Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

MATHEUS MATTIOLI MORO

METODOLOGIAS E TÉCNICAS DE ANÁLISE NA COMPUTAÇÃO FORENSE

Assis

2014

MATHEUS MATTIOLI MORO

METODOLOGIAS E TÉCNICAS DE ANÁLISE NA COMPUTAÇÃO FORENSE

Projeto de pesquisa apresentado ao Curso de Bacharelado em Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e à Fundação Educacional do Município de Assis – FEMA, como requisito parcial para a obtenção do Certificado de Conclusão.

Orientando: Matheus Mattioli Moro

Orientador: Me. Douglas Sanches da Cunha

Avaliador: Esp. Célio Desiró

Assis

2014

MORO, Matheus Mattioli
Metodologias e Técnicas de Análise na Computação Forense / Matheus Mattioli Moro. Fundação Educacional do Município de Assis – FEMA – Assis, 2014.
61p.

Orientador (a): Me. Douglas Sanches da Cunha.
Trabalho de Conclusão de Curso – Instituto Municipal de Ensino Superior de Assis – IMESA.

1. Computação Forense. **2**. FDTK. **3**. Laudo Pericial

CDD: 001.6
Biblioteca FEMA

Metodologias e Técnicas de Análise na Computação Forense

MATHEUS MATTIOLI MORO

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Bacharelado em Ciência da Computação, analisado pela seguinte comissão examinadora:

Orientador: Me. Douglas Sanches da Cunha

Analisador: Esp. Célio Desiró

Assis

2014

AGRADECIMENTOS

Aos meus pais Alécio Paschoal Moro e Beatriz de Sampaio Mattioli Moro, por estarem todos os dias ao meu lado me incentivando a não desistir apesar das dificuldades.

Ao meu professor e orientador, Douglas Sanches Cunha, por aceitar a proposta de trabalho e ensinamentos passados sempre que necessários.

Aos meus amigos Bruno Gaetano, Francisco Modotti e Gabriel Rodrigues pelas eternas risadas, lembranças e ajudas durante esses 4 anos.

A todas as pessoas que, direta ou indiretamente, que passaram ou contribuíram durante esses 4 anos.

RESUMO

O objetivo da Computação Forense é determinar a dinâmica, a materialidade e a autoria de ilícitos ligados diretamente à área de informática. Sendo assim, para que as evidências encontradas possam ser aproveitadas para produzir um laudo pericial, cabe a um profissional coletar as evidências de maneira correta. Para que uma perícia forense seja bem feita, necessita-se de uma distribuição com excelentes ferramentas. Com isso, no cenário brasileiro o primeiro nome que vem à cabeça de profissionais e peritos é a distribuição Linux FDTK, que possui um leque com mais de 100 ferramentas *open source* voltadas para perícia forense computacional. Sendo assim, o foco deste trabalho é abordar os conceitos, técnicas e procedimentos que devem ser seguidos para a elaboração correta de um laudo pericial.

Palavras-chave: Computação Forense; FDTK; Laudo Pericial.

ABSTRACT

The goal of Forensic Computer is to determine the dynamics, materiality and authorship of illicit connected directly to the computer area, so that for the evidence found to be used to produce an expert report it is up to a professional to collect the evidence correctly. For a forensic expertise to be well done, it is necessary a distribution with excellent tools; therefore, in the Brazilian scenario the first name that comes to the professionals and experts minds is FDTK Linux distribution, which has a range of more than 100 open source tools focused on forensic computer expertise. Thus, the focus of this study is to discuss the concepts, techniques, and procedures that must be followed for proper preparation of an expert report.

Keywords: Computer Forensics; FDTK; Forensics Report.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

Os dispositivos eletrônicos existentes hoje, tais como *smartphones*, *notebooks* e *tablets*, tornaram-se essenciais na rotina das pessoas, proporcionando uma maior facilidade em realizar tarefas e atividades cotidianas.

A partir do crescimento da tecnologia computacional, mais pessoas estão utilizando esses meios eletrônicos para se comunicarem com finalidades comerciais, educacionais e sociais.

Por conta destes avanços tecnológicos, os crimes digitais estão em constante crescimento. Portanto, os estudos relacionados à Computação Forense também não param de crescer.

Os estudos relacionados à Computação Forense são utilizados para identificar crimes cibernéticos, com a finalidade de coletar provas deixadas pelos criminosos cibernéticos, conhecidos por *crackers*.

A necessidade de profissionais com um maior conhecimento na área de tecnologia da segurança e o crescimento dos crimes computacionais será essencial para o desenvolvimento do trabalho. No mesmo serão abordadas técnicas e metodologia de uma análise forense, começando pela coleta de materiais e equipamentos até a extração de arquivos e dados. Um estudo de caso será conduzido a partir das informações coletadas e será confeccionado um laudo pericial.

1.1. MOTIVAÇÃO

Com o constante crescimento do estudo da Computação Forense, novas técnicas vêm sendo necessárias para poder conter ações provocadas por criminosos. Contudo, o foco nesta área é essencial para que qualquer empresa possa avaliar e testar como está sua estrutura de segurança, e descobrir se existe algum vazamento de informações dentro de suas dependências.

1.2. OBJETIVOS

1.2.1. Objetivos Gerais

O presente trabalho tem como objetivo apresentar, de forma detalhada, as etapas realizadas em uma análise computacional forense, mostrando as principais ferramentas forenses utilizadas por peritos computacionais.

1.2.2. Objetivos Específicos

Entre os objetivos que focam na formação do aluno no referido projeto de conclusão de curso, destacam-se as técnicas de uma análise forense, os métodos que serão utilizados para formar o conhecimento do aluno em relação ao uso das diferentes ferramentas forenses existentes; trabalhar com equipamentos computacionais, alvos de perícia forense computacional para fazer a extração de dados pertinentes a uma investigação; avaliar e testar a estrutura de segurança de máquinas, utilizando recursos da computação forense, para demonstrar onde estão suas falhas de segurança e ao final confeccionar um laudo pericial sobre todas as informações coletadas durante os testes.

1.3. JUSTIFICATIVA

Os conceitos apresentados sobre Computação Forense visam a apresentar como existem falhas que somente são descobertas com a utilização de equipamentos e ferramentas especializadas, sendo assim possível criar um laudo final com todos os detalhes que, após serem apresentados, poderão ser utilizados para melhorar a segurança do equipamento utilizado.

1.4. REVISÃO DE LITERATURA

De acordo com COSTA (2005) a Computação Forense trata da investigação, análise e exame de um crime computacional, ou seja, tudo que engloba a computação como meio, sob a ótica forense, sendo penal ou civil. Quando se trata da criminalística a Computação Forense cuida do incidente computacional na esfera penal, determinando os meios, autorias, consequências e causas.

GOLDMAN (2008) concorda com COSTA (2005) quanto à Computação Forense; entende-se como o local onde é feita a análise minuciosa de todo o material computacional encontrado no local do crime. Compreendemos que a Computação Forense encaixa-se no ramo da criminalística junto à descoberta, preservação, restauração e análise de evidências computacionais. Os computadores podem e são usados para cometer crimes, entretanto, acabam contendo evidências desses crimes, como dados de contas, com isso, podem ainda conter informações sigilosas fazendo-os serem alvos de crimes.

Por outro lado, BUSTAMANTE (2006) destaca que o objetivo principal da Computação Forense é analisar e extrair dados de diferentes dispositivos, para que as informações coletadas passem a valer como evidências e logo depois como provas legais. Outra definição da Computação Forense encontrada por BUSTAMANTE (2006) é a de que as evidências encontradas geralmente não são

vistas a olho nu e dependem de ferramentas para serem percebidas, por isso, cabe a um profissional de informática coletar as evidências de modo que elas possam ser aproveitadas para produzir um laudo pericial.

Enquanto isso, WENDELL (2012) comenta que a Computação Forense é basicamente um modo de escovar os dados encontrados em busca de evidências de crimes virtuais para serem utilizados em juízo. Através da Computação Forense pode-se resgatar até as informações que foram apagadas do disco rígido. Essas informações resgatadas normalmente são para indiciar criminosos que possuem informações de pedofilia, *spam*, *phishing*, roubos virtuais, desvios de verbas, entre outros. O objetivo que originou a criação da Perícia Forense Computacional é suprir as necessidades das instituições que se referem à manipulação das evidências eletrônicas, sendo ela a ciência que estuda a aquisição, preservação, recuperação e análise de dados que possuem formato eletrônico e são armazenados em alguma mídia computacional.

1.5. METODOLOGIA

Para o desenvolvimento deste trabalho, foram utilizadas diversas fontes para a pesquisa bibliográfica. Além disso, ao final, será apresentado o cenário ideal de segurança utilizando algumas ferramentas da Perícia Forense Computacional.

1.6. ORGANIZAÇÃO DO TRABALHO

Na Introdução é feita uma breve descrição sobre o que o trabalho pretende abordar, assim como seu tema e objetivos. Enquanto no capítulo seguinte encontram-se os métodos e conceitos que são utilizados na Computação Forense, além de como um perito deverá se portar em uma busca. No terceiro capítulo é brevemente abordado o funcionamento dos Sistemas Operacionais, com ênfase no sistema operacional

Linux, sendo assim, são descritos alguns aplicativos e sistemas operacionais forenses e explica-se como e quando os mesmos devem ser utilizados. No capítulo final conta-se a história da *distro* escolhida para a realização deste trabalho seguindo métodos e técnicas da pericia forense. Além disso, ao final são utilizadas algumas ferramentas da *distro* para a elaboração de um formulário de cadeia de custódia.

2. COMPUTAÇÃO FORENSE

Primeiramente este capítulo tem como intenção falar o que é a Computação Forense, sendo assim, explicar o termo forense e quem a utiliza. Com o termo explicado, o objetivo do restante deste capítulo é apresentar onde, como, quando e por que se deve utilizar a Computação Forense para a resolução de crimes computacionais.

2.1. O QUE É COMPUTAÇÃO FORENSE

Antes da definição da Computação Forense é importante definir o termo *forense*, do latim *forensis,* que significa ao público, ao fórum ou à discussão; contudo, tem como finalidade colher evidências científica de fatos ou ocorrências que serão utilizadas em uma corte ou sistema de justiça. O termo *forense* está presente em diversas disciplinas que atuam paralelamente com o investigador na busca pela verdade. A *American Academy of Forensic Sciences* (AAFS), possui os seguintes comitês: Criminalística; Engenharia; Jurisprudência; Odontologia; Patologia/Biologia; Antropologia; Psiquiatria; Toxicologia; Endocrinologia e Computacional (NEUKAMP, 2014).

A Computação Forense tem como intenção a aquisição, a preservação, a identificação, a extração, a restauração, a análise e a documentação de evidências computacionais possivelmente utilizadas para crimes eletrônicos. Utiliza-se esse processo para o rastreamento, identificação e comprovação da autoria dos crimes eletrônicos (ELEUTÉRIO et. al. 2011).

Com o avanço da tecnologia indo cada vez mais rápido e com aparelhos cada vez menores, era apenas questão de tempo para a popularização mundial da Internet, que nos anos 90, explodiu devido à criação do *World Wide Web* (WWW), sendo

assim permitido o compartilhamento de dados e informações entre os usuários de todo o planeta (ELEUTÉRIO et. al. 2011).

Mesmo com todos os benefícios possíveis, essa explosão de compartilhamento de dados e informações acabou acarretando uma serie de novas práticas ilegais e criminosas. Entretanto, uma frase popular muito usada é “crimes sempre deixam vestígios!”, principalmente na área computacional. Neste caso, os vestígios que são deixados do crime são digitais, ou seja, uma vez que são armazenados dentro dos equipamentos computacionais que são compostos por *bits* (zeros e uns), em uma sequência lógica (ELEUTÉRIO et. al. 2011).

Todavia, o objetivo principal da Computação Forense é determinar a dinâmica, a materialidade e a autoria de ilícitos ligados diretamente à área de informática, tendo como principal questão identificar e processar as informações digitais coletadas de provas materiais do crime, usando métodos técnico-científicos, conferindo-lhes sua validade probatória em juízo (ELEUTÉRIO et. al. 2011).

2.2. ONDE UTILIZAMOS COMPUTAÇÃO FORENSE

No local onde supostamente ocorreu o crime, normalmente pode-se encontrar evidências muito úteis à investigação, que podem esclarecer a autoria (quem), a dinâmica (como) e a materialidade (o que aconteceu) do delito (ELEUTÉRIO et. al. 2011).

O local do crime de informática não é nada além de um local de crime comum, acrescido de equipamentos computacionais que podem conter informações necessárias para o esclarecimento do crime. Contudo, hoje em dia é muito comum o cumprimento de mandados de busca e apreensão que envolve equipamentos computacionais. Nestes casos, são de extrema importância o isolamento, a análise, a documentação minuciosa dos vestígios e sua posterior coleta. Já em cumprimento

de um mandado, deve-se primeiramente identificar para logo em seguida selecionar e coletar os equipamentos (ELEUTÉRIO et. al. 2011).

Em ambos os casos descritos anteriormente deve-se tomar cuidados especiais durante a coleta dos vestígios digitais, pois alguns equipamentos são muito sensíveis e assim podem ser facilmente perdidos e/ou destruídos. O impacto, a umidade, a imersão em água, o calor excessivo, o atrito e o eletromagnetismo são alguns exemplos que causam a perda de informações digitais. Após a coleta, devem-se tomar precauções durante o transporte e o armazenamento do material (ELEUTÉRIO et. al. 2011).

De modo semelhante aos crimes que utilizam mandados de busca e apreensão, todos os mesmos procedimentos de identificação e preservação dos dados devem ser realizados. Entretanto, a principal diferença é que será necessária a realização de alguns exames forenses no local do crime para posterior elaboração do laudo (ELEUTÉRIO et. al. 2011).

Em casos assim, poderão ser utilizados técnicas e equipamentos forenses para a verificação do conteúdo de dispositivos computacionais encontrados ainda no local. A utilização dessas técnicas somente deverá ser executada por profissionais capacitados da área de informática, para que nenhum conteúdo armazenado nos equipamentos seja alterado, garantindo assim a preservação das evidências digitais. Para acessar diretamente as informações contidas nos equipamentos encontrados sem que ocorra nenhuma alteração, será necessário o uso de sistemas operacionais forenses e/ou *hardwares* forenses. Este procedimento tem como objetivo evitar a invalidade da prova, caso os dispositivos computacionais não fossem preservados de forma correta (ELEUTÉRIO et. al. 2011).

Os sistemas operacionais forenses normalmente são gravados de forma que quando os computadores forem inicializados, somente será disponibilizada a leitura dos dados (*read-only*), para que os discos rígidos possam ser inspecionados. Os sistemas operacionais forenses que mais se destacam são o Knoppix e o Helix (ELEUTÉRIO et. al. 2011).

Enquanto os sistemas operacionais forenses são utilizados somente no modo leitura, os hardwares forenses são criados especificamente para realizar a cópia dos diversos tipos de mídias, sempre garantindo que o equipamento apreendido não seja alterado (ELEUTÉRIO et. al. 2011).

Caso o perito não esteja preparado para utilizar tais procedimentos forenses, é recomendado coletar tais equipamentos para que posteriormente sejam analisados em laboratório. Como no cumprimento de mandados de busca, as apreensões somente deverão ser realizadas se existirem suspeitas de que os dispositivos contenham evidências necessárias à investigação (ELEUTÉRIO et. al. 2011).

2.3. QUANDO UTILIZAMOS COMPUTAÇÃO FORENSE

Como determinado no Código de Processo Penal em seu artigo 158, “quando a infração deixar vestígios será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.” Sendo assim, será necessário chamar um profissional qualificado para que examine os vestígios e produza um laudo à justiça na apuração de um delito. Entretanto, no caso da computação, este trabalho é realizado por um Perito Criminal em Informática, mas existem vários outros profissionais qualificados para tal trabalho. Entre eles estão: peritos particulares, auditores de sistemas, profissionais de TI e outros (ELEUTÉRIO et. al. 2011).

2.4. COMO UTILIZAR SUAS TÉCNICAS

Quando uma equipe de profissionais é utilizada para o cumprimento do mandado de busca e apreensão, o perito é responsável por orientar a equipe quanto à seleção, preservação e coleta dos equipamentos (SAMPAIO, 2007).

Sua primeira função é fazer a realização do reconhecimento do local, identificando todos os equipamentos computacionais existentes. Contudo, deverão ser tomadas providências para a preservação destes equipamentos que possuírem dados digitais, que incluem: não permitir a utilização destes equipamentos por pessoas estranhas à equipe sem a supervisão do perito e não ligar equipamentos computacionais desligados (SAMPAIO, 2007).

Dependendo da situação que for encontrada no local, recomenda-se interromper as conexões de rede existentes e retirar a fonte de energia dos equipamentos computacionais, desligando-os, exceto na possibilidade de flagrante delito; entretanto, essas ações somente deverão ser realizadas caso o perito tenha certeza de que isso não ocasionará perda de evidências digitais (SAMPAIO, 2007).

Em casos onde computadores estiverem ligados, poderá ser necessário copiar os dados da memória RAM, antes de desligá-los. A memória RAM é volátil, o que significa que assim que o computador é desligado, seus dados são perdidos, portanto, caso o perito suspeite que haja evidências na memória, o mesmo deverá utilizar ferramentas próprias para realizar a cópia dos dados da mesma (SAMPAIO, 2007).

Algo que poderá facilitar a vida do perito quanto à busca por informações em todos os equipamentos computacionais encontrados é entrevistar as pessoas que residem e/ou trabalham no local sobre o uso desses equipamentos, contudo, poderá juntar as informações obtidas para melhor selecionar quais equipamentos deverão ser apreendidos no local (SAMPAIO, 2007).

Não se recomenda a utilização de equipamentos computacionais no local, pois tal prática pode apagar/alterar dados armazenados mesmo que o usuário não apague nenhum arquivo por vontade própria (SAMPAIO, 2007).

Após a realização de tais providências, devem ser coletados somente os equipamentos computacionais que possam conter as evidências desejadas, desde que o acondicionamento seja realizado de forma correta e cuidadosa para que o

perito possa aplicar o uso de ferramentas forenses posteriormente (SAMPAIO, 2007).

Existem vários modos de se aplicar a Computação Forense, entretanto, existe um processo a ser seguido:

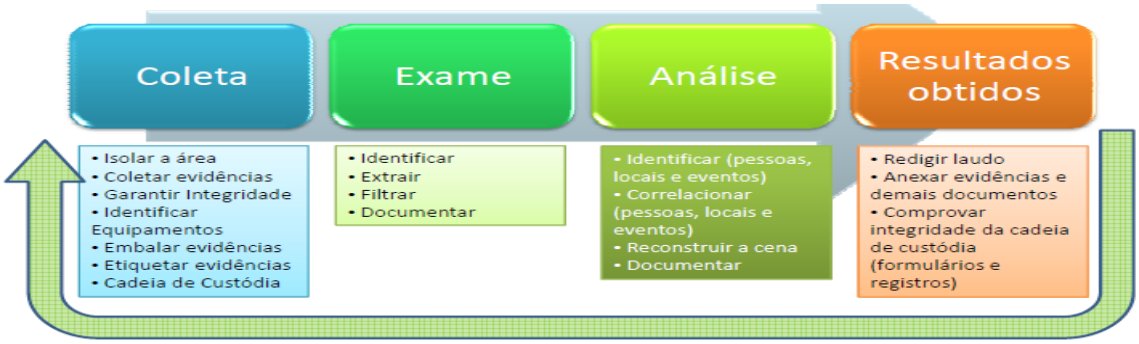

Figura 1: Fases de um Processo de Investigação

Fonte: (<http://www.cin.ufpe.br/~ruy/crypto/seguranca/Forense_Computacional(UFPE).pdf>)

Na fase da Coleta de Dados o foco é a identificação de possíveis fontes de dados. Entre essas fontes estão computadores, *notebooks*, *pendrives*, CDs, DVDs, dispositivos de armazenamento em rede, máquinas fotográficas, etc (SAMPAIO, 2007).

Durante a fase de Coleta, são utilizadas várias ferramentas para a duplicação dos dados encontrados, portanto, deve-se garantir a integridade dos mesmos para que as evidências não sejam invalidadas como provas. Normalmente a garantia da preservação e da integridade destes dados consiste no uso de ferramentas que aplicam o uso de *hash*. Após serem apreendidos, os materiais de informática deverão estar relacionados a uma cadeia de custódia (SAMPAIO, 2007).

Quando a origem dos dados já foi identificada, o perito necessita adquiri-los, e para que essa aquisição seja consolidada, é preciso passar por um processo que

consiste em três etapas: Identificação de Prioridade; Cópia dos Dados; Garantia e Preservação de Integridade (SAMPAIO, 2007).

Na Identificação de Prioridade o perito estabelece a ordem na qual os dados serão coletados. Para o perito saber quais dados devem ser coletados, seguem algumas prioridades: os dados voláteis devem ser coletados imediatamente, pois serão apagados assim que o equipamento for desligado; os dados de esforço são os quais poderão envolver para o perito, o tempo gasto, o custo e possivelmente serviços de terceiros para sua identificação, e por último o valor estimado dos dados a ser coletados; nesta etapa o perito deve estimar o valor para cada fonte de dados e assim definir a sequência na qual essas fontes serão investigadas (SAMPAIO, 2007).

Na etapa de cópia dos dados os peritos normalmente utilizam duas maneiras de salvar os dados encontrados, a cópia lógica (*Backup*), na qual gravam o conteúdo dos arquivos e diretórios de um volume lógico, e a cópia via imagem do disco ou cópia *Bit-a-Bit*, que cria uma imagem do disco a ser examinado por inteiro, desde espaços livres e até os espaços não utilizados. Com isso é possível recuperar arquivos que foram excluídos e dados não alocados pelo sistema (SAMPAIO, 2007).

E por último a garantia e preservação de integridade, que consiste em manter a integridade dos atributos de tempo *mtime (Modification Time), atime (Access Time)* e *ctime (Creation Time*); esses atributos de tempo são conhecidos por *MAC Times (Modification/Access/Creation Time)* (SAMPAIO, 2007).

Com o início da fase de exame dos dados, sua principal finalidade é localizar, filtrar e extrair todas as informações que forem relevantes à investigação, portanto, devemos considerar a capacidade de armazenamento dos dispositivos atuais e os diferentes formatos dos arquivos, já que muitos deles possibilitam o uso da esteganografia para ocultar dados. Contudo, o perito deverá estar atento e apto para identificar e recuperar esses dados ocultados. Com a grande quantidade de dados recuperados, podem existir muitas informações irrelevantes e devem ser filtradas somente as que forem relevantes para a investigação (SAMPAIO, 2007).

Quando a restauração da cópia dos dados estiver concluída, é necessário que o perito faça uma avaliação dos dados encontrados. Nesta avaliação o perito normalmente tem que dizer quais arquivos haviam sido removidos e quais foram recuperados, arquivos ocultos, fragmentos de arquivos encontrados nas áreas não alocadas e fragmentos de arquivos encontrados em setores alocados, mas que não foram utilizados pelo arquivo (SAMPAIO, 2007).

Quando as fases de extração dos dados relevantes são concluídas, a concentração do perito deverá se focar na etapa de análise e interpretação das informações, cuja finalidade é identificar pessoas, locais e eventos e definir como os mesmos estão inter-relacionados, entretanto, normalmente é necessário correlacionar informações de todas as fontes de dados possíveis (SAMPAIO, 2007).

Com a obtenção dos resultados das etapas anteriores, conclui-se que a interpretação e apresentação dos resultados é a etapa conclusiva da investigação. Quando o laudo pericial é elaborado pelo perito, o mesmo deve ser escrito de forma clara e concisa, listando todas as evidências encontradas e analisadas e com todas as informações descritas no laudo, o qual deve apresentar uma conclusão imparcial e final a respeito da investigação (SAMPAIO, 2007).

O laudo pericial tem que ser um documento de fácil interpretação, contudo, é indicado que o mesmo possua as seguintes seções: finalidade da investigação, autor do laudo, resumo do incidente, relação de evidências analisadas e seus detalhes, conclusão, anexos e glossário. Deve constar também no laudo pericial a metodologia, as técnicas e os *softwares* e equipamentos empregados. Com essas informações bem redigidas torna-se mais clara a reprodução das fases da investigação (SAMPAIO, 2007).

2.5. POR QUE UTILIZAR SUAS TÉCNICAS

O uso da Computação Forense atualmente deve-se aos diversos tipos de fraudes e crimes, que utilizaram algum meio eletrônico em algum momento para este fim. Entretanto, a missão da perícia forense é obter provas que irão se tornar o elemento chave na decisão jurídica, tanto na esfera civil quanto na criminal. Por isso na elaboração do laudo pericial é crítico seguir uma metodologia estruturada visando o sucesso nestes projetos (FREITAS, 2003).

Neste capítulo foi apresentado o termo Computação Forense, com isso, foi descrito o que é a Computação Forense nos dias atuais, sendo que somente pessoas especializadas devem aplica-la. A partir dai foi-se apresentado quais são os locais que ela deve ser aplicada no local do crime, portanto, não são todos os locais que se a Computação Forense deve ser aplicada, os locais para serem consideradas cenas de crimes eletrônicos devem conter ao menos um equipamento computacional para que um perito seja chamado para analisar o mesmo. Com o equipamento devidamente localizado, o perito deverá seguir um padrão de investigação na cena de crime, para assim não perder nenhum elemento chave para decisão jurídica, tanto na esfera civil quanto na criminal.

3. SISTEMAS OPERACIONAIS E APLICATIVOS PARA COMPUTAÇÃO FORENSE

Com os diversos tipos de Sistemas Operacionais existentes hoje no mercado, o escolhido para a maioria das distros Forenses é o Linux, por ser *open source*, ser seguro e estar em constantes atualizações, com isso, neste capítulo apresentará as funções de um Sistema Operacional e suas funções e uma breve apresentação do Linux. Sendo assim, serão apresentadas algumas das distribuições Forenses mais conhecidas do mercado de trabalho e também algumas ferramentas utilizadas por profissionais.

3.1. SISTEMAS OPERACIONAIS E SUAS FUNCÕES

Para a inicialização da parte física de um computador, necessita-se de um sistema operacional, que tem como função fornecer tarefas para controlar os dispositivos, da mesma maneira que fornece gerência, escalonamento e interação de tarefas, mantendo a integridade do sistema (LOPES, 2008).

Para o funcionamento adequado do sistema operacional, é necessária a inicialização de todos os processos que serão utilizados. Estes processos podem ser desde arquivos que devem ser atualizados frequentemente até arquivos que processam dados úteis para o sistema. O acesso destes processos pode ser feito pelo gerenciador de tarefas, onde temos todos os processos que estão em funcionamento desde a inicialização do sistema até a sua utilização atual (LOPES, 2008).

Se o sistema operacional de um computador é utilizado por muitas pessoas, podemos considerá-lo um sistema complexo. Todavia, para deixar os mesmos mais

fáceis de serem escritos, ele é dividido em uma série de módulos, que ficam responsáveis cada um por uma função. Geralmente os módulos de um computador multiusuário são: Kernel, Gerenciador de processos, Escalonador e Gerenciador de arquivos (LOPES, 2008).

3.1.1. Kernel

Chamado de executivo em tempo real, e sendo a parte mais importante do sistema operacional, o Kernel é responsável por executar as seguintes informações: Chaveamento de processos, controle e programação de dispositivos de hardware, gerência de memória, gerência de processos e processamento de exceções e de interrupções (LOPES, 2008).

3.2. LINUX

O surgimento do nome Linux deve-se à mistura entre Linus e Unix. O termo *Linus* vem do seu criador Linus Torvalds; já o termo *Unix* deve-se ao nome de um sistema operacional de grande porte (LOPES, 2013).

Segundo sua origem, o Unix tem ligação com o sistema operacional Multics, projetado por volta de 1960. O projeto Unix foi realizado pelo Massachusetts Institute of Tecnology (MIT), General Eletric (GE), pelos laboratórios Bell (Bell Labs) e pela American Telephone na Telegraph (AT&T) (LOPES, 2013).

Enquanto Ken Thompsom era um pesquisador do Multics e trabalhava na Bell Labs, viu a empresa em que trabalhava sair do projeto do Multics, entretanto, continuou por conta própria a estudar o sistema. Com isso, surgiu a ideia de criar algo menor que o Multics, mas que conservasse as ideias básicas do sistema. O nome Unix foi dado por Brian Kernighan, também pesquisador da Bell Labs (LOPES, 2013).

Dennis Ritchie, em 1973, reescreveu todo o código do sistema Unix numa linguagem de alto nível, criada e nomeada por ele próprio, o *C*. Com isso o sistema ganhou grande aceitação por usuários externos a Bell Labs (LOPES, 2013).

Uma alteração no código do Unix, entre 1977 e 1981, pela AT&T, acarretou no lançamento do System III, enquanto em 1983, foi lançado o Unix System IV, que passou a ser vendido. Atualmente o mesmo ainda é comercializado por empresas como IBM, HP, Sun, etc. Por ser um sistema de alto custo, seu uso é voltado para *mainframes* por diversas multinacionais (LOPES, 2013).

O Minix é uma versão do Unix, porém gratuita e de código-fonte aberto. Foi criado originalmente para uso educacional, entretanto, seu código não possui nenhum código da AT&T e graças a isso pode ser distribuído gratuitamente (LOPES, 2013).

3.3. HELIX

Baseado no Ubuntu, com interface Gnome, o Helix é uma distribuição Linux *live*, desenvolvida pela E-Fense. O grande lote de ferramentas forenses presente no Helix auxilia desde a realização da imagem até a análise de mídias. Sua interface de produção de imagem forense é o *Adepto 2.1*, baseada na interface Air, que consegue selecionar informações sobre o dispositivo suspeito e configurar a saída do arquivo de imagem. Sendo assim, é gerado um log que permite o acréscimo de informações pelo usuário. O Helix possui também recursos como restauração de imagem ou clonagem do dispositivo em outra mídia (SAMPAIO, 2013).

3.4. FDTK

Primeiramente iniciado como trabalho de monografia, o FDTK é um sistema operacional baseado no Ubuntu, voltado completamente para a prática Forense

Computacional. Além de possuir centenas de ferramentas, sua interface é totalmente em português, tornando-a uma ferramenta de uso prático cujos resultados são precisos (JUNIOR, 2012).

Durante sua fase de desenvolvimento, foram encontrados três problemas**:** a falta de atualização de todas outras distribuições focadas em Forense Computacional, porém todas as outras distribuições foram completamente desenvolvidas em idioma estrangeiro, com isso, era difícil conhecer profundamente todas as ferramentas (JUNIOR, 2012).

O peso na escolha do *Linux* como projeto base para o desenvolvimento foi a grande possibilidade de customização, interface amigável, documentos disponibilizados e regularidade nas novas atualizações/versões, entretanto, na época não existia ainda nenhuma distribuição com foco forense que utilizava esta distribuição. Isto foi um impulso maior na sua escolha. Por possuir uma série de qualidades, a interface escolhida foi a Gnome (JUNIOR, 2012).

Figura 2: Interface Gráfica do FDTK

3.4.1. Ferramentas do FDTK

As ferramentas encontradas no FDTK são *open source*, e foram separadas por etapas, dentre as quais estão: Coleta de Dados, Exame de Dados, Análise de Evidências e Toolkits.

3.4.1.1. Coleta de Dados

A seguir temos uma lista das ferramentas e comandos utilizados na etapa de Coleta de Dados.

Comando	Descrição
Formulário	Formulário de Cadeia de Custódia
gnome-screenshot	Salvar imagens da àrea de trabalho ou de janelas individuais
aimage	Geração de imagem dos dados das mídias utilizando o padrão aff
air	Interface gráfica para dd/dcfldd, para criar facilmente imagens forense
dc3ddgui	Interface gráfica para O DC3DD, para criar imagens forense
dcfldd	Versão aprimorada pelo DOD-Departament of Defense do dd
dd	Ferramenta para geração de imagem dos dados
ddrescue	Recuperar dados de hds com setores defeituosos (bad blocks)
mondoarquive	Copiar dados de fitas, cd's, nsf ou hd's
mondorestore	Restaurar dados de fitas, cd's, nsf ou hd's
rdd	Versão mais robusta do dd
rddi	Prompt interativo do rdd
sdd	Versão da ferramenta dd para Fitas (DAT, DLT...)
memdump	Dumper de memória para sistemas UNIX-like

md5sum	Gerar hash md5
sha1sum	Gera hash sha 160bits
discover	Informações sobre Hardware
hardinfo	Informações e Testes do Sistema
lshw-gráfico	Lista os dispositivos de hardware em formato HTML
sysinfo	Mostra informações do computador e do sistema
wipe	Remover totalmente os dados das Mídias

Tabela 1 - Lista de ferramentas para Coleta dos Dados

A interface para acesso das ferramentas de Coleta de Dados pode-se ser vista na figura a seguir.

Figura 3: Ferramentas para Coleta dos Dados

3.4.1.2. Exame de Dados

A seguir temos uma lista das ferramentas e comandos utilizados na etapa de Exame de Dados.

Comando	Descrição
cabectract	Acessar conteúdo de arquivos .cab
orange	Ferramenta para manipular arquivos .cab
p7zip	Acessar arquivos zip
unace	Ferramenta para descompactar extensões .ace
unrar-free	Ferramenta para descompactar arquivos rar
unshield	Ferramenta para descompactar arquivos CAB da MS
xarchiver	Criar, modificar e visualizar arquivos compactados
zoo	Acessar arquivos compactados .zoo
dcraw	Acessar imagens cruas de câmeras digitais
exif	Ler informações EXIF de arquivos jpeg
exifprobe	Exame do conteúdo e da estrutura dos arquivos de imagens JPEG e TIFF
exiftran	Transformar imagens raw de câmeras digitais
exiftags	Adquirir informações sobre a câmera e as imagens por ela produzidas
exiv2	Manipular metadados de imagens
jhead	Visualizar e manipular os dados de cabeçalhos de imagens jpeg
jpeginfo	Ferramenta para coletar informações sobre imagens jpeg
antiword	Ferramenta para ler arquivos do MS-Word
dumpster	Acessar os arquivos da lixeira do Windows
fccu-docprop	Ferramenta para visualizar as propriedades de arquivos OLE
mdb-hexdump	Ferramenta para manipulação de arquivos MDB
readpst	Ferramenta para ler arquivos do MS-Outlook
reglookup	Utilitário para leitura e resgate de dados do registro do Windows

regp	Acessar o conteúdo de arquivos .dat
tnef	Acessar anexos de email's MS
bcrypt	Encriptar e decriptar arquivos usando o algoritmo blowfish
ccrypt	Encriptar e decriptar arquivos e streams
outguess	Detectar dados ocultos em imagens JPG
stegcompare	Comparar imagens jpeg e detectar a existência de steganografia
stegdimage	Detectar a existência de steganografia em imagens jpeg
stegdetect	Detectar a existência de steganografia em imagens jpeg
xsteg	Ferramenta gr fica para detectar steganografia em imagens jpeg
ghex2	Visualizar arquivos em formato HEX
hexcat	Visualizar arquivos em formato HEX
ghexdump	Visualizar arquivos em formato HEX
affcat	Verificar conteúdo de arquivos .aff sem montar
afcompare	Comparar dois arquivos .aff
afconvert	Converte aff -> raw, raw -> aff, aff -> aff recompactando-o
afinfo	Visualizar estatísticas sobre um ou mais arquivos aff
afstats	Visualizar estatísticas sobre um ou mais arquivos aff
afxml	Exportar metadados de arquivos aff para um arquivo xml
dcat	Localizar dados dentro de arquivos dd, aff, ewf
glark	Ferramenta semelhante ao grep para localizar dados
gnome-search-tool	Ferramenta gráfica de localização de arquivos
slocate	Localiza arquivos e indexa os disco
mac-robber	Coletar dados de arquivos para criar a linha de tempo (timeline)
mactime	Cria uma linha do tempo ASCII das atividades dos arquivos
ntfscat	Concatenar arquivos e visualizá-los sem montar a partição NTFS
ntfsclone	Clonar um sistema de arquivos NTFS ou somente parte dele
ntfscluster	Localizar arquivo dentro de cluster ou de v rios clusters NTFS
ntfsinfo	Obter informações sobre partições NTFS

ntfslabel	Verificar ou alterar a descrição de partições NTFS
ntfsls	Lista o conteúdo de diretórios em partições NTFS sem montá-los
fcrackzip	Ferramenta para quebrar as senhas de arquivos compactados em ZIP
john-the-ripper	Ferramenta para localizar senhas de usuários
medusa	Crack de senhas
ophcrack	Crack de senhas do Windows
e2undel	Ferramenta para recuperar arquivos em partições ext2
fatback	Ferramenta para recuperar dados de sistemas de arquivos FAT
foremost	Ferramenta para recuperação de imagens a partir dos cabeçalhos
gzrecover	Ferramenta para extrair dados de arquivos gzip corrompidos
magicrescue	Recuperação de imagens RAW, baseando-se nos cabeçalhos
ntfsundelete	Recuperar arquivos deletados em partições NTFS
recover	Ferramenta para recuperar todos inodes deletados de um disco
recoverjpg	Ferramenta para recuperar imagens jpg
scrounge-ntfs	Ferramenta para recuperar dados de partições NTFS
chkrootkit	Ferramenta para identificar a presença de rootkits no sistema
rkhunter	Ferramenta para identificar a presença de rootkits no sistema
fspot	Organizador de imagens fotos
gthumb	Visualizar e organizar imagens
imageindex	Gera galeria de imagens em html

Tabela 2 - Lista de ferramentas para Exame dos Dados

A interface para acesso das ferramentas de Exame de Dados pode-se ser vista na figura a seguir.

Figura 4: Ferramentas para Exame dos Dados

3.4.1.3. Análise de Evidências

A seguir temos uma lista das ferramentas e comandos utilizados na etapa de Análise de Evidências.

Comando	Descrição
coockie_cruncher	Analisar coockies
eindeutig	Analisar arquivos .dbx
fccu-evtreader	Script perl para visualizar arquivos de eventos da MS (EVT)
galleta	Analisar coockies do Windows
grokevt	Coleção de scripts construídos para ler arquivos de eventos do

	Windows
grokevt-addlog	Coleção de scripts construídos para ler arquivos de eventos do Windows
grokevt-builddb	Coleção de scripts construídos para ler arquivos de eventos do Windows
grokevt-dumpmsgs	Coleção de scripts construídos para ler arquivos de eventos do Windows
grokevt-findlogs	Coleção de scripts construídos para ler arquivos de eventos do Windows
grokevt-parselog	Coleção de scripts construídos para ler arquivos de eventos do Windows
grokevt-ripdll	Coleção de scripts construídos para ler arquivos de eventos do Windows
mork	Script perl para visualizar arquivos history.dat do firefox
pasco	Analisar cache do IExplorer
rifiuti	Analisar arquivos INF2 da MS
traceroute	Tracerouter
xtraceroute	Tracerouter gráfico

Tabela 3 - Lista de ferramentas para Análise de Evidências

A interface para acesso das ferramentas de Análise de Evidências pode-se ser vista na figura a seguir.

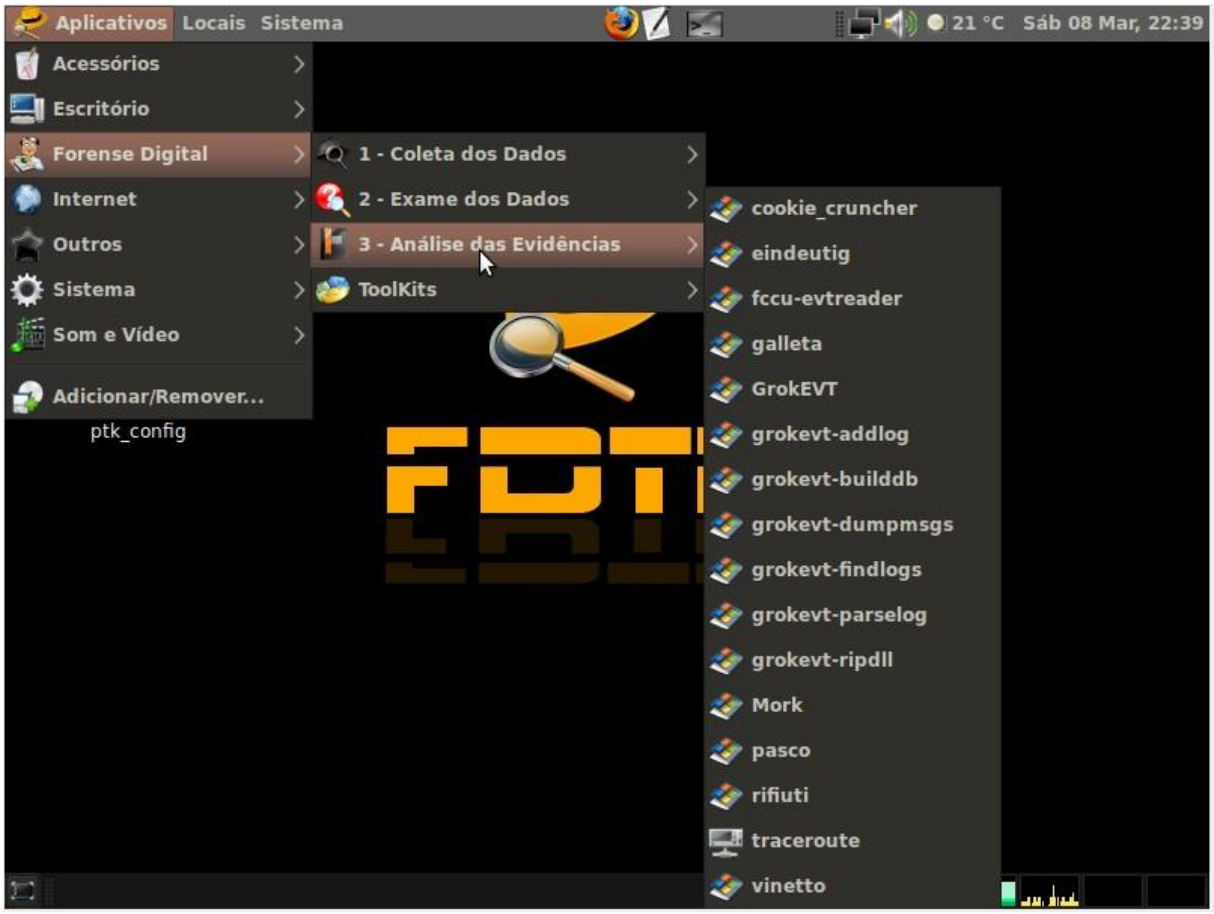

Figura 5: Ferramentas para Análise de Evidências

3.4.1.4. ToolKits

A seguir temos as ferramentas utilizada para realizar perícia em *browsers*.

Comando	Descrição
Autopsy	Framework que roda em um browser para realizar Perícias Forenses (http://www.sleuthkit.org/autopsy/)
PTK	Framework que roda em um browser para realizar Perícias Forenses (http://ptk.dflabs.com/)

Tabela 4 - Lista de Ferramentas ToolKits

A interface para acesso das ferramentas o ToolKit pode-se ser vista na figura a seguir.

Figura 6: Ferramentas ToolKits

3.5. NMAP

Criação de Fyodor, o Nmap é a ferramenta de verificação mais utilizada na Internet, sendo utilizada por milhares de profissionais espalhados pelo mundo. Seu código-fonte é distribuído em arquivos *.tar* comprimidos como *gzip* e *bzip2*, já os binários estão disponíveis para o Linux com formato RPM, Windows, MAC OS X e imagem de disco *.dmg.* O Nmap tem suporte para os diversos sistemas Windows, Linux e os demais sistemas (BEZERRA, 2012).

Com a utilização de pacotes crus de IP, o Nmap tem como objetivo determinar quais máquinas estão disponíveis na rede, quais serviços são oferecidos, quais sistemas operacionais e quais tipos de filtros de segurança são aplicados. Com foco voltado para a análise e retorno rápido de resultados, o Nmap pode fazer isso em uma grande rede de computadores, mas se for necessário utilizá-lo somente em um único computador, seu retorno também será bom (BEZERRA, 2012).

Com o passar dos anos, o número de funcionalidades do Nmap aumentou; mesmo assim sua principal função continua sendo o eficiente scanner de portas. O comando nmap <destino> consegue escanear mais de 1600 portas TCP no host <destino>. Contudo seu diferencial em relação aos outros scanners de portas é que enquanto a maioria somente mostra as portas nos estados abertos e fechado, o Nmap tem mais estados. Ele é dividido em seis estados de portas: aberto (*open*), fechado (*closed*), filtrado (*filtered*), não filtrado (*unfiltered*), open | *filtered* ou *closed* | *filtered* (BEZERRA, 2012).

3.5.1. Os Seis Estados de Portas Reconhecidos Pelo Nmap

É considerado estado aberto (*open*), quando a aplicação está em execução e aceitando conexões TCP ou pacotes UDP nesta porta, contudo, abre-se caminho para invasores e profissionais de segurança poderem infiltrar e explorar os dados. Enquanto a função dos administradores é procurar essas portas abertas e fechá-las ou protegê-las com firewalls, eles não devem deixá-las indisponíveis para os usuários (BEZERRA, 2012).

Quando uma porta se encontra fechada (*closed*) ela está acessível, entretanto, não tem nenhuma aplicação a ser ouvida nela. Mesmo a porta no estado de fechada serve para mostrar que uma máquina se encontra ligada; neste caso, pode-se descobrir o sistema operacional e outras informações do alvo (BEZERRA, 2012).

Em alguns casos o Nmap, não consegue determinar se a porta está aberta, pois a filtragem de pacotes impede que a ação de sondagem alcance a porta. Esses filtros podem ser implementados com *firewalls* dedicados ou de *host* e roteadores (BEZERRA, 2012).

O estado não filtrado (*unfiltered*) indica que a porta está acessível, entretanto, o Nmap é incapaz de dizer se a porta está aberta ou fechada (BEZERRA, 2012).

Se o Nmap não consegue determinar se a porta está aberta ou filtrada, ele coloca a mesma no estado de *open* | *filtered*. Entretanto, se a porta estiver fechada ou filtrada, a mesma é adicionada no estado de *closed* | *filtered* (BEZERRA, 2012).

3.6. FORENSIC TOOLKIT

Produzido pela empresa AccessData, o Forensic ToolKit (FTK), reúne as principais funções para a realização de exames forenses em dispositivos de armazenamento de dados. Seus vários aplicativos possuem recursos que podem ser utilizados a qualquer momento da realização do exame desta natureza (ELEUTÉRIO et. al. 2011).

A versão mais recente desta ferramenta é a 5.2.1, que possui uma interface gráfica intuitiva e permite que o perito tenha uma visão geral do conteúdo a ser analisado. Das muitas funcionalidades presentes na ferramenta, é possível citar: *Data Carving*, a indexação de dados, recuperação de arquivos, visualização de imagens e mensagens eletrônicas e o *Known File Filter* (KFF), que faz a seleção por filtro, palavras-chave, entre outras (ELEUTÉRIO et. al. 2011).

Uma funcionalidade muito útil desta ferramenta é que ao identificar o arquivo de interesse, ela poderá categorizá-lo em *bookmarks*. Com o arquivo categorizado, pode-se utilizar um módulo gerador de relatório da ferramenta, que assim cria vários arquivos em formato HTML, sendo assim, com ajuda de um *browser*, permite

navegar pelos resultados que estão organizados por categorias (ELEUTÉRIO et. al. 2011).

Outros módulos presentes no FTK são os para duplicação de imagem (*Imager*) e para a visualização dos registros internos do sistema operacional (*Registry Viewer*), entretanto, o FTK é uma ferramenta importante que pode ajudar o perito a desenvolver seu trabalho de forma eficiente (MADOOX, 2014).

3.7. ENCASE FORENSIC

Produzido pela Guidance, o software EnCase Forensic atualmente encontra-se na versão 7.09, e possui diversos recursos que auxiliam o perito na execução de exames em dispositivos de armazenamento computacional. Com o EnCase Forensic, o perito conseguirá recuperar arquivos apagados, pesquisar por palavras-chaves, visualizar arquivos em formato adequado, entre outras (ELEUTÉRIO et. al. 2011).

A vantagem de utilizar o EnCase Forensic é que ele pode ser utilizado durante qualquer fase do exame, por conter funcionalidades de duplicação de discos, recuperação de arquivos e visualização adequada. Entretanto, sua interface gráfica e suas funcionalidades ainda são menos intuitivas que a do FTK, contudo, o EnCase Forensic requer um treinamento para seu uso. Seu principal destaque é a possibilidade de programar funções novas por meio dos EnScripts, o que deixa a ferramenta customizada à necessidade do perito e permite que novas funções/procedimentos possam ser implementados com a necessidade de cada caso (ELEUTÉRIO et. al. 2011).

A interface para a utilização do *software* EnCase pode-se ser vista na figura a seguir.

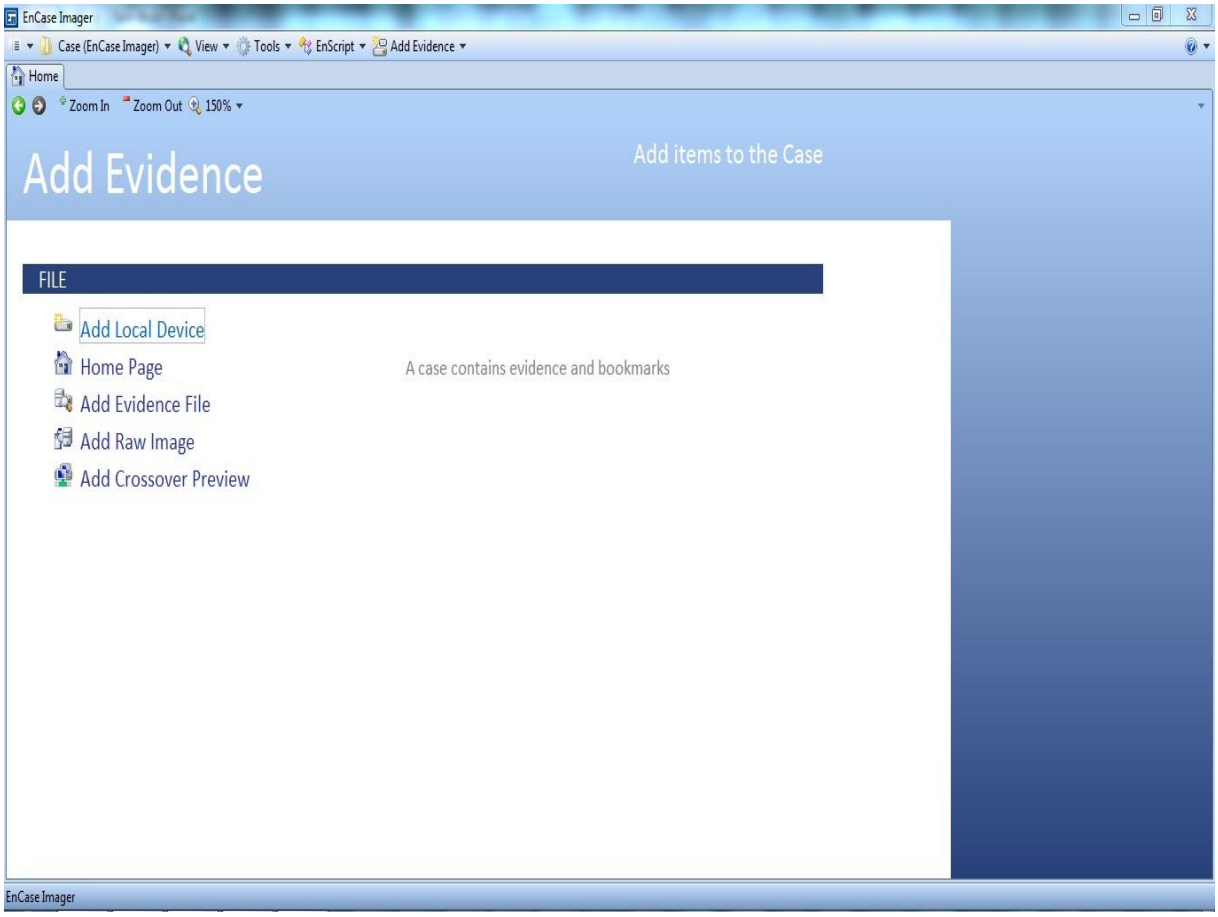

Figura 7: Interface principal do EnCase

Ao decorrer deste capitulo foi apresentado o conceito de Sistemas Operacionais com foco no Linux, sendo que, o mesmo é utilizado como base na maioria dos Sistemas Operacionais Forenses encontrados no mercado. Sendo assim, teve-se uma breve apresentação de algumas distros Forenses e ferramentas que são utilizadas por peritos durante o processo de analise das evidências encontradas no local do crime.

4. FDTK – FORENSE DIGITAL TOOLKIT

Neste capítulo é apresentada a distro FDTK, que é um Sistema Operacional Forense *open source*, desenvolvido totalmente em português com a proposta de estar simplificando o estudo das técnicas e ferramentas utilizadas na Computação Forense para alunos, professores e profissionais da área.

4.1. HISTÓRIA DA DISTRO FDTK

Com a proposta de estudar técnicas utilizadas na Computação Forense, que é uma área de pouco conhecimento dos profissionais de Tecnologia da Informação, o Professor Msc. Leonardo lemes, lança um desafio: “será que é muito difícil fazer uma distribuição Linux focada em Forense Computacional?”. Com o desafio lançado, Paulo Neukamp fez do dele o sucesso que é a ferramenta FDTK hoje em dia (NEUKAMP, 2011).

Com o inicio do da elaboração do trabalho proposto, ficou claro que seria necessário perder horas de estudos na criação da nova distro. Sendo assim, a ideia inicial era apenas criar e customizar os menus de acesso das ferramentas estudadas e definir quais delas fariam parte da distro (NEUKAMP, 2011).

Com o estudo feito, Paulo Neukamp foi capaz de identificar várias discrepâncias em relação às distribuições Linux que se auto intitulavam “Distribuição para Forense Computacional”. Entre essas discrepâncias estavam algumas ferramentas oferecidas por estas distribuições; a maioria delas estava desatualizada havia pelo menos 2 anos, o que em relação à segurança é uma eternidade. Contudo, foram identificados pelo menos três problemas que afastam os profissionais de Segurança da Informação: a barreira de idioma, ter profundo conhecimento das ferramentas e

nenhuma menção a que etapas estavam envolvidas em uma perícia (NEUKAMP, 2011).

À primeira vista, foi identificado que existia a possibilidade de criar uma nova distro com foco direcionado em Forense Computacional que atenderia os três problemas anteriores, além de poder ser utilizada como ferramenta de ensino visando preparar novos profissionais para o mercado (NEUKAMP, 2011).

Quando entrou na etapa de conclusão, o projeto recebeu o nome de FDTK-UbuntuBr. Sendo assim, o primeiro passo foi identificar as ferramentas Open Source disponíveis nas distros estudadas. Com o nome de mais de 100 ferramentas em uma lista, o foco agora era a escolha de qual distribuição iria ser utilizada como base do projeto. Essa escolha foi baseada em uma série de características, dentre elas: regularidade no lançamento de novas versões, facilidade de utilização, disponibilidade de documentação tanto técnicas quanto de utilização e possibilidade de efetuar as customizações necessárias, entre outras (NEUKAMP, 2011).

Com os resultados encontrados por uma minuciosa pesquisa, a distribuição escolhida foi o Ubuntu. Entretanto, essa escolha seria um grande desafio, pois até o momento nenhuma das outras distribuições com foco Forense Computacional a utilizava com base na época, mas olhando com outros olhos, ela seria a primeira a ser baseada no Ubuntu. A escolha pelo Ubuntu acabou se tornando um diferencial, pois anos mais tarde todas as principais distribuições mundiais utilizavam o Ubuntu como base (NEUKAMP, 2011).

Após a definição de quais ferramentas fariam parte do projeto e que a distribuição Linux seria utilizada como base, passou-se para o próximo passo, qual interface gráfica seria utilizada. Contudo, a sua escolha não foi difícil, pois além de possuir uma série de qualidades o Gnome também é a interface gráfica mais utilizada no mundo (NEUKAMP, 2011).

Com as definições concluídas, chegou a hora de por a mão na massa para a criação de mais de 100 scripts que poderão ser executados a partir de um novo menu. Com esse novo menu inserido, passou-se a ter agora um grupo de ferramentas Forense

Digital divididas em quatro etapas, que são: coleta dos dados, exame dos dados, analise das evidencias e ToolKits. Com o menu já adicionado, chegou a hora de escolher um nome para a nova distribuição. O nome recebeu a junção de três menções, a primeira era a abreviação do Forense Digital ToolKit, logo em seguida a menção da distribuição utilizada e o idioma, portanto, o nome acabou ficando FDTK-UbuntuBr (NEUKAMP, 2011).

Com tudo em seus conformes, após horas de ajustes, definições e testes, a versão 1.0 foi concluída a tempo de ser defendida na monografia. Sendo assim, veio à recompensa: o trabalho recebeu nota máxima por tratar de um tema pouco conhecido, deixar um legado para a academia e mostrar áreas ainda carentes de pesquisa relacionadas ao tema (NEUKAMP, 2011).

No inicio não houve nenhum investimento financeiro, pois os mesmos estavam escassos, entretanto, um site foi criado para a divulgação do trabalho e um servidor para hospedar o mesmo, para que tanto a comunidade cientifica quanto a profissional pudesse utilizá-lo. Com o site pronto e a ISO devidamente hospedada em dois repositórios (codigolivre.org e Unicamp), iniciou-se a fase de divulgação, contudo, em 2007 o melhor lugar para isso era a comunidade Linux “Dicas-L” que possuía 40.000 assinantes. Portanto, o professor que incentivou o projeto, Leonardo Lemes, enviou um e-mail ao amigo e mantenedor da Dicas-L, Rubens Queiroz, que assim fez a divulgação do trabalho, e somente nas primeiras duas semanas já foram feitos mais de 7.000 downloads através de sua lista (NEUKAMP, 2011).

Mesmo com o ano de 2007 cheios de boas notícias, a mais relevante entre elas foi a criação de uma disciplina no curso de Graduação em Segurança da Informação na Unisinos com a adoção da distro FDTK como base de estudos pelos alunos. Entretanto, a adoção da distro acarretou a chegada de várias mensagens de dúvidas e sugestões enviadas por alunos e entusiastas da área que passaram a utilizá-la no seu dia-a-dia. Com o passar de um ano do seu lançamento, foi liberada a versão 2.0 com melhorias, atualizações e uma nova interface gráfica com logomarca e detalhes personalizados (NEUKAMP, 2011).

Após o lançamento da nova versão, um fato inusitado aconteceu: o professor Aderbal Botelho, de Forense Computacional e também perito do estado de Alagoas entrou em contato com uma proposta de parceria, já que o mesmo iria ministrar um curso com dois alunos de um órgão Federal de Brasília. Sendo assim, a parceria foi imediatamente fechada. Ainda neste período, foram realizadas diversas palestras, projetos e trabalhos acadêmicos que utilizaram a distro como base em suas pesquisas. Um tempo depois foi lançada a versão 3.0 e sem ser diferente das outras, logo na primeira semana foi baixada 13.000 vezes. Sendo assim, continuam os trabalhos para a versão 4.0 do FDTK-UbuntuBr (NEUKAMP, 2011).

A figura abaixo apresenta a linha do tempo dos dados referentes à história da criação e evolução da distro FDTK.

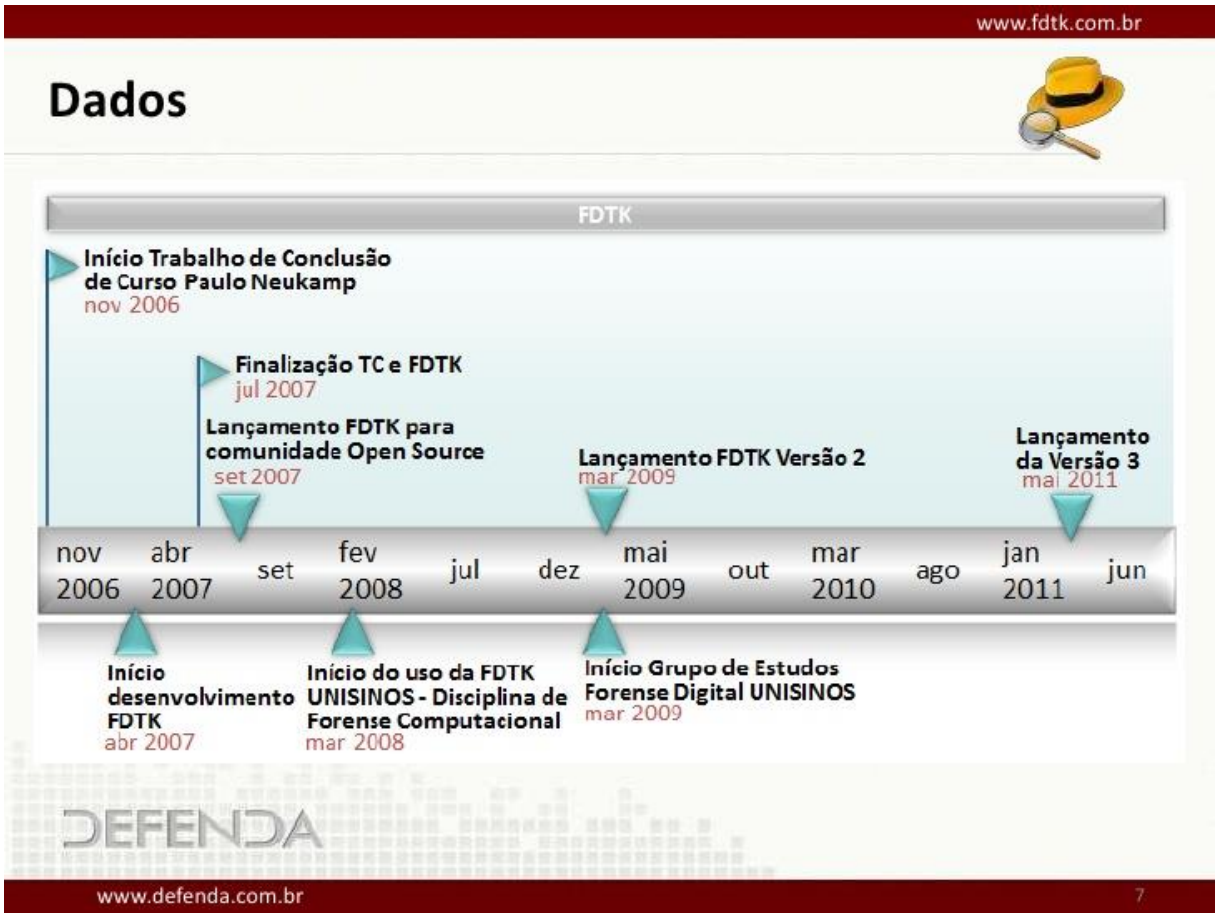

Figura 8: Linha do Tempo: FDTK

Fonte: (<LEMES, L., NEUKAMP, P. A., DA SILVA, P. C., 2011, p. 7>)

4.2. FORENSE DIGITAL

O termo *Forense Digital* é definido como inspeção científica e sistemática em ambiente computacional, com intenção de obter os mais variados tipos de evidências de fontes digitais. Sendo assim, pode-se determinar se o ambiente analisado foi ou não utilizado para a realização de atividades ilegais ou não autorizadas (NEUKAMP, 2014).

Como pode-se ver a seguir, o processo de investigação é dividido em quatro etapas: coleta dos dados, exame dos dados, análise dos dados e laudo pericial (NEUKAMP, 2014).

Figura 9: Ciclo de uma Investigação

Fonte: (<http://fdtk.com.br/wiki/tiki-index.php>)

4.2.1. Coleta dos Dados

A coleta dos dados tem como principal foco a identificação de prováveis fontes de dados como computadores, notebooks, máquinas fotográficas, mídias de armazenamento, entre outros. Contudo, locais fora dos domínios físicos da cena investigada também são averiguados (NEUKAMP, 2014).

Com os dados identificados, é necessária a aquisição dos mesmos, sendo seguidas três etapas: identificação de prioridade, onde é estabelecida a ordem em que os dados foram coletados levando em conta sua volatilidade, esforço e o valor; cópia dos dados: os dados encontrados devem ser copiados com a utilização de ferramentas apropriadas para o serviço; garantia e preservação de integridade: assim que alguma fonte de dados é coletada, é necessário utilizar alguma ferramenta que garanta a integridade dos dados, pois qualquer alteração ou perda da mesma podem cancelar seu uso em um tribunal (NEUKAMP, 2014).

4.2.2. Exame de Evidências

Nesta etapa, somente serão avaliadas e extraídas as informações que são relevantes a uma investigação, através da correta utilização das ferramentas e técnicas que o perito tem ao seu dispor, sendo assim, deve-se filtrar e reduzir somente os dados que precisam de um exame minucioso (NEUKAMP, 2014).

4.2.3. Análise dos Dados

Enquanto as fases de coleta e exame dos dados visam à identificação e investigação das fontes encontradas na cena do crime, a fase de análise tem como objetivo identificar pessoas, locais e eventos apontando como esses elementos

devem estar inter-relacionados. Normalmente correlacionam-se informações de varias fontes de dados (NEUKAMP, 2014).

4.2.4. Laudo Pericial

Com a interpretação dos resultados obtidos nas três etapas anteriores, o perito elabora um Laudo Pericial, que obrigatoriamente tem que ser escrito de forma clara e concisa, categorizando todas as evidências analisadas e localizadas. Sendo assim, apresenta-se uma conclusão imparcial e final sobre a investigação (NEUKAMP, 2014).

4.3. CADEIA DE CUSTÓDIA

O preenchimento do formulário de cadeia de custodia será feito utilizando ferramentas disponíveis no FDTK-V3, entretanto, o seguinte cenário deverá ser imaginado: o perito recebeu um *pen drive* para que a perícia fosse realizada, sendo assim, ao receber a possível prova, foi iniciado um processo de Geração de imagem de dados (DD) para garantir a integridade dos dados (CONSTANTINO, 2012).

Figura 10: Pen drive entregue ao Perito

O *pen drive* possui uma pasta (Gabinete Cooler Master) com quatro arquivos, três deles com a extensão .jpg (1.jpg, 2.jpg e 3.jpg), além de um documento de texto de extensão .txt (Especificações).

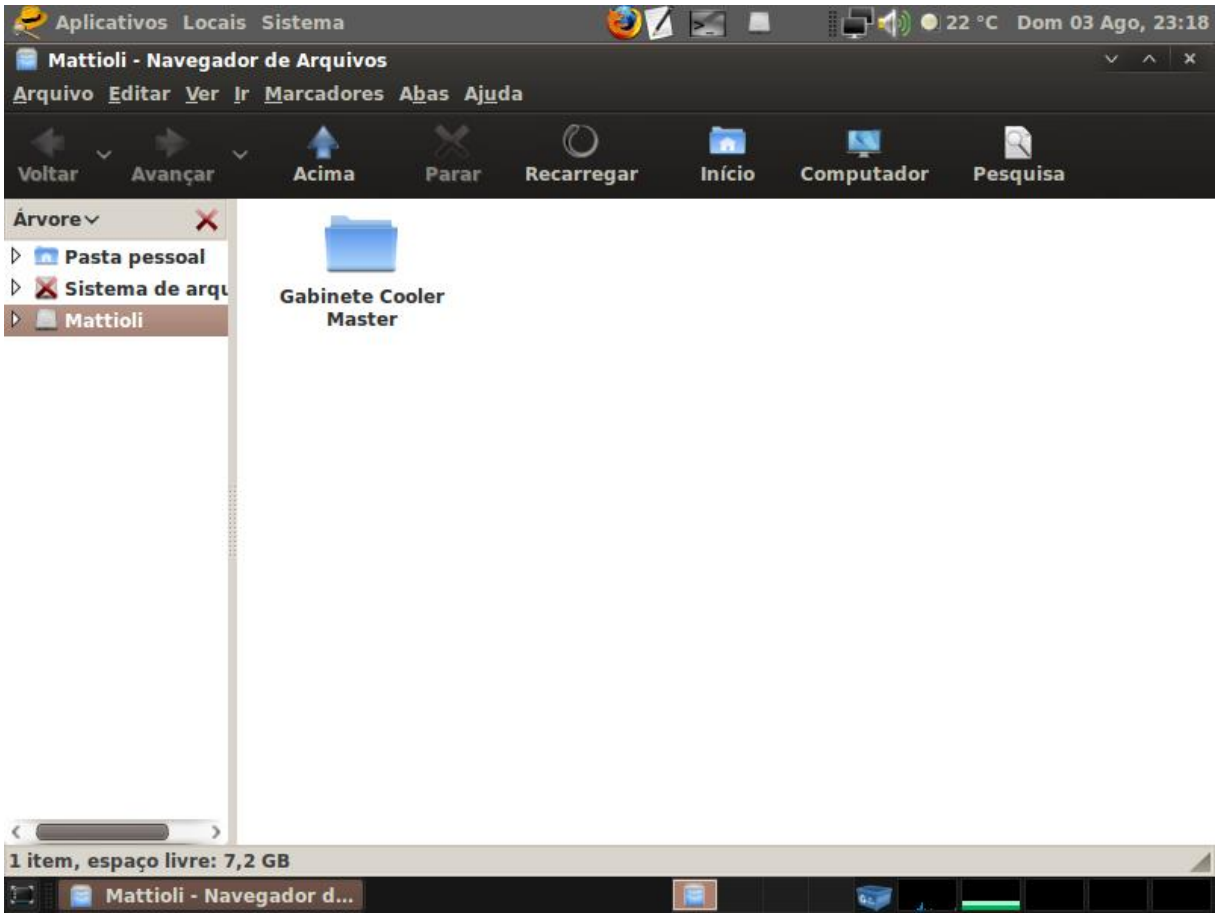

Figura 11: Pasta dentro do pen drive

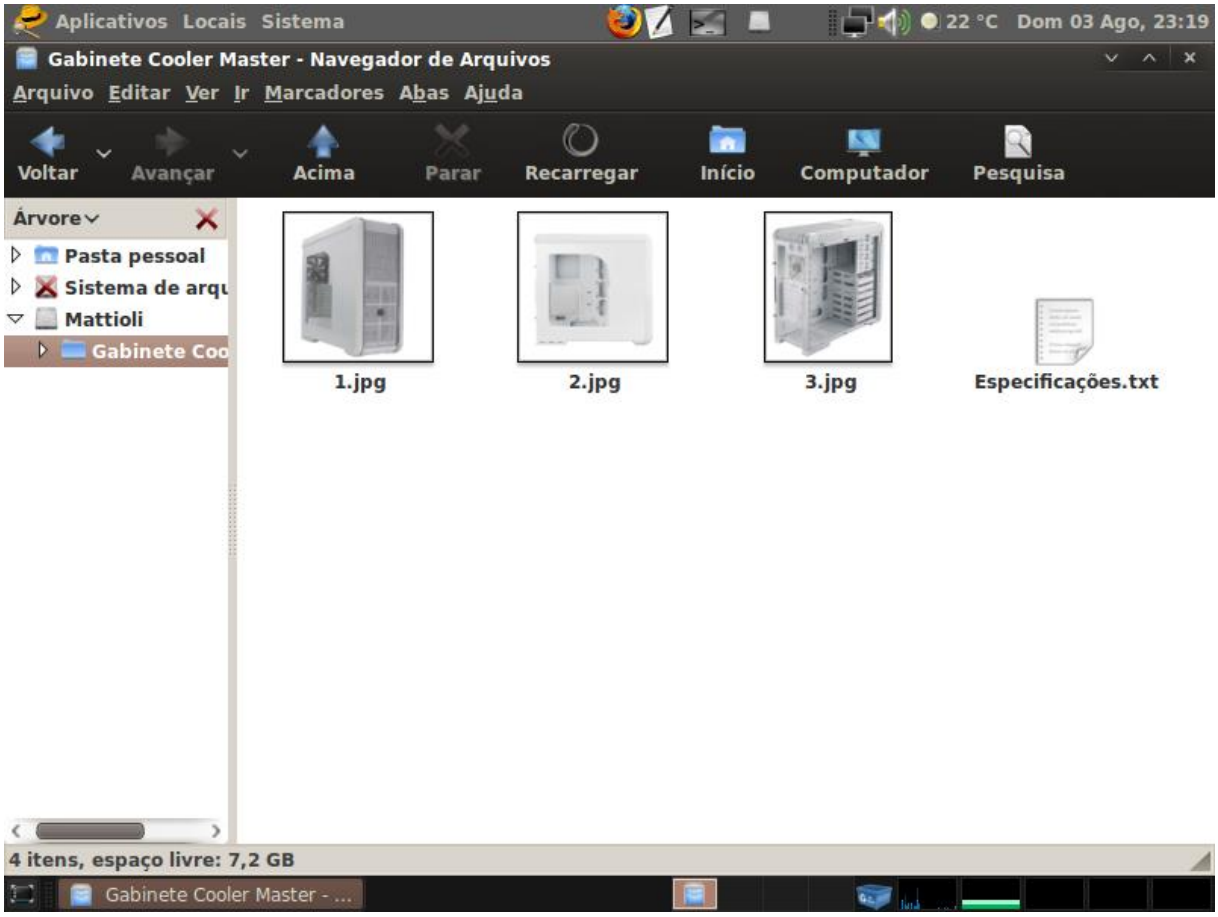

Figura 12: Arquivos dentro da pasta no pen drive

A ferramenta que será utilizada para criar imagem dos dados é a dd. DD (Data Description) tem como finalidade apenas copiar e/ou converter arquivos. A vantagem da utilização do dd é que ele pode ser usado para cópia/manipulação de arquivos sem mudar seu estado original, ou até mesmo realizar *backup* de uma partição, de um disco ou até mesmo de um setor de inicialização de um disco rígido na MBR (*Master Boot Record*) (NEUKAMP, 2014).

O dd tem a característica de fazer a cópia dos arquivos *bit* a *bit* de acordo com o modelo FIFO (*first-in, first-out* – primeiro que entra é o primeiro que sai) (NEUKAMP, 2014).

Basicamente, o dd lê o stdin e escreve o stdout, enquanto na entrada stdin, a ferramenta recebe os dados e envia para a saída do sistema stdout, onde “copia”

cada *bit* para um novo arquivo. O arquivo copiado não possuirá um *hash* diferente do arquivo original, pois nenhum *bit* dos dados foi alterado (NEUKAMP, 2014).

Para a utilização do dd é empregada a seguinte sintaxe:

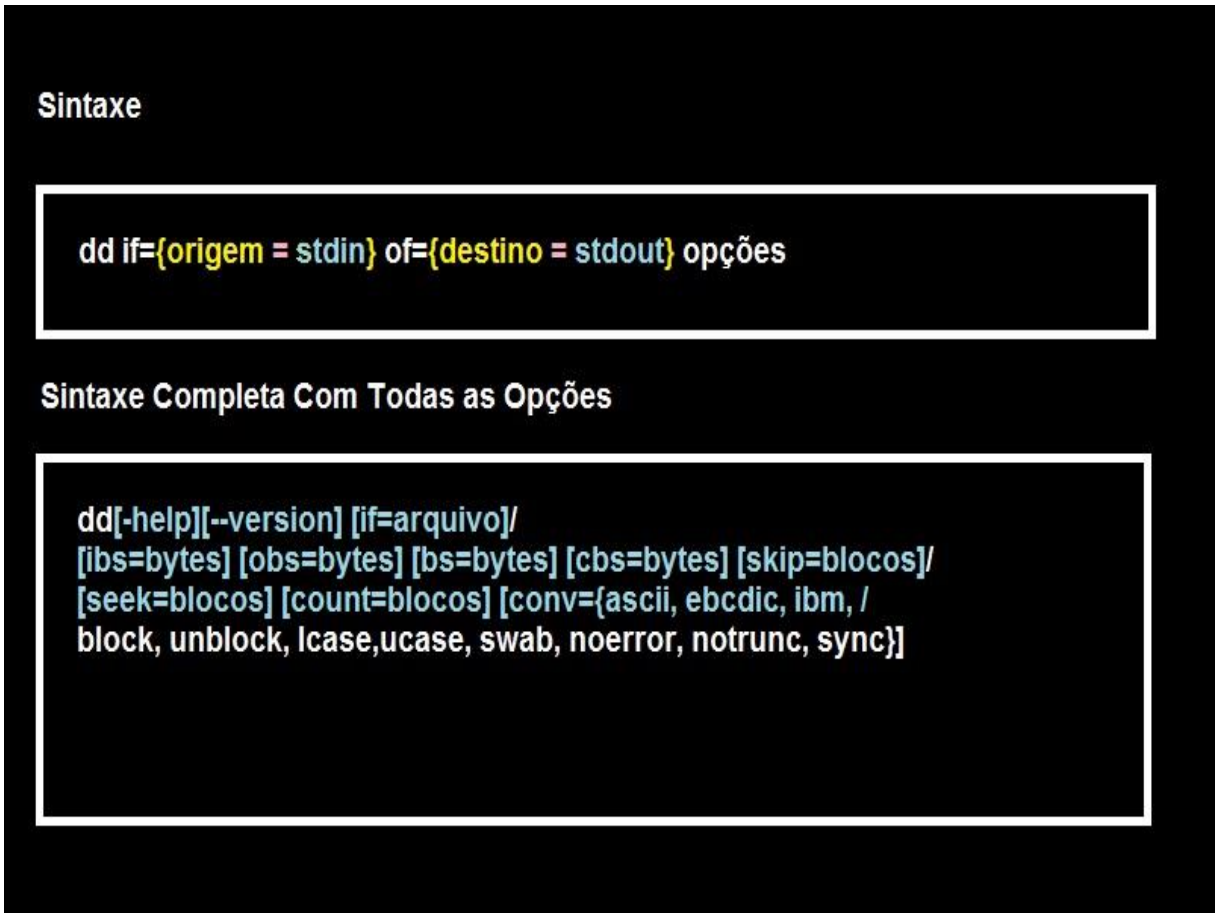

Figura 13: Sintaxe para a utilização da ferramenta DD

Fonte: (<http://fdtk.com.br/wiki/tiki-index.php?page=dd>)

Neste momento será feita a compactação do *pen drive* entregue ao perito para que possa, ao final, preencher o formulário de cadeia de custódia, para que este seja utilizado como prova de crime. O comando utilizado para fazer a compactação do *pen drive* pode ser visto na imagem a seguir.

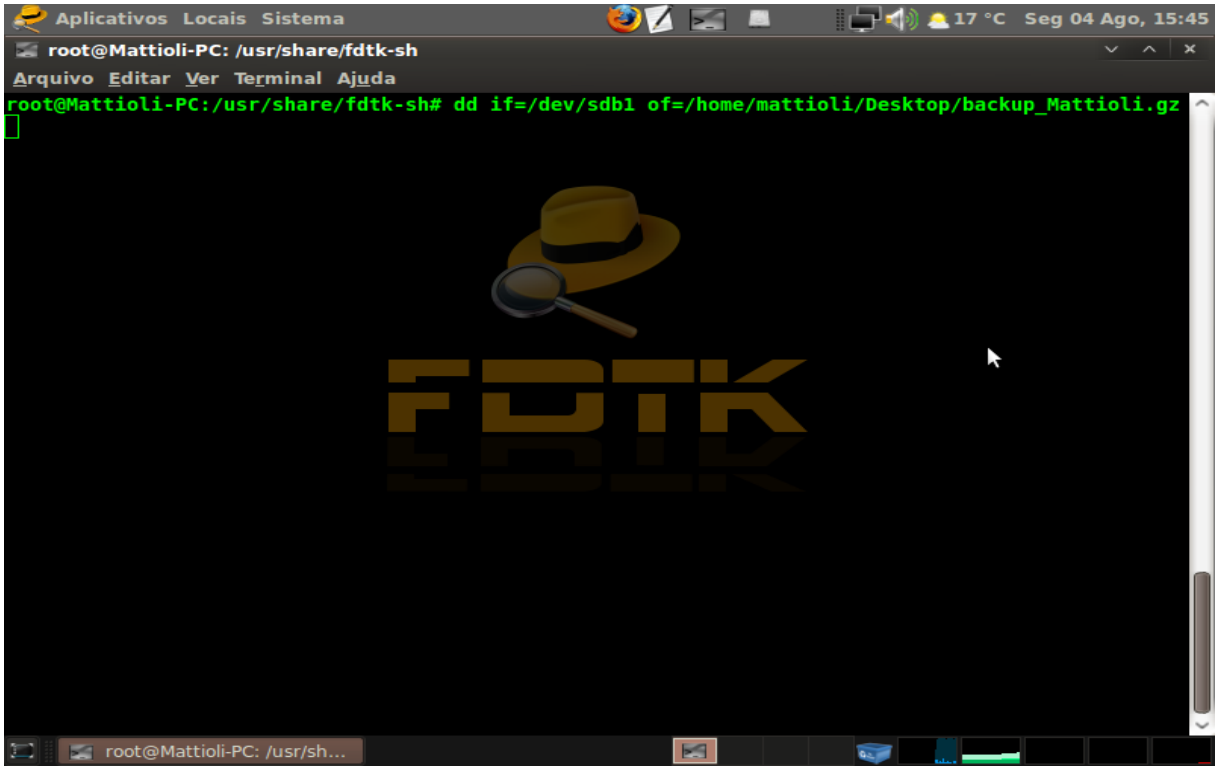

Figura 14: Comando Utilizado para Compactar os Dados do pen drive

Como podemos ver na imagem anterior, o comando dado é dividido em três partes: **dd** sem o qual não seria possível executar o comando; **if=/dev/sdb1** , que é a origem dos dados, ou seja, é o diretório que será compactado; e por ultimo **of=/home/Mattioli/Desktop/backup_Mattioli.gz,** que é o destino que será criado o arquivo compactado contendo os dados do pen drive apreendido.

Após a conclusão da compactação podemos ver na figura a seguir, os dados gerados a partir do comando no terminal, sendo ele: o número de registros de entrada e saída de dados, o tamanho do *pen drive* clonado, o tempo do comando executado e a velocidade da cópia dos dados, sendo assim, o perito terão alguns dos dados necessários para serem relacionados no laudo pericial que deverá ser apresentado com uma conclusão imparcial e final da investigação.

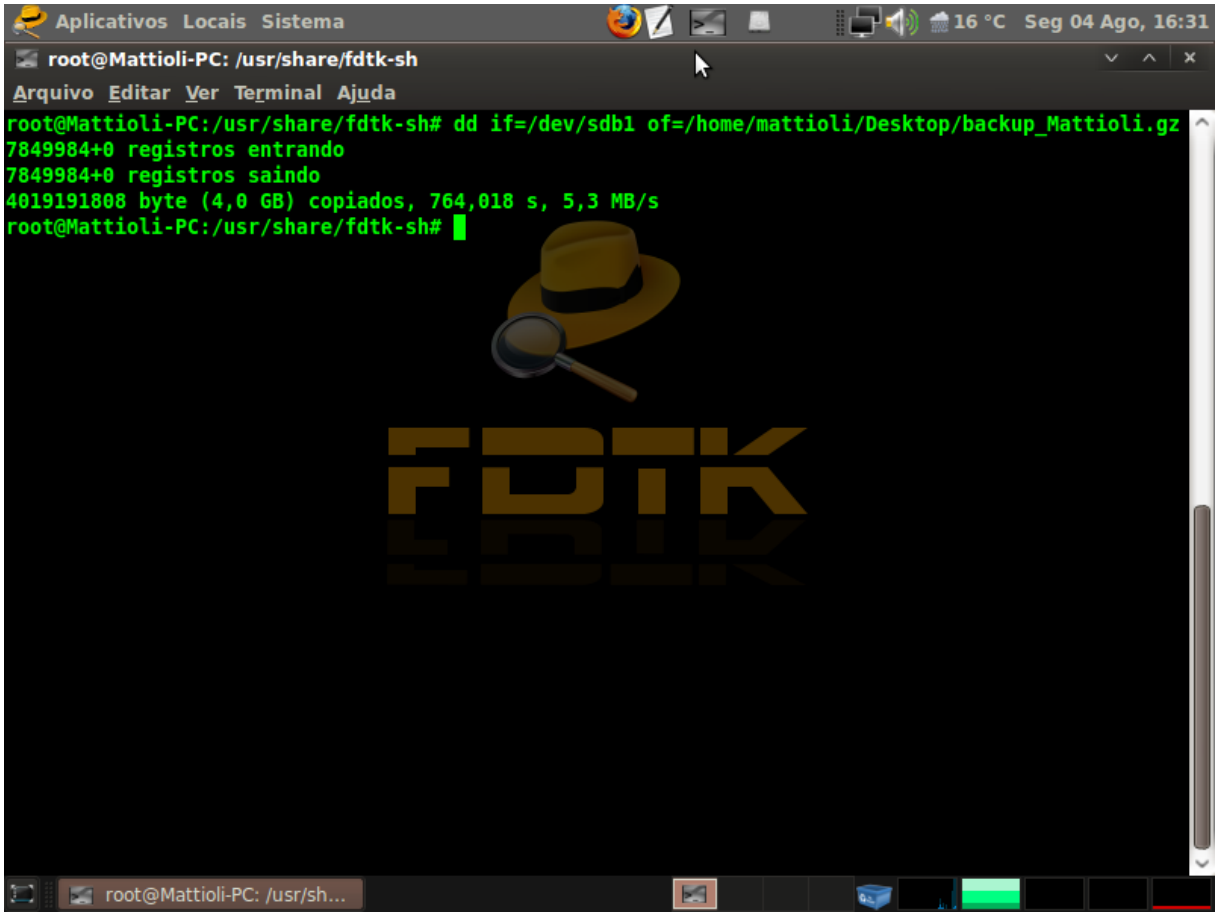

Figura 15: Compactação do pen prive está concluída

Sendo assim, agora pode-se fechar o terminal e ir ate o diretório que foi indicado com destino dos dados (**of=/home/Mattioli/Desktop**) e procurar o arquivo .gz com o nome definido anteriormente (**backup_Mattioli.gz**).

Figura 16: Arquivo .gz Criado no desktop após a conclusão da ferramenta

Com todos os métodos e técnicas utilizados de maneira adequada, deve-se preencher o formulário de cadeia de custódia de maneira clara e correta, já que qualquer divergência encontrada poderá anular a prova coletada na cena do crime. Abaixo segue o formulário preenchido com as informações coletadas do *pen drive* entregue ao perito.

EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Num.: **Pag.:** **De:**

MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO

Item:	Descrição:	
1	PenDrive de 8GB de capacidade	
Fabricante:	Modelo:	Num. de serie:
Kingston	DataTravaler 101 G2	Não Encontrado

DETALHES SOBRE A IMAGEM DOS DADOS

Data/Hora:	Criada por:	Método usado:	Nome da Imagem:	Partes:
16:32	Matheus Mattioli Moro	DD	backup_Mattioli.gz	1
Drive:	HASH:			
/dev/sdb1	dc194505029f7d35a505174b7b9ffaab			

CADEIA DE CUSTÓDIA

Destino:	Data/Hora:	Origem:	Destino	Motivo:
Pericia	Data: 04/08/2014	Nome/Org.: Local Apreensão	Nome/Org.: Matheus	Equipamento apreendido e enviado para a pericia.
	Hora: 16h40m	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	

Figura 17: Formulário de Cadeia de Custódia Preenchido

Por fim, o perito finaliza o formulário de cadeia de custódia, redigido em 08 (oito) folhas que, conferido pelo mesmo. Assim o laudo pericial deverá ser entregue ao Juiz responsável pelo caso, para que o mesmo possa ser utilizado na resolução do caso, se apresentar uma conclusão imparcial e final sobre a investigação.

Neste capitulo foi apresentado a distro FDTK junto com sua história de criação, com isso, foi exemplifico o termo Forense Digital e cada fase do ciclo de uma investigação Forense Computacional. Sendo assim, foi realizado um exemplo de preenchimento de um Formulário de Cadeia de Custódia, que foi feito a partir do uso das ferramentas presentes na distro FDTK para analise do equipamento apreendido pelo perito. Com o Formulário preenchido de forma clara e correto, o mesmo é entregue para o juiz, para ser utilizado na resolução da investigação.

5. CONCLUSÃO

Ao término do presente trabalho, pode-se observar o nível de importância que a Computação Forense possui-nos mais diversos tipos de dispositivos computacionais. Contudo, percebe-se que os usuários dos mais diversos tipos de tecnologias não estão seguros a quaisquer tipos de ataques virtuais, sendo assim, cada vez é mais necessário que qualquer usuário tenha pelo menos o mínimo de conhecimento sobre segurança digital, para que não acabem sendo vitimas de *cyber* criminosos. Entretanto, por meio de distrações, muitas vezes, nem mesmo as pessoas com mais conhecimento estão seguras de ataques, os quais normalmente são feitos para roubar dados ou até mesmo transmitir suas informações pessoais.

Com essas informações obtidas, percebe-se a importância da Computação Forense, pois sem seus métodos e técnicas, não seria possível identificar os rastros deixados nos dispositivos computacionais. Contudo, pode-se identificar qual dispositivo foi utilizado para cometer tal crime, entretanto, nem todo dispositivo pode conter provas suficientes para que seja possível incriminar o criminoso.

A escolha pela distribuição FDTK-UbuntuBr foi por sua grande variedade de ferramentas voltada para perícia forense computacional separada por etapas, além de ser totalmente em português e não ser necessário um conhecimento profundo das ferramentas. Sendo assim, pode-se ver porque sua aceitação pelos peritos foi imediata, fazendo-a ser recomendada para qualquer estudante ou profissional que deseje trabalhar nesta área.

Por fim, conclui-se que a Computação Forense é uma área que está numa crescente, pois todos os objetos pessoais possuem algum tipo de tecnologia para armazenamento ou transmissão de informações valiosas, que são armazenadas em servidores, computadores pessoais ou na nuvem, sendo assim, sempre poderá haver quebra de segurança ou ate mesmo roubo de informações. Por isso o auxilio para os usuários menos informados acabou se tornando um tema muito importante, pois atualmente não se pode falar de Tecnologia da Informação sem colocar a segurança em primeiro lugar.

REFERÊNCIAS BIBLIOGRÁFICAS

BEGOSSO, Raissa Helena. **Computação Forense.** Fundação Educacional do Munícipio de Assis-FEMA, TCC – 2010.

BEZERRA, A. **Evitando Hackers - Controle seus sistemas operacionais antes que alguém o faça!.** Ciência Moderna,2012.

CONSTANTINO, Diego Zaratini. **Técnicas da Computação Forense.** Fundação Educacional do Munícipio de Assis-FEMA, TCC-2012.

COSTA, M.A. **Computação Forense.** Curso de Introdução às Perícias dos Crimes de Informática, jun. 2005.

ELEUTERIO. Pedro M. da Silva, MACHADO, M. Pereira. **Desvendando a Computação Forense**, Novatec, Janeiro-2011.

FREITAS, Andrey Rodrigues. **Perícia Forense Aplicada à Informática.** Instituto Brasileiro de Propriedade Intelectual-IBPI, Monografia-2003.

JUNIOR, Sergio Rosa de Silva. **Uso de Aplicações Open Source na Prática de Perícia Forense Computacional.** Fundação Educacional do Munícipio de Assis-FEMA, TCC-2012.

SAMPAIO, Carlos. Forense Computacional. In Segurança Computacional, 3, 2007, Recife, Pernambuco. **Anais da Segurança Computacional,** janeiro, 2007. p.12-24.

REFERÊNCIAS ELETRONICAS

ACCESS DATA (Org.). **Forensic Toolkit 5.2 Download.** Disponível em: <www.accessdata.com/suport/product-downloads/ftk-download-page>. Acesso em: 07 mar. 2014.

BÜLLE, F. **Computação Móvel.** Disponível em: <http://grenoble.ime.usp.br/~gold/cursos/2008/movel/gradSemCorrecao/FelipeBulleC.pdf>. Acesso em: 14 out. 2013.

BUSTAMANTE, L. **Introdução à Computação Forense.** Disponível em: <http://imasters.com.br/artigo/4175/gerencia-de-ti/introducao-a-computacao-forense/>. Acesso em: 14 out. 2013.

GUIDANCE SOFTWARE (Org.). **EnCase Forensic v7.** Disponível em: <http://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx#>. Acesso em: 07 mar. 2014.

LEMES, L., NEUKAMP, P. A., DA SILVA, P. C. **Ensino da Forense Digital Baseado em Ferramentas Open Source.** Disponível em: < http://www.defenda.com.br/downloads/Artigo_Ensino_da_Forense-Digital_Final.pdf>. Acesso em: 02 ago. 2014.

LOPES, S. **A história do Linux.** Disponível em: < http://www.oficinadanet.com.br/artigo/674/a_historia_do_linux_>. Acesso em: 11 mar. 2014.

LOPES, S. **O que é um Sistema Operacional.** Disponível em: < http://www.oficinadanet.com.br/artigo/851/o_que_e_um_sistema_operacional>. Acesso em: 11 mar. 2014.

MADDOX, N. **O que é um Forensic Toolkit?.** Disponível em: <http://www.ehow.com.br/forensic-toolkit-fatos_225810/>. Acesso em: 07 mar. 2014.

NEUKAMP, P. A. **A verdadeira História da Distro FDTK.** Disponivel em: <http://fdtk.com.br/www/2011/07/a-verdadeira-historia-da-distro-fdtk/#more-837>. Acesso em: 02 ago. 2014.

NEUKAMP, P. A. **Forense Digital.** Disponível em: <http://fdtk.com.br/wiki/tiki-index.php>. Acesso em: 02 ago. 2014.

NEUKAMP, P. A., BOTELHO, A. **Ferramentas. Menu de ferramentas da Distro FDTK-UbuntuBr V 2.01.** Disponível em: <http://www.fdtk.com.br/www/ferramentas/>. Acesso em: 07 mar. 2014.

SAMPAIO, M. **Linux Forense.** Disponível em: <http://www.infocrime.com.br/2013/09/linux-forense/>. Acesso em: 07 mar. 2014.

SILVA, W. **Computação Forense.** Disponível em: <http://caminholivre.wordpress.com/2012/12/26/computacao-forense/>. Acesso em: 14 out. 2013.