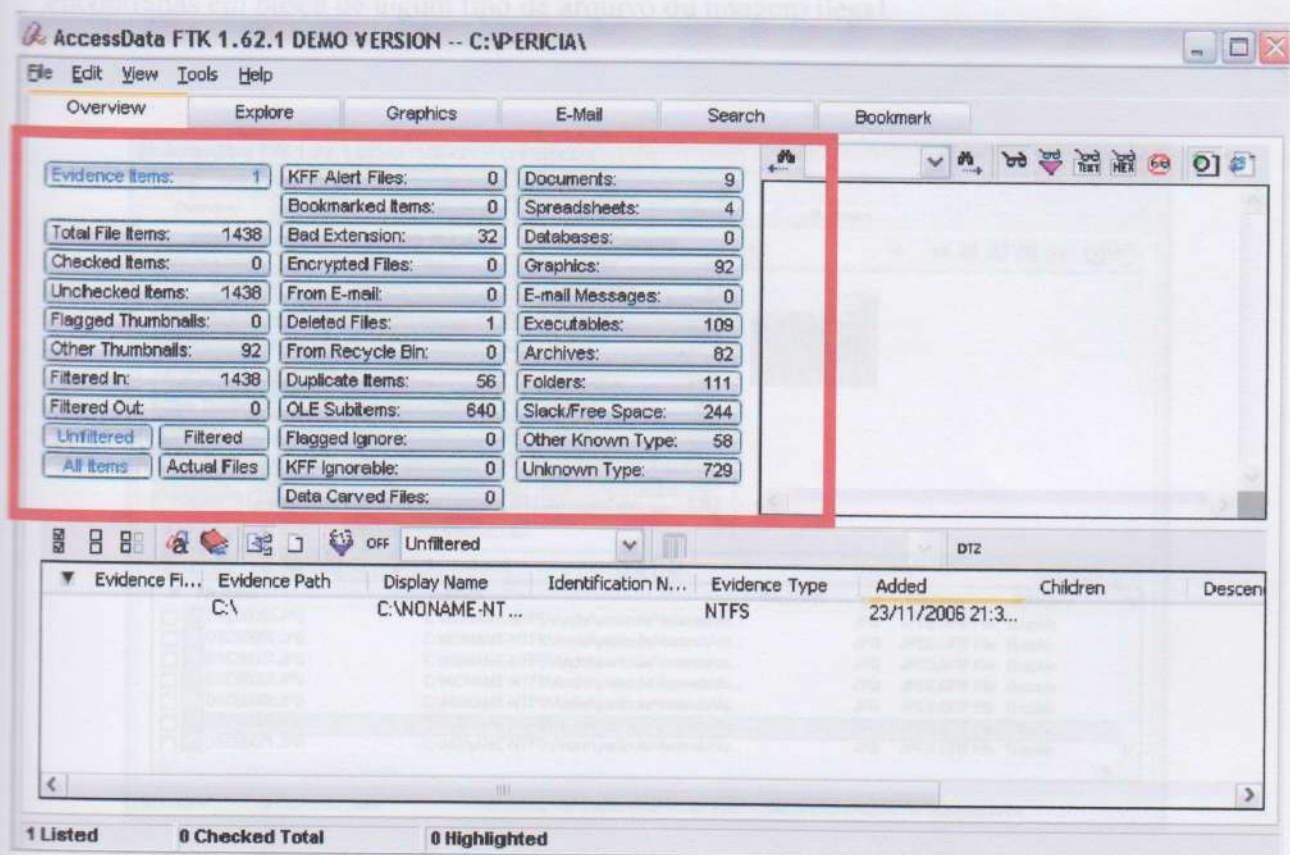


Figura 18 – Tela do Forensic Toolkit (FTK) arquivos analisados
Fonte: Dados da Pesquisa (2006)

ENCASE

O Encase da Guidances (www.guidancesoftware.com) é também uma ferramenta usada especialmente para análise forense, ou seja, para trabalhos periciais. O Encase oferece ao perito a possibilidade de fazer a imagem fiel dos dispositivos analisados, recuperação de dados perdidos de qualquer tipo de partição, análise e-mails, imagens anexadas ao e-mail, etc.

A figura 19 mostra todos os tipos de gráficos encontrados (imagens), agilizando assim o processo de análise, onde o perito pode de forma interativa analisar todas as fotos encontradas em busca de algum tipo de arquivo ou imagem ilegal.

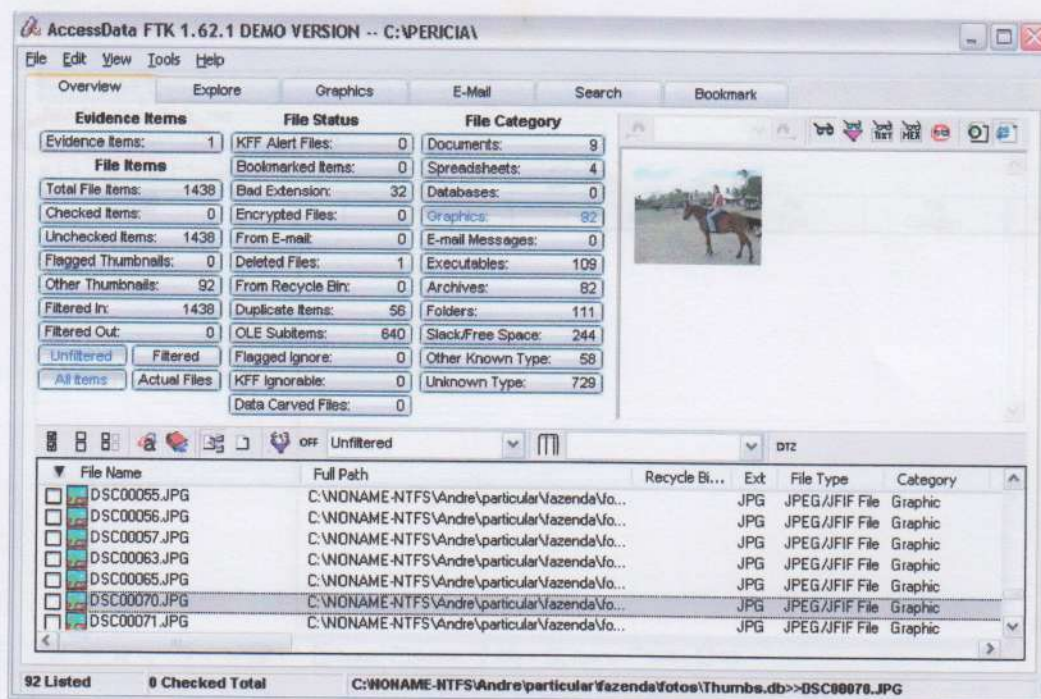


Figura 19 – Tela do Forensic Toolkit (FTK) mostrando os gráficos
Fonte: Dados da Pesquisa (2006)

Figura 20 – Tela inicial do Encase
Fonte: Dados da Pesquisa (2006)

ENCASE

O Encase da Guidance (www.guidancesoftware.com) é também uma ferramenta usada especialmente para análise forense, ou seja, para trabalhos periciais. O Encase oferece ao perito a possibilidade de fazer a imagens fiéis dos dispositivos analisados, recuperação de dados perdidos de qualquer tipo de partição, análise e-mails, imagens anexadas ao e-mail, etc.

A figura 20 mostra a tela inicial do Encase, onde o perito tem as opções de iniciar um novo caso, como também de abrir ou continuar investigando um caso já existente.

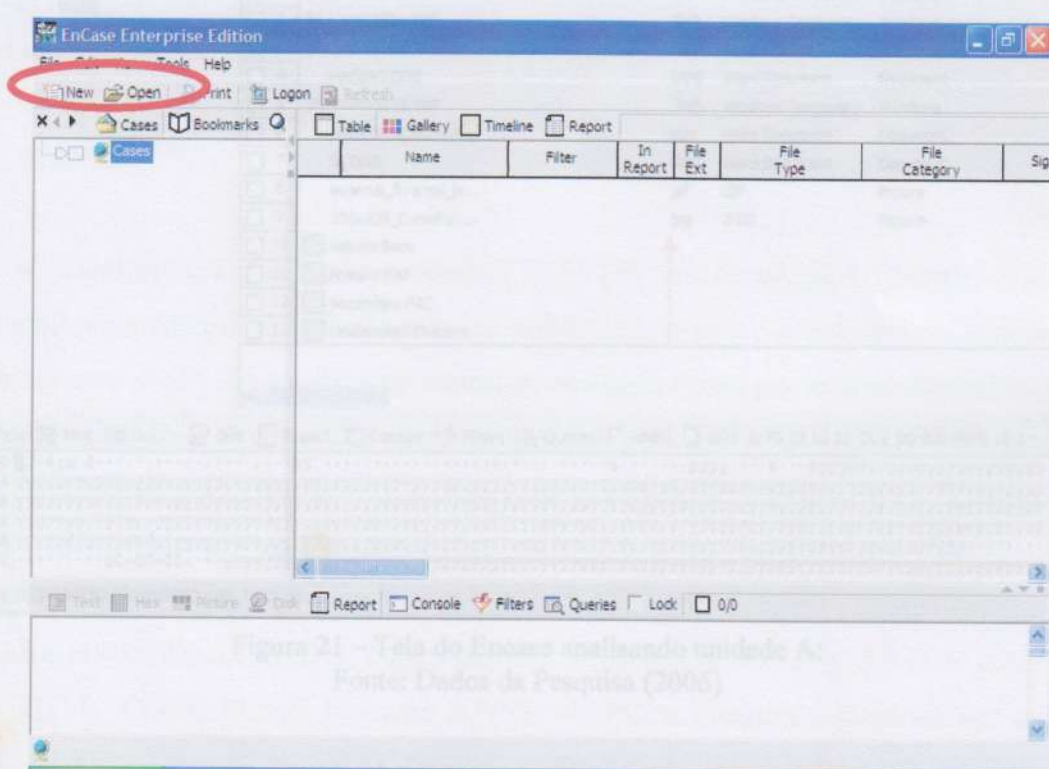


Figura 20 – Tela inicial do Encase
Fonte: Dados da Pesquisa (2006)

A figura 21 mostra a tela do Encase analisando a unidade A:, onde os arquivos visualizados apresentam status indicando se estão acessíveis ou se foram removidos, onde os arquivos que estão marcados com um X vermelho foram removidos, mostrando assim, sua condição para ser recuperado. O Encase mostra também qual a extensão de cada arquivo analisado.

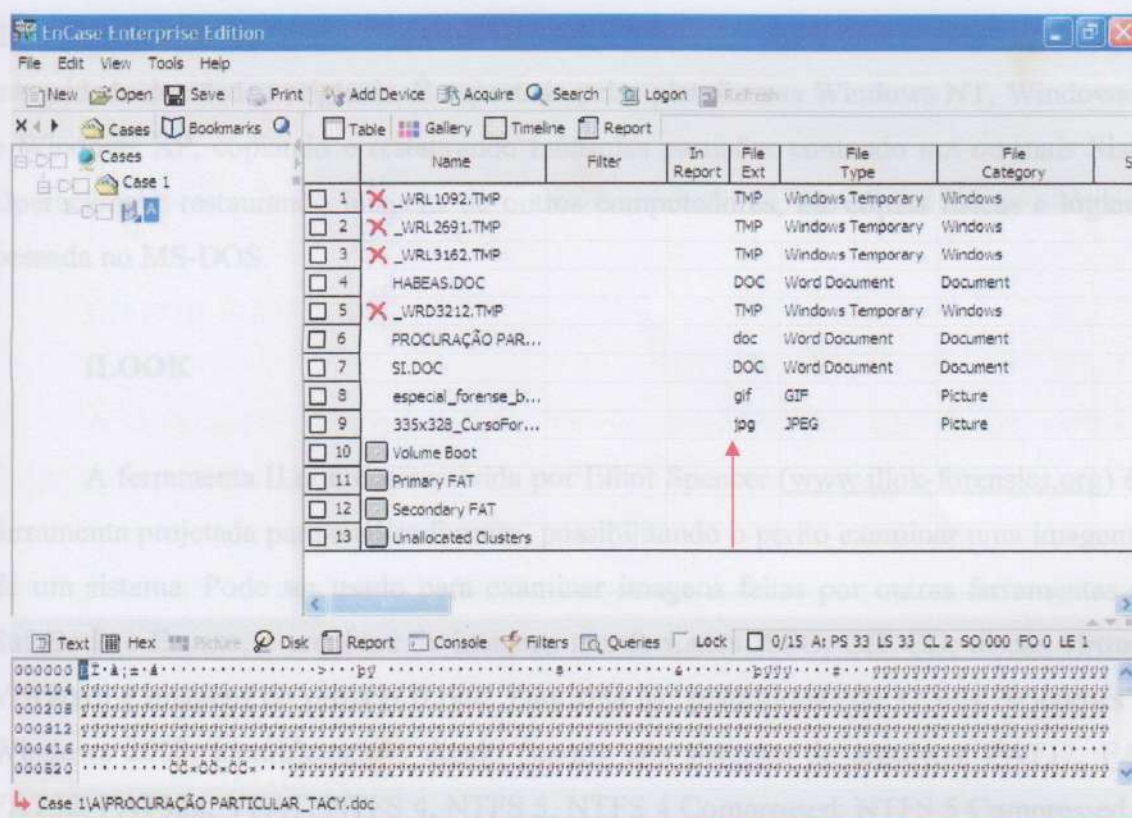


Figura 21 – Tela do Encase analisando unidade A:

Fonte: Dados da Pesquisa (2006)

Existe ainda uma grande variedade de ferramentas que podem ser utilizadas na hora de fazer uma perícia. Ferramentas de duplicação, ferramentas que possibilitam ao perito fazer a imagem da mídia que passará por investigação, como também ferramentas completas. Algumas ferramentas desse tipo são detalhadas a seguir.

SAFEBACK

A ferramenta SafeBack da NTI – New Technologies (www.forensic-intl.com), é uma ferramenta usada para se criar backups de evidências em computadores, preservando todos os dados, incluindo os dados inativos ou deletados, não alterando e nem modificando a integridade dos dados originais. É suportada pelas plataformas Windows NT, Windows 2000 e Windows XP, copiando e restaurando múltiplas partições contendo um ou mais Sistemas Operacionais, restaurando imagens de outros computadores, faz cópias físicas e lógicas e é baseada no MS-DOS.

ILOOK

A ferramenta ILook desenvolvida por Elliot Spencer (www.illok-forensics.org) é uma ferramenta projetada para análise forense, possibilitando o perito examinar uma imagem feita de um sistema. Pode ser usado para examinar imagens feitas por outras ferramentas como SafeBack e Encase, e arquivos de imagens nos formatos ISSO, CIF CD, discos virtuais do VMWare e imagens do próprio ILook. Funciona nas plataformas de 32 bits: Windows NT e Windows 2000, identificando e dando suporte aos sistemas de arquivos: FAT12, FAT16, FAT32, FAT32x, VFAT, NTFS 4, NTFS 5, NTFS 4 Compressed, NTFS 5 Compressed, Mac HFS, Mac HFS+, Linux Ext2FS, Linux Ext3FS, SCO Sys V AFS, SCO Sys V EAFS, SCO Sys V HTFS, CDFS, Novell Netware NWFS. Visualiza imagens integradas nos arquivos, permite ao perito navegar através do sistema de arquivos do computador suspeito.

PRODISCOVER

A ferramenta ProDiscover da Technology Pathways (www.techpathways.com) permite fazer cópia bit stream, tem help online, gera relatórios, cria imagens compactadas, recupera arquivos apagados, detecta qual o sistema operacional instalado, visualiza imagens integradas, cria hash de imagens ou arquivos com MD5 ou SHA1, pesquisando e analisando

mídia de diferentes sistemas de arquivos, incluindo: FAT12, FAT16, FAT32, todas as versões do NTFS e SUN Solaris UFS.

FORENSIC REPLICATOR

O Forensic Replicator é de propriedade da Paraben Corporation (www.paraben-forensics.com). Essa ferramenta foi projetada para criar imagens bit-stream de mídias eletrônicas para que a partir daí possa ser feita uma perícia na máquina suspeita. Podendo também ser utilizada como uma poderosa ferramenta de backup. Ela cria imagens de drives USB, com a opção de imagem de drive para pen drive, imagens ISO CD-Rom, formata e/ou copia disquete DMF/1.68 MB, compacta arquivos em tempo real (on the fly), gera imagens com descompactação automática (self-extracting) e criptografa os dados para um armazenamento seguro das evidências (128 bits).

DD FOR WINDOWS

A ferramenta dd for windows foi desenvolvida por George M. Garner JR (<http://users.erols.com/gmgarner/forensics>). É utilizada para se fazer duplicação pericial. O manuseio dessa ferramenta é feita completamente através de comandos em modo texto que são digitados no "prompt" do MS-DOS. Para que o perito possa fazer uma imagem de um dispositivo é preciso que ele conheça os comandos e os parâmetros necessários.

5 CONCLUSÃO

No mercado atual são muitas as ferramentas utilizadas para se fazer a análise pericial em um sistema operacional Microsoft Windows, o grande problema para a disseminação do uso dessas ferramentas são os preços de suas licenças. Praticamente não existe ferramenta para análise forense computacional que não seja cobrada a taxa de licença, e geralmente os preços não são acessíveis, o que implica diretamente na falta de recursos que auxiliem o trabalho dos peritos.

A ferramenta Norton Ghost da Symantec, é uma ferramenta gráfica, que permite, dentre outras funções, a duplicação pericial. A desvantagem encontrada no uso dessa ferramenta, além do preço de sua licença, é que ela não faz a cópia bit-a-bit, isso significa que o perito pode perder algum tipo de informação na hora da duplicação de imagem, como também não faz cópia de disquete, o ideal então é que se use uma ferramenta adequada para investigação.

Já a ferramenta Power Quest Drive Image da PowerQuest, ferramenta gráfica que realiza tanto a recuperação de dados que foram removidos intencionalmente, como também dados que foram perdidos, garante a realização de cópias fiéis dos dispositivos analisados.

A ferramenta Easy Recovery da Ontrack, recupera desde dados apagados até mesmo partições que foram corrompidas. Os dados recuperados podem ser enviados para disquetes, ou qualquer outro tipo de mídia removível como também para o próprio disco rígido. Sua desvantagem é que se trata de uma ferramenta com uma licença de alto custo.

Enquanto que GetDataBack é também uma ferramenta de recuperação de dados perdidos, recuperando desde HDs, partições, disquetes, imagens de HDs ou disquetes, drives Zip/Jaz e drives remotos. Com avançados algoritmos essa ferramenta assegura que todos os diretórios e subdiretórios se recomponham tal como eram e que os nomes de arquivos se reconstruam corretamente. A grande vantagem encontrada nessa ferramenta além de todas essas possibilidades de recuperação é que não há custo com licenciamento.

No mercado atual existem também ferramentas que são consideradas bastante completas. Ferramentas que foram desenvolvidas para atender às necessidades de investigadores e peritos que, cada vez mais, se deparam com a tarefa de analisar computadores em busca de provas em formato eletrônico.

A ferramenta FTK da Access Data, embora disponha de vários recursos, é uma ferramenta bastante simples de ser usada. Suporta sistemas de arquivos NTFS, FAT 12/16/32, Linux ext2 e ext3. Essa ferramenta oferece aos profissionais a habilidade de executar perícias completas em computadores.

Foram encontrados nessa ferramenta vários pontos positivos, como por exemplo: Recuperar e-mails deletados; Possui visualizador de registro; Gera auditoria de logs e relatórios de casos; Recupera automaticamente arquivos que foram deletados e partições; Visualiza mais de 270 formatos diferentes de arquivos. O fabricante dessa ferramenta disponibiliza em seu site uma versão que pode ser utilizada por qualquer tipo de usuário, o problema é que a versão oferecida, só oferece a análise de até 5.000 arquivos, o que dificulta a perícia completa em um computador suspeito. Para que o perito possa fazer a análise utilizando essa ferramenta é necessário que se pague pelo registro da mesma, com custo aproximado de U\$ 900. (Fonte: www.aceddata.com).

O Encase, da Guidance Softwares também é uma poderosa ferramenta gráfica, específica para análises forenses. Desenvolvido para ambientes Microsoft Windows, é fácil de ser usado, e suporta a maioria dos sistemas de arquivos, como por exemplo: FAT12 (disquete), FAT16, FAT32, NTFS, HFS, HFS+, Solaris UFS, EXT2/3, Reiser, BSD FFS, Palm, CDFS, Joliet, UDF e ISSO 9660.

Ele cria um arquivo de provas (evidence file) de forma que possa ser garantida a integridade e fidelidade original dos dados. Possui também o recurso de procurar um texto específico, pesquisando por palavras-chaves, hashes, assinaturas, filtros, por uma string dentro do arquivo de evidência criado, como também pesquisa por setor de disco em modo hexadecimal.

Os arquivos visualizados apresentam status indicando se estão acessíveis ou se foram excluídos e sua condição para ser recuperado. Suporta também e-mail em arquivos PST, inclusive PST comprimidos, criptografados e com senha, sendo possível também analisar arquivos de e-mails e suas particularidades tais como, cabeçalhos, anexos e seu conteúdo em si, além de históricos de páginas acessadas na internet, suportando vários navegadores. A desvantagem dessa ferramenta é o preço de sua licença, a versão básica chega a custar em torno de U\$ 2.500 (sem impostos). (Fonte: TechBiz).

As ferramentas para análise forense computacional baseadas no sistema operacional Windows são, portanto, completas e auxiliam de fato o trabalho do perito com recursos não convencionais e específicos, apresentando como principal empecilho para a sua utilização em larga escala o custo de licenças para a grande maioria das opções. Portanto, o referido

trabalho mostrou que as ferramentas mais indicadas para o uso de perícia forense computacional são aquelas que podem ser consideradas completas como o Encase da Guidance e o Forensic Toolkit da AccessData, apesar do alto custo de suas licenças.

ANDRADE, Thiago Felipe da. *Perícia Forense Computacional Baseada em Sistema Operacional Windows*. 2005. Disponível em:

<<http://www.burtoni.com.br/downloads/trabalhosacademicos/periciforensecomputacional.pdf>>. Acessado em: 14 set. 2006.

DANTAS, Ednardo Brandão. *Marketing Descomplicado*. Brasília: Senac, 2005.

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

_____. *Onde procurar provas?*. 2004. Disponível em:

<<http://www.guiatecnico.com.br/EvidenciaDigital/>>. Acesso em: 24 out. 2006.

GALVÃO, Ricardo Kleber Martins. *Forense Computacional – Perícia em crimes por computador*. 2005. Disponível em: <<http://www.copyleft.com.br/contendo/artigos.htm>>. Acesso em: 26 mar. 2006.

JOHNSON, Bradley C.; SHIMA, Mike. *Anti-Hacker Tool Kit*. Califórnia: Osborne, 2004.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Fundamentos de metodologia científica*. 4. ed. São Paulo: Atlas, 2001.

LIM-APO, Daniel Linhares. *Aplicação de Técnicas de Forense Computacional e Respostas a Incidentes na Internet*. 2004. Disponível em:

<<http://peritocriminal.com.br/afinformatica.htm>>. Acessado em: 14 jun. 2006.

MANDIA, Kevin; PROSSER, Chris. *Hackers: resposta e contra-ataque: investigando crimes por computador*. Rio de Janeiro: Campus, 2001.

OLIVEIRA, Flávio de Souza; GUIMARÃES, Celso Cardoso; GELUS, Paulo Lício de. *Resposta a incidentes para ambientes corporativos baseados em windows*. 2002. Disponível em: <<http://www.las.le.unicamp.br/paulo/papers/2002-WSeg-flavio.oliveira-resposta.incidentes.pdf>>. Acesso em: 23 mar. 2006.

OLIVEIRA, Flávio de Souza. *Metodologias de Análise Forense para Ambientes Baseados em NTFS*. 2001. Disponível em: <<http://www.las.le.unicamp.br/paulo/papers/2001-SSI-Flavio.oliveira-forense.rtf.pdf>>. Acesso em: 16 set. 2006.

REFERÊNCIAS

- ANDRADE, Thiago Felipe de. **Perícia Forense Computacional Baseada em Sistema Operacional Windows**. 2005, Disponível em:
<<http://www.batori.com.br/downloads/trabalhosacademicos/periciaforensecomputacional.pdf>>
> Acessado em: 14 set. 2006.
- DANTAS, Edmundo Brandão. **Marketing Descomplicado**. Brasília: Senac, 2005.
- FREITAS, Andrey Rodrigues de. **Perícia Forense Aplicada à Informática**. Rio de Janeiro: Brasport, 2006.
- _____. **Onde procurar provas?**. 2004. Disponível em:
<<http://www.guiatecnico.com.br/EvidenciaDigital/>>. Acesso em: 24 out. 2006.
- GALVÃO, Ricardo Kleber Martins. **Forense Computacional – Perícia em crimes por computador**. 2005. Disponível em: <<http://www.copyleft.com.br/conteudo/artigos.htm>>
Acesso em 26 mar. 2006.
- JOHNSON, Bradley C.; SHEMA, Mike. **Anti-Hacker Tool Kit**. Califórnia: Osborne, 2004.
- LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 4. ed. São Paulo: Atlas, 2001.
- LIM-APO, Daniel Linhares. **Aplicação de Técnicas de Forense Computacional e Respostas a Incidentes na Internet**. 2004. Disponível em:
<<http://peritocriminal.com.br/pfinformatica.htm>>. Acessado em: 14 jun. 2006.
- MANDIA, Kevin; PROSISE, Chris. **Hackers: resposta e contra-ataque: investigando crimes por computador**. Rio de Janeiro: Campus, 2001.
- OLIVEIRA, Flávio de Souza; GUIMARÃES, Célio Cardoso; GEUS, Paulo Lício de. **Resposta a incidentes para ambientes corporativos baseados em windows**. 2002. Disponível em: <<http://www.las.ic.unicamp.br/paulo/papers/2002-WSeg-flavio.oliveira-resposta.incidentes.pdf>>. Acesso em: 23 mar. 2006.
- OLIVEIRA, Flávio de Souza. **Metodologias de Análise Forense para Ambientes Baseados em NTFS**. 2001. Disponível em: <<http://www.las.ic.unicamp.br/paulo/papers/2001-SSI-flavio.oliveira-forense.ntfs.pdf>>. Acesso em: 16 set. 2006.

REIS, Marcelo Abdalla dos; GEUS, Paulo Lício de. **Forense computacional: procedimentos e padrões**. 2001. Disponível em: <<http://www.las.ic.unicamp.br/paulo/papers/2001-SSI-marcelo.reis-forense.padroes.pdf>>. Acesso em: 03 abr. 2006.

ROCHA, Luís Fernando. **Perícia forense computacional em debate**. 18 de agosto de 2004. Disponível em: <<http://www.modulo.com.br>>. Acesso em: 27 mar. 2006.

_____. **Forense em windows: características, ferramentas e desafios**. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=7&objid=3999>. Acesso em: 21 mar. 2006.

SHINDER, Debra Littlejohn. **Scene of the Cybercrime**. United States of America: Syngress Publishing, 2002.

VACCA, John R. **Computer Forensics: Computer Crime Scene Investigation**, Second Editon. Hingham:Charles River Media, 2002.

YAMAMOTO, Marcos Massao. **Ferramenta Recuperador de Arquivos Perdidos**. 2004. Disponível em: <<http://www.din.uem.br/~oasantos/Monografias/Recuperador-de-Arquivos.pdf>>. Acesso em: 04 nov. 2006.