Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis - IMESA

Diego Zaratini Constantino

Técnicas da Computação Forense

Assis 2012

Diego Zaratini Constantino

Técnicas da Computação Forense

Trabalho de Conclusão de Curso de Bacharelado em Ciência da Computação do Instituto de Ensino Superior de Assis (IMESA) e Fundação Educacional do Município de Assis (FEMA).

Orientando: Diego Zaratini Constantino

Orientador: Prof. Guilherme de Cleva Farto

Avaliador: Prof. Ms. Osmar Aparecido Machado

Assis 2012

FICHA CATALOGRÁFICA

Zaratini, Diego Constantino

Técnicas da Computação Forense / Diego Zaratini Constantino. Fundação Educacional do Município de Assis – FEMA – Assis, 2012.

67 pág.

Orientador: Guilherme de Cleva Farto

Trabalho de Conclusão de Cursos (TCC) – Instituto Municipal de Ensino Superior de Assis – IMESA.

1. Computação Forense. 2. Técnicas Periciais. 3. Laudo Pericial

CDD: 001.6

Biblioteca FEMA

Agradecimentos

Agradeço a Deus por iluminar meu caminho durante essa jornada de 4 anos e permitir que chegasse ao final de mais essa conquista. À professora Regina Fumie Eto, que aceitou a proposta de realizar este trabalho, também ao professor Guilherme de Cleva Farto por aceitar dar continuidade ao trabalho e a todos os amigos e familiares que apoiaram e deram força para mais esta conquista.

Não faz sentido olhar para trás e pensar: devia ter feito isso ou aquilo, devia ter estado lá. Isso não importa. Vamos inventar o amanhã, e parar de nos preocupar com o passado.

Steve Jobs

RESUMO

O avanço e modernização das tecnologias resultam em maiores facilidades e possibilitam um leque de opções em usabilidade para usuários de todo o mundo, que variam de entretenimento, aspectos profissionais e pessoais. Com isso, grande parte da população, sempre que possível, fica conectada à rede mundial, Internet, de modo que a cada dia esse número vem aumentando e tornando indispensável a utilização da mesma em suas atividades.

O aumento significativo no uso de tais tecnologias faz com que muitos desses usuários tornem-se vulneráveis à ação de criminosos, que atuam no roubo de informações e arquivos que transitam no meio digital. Diante desde contexto surgem as técnicas periciais da computação forense com objetivo de atuar na busca desses criminosos.

Palavras Chave: Computação Forense; Técnicas Periciais; Laudo Pericial

ABSTRACT

The advancement and modernization of technologies result in more facilities and enable a range of options in usability for worldwide users, ranging from entertainment, professional and personal aspects. With so much of the population wherever possible is connected to the global network, the Internet, so that each day that number is increasing and becoming indispensable to use it in their activities.

This significant increase in the use of such technologies is making many of these users become vulnerable to the actions of criminals who operate in the theft of information and files that travel in the digital environment. Given the context arise from the techniques inside the computer forensics expert to act in pursuit of these criminals.

Keywords: Computer Forensics; Technical Expert; Forensics Report

Lista de Figuras

Lista de Tabelas

SUMÁRIO

Capítulo 1 – INTRODUÇÃO

Dispositivos eletrônicos, como smartphones, notebooks, tablets, entre outros, tornaram-se fundamentais no cotidiano de milhares de pessoas, possibilitando uma maior facilidade em executar tarefas e realizar atividades rotineiras.

Cada vez mais pessoas utilizam desses meios eletrônicos para realizar suas tarefas como compras on-line, pagamentos de contas, transferência bancária, redes sociais, entre outras. Com o crescimento e popularização dessas tecnologias, os crimes ligados à essa área também aumentam. Devido a tais fatores, a área da Computação Forense também tem crescido nos campos de estudo tecnológicos.

O estudo da computação forense permite identificar criminosos cibernéticos, também conhecidos como crackers, com a finalidade de coletar provas que possam comprovar os crimes cometidos por eles. Esse estudo deve ser realizado por profissionais graduados na área tecnológica como Ciências da Computação, Análise e Desenvolvimento de Sistemas e outros cursos na área de Tecnologia da Informação e de Software.

Este trabalho tem como objetivo apresentar, de maneira detalhada, as etapas realizadas em uma análise computacional forense, demonstrando as principais ferramentas utilizadas por peritos, assim como algumas ferramentas de software livre disponíveis.

1.1. Motivação

O estudo da computação forense está em crescimento, onde novas técnicas e métodos são necessárias para conter ou lidar com os meios utilizados por criminosos. A partir disso, o foco na área de segurança da informação é fundamental para que qualquer empresa possa avaliar e testar suas estruturas de segurança, assim como verificar se há vazamento de informações de dentro de suas

dependências.

É uma área comumente esquecida e até recusada por profissionais da área de Ciência da Computação e carente de leis específicas que abordam, especialmente, crimes digitais.

1.2. Contextualização

A necessidade de um maior conhecimento dos profissionais da área tecnológica em segurança e o crescimento dos conceitos sobre computação forense tornaram-se fundamentais para o desenvolvimento deste trabalho. Serão abordados as técnicas e metodologia de uma análise forense, iniciando-se pela coleta dos materiais e equipamentos até à extração de arquivos e dados e também a confecção final de um laudo pericial a partir de um estudo de caso.

1.3. Estrutura do Trabalho

O trabalho é dividido em seis capítulos conforme definido abaixo:

Capítulo 1: Introdução

Na introdução é realizada uma descrição sobre o que o trabalho aborda, assim como o tema e os objetivos.

Capítulo 2: Definições e Ferramentas da Computação Forense

No segundo capítulo definem-se os conceitos e métodos utilizados em análises forenses. Também são apresentadas as diversas ferramentas disponíveis: as mais utilizadas por peritos, as restritas e as disponíveis por meio de software livre.

Capítulo 3: Técnicas utilizadas

No terceiro e principal capítulo são abordadas todas as fases de uma análise, detalhando exatamente os procedimentos corretos e legais que devem ser seguidos, além de exemplificar a utilização das ferramentas.

Capítulo 4: Procedimentos e Métodos de analise

Neste capítulo serão conceituados alguns métodos básicos que auxiliam o perito na análise de um material.

Capítulo 5: Exemplo de Laudo Pericial

No quinto capítulo é exemplificada a elaboração de um relatório final, também chamado de laudo pericial, após a conclusão da análise nos equipamentos examinados.

Capítulo 6: Conclusão

No sexto e último capítulo deste trabalho são apresentadas as conclusões de todo o estudo realizado de forma a esclarecer os pontos questionados durante o desenvolvimento.

Capítulo 2 – DEFINIÇÕES E FERRAMENTAS DA COMPUTAÇÃO FORENSE

Antes de definir computação forense é importante definir o termo “forense”. Segundo o US-CERT [1], forense é o processo de usar conhecimento científico para a recolha, análise e apresentação de provas aos tribunais.

Define-se como computação forense, de acordo com Steve Hailey, Cybersecurityt Institute, “Preservação identificação, coleta, interpretação e documentação de evidências computacionais, incluindo as regras de evidência, processo legal, integridade da evidência, relatório fatual da evidência e provisão de opinião de especialista em uma côrte judicial, outro tipo de processo administrativo ou legal com relação ao que foi encontrado”. São a utilização de técnicas científicas e específicas nos meios tecnológicos e digitais, como por exemplo, exames em HD [2] pen-drive, Mídias Digitais, celulares, entre outras. Os profissionais nessa área são chamados *Peritos Criminais.*

O processo de perícia ou análise forense em equipamentos, principalmente em dispositivos de armazenamento está divido em quatro fases: preservação, extração, análise e formalização, ambas detalhadas no terceiro capítulo, de modo que todas elas devem ser seguidas com rigor para que as evidências encontradas tenham valor em juízo.

2.1. Ferramentas Forense

Atualmente há diversas ferramentas, tanto para software quanto para hardware, disponíveis para uso dos peritos. Entre algumas, é comum o uso de ferramentas multiplataforma, funcionando de forma eficiente em ambientes Windows ou Linux, sendo elas softwares livre ou não. As principais e mais utilizadas são fechadas para

1 Departamento de Segurança Interna dos Estados Unidos
2 Hard Disk ou Disco Rígido

uso exclusivo da polícia e algumas instituições de perícia.

2.1.1. Ferramentas de Hardware

As ferramentas de hardware são necessárias em uma análise forense para evitar que dados sejam apagados, alterados ou corrompidos de algum dispositivo que está sendo analisado. São conhecidos como bloqueados de escritas, permitindo ao perito fazer uma cópia exata desse dispositivo em outros, por exemplo, o espelhamento de um Hard Disk (HD) para outro, desse modo o perito pode fazer suas análises sem se preocupar com uma possível alteração indevida no equipamento original.

Outras vantagens da utilização desses bloqueadores são uma maior velocidade na transferência de dados, possibilidade de ter vários HDs conectados e não precisar, necessariamente, de um computador para realizar essas ações de cópias. No mercado estão disponíveis alguns, destacando-se Logicube Forensic Quest (Figura 2), Intelligent Computer Solutions Solo (Figura 1), entre outros.

Figura 1 – Solo III, com HDs conectados

Figura 2 – Logicube Forensic Quest

2.1.2. Ferramentas de Software

Os processos de escrita e gravação podem ser realizados na ausência de aplicações bloqueadoras, portanto, existem softwares que possibilitam a cópia de dispositivos de forma segura, sem o risco de alterar o equipamento analisado, porém a utilização desses softwares requer uma atenção maior do perito, pois é importante não confundir a operação de espelhamento, onde é selecionado o HD a ser copiado e o HD que receberá a cópia. Esse processo dever ser feito por softwares que não acessem o HD durante sua inicialização ou utilização durante o processo de cópia.

Um dos principais e mais conhecido desses tipos de software é o Symantec Norton Ghost, Figura 3. O computador é ligado e o programa é carregado por meio do uso de um *pen-drive*, CD/DVD ou até mesmo por um disquete, sem que haja a necessidade de carregar o sistema operacional. A partir disso, o disco pode ser espelhado (Figura 4) para outro.

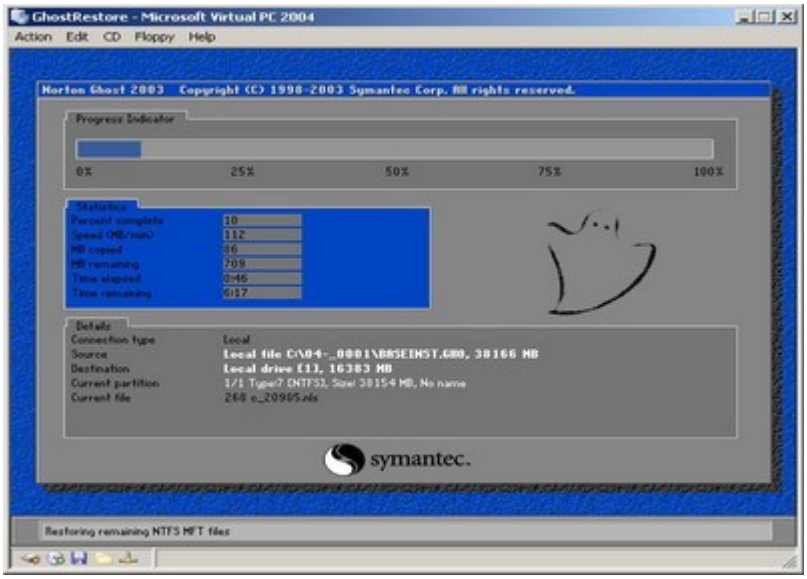

Figura 3 – Interface Symantec Norton Ghost

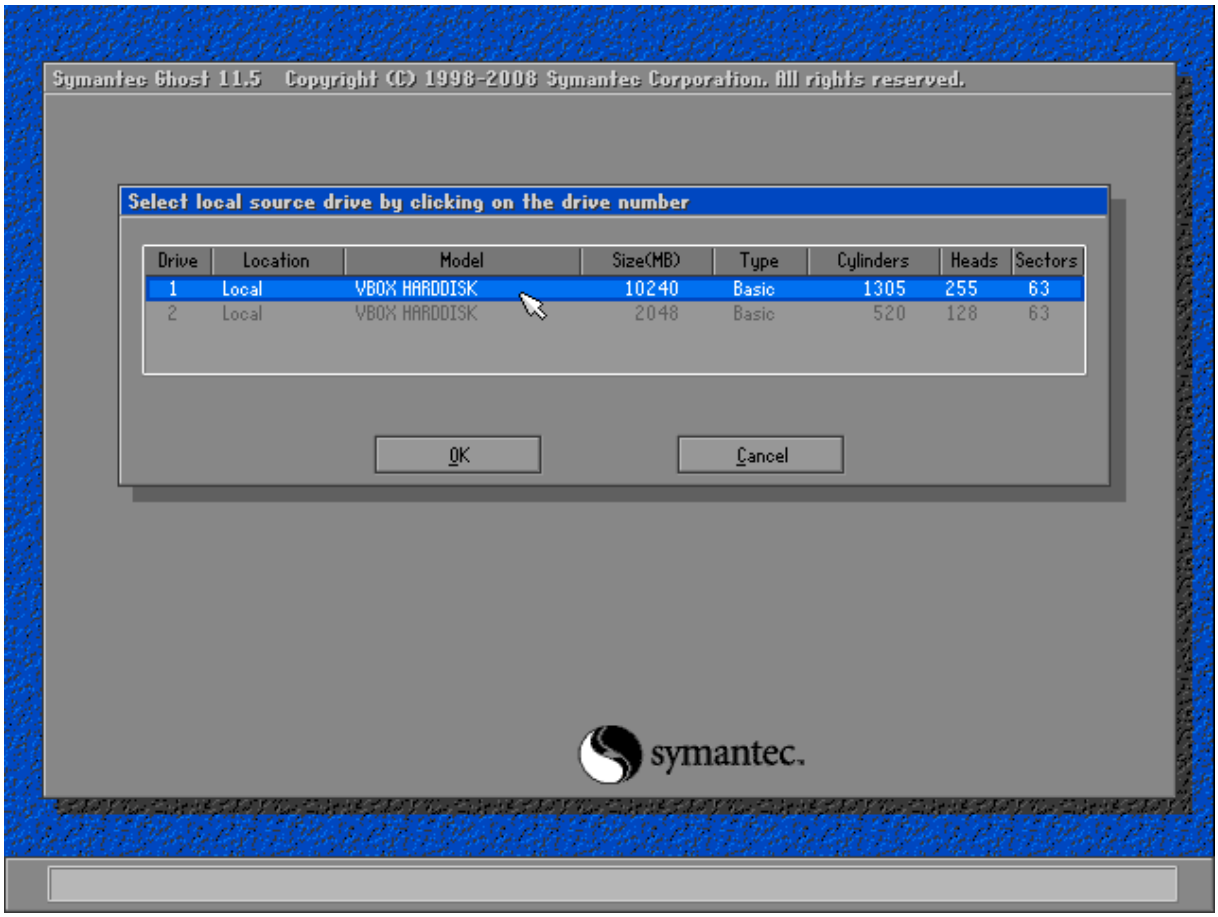

Figura 4 – Dispositivos a serem espelhados

Outra maneira de realizar a duplicação de HDs com o uso de softwares é por meio de sistemas operacionais de forma read-only, como, por exemplo, o KNOPPIX

(Figura 5), que é um sistema operacional GNU/Linux baseado no *kernel* do Debian. A principal característica é a inicialização *live*, onde não é necessário a instalação do sistema no computador, podendo ser inicializado por meio de CD, DVD e dispositivos *flash* como *pen-drive*. A interface padrão é o LXDE. Com o comando *dd* (*duplicate disc*) é possível fazer o espelhamento dos discos. A sintaxe do comando dd é: *dd <hd_origem> <hd_destino>* , onde o “hd_origem” é o HD original e o “hd_destino” o que receberá a cópia. Lembrando-se sempre, a importância de confundir a operação de espelhamento.

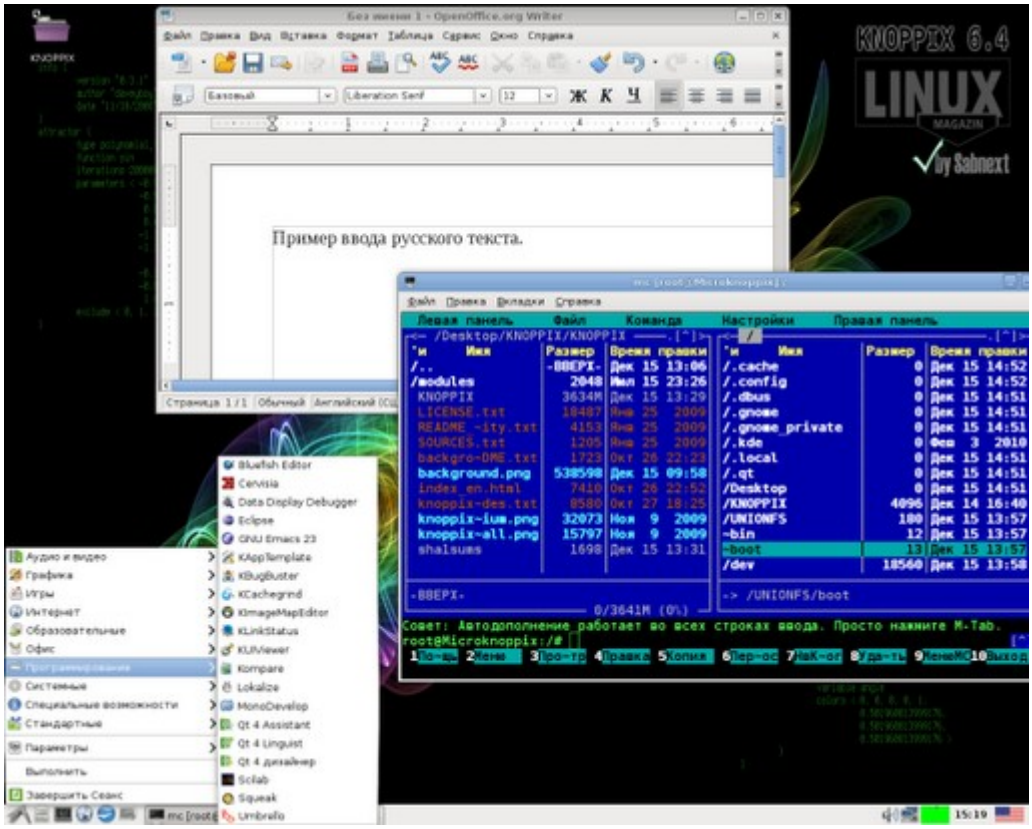

Figura 5 – Sistema KNOPPIX

Contudo, após o espelhamento e a cópia dos discos em questionamento, os peritos necessitam realizar uma análise em cada arquivo do disco. Para essa tarefa, há programas específicos, como o OSForensics (Figura 6), que é um utilitário gratuito para análises forense e, por meio, dele é possível obter várias informações como

senhas salvas e últimas atividades realizadas no computador, entretanto, a aplicação está disponível apenas para a plataforma Windows. Disponível para plataforma Linux há o Foremost, que é uma ferramenta mais limitada que outras disponíveis, sendo apenas possível a recuperação de arquivos excluídos. A configuração e instalação é realizada pelo terminal do sistema.

Figura 6 – Interface OSForensics

Alguns dos programas de software livre para análise forense são disponibilizados junto com o *kernel* do sistema operacional, como é o caso do Back Track (Figura 7), sistema baseado na distribuição Linux Ubuntu, possuindo uma extensa lista de programas já configurado e prontos para serem utilizados. Outra opção bastante eficiente e com as mesmas ferramentas é o Deft (Figura 8), também baseado no Ubuntu. Esses programas variam desde o espelhamento de disco, como análise e

mapeamento de host [3] na rede, recuperação de arquivos e senhas.

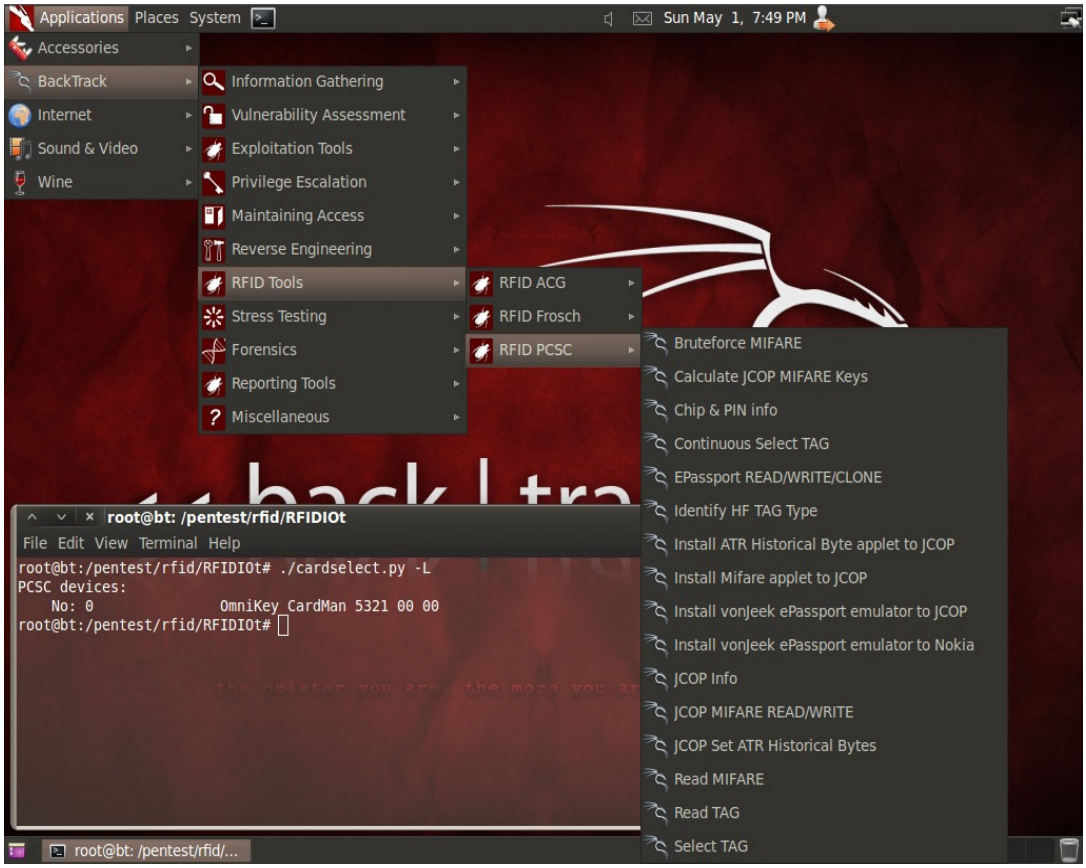

Figura 7 – Lista de ferramentas disponíveis no sistema Back Track

3 Nome definido para um computador conectado em uma rede

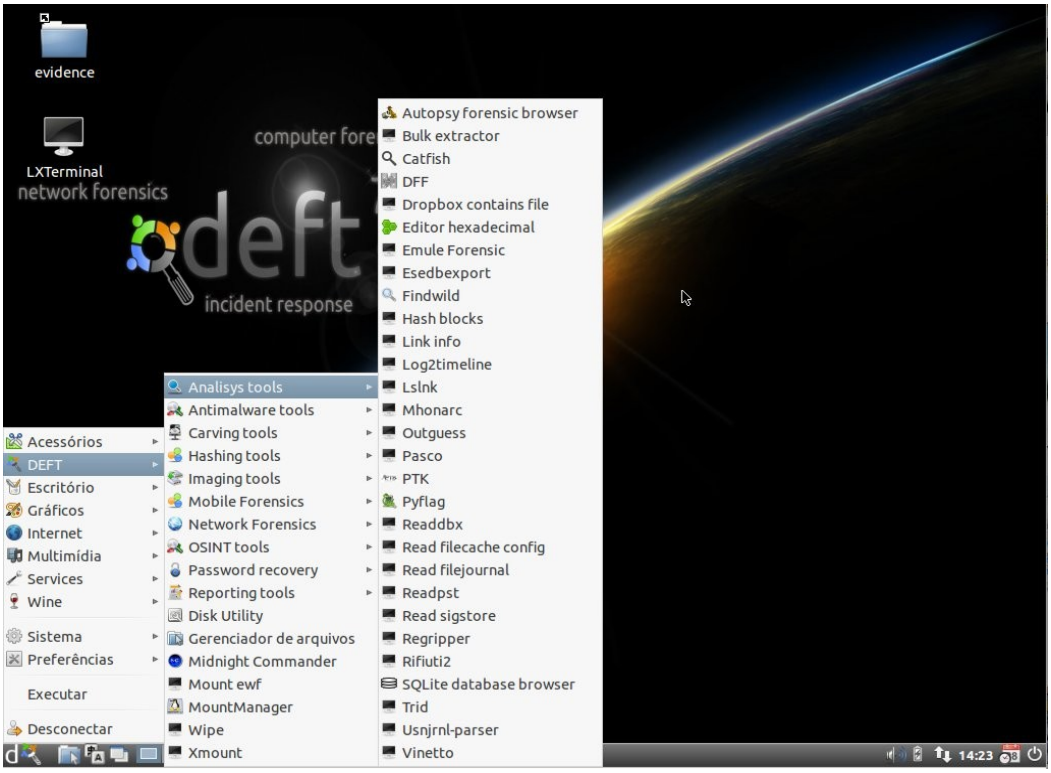

Figura 8 – Lista de ferramentas disponíveis no sistema Deft

As forças policias podem fazer uso de soluções computacionais mais específicas e de uso exclusivo, como exemplo a Encase, desenvolvida pela empresa Guidance, que é a ferramenta mais utilizada por peritos criminais. Está disponível apenas em ambientes com sistema Windows e é bastante conceituada e eficiente em perícias forenses. O perito tem a liberdade de desenvolver e implementar novas funções para o software original, de modo que facilite ou melhore seu modo de trabalhar de acordo com suas necessidades. É importante citar entre essas ferramentas uma outra desenvolvida por dois peritos do Mato Grosso do Sul, chamada NuDetective, “funciona por meio do reconhecimento automatizado de assinaturas de arquivos digitais. O software faz uma triagem na memória da máquina periciada em busca de conteúdos que indiquem a presença de material pornográfico. Em breve, uma nova versão vai reconhecer os padrões de imagens, tornando a varredura nos sistemas suspeitos ainda mais confiáveis e precisas” (LUIS SUCUPIRA , 2010).

Apresentadas algumas das ferramentas mais comuns, finalizamos este capítulo e damos início as técnicas utilizadas para análise.

Capítulo 3 – TÉCNICAS UTILIZADAS

Neste capítulo são tratados todos os processos necessários em uma análise forense, assim como etapas que caracterizam a perícia forense em computadores, celulares dispositivos de armazenamento, entre outros. Esses processos seguem uma padronização de análise onde os resultados devem ser obtidos da maneira mais simples e menos técnica possível, pois o relatório final da análise realizada pelo perito computacional será utilizado por promotores e juízes dos quais não possuem conhecimento avançado na área.

Para uma análise forense em quaisquer dos dispositivos citados anteriormente são necessários seguir quatro etapas: 1 – Preservação, 2 – Extração, 3 – Análise, 4 – Formalização. As etapas serão discutidas nas próximas seções deste trabalho. Há algumas entidades que trabalham na padronização desses termos como por exemplo International Organization on Computer Evidence (IOCE), principal entidade internacional e centralizadora dos esforços de padronização. O principal objetivo da IOCE é o de facilitar a troca de informações entre as diversas agências internacionais acerca de investigações de crimes envolvendo computadores e outros assuntos forenses relacionados ao meio eletrônico. No Brasil, há a Seção de Apuração de Crimes por Computador (SACC) , que atua junto ao Instituto Nacional de Criminalística/Polícia Federal, disponibilizando suporte técnico às investigações conduzidas em que a presença de materiais de informática é constatada [4].

3.1. Preservação

Nessa etapa o perito deve preservar as informações daquele dispositivo apreendido ou questionado. Esse procedimento consiste em realizar um espelhamento do disco ou dispositivo. O espelhamento consiste na cópia fiel e perfeita, ou seja, *bit* a *bit*, do material questionado. Conforme mencionado anteriormente, essa etapa é realizada por meio do uso de ferramentas já discutidas no segundo capítulo. O processo de

4 Forense Computacional: Aspectos Legais e Padronização.

preservação é fundamental e parte de algumas considerações como: o dispositivo que irá receber a cópia do material questionado deve ser do mesmo tamanho ou maior para que todos os dados sejam fielmente copiados. Ressalta-se que o tamanho dos discos, em caso de HDs, devem ser analisados pela Logic Block Addressing (LBA) [5], pois é possível que o tamanho citado na etiqueta do HD não seja realmente o tamanho real disponível.

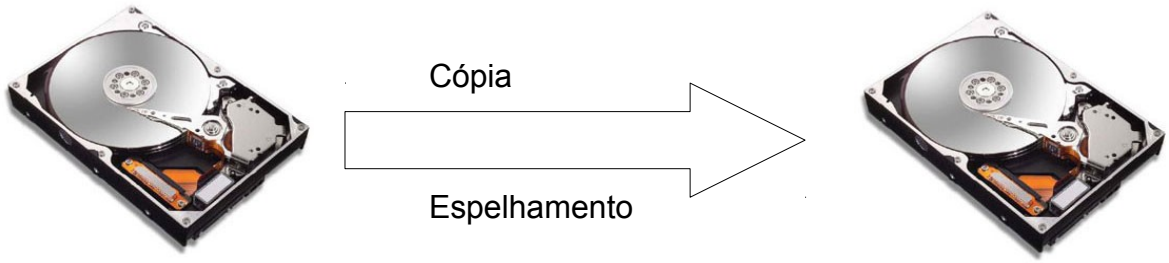

Figura 9 – Cópia dos Dados de HD para HD

Durante o processo de espelhamento, caso o dispositivo questionado esteja sendo copiado para um dispositivo de maior capacidade, torna-se necessário que os espaços não preenchidos durante a cópia sejam “zerados” para garantir que nenhum *bit* presente interfira no processo de análise. Para isso, deve-se utilizar uma técnica chamada de *wipe.* Aplicações como o *Zero Fill* são capazes de auxiliar esse processo.

O dispositivo questionado não necessariamente precisa ser copiado ou espelhado para outro HD, já que é possível gerar uma imagem desse dispositivo e, por meio dela, o perito poderá realizar as análises perfeitamente. Esse processo é bastante eficiente quando o dispositivo a ser analisado é muito grande, pois assim é possível gerar imagens de apenas partes do disco e em tamanhos menores, possibilitando uma análise ainda mais rápida desse disco. Alguns softwares são específicos para criação de imagens de disco como, por exemplo, o *Clonezilla,* em sistemas GNU/Linux (citados no segundo capítulo) que é utilizado para gerar essas imagens por meio do comando “*dd*” [6]*. A sintaxe para execução é:*

5 Endereçamento lógico de setores, faz com que o computador enderece cada setor do disco sequencialmente, ao invés da sua localização física de cilindro, cabeça e setor.

6 *DD - Duplicate Disk*

“dd if=<disco de origem> of=<disco de destino>”

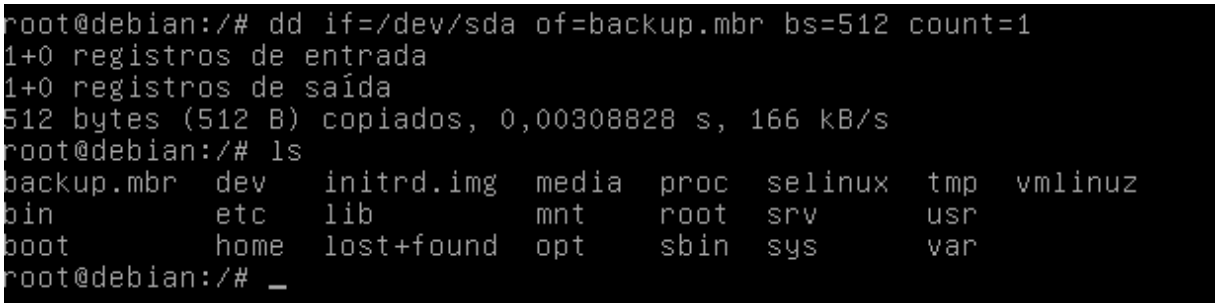

Figura 10 – Exemplo de execução do comando “dd” no sistema Debian

Onde “disco de origem” é o dispositivo questionado e disco de destino é o disco que receberá a imagem gerada. Dependendo do tamanho do disco, o perito deve julgar qual técnica deve ser utilizada para possibilitar uma análise mais eficiente.

Todos esses procedimentos são necessários para a preservação dos dados questionados, pois caso o perito cometa algum erro no qual venha a provocar perda ou alteração de informações, a investigação não estará perdida já que a fonte estará intacta e apenas a cópia fora perdida.

Para (FREITAS, 2007) alguns procedimentos devem ser seguidos pelo perito para garantir que a evidência não seja comprometida, substituída ou perdida, pois, se estes não forem seguidos, num tribunal, os juízes poderão considerar que essas evidências são inválidas e os advogados de defesa poderão contestar sua legitimidade, prejudicando assim o caso.

3.2. Extração

Nessa fase, após o perito ter realizado todo o procedimento de preservação do material, será iniciado o processo de recuperação das informações presentes nas cópias. O material questionado ou original, que fora copiado, é lacrado e guardado como evidência em local específico, podendo ser utilizado em qualquer outro

momento e até em alguma outra investigação criminal.

O principal objetivo dessa fase é recuperar arquivos que possam ter sido excluídos do disco e também realizar a indexação dos dados.

3.2.1. Recuperação de Arquivos

É importante compreender o funcionamento de um HD antes de aprofundar na recuperação dos arquivos. Ao excluir um arquivo do disco, o sistema operacional não sobrescreve o conteúdo que fora excluído com zeros ou “uns” (processo feito no *wipe* para limpar ou zerar os *bits* do dispositivo), entretanto, apenas é marcado o espaço que antes era ocupado por esse conteúdo como livre, processo também chamado de exclusão lógica, dessa forma, os arquivos presentes no HD são tratados pelo sistema operacional como espaço ocupado no disco e ao excluirmos esses arquivos, o sistema os trata como espaços livres. A partir disso, esses trechos tornam-se apenas inacessíveis à nível de usuário (usuários comuns de sistema), porém é possível a recuperação e acesso com técnicas e procedimentos específicos, realizados por técnicos ou peritos com um conhecimento mais avançado. Quanto mais demorado for para iniciar o processo de recuperação, maior será a dificuldade de recuperar as informações contidas nesse dispositivo, pois como o espaço no disco está marcado como livre, o sistema operacional pode utilizá-lo e ocupá-lo com outras informações, comprometendo assim a possibilidade de recuperação e leitura completa das mesmas.

A recuperação é realizada por meio de cabeçalhos ou assinaturas presente nesses arquivos. Todo tido de arquivo, como JPEG, BMP, GIF, AVI, DOC, TXT, MP3, entre outros, possui uma assinatura no início que os identificam e diferenciam. Na busca por um arquivo removido, é realizada primeiramente a busca por sua assinatura, e após a identificação dessa, torna-se possível a busca de seu conteúdo, podendo ser de forma integral (recuperação completa) ou parcial (recuperação de parte do arquivo, caso este já tenha sido sobrescrito).

O processo de recuperação por meio das assinaturas é conhecido como *Data Carving*. Em sistemas GNU/Linux pode ser realizado por programas como "*FOREMOST", "SCALPEL"* e outros mais. Abaixo segue exemplo de utilização desses comandos:

"foremost -i arquivo_de_entrada -o diretório_de_saída"

Para a execução do *FOREMOST* , deve-se instalá-lo pelo terminal do sistema e executá-lo como no exemplo. Esse programa possui diversos parâmetros e pode ser utilizado de diversas maneiras, como, por exemplo, acessar toda a documentação do programa digitando, no terminal do sistema, "man foremost". A partir desse momento, é possível identificar os parâmetros disponíveis e sua correta maneira de utilização. No exemplo citado anteriormente, o "arquivo_de_entrada" é a partição ou os arquivos a serem analisados enquanto que o "diretório_de_saída" indica onde os resultados da busca serão salvos.

A busca pode ser filtrada por meio do tipo de arquivo. O comando para tal tarefa é apresentado abaixo:

‘‘*foremost -t gif,pdf -i image.dd"*

Para essa situação, o programa irá procurar apenas por arquivos GIF e PDF, a "*image.dd*" pode ser uma partição específica do sistema.

```
Arquivo  Editar  Ver  Terminal  Ajuda
root@pc-dti:/# foremost -t doc,xls -i /dev/sdb -a -o /media/BACKUP/Backup -v
Foremost version 1.5.6 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Wed Dec  7 16:02:05 2011
Invocation: foremost -t doc,xls -i /dev/sdb -a -o /media/BACKUP/Backup -v
Output directory: /media/BACKUP/Backup
Configuration file: /etc/foremost.conf
Processing: /dev/sdb
|------------------------------------------------------------------
File: /dev/sdb
Start: Wed Dec  7 16:02:05 2011
Length: 28 GB (30750031872 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00000191.ole          20 MB           97792       (Header dump)
1:      00001735.ole          20 MB          888320       (Header dump)
2:      00001855.ole          20 MB          949760       (Header dump)
3:      00075053.ole          20 MB        38427420       (Header dump)
4:      00089477.ole          20 MB        45812508       (Header dump)
5:      00000191_1.ole        10 MB           97792       (Header dump)
6:      00001735_1.ole        10 MB          888320       (Header dump)
7:      00001855_1.ole        10 MB          949760       (Header dump)
```

Figura 11 – Exemplo do começo da execução do foremost

```
Arquivo  Editar  Ver  Terminal  Ajuda
1273:   59917447.doc          20 MB      30677732864      (Header dump)
1274:   59972639.doc         123 KB      30705991168
1275:   59984063.doc         427 KB      30711840256
1276:   59858607_1.doc        10 MB      30647606784      (Header dump)
1277:   59876983_1.doc        10 MB      30657015296      (Header dump)
1278:   59877063_1.doc        10 MB      30657056256      (Header dump)
1279:   59892311_1.doc        10 MB      30664863232      (Header dump)
1280:   59896975_1.doc        10 MB      30667251200      (Header dump)
1281:   59899743_1.doc        10 MB      30668668416      (Header dump)
1282:   59901991_1.doc        10 MB      30669819392      (Header dump)
1283:   59917447.ole          10 MB      30677732864      (Header dump)
1284:   59972639_1.doc        10 MB      30705991168      (Header dump)
1285:   59984063_1.doc        10 MB      30711840256      (Header dump)
**|
Finish: Wed Dec  7 16:21:14 2011

1286 FILES EXTRACTED

doc:= 643
doc:= 643
------------------------------------------------------------------

Foremost finished at Wed Dec  7 16:21:16 2011
root@pc-dti:/#
```

Figura 12 – Exemplo do resultado final da execução do foremost

Para utilizar o programa SCALPEL, é necessário configurá-lo de acordo com o tipo de busca que irá realizar. Para isso, deve-se editar o arquivo de configuração (*scalpel.conf*).

"scalpel ARQUIVO -o Diretório"

Nesse exemplo o "ARQUIVO" é a imagem, partição ou o dispositivo que será analisado, enquanto que o "DIRETORIO" indica onde serão salvos os resultados da execução.

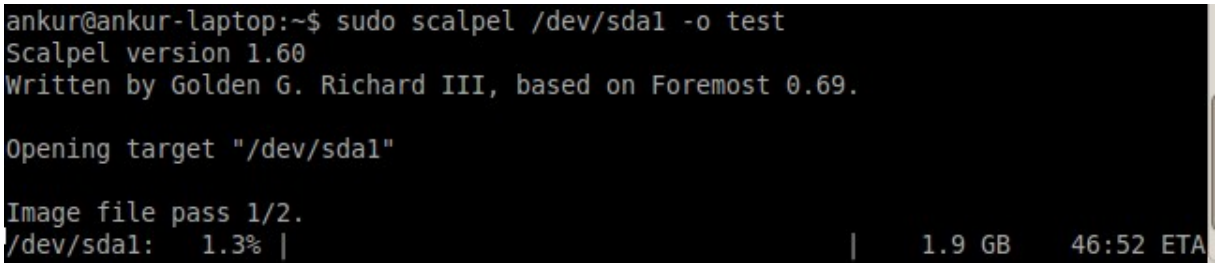

Figura 13 – Exemplo da execução do scalpel

3.2.1.1. Data Carving

> *"Data carving is the process of extracting a collection of data from a larger data set. Data carving techniques frequently occur during a digital investigation when the unallocated file system space is analyzed to extract files. The files are "carved" from the unallocated space using file type-specific header and footer values. File system structures are not used during the process" (2006, Digital Forensic Research Workshop - DFRWS).*[7]

Data Carving ou também conhecido como *File Carving*, é um método para identificação de arquivos independente do sistema operacional ou sistema de

7 http://www.dfrws.org/2006/challenge/

arquivos existente [8]. Funciona como assinatura de um determinado tipo de arquivo e é baseado nas informações contidas nos cabeçalhos, rodapés e setores de um disco.

3.2.2. Indexação de Dados

A Indexação de Dados, segundo (ELEUTÉRIO, MACHADO, 2011), consiste em varrer todos os dados ou *bits* do dispositivo, localizando as ocorrências alfanuméricas, assim como organizá-las de forma que possam ser acessadas e recuperadas rapidamente. Ao término desse processo é possível saber quais e quantas são as ocorrências de cada uma das cadeias alfanuméricas. Dessa forma, é criada uma espécie de catálogo contendo cada uma das cadeias encontradas.

Essa técnica é utilizada por peritos na fase de análise dos dados. Possibilita realizar buscas rápidas por palavras-chave no conteúdo dos materiais questionado, assim como permite que o procedimento de *Data* Carving seja realizado de maneira mais rápida e eficiente, pois todo conteúdo foi percorrido e as assinaturas dos arquivos ficaram organizadas e identificadas.

Algumas ferramentas mais utilizadas para realização desse processo são a Forensic Toolkit (FTK) e Encase, mas também estão disponíveis no mercado várias soluções.

3.3 Análise

A fase de Análise, (ELEUTÉRIO, MACHADO, 2011), é onde são feitos os exames nos arquivos recuperados do material questionado da segunda fase (extração). Nesse momento, o objetivo é identificar evidências digitais relacionadas com o crime que está sob investigação. Como durante a fase de extração podem ser recuperados milhares de arquivos, algumas técnicas e ferramentas auxiliam o perito na busca pela informação ou arquivo desejado. Conforme a complexidade do caso

8 Sistema de Arquivos podem ser do tipo NTFS, FAT, FAT32, ext4, ext3, xfx, entre outros

deve-se trabalhar com vários peritos ao mesmo tempo, sendo que há casos de necessitam de, pelo menos, quatro ou mais peritos trabalhando em conjunto para realizar a análise em um material.

Para (FREITAS, 2007), diferentes crimes resultam em diferentes tipos de evidência, e, por este motivo, cada caso deve ser tratado de forma específica. Por exemplo, em um caso de acesso não autorizado, o perito deverá procurar por arquivos log, conexões e compartilhamentos suspeitos; já em casos de pornografia, buscará por imagens armazenadas no computador, histórico dos sites visitados recentemente, arquivos temporários entre outros.

O propósito desta fase é tentar identificar quem fez, quando fez, que dano causou e como foi realizado o crime. Mas, para isso, o perito deverá saber o que procurar, onde procurar e como procurar. Para (FREITAS, 2007), após analisar as evidências o perito poderá responder às seguintes questões:

- Qual a versão do Sistema Operacional que estava sendo investigado?
- Quem estava conectado ao sistema no momento do crime?
- Quais arquivos foram usados pelo suspeito?
- Quais portas estavam abertas no Sistema Operacional?
- Quem logou ou tentou logar no computador recentemente?
- Quem eram os usuários e a quais grupos pertenciam?
- Quais arquivos foram excluídos?

> *"Antes de iniciar uma análise, o perito deverá avaliar qual procedimento utilizar para a coleta dos dados. A escolha deverá levar em conta o cenário e as circunstâncias em que se encontram o sistema a ser analisado. Alguns questionamentos devem ser feitos, como por exemplo: O que deverá ser coletado? O que coletar primeiro? Vale a pena coletar tudo? Será que não serão colocadas em risco todas as outras evidências só porque se pretende coletar algumas evidências em tempo de execução?"(SANTOS, 2008)* [9]

Conforme avaliação do perito, pode-se optar por uma técnica denominada de *forense in vivo,* que segundo (SANTOS, 2008), consiste num conjunto de procedimentos que são utilizados para a coleta de dados sem que o sistema seja desligado. Nesta modalidade, é priorizada a coleta dos dados mais voláteis [10] para os menos voláteis, pois em sua maioria os dados mais voláteis serão perdidos. Ainda segundo Azeredo, define-se também a *post mortem forense.* Conforme a ordem de volatilidade, esse procedimento é feito após o desligamento do computador, ou seja, neste momento só existe a memória não volátil para a análise, como HD, DVDs, entre outros, considerada a mais custosa quanto ao tempo, dada a quantidade imensa de informações a serem analisados.

Pode ser utilizado o Know File Filter (KFF), que funciona como um filtro dos arquivos encontrados, visando diminuir ou restringir a busca ao máximo possível para um conteúdo específico. Porém essa técnica somente é eficaz quando se sabe exatamente o tipo ou os arquivos a serem examinados a ser examinado no dispositivo.

---

9 Laudelino Azeredo Dos Santos – Computação Forense em Sistemas GNU/Linux

10 Perda de dados com ausência de energia, ou seja, quando o sistema por desligado

Outra técnica também eficiente é a busca por palavras-chave, realizada após a Indexação de Dados, os arquivos ficam em certo ponto organizados, possibilitando que o perito busque por palavras específicas, de modo que, quando for realizada a busca por essa palavra, sejam listados os arquivos que contenham a palavra ou arquivos que contenham trechos semelhantes. O perito tem a possibilidade de buscar pelos arquivos navegando por pastas do sistema. Esse processo, apesar de mais demorado, ainda é eficiente para localizar os arquivos. É importante que o perito tenha consigo os programas necessários para a visualização correta dos mais diversos tipos de arquivos como por exemplo .AVI, .RMVB, .JPEG, .ODT, entre outros. Os programas que auxiliam os peritos nas buscas por esses arquivos já foram apresentados no segundo capítulo.

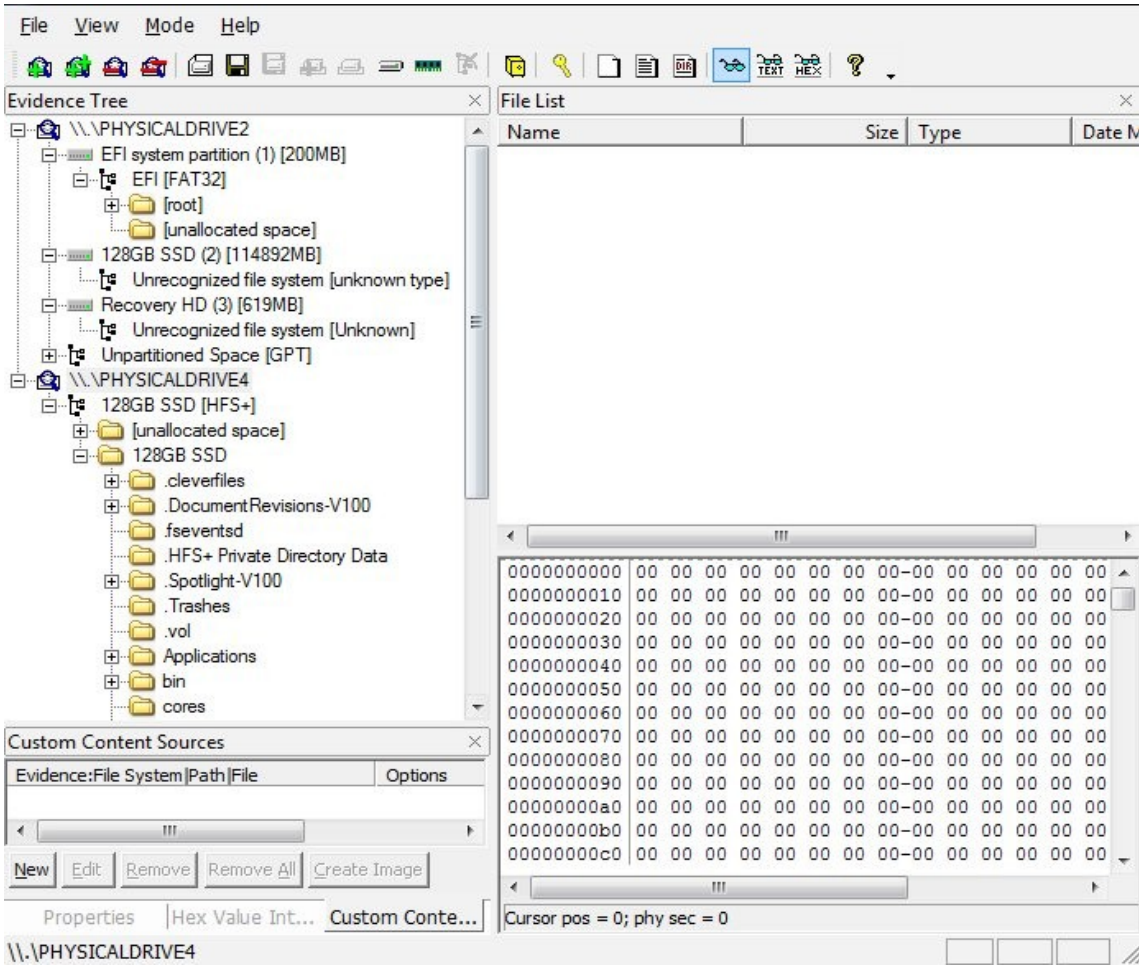

Figura 14 – Lista de partições localizadas pelo FTK

Nas próximas seções são apresentados alguns exemplos da busca por arquivos com a ferramenta Forensic ToolKit:

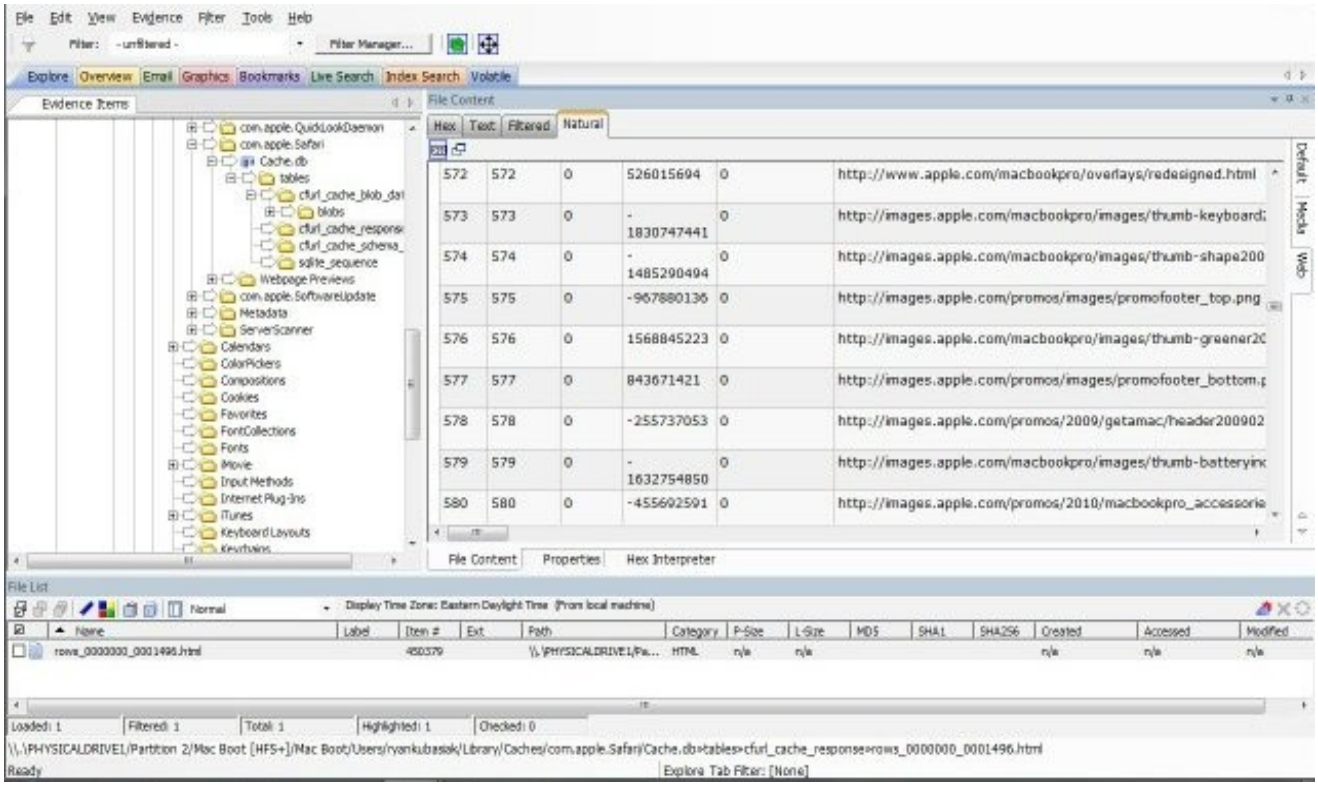

Figura 15 – Caminhos e arquivos de imagens recuperadas

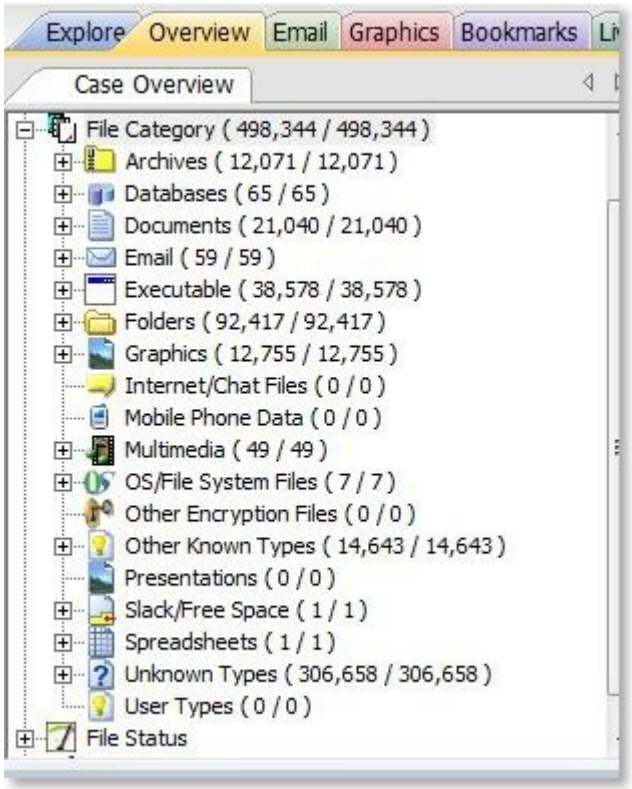

Figura 16 – Arquivos encontrados organizados e separados por tipo

3.4 Formalização

'Em muitos casos, as únicas evidências disponíveis são as existentes em formato digital. Isto poderia significar que a capacidade de punição a um invasor pode estar diretamente relacionada com a competência do perito em identificar, preservar, analisar e apresentar as evidências.' (FREITAS, 2007, p. 2)

Esta é a fase final de uma análise forense, onde o perito responsável elabora um laudo com os resultados encontrados em toda a análise, juntamente com as técnicas utilizadas na preservação, extração e análise. As evidências encontradas são copiadas e armazenas em mídias digitais, como CDs ou DVDs.

O laudo pericial é um documento técnico-científico e deve ser escrito com clareza e objetividade, detalhando todos os processos e métodos dos exames realizados, para que o mesmo não gere nenhum tipo de dúvida em relação a sua veracidade. O laudo tem uma estrutura própria e bem definida, formada por seções, são elas: Preâmbulo – identificação do laudo, Histórico – é opcional, caso o perito julgue necessário, são informados os fatos e interesses que levaram ao laudo, Material – onde descreve detalhadamente o que foi analisado, Objetivo – qual o objetivo desse laudo, Considerações técnicas/periciais – também opcional, algum detalhe importante que o perito identificou durante a análise, Exames – descreve os passos e procedimentos realizado, Respostas aos quesitos/conclusões – resumo dos resultados. Essa estrutura é utilizada em qualquer tipo de laudo pericial computacional.

3.4.1. Preâmbulo

Nessa seção, o objetivo é a identificação do laudo pericial, onde se deve conter o título, subtítulo, numero de identificação do laudo, os peritos responsáveis, autoridade solicitante, unidade ou laboratório responsável e outras informações relevantes na identificação deste.

Na tabela abaixo segue um exemplo de como deve ser feito o preâmbulo: (ELEUTÉRIO, MACHADO, 2011)[11]

Título (subtítulo) Nº do laudo – Unidade/Laboratório Data, Peritos responsáveis, Autoridade solicitante, Nº Processo, outras considerações, Data Solicitante do Laudo Quesitos ou Duvidas levantadas para Análise

Tabela 1 – Exemplo do Preâmbulo de um Laudo Pericial, Fonte: (ELEUTÉRIO, MACHADO, 2011)

3.4.2. Histórico

Nessa seção, são informadas o histórico daquele material questionado, por exemplo, caso esse material já tenha sido analisado e por outros motivos a autoridade solicitante levantou novos quesitos ou duvidas em relação a esse material, aquela análise posterior deve ser informada nessa seção. Essa seção é utilizada somente se o referido material já possuir informações previas, e que essas possam alterar ou influenciar no laudo final. (ELEUTÉRIO, MACHADO, 2011)

As informações necessárias para formular corretamente o histórico desse determinado material, podem conter, o número do laudo anterior, data da última análise, tipo de material, peritos responsáveis, quesitos levantados pela autoridade responsável, e outras considerações que o perito julgar necessário. (ELEUTÉRIO, MACHADO, 2011)

Na tabela abaixo segue um exemplo de como deve ser o Histórico:

11 Desvendando a Computação Forense

1 – Histórico Em 3 de Fevereiro de 2012, os peritos XXX retiraram o disco rígido de um computador que, conforme solicitação do Juiz Dr. XXX, deveria ser periciado. Após a retirada do disco rígido questionado, o mesmo foi lacrado no envelope de segurança de número xxxx, sendo prontamente acondicionado e levado para unidade de criminalística XXXX.

Tabela 2 – Exemplo do Histórico de um Laudo Pericial, Fonte: (ELEUTÉRIO, MACHADO, 2011)

3.4.3. Material

É a seção onde devem ser detalhados todos os materiais que foram analisados na investigação. Esses materiais devem ser descritos detalhadamente, pois o material analisado jamais pode ser confundido com algum outro ou gerar alguma dúvida de qual foi realmente analisado. Nesses detalhes devem constar, marca, modelo, tamanho, número de série, características específicas, estado de conservação, país onde foi feito e outras considerações informadas pelo fabricante (ELEUTÉRIO, MACHADO, 2011).

Para analises feitas em gabinetes, todas as peças desse devem ser detalhadas, como: quantidade (lógica) de memória *RAM* [12], marca, tipo de *slot* [13], quantidade (física) dessa memória, placa mãe com modelo e fabricante especificado, processador, marca, modelo, fabricante e capacidade, placa de vídeo (se existente), e outras placas ou dispositivos pertencentes a esse gabinete. Todos os materiais recebidos pelos peritos devem ser depois de periciados devolvidos com o laudo pericial, e as especificações de cada uma dessas peças garantem ao perito uma resposta para qualquer possível pergunta sobre o material analisado. Caso o perito receba esse material lacrado, devido a apreensão, deve-se registrar o número do lacre correspondente, pois esse será rompido para realização da análise, é importante também que ele informe as condições de conservação que foram recebidos esse material (ELEUTÉRIO, MACHADO, 2011).

12 Random Access Memory – Memória do sistema do tipo volátil
13 Os slots são o tipo de conector, podendo ser, DIM, DDR, DDR2, DDR3

Na tabela abaixo segue um exemplo de como devem ser especificado as características de um material, no exemplo, será descrito de um Disco Rígido: (ELEUTÉRIO, MACHADO, 2011)[14]

Referência	Tipo	Características
HD	Disco Rígido	**Marca:** Samsung **Capacidade Nominal:** 40 GB **Modelo:** SP0411N **P/N:** 0881J1CXA01413 **S/N:** S01JJ50XC84329 **País de Fabricação:** Coréia

Tabela 3 – Exemplo de especificação de um material, Fonte: (ELEUTÉRIO, MACHADO, 2011)

Caso haja possibilidade o perito deve demonstrar uma imagem desse material:

Figura 17 – HD analisado

14 Desvendando a Computação Forense

3.4.4. Objetivo

Nessa seção o perito deve informar de maneira resumida destacando os objetivos principais que levam à aquele, se contiver alguma quesitação deve ser informado juntamente nesse texto (ELEUTÉRIO, MACHADO, 2011). [15]

Na tabela abaixo segue um exemplo de como deve ser o Objetivo:

3 – Objetivo
Os exames visam a fornecer as características do material encaminhado, bem como recuperar e identificar documentos de texto, planilhas eletrônicas e mensagens de correio eletrônico relacionadas à empresa de nome xxxx, CNPJ xxxx, entre outros, presentes no material encaminhado a exame.

Tabela 4 – Exemplo do Objetivo de um Laudo Pericial, Fonte: (ELEUTÉRIO, MACHADO, 2011)

3.4.5. Considerações técnicas/periciais

Essa seção é opcional para utilização, pois aqui o perito explica alguma técnica, que julgue importante detalhar, utilizada durante sua análise. Um exemplo disso é como é feita a segurança dos laudos que são armazenados em mídias digitais, para que os mesmos não sejam alterados de maneira que corrompam o resultado do Laudo Pericial, a segurança é feita a partir do conceito de *hash* que será discutido no capítulo seguinte.

3.4.6. Exames

Essa é a principal seção do laudo pericial, onde o perito irá detalhar exatamente todos os procedimentos realizados na análise. Quais as técnicas utilizadas para a recuperação dos arquivos, quais ferramentas foram necessárias, qual sistema

15 Desvendando a Computação Forense

operacional foi utilizado e qual sistema existia no disco analisado, quais foram os meio utilizados na preservação do material questionado e outros diversos procedimentos que foram efetivamente utilizados.

Durante todo o laudo é aconselhável ao perito evitar ao máximo o uso de palavras técnicas, de modo que pessoas com pouco conhecimento sobre os meios e procedimentos forense utilizados na analise entendam claramente o resultado do laudo. Porém essa seção é a única que permite ao perito a utilização dos termos mais técnicos, pois é aqui que explica e garante toda a integridade dos procedimentos realizados. É onde também, o perito busca respostas para os quesitos ou duvidas levantadas no inicio das investigações pela autoridade solicitante (ELEUTÉRIO, MACHADO, 2011).

3.4.7. Respostas aos quesitos/conclusões

A última seção do laudo pericial, segundo (ELEUTÉRIO, MACHADO, 2011), pode ser chamada de respostas aos quesitos ou de conclusões. *Respostas aos quesitos,* caso a autoridade solicitante formulou algum quesito para focar na analise e o perito ao final deve responder esses quesitos; e *conclusões,* caso nenhuma quesitação foi formulada pela autoridade solicitante durante as investigações, com isso ao final do laudo o perito informa suas as conclusões retidas do material ao termino da analise.

Essa é a parte mais lida de todo o laudo, aonde, geralmente juízes, advogados e promotores vão direto na busca dos resultados. O texto formulado nessa seção deve ser o mais bem escrito e menos técnico possível, devendo ser o mais objetivo e claro, evitando até mesmo siglas ou nome de tecnologias mais complexas (ELEUTÉRIO, MACHADO, 2011).

Segundo (ELEUTÉRIO, MACHADO, 2011), as respostas aos quesitos ou conclusões devem ser muito bem elaboradas pelo perito, sem nenhuma ambiguidade, possibilidade de dupla interpretação. Caso isso aconteça todo o trabalho poderá ser

comprometido e a analise ser impossibilitada de uso legal.

É importante copiar os quesitos (caso existam) que foram formulados na primeira seção de Preâmbulo para essa última seção, a fim de facilitar o entendimento das respostas no laudo.

Para a elaboração do laudo segue algumas dicas segundo (ELEUTÉRIO, MACHADO, 2011) [16]:

- Caso as evidência não forem encontradas o perito deverá deixar claro que, após a realização dos procedimentos elas não foram encontradas.

- É recomendável referenciar a seção de Exames para informar as técnicas e procedimentos utilizados.

- As respostas devem ser de forma objetiva como para a pergunta: “Foram encontrados arquivos referentes à movimentação financeira da empresa X ?” Possíveis respostas:

    - Sim. Conforme detalhado na seção de Exames, diversas planilhas eletrônicas e documentos de texto foram encontrados no material examinado. Tais planilhas e documentos foram copiadas na mídia óptica anexa.

    - Não. Após a recuperação dos arquivos contidos no disco rígido examinado, conforme detalhado na seção Exames, não foram encontrados arquivos relacionado ao assunto no material examinado.

Ao termino das analises, é importante que o perito inclua explicitamente que o

16 Desvendando a Computação Forense

material está sendo devolvido e lacrado à autoridade solicitante, incluindo número do lacre no laudo. Por ser o final do laudo o perito deve incluir o número de páginas e os anexos contidos no mesmo e finalizar com assinatura e dados que identificam o responsável das análises, conforme tabela abaixo [17] (ELEUTÉRIO, MACHADO, 2011).

Com o Laudo, os peritos devolvem todo o material encaminhado a exame devidamente lacrado no envelope de segurança número xxxx. Nada mais havendo a lavrar, os perito encerram o presente Laudo que, elaborado em dezessete páginas e uma mídia ótica (DVD) em anexo, lido e achado conforme, assim acordes. Assinatura Perito 1 — Perito Criminal – Matrícula xxx Assinatura Perito 2 — Perito Criminal – Matrícula xxx Assinatura Perito 3 — Perito Criminal – Matrícula xxx Assinatura Perito 4 — Perito Criminal – Matrícula xxx

Tabela 5 – Exemplo da finalização do Laudo Pericial, Fonte: (ELEUTÉRIO, MACHADO, 2011)

3.5 Código de Integridade Hash

O *hash* ou código de integridade é utilizado para garantir a integridade dos dados de um determinado arquivo. No laudo pericial esse conceito é utilizado para garantir a segurança dos anexos que são armazenados em mídias digitais. Conforme foi transcrito no decorrer deste capítulo, o laudo, anexos e informações relacionadas as analises do material questionado são armazenadas em mídias como CDs e DVDs, e para garantir a integridade desses dados, impedindo que o mesmo possa sofrer algum tipo de adulteração, é criado o código *hash.*

Esse código é uma sequência de *bits* que é gerada através de alguns algoritmos específicos, como MD4, MD5, SHA-512, SHA1 e outros mais. O *hash* de um arquivo

17 Desvendando a Computação Forense

informa todo o conteúdo desse, se depois de gerado esse código o arquivo sofrer alguma alteração, por menor que seja, desde um espaço ou um ponto final em um arquivo de texto , o código *hash* será modificado.

Segundo (ELEUTÉRIO, MACHADO, 2011) [18], a segurança do procedimento consiste no fato de não se conhecer o método computacional para produzir o mesmo código a partir de duas mensagens distintas, sendo assim impossível gerar dois arquivos com mesmo código *hash.*

A lista de *hash* dos arquivos e anexos são armazenadas em um arquivo .txt, e o *hash* desse arquivo .txt é encontrado na seção de Exames do laudo pericial. É assim que é garantida a integridade dos arquivos armazenados nas mídias ópticas.

Em sistemas GNU/Linux o código *hash* pode ser gerado a partir do comando abaixo (digitado no terminal do sistema), onde o 'NOME_DO_ARQUIVO' é o arquivo que deseja obter o código, nesse caso foi utilizado o algoritmo *md5*:

“md5sum NOME_DO_ARQUIVO”

Como exemplo, foi criado um *hash* de um arquivo chamado “teste”, utilizando o algoritmo MD5 através da execução, “md5sum teste”, o código gerado foi “d41d8cd98f00b204e9800998ecf8427e”. Conforme imagem abaixo (figura 18):

18 Desvendando a Computação Forense

Figura 18 – Exemplo de código *hash* gerado de um arquivo

Foram apresentadas neste capítulo os meios necessários para que, a análise forense seja efetuada de maneira correta, e os resultados e procedimentos documentados em um laudo pericial, para que este possa ser utilizado em julgamento.

Capítulo 4 – PROCEDIMENTOS E MÉTODOS DE ANÁLISE

Em todo o terceiro capítulo, foram citadas técnicas utilizadas por peritos para realizar analises nos materiais questionados. Nesse capítulo serão tratados alguns procedimentos e métodos mais comum praticados por eles nessas analises, procedimentos que envolvem quebra de senhas, engenharia social, criptografia e algumas outras mais.

Durante todo o processo de análise os peritos deparam-se com diversas dificuldades para acessar os arquivos requeridos na quesitação da investigação, essas como encontrar o arquivo e o mesmo estar criptografado, dificultando o acesso ao seu conteúdo. Arquivos protegidos por senha, em casos onde o usuário se recusa a informá-la o pode haver necessidade de o perito entrar em contato com a empresa responsável pedindo a senha de administrador. Casos que serão tratados na sequência.

4.1. Protegidos por Senha

Quando algum arquivo é encontrado com proteção de senha, é necessário que o perito “quebre” essas senhas para acessar o arquivo. Para esse procedimento, caso o usuário se recuse a informar a senha do arquivo, poderão ser aplicados diversas técnicas, descritas na sequência.

4.1.1. Ataque de força bruta

Também conhecida como, *brute force,* essa técnica consiste em descobrir a senha de um sistema ou arquivo, testando todas as combinações possíveis (tentativa de erro), essas combinações envolvem números, letras, símbolos, letras maiúsculas e minúsculas e caracteres especiais. Devido grande quantidade de combinações possíveis esse processo pode se tornar bastante demorado, é interessante definir

algumas possíveis combinações a princípio a fim de agilizar o processo, por exemplo, testar letras e números, apenas letras, apenas números e assim por diante. Apesar de ser simples e fácil para utilizá-lo, em alguns casos, pela grande possibilidade de combinações, o processo exige um poder computacional muito grande e pode se tornar inviável utilizá-la.

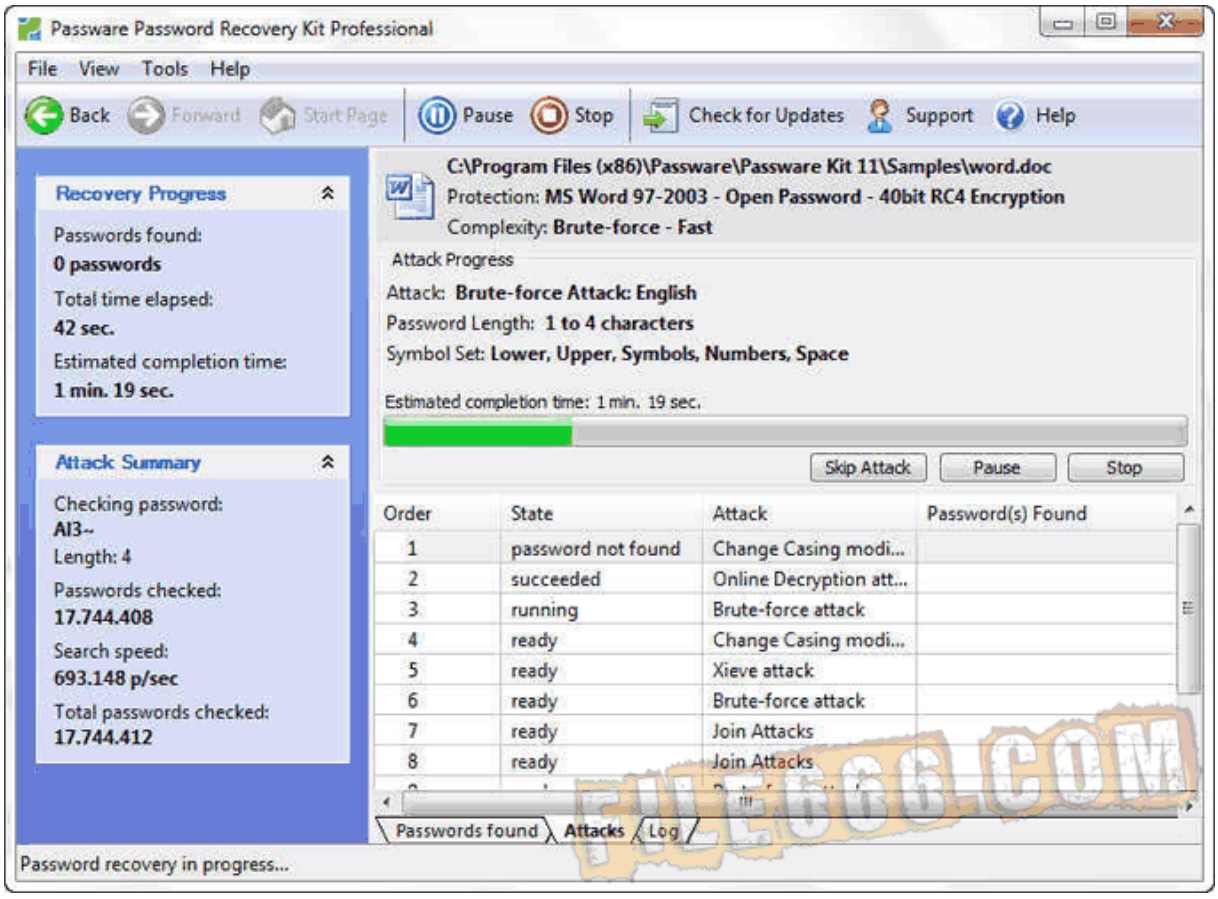

Figura 19 – Programa de ataque *brute force*

A figura 19 ilustra as propriedades do programa *Password Recovery Kit*, onde o arquivo, word.doc, está sendo testado com o objetivo de recuperar a senha do arquivo. Nessa ferramenta é possível definir um tipo da senha, por exemplo uma data, então o programa executa as combinações definidas com uma máscara, que no caso uma data poderia ser a máscara do tipo “01/01/1111”, dessa maneira o programa executa todas as combinações com os números que possam definir uma data válida.

4.1.2. RainBow Tables

As *RainBow Tables* são tabelas previamente criadas de *hash* que são utilizadas na quebra de senhas, são mais eficientes que o ataque de força bruta e leva um tempo muito menor para chegar ao resultado final. Com elas é possível recuperar senhas geradas a partir do seu código *hash. O* método utilizado por essa técnica consiste em comparar os diversos *hash* existentes em uma tabela pré existente, com o *hash* encontrado um arquivo protegido por uma senha, quando os códigos forem idênticos, obtém-se a senha do arquivo (ELEUTÉRIO, MACHADO, 2011).

Para utilização dessa técnica, programas como, *ophcrack,* (Figura 20), auxiliam na recuperação das senhas, esse programa está disponível em ambientes GNU/Linux e Windows

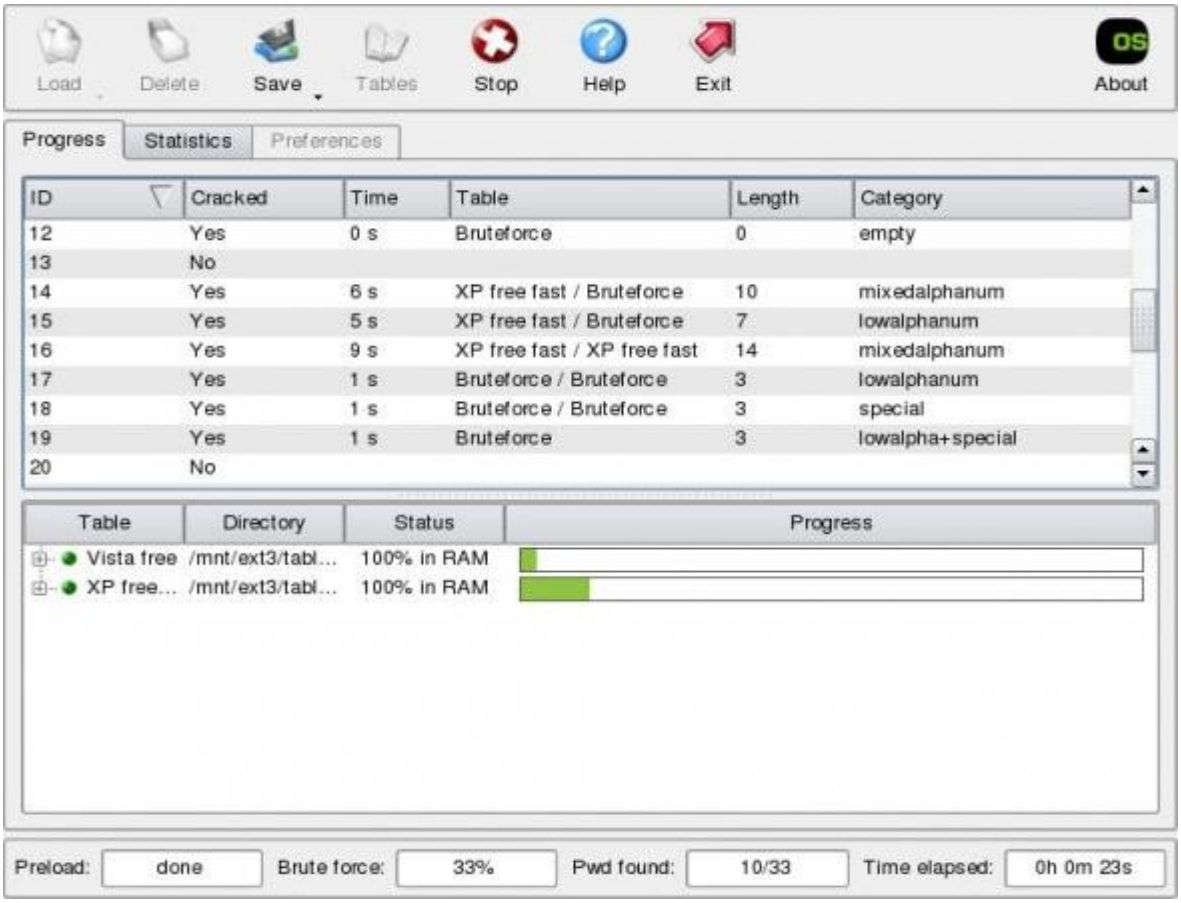

Figura 20 – Interface do programa *ophcrack*

4.1.3. Engenharia Reversa

Segundo Roger Pressman (2006), a engenharia reversa de um software é o processo que consiste basicamente em analisar um programa, a fim de criar uma representação de alto nível, ou seja, recuperar um projeto de software para que ele possa ser entendido. [19]

A utilização dessa técnica na recuperação de senhas consiste em analisar todo o programa que gera ou cria essa senha, identificar o trecho responsável pela criação dentro do programa, e alterando ou excluindo a necessidade da mesma, esse processo é denominado alteração de código-fonte.

Essa técnica é muito trabalhosa e exige alto conhecimento e capacidades técnicas por parte do profissional responsável. A alteração do código-fonte ocorre no nível mais baixo da linguagem, e em alguns casos o código executável utiliza de meios de compactação a fim de dificultar ainda mais a engenharia reversa. Existem programas que auxiliam na analise desses arquivos executáveis, o mais conhecido é o Olly Debugger (Figura 21).

19 Desvendando a Computação Forense

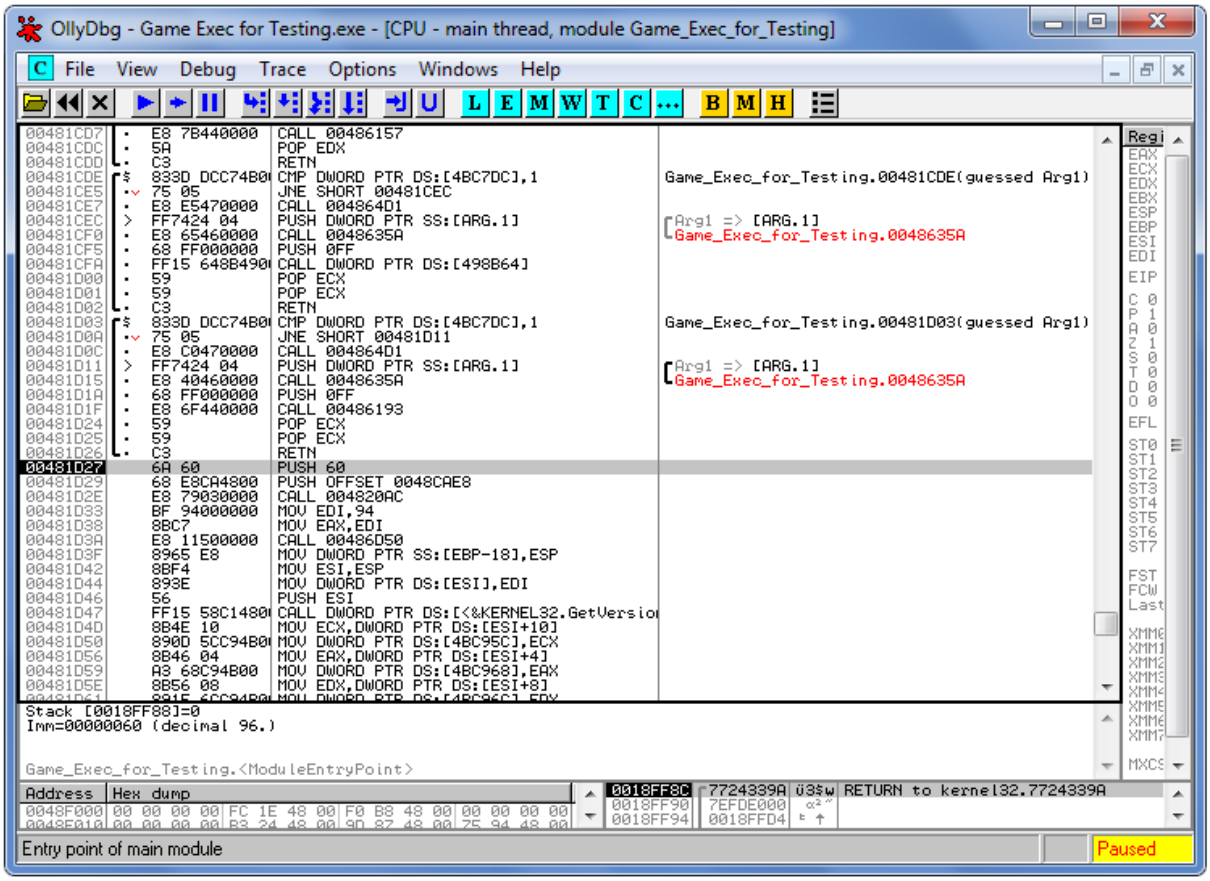

Figura 21 – Interface do programa Olly Debugger

4.2. Criptografia

O termo criptografia significa, 'escrita escondida', essa técnica consiste em ocultar ou codificar uma determinada informação, de maneira que somente o emissor e o receptor consigam acessá-las. É muito utilizada em cadastros efetuados na web por exemplo; sites bancários (*Internet Bankings*), onde as informações dos clientes são criptografadas para impedir que pessoas não autorizadas possam acessar as informações correspondentes.

Os métodos mais conhecidos de criptografia são o uso de chaves criptográficas, no processo de criptografia é criada essa chave e somente o detentor dessa consegue acessar todo o conteúdo do arquivo criptografado. Vários algoritmos são utilizados para criar essa criptografia, mesmo que alguém conheça o algoritmo que está sendo

utilizado para gerar essa criptografia ele só conseguirá acessar as informação com a respectiva chave criptográfica.

Existem chaves de 8bits, 64 bits, 128 bits, 256 bits, entre outros, esses valores são referentes ao tamanho da chave gerada. Para calcular o número possível de combinações de acordo com o algoritmo utilizado basta fazer uma potência de 2 elevando o número de bits do algoritmo, por exemplo, se for utilizado um algoritmo de 8 bits o número possível de combinações para aquela chave será 256 (2^8), nesse caso o algoritmo de 8 bits não é seguro, pois esse número de combinações é rapidamente acessível pois um computador pode calcular todas as combinações em questão de minutos. Já um algoritmo de 128 bits gera uma possibilidade muito grande de combinações e mesmo com um computador com alto poder computacional levaria muito tempo para conseguir "quebrar" essa criptografia. Considerando em termos de segurança, chaves geradas a partir de algoritmos de 256 bits, é extremamente difícil decodificar, e na maioria dos casos impossível, pois as milhares de combinações possíveis geradas a partir desse algoritmo os computadores levariam meses para obter apenas um caractere dessa chave.

Figura 22 – Exemplo do processo de criptografia.

Durante o processo de analise se os peritos encontrarem algum arquivo criptografado, alguns dos programas que são utilizados na analise como o FTK, possuem algumas possibilidades para encontrar a chave porém não possuem todas a possibilidades, caso por esse meio não seja possível o processo de decriptografia o perito deve procurar pelo software responsável por gerar a criptografia, para que

assim ela possa identificar o tipo de algoritmo utilizado e tentar realizar os procedimentos inversos. Se ainda não for possível encontrar a chave para acessar o arquivo, o perito deve entrar em contato com o fabricante do software para que o mesmo possa realizar a “quebra” dessa chave e possibilitar o acesso necessário para analise do material.

Após detalhado todo o processo de análise e de alguns métodos utilizados por peritos para o exame forense, segue no próximo capítulo um exemplo de laudo pericial, onde são tratados toda sua estrutura já discutida anteriormente.

Capítulo 5 – EXEMPLO DE LAUDO PERICIAL

Nesse capítulo será elaborado um exemplo de laudo pericial utilizando todos os padrões descritos no terceiro capítulo deste trabalho. O modelo de laudo utilizado será o disponibilizado por Pedro Monteiro e Marcio Machado, disponível na obra 'Desvendando a Computação Forense'. O caso fictício, foi desenvolvido apenas à título ilustrativo e informativo, onde todo material, informações e figuras utilizadas não possuem nenhum valor legal. Abaixo segue o laudo elaborado:

LAUDO N.º 0001/01

LAUDO DE EXAME DE LOCAL DE INFORMÁTICA

Em 10 de Julho de 2012, descrevendo com verdade e com todas as circunstâncias tudo quanto possa interessar à Justiça e respondendo aos quesitos formulados abaixo transcritos:

"1. Em relação ao serviço de acesso à Internet, no local examinado, o IP de acesso à Internet gerado em cada conexão local é compartilhado com todos os computadores disponíveis aos alunos?

2. Foi possível a identificação da máquina utilizada pelo titular da conta de e-mail exemplo@exemplo.com.br ? Em caso negativo, quais foram os fatores que contribuíram para tal impossibilidade?

3. Outros dados julgados úteis, pertinentes e esclarecedores.”

I – Histórico

Em 10 de Julho do ano de 2012, os Peritos Diego e Guilherme compareceram, por volta das 9:00h do mesmo dia, na FEMA - IMESA de Assis/SP, e colheram informações sobre e-mail enviado veiculando ameaças ao Sr. Osmar Machado. Após os exames, os Peritos emitiram o Laudo nº 0001/01, que sugeria, entre outras resoluções, a quebra de sigilo do endereço IP 200.230.71.24 utilizado por volta das 22:10:43 do horário de Brasília (GMT-03) no dia 30 de Junho de 2012.

Os Peritos foram novamente acionados pela autoridade policial, de acordo com a solicitação supracitada, pois o endereço IP na data/hora em questão estava sendo utilizado pela fundação educacional “FEMA-IMESA”, situado na Avenida Getúlio Vargas, número 1200, CEP 19807-634, no município de Assis/SP. Logo, por volta das 14:30 do dia 08 de Julho do ano 2012, os Peritos compareceram à fundação educacional, acompanhados pelos Policiais Federais: DPF João da Silva, EPF João de Souza e o APF João Soares.

II – Objetivo

Os exames visam a identificar o computador que foi utilizado para enviar a mensagem de correio eletrônico, a partir da conta de e-mail exemplo@exemplo.com.br. Além disso, os exames visam a esclarecer sobre como o local examinado realiza acesso à Internet, bem como outros dados úteis para a investigação.

III – Local

Trata-se da Fundação Educacional do Município de Assis “FEMA-IMESA”, localizado na Avenida Getúlio Vargas, número 1200, CEP 19807-634, no município de Assis/SP. O local em questão possui 20 computadores (clientes) equipados com processador Athlon XP 1.49 Ghz, 2 Gb de memória RAM e sistema operacional Windows Seven e um computador com processador Athlon XP 1,67 Ghz, 2 Gb de memória RAM e sistema operacional Windows XP, que é utilizado pela funcionário da fundação como servidor local. As figuras 22, 23, 24 mostram a entrada para a sala F do laboratório de informática em questão, suposto computador utilizado para envio das mensagens e a identificação desse suposto computador dentro do laboratório.

Figura 23 – Entrada para sala F da Fundação Educacional do Município de Assis

Figura 24 - Computador utilizado no envio das mensagens

Figura 25 – Etiqueta de identificação do computador do laboratório

IV – Exames

Os peritos compareceram à Fundação Educacional do Município de Assis “FEMA-IMESA”, onde tiveram acesso aos 21 computadores da fundação. Ao chegarem ao local, analisaram a topologia da rede da fundação e a forma de conexão com a Internet, e concluíram que as máquinas da fundação compartilhavam um único link com a Internet e utilizavam um mesmo endereço IP para acesso externo à rede local. Logo, qualquer um dos 21 computadores poderia ter sido utilizado para enviar a mensagem eletrônica em questão.

Os vinte e um computadores estão ligados ao Switch 3Com 3CRBSG2093 (Figura 25), que está conectado ao Roteador ADSLDSLink 260E (Figura A.6), responsável pela conexão da rede local à Internet. O Link com a Internet é disponibilizado por meio de serviços da própria fundação educacional, cujo setor responsável, é o FEMANET.

Figura 26 – Switch 3Com 3CRBSG2093 responsável pela distribuição da Internet aos computadores do laboratório da sala F

As imagens 26 e 27 mostram o servidor *proxy* responsável pelo o acesso a internet aos computadores dos laboratórios, o roteador e h*ub* responsáveis por disponibilizar o acesso dos computadores ao servidor de Internet.

Figura 27 – Servidor *proxy* responsável pelo acesso a Internet

Figura 28 – Roteador e *hub* responsáveis por disponibilizar acesso à Internet

O computador utilizado pelo funcionário continha um programa próprio de controle de uso das máquinas da fundação, com cadastro dos alunos (clientes). Analisando o programa, os Peritos buscaram identificar as máquinas que estavam sendo utilizadas na data/hora do envio da mensagem eletrônica, por volta 22:10:43 do horário de Brasília (GMT-03) no dia 30 de Junho de 2012, ou seja, 22:10:43 do horário local de Assis/SP. A tabela 5 ilustra parte dos dados coletados do programa de controle da fundação educacional, com as linhas destacadas como sendo de maior probabilidade de ser o computador em questão.

RA	Nome	Computador	Entrada	Saída	Tempo Total
1234	Aluno 1	10	30/06 21:00	30/06 22:05	1:05
2345	Aluno 2	15	30/06 21:30	30/06 22:30	1:00
3456	Aluno 3	03	30/06 22:00	30/06 22:20	0:20
4567	Aluno 4	09	30/06 22:30	30/06 23:00	0:30

Tabela 6 – Trecho do registro de uso dos computadores

Com essas informações, iniciaram-se as buscas nas máquinas mais prováveis de terem sido utilizadas para o envio da mensagem eletrônica. Por meio de softwares próprios e sem copiar qualquer conteúdo para o disco rígido das máquinas, os Peritos procuraram identificar indícios que possibilitariam a identificação do computador utilizado por meio de pesquisas por palavras-chave. Como o objeto de busca era uma mensagem eletrônica enviada por meio de Web Mail, os Peritos optaram em procurar nos discos rígidos as seguintes palavras-chave: “e-mail”, “ameaça”, “Osmar Machado”, “mensagem”, entre outras.

Sem sucesso nas buscas iniciais, os Peritos estenderam as buscas para todas as máquinas do laboratório, incluindo também a máquina utilizada pelo funcionário da fundação educacional. Não foram encontrados vestígios que permitissem identificar de qual máquina partiu a mensagem questionada.

Durante as buscas, percebeu-se que alguns programas estavam sendo executados em todas as máquinas da fundação educacional, sendo carregados na memória assim que estas eram ligadas. Um dos programas encontrados foi o “Garbage Sweeper 2.0 by lockngo.com”, que é um programa que limpa arquivos temporários, cache, cookies, arquivos de lixeira, swap e outros arquivos do computador. De acordo com pesquisas na Internet, foi obtida a seguinte descrição no sítio http:// www.softplatz... :

“(...) Garbage Sweeper is a FREE software utility that helps you maintain a cleaner computer. Garbage …...”

Os Peritos contataram que esse programa estava configurado para executar a limpeza de disco toda vez que o sistema operacional fosse carregado, ou seja, no mínimo, uma vez por dia, pois, de acordo com o funcionário da fundação educacional, os computadores são desligados diariamente durante a noite.

A fim de verificar se o programa realmente apagava arquivos temporários, cache, histórico, entre outros, foram realizados testes nas máquinas utilizando o programa em questão. Esses testes foram feitos após as buscas por indícios sobre origem da mensagem eletrônica. Primeiramente, os Peritos acessaram alguns sítios na Internet, utilizando o programa Internet Explorer, e verificaram que os endereços físicos 058613E90 e 0E7E821D0 do disco rígido continham as expressões “Nabaztag” e “Camera Digital Sony”, respectivamente. Depois, o computador foi desligado e ligado novamente, quando o programa “Garbage Sweeper” foi executado. Os Peritos acessaram os mesmos endereços físicos do disco rígido e constataram que as expressões haviam sido sobrescritas com caracteres aleatórios, ou seja, os dados já não eram mais acessíveis. Com o teste, ficou comprovado que o programa em questão pode ter apagado os indícios da origem da mensagem eletrônica procurados nas máquinas da fundação educacional.

Os Peritos ainda levantaram mais informações no programa de controle das máquinas da fundação educacional e copiaram os dados de todos os usuários cadastrados no sistema, além de recuperarem todas as visitas cadastradas dos usuários presentes nas linhas da tabela 5. Todas as visitas cadastradas dos usuários “Aluno1”, “Aluno2”, “Aluno3” e “Aluno4” à fundação educacional estão arquivadas. O registro completo de uso do laboratório da fundação educacional da sala F no dia 30 de Junho de 2012 está na tabela 6.

RA	Nome	Computador	Entrada	Saída	Tempo Total
3210	Aluno 10	20	30/06 08:15	30/06 08:45	0:30
4321	Aluno 21	02	30/06 08:30	30/06 10:20	1:50
5436	Aluno 6	09	30/06 09:00	30/06 09:15	0:15
3212	Aluno 9	10	30/06 09:00	30/06 10:30	1:30
7897	Aluno 17	01	30/06 11:00	30/06 13:00	2:00
8970	Aluno 13	03	30/06 14:30	30/06 15:45	1:15
0102	Aluno 5	17	30/06 16:10	30/06 17:35	1:25
4323	Aluno 8	12	30/06 19:00	30/06 20:20	1:20
6578	Aluno16	11	30/06 20:20	30/06 21:00	0:40
9829	Aluno 20	01	30/06 20:45	30/06 21:00	0:15
1234	Aluno 1	10	30/06 21:00	30/06 22:05	1:05
2345	Aluno 2	15	30/06 21:30	30/06 22:30	1:00
3456	Aluno 3	03	30/06 22:00	30/06 22:20	0:20
4567	Aluno 4	09	30/06 22:30	30/06 23:00	0:30

Tabela 7 – Registro completo do uso da sala F do laboratório da Fundação Educacional

V – Respostas aos quesitos

“ 1. Em relação ao serviço de acesso à Internet, no local examinado, o IP de acesso à Internet gerado em cada conexão local é compartilhado com todos os computadores disponíveis aos clientes ? Outros dados pertinentes.”

Sim todos os 21 computadores da fundação educacional compartilhavam de uma mesma conexão e de um mesmo endereço IP externo, disponibilizado pelo setor FEMANET. Logo, qualquer um dos 21 computadores poderia ter sido utilizado para enviar a mensagem eletrônica em questão, conforme explicado na seção IV.

“2. Foi possível a identificação da máquina utilizada pelo titular da conta de e-mail exemplo@exemplo.com.br ? Em caso negativo, quais foram os fatores que contribuíram para tal impossibilidade ? ”.

Durante as buscas realizadas nos treze computadores, não foram encontrados vestígios que permitissem identificar de qual máquina partiu a mensagem eletrônica em questão. Foi encontrado o programa “Gargabe Sweeper”, instalado em todas as máquinas da fundação educacional. Tal programa, quando executado, realiza a limpeza de dados temporários, históricos, cache e outros dados importantes para a realização de buscas por evidências digitais. Logo, esse programa pode ter apagado os vestígios e ser o responsável pela ausência de resultados das buscas realizadas, conforme explicado na seção IV do presente Laudo Pericial.

“3. Outros dados julgados úteis, pertinentes e esclarecedores.”

O laboratório tinha um programa que controlava o uso dos computadores e usuários. As principais informações foram coletadas pelos Peritos e apresentadas nas tabelas 5 e 6 da seção IV do presente laudo pericial.

Os Peritos têm por bem esclarecido o assunto.

Nada havendo a lavrar , os Peritos encerram os presente Laudo, produzido em 10 (dez) folhas que, lido e achado conforme, assim acordes.

Diego Zaratini Constantino Guilherme de Cleva Farto

Capítulo 6 – Conclusão

Ao término do presente trabalho, foi possível identificar a função e fundamentação da computação forense em dispositivos computacionais, possibilitando maior segurança dos dados. Usuários das diversas tecnologias citadas no decorrer desta obra, estão vulneráveis a quaisquer tipos de ataques virtuais, muitos acabam se tornando vítimas por não possuir o conhecimento mínimo necessário sobre segurança virtual. Alvo de *cyber* criminosos, que tiram vantagem desse baixo conhecimento, essas pessoas acabam tendo seus dados pessoais, arquivos e os mais variados tipos de dados roubados. Contudo mesmo pessoas com um maior conhecimento também estão vulneráveis, algumas vezes por distrações que, por exemplo, não percebem a irregularidade de um determinado site e acabam transmitindo suas informações pessoais.

Com a computação forense, através de seus métodos e técnicas detalhadas nessa obra, é possível identificar tudo e qualquer tipo de informações que são e foram transmitidas de um dispositivo, tudo o que é feito em qualquer desses dispositivos, deixa algum vestígio ou rastro, esses que são possíveis de identificar e rastrear dispondo dos meios forenses computacionais. Porém, pode ser rastreável o computador o dispositivo utilizado para cometer tais ilegalidades, mas o criminoso responsável pode não ser identificado ou não existir provas suficientes que o incrimine nos dispositivos analisados, de maneira que os dados presentes nos mesmo possam ter sido excluídos de forma que não seja possível a recuperação desses.

As técnicas utilizadas por peritos para quebra de senhas e analise gerais em busca das mais variadas informações, também podem ser utilizadas por criminosos na intenção de roubar e infringir as leis a fim de prejudicar algum usuário, até mesmo as ferramentas disponíveis são utilizadas com esses objetivos. Assim conforme aumentam as opções de segurança também aumentam as possibilidades de invasões.

A computação forense pode ser utilizada não somente como meios de identificação de crimes, mas também como uma maneira de testar e avaliar a segurança de sistemas e empresas, detectando vulnerabilidades existentes e já disponibilizando opções para correções dessas, garantindo a segurança e integridade dos dados.

Para finalizar esse trabalho, conclui-se que a computação forense está numa crescente, pois com um grande número de informações valiosas sendo transmitidas e armazenadas em servidores ou computadores pessoais, sempre haverá quebras de segurança e roubo de informações. Com objetivo de auxiliar usuários e tentar inibir a atuação de criminosos, vem se tornando um tema bastante importante, no qual atualmente não se fala em grandes servidores, sistemas, entre outros, sem colocar a segurança em primeiro lugar.

Trabalhos Futuros

Devido à escassez de material e poucas informações sobre um assunto bastante importante, pretende-se aprofundar os estudos sobre o tema, focando ainda mais a segurança dos dados, e como possível projeto de mestrado, desenvolver um sistema em nível acadêmico com objetivo de facilitar o entendimento e utilização desse sistema para futuros graduandos que tenham interesse em conhecer e seguir na área de segurança utilizando a computação forense.

Referências

BEGOSSO, Raíssa Helena. “Computação Forense”, Fundação Educacional do Município de Assis-FEMA, TCC – 2010

ELEUTÉRIO. Pedro M. da Silva, MACHADO, M. Pereira. “Desvendando a Computação Forense”, Novatec, Janeiro-2011

FREITAS, Andrey Rodrigues. Pericia Forense Aplicada à Informática. São Paulo – SP. Instituto Brasileiro de Propriedade Intelectual – IBPI, 2007.

RAMOS, Danielle; FIGUEIREDO, Taynara. Local de Crime. Pericia Federal: Local de Crime, v. 29, p.26-30, mar. 2012.

RICARDO KLÉBER M. GALVÃO. Coleta, Identificação e Extração de Dados (Data Carving) em Mídias e em Redes. Rio Grande do Norte, 2010. 50 p.

RODRIGUES, Jorilson da Silva. Pedofilia crime contra Infância. Pericia Federal: Pedofilia crime contra Infância, v. 3, p.16-18, out. 1999.

SANTOS, Laudelino Azeredo Dos.COMPUTAÇÃO FORENSE EM SISTEMAS GNU/LINUX. 2008. 54 f. Monografia (Pós-Graduação) - Departamento de Ciência da Computação, Universidade Federal de Lavras, Lavras, 2008.

SÉRGIO LUÍS FAVA . A polícia federal e o combate aos crimes pela Internet. Pericia Federal: Combate aos crimes pela Internet, v. 17, p.14-17, jan. 2012.

Links acessados

ALTIERES ROHR. Pacotão de segurança: computação forense e proteção total do PC. Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/07/pacotao-de-seguranca-computacao-forense-e-protecao-total-do-pc.html>. Acesso em: 30 maio 12.

ANÁLISE Forense Computacional Disponível em: <http://www.clavis.com.br/treinamento-ensino-a-distancia-ead/analise-forense-computacional/index.php>. Acesso em: 13 fev. 12.

BRIAN SALMON (Org.). AccessData FTK v3 & Macintosh Forensics. Disponível em: <http://www.appleexaminer.com/Resources/FTKMacForensics/FTKMacForensics.html>. Acesso em: 06 ago. 2012.

LUIS SUCUPIRA (Org.). PF exporta tecnologia contra exploração sexual infantil na web. Disponível em: <http://tecnologia.terra.com.br/noticias/0,,OI4672063-EI12884,00-PF+exporta+tecnologia+contra+exploracao+sexual+infantil+na+web.html>. Acesso em: 18 jun. 12.

LUIZ CRUZ. Computação forense com o Linux DEFT 7.1. Disponível em: <http://info.abril.com.br/noticias/blogs/zonalivre/distribuicoes/computacao-forense-com-o-linux-deft-7-1/>. Acesso em: 05 jun. 12.

SANDRO SÜFFERT. Ferramentas de forense. Disponível em: <http://forensedigital.com.br/new/entrevista-da-semana-sandro-suffert-fala-sobre-ferramentas-de-forense/>. Acesso em: 29 maio 12.

US-CERT (Org.). Computer Forensics. Disponível em: <http://www.us-cert.gov/reading_room/forensics.pdf>. Acesso em: 14 jun. 12.