ANÁLISE DE FERRAMENTAS LIVRES PARA PERÍCIA FORENSE COMPUTACIONAL

Vinicius Amorim Silva[1], Cleber Henrique de Oliveira[1]

[1]Faculdade de Tecnologia de Ourinhos

Centro Paula Souza – Ourinhos, SP – Brasil

viniasilva@hotmail.com cleberho@hotmail.com

RESUMO: *O grande desenvolvimento tecnológico e consequente ascensão da internet propiciaram uma nova forma de crime, os crimes digitais, também conhecidos como cibercrimes. Como forma de combate foi criado um novo ramo na Perícia Forense, a Perícia Forense Computacional. A cada dia torna-se mais importante o apelo à Forense Computacional, já que os criminosos vêm desenvolvendo técnicas anti-forense com o intuito de ocultar as evidências que possam ser usadas contra os mesmos. Os peritos forenses utilizam diversas ferramentas e softwares durante os processos de coleta e análise de dados que compõem as investigações. Muitas dessas ferramentas pertencem a empresas privadas e são pagas. O objetivo desse artigo é justamente a análise de ferramentas livres para a Forense Computacional. Para isso foram utilizados os projetos Forense Digital ToolKit (FDTK-UbuntuBr) e Computer Aided Investigative Environment (CAINE), duas distribuições Linux que possuem um vasto conjunto de ferramentas que atendem aos diversos processos de investigação. Durante o processo de coleta de dados às ferramentas mostraram-se funcionais, fator que indica eficiência de ferramentas livre para a Perícia Forense Computacional.*

Palavras-Chave*: Perícia, Forense, Computacional, FDTK, CAINE*

ABSTRACT : *The great technological development and consequent rise of the internet provided a new form of crime, digital crime, also known as cybercrimes. As a way to combat them, a new branch was created in Forensics, the Computer Forensics. Every day it becomes more important to appeal to Computer Forensics, since criminals have developed anti-forensic techniques in order to hide the evidence that could be used against them. The forensic experts use various softwares and tools during the processes for the collection and analysis of data that make up the investigations. Many of these tools belong to private companies and are paid. The aim of this article is precisely the analysis of free tools for Computational Forensics. For this project we used the Digital Forensic ToolKit (FDTK-UbuntuBr) and Computer Aided Investigative Environment (CAINE), two Linux distributions that have a wide range of tools that meet the several processes of investigation. During the process of data collection, the tools shown to be functional, a factor that indicates the efficiency of free tools for the Computer Forensics.*

Keywords*: Expertise, Forensic, Computing, FDTK, CAINE*

RESUMEN: *El gran desarrollo tecnológico y el consiguiente aumento de la internet proporcionado una nueva forma de delincuencia, los delitos digitales, también conocidos como ciberdelitos. Como una manera de luchar contra ellos, una nueva sucursal fue creada en medicina forense, en informática forense. Cada día se hace más importante para atraer a Forense Computacional, ya que los criminales han desarrollado técnicas anti-forenses con el fin de ocultar la evidencia de que podría ser utilizado en su contra. Los expertos forenses utilizan diversas herramientas de software y los procesos de recopilación y análisis de los datos que conforman las investigaciones. Muchas de estas herramientas pertenecen a empresas privadas y son pagados. El objetivo de este artículo es, precisamente, el análisis de las herramientas gratuitas para Forense Computacional. Para este proyecto se utilizó el Digital Forensic Toolkit (FDTK-UbuntuBr) y asistido por ordenador para el Medio Ambiente Investigación (Caine), dos distribuciones de Linux que tienen una amplia gama de herramientas que cumplen los diversos procesos de investigación. Durante el proceso de recogida de datos que se muestran las herramientas para ser funcional, un factor que indica la eficiencia herramientas gratuitas para Forense Computacional.*

Palabras clave*: Experto, Informática Forense, FDTK, CAINE*

INTRODUÇÃO

Com o passar dos tempos tornou-se notável o grande aumento em relação ao uso da tecnologia computacional na sociedade. Além da abrangente evolução em toda a rede de computadores, houve a grande ascensão da internet, o que levou a comunicação a um nível muito elevado, popularizando ainda mais o uso de computadores pessoais (RODRIGUES E FOLTRAN, 2010).

Diversas atividades como compras virtuais, acesso a contas de bancos pela internet, comunicações *online*, serviços remotos, dentre outras, tornaram-se possíveis, crescendo cada vez mais a produtividade. As empresas passaram a investir cada vez mais na tecnologia, dependendo assim dos sistemas computacionais para atingir eficiência em seu funcionamento. Paralelamente, pessoas mal intencionadas acabaram dedicando-se a atividades ilícitas, passando a utilizar de toda essa inovação (FREITAS, 2006).

O uso de ferramentas para atividades como invasão de sistemas, roubo de dados, fraudes, dentre outros, passou a atingir uma ascensão assustadora. Essas atividades são conhecidas como cibercrimes sendo o que os diferencia dos crimes tradicionais é justamente o uso de computadores, internet além de outros dispositivos eletrônicos para a prática do delito (PEREIRA, E. et.al, 2007).

Em resposta a isso houve a necessidade da utilização de métodos científicos com o intuito de investigar, preservar, analisar e documentar evidências de computadores ou outros dispositivos eletrônicos. Uma área relativamente nova, a Perícia Forense Computacional, também conhecida como Computação Forense ou Forense Computacional (FREITAS, 2006).

A Forense Computacional não se trata apenas de investigação, mas sim de todo um conjunto de metodologias de investigação e armazenamento de evidências, itens mais importantes, que caso sejam manuseadas sem seu devido cuidado, podem acarretar na perda dos dados contidos na mesma e consequentemente das provas do crime (QUEIROZ e VARGAS, 2010).

A constante luta entre os peritos forense e o mundo dos crimes digitais vem aumentando cada vez mais. Novas técnicas surgem com a função de ocultar as evidências que possam ser usadas contra o autor.

Segundo Bessa (2006), das formas de crimes virtuais mais comuns podemos citar a calúnia, a difamação, o roubo de informações e a remoção de arquivos, além de fraudes e pedofilia.

Esses crimes vêm sendo associados ao uso de técnicas anti-forense com a finalidade de ocultar dados que possam comprometer o autor do crime e peritos estão sempre buscando novas formas de quebrá-las, resultando em uma disputa constante (HARRIS, 2006).

Este artigo consiste em analisar a eficiência de ferramentas livres para Perícia Forense Computacional. Para isso, é explorado o FDTK-UbuntuBr e o CAINE, dois projetos de distribuição Linux, livre, que visam auxiliar os peritos forense através de um vasto conjunto de ferramentas que atendem às diversas etapas das investigações.

Seguindo este princípio, são exploradas as ferramentas mais utilizadas em uma das etapas mais importantes da metodologia que consiste a Forense Computacional, a extração de dados. Para isso foram escolhidas as ferramentas: DC3DD, Guymager e Photorec através da distribuição CAINE 2.5.1. Para a distribuição FDTK 3.0 foram analisadas as ferramentas: Wipe, AIR 2.0.0 e Scrounge-Ntfs.

O artigo está organizado da seguinte maneira. As características da Perícia Forense Computacional, seguido das etapas que compõem a sua metodologia são descritas. Logo após são apresentadas às ferramentas exploradas no CAINE e FDTK. Na seqüência tais ferramentas são analisadas e comparadas. As considerações finais sobre a análise são exibidas.

Características da perícia forense computacional

Segundo Queiroz e Vargas (2010), a forense computacional é um conjunto de procedimentos e metodologias com a função de investigar e armazenar evidências que possam responder se houve ou não um crime, tendo como base de análise equipamentos de processamento de dados (computadores pessoais, *laptops*, servidores, estações de trabalho ou outras mídias eletrônicas). De acordo com Farmer e Venema (2006), é o recolhimento e análise de dados de forma a investigar e reconstruir os fatos acontecidos no passado em um determinado sistema.

O propósito principal da forense computacional consiste na extração de evidências relacionadas a um caso investigado, para que propicie conclusões sobre o desfecho do delito (REIS e GEUS, 2002).

Existem fatores chave que consistem o processo de investigação (CASEY, 2000):

Primeiramente é realizada a coleta de informações. Posteriormente é realizado o reconhecimento da evidência, seguido de sua coleta, restauração, documentação e preservação. Finalmente há a correlação das evidências coletadas para que haja a reconstrução dos eventos.

Segundo Reis e Geus (2002), qualquer conjunto de dados (arquivos) importante torna-se necessário ser coletado para a análise. Conforme as evidências são encontradas, deve ser realizado a sua extração e restauração (no caso de danificação das provas), além de sua preservação e devida documentação. Finalmente as informações coletadas podem ser correlacionadas para uma possível reconstrução dos eventos que responderão se a atividade suspeita de fato é ilícita. Isso faz com que a forense computacional reproduza muitas vezes resultados mais diretos em relação a outras disciplinas forense, sendo decisiva em diversos casos.

Houve a necessidade de um estudo detalhado nas legislações, introduzindo-as ao ramo tecnológico para que a justiça pudesse validar um crime cibernético. A área jurídica ainda está em processo de desenvolvimento em relação a cibercrimes, de modo em que novas tecnologias, técnicas e delitos virtuais surgem. Por ser um ramo relativamente novo a forense computacional está sempre buscando se adequar a essas mudanças. (QUEIROZ E VARGAS, 2010).

Metodologia da perícia forense computacional

Segundo Noblett, Pollitt e Presley (2000), para que os resultados da perícia sejam válidos, é necessário que sejam postos em práticas procedimentos e protocolos (documentados) que garantam assim os requisitos legais e técnicos para a evidência pericial.

Existem fatores fundamentais que consistem o processo de investigação na Forense Computacional (CASEY, 2000):

Primeiramente é realizada a coleta de informações nas mídias envolvidas. Posteriormente é feito o reconhecimento da evidência, seguido de sua coleta, restauração, documentação e preservação. Finalmente há a correlação das evidências coletadas para que haja a reconstrução dos eventos.

Segundo Queiroz e Vargas (2010) o procedimento que envolve o processo da perícia é composto pela:

- Identificação da mídia (obtenção das evidências a serem periciadas)

- Coleta (mapeamento de tudo o que foi coletado)

- Preservação da evidência (realização da função hash e cópias dos dados para que a original mantenha-se segura)

- Análise (onde exige o maior conhecimento do perito, com o uso de ferramentas)

- Apresentação (criação de um relatório, laudo do perito sobre os dados encontrados durante a análise).

Na próxima seção serão analisadas as ferramentas para a coleta de dados em dispositivos de armazenamento de dados.

ANÁLISE DE FERRAMENTAS LIVRES PARA COLETA DE DADOS NO CAINE 2.5.1

Esta sessão exibe às ferramentas livres para a coleta de dados na Perícia Forense Computacional. As ferramentas DC3DD, Guymager e Photorec do sistema CAINE 2.5.1 serão analisadas. A distribuição FDTK 3.0 será utilizada para as ferramentas Wipe, AIR 2.0.0 e Scrounge-Ntfs.

O primeiro dentre os processos que compõem a metodologia da Perícia Forense Computacional é a coleta de dados, segundo a qual são utilizadas ferramentas para a obtenção de informações no equipamento periciado em questão, para que possam ser analisadas, finalmente arquivadas e utilizadas como evidências (FARMER e VENEMA, 2006).

Segundo Silva e Lorens (2009), o processo de coleta de dados mais comum na Forense Computacional, tratando-se de um procedimento que envolva memória volátil é o *Dump* de memória. Através do uso de ferramentas para a realização do *Dump* é possível obter uma cópia bit a bit da memória contida na máquina periciada. Dessa forma os peritos podem ter acesso a informações sobre todos os processos, arquivos, bibliotecas, conexões abertas, chaves de registro ou sockets que estavam em uso ou foram acessados até o momento da abordagem. O *Dump* de memória é um arquivo criado que, através do uso de ferramentas específicas, recebe a cópia (bit a bit) de todo conteúdo da memória em um sistema. Dessa forma, se a memória possuir 2 Gb de capacidade de armazenamento, o arquivo *Dump* terá 2 Gb de tamanho. Todo o processo é relevante de forma que deve ser realizado de maneira automática, sem nenhuma intervenção ou qualquer interferência que venha a afetar o conteúdo da memória enquanto ocorrer a extração (SILVA e LORENS, 2009).

De acordo com Farmer e Venema (2006), outro processo de coleta de dados muito utilizado é a criação de imagens forense, isto é, uma cópia autêntica e íntegra de um disco rígido, ou outro dispositivo de armazenamento de dados suspeito. Serão analisadas três ferramentas para coleta de dados através do sistema CAINE 2.5.1, sendo elas, DC3DD, GUYMAGER e PHOTOREC.

Ferramenta DC3DD

Sendo uma versão baseada na DCFLDD (aplicativo dd com novos recursos) essa ferramenta possui diversas funcionalidades. Seu principal recurso é a criação de imagens forense, ou seja, criação de imagens bit-a-bit de uma mídia.

Antes de uma coleta de dados é importante que utilize uma mídia de armazenamento sanitizada, isto é, que tenha passado por um processo de limpeza, conhecido como *wipe*, uma formatação completa sem recuperação dos dados. Essa ferramenta também possui o recurso de *wipe* de mídia, com um diferencial, gera o percentual de trabalho real que está sendo executado durante o processo. Além disso, possui outras funcionalidades como quebra de imagens, processo conhecido como *split*, além da geração de logs de erros.

O recurso de sanitização de mídia da ferramenta DC3DD foi escolhido para o teste prático, por se tratar de uma etapa fundamental na obtenção de uma imagem forense íntegra.

Durante os testes foi utilizada a versão 2.5.1 do CAINE como *liveCD* (*boot* pelo *cd*) para o sistema Windows Seven Ultimate (*service pack 2*), além de 2 *pen drives* Kingston DT101, sendo, um com capacidade de 4 Gb (que será o dispositivo suspeito para coleta) e outro com capacidade de 8 Gb (onde será criada a imagem forense).

O sistema CAINE 2.5.1 possui um ótimo atributo, não faz montagens automáticas de dispositivos, o que pode interferir no processo da obtenção da imagem. Um perito forense deve sempre relatar o processo de coleta e análise de dados passo a passo, com fotos de cada etapa, o que não é a proposta do trabalho. A análise consiste em sanitizar o *pen drive* que receberá os dados coletados com o recurso *wipe* do DC3DD.

Ao iniciar o CAINE no modo gráfico seguro (sem alteração do sistema instalado na máquina), plugar o *pen drive*, e verificar os dispositivos de armazenamento conectados na máquina, no caso o disco rígido e suas partições, além do *pen drive* de 8 Gb que será sanitizado, reconhecido pelo sistema como “sdb1”, ilustrado na figura 1.

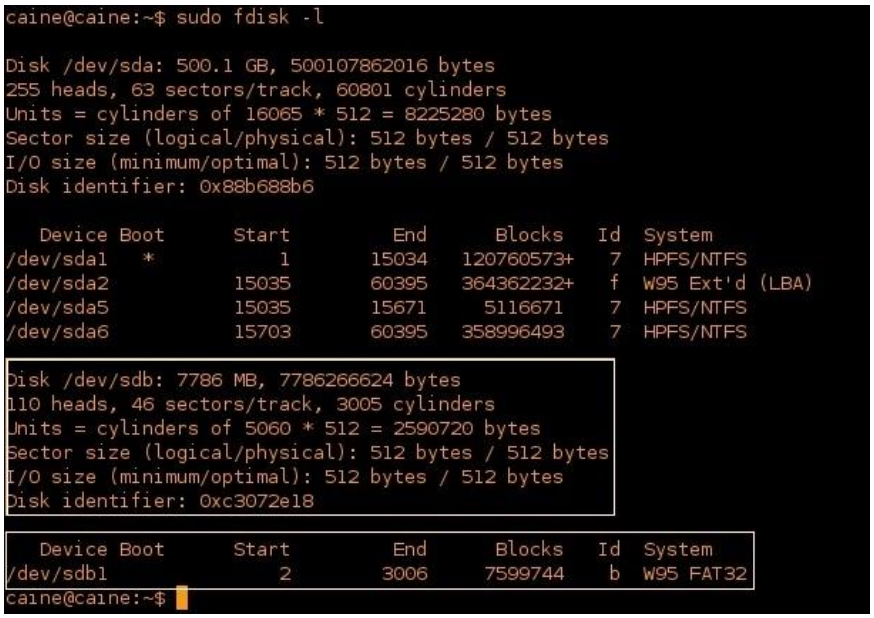

Figura 1- Dispositivos de armazenamento.

O comando também relata o sistema de arquivos utilizado pelos dispositivos e o seu número de blocos. Após o reconhecimento do *pen drive*, realiza o processo *wipe*, lembrando que ainda não foi montado no sistema.

 # sudo dc3dd progress=on wipe=/dev/sdb1

Este comando com permissão root utiliza a função de sanitização de mídia da ferramenta. É necessário muito cuidado ao indicar a mídia a ser formatada, pois o processo é irreversível. Tal processo é demonstrado na figura 2. É relatada a data, o horário de início e de término de todo o processo, além da quantidade de mega bytes por segundo apagados.

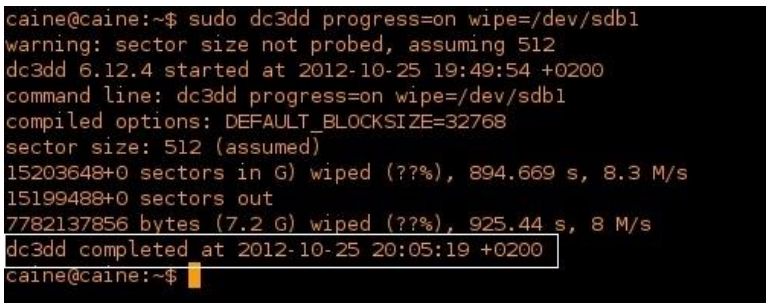

Figura 2- Função Wipe.

Ferramenta Guymager

A ferramenta Guymager é usada para criação de imagens forense. Além da coleta de dados completa de um *hard disk* ou outro dispositivo de armazenamento de dados, ela também possui opções de cálculo de hash em MD5 e SHA-256, além de salvar a imagem nos formatos dd (raw image), Exx (sub-format Encase5) e aff (Forense Advaced Image).

Outro recurso da ferramenta é a interface gráfica, facilitando ao perito o processo de coleta e arquivamento das informações, já que também possui campos de preenchimento onde é possível ser anotado o número do caso, o número da evidência, o nome do examinador, a descrição do caso e as anotações à respeito do disco onde foram coletados os dados.

Após a sanitização da mídia, realizado através do DC3DD no *pen drive*, o mesmo deve ser montado no sistema. É importante que o dispositivo seja montado para leitura e escrita (RW).

 # sudo mount –t vfat –o rw /dev/sdb1 /media/sdb1

A linha de comando acima indica que o *pen drive* será montado como rw (*read and write*), isto é, com atributos de leitura e escrita, no destino "/media".

Na seqüência, o *pen drive* suspeito é inserido no microcomputador. Com a ferramenta Guymager, será escolhido o dispositivo ao qual serão coletados os dados para a criação da imagem, como demonstrado na figura 3.

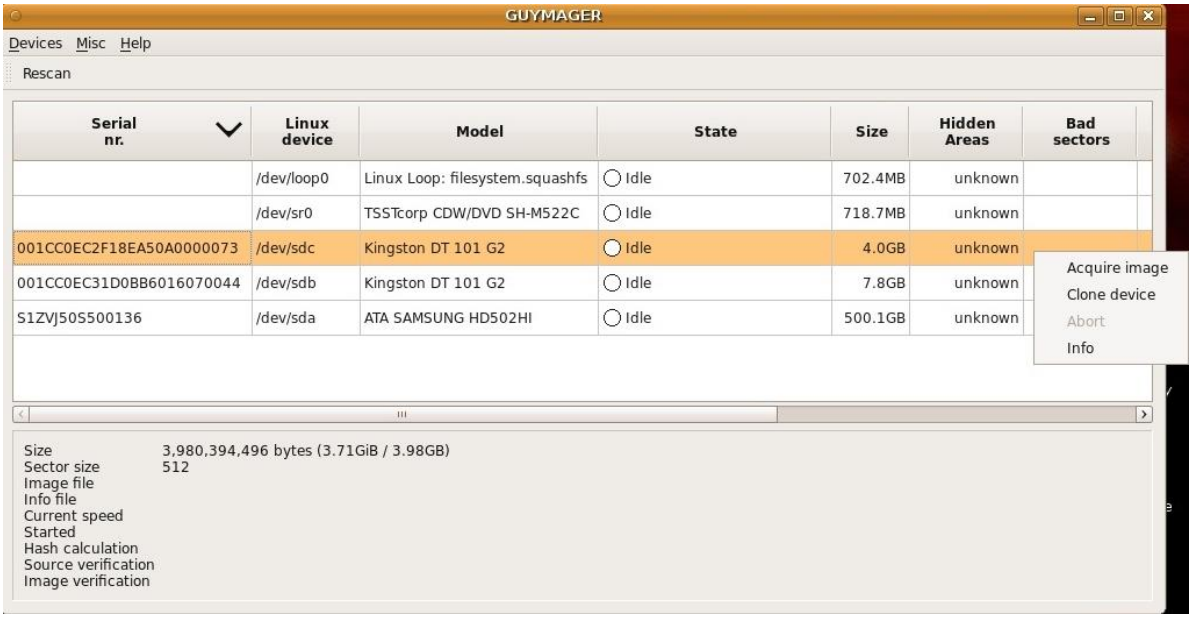

Figura 3- Dispositivo de destino.

O formato de imagem para a análise será a “Expert Witness Format, sub-format Encase5”, isto é, extensão Exx. Além da escolha da extensão, há um formulário com informações da imagem além dos recursos de cálculo de algoritmos de hash: MD5 e SHA-256, ilustrado na figura 4.

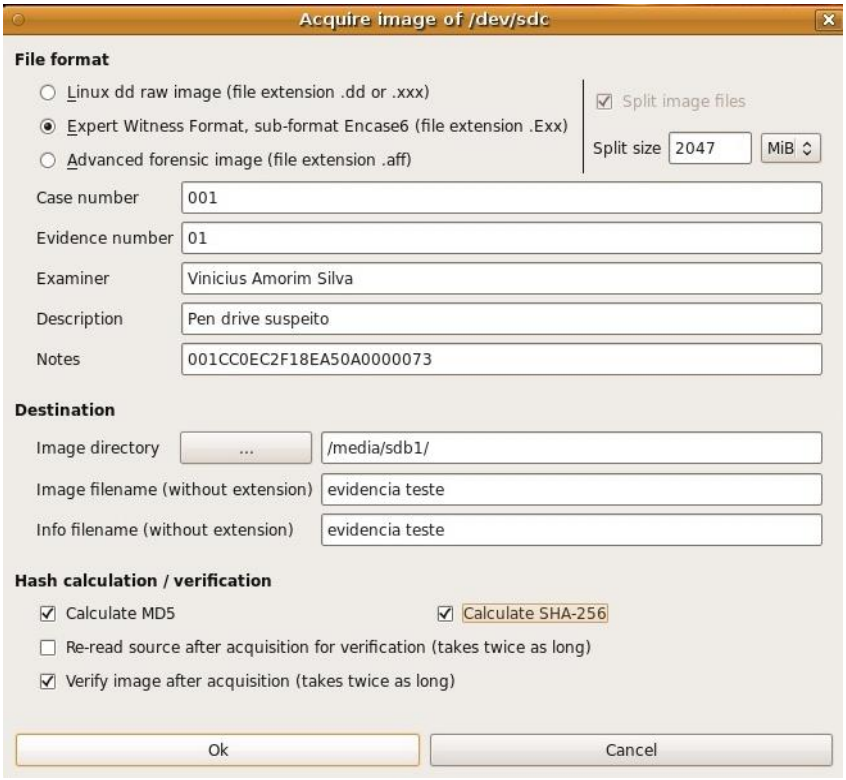

Figura 4- Informações e opções de imagem.

O programa também fornece a porcentagem do processo de criação da imagem. Após o fim do procedimento torna-se possível conferir os dados obtidos listando os arquivos no *pen drive*.

```
caine@caine:~$ cd /media/sdb1
caine@caine:/media/sdb1$ ls
evidencia_teste.E01  evidencia_teste.E02  evidencia_teste.info
caine@caine:/media/sdb1$ ls -lh
total 3.7G
-rwxr-xr-x 1 root root 2.0G 2012-10-25 20:44 evidencia_teste.E01
-rwxr-xr-x 1 root root 1.8G 2012-10-25 20:49 evidencia_teste.E02
-rwxr-xr-x 1 root root 4.2K 2012-10-25 20:53 evidencia_teste.info
caine@caine:/media/sdb1$
```

Figura 5- Verificação da imagem.

Como exibido na figura 5, a imagem completa do conteúdo do *pen drive* é dividida em pedaços (split) e salva no formato “Expert Witness” (E01), um formato seguro, proprietário do Encase que permite compactação sem perdas. Existem outros formatos de imagens forense, tais como o “Raw” (formato mais comum) e “Advanced Forense Format” (AFF).

Ferramenta Photorec

Existem diversas ferramentas livres disponíveis para a recuperação de dados perdidos em um dispositivo de armazenamento. Porém poucas apresentam resultados satisfatórios para recuperação de arquivos perdidos, tais como vídeos, músicas, documentos de texto, imagens além de muitos outros formatos de arquivos.

O "Photorec" funciona mesmo se o sistema de arquivos ao qual será realizada a recuperação de dados estiver comprometido ou danificado. Alguns dos sistemas de arquivos compatíveis com a ferramenta são: FAT, NTFS, EXT2, EXT3, EXT4, HFS além do ReiserFS. A ferramenta é aplicada em discos rígidos, *CD-ROMs*, cartões de memória (incluindo o *Compact Flash, Memory Stick, Secure Digital e SD), Smart Media, Micro drives*, além de outros dispositivos de memória USB e vêm sendo utilizada tanto por usuários comuns quanto por peritos forense. A ferramenta possui uma interface gráfica que facilita todo o processo.

Para o teste da ferramenta foi criada uma partição (Z:) de 5 Gb em um Hd Samsung de 500 Gb no sistema Windows Seven Ultimate com o nome "Teste_Forense". Essa partição possuía 4 Gb de arquivos em diversos formatos (doc, mp3, txt, jpeg, gif, entre outros). Os arquivos foram apagados da partição, o qual passará pelo programa de recuperação de dados.

Nesse processo, o *pen drive* (reconhecido como sdc1) é montado no destino "/media". A ferramenta apresenta algumas configurações de recuperação. A opção "*Paranoid*" faz com que os arquivos recuperados sejam verificados e os inválidos rejeitados (ela é ativada por padrão). Caso o recurso "*Brute Force*" seja ativado, os arquivos mais fragmentados (ou apenas seus metadados) serão salvos. Em "*Allow Partial Last Cilinder*", modifica a forma como a geometria do disco é determinada pelo programa (apenas os meios não particionados devem ser afetados). Com "*Keep Corrupted File*" os arquivos corrompidos serão mantidos, para que possam ser recuperados por outras ferramentas dedicadas, sendo que no "*Expert Mode"*, qualquer dado referente a um arquivo (mesmo que corrompido) será salvo. A opção "*Low Memory*" é utilizada para equipamentos com pouca memória, que podem ocasionar falhas durante a recuperação. Durante a varredura também há como escolher a extensão dos arquivos de busca. Foi utilizada a configuração padrão do software. Tais características estão ilustradas na figura 6.

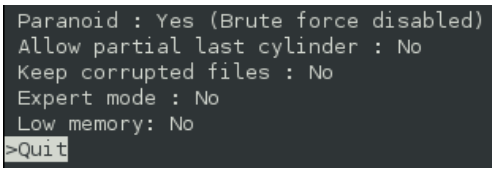

Figura 6- Opções de Varredura.

O próximo passo é a escolha do sistema de arquivos a ser utilizado, no caso o Ntfs. Em seguida o espaço a ser analisado deve ser selecionado. O recurso "free" é indicado a partições que apenas tiveram dados perdidos, ao contrário do "whole", dedicado a situações onde o sistema de arquivos está corrompido. Após esta etapa, o destino dos dados deve ser apontado, como exibido na figura 7.

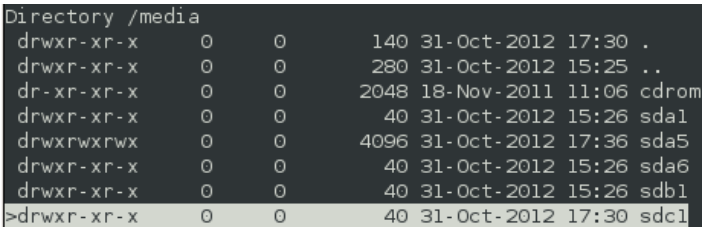

Figura 7- Escolha do destino dos dados.

Durante o processo de varredura, é relatado o tempo estimado e os dados incluindo extensões que estão sendo salvos. Após o término do procedimento, como exibido na figura 8, são apresentados os dados recuperados.

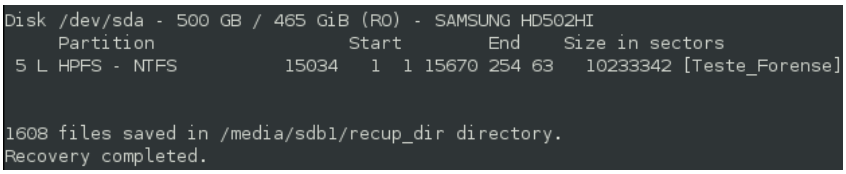

Figura 8- Conclusão do processo.

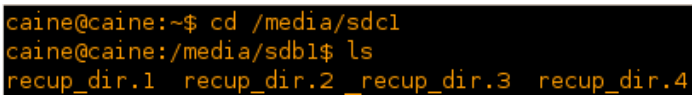

Figura 9- Conteúdo recuperado.

Neste caso, foram salvos 2.9 Gb de dados em diversas extensões.

ANÁLISE DE FERRAMENTAS LIVRES PARA COLETA DE DADOS NO FDTK 3.0

O sistema FDTK foi projetado para atender a todas as etapas que compõem a metodologia da pericia forense computacional. O processo de análise das ferramentas para coleta de dados será o mesmo utilizado no sistema CAINE, isto é, o boot do sistema será realizado através de um *liveCD*. Primeiramente a mídia a qual armazenará a imagem, no caso o *pen drive* Kingston DT101 de 8 Gb, receberá uma sanitização através da ferramenta WIPE. Com o dispositivo preparado para a coleta, será usada a ferramenta AIR 2.0.0 para a criação da imagem do *pen drive* suspeito de 4 Gb. É importante lembrar que o dispositivo de destino deve ter capacidade de armazenamento de dados igual ou superior ao do dispositivo de origem.

Ferramenta WIPE

A ferramenta Wipe é voltada para o processo de formatação e sanitização de uma mídia de armazenamento, buscando evitar que seja possível a recuperação de seus dados. Para isso, ela possui uma configuração padrão onde o processo *wipe* é repetido 4 vezes sobre o mesmo dispositivo. Mesmo havendo ferramentas voltadas para a recuperação de dados de uma mídia, ela desempenha bem o seu papel.

O comando usado para realizar tal procedimento é:

 # wipe [atributos] [mídia]

Para o teste foi escolhido uma opção de processamento rápido da ferramenta (-q), já que, por padrão, a mesma realiza a formatação por 4 vezes consecutivas. Primeiramente o *pen drive* foi verificado e montado na pasta “media”. Nesse diretório foi criada uma pasta com o nome “sdb1”.

Segue abaixo o comando usado para o processo de sanitização da mídia:

 # sudo wipe -kq -r /media/sdb1

É exibida uma mensagem para confirmação do processo. Esse comando faz com que o processo esteja no modo “*quickly*” (rápido) e que formate o diretório apontado, no caso o *pen drive* montado na pasta “media”.

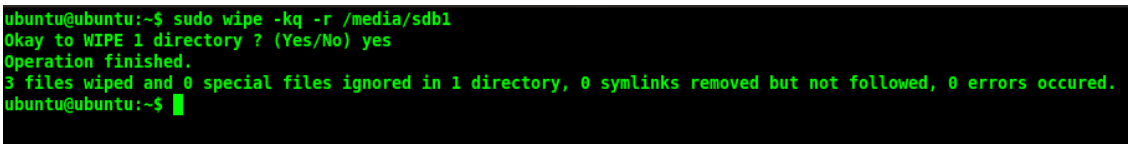

Figura 10- Execução do processo wipe.

Como exibido na figura 10, a ferramenta não apresenta o horário de início, término e a porcentagem do processo em execução, porém realiza a sua função.

Ferramenta AIR 2.0.0

O software conhecido como AIR é a implementação de uma interface gráfica para as ferramentas DD e DC3DD, sendo utilizada na criação de imagens forense, isto é, cópias completas do conteúdo de um *hard disk* ou outro dispositivo de armazenamento de dados. A imagem forense é salva no formato raw.

Como já mencionado, antes de ser utilizada a ferramenta para a criação da imagem, é necessário que a mídia na qual a cópia será armazenada esteja sanitizada. Esse processo foi realizado através da ferramenta WIPE. O mesmo processo de coleta realizado no sistema CAINE será feito no FDTK, porém com a utilização da ferramenta "AIR 2.0.0".

O FDTK 3.0 possui uma pequena falha na configuração, que deve ser corrigida antes do início da coleta de dados. O sistema operacional monta automaticamente o dispositivo inserido no microcomputador, no caso o *pen drive*, fato que pode alterar os resultados da coleta, pois o ideal é que haja capturas de tela de cada etapa do processo, inclusive da montagem das mídias. Para alterar a montagem automática basta apertar "Alt + F2" para que abra a janela de execução de aplicativos. Nela deve-se executar o aplicativo "*gconf-editor*", entrar em "*apps*", seguido de "*nautilus*" e "*preferences*". Finalmente desmarcar as opções "*media_automount*" e "*media_automount open*".

Logo após, os *pen drives:* suspeito, e o qual receberá a imagem forense são inseridos no microcomputador. Com os *pen drives* de origem e destino já identificados pode-se criar um destino para o armazenamento da imagem forense. O *pen drive* de destino já pode ser montado para uma futura verificação. O programa AIR exige que o número de blocos utilizado pelos dispositivos seja inserido antes da montagem. O comando "fdisk" identifica o número de blocos de cada *pen drive*.

De acordo com a figura 11, são observadas diversas opções para a montagem, como verificações da imagem criada pelos algoritmos de hash: MD5, SHA-1, SHA-256, entre outros, utilização do DC3DD (o dd é padrão), a opção "noerror,sync" que impede que a montagem se encerre com algum erro inesperado, a opção de "*split*" que divide a imagem em pedaços entre outros. Os dispositivos de origem e destino são inseridos nos campos, seguidos do número de blocos utilizados, no caso 512 bytes para ambos. Na sequência, inserir o nome do arquivo a ser criado após o caminho de destino, ou apenas o conteúdo será copiado (sem a criação da imagem).

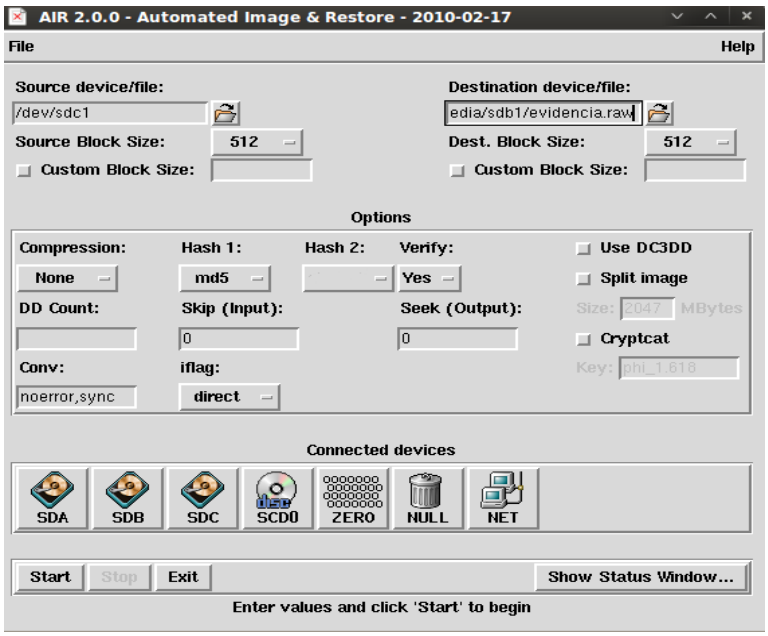

Figura 11- Opções de criação de imagem

Com as opções configuradas, basta pressionar "*start*" para iniciar a montagem. Será relatado todo o processo além dos comandos "dd" utilizados. O procedimento leva um tempo. Após a montagem, o programa verifica se a imagem criada é íntegra através do hash selecionado (MD5) para os dispositivos de origem e de destino. Além disso, é possível observar a data e hora de início e término do processo, demonstrado através da figura 12.

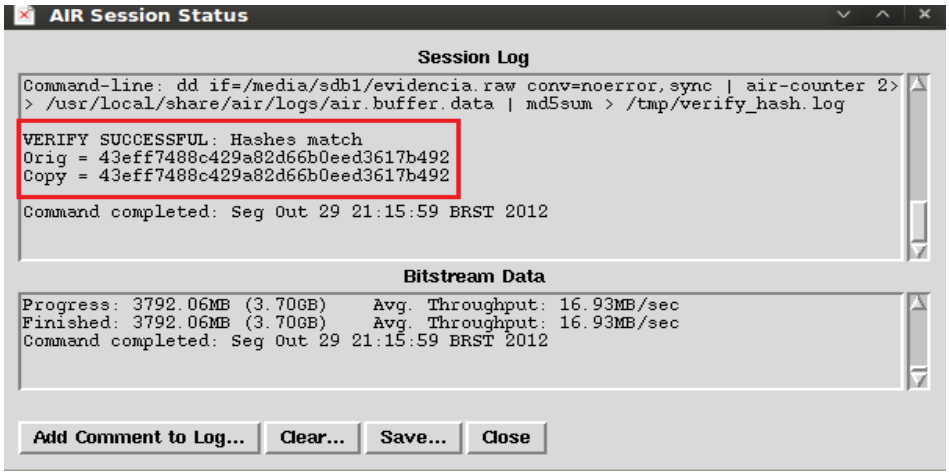

Figura 12- Integridade da imagem.

Para finalizar basta verificar se a imagem realmente foi criada no destino indicado através do comando "ls".

Ferramenta Scrounge-Ntfs

A Scrounge-Ntfs é uma ferramenta desenvolvida exclusivamente para a recuperação de dados em sistemas de arquivos ntfs. Tal ferramenta é aplicada sobre cada bloco de armazenamento do disco rígido (ou outro dispositivo que utilize o ntfs) mesmo que o sistema de arquivos estiver comprometido, de forma que sua raíz seja recriada e restaurada.

O funcionamento da varredura do Scrounge-Ntfs é baseada do início ao fim dos blocos do *hard disk*. Os setores de início e fim da partição analisada devem ser indicados, geralmente o primeiro setor é o 63 (para a primeira partição do disco rígido). Outra informação a ser obtida é o tamanho do *cluster*, que por padrão é 8, sendo múltiplo de dois (2, 4, 8,16, 32, 64). O Mft (Master File Table) é uma unidade que contém a estrutura de diretórios do disco, caso ele não seja incluso no processo, os arquivos serão salvos em apenas uma pasta.

As mesmas condições foram usadas durante o teste do Scrounge-Ntfs, uma partição Z: com o nome "Teste_Forense" de apenas 5 Gb, criada em um Hd Samsung de 500 Gb e contendo 4 Gb de dados apagados (formatação da partição).

Os comandos de utilização são:

 # scrounge-ntfs -m [mft] -c [cluster] -o [destino] [disco] start [início dos setores]end [fim dos setores]

Após a ferramenta de permissão de acesso root ser ativada. Primeiramente deve obter as informações sobre o disco rígido (sda).

O mesmo comando corresponde para qualquer outro dispositivo, no caso torna-se necessário obter os setores iniciais e finais da partição em questão (sda5), exibidos na figura 13.

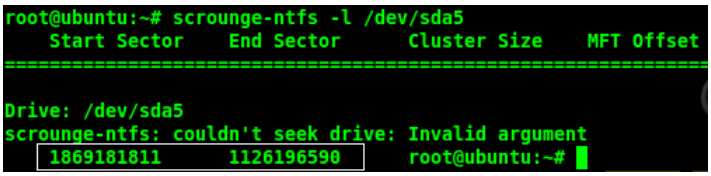

Figura 13- Informações da partição.

Os setores de início e fim para a partição são "1869181811" e "1126196590". Não será indicado o Mft Offset. Um diretório para receber os dados no *pen drive* foi montado na pasta "media".

O processo é analisado, como exibido na figura 14.

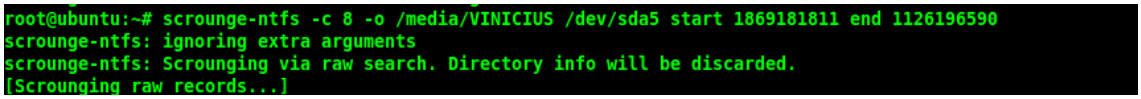

Figura 14- Programa em execução.

Não são indicadas informações a respeito do andamento do processo, apenas os dados que estão sendo encontrados. Ao fim da recuperação basta verificar o destino dos dados através do comando "ls", conforme demonstrado na figura 15. Os arquivos de diversas extensões foram salvos todos em uma única pasta.

Figura 15- Arquivos recuperados.

Foram recuperados 2,5 Gb de dados da partição em questão. Como os programas com a mesma funcionalidade trabalham sobre os blocos e setores, podem ser encontrados arquivos antigos que

estavam escritos na região do disco rígido onde foi criada a partição. O comando “df -h” indica a quantidade utilizada nos dispositivos, demonstrada na figura 16.

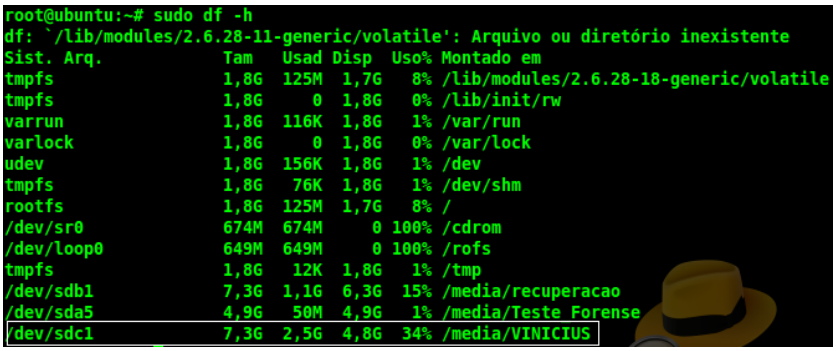

Figura 16- Quantidade de dados recuperados.

COMPARAÇÃO ENTRE AS FERRAMENTAS DOS SISTEMAS FDTK 3.0 E CAINE 2.5.1

As ferramentas livres destinadas às diversas funcionalidades que uma metodologia de forense computacional exige estão se tornando cada vez mais robustas, e recebem diversas atualizações para correções de “*bugs*” (erros). Estão disponíveis para download várias distribuições Linux, tais como, Helix, Caine, Back Track, Deft, Fdtk, entre outras que compõem um determinado conjunto de programas periciais. Foram analisadas as ferramentas DC3DD, Guymager e Photorec através do projeto Caine 2.5.1 além da Wipe, Air 2.0.0 e Scrounge-Ntfs no sistema FDTK 3.0.

Para a criação de uma imagem forense, isto é, cópia bit-a-bit do conteúdo de um dispositivo de armazenamento é necessário que a mídia de destino dos dados seja preparada, em um processo conhecido por “sanitização”, ou “*wipe*” (formatação de mídia minimizando uma possível recuperação de dados). As ferramentas utilizadas para o procedimento de *wipe* foram a DC3DD (Caine) e Wipe (Fdtk). Ambas operam através de comandos shell. O software DC3DD possui a principal funcionalidade de criação de imagens com recursos de quebra de imagens, conhecido como “*split*”, além da criação de *logs* de erros, possui o recurso *wipe*, o qual foi utilizado na análise. Essa ferramenta mostrou-se eficiente no que se diz respeito a sanitização, relatando a data e tempo exatos do início e fim de todo o processamento, a quantidade de bytes por segundo e o número total de bytes apagados, além do tamanho do setor do dispositivo de armazenamento de dados.

O programa Wipe também cumpre a sua função. Tal ferramenta possui um ponto positivo, vem configurada para realizar a formatação por quatro vezes consecutivas no dispositivo, contudo não apresenta a data e hora de início e término de formatação. A ferramenta também não apresenta a

quantidade de dados (bytes) apagados durante o processo, apenas o número de arquivo e a quantidade de erros.

Mesmo durante processos como a preparação de uma mídia para uma coleta de dados é importante que seja relatada cada etapa dos mesmos. Dessa forma a base para a análise entre as duas ferramentas foi a quantidade de dados a respeito do processamento e recursos fornecidos. As duas ferramentas analisadas através do processo *wipe* realizaram as suas funções, porém a DC3DD mostrou-se mais eficiente, apresentando informações importantes para o relatório de um perito forense.

Os softwares voltados para a criação de imagens forense disponíveis são inúmeros. Com o AIR 2.0.0 (Fdtk) e o Guymager (Caine) foram obtidos resultados satisfatórios na coleta de dados. Ambos apresentam interfaces gráficas, que facilitam todo o processo de coleta. A AIR foi desenvolvida como uma implementação de interface gráfica às ferramentas DD e DC3DD, portanto salva por padrão as imagens na extensão dd ou raw, as mais comuns e utilizadas. O programa apresenta muitas funcionalidades, como compressão de imagem através do gzip e bzip2, sanitização de mídia (opção "Zero"), utilização da ferramenta DC3DD ao invés da DD, verificação da integridade da imagem através dos algoritmos de hash: MD5, SHA-1, SHA-256, SHA-384 e SHA-512, além da criação de imagens através de redes TCP/IP e exibição de um log que contém as linhas de comandos shell utilizadas pela interface gráfica, a data e hora do início e término de todo o processo. Um detalhe importante é que seja necessário inserir o número de blocos utilizados nos dispositivos envolvidos no processo de criação de imagem.

O programa Guymager possui uma interface amigável, facilitando seu uso, com um processamento rápido na criação de imagens e detecção automática das mídias de armazenamento de dados. Possui recursos de *split* (divisão de imagens), clonagem de mídias, extensões DD (raw image), EXX (Sub-Format Encase5) e AFF (Forense Advanced Image), além de um formulário para o preenchimento de dados importantes, como informações da mídia, do perito e do caso. A verificação de integridade é realizada através dos algoritmos de hash: MD5 e SHA-256.

A integridade da imagem forense criada através das informações de um dispositivo suspeito é fundamental. A quantidade de opções e recursos envolvidos nessa cópia, principalmente em uma verificação de integridade é relevante e foi a base utilizada para a comparação das duas ferramentas. No que se diz respeito à criação de imagens forense, o programa "AIR 2.0.0" mostrou-se mais completo, com maior quantidade de recursos, como criação de imagens via rede TCP/IP e

compressão através dos aplicativos gzip e bzip2, além do maior número de algoritmos de verificação hash.

Em relação às ferramentas para recuperação de dados perdidos em uma mídia de armazenamento, foram analisadas duas ferramentas muito utilizadas, tanto pelos peritos quanto por usuários comuns. O software Photorec é acompanhado por uma interface gráfica simples e possui configurações básicas (*default*) voltadas a qualquer pessoa que deseja que seus dados perdidos sejam recuperados. Alguns dos sistemas de arquivos compatíveis com a ferramenta são: FAT, NTFS, EXT2, EXT3, EXT4, HFS além do ReiserFS. Essa ferramenta é aplicada em discos rígidos, *CD-ROMs*, cartões de memória (incluindo o *Compact Flash, Memory Stick, Secure Digital e SD*), *Smart Media, Microdrives*, além de outros dispositivos de memória USB. Um fator determinante são os recursos de recuperação disponíveis: o "*Paranoid*" (que faz com que os arquivos recuperados sejam verificados e os inválidos rejeitados), "*Brute Force*" (os arquivos mais fragmentados, ou apenas seus metadados, são salvos), "*Allow Partial Last Cilinder*" (modifica-se a forma como a geometria do disco é determinada pelo programa), "*Keep Corrupted File*" (os arquivos corrompidos são mantidos, para que possam ser recuperados por outras ferramentas dedicadas), "*Expert Mode*" (qualquer informação referente a algum arquivo, mesmo que corrompido, será salvo) e o "*Low Memory*" (utilizado em equipamentos com pouca memória, que podem ocasionar falhas durante a recuperação). Além disso, é possível escolher as extensões dos arquivos a serem recuperados.

A ferramenta Scrounge-Ntfs baseia-se apenas em comandos shell e é totalmente dedicada a dispositivos que utilizam sistema de arquivos Ntfs, mesmo que estejam corrompidos. Como outros programas de mesma funcionalidade, sua varredura ocorre através do início e fim dos blocos de dados da mídia ou partição desejada, porém com um diferencial, é necessário que sejam analisadas algumas informações antes do início do processo. Os setores de início e fim da mídia ou partição analisada devem ser indicados, geralmente o primeiro setor é o 63 (para a primeira partição do disco rígido). Outra informação a ser obtida é o tamanho do cluster, que por padrão é 8, sendo múltiplo de dois (2, 4, 8,16, 32, 64). O Mft (*Master File Table*) é uma unidade que contém a estrutura de diretórios do disco, caso ele não seja incluso no processo, os arquivos serão salvos em apenas uma pasta.

A quantidade de bytes de dados recuperados foi a unidade de comparação entre as duas ferramentas. Mesmo destinada apenas a sistemas de arquivos Ntfs, a Scrounge-Ntfs recuperou uma quantidade menor de dados. É importante salientar que nenhum dos arquivos foram testados, a

referência para a análise foi apenas a quantidade de informação recuperada. O Photorec foi mais eficiente nesse requisito (recuperação em Ntfs), além de possuir compatibilidade com outros sistemas de arquivos (FAT, Ntfs, EXT2, EXT3, EXT4, HFS, ReiserFS). É importante salientar que nenhuma ferramenta voltada a recuperação de dados possui resultados garantidos.

Todos os softwares analisados funcionam nos dois sistemas operacionais de pesquisa, além de outras distribuições Linux. Apenas houve a escolha de programas específicos que fazem parte do conjunto de ferramentas de cada projeto, sendo eles, CAINE e FDTK.

Como observado, foram escolhidos alguns critérios para as comparações entre as ferramentas em questão. Independente dos resultados, todas elas cumpriram a sua função, indicando a eficiência na utilização de ferramentas livres para a Perícia Forense Computacional.

CONSIDERAÇÕES FINAIS

Na medida em que a Perícia Forense Computacional vem se desenvolvendo, novas ferramentas são criadas para atender às diversas etapas que compõem sua metodologia. Muitas dessas ferramentas são proprietárias, porém a utilização de softwares livres vem crescendo cada vez mais tanto pelos peritos forenses, quanto por usuários comuns.

O artigo verificou a eficiência das ferramentas livres utilizadas pela Forense Computacional. Para isso foram utilizados os sistemas Caine 2.5.1 e Fdtk 3.0, pelas quais foram analisadas e comparadas em uma das etapas mais importantes da Forense Computacional, a coleta de dados.

Após a análise do conjunto das funções e opções que as ferramentas oferecem, foram realizados testes descritos por etapas. Durante o processo de coleta de dados às ferramentas mostraram-se funcionais, fator que garante a eficiência de ferramentas livres para a Perícia Forense Computacional.

REFERÊNCIAS

BESSA, L. Websense revela suas previsões sobre a segurança da internet para 2007. IMS Marketing.Websense, Inc. Disponível em: <http://www.websense.com/global/pt/PressRoom/PressReleases/PressReleaseDetail/index.php?Release=0612191332>. Acesso em: 25 maio, 2012.

BRAZILINO JR, A. S..; ZAPELINI, C. Z.. Lvm, Logical Volume Manager: uma solução dinâmica para gerenciamento de discos a plataformas Unix e Linux. Disponível em: <http://201.77.115.89:8080/ojs2009/index.php/technologies/article/viewFile/100/100> Acesso em: 3 out, 2012.

CAINE-LIVE, projeto CAINE. Disponível em: <http://www.caine-live.net>. Acesso em: 20 maio, 2012.

CARRIER, B. File System Forensic Analysis. Addison - Wesley Professional, 2005.

CASEY, E. Manual de investigação de crime computacional: tecnologia e ferramentas forenses. San Diego, Calif.: Academic Press, 2002.

FDTK, projeto FDTK. Disponível em:<http://fdtk.com.br.>. Acesso em: 12 maio, 2012.

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

FARMER, D.; VENEMA, W. Perícia Forense Computacional - Teoria e Prática Aplicada. 1edition, 2006.

FLYNN, I. M.; MCHOES, A. M. Introdução aos Sistemas Operacionais. São Paulo: Pioneira Thomson Learning, 2002.

GOLDMAN, A.; CARVALHO, R. P. Sistemas de Arquivos Paralelos: Alternativas para a redução do gargalo no acesso ao sistema de arquivos. Disponível em: <http://www.ime.usp.br/~carvalho/ctd2006/artigo.pdf>. Acesso: 25 set, 2012.

HARRIS, R. Chegando a um consenso anti-forensis: examinando como definir e controlar o problema anti-forense. Disponível em: <http://www.dfrws.org/2006/proceedings/6-Harris.pdf>. Acesso: 5 abr, 2012.

HENSON, V. A Brief History of Unix File Systems. Disponível em: <http://kraemer.pro.br/outros/2011-1/sd/fs_slides.pdf>. Acesso: 25 set, 2012.

MANZUR, C. L. Chile: los delictos de hackin gensus diversas manifestaciones. In: Revista Electrónica de Derecho Informático, n. 21, Abril del 2000. Disponível em: <http://libros-revistas-derecho.vlex.es/vid/delitos-hacking-diversas-manifestaciones-107511>. Acesso: 25 ago, 2012.

MARTINS, G. R.; SAALFELD, L. Sistemas de Arquivos- Windows x Linux. Disponível em: <http://webaula.unipar.br/henrique/aulas/2009/Sistemas%20de%20Informacao/Sistemas%20Operacionais/3%20bimestre/fat1.pdf>. Acesso: 3 out, 2012.

NAKAMURA, E. T.; GEUS, P. L. Segurança de Redes Em Ambientes Cooperativos. Ed Novatec, 2007.

NOBLETT, M.; POLLIT, M.; PRESLEY, L. Recovering and Examining Computer Forensic Evidence. Forensic Science Communication, Volume 2, Número 4, 2000. Disponível em: <http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.html>. Acesso: 5 abr, 2012.

OLIVEIRA, R. S.; CARISSIMI, A. S.; TOSCANI, S. S. Sistemas Operacionais. Revista de Informática Teórica e Aplicada. RITA. Volume VIII, nº 3, dezembro de 2001. Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/19242/000102159.pdf?sequence=1>. Acesso: 5 set, 2012.

PEREIRA, E. et.al. Forense Computacional: fundamentos, tecnologias e desafios atuais**.** Disponível em: <http://www.dainf.ct.utfpr.edu.br/~maziero/lib/exe/fetch.php/ceseg:2007-sbseg-mc1.pdf>. Acesso: 5 abr, 2012.

PINHEIRO, R. C. Os cybercrimes na esfera jurídica brasileira . Jus Navigandi, Teresina, ano 4, n. 44, ago. 2000. Disponível em:

<http://www.egov.ufsc.br/portal/sites/default/files/anexos/19747-19748-1-PB.pdf>. Acesso: 25 ago, 2012.

QUEIROZ, C.; VARGAS, R. Investigação e Pericia Forense Computacional: Certificações, Leis Processuais, Estudos de Caso. Rio de Janeiro – RJ: Ed Brasport, 2010.

REIS, M.A.; GEUS, P.L. Análise Forense de Intrusões em Sistemas Computacionais: Técnicas, Procedimentos e Ferramentas. Instituto de Computação - Universidade Estadual de Campinas, 2002.

RODRIGUES,T. S.; FOLTRAN JR, D. Análise de Ferramentas Forenses na Investigação Digital. Disponível em: <http://ri.uepg.br:8080/riuepg/bitstream/handle/123456789/530/ARTIGO_AnaliseFerramentasForenses.pdf?sequence=1>. Acesso: 5 abr, 2012.

SILVA, G. M.; LORENS, E. M. Extração e Análise de Dados em Memória na Perícia Forense Computacional. Disponível em: <http://www.icofcs.org/2009/ICoFCS2009-PP03.pdf>. Acesso: 25 maio, 2012.

SYSTEM-NTFS, Microsoft. Disponível em: http://technet.microsoft.com/pt-br/. Acesso:15 de set, 2012.

TANENBAUM, A. S. Sistemas Operacionais Modernos. 2ª.Ed. São Paulo: Prentice Hall, 2003.