UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC
CURSO DE CIÊNCIA DA COMPUTAÇÃO

NATANIEL CORRÊA DE OLIVEIRA

APLICAÇÃO DE TÉCNICAS DE ANTI-FORENSE COMPUTACIONAL EM ARQUIVOS NTFS

CRICIÚMA
2012

NATANIEL CORRÊA DE OLIVEIRA

APLICAÇÃO DE TÉCNICAS DE ANTI-FORENSE COMPUTACIONAL EM ARQUIVOS NTFS

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA

2012

NATANIEL CORRÊA DE OLIVEIRA

APLICAÇÃO DE TÉCNICAS DE ANTI-FORENSE COMPUTACIONAL EM ARQUIVOS NTFS

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Computação Forense.

Criciúma, 27 de junho de 2012.

BANCA EXAMINADORA

Prof. Paulo João Martins - MSc. - (UNESC) - Orientador

Prof. Fabrício Giordani - Esp. - (UNESC)

Prof. Sérgio Coral - Esp. - (UNESC)

Dedico este trabalho à minha família, em especial a meus pais, Edson e Tânia, esposa Jocimara e filha Rafaela pela compreensão, apoio e incentivo em todos os momentos dessa jornada.

AGRADECIMENTOS

Agradeço primeiramente aos meus pais, minha esposa e filha que sempre acreditaram e me apoiaram no sonho de mais uma graduação.

Meu sincero agradecimento a todos os professores e funcionários da UNESC, em especial ao professor e orientador deste trabalho, Paulo João Martins.

Um agradecimento especial ao professor Fernando Fonseca da Segurança Objetiva pela prontidão no auxílio sobre algumas questões desta pesquisa.

Não poderia deixar de agradecer aos colegas de graduação pelo companheirismo e experiência compartilhada ao longo destes anos.

Muito obrigado a todos!

“Nunca deixe para amanhã a segurança que se pode praticar hoje.”

Autor desconhecido

RESUMO

Existem informações valiosas e sigilosas que devem estar protegidas das técnicas de análise forense, visando evitar a quebra da confidencialidade dos dados. O objetivo deste trabalho baseia-se no uso de ferramentas e técnicas de anti-forense computacional em um dispositivo com sistema de arquivos NTFS, buscando a proteção dos arquivos para garantir a segurança e privacidade de seu conteúdo. Um dos objetivos da anti-forense é bloquear diferentes tipos de análise alterando o modo como estes dados estão armazenados e organizados, impedindo ou pelo menos dificultando o acesso às informações sigilosas. A criptografia destaca-se como método mais conhecido ou, podem-se esconder arquivos empregando a esteganografia. Ferramentas de perícia forense foram utilizadas para vasculhar o dispositivo, inicialmente sem técnicas anti-forense e em um segundo momento, aplicando criptografia com as ferramentas TrueCrypt e BitLocker. Como resultado, ao fazer uso de uma chave forte, não foi possível quebrar a criptografia na unidade de armazenamento com sistema de arquivos NTFS, mantendo assim a confidencialidade dos arquivos nela contidos. Em contrapartida, com o dispositivo desprotegido todo seu conteúdo foi recuperado, inclusive arquivos que haviam sido excluídos. Da mesma forma, mesmo com criptografia AES-256, ao utilizar-se uma chave fraca, conseguiu-se a quebra da mesma.

Palavras-chave: Forense computacional. Perícia forense. Anti-forense. Criptografia.

ABSTRACT

There are valuable and confidential information that should be protected from forensic analysis techniques in order to avoid breaking of data confidentiality. The objective of the study is based on the use of tools and anti-forensics techniques in a device with NTFS file system, seeking the protection of the files to ensure their content security and privacy. One of the aims of anti-forensic is to block different types of analysis by changing the way these data are stored and organized, preventing or, at least, hindering access to confidential information. The encryption stands out as the best known method to hide files, but steganography can also be used. Forensic expertise tools were used to scan the device, first without anti-forensic techniques, then, as a second step, applying encryption through TrueCrypt and BitLocker tools. Results show that, by using a strong key, the encryption in the storage unit with NTFS file system could not be broken, thus maintaining the confidentiality of its files. On the other hand, with the device being unprotected all its contents could be recovered, including files that had been deleted; similarly, even the AES-256 encryption could be broken by using a weak key.

Keywords: Computer forensics; Forensic expertise; Anti-forensic; Encryption.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACM	Association for Computing Machinery
AES	Advanced Encryption Standart
AFF	Advanced Forensic Format
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
CND	Central Nacional de Denúncias de Crimes Cibernéticos
CPU	Central Processing Unit
DES	Data Encryption Algorithm
DoS	Denial of Service
EDRM	Eletronic Discovery Reference Model
FAT	File Allocation Table
FTK	Forensic Toolkit
GPU	Graphics Processing Unit
HD	Hard Disk
INPC	Instituto Nacional de Criminalística da Polícia Federal
IOCE	International Organization on Computer Evidence
IP	Internet Protocol
JPHS	JP Hide and Seek
LSB	Least Significant Bit
MBR	Master Boot Record
MTF	Master File Table
NTFS	New Technologies File Systems
PL	Projeto Lei
RIPEMD	Race Integrity Primitives Evaluation Message Digest

SBC	Sociedade Brasileira de Computação
SHA	Secure Hash Algorithm
SO	Sistema Operacional
SOP	Standart Operating Procedures
SUCESU	Associação de Usuários de Informática e Telecomunicações
SWGDE	Scientific Working Group on Digital Evidence
TCC	Trabalho de Conclusão de Curso
TPM	Trusted Platform Module
USB	Universal Serial Bus

SUMÁRIO

1 INTRODUÇÃO

Atualmente, uma gama de produtos e serviços encontram-se disponíveis na rede mundial de computadores no intuito de facilitar o dia a dia das pessoas. Porém, a utilização destas facilidades por pessoas mal intencionadas acabou por gerar um antagonismo entre o bom e o mau uso dos recursos, não tardando para que fossem utilizados em práticas ilegais e criminosas.

Ferramentas específicas e poderosas são criadas para investigar máquinas, periféricos e dispositivos em busca de vestígios e provas desta nova modalidade de crime.

Torna-se importante empregar boas práticas na coleta, restauração, identificação, preservação, documentação, análise de dados periciais, apresentação de vestígios, evidências e provas digitais e interpretação, sejam elas aplicadas a componentes físicos ou dados processados e/ou armazenamento em mídias computacionais (MELO, 2009).

A Computação Forense tem como objetivo principal determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área de informática, tendo como questão principal o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhe validade probatória em juízo (ELEUTÉRIO; MACHADO, 2011).

Em contrapartida, empresas possuem informações valiosas que devem estar seguras e protegidas inclusive das técnicas de análise forense com o objetivo de evitar a quebra da confidencialidade de dados. As organizações passam a necessitar de técnicas, visando proteger, por exemplo, informações delicadas dos usuários ou clientes, detalhes de contas bancárias, históricos médicos, dados financeiros, números pessoais de identificação, planos de negócios confidenciais, descrição detalhada de projetos, e-mail entre outros.

Anti-forense, portanto, são técnicas de remoção, ocultação e subversão de evidências com o objetivo de mitigar os resultados de análises forenses computacionais (HENRIQUE, 2006).

Técnicas anti-forense dificultam o trabalho do perito forense por apagar ou ocultar informações, plantar provas falsas, explorar bugs de implementação em ferramentas conhecidas, geralmente gerando um grande aumento no tempo gasto na investigação.

Pode-se identificar quatro metas principais para a anti-forense: evitar a detecção de algum tipo de evento que tenha ocorrido; interromper a coleta de informações; aumentar o tempo que o examinador precisa gastar em um caso e, colocar em dúvida um relatório forense ou testemunho (BROWN; LIU, 2006).

Alguns autores definem que estas técnicas tem um objetivo puramente malicioso, buscando burlar técnicas forenses para se esconder e camuflar seus atos. Outros autores defendem que esta técnica objetiva aprimorar técnicas de computação forense, obrigando investigadores a criar novos procedimentos de análise em um crime digital (BARRETO, 2009).

Entre as técnicas anti-forense mais conhecidas e utilizadas há a criptografia, o saneamento de discos para remover dados confidenciais com segurança e técnicas de esconder dados como a esteganografia ou mesmo, utilizar ferramentas que escondem os dados em algum local no disco.

Diante deste contexto, este trabalho de pesquisa visa descrever e demonstrar as técnicas utilizadas na anti-forense quando a investigação forense possuir objetivos ilícitos.

1.1 OBJETIVO GERAL

Utilização de técnicas e procedimentos de anti-forense computacional, como forma de proteger dados sigilosos em discos rígidos.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos definidos para elaboração deste trabalho seguem abaixo:

a) compreender os conceitos da Computação Forense;
b) entender e aplicar as técnicas e procedimentos de ferramentas da Computação Forense;
c) pesquisar (conhecer) técnicas anti-forense com o objetivo de proteger dados sigilosos em um dispositivo de armazenamento;
d) aplicar técnicas anti-forense sob uso de ferramentas forenses (Forense Tool Kit, Encase, Autopsy e Passware Kit Forensic).

1.3 JUSTIFICATIVA

O crescente armazenamento de informações em ambiente digital aumentou a chance de exposição de dados sensíveis, sejam pessoais ou corporativos.

Com a popularidade de ferramentas e técnicas, a análise forense em um computador vem se tornando cada dia mais fácil, viabilizando sua utilização não só para investigadores forenses (BARRETO, 2009).

Pode-se citar o caso da Petrobrás, em fevereiro de 2008, onde foram roubados de um contêiner dois computadores portáteis e um disco rígido contendo informações importantes (JUNIOR, 2008).

Uma pesquisa realizada pelo Centro de Segurança e Pesquisa BT em colaboração com a Universidade de Glamorgam na Inglaterra, Universidade Edith Cowan da Austrália e Universidade Longwood dos Estados Unidos, revelaram que discos rígidos são vendidos em vários países no mercado paralelo (LLEWELLYN, 2009).

Mais de trezentos discos foram analisados durante a pesquisa e o resultado mostrou que 34% continham informações de dados pessoais e organizacionais. Entre os achados, destacam-se dados delicados de usuários, detalhes de contas bancárias, históricos médicos, informações financeiras de corporações, números de identificação pessoal, planos de negócios confidenciais e ainda descrição detalhada de trabalhos (LLEWELLYN, 2009).

Ainda de acordo com os pesquisadores o mais impressionante e preocupante foi o de um *hard disk* (HD) vendido pelo eBay nos Estados Unidos. Uma análise neste disco mostrou detalhes de lançamento de um míssil THAAD, do sistema de defesa norte-americano (LLEWELLYN, 2009).

São apenas alguns exemplos que justificam o uso de técnicas e ferramentas de anti-forense computacional, objetivando a esterilização ou proteção de arquivos para garantir a segurança e privacidade de seu conteúdo.

O escopo deste trabalho é, portanto, descrever e demonstrar procedimentos e ferramentas anti-forense em dispositivos de armazenamento com sistema de arquivos NTFS, com o objetivo de preservar a confidencialidade de determinados arquivos de uma análise forense.

1.4 ESTRUTURA DO TRABALHO

O capítulo 1 deste trabalho apresenta a definição do problema, bem como objetivos gerais e específicos a serem abordados no mesmo. Contém também a justificativa que demonstra a importância do uso da anti-forense para manter a confidencialidade de certas informações e dados.

O capitulo 2 trata de crimes digitais trazendo conceitos, estatísticas, tipos de ataques e formas de utilização do equipamento computacional como apoio na prática de tais delitos.

Explana ainda sobre a situação da legislação frente aos procedimentos de uma perícia forense computacional, diante do elevado aumento na criminalidade digital e aborda ao final, algumas questões sobre a ética na computação.

No capítulo 3, sobre perícia forense computacional, abordam-se conceitos, fases da perícia, uso de ferramentas forense para fins ilícitos bem como, são apresentadas algumas das principais ferramentas utilizadas pelos peritos.

Já no capítulo 4, conceitua-se a anti-forense computacional. A seguir são abordados conceitos de disco rígido, sistema de arquivos em geral e sistema de arquivos NTFS.

Ainda neste capítulo são abordadas algumas técnicas para proteção de informações, como a ocultação de dados, a criptografia e a esteganografia.

Trabalhos correlatos são apresentados no capítulo 5.

A metodologia, análises e todos os resultados obtidos e respectivas análises estão dispostos no capítulo 6.

O capítulo 7 relata a conclusão desta pesquisa.

2 CRIMES DIGITAIS

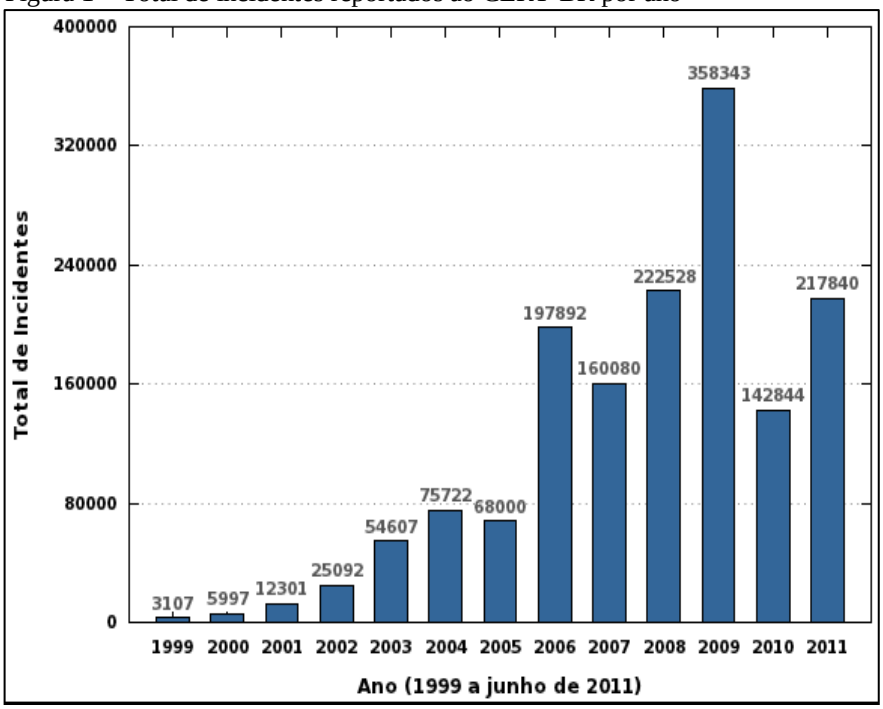
O crescimento tecnológico ao longo da história contribuiu para o surgimento de novas atividades criminosas. Assim, como muitas pessoas beneficiam-se desta tecnologia por razões legítimas, existem as que a utilizam com intenção de cometer o crime (BRYANT, 2008, tradução nossa).

Crimes virtuais ocorrem com alta frequência. Criminosos utilizam ferramentas de alta tecnologia, seja para destruir dados, seja para obter informações sigilosas. Cresce assim, a necessidade de proteger a informação e a disponibilidade da informação (SANTOS, 2009).

Tais crimes crescem na proporção do avanço tecnológico. O sentimento de anonimato, a impunidade e a facilidade de alcance global dos meios de comunicação são elementos que norteiam o aumento do número de infratores dessa natureza (ABRUSIO; BLUM, 2004).

É nítido que a Internet simboliza todo esse grande avanço tecnológico. Com a falsa impressão de anonimato ao praticar atos ilícitos, houve a migração dos criminosos para o *cyberspace*. Na realidade são os mesmos crimes, apenas alterado o *modus operandi* [1] (TRUZZI, 2008).

Figura 1 – Total de incidentes reportados ao CERT-BR por ano



Fonte: CERT-BR

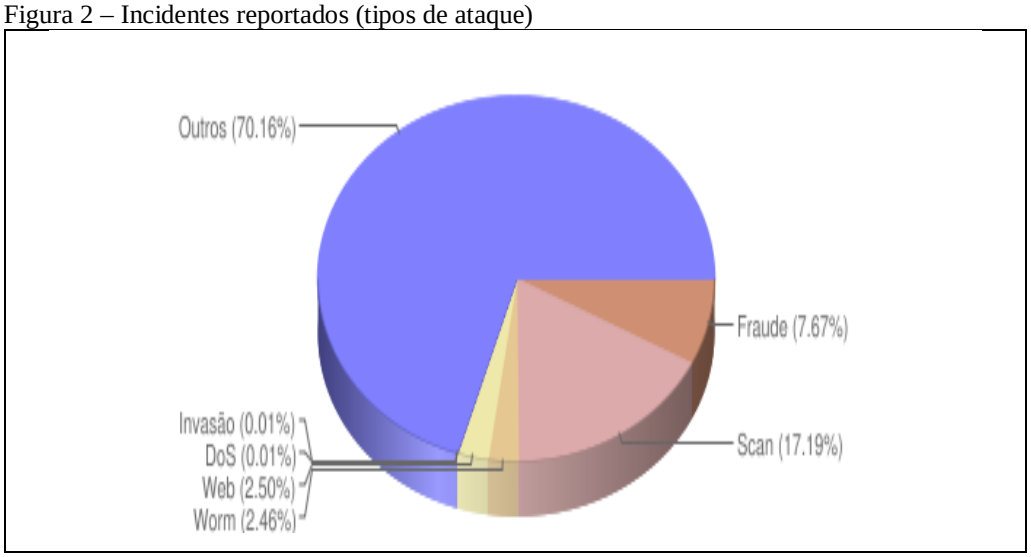
[1] Modus operandi é uma expressão em latim que significa "modo de operação". Utilizada para designar uma maneira de agir, operar ou executar uma atividade seguindo os mesmos procedimentos.

A Figura 1 demonstra a evolução de ações ilícitas na Internet. Esse dado quantificado reforça o argumento da necessidade de, cada vez mais, o profissional de segurança utilizar as técnicas de perícia forense computacional (MELO, 2009).

Entre os tipos de ataques reportados (figura 2) encontram-se:

a) *worm*: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede;
b) *Denial of Service* (DoS): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede;
c) invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede;
d) web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet;
e) *scan*: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles;
f) fraude: esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem;
g) outros: notificações de incidentes que não se enquadram nas categorias anteriores.

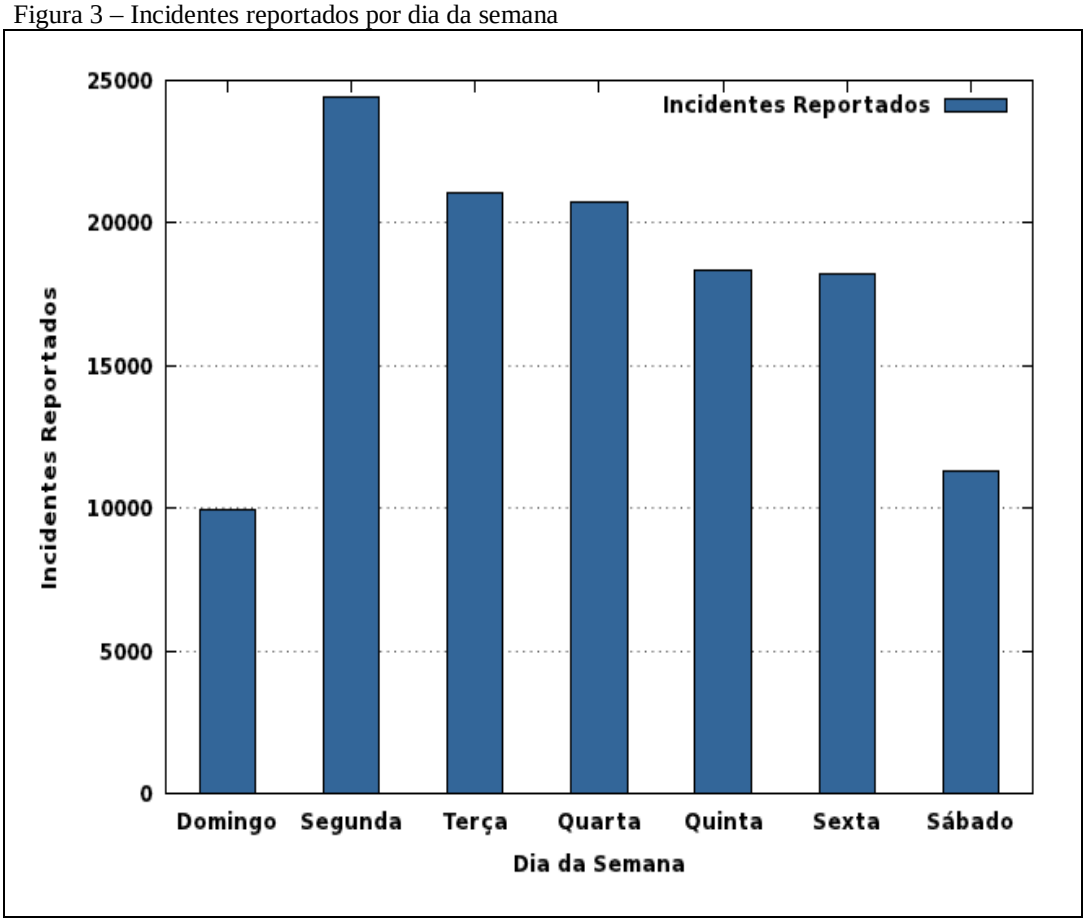
Figura 2 – Incidentes reportados (tipos de ataque)



Fonte: CERT-BR (2011)

Outro dado interessante visualizado nas estatísticas do CERT-BR, figura 3, é que a maioria dos ataques ocorre nos finais de semana e são identificados e reportados nas segundas-feiras. Tal fato acontece pela falta de um profissional no fim de semana, atuando na segurança de redes.

Figura 3 – Incidentes reportados por dia da semana



Fonte: CERT-BR (2011)

Sendo os crimes digitais ou crimes tecnológicos uma nova modalidade de delito, lesando cidadãos, corporações, governos, não existem punições adequadas previstas em lei (SANTOS, 2009).

Existem projetos de leis com objetivo de regularizar a utilização de sistemas informáticos, alavancados pela necessidade de punição de atos ilícitos pelas instituições legais (THOMAS, 2010).

Destacam-se alguns dos novos delitos de crimes digitais como o *cracking* que é a quebra de um sistema de segurança, ilegalmente e sem ética por um cracker. Há uma técnica que permite o roubo de informações de uma máquina com o objetivo de burlar uma transação financeira denominada *phishing scam* (SANTOS, 2009).

Citam-se ainda a espionagem digital que é a obtenção ou divulgação sem autorização de um segredo comercial ou industrial; o pichamento digital que consiste em inserir textos ou imagens em sites sem a autorização destes e ainda, práticas hacker de *gray hat*[2] ou *black hat*[3] (SANTOS, 2009).

Nessa modalidade, o equipamento computacional é utilizado como ferramenta de apoio ou como meio para realização do crime (ELEUTÉRIO; MACHADO, 2011).

2.1 COMPUTADOR COMO FERRAMENTA DE APOIO AOS CRIMES

O computador auxilia nas práticas criminosas como sonegação fiscal, compra de votos em eleições, tráfico de entorpecentes, falsificação de documentos e outros (ELEUTÉRIO; MACHADO, 2011).

Como o computador está associado ao delito, exames forenses configuram-se em ótima prova técnica e seus laudos contribuem fortemente para convencer o juiz na elaboração da sentença (ELEUTÉRIO; MACHADO, 2011).

A utilização do equipamento como apoio corresponde a aproximadamente 90% dos exames forenses computacionais (ELEUTÉRIO; MACHADO, 2011).

2.2 COMPUTADOR COMO MEIO DE REALIZAÇÃO DO CRIME

O computador é peça fundamental para que o crime seja praticado. Faz-se necessária a existência de algum tipo de dispositivo para efetivação do crime (ELEUTÉRIO; MACHADO, 2011).

As práticas nesse módulo incluem ataques a sites, roubo de informações, *phishing*, programas maliciosos para roubo de senhas (*malwares*) e outros.

Tal prática ocupa os 10% restantes das pericias forenses computacionais devendo crescer em um futuro próximo (ELEUTÉRIO; MACHADO, 2011).

2.3 LEGISLAÇÃO

Inicialmente, vale destacar que a nomenclatura para crimes digitais, tanto no Brasil como em outros países, não está uniformizada (DAUON; LIMA, 2006).

---

[2] Hacker que penetra em sistemas desde que não cometa roubo, vandalismo ou infrinja a confidencialidade.
[3] Hacker criminoso ou malicioso, não possui ética. Especializados em invasões maliciosas e silenciosas.

A legislação é a principal barreira para as perícias forenses. O perito deve obter informações sobre ações, dispositivos, sistemas, podendo acabar em quebra de sigilo e privacidade do autor dessas ações. Para que tal atividade seja executada legalmente faz-se necessário um pacote de normas e leis que regulamentem os crimes e a prestação de serviços de informática (COSTA, 2003).

Administradores de sistemas corporativos investigam condutas irregulares, documentando-as para servirem como prova em ação trabalhista. Mas isso só pode ocorrer com normas, regulamentos e políticas que protejam os direitos da empresa e do empregado (COSTA, 2003).

A efetividade da justiça depende de vários fatores que vão desde a recepção das mudanças tecnológicas pelo Direito Processual no âmbito civil e criminal, e também pelo judiciário e demais órgãos envolvidos com esse objetivo (SANTOS, 2009).

Deve ser efetuada uma análise extremamente cautelosa acerca da criação de leis penais envolvendo tecnologia da informação (DAUON; LIMA, 2006).

Projetos de leis tramitam quase que em *loop*[4] no congresso nacional por falta de informação ou excesso burocrático. Consequentemente, nenhum projeto importante que venha agregar à nossa legislação as modificações necessárias tem sido sancionado (THOMAS, 2010).

A Câmara dos Deputados aprovou recentemente (maio/2012) o projeto 2973/2011 que trata de crimes digitais. As condutas ilícitas consideradas neste projeto lei: invasão de computadores, ataques de negação de serviço, instalação de vulnerabilidades, venda de dispositivo ou programa que permita a prática ilícita e, falsificação de documento particular ou cartão de débito ou crédito. Agora precisa tramitar pelo Senado onde ainda pode sofrer alterações (ROHR, 2012).

O projeto lei (PL) 84/99 proposto no ano de 1999 pelo ex-deputado Luiz Piauhylino, que recebeu em 2008 um texto substitutivo pelo Senador Eduardo Azeredo, foi recém-aprovado (maio/2012) na Comissão de Ciência e Tecnologia da Câmara. Para que se torne lei ainda precisa de aprovação pela Comissão de Constituição e Justiça e a seguir, a sanção da presidência da república (SILVA, 2012).

O texto do projeto foi bastante reduzido, dos vinte e três artigos originais apenas seis foram mantidos. A falsificação de dados eletrônicos (com um parágrafo apenas para incluir nesse crime a falsificação de dados de cartão de crédito ou débito) e traição por

[4] Palavra inglesa que no contexto da língua portuguesa significa uma sequência, conjunto de instruções repetidas até que se alcance determinada situação.

transferência de dados ao inimigo são os crimes tipificados no PL. Também permite a retirada do ar de páginas com mensagens racistas e a criação de um órgão ligado à polícia especializada no combate à delitos na internet (SILVA,2012).

Como o avanço tecnológico é bastante dinâmico, existe ainda um descompasso na atuação de órgãos que atuam no combate de crimes digitais (SANTOS, 2009).

Foi criada a SaferNet Brasil, que por meio da CND, operando em conjunto com o Ministério Público Federal, oferece aos brasileiros e à comunidade internacional um serviço anônimo de recebimento, processamento, encaminhamento e acompanhamento on-line de denúncias sobre qualquer crime ou violação aos Direitos Humanos praticado por meio da Internet (SANTOS, 2009).

Existe ainda o INPC, destaque na comunidade cientifica internacional, como um dos mais completos e modernos do mundo (SANTOS, 2009).

É importante destacar que independente da criação de uma lei para crimes digitais, cabe a cada usuário conhecer as práticas fraudulentas circulantes na Internet e prevenir-se dos riscos por meio da adoção de uma postura consciente (TRUZZI, 2008).

Diante deste contexto cabe trazer nesta pesquisa algumas questões éticas relacionadas à informática.

2.4 ÉTICA EM INFORMÁTICA

Embora não tenhamos a regulação, todo profissional de informática deve ser consciente e honesto, zelando pelo seu nome e pela classe (MENESES, 2011).

A questão pessoal é sempre de grande importância quando o assunto é a ética. Na informática como na maior parte das profissões, a ética deve englobar dois aspectos, a conduta pessoal como ser humano e a conduta profissional (LEMOS, 2009).

A ética tem uma relação direta com o comportamento moral. Portanto, diz respeito a uma conduta responsável ou irresponsável, ao mau ou ao bom, ao proibido, ao facultativo ou ao obrigatório (OTERO, 2003).

Ao agir em desacordo com a sociedade na qual se encontra inserido, inclusive prejudicando terceiros, ainda assim pode ser considerado um comportamento ético desde que estas ações sejam justificáveis para o próprio indivíduo. No entanto, não será ético perante o grupo ou sociedade a qual pertence (LEMOS, 2009).

Um código de ética compreende, portanto, um conjunto de diretrizes, as quais, vem esclarecer as circunstâncias em que cada caso se aplica, podendo existir um conjunto de casos para estudo comparativo, ajudando na solução de situações novas (LEMOS, 2009).

Deve ficar claro que um conjunto mínimo precisa ser identificado para que sejam possíveis análises de abusos ou contravenções (OTERO, 2003).

Como em qualquer profissão, ser ético é imprescindível também nas atividades da área de informática. Talvez a regulamentação da profissão servisse para criar um código com os parâmetros necessários para manutenção da ética (MENESES, 2011).

A Sociedade Brasileira de Computação (SBC) não possui um código de ética para orientação de seus afiliados, apenas um projeto baseado no código da ACM e da British Computer Society. A SUCESU que também atua no ramo, por ter sua composição basicamente de instituições, também não possui um código a ser seguido (MENESES, 2011).

O Instituto para Ética da Computação elaborou um pequeno código de conduta que ficou conhecido como "Os Dez Mandamentos para Ética na Informática", disposto a seguir:

a) você não deverá usar o computador para produzir danos a outra pessoa;
b) você não deve interferir no trabalho de computação de outra pessoa;
c) você não deve interferir nos arquivos de outra pessoa;
d) você não deve usar o computador para roubar;
e) você não deve usar o computador para dar falso testemunho;
f) você não deverá usar software pirateado;
g) você não deverá usar recursos de computadores de outras pessoas;
h) você não deverá se apropriar do trabalho intelectual de outra pessoa;
i) você deverá refletir sobre as consequências sociais do que escreve;
j) você deverá usar o computador de maneira que mostre consideração e respeito ao interlocutor.

Alguns indivíduos não seguem os preceitos da ética e utilizam de forma indevida equipamentos e softwares como, por exemplo, as ferramentas da perícia forense computacional.

3 PERICIA FORENSE COMPUTACIONAL

A existência de um sistema forense e a execução de práticas de investigação são de grande importância para que se obtenha um sistema condizente com a realidade do ambiente em que se encontra (ROSA, 2004).

Pericia forense computacional é um processo em que utiliza o conhecimento de técnicas e métodos apoiados por ferramentas apropriadas, com o intuito de obter dados e equipamentos com o objetivo de classifica-los como vestígio, evidências ou prova em caráter judicial (MELO, 2009).

Diferentes crimes geram diferentes tipos de evidência. Consequentemente, a habilidade do perito em identificar essas evidências depende do seu conhecimento sobre o tipo do crime cometido e dos programas e Sistemas Operacionais envolvidos (FREITAS, 2006).

Todo e qualquer evento em um computador acaba deixando alguma fonte de informação residente em algum tipo de memória, seja volátil ou não volátil, salvo a memória volátil após algum tempo de utilização ou interrompendo a alimentação elétrica do sistema (PAIVA, 2009).

3.1 FASES DO EXAME FORENSE EM DISPOSITIVOS DE ARMAZENAMENTO

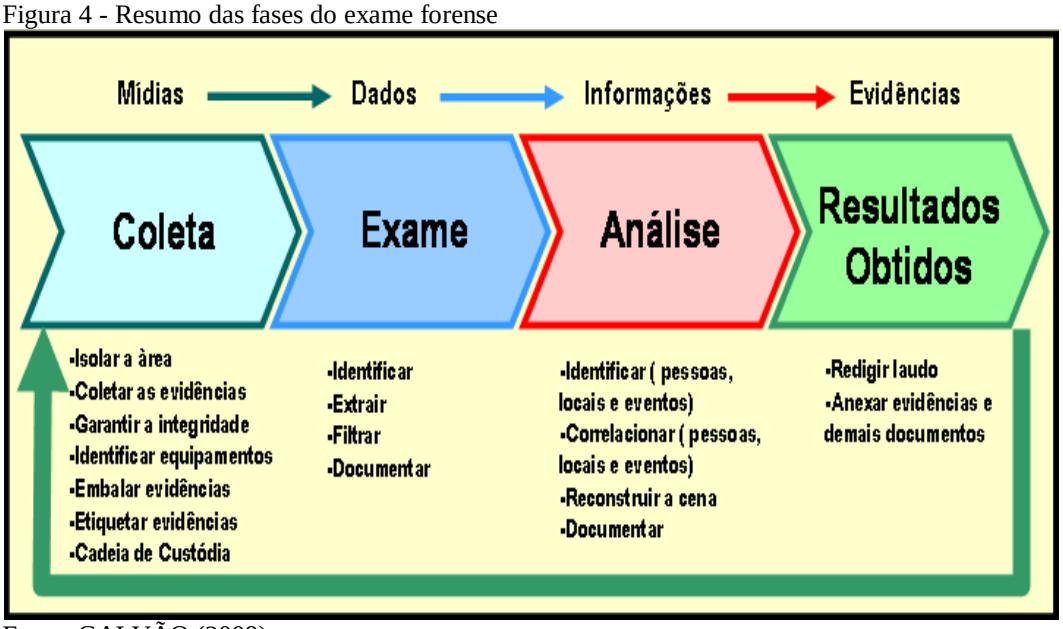
Tratando-se de uma possível prova de crime os dispositivos de armazenamento devem ser manuseados com extremo cuidado. As principais características desses dispositivos são: fragilidade, facilidade de cópia, sensibilidade ao tempo de vida e sensibilidade ao tempo de uso (ELEUTÉRIO; MACHADO, 2011).

Dentre os procedimentos ou fases de uma perícia forense, figura 4, encontram-se: aquisição, preservação, extração, análise e formalização (MELO, 2009; ELEUTÉRIO; MACHADO, 2011).

3.1.1 Aquisição

É a primeira fase do processo. A qualidade do material coletado e a validade dos procedimentos efetuados é crucial nesse momento de aquisição de provas. Devem ser pesquisados todos os possíveis dispositivos que contenham dados passíveis de tornarem-se provas relevantes (MELO, 2009).

Figura 4 - Resumo das fases do exame forense



Fonte: GALVÃO (2009)

3.1.2 Preservação

É a garantia de que todas as informações armazenadas no material coletado jamais sejam alteradas. O simples fato de ligar um computador, por exemplo, pode alterar dados armazenados em mídia digital (ELEUTÉRIO; MACHADO, 2011).

As evidências devem ser preservadas de tal modo que não exista dúvida alguma quanto a sua veracidade (FREITAS, 2006).

Pela fragilidade e sensibilidade das mídias de armazenamento computacional, cópias fiéis devem ser obtidas a partir do material original (ELEUTÉRIO; MACHADO, 2011).

O dispositivo de armazenamento deve ser lacrado, etiquetado e guardado (figura 5) em local apropriado (ELEUTÉRIO; MACHADO, 2011).

A investigação forense deve manter um alto padrão de qualidade empregando tais procedimentos dentro de uma metodologia adequada, com o objetivo de garantir a confiabilidade e precisão das evidências (VARGAS, 2007).

3.1.3 Extração

A fase de extração compreende a recuperação de todas as informações contidas na cópia dos dados efetuadas na fase de preservação. Os principais procedimentos desta fase são

a recuperação de arquivos apagados e a indexação de dados (ELEUTÉRIO; MACHADO, 2011).

Figura 5 – Material de perícia forense lacrado e etiquetado

Fonte: GALVÃO (2009)

3.1.4 Análise

O objetivo desta fase é tentar identificar quem fez, quando fez, que dano causou e como foi consumado o crime. Deve-se ter o conhecimento para saber o que procurar, onde procurar e como procurar. Tudo que for aqui descoberto deve ser documentado para posterior uso como prova no tribunal (FREITAS, 2006).

3.1.5 Formalização

Fase final de uma perícia forense, compreende a elaboração do laudo pelo perito, identificando o resultado e mostrando as evidências digitais encontradas nos materiais analisados (ELEUTÉRIO; MACHADO, 2011).

O laudo pericial é um relatório técnico de toda investigação, apontando os fatos, procedimentos, análises e resultado. A partir dessas evidências a decisão é da justiça (FREITAS, 2006).

Dentro das três metodologias forenses existentes estas fases podem ser subdivididas ou receber uma nomenclatura própria, tabela 1.

Tabela 1 – Metodologias forenses e respectivas fases

SOP	Reith, Carr e Gunsh	EDRM
Coleta da prova	Identificação	Identificação
Preparação do Equipamento	Preparação	Preservação
Imagem Forense	Abordagem estratégica	Coleta
Exame/análise	Preservação	Processamento
Documentação	Coleção	Revisão
Relatórios	Exame	Análise
Revisão	Análise	Produção
	Apresentação	Apresentação
	Devolução de provas	

Fonte: Do autor.

3.2 UTILIZAÇÃO DA PERÍCIA FORENSE COM FINS ILÍCITOS

Com a facilidade de acesso às ferramentas e técnicas de análise forense, indivíduos passam a utilizar os procedimentos de forma ilícita visando quebrar a confidencialidade de dados (BARRETO, 2009).

Um criminoso pode obter várias informações sigilosas em uma estação de trabalho como o perfil de quem a utiliza, os sites que utiliza, documentos sigilosos, senhas, projetos, entre outros (BARRETO, 2009).

O indivíduo interessado nesse tipo de prática pode ter acesso vasculhando o HD utilizando-se de técnicas forenses, avançadas ou não, para obter ou até recuperar dados deletados. Torna-se necessária a utilização de alguns métodos, anti-forense, para tornar impossível ou mais difícil esse acesso a dados confidenciais (BARRETO, 2009).

3.3 FERRAMENTAS PARA EXAME FORENSE COMPUTACIONAL

As ferramentas são um conjunto de softwares confiáveis, componente fundamental na perícia forense, obtendo-se através dele as evidências do crime (FREITAS, 2006).

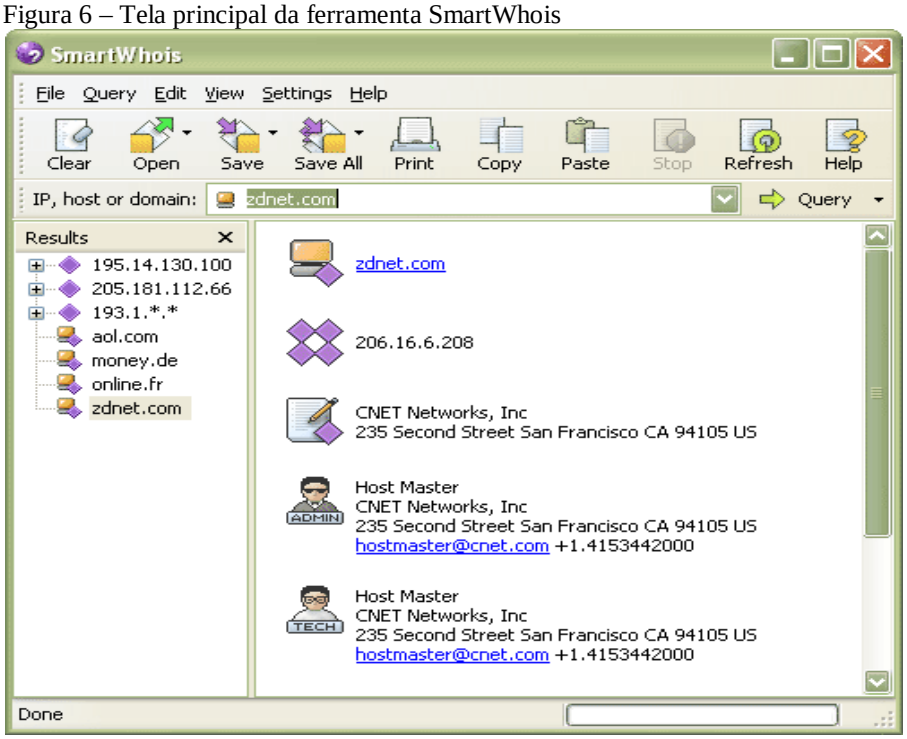
Com o desenvolvimento tecnológico dos últimos anos tornou-se necessário o uso de ferramentas mais modernas e mais incrementadas na busca de infratores (VARGAS, 2011).

3.3.1 SmartWhois

Criada pela empresa especializada em segurança de informação Tamasoft, auxilia na verificação de IPs e domínios na Internet (VARGAS, 2011)

A figura 6 ilustra a tela de abertura do SmartWhois. O usuário indica o domínio ou IP que deseja pesquisar e a ferramenta retorna todas as informações destes.

Figura 6 – Tela principal da ferramenta SmartWhois



Fonte: VARGAS (2011)

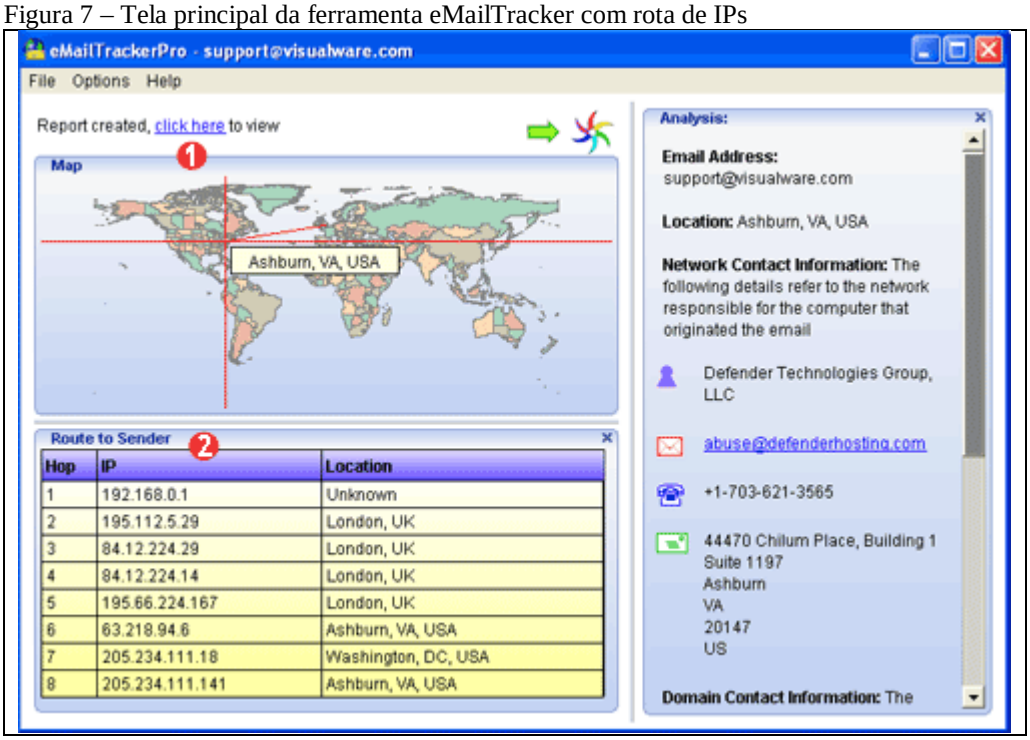
3.3.2 Emailtracker

Criada e distribuída pela empresa Visualware, a ferramenta eMailTracker fornece através de uma entrada de um e-mail ou uma lista de e-mails, o local de origem, onde fora criado este e-mail (VARGAS, 2011).

Além da localização da origem do e-mail, eMailTracker possui tecnologia de filtragem de spam, detecta anormalidades no cabeçalho do e-mail e apresenta um relatório de rastreamento (VISUALWARE, 2011).

A figura 7 apresenta à esquerda a rota de um determinado e-mail por IPs e a rota do mesmo no mapa mundial, enquanto que à direita é mostrada a empresa responsável pelos serviços de e-mail.

Figura 7 – Tela principal da ferramenta eMailTracker com rota de IPs



Fonte: VARGAS (2011)

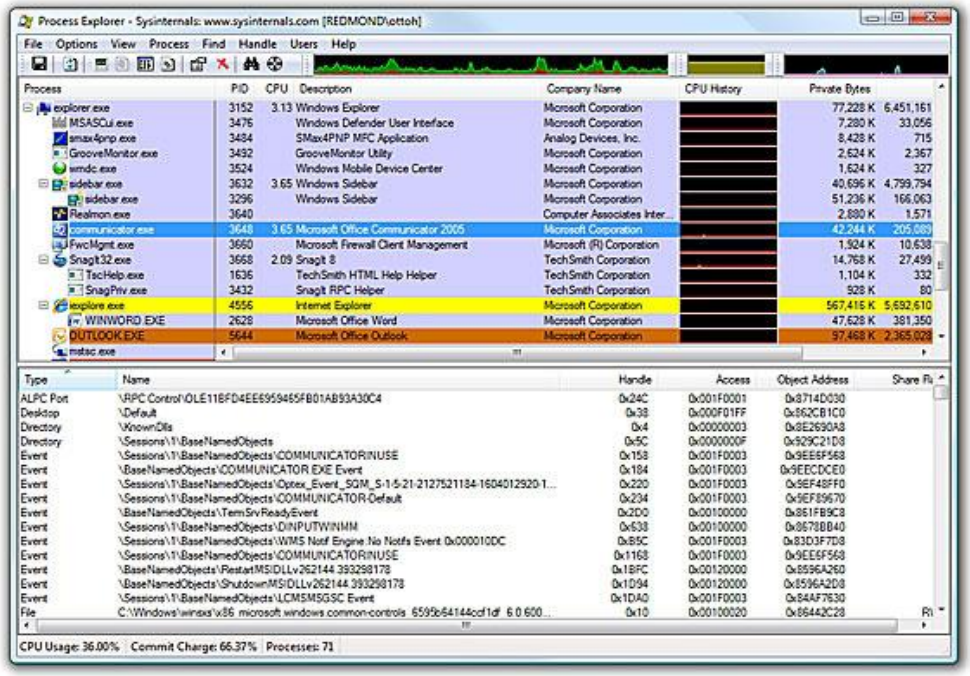
3.3.3 Windows SysInternals

Criada em 1996 por Mark Russinovich e Bryce Cogswell, acabou comprada pela Microsoft em julho de 2006. Trata-se de uma ferramenta avançada para manipulação e coleta de informações de sistemas Windows (GALVÃO, 2009).

Os principais componentes dessa ferramenta são o Process Explorer, Process Monitor, Autoruns, RootkitRevealer apresentado na figura 9, o TCPview, BgInfo e o Strings (GALVÃO, 2009).

O Process Explorer mostrado na figura 8 apresenta os processos abertos e quais bibliotecas DLL estão sendo carregadas. As informações são mostradas em duas sub-janelas. A janela superior mostra a lista dos processos ativos e na inferior o mapeamento de onde o processo foi carregado (RUSSINOVICH, 2011, tradução nossa).

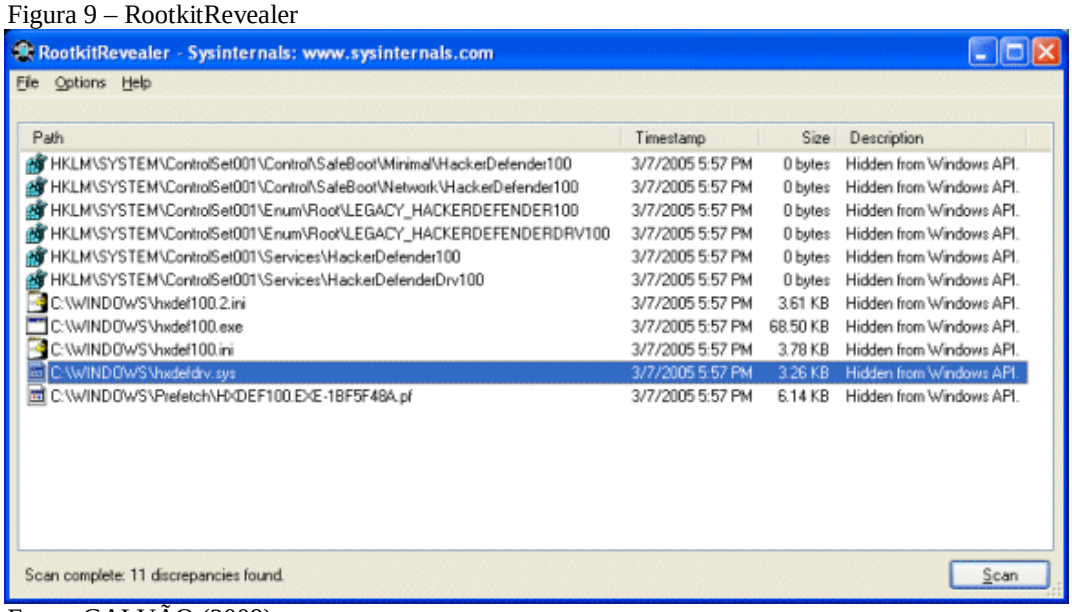
Figura 8 – Process Explorer (lista detalhada dos processos em execução e DLLs)



Fonte: GALVÃO (2009)

A ferramenta RootkitRevealer mostra na figura 9 uma lista com detecção de rootkits. O Autoruns lista os programas ou aplicativos iniciados automaticamente quando o Windows é iniciado. BGInfo mostra na área de trabalho informações como o nome do computador, endereço IP, versão do SO (RUSSINOVICH, 2011, tradução nossa).

Figura 9 – RootkitRevealer



Fonte: GALVÃO (2009)

3.3.4 Encase

Software desenvolvido pela Guidance, é considerada a ferramenta comercial mais conhecida e recomendada para perícia forense em ambiente Windows (GALVÃO, 2009).

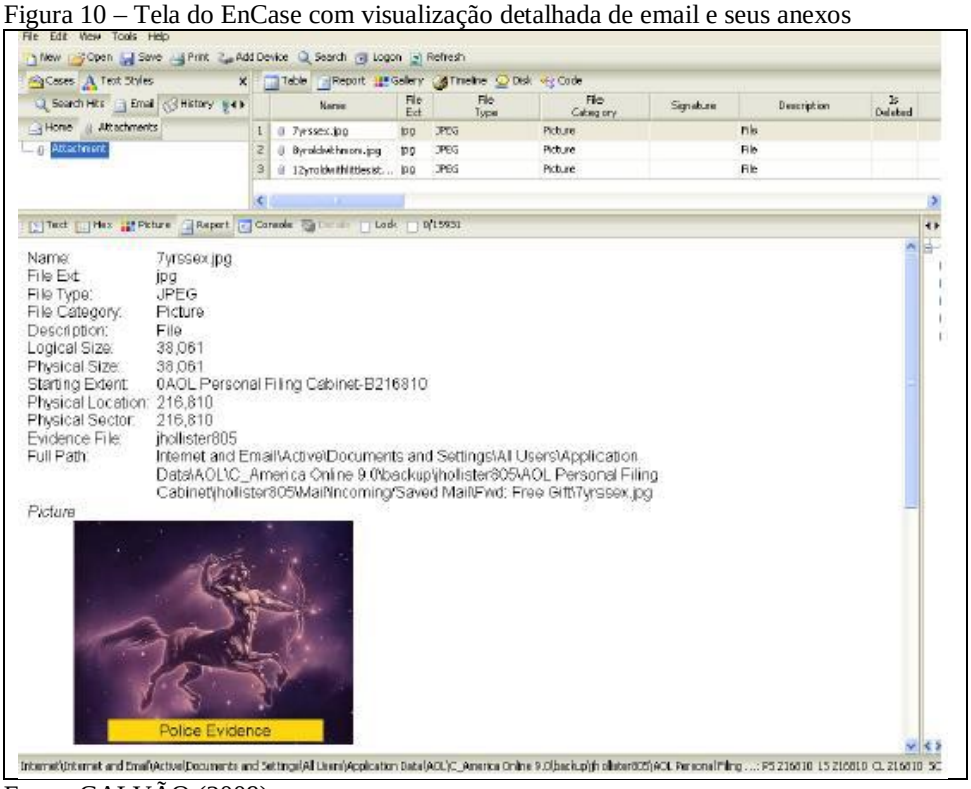
Além de auxiliar na recuperação de arquivos excluídos, padroniza laudos periciais, organiza um banco de dados com as evidências, faz o *encryption* (fornece senhas do arquivo) e o *decryption* (quebra as senhas dos arquivos) (VARGAS, 2011).

Ainda analisa hardwares, logs, formatos e tipos de e-mails e fornece a opção de manusear uma evidência sem danificá-la, entre outras características (VARGAS, 2011).

O EnCase pode ser usado em todas as fases da perícia porém por possui uma interface gráfica e funcionalidades nem tanto intuitivas, requer um treinamento mais específico (ELEUTÉRIO; MACHADO, 2011).

A figura 10 ilustra a verificação da ferramenta na caixa de entrada de email, utilizando métodos de busca e investigação da EnCase em e-mails.

Figura 10 – Tela do EnCase com visualização detalhada de email e seus anexos



Fonte: GALVÃO (2009)

3.3.5 Forense Toolkit (FTK)

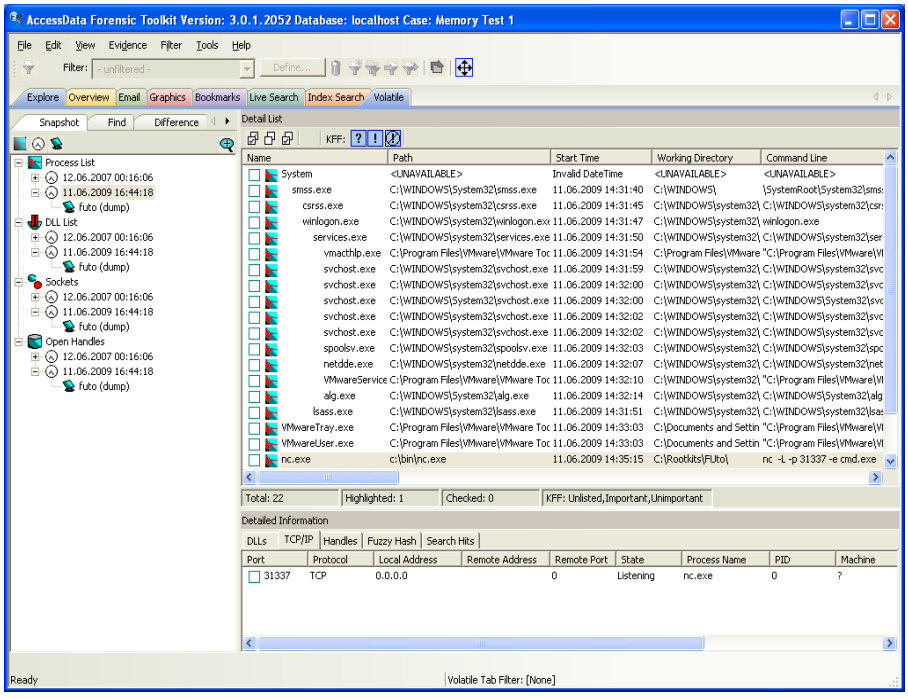
Produzido pela empresa Access Data, com versões específicas para sistema Windows ou Linux, possui as principais funcionalidades para realização da perícia forense em dispositivos de armazenamento de dados. Pode ser utilizado em todas as fases dos exames (ELEUTÉRIO; MACHADO, 2011).

Considerado concorrente do EnCase, mais fácil de operar mas, com menos recursos. Também é um software comercial porém, mais barato (GALVÃO, 2009).

A partir da versão 3 apresenta novas funcionalidades, interfaces gráficas e facilidades ao perito, tornando-se uma ferramenta mais estável e robusta, utilizando o banco de dados Oracle para organizar os dados internamente (ELEUTÉRIO; MACHADO, 2011).

Uma das novas funcionalidades adicionadas no FTK pela AccessData é a análise de memória mostrada na figura 11.

Figura 11 – Tela da ferramenta FTK efetuando análise de memória



Fonte: ACESSDATA (2011)

3.3.6 Autopsy

Autopsy Forensic Browser, desenvolvido por Brian Carrier, consiste em uma aplicação gráfica livre que utiliza um conjunto de ferramentas em linha de comando de forma

intuitiva e automatizada, permitindo pericias em variados tipos de sistemas de arquivos. Permite análise de dispositivos com sistema Windows ou Unix e sistemas de arquivos NTFS, FAT, UFS1/2 ou Ext2/3 (CARRIER, 2010).

É uma ferramenta orientada a casos e que possui diferentes modos de operação a serem selecionados de acordo com a necessidade de cada pericia (CARRIER, 2010).

3.3.7 Passware Kit Forensic

Fabricado pela empresa Passware Inc., considerada a principal fabricante mundial de software para recuperar senhas, sistemas de decodificação e especializada na descoberta de evidências eletrônicas (LEMKE, 2011).

Passware Kit Forensic possui a capacidade de recuperação de senhas de mais de 200 tipos de arquivos e imagens do disco rígido em sistema operacional Windows (7/2008/Vista/XP/2003/2000/NT). Pode distribuir esse processo de recuperação entre oito instâncias de cluster GPU da Amazon podendo atingir, dependendo da velocidade de conexão à Internet, uma velocidade de busca de 30.000 senhas por segundo (LEMKE, 2011).

3.3.8 Hardware

Além de softwares, o perito forense conta com hardwares específicos para auxílio na investigação, mostrado na figura 12, com o objetivo de melhorar o tempo de aquisição, a confiabilidade e a análise que podem ser lentos em sistemas convencionais.

Figura 12 – Duplicador de imagens Forensics SF-5000

Fonte: LOGICUBE (2011)

Empregada para fins ilícitos, buscando dificultar, invalidar ou até mesmo impossibilitar uma perícia forense ou então, com objetivos benéficos para proteção de dados e informações, aborda-se na sequência sobre a anti-forense computacional.

4 ANTI-FORENSE COMPUTACIONAL

Grande parte das empresas não gosta de investir em recursos de segurança pelo simples fato de não considerar necessário. A maioria apenas investe após já terem sido invadidas e consequentemente perderam muitos pontos com seus clientes (BARROS, 2007).

O número de incidentes na WEB possibilita verificar que o risco de segurança é um fator assumido desde o instante em que se disponibiliza um servidor com acesso à Internet (MELO, 2009).

Conhecendo o modus operandi dos atacantes, suas técnicas e ferramentas, é possível pensar em maneiras de proteger as informações com desenvolvimento tanto de ferramentas como técnicas concisas e eficientes (MELO, 2009).

As técnicas de invasão são cada vez mais sofisticadas e efetivas em sistemas computacionais. Assim, surgem as chamadas técnicas anti-forense com intuito de comprometer a disponibilidade de evidências em um processo forense (BOTERO; CAMERO; CANO, 2009, tradução nossa).

Pode-se utilizar assim estas técnicas para dificultar o acesso à informações sigilosas em dispositivos de armazenamento, mesmo por um perito forense (PERON; LEGARY, 2008, tradução nossa).

Anti-forense computacional são métodos utilizados para remover, ocultar, falsificar ou destruir evidências com o objetivo de dificultar resultados de perícias forenses (BARRETO, 2009).

Analisar separadamente as palavras que a definem talvez seja o melhor método de descrevê-la. O prefixo anti é definido como oposição ou ação contrária. Combinando os termos, define-se como métodos usados para impedir a ação da ciência na coleta de evidências que acabem na quebra de privacidade individual ou exposição de segredos corporativos (HARRIS, 2006).

Do mesmo modo como existem várias definições para anti-forense, diversos métodos foram propostos buscando garantir o sigilo das informações armazenadas. Uma das classificações destes métodos inclui: destruição, ocultação, eliminação da fonte e falsificação (WEBER; PEREIRA; GOLDANI, 2011).

Um de seus objetivos é bloquear diferentes tipos de análise alterando o modo como os dados são armazenados e organizados. Fazem parte das estratégias de anti-forense: a destruição de dados, ocultação de dados, transformação de dados, contracepção de dados, fabricação de dados e ataques de sistema de arquivo (BLUNDEN, 2009, tradução nossa).

Ocultar dados diminui a chance de que venham a ser encontrados, exigindo uma busca mais detalhada. Dependendo da ocultação, a descoberta do que está oculto pode levar anos ou nunca se descobrir (PAIVA, 2009).

A ocultação de dados pode ser aplicada na proteção de informações em situações em que deve ser garantida a possibilidade de recuperação dos dados. O acesso é limitado ao proprietário do conteúdo ou alguém que consiga descobrir a proteção ou algoritmo e chave que foram empregados (PERON; LEGARY, 2008, tradução nossa).

São várias as possibilidades de se proteger eletronicamente. A criptografia é o método mais conhecido, mas não é o único. Podemos também utilizar técnicas de saneamento de disco para remover dados confidenciais com segurança (BARRETO, 2009).

Outra técnica para prover segurança nos dados é a de esconder arquivos, seja ela por esteganografia ou a utilização de ferramentas que esconde os dados em alguns lugares no disco (BARRETO, 2009).

4.1 DISCOS RÍGIDOS

O disco rígido é a maior fonte de informações para uma perícia forense. Portanto, o disco não é simplesmente um conjunto de partições e sistemas de arquivos (MELO, 2009).

Quando um arquivo é apagado apenas sua referência é removida das estruturas de sistemas de arquivos. Tais dados permanecem no disco até que sejam sobrescritos por outros arquivos (MELO, 2009).

4.1.1 Sistema de arquivos

A função de um sistema de arquivos é garantir um método de organização para armazenar e recuperar dados a qualquer momento (CARRIER, 2005, tradução nossa).

Portanto o sistema de arquivos é a parte do sistema operacional responsável por organizar as informações do disco na forma de arquivos (MELO, 2009).

Para que os arquivos sejam posteriormente localizados no disco, são referenciados por flags[5], que estão organizadas dentro de uma tabela de alocação de arquivos (PAIVA, 2009).

[5] Flags são utilizados para otimizar as estruturas de dados, na medida que basta apenas um bit para ativar determinada característica.

4.1.2 Sistema de arquivos NTFS

O sistema de arquivos NTFS surge como uma necessidade de corrigir falhas de segurança, desempenho e confiabilidade que o sistema de arquivos FAT possuía (BOTERO; CAMERO; CANO, 2009, tradução nossa).

Desenvolvido pela Microsoft, é muito mais complexo que o FAT por sua maior robustez, provendo suporte para discos de grande capacidade (CARRIER, 2005, tradução nossa).

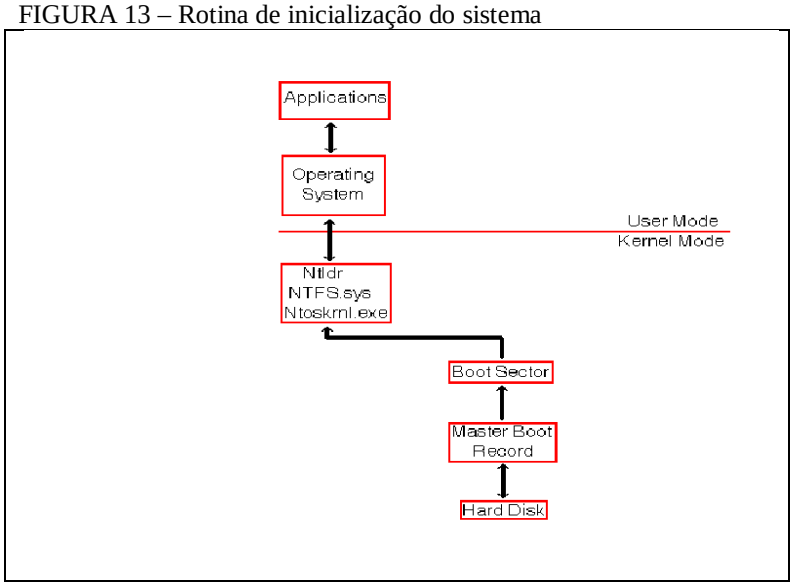
O controle da partição é mais sensível apresentando um bloco de informação de controle armazenado em arquivos desde a criação da partição, permitindo ao sistema operacional identificar e localizar qualquer arquivo de forma mais eficiente (BOTERO; CAMERO; CANO, 2009, tradução nossa).

Para o reconhecimento e funcionamento do sistema de arquivos este necessita o carregamento inicial do *Master Boot Record* (MBR) em memória DRAM. O MBR é um setor de inicialização de qualquer unidade de armazenamento, e está localizado de forma estratégica no primeiro setor do disco (PAIVA, 2009).

Todo sistema de arquivos possui um setor de inicialização (*boot*) para guardar informações específicas do próprio sistema de arquivos e permitir a inicialização do sistema operacional (CARRIER, 2005, tradução nossa).

Por meio da figura 13 podemos entender as rotinas de inicialização do sistema com NTFS (PAIVA, 2009).

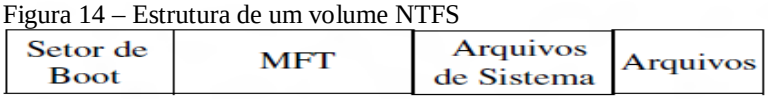
FIGURA 13 – Rotina de inicialização do sistema



Fonte: PAIVA (2009)

A formatação de uma partição NTFS resulta na criação da Master File Table (MTF) e outros arquivos de sistema. A MFT contém informações sobre todos os arquivos e diretórios da partição. Na figura 14 observa-se o posicionamento padrão da MFT (OLIVEIRA, 2001).

Figura 14 – Estrutura de um volume NTFS



Fonte: OLIVEIRA (2001)

Neste sistema existe um conjunto de arquivos contendo meta informações, usadas para implementar sua estrutura. Estes são mapeados nos primeiros registros da MFT, figura 15, incluindo ela própria (OLIVEIRA, 2001).

Figura 15 – Arquivos de Meta informação

File Name	MFT Record	Descrição
$MFT	0	Master File Table
$MftMirr	1	Cópia dos 16 primeiros registros da MFT
$LogFile	2	Arquivo de log das trasações efetuadas no disco
$Volume	3	Número de série do volume, data de criação e o *dirty flag*
$AttrDef	4	Definição dos atributos
$.	5	Diretório raiz do volume
$Bitmap	6	Representação do disco indicando que clusters estão sendo utilizados
$Boot	7	Setor de *boot* do volume
$BadClus	8	*Clusters* defeituosos
$Secure	9	Contém *security descriptors* únicos para todos os arquivos do volume
$Upcase	10	Mapeia caracteres minúsculos em seus correspondentes maiúsculos
$Extend	11	Usado por várias extensões opcionais, como quotas e reparse points
	12-15	Reservados para uso futuro.

Fonte: OLIVEIRA (2001)

Enfim, os objetivos atrás do NTFS eram trazer um sistema mais flexível, adaptável, com segurança e confiabilidade de arquivos. Espaços conhecidos como *slack area*, presentes neste sistema de arquivos, podem servir para ocultação de dados.

4.2 OCULTAÇÃO DE DADOS

São várias as maneiras de se proteger uma informação digital. A ocultação física é um caso especial de proteção dessas informações (WEBER; PEREIRA; GOLDANI, 2011).

A escrita de dados no espaço entre o fim lógico do arquivo e o final do *cluster*[6] onde se encontra (*slack area*) já é uma técnica bastante explorada, porém estes dados ocultos podem ser recuperados de maneira fácil por um editor de discos básico (WEE, 2006, tradução nossa).

Depende da arquitetura do sistema operacional a habilidade de ocultar informações em uma mídia. Se a área de armazenamento de um dispositivo é endereçada a nível de byte, não deveria existir espaço físico para ocultação de dados mas, essa não é a realidade (WEBER; PEREIRA; GOLDANI, 2011).

Como não existe um mapeamento 1:1 entre os ambientes físico e lógico, aparecem os espaços onde se podem ocultar dados (BERGHEL, 2007, tradução nossa).

Sendo que programas de aplicações e sistemas de arquivos reconhecem somente a estrutura lógica, várias implicações decorrem desse fato. Do ponto de vista forense é um grande problema, visto que as ferramentas atuais não conseguem recuperar todas as possibilidades de armazenamento de dados (WEBER; PEREIRA; GOLDANI, 2011).

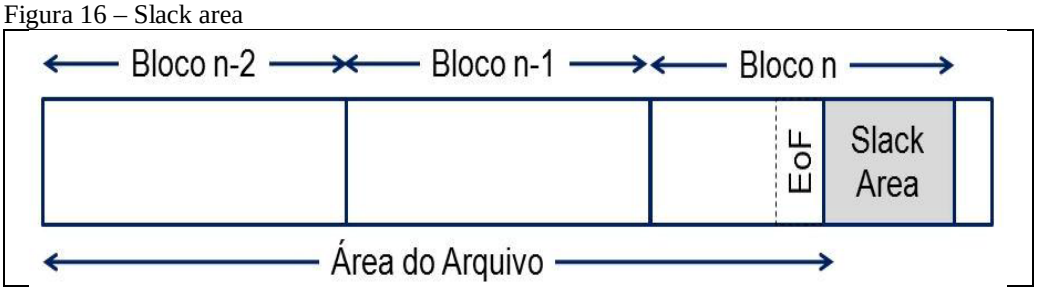
4.2.1 Slack area

No sistema de arquivos NTFS com tamanho do cluster de 4KB, um arquivo de 1KB ocupa a área de 4KB no dispositivo de armazenamento. Esta característica aponta a definição de *slack area*, demonstrada na figura 16 como: espaço existente entre o fim do arquivo e o fim do cluster onde ele está armazenado (WEBER; PEREIRA; GOLDANI, 2011).

Os sistemas de arquivos determinam o método de armazenamento e organização dos arquivos de forma a poder habilitar seu acesso quando necessário. Com base nessas características operacionais define-se a *slack area* como possível local para ocultar informações (BERGHEL, 2007, tradução nossa).

[6] *Cluster* é a menor parcela do HD que pode ser alocada para armazenar um arquivo.

Figura 16 – Slack area



Fonte: WEBER; PEREIRA; GOLDANI (2011)

Com os programas certos, é possível utilizar este espaço para proteção de dados. Como as informações são armazenadas em blocos inutilizados, consegue-se despistar invasores mesmo que utilizem a maior parte das ferramentas de análise forense (SILVA, 2003).

4.3 CRIPTOGRAFIA

Uma técnica de criptografia é empregada para esconder o número do cartão de crédito ou os dados bancários quando se utiliza *home banking* (MADEIRA et al, 2007).

A criptografia é uma técnica que visa transformar uma informação na sua forma original em outra ilegível. Esse processo é executado para que somente o detentor da chave criptográfica consiga realizar o processo inverso e ler o arquivo original (ELEUTÉRIO; MACHADO, 2011).

Por meio da criptografia pode-se garantir (MADEIRA et al, 2007):

a) confidencialidade: garante que os dados permaneçam privados;
b) integridade de dados: proteção de dados contra alteração acidental ou deliberada (mal-intencionada);
c) autenticação: garante que os dados tenham origem de uma parte específica. Os certificados digitais fornecem a autenticação.

Com a criptografia de arquivos o acesso não-autorizado torna-se complicado. Essa dificuldade pode ser medida pela complexidade do algoritmo de criptografia utilizado (BARRETO, 2009).

A criptografia pode ser considerada a melhor técnica anti-forense para ocultação de evidências. A quebra da criptografia pode levar anos dependendo da chave, do algoritmo e do poder computacional empregado (PAIVA, 2009).

O objetivo principal dos algoritmos de criptografia é a geração de chaves cada vez mais complexas. Em virtude do rápido avanço na área de hardware, muitos desses algoritmos já são considerados obsoletos (BARRETO, 2009).

Por este motivo, matemáticos e profissionais da área de computação estudam e inventam algoritmos complexos no intuito de proteger a informação e dificultar o processo inverso, buscando mecanismos cada vez mais seguros (ELEUTÉRIO; MACHADO, 2011).

Como exemplos de algoritmos em uso na atualidade pode-se citar o AES, TripleDES, Blowfish e RSA (SAMMONS, 2012, tradução nossa).

Uma chave com comprimento n bits terá 2^n chaves possíveis, então uma chave de 40 bits possuirá 2^{40} (um trilhão) de chaves possíveis (BARRETO, 2009).

Uma máquina com frequência de processamento de 1600 MHz gastaria 1.713.698 anos para quebrar uma chave criptográfica de 56 bits. Atualmente já existem chaves de até 2048 bits (PAIVA, 2009).

A criptografia, portanto, é capaz de inviabilizar uma perícia ou um ataque desde que utilizadas chaves criptográficas a partir de 128 bits e que o sistema seja desligado após qualquer criptografia para que as chaves sejam volatizadas na DRAM (PAIVA, 2009).

4.3.1 TrueCrypt

TrueCrypt é um software código aberto, gratuito, capaz de executar criptografia completa de disco. Utiliza o método *on-the-fly* em que os dados são criptografados e descriptografados de forma automática à medida que são salvos e abertos (SAMMONS, 2012, tradução nossa).

Possui compatibilidade com sistemas Windows, Mac e Linux. Pode fornecer criptografia múltipla incluindo AES, Serpent, Twofish ou alguma combinação destes (SAMMONS, 2012, tradução nossa).

4.3.2 Bitlocker

Disponível apenas no Windows 7, pode criptografar um disco rígido inteiro ou um dispositivo de armazenamento USB. Normalmente, funciona em conjunto com o hardware TPM, porém, pode ser configurado para trabalhar sem este. O TPM é um circuito integrado na placa-mãe que fornece funções criptográficas (SAMMONS, 2012, tradução nossa).

A criptografia Bitlocker é bastante robusta, usando AES com chave de 128 bits em combinação com outro algoritmo, o Elephant Diffuser, tornando duvidosa a decodificação sem a chave (SAMMONS, 2012, tradução nossa).

4.4 ESTEGANOGRAFIA

São técnicas que consistem em ocultar uma mensagem dentro de outra. A criptografia codifica o conteúdo, a esteganografia camufla uma mensagem em outra (ELEUTÉRIO; MACHADO, 2011).

Na atualidade são várias e bastante complexas as técnicas, podendo ser aplicadas a inúmeros tipos de arquivos, inclusive imagens e vídeos (ELEUTÉRIO; MACHADO, 2011).

Em imagens as informações podem ser ocultadas por inserção no bit menos significativo (LSB); máscara e filtragem; algoritmos e transformações (BARRETO, 2009).

Já em textos utiliza-se a codificação por deslocamento de linhas verticalmente, codificação por deslocamento de palavra em textos justificados e a codificação por deslocamento do caractere de fim de linha (BARRETO, 2009).

Em se tratando de áudio os métodos são a codificação do bit menos significativo e a ocultação de dados no eco do áudio (BARRETO, 2009).

Existem dois tipos de ataques contra a esteganografia que são a detecção e a destruição. O importante é evitar que o objeto esteganografado seja detectado e então destruído ou estego-analisado (RIBEIRO; CHICARELLI; ALBUQUERQUE, 2008).

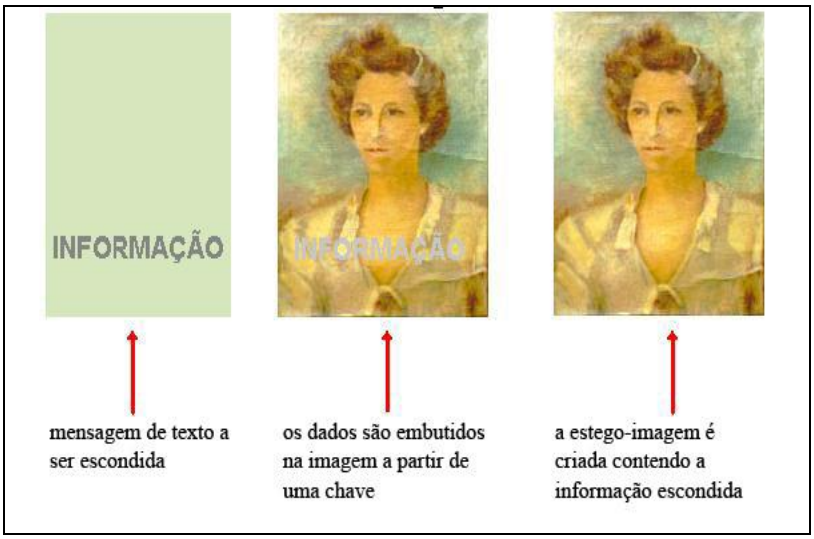
A esteganografia também é utilizada através do uso de softwares. Observando a figura 17 é possível acreditar que um usuário não espere encontrar informações ocultas pois não deve perceber diferença entre as imagens.

O funcionamento se dá através de quatro componentes. O dado embutido (embedded data) é a informação que alguém deseja enviar em segredo (OHASHI et al, 2006).

Este dado fica escondido em uma mensagem aparentemente inocente chamada recipiente (container), que pode ser um arquivo de áudio, vídeo, texto, figuras, formando o estego-objeto, um arquivo com uma mensagem oculta (OHASHI et al, 2006).

Uma estego-key (*stego-key*) ou senha é a chave usada para controlar todo o processo de ocultamento. Somente quem a conhece consegue recuperar o dado embutido ou restringir sua detecção (ROCHA et al, 2004).

Figura 17 – Informação Esteganografada



Fonte: RIBEIRO; CHICARELLI; ALBUQUERQUE (2008).

Se bem empregadas, as técnicas fornecem meios eficazes e eficientes de proteção digital. A associação de criptografia e esteganografia como solução implementada configura-se como opção para manutenção da confidencialidade de informações (ROCHA et al, 2004).

A preocupação com a esteganografia está baseada na dificuldade ou mesmo impossibilidade de detectá-la. Ainda que descoberta, o que é muito difícil, para extrair seu conteúdo deve-se conhecer a aplicação e senha utilizados para criá-la (SAMMONS, 2012, tradução nossa).

4.4.1 JPHS

JPHS é um software gratuito para esteganografia. Pode ser utilizado para esconder arquivos de áudio, texto, imagem e vídeo, usando imagens JPEG como base (BEZDZIECKI, 2009, tradução nossa).

O criador do JPHS recomenda que o tamanho físico do arquivo a se esteganografar seja algo em torno de 10% do tamanho da imagem jpeg original (BEZDZIECKI, 2009, tradução nossa).

5 TRABALHOS CORRELATOS

Neste capítulo são apresentados os trabalhos relacionados mais importantes que serviram de base para este projeto, com o objetivo de transmitir melhor entendimento das propostas apresentadas.

5.1 UTILIZAÇÃO DE TÉCNICAS ANTI-FORENSES PARA GARANTIR A CONFIDENCIALIDADE

Barreto (2009) em seu TCC pela Pontifícia Universidade Católica do Paraná, apresenta ao leitor algumas técnicas anti-forense. Tais técnicas foram desenvolvidas para esconder um indivíduo em atividades ilegais, porém, este documento tem como objetivo apresentar ao leitor a utilização dessas para proteger e manter informações confidenciais. Foram abordados alguns conceitos de saneamento de disco (remoção segura de arquivos), criptografia de arquivos; esconder informações em arquivos multimídias (esteganografia) e em espaços ocultos de discos.

Como conclusão o autor definiu que sempre se faz necessário buscar novas técnicas para assegurar a confidencialidade dos dados.

5.2 PRÁTICAS ANTI-FORENSE: UM ESTUDO DE SEUS IMPACTOS NA FORENSE COMPUTACIONAL

Esta monografia apresentada por Paiva (2009) na pós-graduação em segurança da informação da Faculdade de Tecnologia IBRATEC de João Pessoa, mostra que o crescimento desordenado do uso de computadores com procedimentos de segurança pouco disseminados e com a ausência de regulamentação das leis de uso do computador, promove a criatividade para crimes cibernéticos.

Diante do aspecto da crescente criminalidade cibernética, surgem os peritos forenses computacionais que tem como função, levantar todo histórico de uso dos computadores a procura de evidências que levem ao possível culpado pelos crimes.

Em contra partida, os criminosos estudam a forma de como os peritos forenses trabalham e desenvolvem as técnicas anti-forense para dificultar ou inviabilizar o trabalho do perito, além de causar danos sem precedentes em empresas e/ou pessoas.

Este trabalho apresenta de um modo geral as aplicações práticas das técnicas anti-forense mostrando os impactos de cada técnica em um cenário de análise forense, como forma de alerta emergencial para estudos futuros de como se precaver desses tipos de ataque.

5.3 ANÁLISE DO USO DE ANTIFORENSE DIGITAL PARA DESTRUIÇÃO DE DADOS

Weber, Pereira e Goldani (2011) mostram que a atividade anti-forense contempla a esterilização ou ocultação de arquivos para garantir a segurança e privacidade de seu conteúdo, e as técnicas e recursos desenvolvidos para esta finalidade podem ser utilizados para sonegar evidências de crimes, que podem ser obtidas a partir de discos rígidos. Quando a justiça decide apreender um equipamento para realizar uma pericia "post mortem", cabe ao perito forense utilizar o seu conhecimento e as ferramentas disponíveis para recuperar evidências, que podem ter sido destruídas ou estarem ocultas em discos rígidos.

O escopo deste trabalho foi descrever características e propriedades de dispositivos de armazenamento que possam ser utilizadas por procedimentos anti-forense com o objetivo de ocultar ou destruir informações.

5.4 ESTEGANOGRAFIA

Trabalho apresentado por Ohashi et al. na Universidade Católica de Brasília.

Com o rápido e crescente avanço de tecnologia de comunicações, formou-se um novo campo de batalha, a internet, onde não existem objetivos concretos, nem se sabe quem realmente é inimigo, muito menos os tipos de armas utilizadas, técnicas aplicadas e o tamanho dos danos que podem ser causados. Por estes motivos, a chamada guerra da informação é o tipo de batalha mais temida atualmente.

Uma das técnicas mais eficazes utilizadas na guerra da informação é a esteganografia. Tal técnica consiste na ocultação de informações em diversos meios, como imagens, textos, áudio e vídeo.

A esteganografia pode ser usada para várias razões, como no roubo de dados ou para comunicar uma guerra.

A conclusão obtida foi que todas as formas de se preservar devem ser consideradas, pois sempre haverá alguém com tempo e talento suficiente para conseguir transpô-las. Contudo é necessário muita tática de defesa, obrigatoriamente contra os ataques mais conhecidos, mas também é imprescindível estudar e entender outras tecnologias, como a

esteganografia, que desde antes de Cristo é utilizada, mas que quase ninguém conhece sua forma digital (OHASHI et al, 2006).

5.5 CRIPTOGRAFIA DE DISCO: GARANTINDO A SEGURANÇA DAS INFORMAÇÕES

Monografia de pós-graduação em segurança de redes nas Faculdades Integradas Barros Melo (AESO).

Frequentemente, uma técnica de criptografia conhecida como RSA é usada para esconder o número do seu cartão de crédito ou os seus dados bancários em quanto faz "*home banking*". Com a RSA temos duas chaves, uma pública para esconder suas informações e outra privada para revelá-las.

O uso de algoritmos de criptografia está se tornando cada vez mais comum. Hoje em dia, a segurança de rede e segurança física não são os maiores problemas e sim pessoas que de alguma forma têm acesso ao seu computador.

Imagine que você faz parte de uma empresa, a qual disponibiliza um notebook para suas atividades e você possui informações sigilosas nele. Durante uma viagem, você é assaltado e fica sem seu notebook, o assaltante abre seus arquivos, identifica sua empresa e decide vender as informações para seu concorrente. Qual será o impacto dessa perda para a empresa ? Qual o valor das informações perdidas ?

Para evitar esse tipo de perda, são usadas técnicas de criptografia de forma a garantir que a CIA (Confiabilidade, integridade de disponibilidade) seja garantida.

Poderíamos encriptar toda a partição onde as informações da empresa estariam guardadas, tornando-as inúteis para alguém que não possua a chave para decriptar as informações.

Existem diversos algoritmos de criptografia disponíveis. Ao longo desse trabalho, descreve-se os mais comumente utilizados em corporações e governos mundiais além de mostrar como é possível encriptar um disco rígido em sistemas operacionais Windows e Linux (MADEIRA et al, 2007).

6 PROTEÇÃO DE DADOS EM DISPOSITIVOS DE ARMAZENAMENTO

Um incidente de segurança em uma empresa com vazamento de informações sigilosas, por exemplo, pode causar impacto negativo nas finanças da organização, perda da confiabilidade de clientes e ainda prejudicar o relacionamento com parceiros e fornecedores.

Técnicas de anti-forense computacional são utilizadas de forma benéfica, para proteger a confidencialidade desses dados e informações.

Com a disponibilidade atual de ferramentas forenses e com a facilidade em dominar seu uso, estas podem ser empregadas com a finalidade única de quebrar o sigilo de informações pessoais e corporativas.

Baseado nessa realidade, foram utilizadas ferramentas que aplicam as técnicas anti-forense de criptografia e esteganografia para proteção de dados e/ou informações sob sistema de arquivos NTFS e posteriormente, aplicação das ferramentas de análise forense.

Em seguida foi efetuada uma análise e descrição dos resultados alcançados.

6.1 METODOLOGIA

A metodologia empregada na elaboração deste trabalho iniciou com um levantamento bibliográfico dos assuntos a serem tratados.

Este processo forneceu subsidio para estudar e descrever ferramentas e técnicas da computação forense e anti-forense computacional.

Estudo das ferramentas Forense Tool Kit, EnCase, Autopsy e Passware Kit Forensic, para sua aplicação em dispositivos de armazenamento com sistema de arquivos NTFS.

A seguir, estudo de ferramentas e técnicas anti-forense no dispositivo utilizado, um *pendrive* com capacidade de um Gigabyte. A capacidade de armazenamento reduzida deste dispositivo foi o critério para sua seleção. Assim, conseguiu-se uma redução no tempo de recuperação das imagens e criptografia durante a pesquisa.

Criptografia e esteganografia foram as técnicas escolhidas e aplicadas por meio dos softwares TrueCrypt e BitLocker para criptografia e JPHS, esteganografia. Dentre as técnicas anti-forense, são as que melhor se enquadram no contexto desta pesquisa, a proteção de dados e informações.

Efetuou-se inicialmente uma análise do dispositivo sem proteção de seu conteúdo. Na sequência utilizou-se as mesmas ferramentas forenses, porém, com criptografia completa do *pendrive*.

Finalmente, efetuou-se a leitura e descrição dos resultados obtidos.

6.2 APRESENTAÇÃO, ANÁLISE DOS DADOS E RESULTADOS

A realização de uma perícia forense computacional segundo a metodologia SOP envolve sete fases: coleta da prova, preparação do equipamento, imagem forense (aquisição), exame/análise, documentação relatórios e revisão. Sendo o objetivo deste trabalho a proteção da confidencialidade das informações em um dispositivo de armazenamento, somente as fases de aquisição e exame/análise foram empregadas.

As ferramentas periciais, Encase, FTK, Passware Kit Forensic e uma ferramenta gratuita e de código aberto, o Autopsy, desenvolvida originalmente em março de 2001 por Brian Carrier possuindo suporte para as principais plataformas, foram selecionadas para efetivação deste trabalho.

6.2.1 Análise e resultados do dispositivo sem proteção anti-forense

No primeiro estágio de desenvolvimento, arquivos foram inseridos num dispositivo de armazenamento USB formatado com sistema de arquivos NTFS. Alguns destes dados foram selecionados e deletados propositalmente. Ferramentas anti-forense não foram utilizadas neste momento.

Existem várias maneiras de aquisição ou criação de uma imagem forense.

6.2.1.1 Criação da imagem

A ferramenta FTKImager nos oferece quatro opções: imagem não processada, *Smart*, *Expert Witness*(E01) ou *Advanced Forensic Format* (AFF).

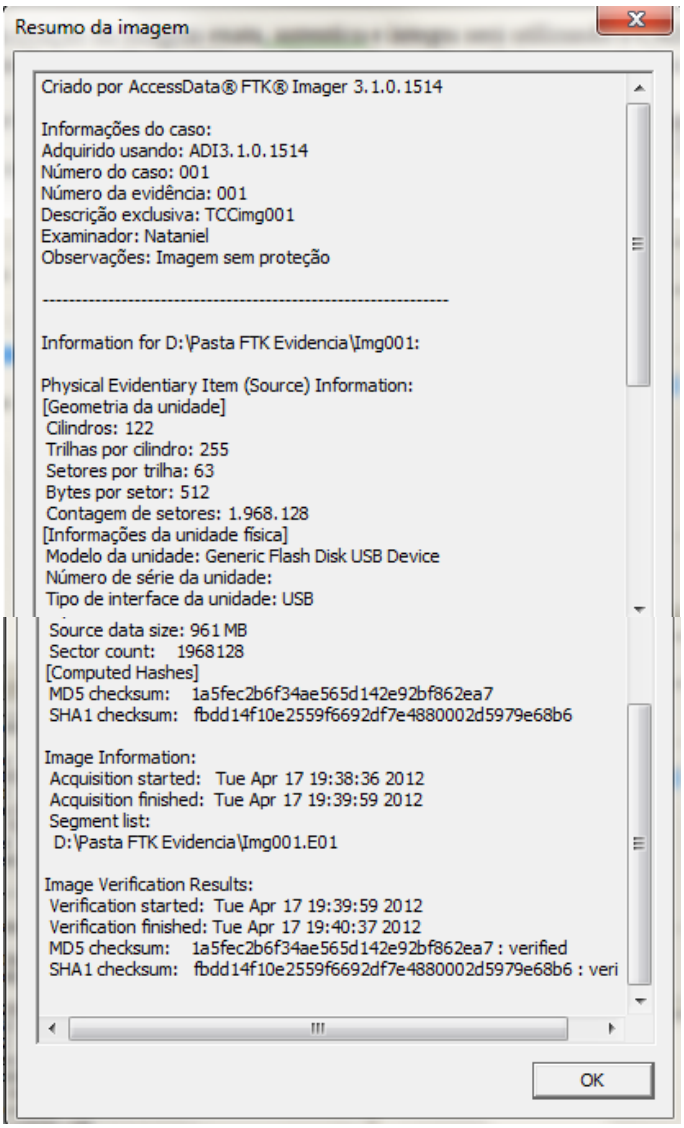
A imagem não processada está disponível em utilitários tanto para Windows como para Linux porém, os arquivos são muito grandes, não há compactação. Além disso, não é possível a adição de dados na investigação e algumas operações são mais lentas devido ao grande tamanho.

O padrão Smart foi desenvolvido para sistemas Linux pelos criadores do padrão Expert Witness.

Na tentativa de padronização de formatos foi criado o *Advanced Forensic Format* o qual, utiliza compactação, tratamento de erros e oferece bibliotecas para adaptação.

A escolha recaiu no padrão *Expert Witness* (E01) por ser proprietário do Encase e permitir compactação, sem perdas. A figura 18 mostra o resumo da criação da imagem.

Figura 18 – Resumo da Criação da Imagem



Fonte: Do autor.

6.2.1.2 Análise dos dados

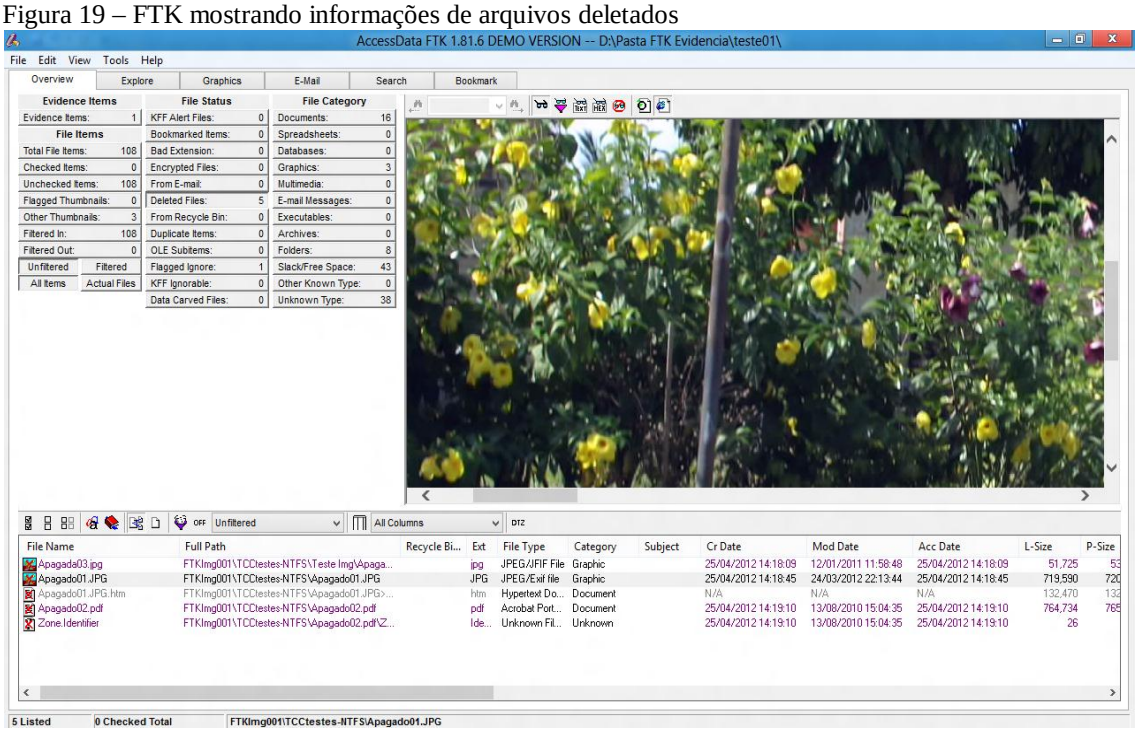
Criada a imagem do dispositivo, iniciou-se a análise da mesma empregando as ferramentas forenses.

6.2.1.2.1 Análise utilizando a ferramenta Forense Tool Kit (FTK)

Executando a ferramenta em sua versão 1.81.6, cria-se o caso e adiciona-se a imagem criada ao mesmo. Ao término da adição temos como resultado a visualização completa de todos os arquivos que se encontravam no dispositivo, inclusive os deletados.

Várias informações a respeito dos dados podem ser obtidas, figura 19, como data e horário da criação, acesso ao arquivo, modificações, quando foram excluídos.

Figura 19 – FTK mostrando informações de arquivos deletados



Fonte: Do autor.

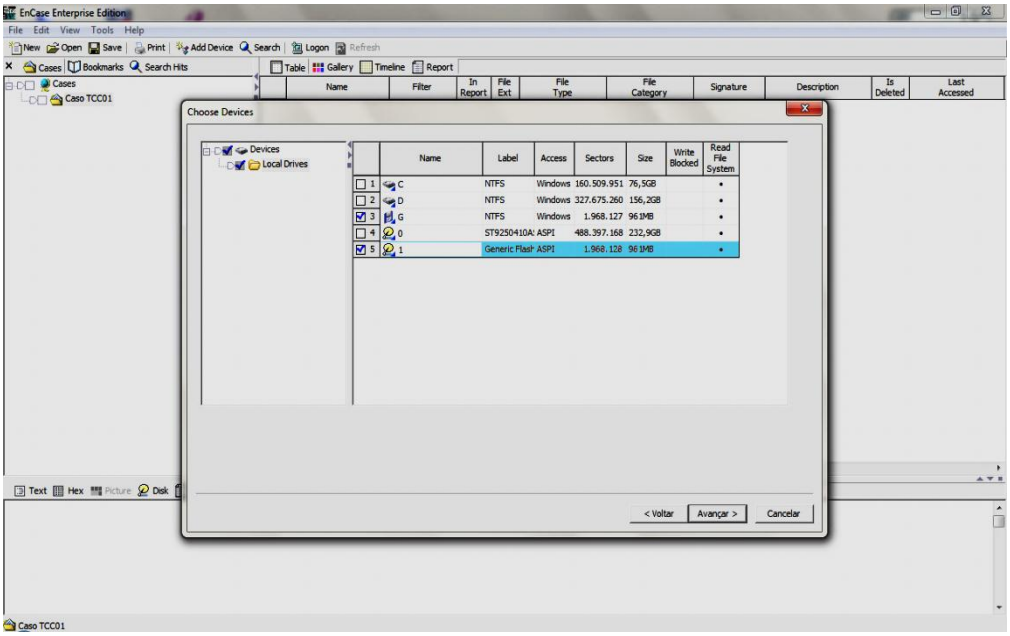
6.2.1.2.2 Análise utilizando a ferramenta Encase

A versão 6.1 do software Encase foi utilizada. Um novo caso deve ser criado e então adicionado o dispositivo para análise ao mesmo. Deve-se selecionar a unidade física e a unidade virtual do *pendrive*, conforme figura 20.

A mesma eficácia e resultados obtidos com a ferramenta FTK também puderam ser observadas no Encase. Todos os arquivos inclusive aqueles que haviam sido excluídos estavam disponíveis para recuperação.

A ferramenta possibilita a verificação da ocorrência de uma palavra chave no conteúdo do dispositivo, em endereços de e-mail e endereços web.

Figura 20 – Adicionando um dispositivo ao caso

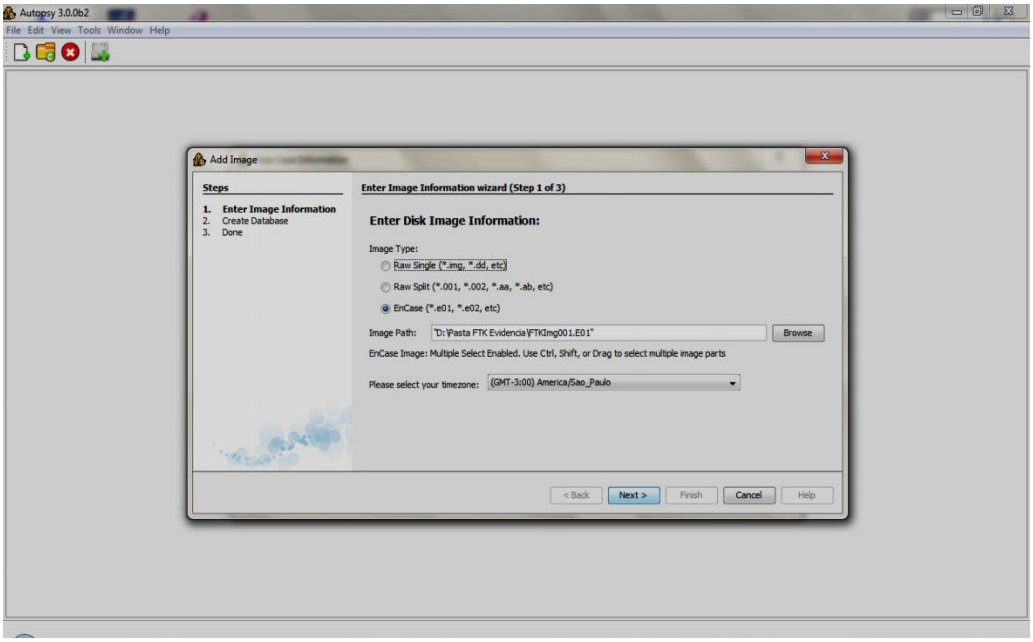


Fonte: Do autor.

6.2.1.2.3 Análise utilizando a ferramenta Autopsy

A ferramenta forense Autopsy não requer instalação, apenas descompactar o arquivo para um local de destino. Ao executá-la também cria-se um caso, figura 21, para adição da imagem do dispositivo. Utilizou-se a versão 3.0, a mais recente do software.

Figura 21 – Adição de imagem ao caso na ferramenta Autopsy



Fonte: Do autor.

A análise trouxe os mesmos resultados já encontrados com as ferramentas anteriores. Foram encontrados todos os arquivos no dispositivo, mesmo os deletados. Nas três ferramentas é possível recuperar estes arquivos e salvá-los em disco.

Deve-se considerar a possibilidade de utilização de softwares como o File Shredder, que permite escolher entre cinco algoritmos para sobrescrever o espaço anteriormente utilizado pelo arquivo excluído, impedindo assim sua recuperação.

6.2.2 Análise e resultados do dispositivo utilizando criptografia

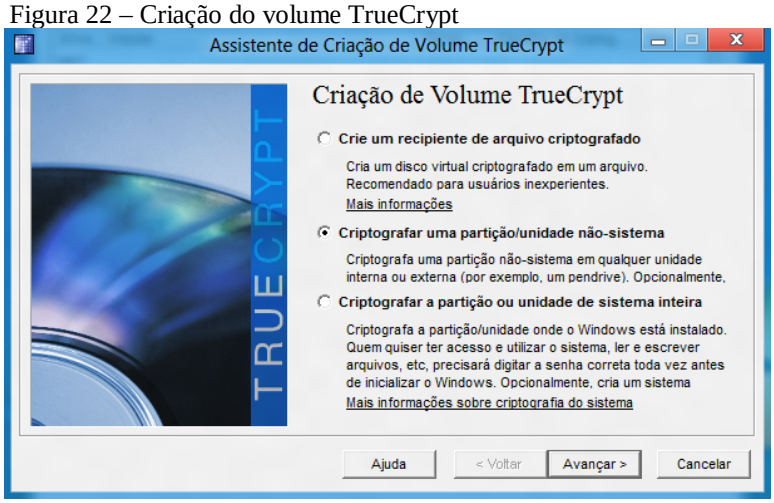
Neste estágio, foi efetuada a criptografia completa do dispositivo de armazenamento USB contendo os mesmos dados da análise anterior. Utilizou-se dois softwares de criptografia, o TrueCrypt e o Bitlocker. Estas ferramentas não oferecem a possibilidade de encriptar somente parte dos arquivos do dispositivo.

Obteve-se a imagem do dispositivo criptografado, padrão Expert Witness (E01), utilizando o software FTKImager, mesmo procedimento da análise sem utilização de ferramentas anti-forenses.

6.2.2.1 Criptografia utilizando o software TrueCrypt

O software TrueCrypt possui suporte ao idioma português-BR. Inicia-se com a criação do volume TrueCrypt. Para este procedimento foi escolhida a opção para criptografar uma partição/unidade não sistema, ou seja, unidade sem sistema operacional instalado, figura 22.

Figura 22 – Criação do volume TrueCrypt



Fonte: Do autor.

A etapa seguinte é a escolha das opções de criptografia. Como algoritmo de criptografia foi selecionado o AES, cifra aprovada para ser usada pelos departamentos e agências do governo dos Estados Unidos para proteger suas informações mais confidenciais. A chave é de 256 bits, bloco de 128 bits, 14 ciclos (AES-256).

Whirlpool foi escolhido aleatoriamente como algoritmo de *hash*, com tamanho de saída de 512 bits. O TrueCrypt utiliza a terceira versão deste algoritmo, adotada pela Organização Internacional de Normalização em 2004. Outros algoritmos de *hash* disponibilizados para seleção pelo software são o SHA-512 e o RIPEMD-160.

O algoritmo SHA-512, assim como o Whirlpool, apresenta tamanho de saída de 512 bits enquanto no caso do RIPEMD-160, tamanho de 160 bits.

Após escolher os algoritmos é requisitada a criação da chave (senha). Na tela o software apresenta a sugestão para uma mistura de letras maiúscula e minúsculas, números e caracteres especiais com no mínimo vinte e até sessenta e quatro caracteres.

Existem softwares e sites com ferramentas para auxiliar na criação de uma boa senha.

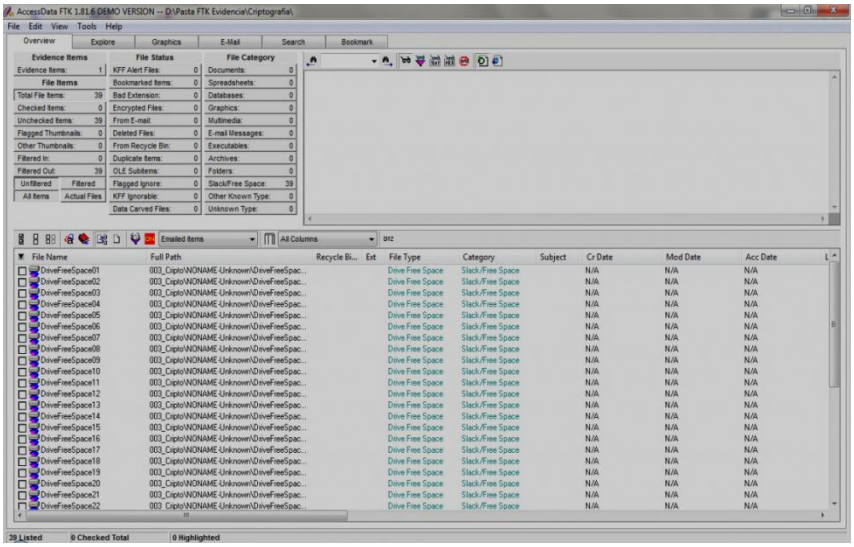
O tempo de criptografia utilizando um *pendrive* com capacidade de armazenamento de um Gigabyte e sistema de arquivos NTFS foi de aproximadamente trinta e três minutos.

6.2.2.1.1 Análise e resultado do dispositivo criptografado com TrueCrypt

Inicialmente foi criada uma nova imagem do dispositivo utilizando o software FTKImager, imagem padrão Expert Witness(E01).

A primeira ferramenta utilizada para análise foi o FTK(Forense Tool Kit), e a mesma não obteve sucesso em trazer os dados contidos no *pendrive*, conforme pode-se visualizar na figura 23.

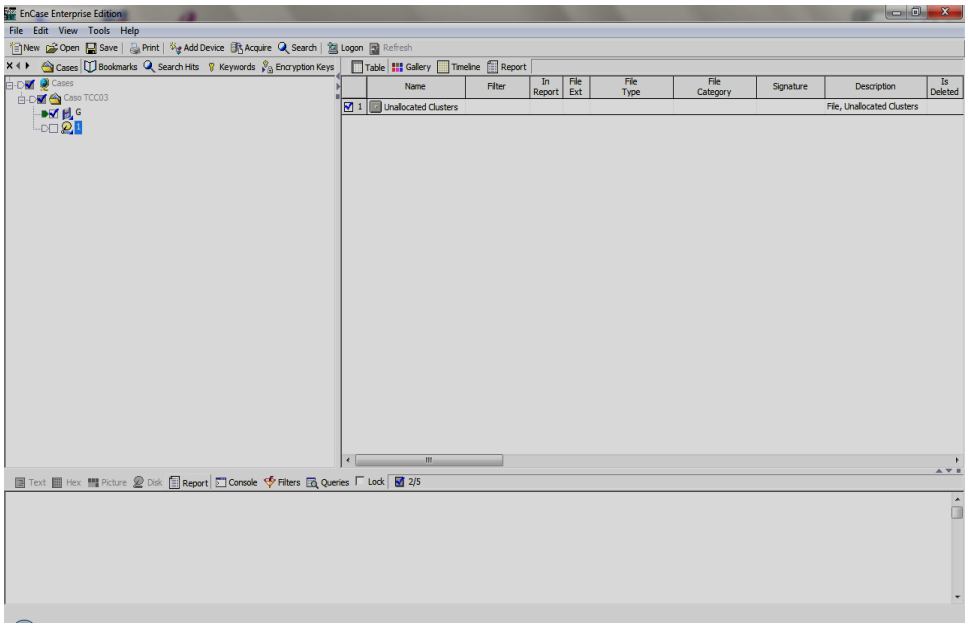
Figura 23 – Resultado de análise com dispositivo criptografado utilizando FTK



Fonte: Do autor.

O Encase, segunda ferramenta empregada também teve como resultado o insucesso na tentativa de recuperação dos dados presentes no dispositivo, identificando os clusters como não-alocados, figura 24.

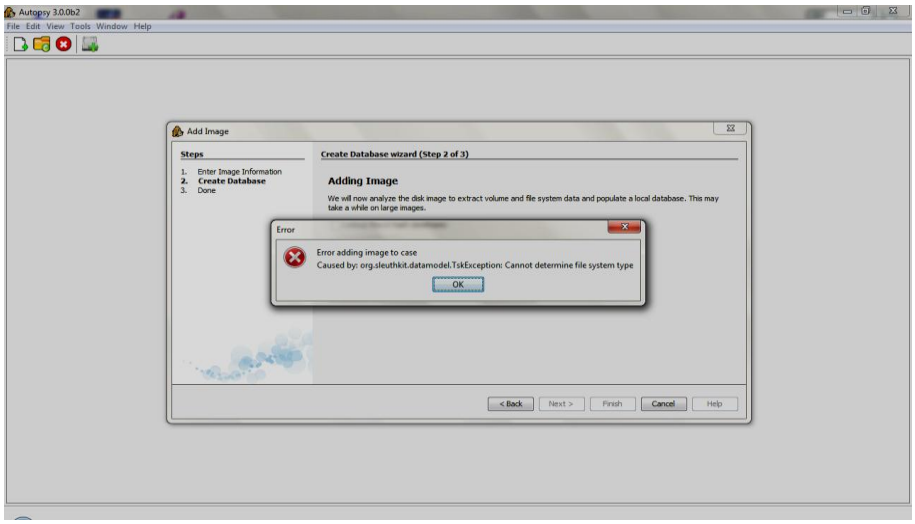
Figura 24 – Resultado de análise do dispositivo criptografado utilizando Encase



Fonte: Do autor.

Finalizando as análises com criptografia, ao fazer a inserção da imagem do dispositivo ao caso, na ferramenta Autopsy, uma tela de erro era apresentada mostrando que não foi possível determinar o tipo de arquivos de sistema, figura 25.

Figura 25 - Resultado de análise do dispositivo criptografado utilizando Autopsy



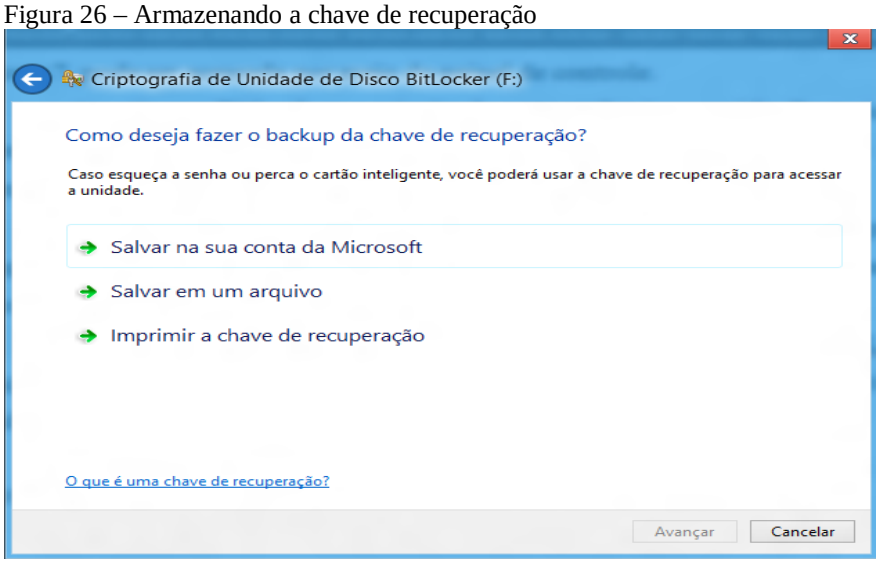
Fonte: Do autor.

6.2.2.2 Criptografia utilizando BitLocker

A ferramenta de criptografia de disco BitLocker, presente no sistema operacional Windows 7, pode ser acessada por meio do painel de controle.

Ao ativar o BitLocker, a criação de uma senha é requerida. Posteriormente uma tela para salvar em arquivo ou imprimir a chave de recuperação de acesso à unidade é apresentada, figura 26.

Figura 26 – Armazenando a chave de recuperação

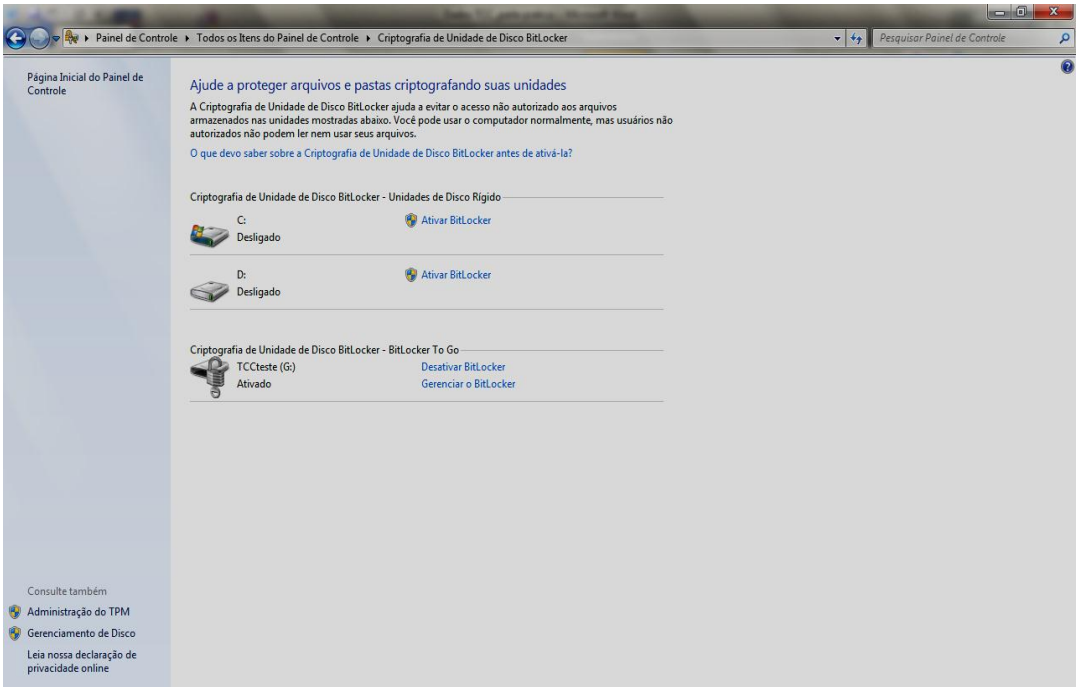


Fonte: Do autor.

Efetivando a impressão ou o salvamento da chave uma nova tela para iniciar a criptografia é mostrada. A criptografia da mesma unidade utilizada com o software TrueCrypt mostrou-se mais rápida, em torno de oito minutos.

Ao acessar o painel de controle, criptografia de unidade de disco BitLocker após a execução dos passos anteriores pode-se visualizar que a criptografia está ativada para a unidade, figura 27.

Figura 27 – Unidade com criptografia BitLocker



Fonte: Do autor.

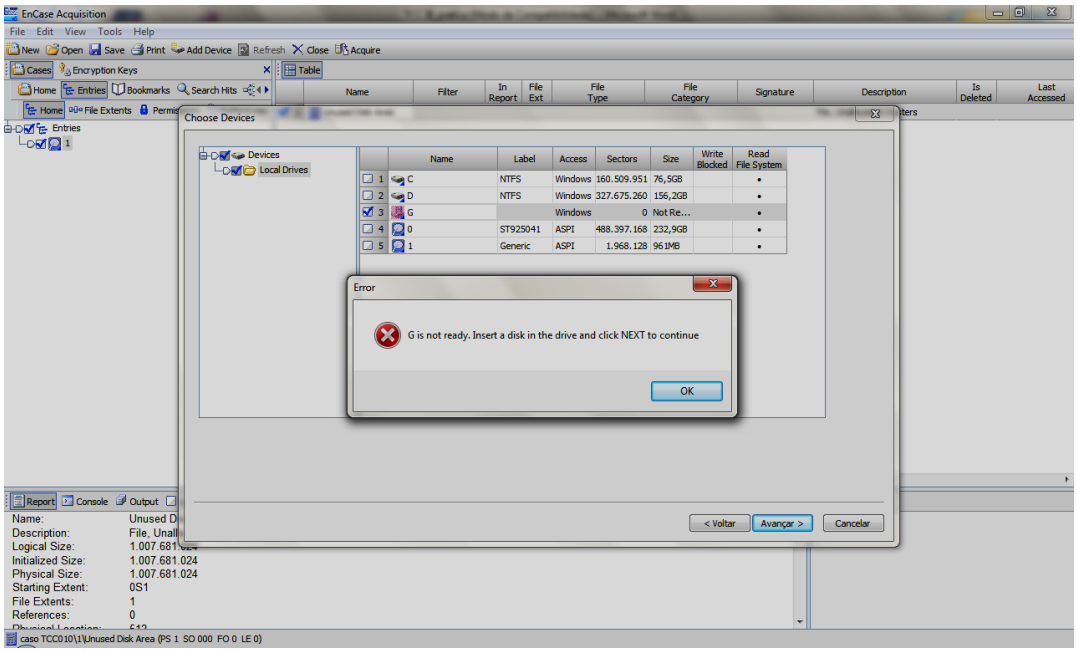
6.2.2.2.1 Análise e resultado do dispositivo criptografado com BitLocker

Seguindo a mesma sequência de procedimentos utilizada com o TrueCrypt, iniciou-se o processo com a criação de uma nova imagem do dispositivo, agora criptografado com BitLocker.

O FTK não obteve sucesso no acesso aos dados do dispositivo assim como havia ocorrido no caso anterior.

Com o Encase não foi possível adicionar o dispositivo ao caso. Uma mensagem alertando que o dispositivo não está pronto é mostrada na tela, figura 28.

Figura 28 – Resultado da análise utilizando Encase



Fonte: Do autor.

O resultado obtido com o Autopsy não apresentou diferença em relação ao uso com TrueCrypt, não conseguindo processar a imagem do dispositivo criptografado.

6.2.2.3 Análise e resultados com Passware Kit Forensic

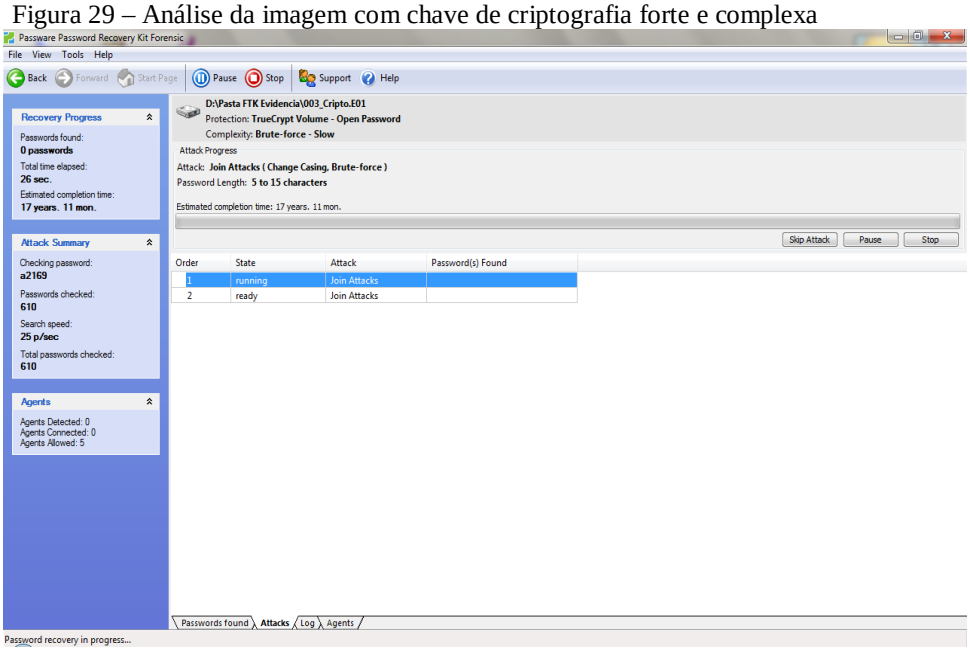
Utilizou-se a ferramenta Passware Kit Forensic em sua versão mais atual, 10.1.1986.

Inicialmente foi efetuada a análise da imagem com criptografia BitLocker, o qual, permite chave com no mínimo oito caracteres. Não houve sucesso na tentativa de recuperação da chave.

Para análise da criptografia com TrueCrypt utilizou-se três imagens do dispositivo, com três exemplos de chaves diferentes. Os algoritmos foram os mesmos empregados nas análises com as ferramentas forenses anteriores.

A primeira análise foi efetuada sobre a imagem com uma chave forte e complexa, englobando uma mescla de letras, números e símbolos especiais e comprimento de 50 caracteres. Tornou-se inviável a espera pela possível quebra da senha pelo tempo estimado para conclusão do processo, figura 29, aproximadamente 17 anos.

Figura 29 – Análise da imagem com chave de criptografia forte e complexa

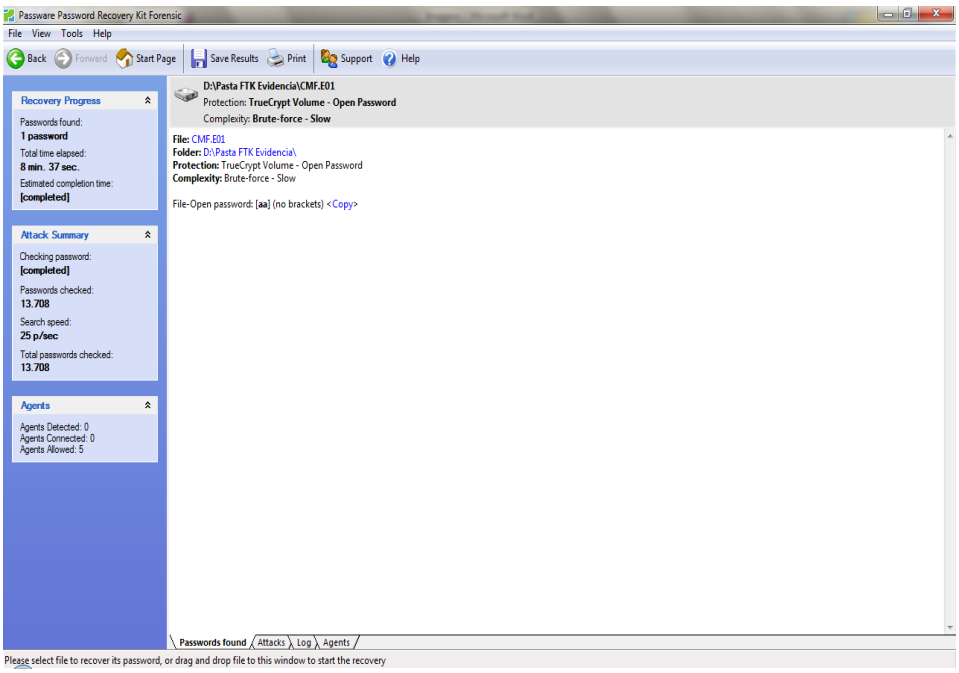


Fonte: Do autor.

Na segunda imagem analisada, o dispositivo apresentava uma senha que mesclava letras e números somente e um comprimento de nove caracteres. A estimativa de conclusão foi reduzida para pouco mais de um mês.

A tentativa de recuperação de senha na terceira imagem obteve sucesso, figura 30. Na criptografia foi utilizada uma chave extremamente fraca, constituída por apenas duas letras (aa). O tempo de quebra foi de oito minutos, trinta e sete segundos.

Figura 30 – Recuperação de chave (aa)



Fonte: Do autor.

A importância da criação de uma chave o mais forte e complexa possível para efetivamente garantir a proteção e confidencialidade das informações é comprovada na análise destas três imagens do dispositivo.

Embora esta pesquisa tenha sido elaborada com sistema de arquivos NTFS, a tabela 2 apresenta a lista das ferramentas utilizadas e suas versões disponíveis para Windows, Linux ou ambos.

Tabela 2 – Ferramentas X Sistema Operacional

	FTK	Encase	Autopsy	Passware	TrueCrypt	BitLocker	JPHS
Windows	X	X		X		X	
Linux	X						
Multiplataforma			X		X		X

6.2.3 Dispositivo com esteganografia em imagem

Utilizando o software JPHS em sua versão 0.5, um arquivo de texto extensão tipo .doc foi inserido à imagem. A figura 31 apresenta à esquerda a imagem original e, à direita, a mesma imagem já com esteganografia.

Figura 31 – Imagem com esteganografia

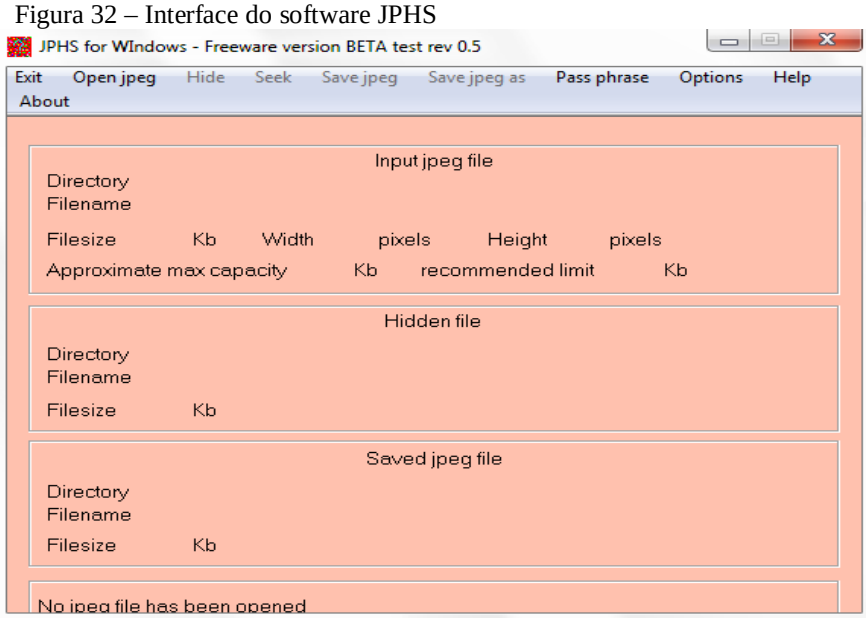
Fonte: Do autor.

Todos os comandos que envolvem a execução da esteganografia estão presentes na janela aberta ao executar o software, figura 32. Seleciona-se o arquivo de imagem no *Open* jpeg. Em *Hide* é feita a escolha do arquivo a ser escondido. A criação de uma *stego-key* ou senha é requerida na sequencia.

Para finalizar a esteganografia, basta salvar a imagem, ou com o mesmo nome em *Save* jpeg, ou modificando-o em *Save jpeg as*.

A reversão é efetuada através do comando *Seek*. Somente conhecendo-se a *stego-key* é possível recuperar o arquivo esteganografado.

Figura 32 – Interface do software JPHS



Fonte: Do autor.

7 CONCLUSÃO

Houve um tempo em que manter as informações protegidas, em muitos aspectos, era muito menos complicado. Corporações, governo, indivíduos, todos possuem dados que precisam estar seguros em relação ao acesso alheio não autorizado.

Todo o avanço tecnológico vivenciado na atualidade gerou ferramentas poderosas que, se empregadas com objetivos ilícitos na busca destas informações, poderia facilmente acessar ou recuperar tais dados de qualquer dispositivo desprotegido.

Diante deste quadro não seria de forma alguma desperdício de tempo ou dinheiro o investimento em ferramentas que viessem a garantir de maneira eficaz a confidencialidade das informações.

Mesmo porque como foi demonstrado através deste trabalho, existem softwares gratuitos e de grande eficiência para obtenção deste objetivo.

Utilizando as ferramentas da perícia forense não foi possível quebrar a criptografia na unidade de armazenamento com sistema de arquivos NTFS, seja utilizando o TrueCrypt, software livre e gratuito, como o BitLocker, presente no Windows 7.

Demonstra-se assim que o emprego destas ferramentas deveria ser preconizado por qualquer órgão, empresa ou indivíduo que não deseje que informações privadas e sigilosas sejam acessadas e expostas.

Torna-se importante salientar que o ser humano muitas vezes é o elo mais fraco nesta questão segurança. Por ser necessária a criação de uma chave(senha) o mais complexa possível com uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais como @, ^, $, e o preconizado pelo próprio TrueCrypt que possua no mínimo 20 e até 64 caracteres(quanto mais longo, melhor), o local de armazenamento desta senha é de primordial importância.

Os objetivos propostos inicialmente foram atingidos durante a execução deste trabalho. Os conceitos assim como todo o processo de perícia forense foram estudados e compreendidos. Desta forma, pode-se selecionar apenas as etapas que interessavam para o cumprimento do objetivo geral desta pesquisa.

Ferramentas utilizadas pelos peritos foram estudadas, compreendidas e aplicadas. A criptografia foi a ferramenta anti-forense aplicada ao dispositivo e os softwares utilizados para tal, estudados, entendidos e aplicados.

O objetivo geral de proteção das informações no dispositivo de armazenamento alvo, com sistema de arquivos NTFS, foi atingido visto que as ferramentas de perícia forense

não mais obtiveram sucesso no acesso aos dados após a criptografia do dispositivo com o algoritmo AES-256 e uso de uma chave forte.

Como dificuldade na efetivação do trabalho saliento a indisponibilidade total ou das últimas versões das principais ferramentas forenses sem aquisição de suas respectivas licenças.

Além da criptografia foi realizado um estudo sobre esteganografia e utilizado o software JPHS escondendo arquivos dentro de uma imagem previamente escolhida. Porém, o custo e a indisponibilidade do software StegoSuite ou StegoHunt(versão mais atual) da empresa WetStone Technologies em uma versão demo, impossibilitou um resultado mais fidedigno por ser esta a ferramenta apropriada para perícia em imagens esteganografadas.

O procedimento forense caso as ferramentas não consigam recuperar a chave no dispositivo criptografado, é utilizar softwares específicos para recuperação da mesma. O kit forense inclui servidores com centenas de GPU's CUDA porém, ainda assim seria difícil quebrar uma senha do TrueCrypt com AES 256, desde que seja uma senha forte.

Outra possibilidade seria alugar servidores da Amazon Web Service para quebrar a senha ou, utilizar o tempo ocioso de CPU de desktops em rede para fazer um ataque de quebra distribuída.

Diante do exposto acima, um estudo sobre as possibilidades forenses para quebra desta senha fica como sugestão para trabalhos futuros.

REFERÊNCIAS

BARRETO, Luiz Gustavo. **Utilização de Técnicas Anti-Forense Para Garantir a Confidencialidade.** Curitiba, PUC-PR, 2009. Disponível em: < **h**ttp://www.ppgia.pucpr.br/~jamhour/Download/pub/RSS/MTC/referencias/TCC%20-%20Gustavo%20Luis%20Barreto.pdf > Acesso em: 16 maio 2011.

BARROS, Jairo Moreno de. **Universidade Espionagem Digital.** São Paulo: Digerati Books, 2007. 304p.

BERGHEL, Hal. **Data Hiding Tactics for Windows and Unix File Systems.** 2007. Disponível em: < http://www.berghel.net/publications/data_hiding/data_hiding.php > Acesso em: out. 2011.

BEZDZIECKI, David J. **Steganography Home Page.** USA, Walsh College, 2009. Disponível em: <http://bit599.netai.net/index.htm> Acesso em: abril 2012.

BLUM, Renato O.; ABRUSIO, Juliana C. Crimes Eletrônicos. **Evidência Digital**, Rio de Janeiro, n. 1, 2004.

BLUNDEN, Bill. **The Rootkit Arsenal:** Escape and Evasion in the Dark Corners of the System. Plano, Texas: Jones & Bartlett Publishers, 2009. 908p.

BOTERO, Armando; CAMERO, Iván; CANO, Jeimy. **Técnicas Anti-Forense Em Informática: Ingeniería Reversa Aplicada a TimeStomp.** Bogotá, Colômbia: PUJ, 2009. Disponível em: <http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia3-Sesion6%283%29.pdf> Acesso em: maio 2011.

BRYANT, Robin. **The Challenge Of Digital Crime.** 2008. Disponível em: < http://media.wiley.com/product_data/excerpt/03/04705160/0470516003.pdf> Acesso em: out. 2011.

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

COSTA, Marcelo A.S.L. **Computação Forense.** Campinas: Millennium, 2003. 246p.

DAUON, A.J.; LIMA, G.T. **Crimes Informaticos O Direito Penal Na Era da Informação.** 2006. Disponível em: <http://www.truzzi.com.br/pdf/artigo-crimes-informativos-gisele-truzzi-alexandre-daoun.pdf> Acesso em: out. 2011.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando A Computação Forense.** São Paulo: Novatec, 2011. 200p.

FREITAS, Andrey Rodrigues de. **Perícia Forense Aplicada à Informática.** Rio de Janeiro: Brasport, 2006. 216p.

GALVÃO, Kléber Ricardo M. Perícia Forense Computacional. In: SEGINFO WORKSHOP DE SEGURANÇA DA INFORMAÇÃO, 4., 2009, Rio de Janeiro. Disponível em: < http://www.cefetrn.br/~rk/seginfo2009_2_rk.pdf> Acesso em: out. 2011.

HARRIS, Ryan. **Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem.** Elsevier Ltd.: 2006. Disponível em: <http://dfrws.org/2006/proceedings/6-Harris.pdf >. Acesso em: out.2011.

HENRIQUE, Wendel Guglielmetti. **Anti Forensics: Dificultando Análises Forenses Computacionais**, 2006. Disponível em: <http://ws.hackaholic.org/artigos/AntiForensics.ppt> Acesso em: maio 2011.

JUNIOR, Cirilo. **Petrobrás confirma furto de dados sigilosos.** Folha Online. Rio de Janeiro, 14 fev. 2008. Disponível em: <http://www1.folha.uol.com.br/folha/dinheiro/ult91u372404.shtml> Acesso em: 16 maio 2011.

LEMKE, Camilla. **Passware Kit Forensic**: Benefícios da Computação em Nuvem Aceleram Recuperação de Senhas. Under-Linux.Org. 16 abr. 2011. Disponível em: < http://under-linux.org/passware-kit-forensic-beneficios-da-computacao-em-nuvem-aceleram-recuperacao-2664/> Acesso em: out. 2011.

LEMOS, Hailton David. Ética Em Informática. **Revista Espírito Livre.** Novembro, 2009.

LIU, Vincent; BROWN, Francis. Bleeding-Edge Anti-Forensics. In: INFOSEC WORLD CONFERENCE & EXPO. MIS Training Institute, 2006. Disponível em: < http://www.slideworld.com/slideshows.aspx/BleedingEdge-AntiForensics-ppt-714491 > Acesso em: 16 maio 2011.

LLEWELLYN, Gareth. US missile data found on eBay hard drive. **The Independent.** Londres, 07 maio 2009. Disponível em: <http://www.independent.co.uk/news/world/americas/us-missile-data-found-on-ebay-hard-drive-1680529.html> Acesso em 16 maio 2011.

MADEIRA et al. **Criptografia de Disco – Garantindo a Segurança de Suas Informações.** Olinda-PE: AESO, 2007. Disponível em: <http://www.madeira.eng.br/wiki/index.php?page=Criptografia+de+Disco+%E2%80%93+Garantindo+a+seguran%C3%A7a+de+suas+informa%C3%A7%C3%B5es> Acesso em: out. 2011.

MELO, Sandro. **Computação Forense Com Software Livre.** Rio de Janeiro: Alta Books, 2009. 152p.

MENESES, Francisco Gerson A. **A Ética e o Profissional de Informática.** Parnaíba-PI: Instituto Federal de Educação, Ciência e Tecnologia, 2011. Disponível em: < http://ifpiparnaiba.edu.br/index.php?option=com_docman&task=doc_details&gid=384&Itemid=79> Acesso em: fev. 2011.

OHASHI et al. **Esteganografia.** Brasília-DF: UCB, 2006. Disponível em: <lyfreitas.com.br/artigos_mba/esteganografia.pdf> Acesso em: out. 2011.

OLIVEIRA, Flávio. **Metodologias de Análise Forense Para Ambientes Baseados em NTFS.** Campinas: UNICAMP**,** 2001. Disponível em: <

http://www.las.ic.unicamp.br/paulo/papers/2001-SSI-flavio.oliveira-forense.ntfs.pdf> Acesso em: maio 2012.

OTERO, Anne-Marie. Ética e Informática. **Metanoia Revista Eletrônica.** São João del-Rei, UFSJ, n.5, p.111-121, jul.2003.

PAIVA, Jadilson Alves de. **Práticas Anti-Forense: Um Estudo de Seus Impactos na Forense Computacional.** João Pessoa: IBRATEC, 2009. Disponível em: < http://www.nogueira.eti.br/profmarcio/obras/Jadilson%20-%20Anti-Forense.pdf> Acesso em: out. 2011.

PERON, Christian S.J; LEGARY, Michael. **Digital anti-forensics: emerging trends in data transformation techniques.** Seccuris Labs. 2008. Disponível em: <http://www.seccuris.com/documents/whitepapers/Seccuris-Antiforensics.pdf > Acesso em: out. 2011.

RIBEIRO, C.H.C.; CHICARELLI, D.P.; ALBUQUERQUE, Neila. Transmissão de Informações Sigilosas Através de Sites na Internet Utilizando Esteganografia. In: SIMPÓSIO DE INFORMÁTICA DA REGIÃO CENTRO DO RS, 7., 2008, Santa Maria. **Anais...** Santa Maria: UNIFRA, 2008. Disponível em: <http://www.sirc.unifra.br/artigos2008/39190_1.pdf> Acesso em: out. 2011.

ROCHA et al. **Segurança e Privacidade na Internet por Esteganografia em Imagens.** Campinas: UNICAMP, 2004. Disponível em: <http://www.ic.unicamp.br/~rocha/pub/papers/segurancaInternetEsteganografia.pdf> Acesso em: out. 2011.

ROHR, Altieres. **O Novo e o Velho Projetos de Crimes Digitais Agora são a Mesma Coisa.** Linha Defensiva. 18 maio 2012. Disponível em: < http://www.linhadefensiva.org/2012/05/o-novo-e-o-velho-projeto-de-crimes-digitais-agora-sao-a-mesma-coisa/> Acesso em: maio 2012.

ROSA, Daniel Accioly. Contextualização da Prática Forense. **Evidência Digital.** Rio de Janeiro, n. 1, 2004.

RUSSINOVICH, Mark. **Sysinternals Suite.** 2011. Disponível em: < http://technet.microsoft.com/en-us/sysinternals/0e18b180-9b7a-4c49-8120-c47c5a693683%28en-us%29.aspx> Acesso em 05 nov. 2011.

SAMMONS, John. **The Basics Of Digital Forensics.** Waltham, MA,USA: Elsevier, 2012.

SANTOS, Coriolano A.A.C. **As Múltiplas Faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e Seus Reflexos No Universo Jurídico.** São Paulo: OAB-SP, 2009. 163p.

SILVA, Luís Miguel. **Anti-Análise Forense.** CIISP: 2003. Disponível em: < http://lms.ispgaya.pt/documentacao/anti-analise.forense.pdf> Acesso em: out. 2011.

SILVA, Rafael. **Versão reduzida da Lei Azeredo é aprovada na Câmara.** Tecnoblog – diário tecnológico. 23 maio 2012. Disponível em: <http://tecnoblog.net/102183/lei-azeredo-aprovada/ > Acesso em: maio 2012.

THOMAS, Eliane. **Crimes Informáticos: Legislação Brasileira e Técnicas de Forense Computacional Aplicadas à Essa Modalidade de Crime.** 2010. Disponível em: <http://www.artigos.etc.br/crimes-informaticos-legislacao-brasileira-e-tecnicas-de-forense-computacional-aplicadas-a-essa-modalidade-de-crime.html> Acesso em: nov. 2011.

TRUZZI, Gisele. **Crimes Virtuais.** 2008. Disponível em: < http://www.truzzi.com.br/artigos/> Acesso em: out. 2011

VARGAS, Raffael Gommes. **Perícia forense Computacional e Metodologias Para Obtenção de Evidências.** 2007. Disponível em: < http://imasters.com.br/artigo/6225> Acesso em: mar. 2012.

_____. Perícia Forense Computacional Metodologia e Ferramentas Periciais. **Evidência Digital.** Rio de Janeiro, n. 5, 2011.

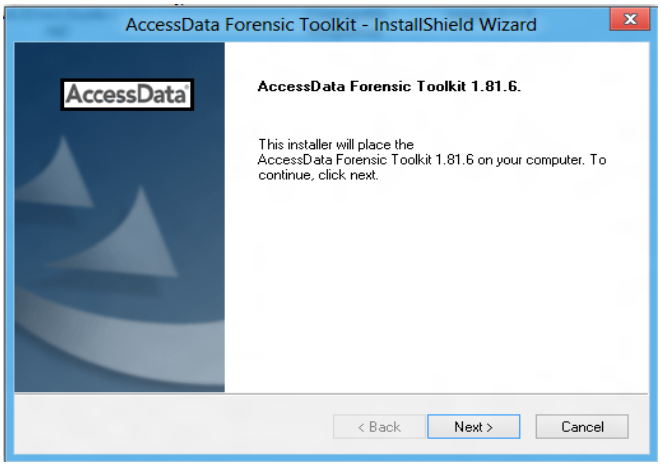
VISUALWARE. eMailTrackerPro Email tracing and spam filter. Disponível em: < http://www.emailtrackerpro.com/> Acesso em: out. 2011.

WEBER, Daniel; PEREIRA, Evandro Della Vecchia; GOLDANI, Carlos Alberto. Análise do Uso de Antiforense Digital Para Destruição de Dados. **ACRIGS,** 2011. Disponível em: <http://www.acrigs.com.br/Artigos.htm> Acesso em: 16 maio 2011.

WEE, Cheong Kai. **Analysis of hidden data in NTFS file system.** 2006. Disponível em: < http://www.forensicfocus.com/downloads/ntfs-hidden-data-analysis.pdf >. Acesso em: out. 2011.

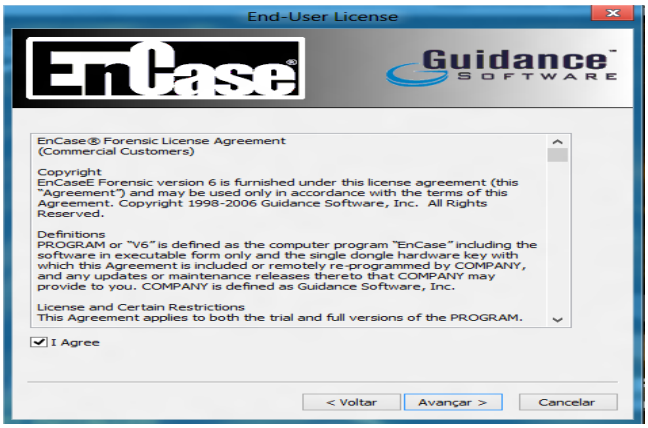
APÊNDICE A – INSTALAÇÃO DAS FERRAMENTAS

A instalação da ferramenta Forense Tool Kit difere de acordo com a versão utilizada. O procedimento até a versão 1.81.6 é bastante simples. No pacote de instalação estavam incluídos o Codemeter e o FTK propriamente dito. Inicialmente temos a escolha da versão do sistema operacional, 32 ou 64 bits, instala-se então o CodeMeter que é o componente que gerencia o licenciamento da solução e a seguir o FTK.

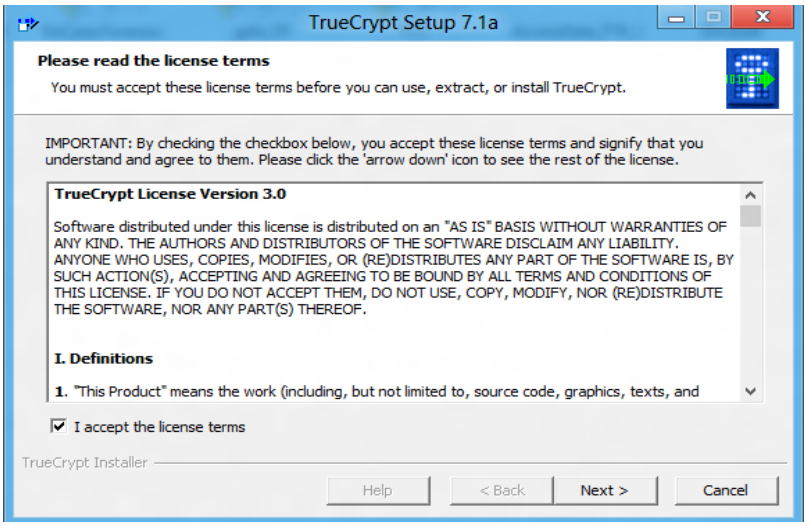


A partir da versão 3 o banco de dados Oracle passou a ser utilizado como database das análises e é necessária sua instalação prévia. Na atual versão 4, o Oracle foi substituído pelo PostgreSQL. A seguir instala-se o CodeMeter. Na sequencia mais uma novidade, o FTK Process Engine, responsável pelo processamento das evidências do caso. Finalizando, instala-se o FTK propriamente dito.

A ferramenta Encase em sua versão 6.1 possui processo de instalação padrão, bastando aceitar a licença e segue clicando em avançar.



O software de criptografia TrueCrypt em sua versão 7.1a segue a mesma sequência, aceita-se os termos de licença e em seguida segue clicando em next.



Já a ferramenta forense Passware Password Recovery Kit Forensic 10.1.1986, tem sua instalação apenas seguindo o padrão next-next.

APÊNDICE B - ARTIGO: APLICAÇÃO DE TÉCNICAS DE ANTI-FORENSE COMPUTACIONAL EM ARQUIVOS NTFS

APLICAÇÃO DE TÉCNICAS DE ANTI-FORENSE COMPUTACIONAL EM ARQUIVOS NTFS

Nataniel Corrêa de Oliveira[1], Paulo João Martins[2]

[1]Acadêmico do Curso Ciência da Computação - Universidade do Extremo Sul Catarinense (UNESC) - Criciúma - SC - Brasil.

[2] MSc. Professor do Curso Ciência da Computação - Universidade do Extremo Sul Catarinense (UNESC) - Criciúma - SC - Brasil.

nco@terra.com.br, pjm@unesc.net

Abstract. The objective of the study is based on the use of tools and anti-forensics techniques in a device with NTFS file system, seeking the protection of the files to ensure their content security and privacy. The encryption stands out as the best known method to hide files, but steganography can also be used. Forensic expertise tools were used to scan the device, first without anti-forensic techniques, then, as a second step, applying encryption through TrueCrypt and BitLocker tools. Results show that, by using a strong key, the encryption in the storage unit with NTFS files system could not be broken. On the other hand, with the device being unprotected all its contents could be recovered, including files that had been deleted; similarly, even the AES-256 encryption could be broken by using a weak key.

Resumo. O objetivo deste trabalho baseia-se no uso de ferramentas e técnicas de anti-forense computacional em um dispositivo com sistema de arquivos NTFS, buscando a proteção dos arquivos para garantir a segurança e privacidade de seu conteúdo. A criptografia destaca-se como método mais conhecido ou, podem-se esconder arquivos empregando a esteganografia. Ferramentas de perícia forense foram utilizadas para vasculhar o dispositivo, inicialmente sem técnicas anti-forense e em um segundo momento, aplicando criptografia com as ferramentas TrueCrypt e BitLocker. Como resultado, ao fazer uso de uma chave forte, não foi possível quebrar a criptografia na unidade de armazenamento com sistema de arquivos NTFS. Em contrapartida, com o dispositivo desprotegido todo seu conteúdo foi recuperado, inclusive arquivos que haviam sido excluídos. Da mesma forma, mesmo com criptografia AES-256, ao utilizar-se uma chave fraca, conseguiu-se a quebra da mesma.

1. Introdução

Atualmente, uma gama de produtos e serviços encontram-se disponíveis na rede mundial de computadores no intuito de facilitar o dia a dia das pessoas. Porém, a utilização destas facilidades por pessoas mal intencionadas acabou por gerar um antagonismo entre o bom e o mau uso dos recursos, não tardando para que fossem utilizados em práticas ilegais e criminosas.

Ferramentas específicas e poderosas são criadas para investigar máquinas, periféricos e dispositivos em busca de vestígios e provas desta nova modalidade de crime.

A Computação Forense tem como objetivo principal determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área de informática, tendo como questão principal o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhe validade probatória em juízo (ELEUTÉRIO; MACHADO, 2011).

Em contrapartida, empresas possuem informações valiosas que devem estar seguras e protegidas inclusive das técnicas de análise forense com o objetivo de evitar a quebra da confidencialidade de dados.

Anti-forense, portanto, são técnicas de remoção, ocultação e subversão de evidências com o objetivo de mitigar os resultados de análises forenses computacionais (HENRIQUE, 2006).

Diante deste contexto, este trabalho de pesquisa visa descrever e demonstrar as técnicas anti-forense quando a investigação forense possuir objetivos ilícitos.

2. Crimes Digitais

O crescimento tecnológico ao longo da história contribuiu para o surgimento de novas atividades criminosas. Assim, como muitas pessoas beneficiam-se desta tecnologia por razões legítimas, existem as que a utilizam com intenção de cometer o crime (BRYANT, 2008, tradução nossa).

O equipamento computacional é utilizado como ferramenta de apoio ou como meio para realização do crime (ELEUTÉRIO; MACHADO, 2011).

2.1 Legislação

Projetos de leis tramitam quase que em *loop* no congresso nacional por falta de informação ou excesso burocrático (THOMAS, 2010).

Dois projetos de lei foram recentemente aprovados (maio/2012), o projeto 2973/2011 e o projeto 84/99. As condutas ilícitas consideradas nestes projetos: invasão de computadores, ataques de negação de serviço, instalação de vulnerabilidades, venda de dispositivo ou programa que permita a prática ilícita e, falsificação de documento particular ou cartão de débito ou crédito (ROHR, 2012).

Também permitem a retirada do ar de páginas com mensagens racistas e a criação de um órgão ligado à polícia especializada no combate à delitos na internet (SILVA,2012).

2.2 Ética Em Informática

Embora não tenhamos a regulação, todo profissional de informática deve ser consciente e honesto, zelando pelo seu nome e pela classe (MENESES, 2011).

A questão pessoal é sempre de grande importância quando o assunto é a ética. Na informática como na maior parte das profissões, a ética deve englobar dois aspectos, a conduta pessoal como ser humano e a conduta profissional (LEMOS, 2009).

3 Perícia Forense Computacional

Pericia forense computacional é um processo em que utiliza o conhecimento de técnicas e métodos apoiados por ferramentas apropriadas, com o intuito de obter dados e equipamentos com o objetivo de classifica-los como vestígio, evidências ou prova em caráter judicial (MELO, 2009).

Dentre os procedimentos ou fases de uma perícia forense encontram-se: aquisição, preservação, extração, análise e formalização (MELO, 2009; ELEUTÉRIO; MACHADO, 2011).

São três metodologias forenses existentes subdivididas em suas respectivas fases, tabela 1.

Tabela 1 – Metodologias forenses e respectivas fases

SOP	Reith, Carr e Gunsh	EDRM
Coleta da prova	Identificação	Identificação
Preparação do Equipamento	Preparação	Preservação
Imagem Forense	Abordagem estratégica	Coleta
Exame/análise	Preservação	Processamento
Documentação	Coleção	Revisão
Relatórios	Exame	Análise
Revisão	Análise	Produção
	Apresentação	Apresentação
	Devolução de provas	

3.1 Utilização Da Perícia Forense Com Fins Ilícitos

Com a facilidade de acesso às ferramentas e técnicas de análise forense, indivíduos passam a utilizar os procedimentos de forma ilícita visando quebrar a confidencialidade de dados (BARRETO, 2009).

O indivíduo interessado nesse tipo de prática pode ter acesso vasculhando o HD utilizando-se de técnicas forenses, avançadas ou não, para obter ou até recuperar dados deletados. Torna-se necessária a utilização de alguns métodos, anti-forense, para tornar impossível ou mais difícil esse acesso a dados confidenciais (BARRETO, 2009).

4. Anti-forense Computacional

Grande parte das empresas não gosta de investir em recursos de segurança pelo simples fato de não considerar necessário. A maioria apenas investe após já terem sido invadidas e consequentemente perderam muitos pontos com seus clientes (BARROS, 2007).

As técnicas de invasão são cada vez mais sofisticadas e efetivas em sistemas computacionais. Assim, surgem as chamadas técnicas anti-forense com intuito de comprometer a disponibilidade de evidências em um processo forense (BOTERO; CAMERO; CANO, 2009, tradução nossa).

Pode-se utilizar assim estas técnicas para dificultar o acesso à informações sigilosas em dispositivos de armazenamento, mesmo por um perito forense (PERON; LEGARY, 2008, tradução nossa).

Anti-forense computacional são métodos utilizados para remover, ocultar, falsificar ou destruir evidências com o objetivo de dificultar resultados de perícias forenses (BARRETO, 2009).

4.1 Sistema De Arquivos NTFS

A função de um sistema de arquivos é garantir um método de organização para armazenar e recuperar dados a qualquer momento (CARRIER, 2005, tradução nossa).

O sistema de arquivos NTFS surge como uma necessidade de corrigir falhas de segurança, desempenho e confiabilidade que o sistema de arquivos FAT possuía (BOTERO; CAMERO; CANO, 2009, tradução nossa).

A formatação de uma partição NTFS resulta na criação da Master File Table (MTF) e outros arquivos de sistema. A MFT contém informações sobre todos os arquivos e diretórios da partição (OLIVEIRA, 2001).

4.2 Criptografia

A criptografia é uma técnica que visa transformar uma informação na sua forma original em outra ilegível. Esse processo é executado para que somente o detentor da chave criptográfica consiga realizar o processo inverso e ler o arquivo original (ELEUTÉRIO; MACHADO, 2011).

A criptografia pode ser considerada a melhor técnica anti-forense para ocultação de evidências. A quebra da criptografia pode levar anos dependendo da chave, do algoritmo e do poder computacional empregado (PAIVA, 2009).

A criptografia, portanto, é capaz de inviabilizar uma perícia ou um ataque desde que utilizadas chaves criptográficas a partir de 128 bits e que o sistema seja desligado após qualquer criptografia para que as chaves sejam volatizadas na DRAM (PAIVA, 2009).

4.3 Esteganografia

São técnicas que consistem em ocultar uma mensagem dentro de outra. A criptografia codifica o conteúdo, a esteganografia camufla uma mensagem em outra (ELEUTÉRIO; MACHADO, 2011).

Na atualidade são várias e bastante complexas as técnicas, podendo ser aplicadas a inúmeros tipos de arquivos, inclusive imagens e vídeos (ELEUTÉRIO; MACHADO, 2011).

Uma estego-key (*stego-key*) ou senha é a chave usada para controlar todo o processo de ocultamento. Somente quem a conhece consegue recuperar o dado embutido ou restringir sua detecção (ROCHA et al, 2004).

5. Proteção De Dados Em Dispositivo De Armazenamento

Um incidente de segurança em uma empresa com vazamento de informações sigilosas, por exemplo, pode causar impacto negativo nas finanças da organização, perda da confiabilidade de clientes e ainda prejudicar o relacionamento com parceiros e fornecedores.

Técnicas de anti-forense computacional são utilizadas de forma benéfica, para proteger a confidencialidade desses dados e informações.

Com a disponibilidade atual de ferramentas forenses e com a facilidade em dominar seu uso, estas podem ser empregadas com a finalidade única de quebrar o sigilo de informações pessoais e corporativas.

Baseado nessa realidade, foram utilizadas ferramentas que aplicam as técnicas anti-forense de criptografia e esteganografia para proteção de dados e/ou informações sob sistema de arquivos NTFS e posteriormente, aplicação das ferramentas de análise forense.

5.1 Metodologia

Criptografia e esteganografia foram as técnicas escolhidas e aplicadas por meio dos softwares TrueCrypt e BitLocker para criptografia e JPHS, esteganografia. Dentre as técnicas anti-forense, são as que melhor se enquadram no contexto desta pesquisa, a proteção de dados e informações.

5.2 Análise Dos Dados E Resultados

A realização de uma perícia forense computacional segundo a metodologia SOP envolve sete fases. Sendo o objetivo deste trabalho a proteção da confidencialidade das informações em um dispositivo de armazenamento, somente as fases de aquisição e exame/análise foram empregadas.

As ferramentas periciais, Encase, FTK, Passware Kit Forensic e uma ferramenta gratuita e de código aberto, o Autopsy, foram selecionadas para efetivação deste trabalho.

No primeiro estágio de desenvolvimento, arquivos foram inseridos num dispositivo de armazenamento USB formatado com sistema de arquivos NTFS. Alguns destes dados foram selecionados e deletados propositalmente. Ferramentas anti-forense não foram utilizadas neste momento.

FTK, Encase e Autopsy recuperaram todos os dados do dispositivo, inclusive aqueles que haviam sido excluídos.

Num segundo estágio, foi efetuada a criptografia completa do dispositivo de armazenamento USB contendo os mesmos dados da análise anterior. Utilizou-se dois softwares de criptografia, o TrueCrypt e o Bitlocker. A recuperação dos arquivos não foi possível em ambos os casos.

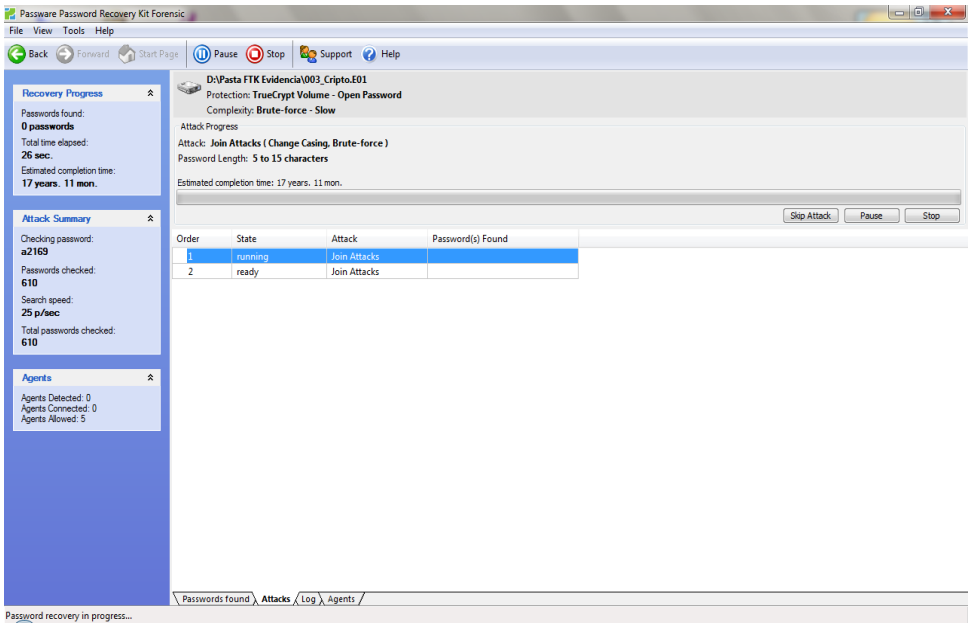


Figura 1. Análise da imagem com chave de criptografia forte e complexa

Passou-se a empregar a ferramenta Passware Forense Kit na tentativa de quebra da chave criptográfica. Uma análise foi efetuada sobre a imagem com uma chave forte e complexa, englobando uma mescla de letras, números e símbolos especiais e comprimento de 50 caracteres. Tornou-se inviável a espera pela possível quebra da senha pelo tempo estimado para conclusão do processo, figura 1, aproximadamente 17 anos.

A tentativa de recuperação de senha obteve sucesso, figura 2, com criptografia utilizando uma chave extremamente fraca, constituída por apenas duas letras (aa). O tempo de quebra foi de oito minutos, trinta e sete segundos.

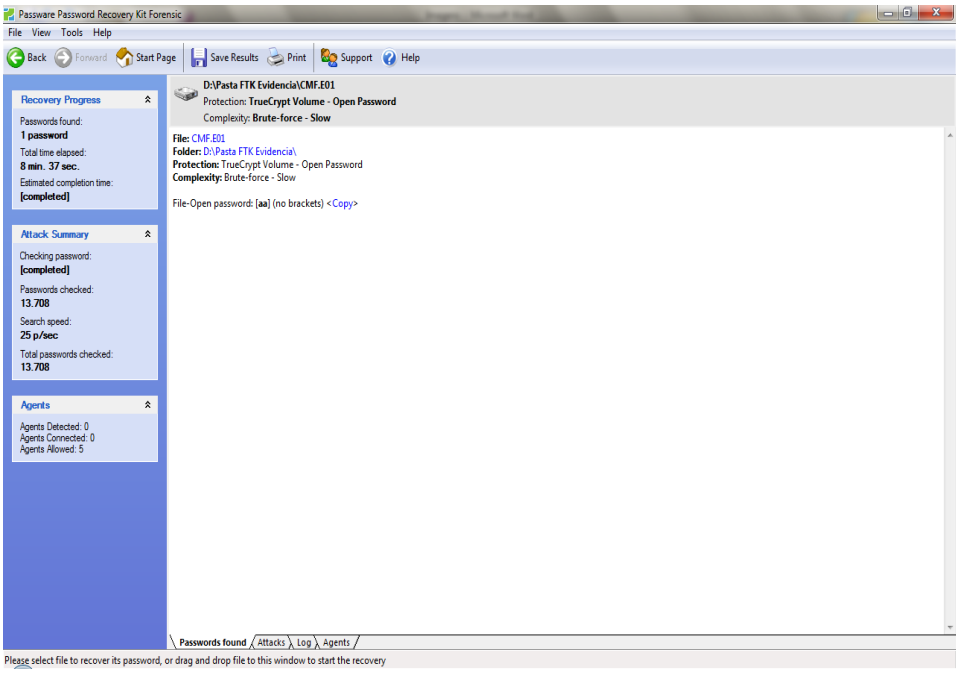


Figura 2. Recuperação de chave (aa)

6. Conclusão

Utilizando as ferramentas da perícia forense não foi possível quebrar a criptografia na unidade de armazenamento com sistema de arquivos NTFS, seja utilizando o TrueCrypt, software livre e gratuito, como o BitLocker, presente no Windows 7.

Demonstra-se assim que o emprego destas ferramentas deveria ser preconizado por qualquer órgão, empresa ou indivíduo que não deseje que informações privadas e sigilosas sejam acessadas e expostas.

Torna-se importante salientar que o ser humano muitas vezes é o elo mais fraco nesta questão segurança. Por ser necessária a criação de uma chave(senha) o mais complexa possível com uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais como @, ^, $, e o preconizado pelo próprio TrueCrypt que possua no mínimo 20 e até 64 caracteres(quanto mais longo, melhor), o local de armazenamento desta senha é de primordial importância.

Referências

BARRETO, Luiz Gustavo (2009). Utilização de Técnicas Anti-Forense Para Garantir a Confidencialidade. Curitiba, PUC-PR. Disponível em: < http://www.ppgia.pucpr.br/~jamhour/Download/pub/RSS/MTC/referencias/TCC%20-%20Gustavo%20Luis%20Barreto.pdf > Acesso em: 16 maio 2011.

BOTERO, Armando; CAMERO, Iván; CANO, Jeimy (2009) . Técnicas Anti-Forense Em Informática: Ingeniería Reversa Aplicada a TimeStomp. Bogotá, Colômbia: PUJ. Disponível em: <http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia3-Sesion6%283%29.pdf> Acesso em: maio 2011.

BRYANT, Robin. The Challenge Of Digital Crime (2008). Disponível em: < http://media.wiley.com/product_data/excerpt/03/04705160/0470516003.pdf> Acesso em: out. 2011

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira (2011). Desvendando A Computação Forense. São Paulo: Novatec. 200p.

FREITAS, Andrey Rodrigues de (2006). Perícia Forense Aplicada à Informática. Rio de Janeiro: Brasport. 216p.

GALVÃO, Kléber Ricardo M. (2009). Perícia Forense Computacional. In: SEGINFO WORKSHOP DE SEGURANÇA DA INFORMAÇÃO, 4., Rio de Janeiro. Disponível em: < http://www.cefetrn.br/~rk/seginfo2009_2_rk.pdf> Acesso em: out. 2011.

HENRIQUE, Wendel Guglielmetti (2006). Anti Forensics: Dificultando Análises Forenses Computacionais. Disponível em: <http://ws.hackaholic.org/artigos/AntiForensics.ppt> Acesso em: maio 2011.

LEMOS, Hailton David (2009). Ética Em Informática. Revista Espírito Livre.

MADEIRA et al (2007). Criptografia de Disco – Garantindo a Segurança de Suas Informações. Olinda-PE: AESO. Disponível em: <http://www.madeira.eng.br/wiki/index.php?page=Criptografia+de+Disco+%E2%80%93+Garantindo+a+seguran%C3%A7a+de+suas+informa%C3%A7%C3%B5es> Acesso em: out. 2011.

MELO, Sandro (2009). Computação Forense Com Software Livre. Rio de Janeiro: Alta Books. 152p.

MENESES, Francisco Gerson A (2011). A Ética e o Profissional de Informática. Parnaíba-PI: Instituto Federal de Educação, Ciência e Tecnologia. Disponível em: < http://ifpiparnaiba.edu.br/index.php?option=com_docman&task=doc_details&gid=384&Itemid=79> Acesso em: fev. 2011.

OLIVEIRA, Flávio. Metodologias de Análise Forense Para Ambientes Baseados em NTFS. Campinas: UNICAMP, 2001. Disponível em: < http://www.las.ic.unicamp.br/paulo/papers/2001-SSI-flavio.oliveira-forense.ntfs.pdf> Acesso em: maio 2012.

PAIVA, Jadilson Alves de. Práticas Anti-Forense: Um Estudo de Seus Impactos na Forense Computacional (2009). João Pessoa: IBRATEC. Disponível em: < http://www.nogueira.eti.br/profmarcio/obras/Jadilson%20-%20Anti-Forense.pdf> Acesso em: out. 2011.

PERON, Christian S.J; LEGARY, Michael (2008). Digital anti-forensics: emerging trends in data transformation techniques. Seccuris Labs. Disponível em:

<http://www.seccuris.com/documents/whitepapers/Seccuris-Antiforensics.pdf > Acesso em: out. 2011.

ROCHA et al. Segurança e Privacidade na Internet por Esteganografia em Imagens (2004). Campinas: UNICAMP. Disponível em: <http://www.ic.unicamp.br/~rocha/pub/papers/segurancaInternetEsteganografia.pdf> Acesso em: out. 2011.

ROHR, Altieres (2012). O Novo e o Velho Projetos de Crimes Digitais Agora são a Mesma Coisa. Linha Defensiva. Disponível em: < http://www.linhadefensiva.org/2012/05/o-novo-e-o-velho-projeto-de-crimes-digitais-agora-sao-a-mesma-coisa/> Acesso em: maio 2012.

SAMMONS, John (2012). The Basics Of Digital Forensics. Waltham, MA,USA: Elsevier.

SANTOS, Coriolano A.A.C. (2009). As Múltiplas Faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e Seus Reflexos No Universo Jurídico. São Paulo: OAB-SP. 163p.

TRUZZI, Gisele (2008). Crimes Virtuais. Disponível em: < http://www.truzzi.com.br/artigos/> Acesso em: out. 2011.

VARGAS, Raffael Gommes (2011). Perícia Forense Computacional Metodologia e Ferramentas Periciais. Evidência Digital. Rio de Janeiro, n. 5.

WEBER, Daniel; PEREIRA, Evandro Della Vecchia; GOLDANI, Carlos Alberto (2011). Análise do Uso de Antiforense Digital Para Destruição de Dados. ACRIGS. Disponível em: <http://www.acrigs.com.br/Artigos.htm> Acesso em: 16 maio 2011.