ANÁLISE DE FERRAMENTAS FORENSES NA INVESTIGAÇÃO DIGITAL

Thalita Scharr Rodrigues – Universidade Estadual de Ponta Grossa - thalitascharr@gmail.com
Dierone César Foltran Jr. – Universidade Estadual de Ponta Grossa - dcfoltran@gmail.com

Resumo: A Forense Computacional é uma área que tem recebido significativa atenção atualmente. A investigação e extração de vestígios eletrônicos em ambientes computacionais com a finalidade de tentar reconstituir eventos e verificar se o computador foi utilizado para atos ilícitos não se trata de um processo trivial. Além de noções de Forense e Anti-forense Computacional, neste trabalho são analisadas ferramentas que podem ser utilizadas para auxiliar o perito na coleta e análise de evidências digitais.

Palavras-chave: Forense computacional, segurança, coleta e correlação de evidências.

ANALYSIS OF FORENSIC TOOLS IN DIGITAL INVESTIGATION

Abstract: Computer Forensics is an area which has recently received meaningful attention. Investigation and extraction of electronic traces in computational systems trying recreate events and verifiy if the computer was used to illicits acts is not a trivial process. Besides notions of Computer Forensics and Anti - forensics , in this paper we analyze tools that are able to auxiliate experts in colect and analysis of digital evidences.

Key words: Computer Forensics, security, evidence collection and correlation evidence.

1. Introdução

Devido ao aumento exponencial da utilização de computadores e da Internet nos últimos anos, tornou-se essencial a apuração dos crimes realizados através de ambientes computacionais. Assim, para a investigação e coleta de evidências de atos ilícitos cometidos por meio de computadores surgiu a Forense Computacional. Portanto, define-se Forense Computacional como a inspeção científica e sistemática em ambientes computacionais, com o objetivo de coletar evidências digitais, com a finalidade de promover a reconstituição dos eventos encontrados, podendo determinar se o ambiente em análise foi utilizado na realização de atividades ilegais ou não autorizadas (PALMER, 2001).

Dessa forma, a investigação digital consiste das seguintes etapas: preservação da cena do crime e das evidências, análise, documentação, pesquisa e coleta, reconstrução do ato e apresentação das evidências. Na fase de pesquisa e coleta de informações são utilizadas ferramentas forenses e devem ser criadas imagens (cópias físicas) dos discos rígidos dos computadores que são considerados suspeitos de terem sido utilizados no ato ilícito (CARRIER, 2003).

Nas imagens criadas podem existir arquivos normais, excluídos e danificados, os quais podem ser recuperados através de ferramentas forenses. Dessa maneira, as ferramentas devem garantir a validade e a integridade dos resultados obtidos para serem apresentados na Corte. Adicionalmente, existem padrões que devem ser seguidos para a verificação da legitimidade das ferramentas forenses utilizadas na coleta e análise das evidências. (CRAIGER, 2006).

Por outro lado, criminosos podem utilizar métodos denominados anti-forenses com a finalidade de esconder vestígios e dificultar o processo de investigação digital. As ferramentas e técnicas anti-forenses possibilitam o uso de funções que apagam e sobrescrevem os dados e traços deixados em arquivos do sistema como histórico, *cookies*, lista de arquivos recentemente usados, entre outros (GEIGER, 2005).

Assim, considerando-se a quantidade de softwares e métodos existentes para a investigação de crimes digitais nos dias de hoje, o presente trabalho objetiva analisar ferramentas e técnicas

de Forense Computacional utilizadas na coleta de informações e perícias em imagens de mídias digitais, muitas das quais são disponibilizadas na Internet para estudo de peritos digitais.

2. Forense Computacional

O crescimento excessivo de atos ilícitos relacionados com computadores exige um conhecimento extenso da obtenção e utilização de evidências digitais contidas em computadores. Através de conceitos e metodologias existentes na Forense Computacional pode-se obter tal conhecimento (REIS, 2003).

Convencionalmente define-se a Forense Computacional como um conjunto de técnicas e ferramentas utilizadas para encontrar evidências em um computador (CALOYANNIDES, 2001). Portanto, o principal objetivo deste tipo de perícia forense pode ser definido como a coleta de vestígios relacionados ao crime investigado, os quais possibilitem a formulação de conclusões sobre o caso (REIS, 2003).

O campo da pesquisa sobre investigação digital surgiu na década de 80, sendo que em 1984 foi criado um programa dentro do Federal Bureau of Investigation (FBI) (CUMMINGS, 2010). Porém, naquela época este programa era conhecido apenas como sendo um grupo de análises e estudos sobre mídias magnéticas. Alguns anos após a criação do programa, o agente especial Michael Anderson, o qual é considerado o "Pai da Forense Computacional", começou na trabalhar neste departamento do FBI (CUMMINGS, 2010). Este agente trabalhou no programa até a década de 90 e, posteriormente começou sua própria empresa de investigação forense. O termo Forense Computacional foi mencionado pela primeira vez em 1988, no primeiro treinamento realizado pela Associação Internacional de Especialistas em Investigação Computacional (IACIS) em Portland, Oregon (ARTHUR, 2004).

2.1 Processo de Investigação da Forense Computacional

Nos últimos anos, advogados passaram a utilizar evidências digitais em tribunais e cortes de muitos países. Entretanto, para que sejam consideradas provas válidas o perito deve realizar o processo de investigação cuidadosa e sistematicamente, desse modo preservando as evidências e as documentando detalhadamente, com a finalidade de autenticá-las (PEREIRA, 2007).

Portanto, o processo investigativo da Forense Computacional deve assegurar a integridade dos vestígios coletados, porém devido à volatilidade das evidências eletrônicas, essa tarefa pode ser considerada difícil. Sendo assim, para garantir a integridade e confiabilidade das evidências coletadas, o perito forense deve seguir procedimentos e protocolos reconhecidos pela comunidade científica, e a cada passo, deve detalhar e revisar a documentação desenvolvida, para que deste modo, evite erros durante o processo investigativo (EOGHAN, 2002).

A documentação confeccionada pelo investigador deve conter a identificação de todos os arquivos coletados (contendo dados como número do caso, nome da pessoa que fez a coleta, data e local) e do armazenamento de cada evidência coletada (REIS, 2003). Além do mais, no tribunal pode-se utilizar um laudo para assegurar a legitimidade das evidências obtidas durante o processo investigativo (FREITAS, 2006). Esse laudo denomina-se cadeia de custódia e é uma peça fundamental no processo de investigação forense.

Com o passar dos anos e devido à realização de vários estudos, surgiram diversos modelos de processo para a investigação de crimes digitais. Um modelo internacionalmente utilizado de processo investigativo trata-se do publicado pelo Departamento de Justiça dos Estados

Unidos. As etapas apresentadas a seguir são citadas neste modelo de processo investigativo (BARYAMUREEBA, 2004).

a. Preparação: o perito deve preparar equipamentos e ferramentas de apoio às tarefas da investigação.
b. Coleta: fase que envolve a busca e o reconhecimento de evidências, posteriormente extração das mesmas e a documentação dos vestígios.
c. Exame: na fase de exame procura-se revelar dados escondidos e informações obscuras nas evidências coletadas.
d. Análise: esta etapa refere-se à análise do relatório resultante da fase de exame, desse modo analisando as evidências consideradas de valor e relevantes para o caso.
e. Apresentação: gera-se o relatório final do processo de investigação e dos dados recuperados durante todo a investigação.

2.2 Live Analisys vs Postmortem

Em uma investigação forense podem ocorrer análises em sistema onde existem situações em que houve o desligamento do sistema ou não. Nomeia-se *Live Analisys* o processo realizado sem o desligamento da máquina vítima (PEREIRA, 2007). A importância deste tipo de investigação consiste na existência de informações voláteis, as quais serão perdidas com o desligamento da máquina. Informações como conexões de redes e processos em execução são exemplos de dados coletados durante este tipo de análise.

Ocorrem situações onde a máquina analisada ainda pode estar sobre domínio do atacante, desse modo o sistema pode estar executando programas que escondam informações e dificultem o trabalho do perito. Baseando-se neste fato, o perito necessita usar um conjunto de ferramentas confiáveis e assim poderá garantir a integridade das tarefas realizadas com o auxílio das mesmas (PEREIRA, 2007).

Já o processo de investigação realizado nas cópias da mídia original chama-se *Postmortem*. Este tipo de análise é executado com o auxílio de um computador, denominado estação forense, preparada com ferramentas apropriadas, além de sistema operacional adequado e uma grande capacidade de armazenagem de dados (PEREIRA, 2007). Na análise *Postmortem* técnicas de pesquisa de arquivos como *logs* de dados, verificação de data de dados e recuperação de informações excluídas e escondidas são exemplos de operações realizadas trivialmente.

Uma das grandes dificuldades da investigação *Postmortem* atualmente trata-se do aumento da capacidade de armazenamento dos discos rígidos, de modo que o tempo e o esforço necessário para criar imagens é diretamente proporcional ao tamanho do disco (ADELSTEIN, 2006). Enquanto a imagem está sendo criada, a mídia precisa permanecer off-line, sendo assim considera-se inaceitável perder horas em casos de incidentes em sistemas de tempo real ou até mesmo os de comércio eletrônico. Por causa disso, muitos juízes não ordenam mais o desligamento de servidores (ADELSTEIN, 2006).

3. Anti-Forense

A investigação de crimes digitais, do mesmo modo que a apuração de crimes do mundo real, não é uma tarefa trivial. Podem ocorrer muitas dificuldades na coleta e análise de vestígios deixados na máquina utilizada no ato ilícito, sendo que a quantidade de evidências deixadas é inversamente proporcional às habilidades apresentadas pelo criminoso (REIS, 2003).

Sendo assim, do mesmo modo que a Forense Computacional surgiu para a investigação de atos ilícitos, criminosos podem utilizar métodos denominados anti-forenses para esconder, danificar ou excluir seus rastros digitais na cena do crime. Portanto, a Anti-Forense pode ser definida como a tentativa negativa de alterar a existência, quantidade e qualidade dos vestígios eletrônicos, ou também, dificultar ou impossibilitar a realização da investigação destas evidências (ROGERS, 2006).

Embora seja utilizada principalmente para ações negativas, existem profissionais de Forense Computacional que estudam técnicas de Anti-forense para não serem deixados para trás.

3.1 Técnicas anti-forenses

A Anti-Forense é um campo relativamente novo, mas enquadram diversos tipos de atividades, tais como ocultação de dados, limpeza de registros, destruição de traços, ataques contra ferramentas forenses, entre outras (ROGERS, 2006).

3.1.1 Ocultação de dados

Existem várias técnicas utilizadas para evitar a detecção de dados. Uma das maneiras mais conhecidas e utilizadas trata-se da esteganografia. Pode-se definir esta técnica como sendo um processo realizado para mascarar informações com a finalidade de evitar a sua descoberta (ROCHA, 2004).

O processo de esteganografia consiste em esconder uma informação através de uma mensagem de menor importância, conhecida como mensagem de cobertura. Após inserir os dados na mensagem de cobertura, obtém-se o chamado estego-objeto, que é uma mensagem inócua que contém secretamente uma mensagem de maior importância (ROCHA, 2004). Atualmente utilizam-se recursos como imagens, áudios e vídeos como meios de mensagem de cobertura (KESLER, 2007).

Um exemplo de como é feito o processo de ocultamento pode ser visto na Figura 1. A olho nu não se percebem as alterações nos arquivos que possuem os dados escondidos, porém existem casos onde eles podem ser percebidos devido ao aumento do tamanho do arquivo. Caso contrário, o investigador não será capaz de fazer uso da evidência se não obter métodos para recuperar a informação escondida no outro arquivo.

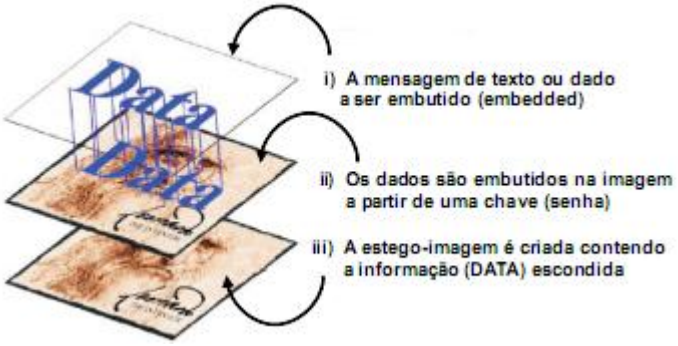

Figura 1 – Exemplo de ocultamento de uma mensagem (ROCHA, 2004)

Outra maneira utilizada para esconder dados trata-se de fraquezas exploradas do protocolo TCP/IP (KESLER, 2007). Através de falhas de segurança deste protocolo, invasores conseguem omitir informações e assim são capazes de criar um canal de comunicação encoberto em redes públicas e privadas. Espaços desalocados em setores como áreas localizadas no MBR (The Master Boot Record) e na BIOS (Basic Input/ Output System)

também permitem o armazenamento oculto de dados e, além disso, aceitam dados criptografados.

Profissionais habilidosos de Forense Computacional conseguem descobrir informações escondidas em espaços desalocados utilizando ferramentas adequadas, porém dados omitidos são mais difíceis de ser encontrados e também de ser utilizados como evidências em audiências não-técnicas (KESLER, 2007).

3.1.2 Limpeza de rastros

A procura por softwares de exclusão de rastros tem crescido ao longo dos anos. Muitos softwares disponíveis são capazes de zerar e sobrescrever arquivos de dados. Sendo assim, essas ferramentas utilizam múltiplos processos de escritas e conseqüentemente qualquer tentativa de recuperação se torna impraticável ou até impossível de ser realizada (KESLER, 2007).

Entretanto, os softwares utilizados pelos criminosos para limpar seus rastros não são perfeitos e podem criar uma trilha de vestígios adicionais (CARVEY, 2007). Além disso, muitas destas ferramentas não cumprem tudo o que prometem fazer e freqüentemente deixam para trás rastros como nome e tamanho do arquivo, data de criação e exclusão dos arquivos removidos, dentre outros dados que podem identificar os invasores (BURKE, 2006).

3.1.3 Uso de RootKits

Desde a década de 80 foram desenvolvidos programas para ocultar a presença de atacantes em um sistema computacional e também permitir seu acesso futuro a esse sistema (PEREIRA, 2007). Sendo assim, programas (ou com um conjunto de programas) com este propósito denominam-se *rootkit*. Atualmente, eles podem ser divididos como tradicionais ou baseados em Loadable Kernel Modules (LKM) (KLAUS, 2001).

Os *rootkits* tradicionais são aqueles que possuem versões de comandos do sistema alterados, sendo que esses comandos servem para ocultar informações dos processos, os arquivos e as conexões utilizados pelo atacante (KLAUS, 2001). Por meio de programas específicos, profissionais da Forense Computacional conseguem neutralizar *rootkits* tradicionais através do monitoramento do sistema computacional atacado e do armazenamento das informações do mesmo. Caso exista algum arquivo alterado ao longo do tempo, o programa identifica essa modificação e aponta a possibilidade do sistema estar comprometido (PEREIRA, 2007).

A partir do ano de 1997 surgiram os *rootkits* baseados em LKM. Esses programas conseguem alterar dinamicamente os módulos do núcleo do sistema operacional porque são capazes de modificar as chamadas de sistema. Sendo assim, estes programas maliciosos modificam a funcionalidade de um sistema sem a necessidade de uma reinicialização do mesmo (PEREIRA, 2007).

Conseqüentemente, a detecção dos *rootkits* não tradicionais é extremamente mais complexa porque os comandos do sistema continuam funcionando e o próprio núcleo do sistema responde às requisições realizadas (PEREIRA, 2007).

4. Ferramentas de Forense Computacional

No processo de investigação forense existem diferentes tipos de tarefas de realização essencial. Além das ações de confeccionar cópias de segurança de evidências, documentação, pesquisa e outros processos como esses, o investigador precisa de softwares específicos para

realizar tarefas forenses. Como requisitos destas ferramentas podem ser citadas a garantia de acesso a informações que possam ter sido excluídas ou possam estar escondidas, além do manejo de arquivos criptografados e armazenados em espaços não-alocados (LAWRENCE, 2009).

Entretanto, a maioria dos softwares possui algumas falhas. Sabe-se que existem setores no disco rígido que podem ser utilizadas para esconder dados, como por exemplo, as áreas conhecidas como Host Protected Areas (HPA) e Device Configuration Overlays (DCO) (GUPTA, 2006). Estes setores são desafios para a investigação digital porque diversas ferramentas amplamente utilizadas pelos peritos não são capazes de detectar intrusões nestas áreas, como o software Sleuth Kit e a versão 4.18a do Encase rodando em ambiente Windows (GUPTA, 2006). Dessa maneira, técnicas da Anti-forense se aproveitam destas falhas do sistema operacional para realizarem atos ilícitos.

A seguir comenta-se sobre algumas ferramentas forenses comerciais e livres que são populares dentre os investigadores de vários países.

4.1 Encase

O software EnCase trata-se de um conjunto de ferramentas baseadas em interface gráfica Windows (GUI), como pode ser visualizado na Figura 2. Apesar do custo altíssimo, esta ferramenta é a mais popular entre os investigadores em diversos países (GARBER, 2001).

Pode-se citar como uma das principais vantagens no uso do Encase a sua documentação clara, extensa e cheia de ilustrações (LAWRENCE, 2009). (LAWRENCE, 2009). A interface organizada permite ao usuário visualizar os dados através de três maneiras diferentes, sendo que essas visões incluem galerias de fotos e imagens de evidências. O software EnCase Forensic também pode ser utilizado para analisar diferentes tipos de mídias como *Palm tops* e a maioria de unidades removíveis (LAWRENCE, 2009).

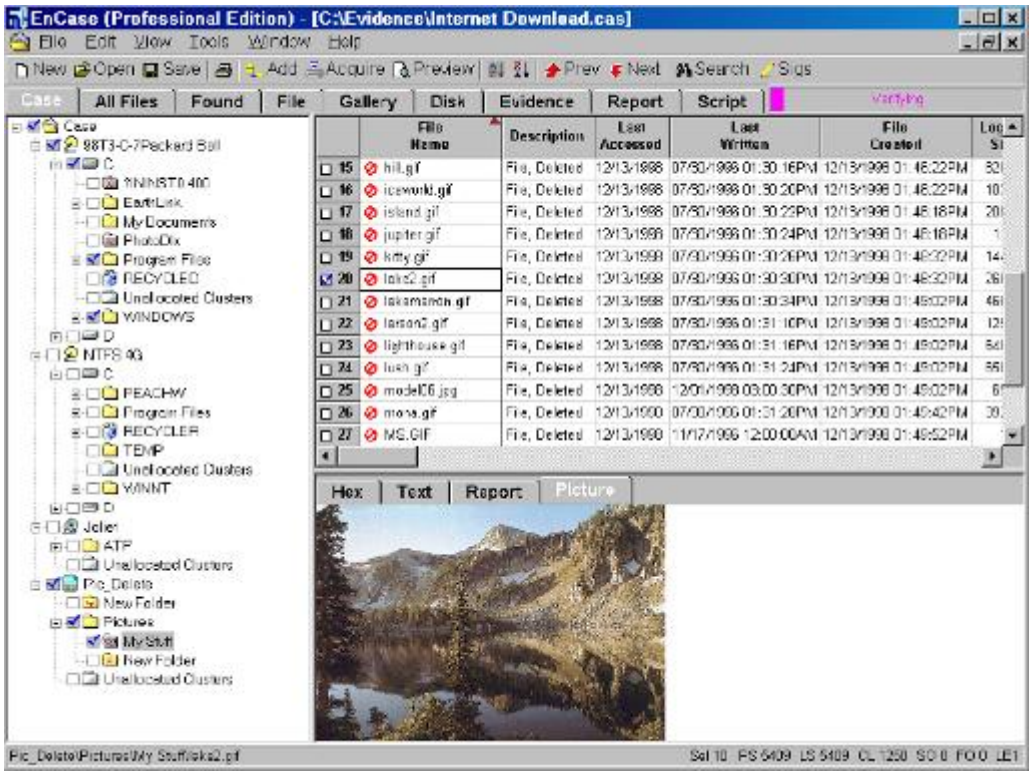

Figura 2 – A Interface gráfica do EnCase Forensic (GARBER, 2001).

Graças à completude deste excelente conjunto de ferramentas forense, as fases de criação de imagens, visualização e aquisição de vestígios, verificação, recuperação, análise, preservação e documentação das evidências coletadas podem ser realizadas (CASEY, 2000).

4.2 AccessData Forensic Toolkit

O software AccessData Forensic Toolkit, também conhecido como FTK, é considerado de fácil utilização para profissionais que estão familiarizados com ferramentas forenses (LAWRENCE, 2009). Este conjunto comercial de ferramentas além de conter limpadores de mídias, que são utilizados para salvar imagens de discos rígidos em mídias removíveis de maneira limpa e íntegra, possui programas para recuperação de dados e discos, assim como e visualizadores de registros e outros utilitários (LAWRENCE, 2009).

O FTK pode ser utilizado apenas em plataforma Windows e Linux, sendo que desse modo apresenta uma desvantagem se comparado a outros softwares que suportam mais modelos de sistemas de arquivos. Além do software possuir sua própria ferramenta para criação de imagens, o FTK pode ler imagens produzidas pelo Encase, pelo Linux DD, Safeback e outros softwares forenses (LAWRENCE, 2009).

O perito pode utilizar o FTK para realizar as tarefas correspondentes as fases de Aquisição, Análise, Preservação e Documentação do processo de investigação forense.

4.4 Sleuth Kit

O Sleuth Kit (TSK) também é um conjunto de ferramentas de código aberto e foi desenvolvido com base no software The Coroner's Toolkit (TCT) (LIMA, 2009). Este toolkit foi desenvolvido estritamente para rodar em plataforma Unix/Linux (LAWRENCE, 2009). O desempenho deste conjunto de ferramentas é considerado alto e de qualidade similar a sistemas forenses comerciais. Entretanto, não existe suporte direto, exceto contato através do e-mail do desenvolvedor da ferramenta (LAWRENCE, 2009).

O TSK tem ênfase em análise Postmortem, porém foi desenvolvido com a finalidade de evitar alterações durante a execução de suas funcionalidades, desse modo permitindo o seu uso com o computador investigado ainda ligado (LIMA, 2009). A recuperação de arquivos apagados, exibição de informações do sistema de arquivos e de dados sobre tempos de acesso são funcionalidades do TSK.

4.3 Helix

Os investigadores de crimes digitais necessitam do auxílio de softwares para a aquisição de vestígios da máquina suspeita. Desse modo, os profissionais precisam adquirir estes programas e levá-los a cena do crime. Além disso, podem ocorrer problemas de incompatibilidade com o sistema operacional do computador a ser investigado ou outros imprevistos que resultam em atrasos e desperdício de tempo durante o processo investigativo (IEONG, 2006). Uma opção para facilitar as tarefas do investigador e otimizar a coleta de dados é o uso de ferramentas do sistema operacional Linux do tipo Live CD, que possibilita utilizar completamente este sistema operacional sem precisar instalá-lo na máquina analisada (IEONG, 2006).

Uma das distribuições do sistema operacional Linux mais populares entre os profissionais da Forense Computacional trata-se da Helix (IEONG, 2006). Esta distribuição trata-se de um conjunto de ferramentas que é considerado poderoso e facilita a interação com o usuário graças a sua interface GUI. Programas de análise forense como o Windows Forensics Toolchest (WFT), Incident Response Collection Report (IRCR) e o First Responders

Evidence Disk (FRED) estão incluídas na Helix e podem ser executadas instantaneamente, sem a necessidade de extrair arquivos ou tarefas adicionais (IEONG, 2006).

A ferramenta WFT foi criada por Monty McODougal em 2003, sendo esta considerada a mais completa e sofisticada dentre os programas forenses da época (IEONG, 2006). Além de analisar dados da memória, informações do sistema, número de portas, processos em execução, usuários registrados, configurações de rede e todos os outros dados que as ferramentas FRED e IRCR também analisam, o WFT contém um gerador de relatórios no formato HTML, o qual facilita ainda mais o trabalho do perito forense (IEONG, 2006).

5.Estudo de caso

Muitos investigadores e estudantes de Forense Computacional disponibilizam em diversos web sites e fóruns de discussão imagens de mídias digitais relacionadas a casos reais de investigação forense. Uma conhecida fonte de evidências digitais documentadas para estudo e simulações se trata do Computer Forensic Reference Data Sets (CFReDS) , um projeto do National Institute of Standards and Technology (NIST) (CFREDS, 2010). O CFReDS disponibiliza livremente um repositório com diversos documentos e evidências digitais para simulação de investigações.

Neste capítulo serão apresentadas informações sobre uma investigação realizada em uma mídia disponibilizada pelo projeto CFReDS (CFREDS, 2010). As ferramentas definidas para estudo no presente trabalho, Encase, Helix,FTK e Sleuth Kit serão utilizadas neste processo investigativo.

5.1 Caso Greg Schardt: ataque a redes wireless

Em setembro de 2009 um notebook Dell foi encontrado abandonado com um cartão wireless PCMCIA e uma antena do modelo 802.11b feita em casa. Suspeitou-se que o computador foi utilizado para ações de propósito hacker. O computador pertencia a Greg Shardt, o qual possuía o nome de "Mr.Evil" para ações on-line. Alguns dos conhecidos de Shardt afirmaram que o mesmo estacionava seu veículo em áreas com acesso gratuito a internet sem fio, onde ele poderia interceptar o tráfego da rede, desse modo capturando dados como senhas e números de cartões de crédito.

Para incriminar o suspeito Greg Shardt, necessita-se de evidências como informações e datas que comprovassem que ele utilizava a máquina para propósitos ilícitos, como o uso de softwares de natureza hacker, por exemplo. O processo de análise e coleta de vestígios será apresentado a seguir:

5.2 Processo investigativo

Após o download dos arquivos de imagens do HD a ser analisado no caso a partir do web site da CFReDS utilizou-se algoritmo *hash* MD5 com o auxílio das ferramentas forenses. O resultado obtido pelo algoritmo é a *string* AEE4FCD9301C03B3B054623CA261959A, a qual é a mesma que a string disponibilizada no web site (CFREDS, 2010).

Para ter acesso aos arquivos do disco rígido, as partições contidas na imagem do disco rígido precisam ser montadas. A Figura 3 apresenta o diretório principal do disco que obtido após o processo de montagem.

Através das ferramentas na fase de análise verificou-se que o sistema operacional Windows XP estava instalado na máquina, a qual estava registrada no nome de Greg Schardt.

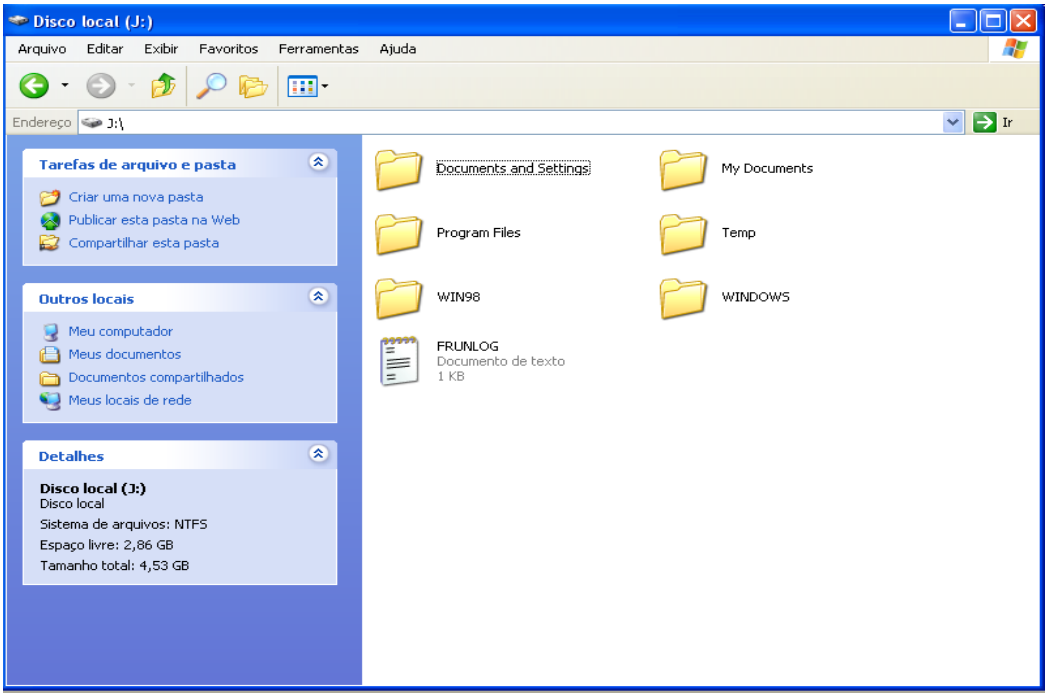

Figura 3 – Visualização do disco rígido montado

A análise dos softwares instalados demonstrou a presença de softwares de natureza hacker, como: Cain & Abel v2.5 beta45, Ethereal (atualmente chamado Wireshark), 123 Write All Stored Passwords,Anonymizer , CuteFTP ,Look&LAN_1.0 e NetStumbler. Outra informação obtida na análise é a presença de arquivos executáveis na lixeira do computador e também a existência de infecção de vírus no computador de Greg Schardt.

Além disso, encontrou-se um arquivo de texto chamado Interception na pasta \My Documents directory. Este arquivo de texto foi criado após o uso do software Ethereal e contém muitas informações relacionadas a quem e o que tipo de computador que foi interceptado. Desse modo, analisando o arquivo verifica-se que um computador de bolso (*Pocket PC*) foi atacado e o sistema operacional utilizado pela vítima do ataque é o Windows CE. Além disso, durante o ataque a vítima estava acessando os web sites Mobile.msn.com e Hotmail.com.

Portanto, através dos vestígios encontrados nos arquivos analisados comprova-se que o proprietário do computador realmente o utilizou para propósitos de natureza ilícita e que conseguem interceptar os dados que estavam trafegando na rede *wireless* aberta do local onde foi encontrado o computador.

5.3 Desempenho das ferramentas utilizadas

Estudos de outras imagens serão realizados, porém com a investigação deste caso, diversas características das ferramentas puderam ser definidas. Como pode ser visualizado no Quadro 1, as ferramentas Encase e a FTK possuem a desvantagem de terem custo alto, mas apresentam diversos benefícios, como: documentação gerada automaticamente, busca de arquivos escondidos em áreas protegidas e não alocadas, filtro de arquivos criptografados, etc. Entretanto, de acordo com o quadro comparativo (Quadro 1), a ferramenta FTK apresenta 80% dos requisitos que foram analisados, sendo que a Encase apresenta apenas 50%. Além disso, a interface gráfica da FTK pode ser considerada mais agradável e fácil de usar em comparação a interface do software Encase.

Já a versão free da Helix apresentou benefícios excelentes, sendo que 90% dos requisitos analisados foram verificados nesta ferramenta. A ferramenta TSK possui diversas funcionalidades, porém apresentou apenas 30% dos requisitos analisados em todas as ferramentas. Portanto, conclui-se que a utilização de ferramentas livres como a Helix por profissionais na investigação digital é uma opção segura, estável, ágil e econômica.

Quadro 1- Comparativo das ferramentas analisadas

Ferramentas/ Características	Encase	Helix	FTK	TSK
Licença *free*		X		X
Facilidade de uso		X	X	
Interface Gráfica fácil		X	X	
Busca de arquivos em áreas protegidas, escondidas e não alocadas	X	X	X	
Filtro de arquivos criptografados	X		X	
Visualização do registro do sistema operacional	X	X	X	X
Geração automática de relatórios	X	X	X	
Extração de arquivos e pastas		X	X	
Suporte a boot	X	X		
Suporte a grande quantidade de dados		X	X	X

6. Conclusão

A pesquisa sobre Forense Computacional é uma área bastante atual. Com a expansão da Internet e, conseqüentemente, com aumento de crimes eletrônicos surgem inúmeras questões sem respostas, sendo que a quantidade de profissionais desta área não é suficiente para apurar os atos ilícitos cometidos diariamente em vários países.

Através do estudo realizado e dos experimentos em andamento, pode-se verificar a existência de ferramentas que facilitam e otimizam as tarefas executadas pelos profissionais de Forense Computacional. Por outro lado, por meio da pesquisa de técnicas utilizadas para dificultar o

trabalho dos peritos, percebe-se que assim como acontece com os softwares de Forense, as ferramentas de Anti-forense também devem ser estudadas com a finalidade de aprender como os criminosos agem e desta forma conseguir obter evidências significativas, até em situações onde a maioria dos vestígios possam ter sido danificados.

Após a investigação do caso estudado verificou-se que a investigação forense não é um processo trivial, assim tarefas podem exigir tempo e conhecimento. Conclui-se que a ferramenta comercial FTK apresentou quantidade superior de recursos em comparação com o software Encase. No caso dos softwares livres aqui apresentados, o conjunto de ferramentas Helix pode ser considerado mais econômico e apresenta recursos suficientes para auxiliar o investigador nas diversas tarefas necessárias na apuração de crimes eletrônicos.

Referências

ADELSTEIN, F. *Live Forensics: Diagnosing your system without killing it first* .Communications of the ACM 49(2), 63-66, 2006.

ARTHUR, K. K. *An Investigation Into Computer Forensic Tools*. Acessado em Abril 2, 2010, disponível em http://www.infosecsa.co.za/proceedings2004/060.pdf, 2004.

BARYAMUREEBA V, TUSHABE F. *The Enhanced Digital Investigation Process Model***.** Institute of Computer Science, Makerere University, Uganda, 2004.

BURKE,P. , CRAIGER, P ; *Assessing trace evidence left by secure deletion programs*, in Advances in Digital Forensics II,M. Olivier and S. Shenoi (Eds.), Springer, New York, pp. 185-195, 2006.

CALOYANNIDES, M. A. *Computer Forensics and Privacy*. Artech House, Inc. 2001.CARRIER, B., SPAFFORD, E. H. *Getting Physical with the Digital Investigation Process*. International Journal of Digital Evidence, Fall 2003, Volume 2, Issue 2, 2003.

CARVEY, H. *Windows Forensic Analysis*. DVD Tolkit. Syngress Publishing, Inc, 2007.

CASEY, E. *Handbook of computer crime investigation : forensic tools and technology*. San Diego, Calif.: Academic Press, 2002.

CFReDS. *The CFReDS Project*. http:// www.cfreds.nist.gov. Acesso em: 17 ab. 2010.**CRAIGER, P.,WAUGER,J.,MARBERRY,C. et al**. *Validation of Digital Forensics Tools*. IDEA Group Publishing, 2006.

CUMMINGS,T. *The History of Computer Forensics*. Disponível em: <http://www.ehow.com/about_5813564_history-computer-forensics.html>. Acesso em: 05 abril 2010.

EOGHAN C. *Handbook of computer crime investigation*. Academic Press, San Diego, California, 2002.

FREITAS,A. R. *Perícia Forense Aplicada à Informática*. Rio de Janeiro: Brasport,. 240 p. 2006.

GARBER ,L. *EnCase: A Case Study in Computer-Forensic Technology***.** IEEE Computer Magazine January, 2001. **GEIGER, M.** *Evaluating Commercial Counter-Forensic Tools*. Digital Forensics Research Conference,New Orleans,2005.

GUPTA, Mayank R. et al. *Hidden Disk Areas: HPA and DCO.*. Internacional Journal of Digital Evidence. Fall 2006, Volume 5, Issue 1. Disponível em: http://www.utica.edu/academic/institutes/ecii/ publications/articles/EFE36584-D13F-2962-67BEB146864A2671.pdf, Acesso em 28 abril 2010, 2006.

IEONG R. S. C. *Freeware Live Forensic tools evaluation and operation tips*. 4th Australian Digital Forensic Conference,2006,Information Systems, Vol. 12, 2006.

KESSLER, G. *Anti-Forensics and the Digital Investigator*. Disponível em http://scissec.scis.ecu.edu.au/ conference_proceedings 2007/forensics/01_Kessler_Anti-Forensics.pdf. Acesso em 28 abril 2010, 2007.

KLAUS, S. and NELSON, M. Métodos *para detecção localde rootkits e módulos de kernel maliciosos em sistemas unix*. In III Simpósio sobreSegurança em Informática (SSI), São José dos Campos, SP, 2001.

LAWRENCE ,K. R. *Tools for Computer Forensics: A Review and Future Works*. Proceedings of the 47th Annual Southeast Regional Conference, 2009, Clemson, South Carolina, USA, March 19-21, 2009.

LIMA, A. D. L. FARO. *Ferramenta de análise forense computacional em sistemas Linux vivos*. In: XIX Congresso de Iniciação Científica., 2009, Natal. Anais do CIC 2009, 2009.

PALMER, G. and CORPORATION, M. *A road map for digital forensic research*. Technical report, 2001.

PEREIRA, E; FAGUNDES, L; NEUKAMP, P et al. *Forense Computacional: fundamentos, tecnologias e desafios atuais*. Em VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, p. 3-53, Rio de Janeiro, RJ, 2007.

REIS, M. A. *Forense computacional e sua aplicação em segurança imunológica*. Dissertação de mestrado, Instituto de Computação, Universidade Estadual de Campinas, 2003.

ROCHA, A; GOLDENSTEIN,S. ; COSTA, H. and CHAVES, L. M. *Segurança e privacidade na internet por esteganografia em imagens*. In Webmedia & LA Web Joint Conference 2004,2004.

ROGERS, M. *Panel session at CERIAS 2006*. Information Security Symposium. Disponível em http://www.cerias.purdue.edu/symposium/2006/materials/pdfs/antiforensics.pdf. Acesso em 31 Maio 2010, 2006.