Forensic Expertise in Storage Device USB Flash Drive: Procedures and Techniques for Evidence

L. M. O. Campos, E. Gomes and H. P. Martins

Abstract— **This research aims to describe the phases and the proper procedures for recovering storage device data, analyzing the computational forensics tools: Autopsy Forensic Browser and Foremost, used for information retrieval, review the evidence and give it probative value before a jury. Check which of the tools used is the best performer, stressing the runtime and the performance of these tools.**

Keywords— **phases of computer forensics, data recovery, storage device, Autopsy Forensic Browser, Foremost.**

I. INTRODUÇÃO

AS INOVAÇÕES da Tecnologia da Informação avançam cada vez mais, e a cada dia novas tecnologias estão surgindo. O hardware está cada vez mais moderno, menor, veloz e com capacidade de armazenamento muito maior. O software é desenvolvido para todos os tipos de aplicações, e para as mais variadas áreas.

Somando as qualidades de hardware e software, a falta de legislação sobre crimes cibernéticos, a falta de conhecimento da grande maioria da população sobre Perícia Forense e Ferramentas de Perícia Forense, há um grande aumento no número de crimes praticados pela internet, utilizando recursos de Tecnologia da Informação.

Este estudo esclarecerá as técnicas que o profissional forense deve utilizar para a preservação, extração, análise e formalização de evidências, mostrará à metodologia, as ferramentas Autopsy Forensic Browser e Foremost, utilizadas para a análise forense de dispositivos de armazenamento, e como essas ferramentas podem ser utilizadas para a recuperação de informações, possibilitando a utilização dessas evidências para solucionar crimes.

A análise Forense Computacional necessita cumprir fases que são de fundamental importância para se obter evidências forenses incontestáveis. A falta de informação ou a falta de cuidado em cumprir todos os procedimentos e etapas, pode gerar informações sem confiabilidade e credibilidade, inutilizando a informação, impossibilitando sua utilização como prova, prejudicando o prosseguimento de processos judiciais.

Para efetuar a recuperação dos dados, serão utilizadas ferramentas de acesso gratuito “Software Livre” e de código aberto “Open Source”, proporcionando fácil acesso às ferramentas, e será descrita como cada ferramenta funciona, favorecendo sua utilização.

Este estudo dispõe-se a contribuir para o conhecimento do profissional que atua na área de Perícia Forense, enfatizando todas as fases, técnicas e ferramentas utilizadas para recuperação de arquivos em dispositivos de armazenamento, propondo-se obter evidências forenses digitais.

II. SEGURANÇA DA INFORMAÇÃO

As informações constituem o bem mais precioso das organizações, a compreensão de que nenhuma informação está totalmente segura é de fundamental importância. Partindo deste entendimento podemos perceber a importância de se ter um comportamento seguro, minimizando os riscos com a segurança da informação.

Um grande problema para a segurança da informação é a negligência de funcionários, que gera grande quantidade de invasões, são necessários investimentos na capacitação de funcionários, para que compreendam a importância da segurança da informação quando incorporados às atividades do trabalho [1].

É de grande importância que haja uma preocupação com a segurança da informação. São destacados quatro pontos importantes: Sigilo: pessoas não autorizadas não podem ter acesso a informações sigilosas; Integridade: dados devem se manter íntegros e devem ser armazenados de forma cuidadosa evitando a perca de informações; Disponibilidade: esses dados devem estar disponíveis continuamente e livres de falhas de hardware e software; Autenticação mútua: a autenticação é essencial para identificação de todos (usuários e hardware). Os principais fatores de risco são: Catástrofes naturais: alagamento ou descarga elétrica que pode causar um incêndio; Criminais: a organização pode ter computadores roubados ou funcionários podem vender informações privilegiadas; Pessoais: os funcionários podem ser descuidados; e Técnicos: os equipamentos podem apresentar defeitos [2].

Um problema delicado é o acesso indevido, que pode ser involuntário ou proposital, o acesso involuntário acontece quando pessoas não autorizadas tem acesso a informações que deveriam manter-se ocultas, o maior problema acontece com o acesso proposital, em que pessoas, por diversos motivos, buscam maneiras para ludibriar o sistema e acessar informações confidenciais [2].

As ameaças aos sistemas de informação podem ser divididas em cinco: Atos involuntários: os erros humanos são as principais ameaças a segurança, deve-se ter um cuidado especial com pessoal terceirizado que possuem acesso a praticamente todas as áreas da organização; Desastres naturais: acontecem sem nenhum aviso entre eles estão alagamentos, raios, e outros; Falhas técnicas: as falhas técnicas podem ser de software com bugs ou hardware com defeito; Falhas gerenciais: se refere à falta de comprometimento da gerência prejudicando todos os esforços com a segurança da informação; e Atos deliberados: esses são falhas na segurança provocadas por funcionários que

L. M. O. Campos, Faculdade de Tecnologia de Bauru, Bauru, Brasil, ligia.maira@hotmail.com

E. Gomes, Faculdade de Tecnologia de Bauru, Bauru, Brasil, everaldogoms@gmail.com

H. P. Martins, Faculdade de Tecnologia de Bauru, Bauru, Brasil, henmartins@gmail.com

entendem e querem prejudicar a empresa ou tirar proveito vendendo informações [1].

A rede com acesso a internet é uma ameaça, desde invasores a procura de informações até invasores com o intuito de prejudicar as operações da empresa. Algumas formas de invasão são browsers, cookies, banners, etc [2].

Existem muitas ameaças a Segurança da Informação, as empresas devem assumir uma política de segurança da informação que contemple o treinamento dos funcionários, e fazer com que esses profissionais entendam a necessidade de praticar essa política, com um controle de autenticação, monitorando o acesso físico e lógico, mantendo backup em locais geograficamente distantes, protegendo sua rede, resguardando suas informações de todas as formas possíveis. E sempre se atualizando, por se tratar de segurança é necessária uma busca constante pelo aperfeiçoamento.

III. PERÍCIA FORENSE COMPUTACIONAL

Os computadores fazem parte da rotina dos seres humanos, estão presentes em todos os lugares, em casa, no trabalho, até mesmo em momentos de lazer, o smartphone e o notebook nos acompanham, estamos cada vez mais dependentes da tecnologia e de todas as facilidades que ela nos traz. O grande problema acontece quando pessoas utilizam os recursos de tecnologia para praticar crimes. A incidência de crimes cibernéticos vem aumentando assustadoramente.

Todo o crime deixa vestígios no caso do cibercrime que utiliza o computador como meio, deixa uma sequência lógica de bits, 0 e 1. O principal objetivo da perícia forense computacional é mostrar como ocorreu o crime e seus autores, sendo essencial a detecção e o processamento de evidências digitais, que se convertem em provas concretas de um crime, utilizando procedimentos técnicos científicos, atribuindo-lhe valor probatório diante de um tribunal. O Código do Processo Penal define que será indispensável o exame de corpo e delito, sendo assim faz-se necessário um profissional especializado, que investigue vestígios e forneça laudos de interesse da justiça na investigação de um delito. Esse profissional deve portar diploma de nível superior e deve emitir um laudo pericial minucioso [3].

A quantidade de informações utilizadas em um sistema no período de um ano é mínima, em sua maioria os acessos estão concentrados em uma pequena parte dos dados, que são acessados de forma repetida, deixando todas as outras partes intactas por um grande período de tempo. Mesmo quando excluídos os arquivos podem permanecer íntegros por anos [4].

A perícia forense tem como missão conseguir provas incontestáveis, tornando estas provas principal elemento em decisões judiciais, tanto na esfera civil, como na esfera criminal. A análise forense é dividida em quatro etapas: identificação, preservação, análise e apresentação [5].

A investigação é necessária para definir os fatos ocorridos, e sua dinâmica e também quem foi o autor do delito. Uma análise em dispositivos computacionais deve passar por quatro etapas: coleta, exame, análise e resultado [6].

A análise pericial mais solicitada na computação forense é o exame em arquivos, sistemas e programas instalados em dispositivos de armazenamento, esse exame é formado de quatro fases: preservação, extração, análise e formalização e se utiliza de algumas técnicas, entre elas a recuperação de arquivos apagados [3].

IV. ETAPAS DA PERÍCIA FORENSE COMPUTACIONAL

No decorrer de um dia muitos dados são salvos ou excluídos em dispositivos de armazenamento, há arquivos que ficam inutilizados por muito tempo, e mesmo arquivos que são excluídos podem permanecer em um dispositivo durante anos. Dispositivos de armazenamento são frágeis, dessa forma deve-se tomar muito cuidado para não afetar os dados contidos neles, assim se faz necessário cuidados especiais contra poeira, umidade, calor e descargas de energia estática.

O perito necessita tomar precauções durante a coleta, transporte e armazenamento do material apreendido, devido à fragilidade de dispositivos computacionais para evitar a destruição de informações valiosas, pois esses dispositivos são sensíveis à descarga eletromagnética, impacto, excesso de calor, atrito, excesso de umidade e vários outros [6].

Os dispositivos de armazenamentos são delicados, e devemos ter imenso cuidado, pois eles podem conter provas de um delito. As principais características do dispositivo de armazenamento serão descritas a seguir:

Fragilidade: Os dispositivos magnéticos devem ser acondicionados em embalagens antiestáticas, no entanto discos ópticos merecem atenção especial em sua superfície, pois elas devem ficar protegidas de arranhões e sujeiras. Todos os dispositivos de armazenamento devem ficar protegidos do calor exagerado, umidade e poeira, porque esses dispositivos podem ser danificados se houver o descumprimento dessas precauções.

Facilidade de cópia: Esses dispositivos armazenam dados binários, 0 e 1, em uma estrutura de bits, aplicando um mecanismo de correção de erros, facilitando sua cópia sem risco de perda de informações, essa cópia pode ser feita por meio da internet, ou pode se utilizar da rede local ou utilizar dois dispositivos de armazenamento. É necessária a realização de uma cópia fiel para que a análise seja efetuada na cópia, preservando as informações originais.

Sensibilidade ao tempo de vida: Dispositivos de armazenamento são sensíveis ao tempo, pode ocorrer falha de hardware, desmagnetização ou mesmo o fim de sua vida útil, levando a perda de informações. Consequentemente a perícia forense deve ser efetuada imediatamente após sua apreensão.

Sensibilidade ao tempo de uso: O tempo é um fator determinante quando falamos em evidências computacionais, assim que o crime é praticado existem várias evidências, mas com a utilização desse dispositivo diminui as chances de se obter provas, destaca ainda a importância da rapidez na apreensão destes dispositivos [3].

A etapa de coleta consiste em fazer o isolamento da área, proceder à identificação dos equipamentos e coletá-los, colocá-los em embalagens devidamente etiquetadas. Todo o material apreendido deve ser descrito em um auto por uma autoridade competente, e deve conter a quantidade, o tipo do dispositivo e toda a sua descrição, como marca, modelo, número de série e país onde foi fabricado, no caso de dispositivo de armazenamento é necessário informar sua capacidade. Os dispositivos computacionais devem ser preservados e também é necessário garantir a cadeia de

custódia, para assegurar a proteção e a idoneidade da prova. O profissional forense necessita seguir algumas etapas como: preservação, coleta de dados, análise e formalização [6].

Para um completo exame forense em dispositivos de armazenamento devem-se seguir quatro fases principais: preservação, extração, análise e formalização, as fases se iniciam ao receber os dispositivos e concluem-se na entrega do laudo pericial [3].

A. Preservação

O profissional de perícia forense precisa se cercar de cuidados para examinar um dispositivo de armazenamento, o perito precisa fazer uma cópia fiel do dispositivo original, ele deve utilizar ferramentas forenses adequadas para garantir que os dados do dispositivo não sofram alteração.

O profissional de perícia deve garantir que as informações contidas em um dispositivo de armazenamento jamais sejam alteradas. O perito deve proceder cuidadosamente nesta fase, utilizando ferramentas e softwares específicos para garantir que os dados não sofram alterações. Os exames forenses devem ser efetuados em cópias fiéis criadas a partir do dispositivo original. Recomenda-se ainda que o profissional faça o registro com o conteúdo dos dados presentes no dispositivo, o perito pode utilizar o calculo do hash de partes ou do conteúdo total da mídia. Após esta fase o dispositivo deverá ser lacrado e mantido em local seguro, visto que sua utilização não será mais necessária [3].

A preservação é essencial para garantir que as informações contidas no material apreendido nunca sejam alteradas, durante toda a investigação e processo. Os exames forenses devem ser realizados em uma cópia fiel, realizada a partir do material original. O perito deve fazer a cópia de forma que nenhum dado seja alterado, o acesso deve ser feito como somente leitura. A cópia pode ser efetuada com a utilização de duas técnicas, o espelhamento e a imagem [6].

O perito forense pode escolher a forma de cópia que melhor se encaixa a sua realidade em termos de hardware disponível, o profissional pode fazer um espelhamento, que copia os dados bit a bit ou fazer uma imagem do dispositivo que copia os dados em arquivos.

Existem duas técnicas para copiar os dispositivos de armazenamento: Espelhamento e Imagem, que serão descritas a seguir.

Espelhamento: Esta técnica copia os dados bit a bit gerando uma cópia fiel dos dados armazenados no dispositivo. O dispositivo que receberá a cópia deve ter o mesmo tamanho ou ser maior, é necessária a comparação do número de setores, se o dispositivo que receberá a cópia for maior, o profissional precisa ter certeza que não haverá informações que não fazem parte do dispositivo original, para isso ele pode utilizar o procedimento wipe. O espelhamento deve ser feito utilizando software específico, há a necessidade de se bloquear a escrita e a montagem do dispositivo em somente leitura.

Imagem: Quando se copia uma imagem do dispositivo os dados são copiados em arquivos, esse procedimento tem algumas vantagens como: o dispositivo que receberá a cópia pode receber várias imagens de dispositivos diferentes, os arquivos podem ser compactados, fácil replicação, pois qualquer sistema operacional pode efetuar a cópia e o disco que receberá a imagem pode ter setores com defeito que esses setores não influenciarão na imagem. O profissional deve tomar todos os cuidados para não alterar os dados do dispositivo de armazenamento [3].

O espelhamento é uma técnica de duplicação que é feita bit a bit, por isso o dispositivo de destino deverá possuir capacidade de armazenamento igual ou maior ao original, também se faz necessário verificar na etiqueta do fabricante a quantidade de setores do disco e compará-las. Caso o dispositivo que receberá a cópia seja maior que o original, o perito deve se certificar que o espaço excedente esteja vazio, o perito pode utilizar o wipe que exclui os arquivos e depois grava bits no mesmo espaço do disco. Não se deve utilizar discos com setores danificados, já que os dados copiados nos setores defeituosos serão perdidos. Já a duplicação utilizando a técnica para gerar uma imagem, faz uma reprodução precisa e fiel do dispositivo de armazenamento, copiando os dados para arquivos de imagem. Esta técnica gera uma imagem e tem algumas vantagens em relação ao espelhamento como: escolher se copia o dispositivo todo ou apenas parte dele, pode se utilizar um único dispositivo para armazenar imagens de diversos dispositivos, fácil manipulação e possibilidade de compactação das imagens. Após essa fase o dispositivo original deve ser lacrado, e armazenado em local seguro, até que a justiça determine seu descarte ou devolução [6].

B. Extração

O exame forense para a extração dos dados é obrigatoriamente efetuada na cópia, seja ela o espelho ou a imagem, a análise consiste em recuperar não somente os arquivos visíveis, mas também os que foram excluídos e que ainda permanecem no dispositivo.

A coleta de dados é basicamente a recuperação e a classificação de todos os dados contidos na imagem ou espelho do dispositivo de armazenamento, independente de esses dados estarem ocultos ou explícitos. Dispositivos de armazenamento guardam muitas informações que usuários comuns não conseguem ver, isso ocorre devido organização do dispositivo, que podemos dividir em camadas dos dispositivos, onde quanto mais superficial, mais visível está à informação, à medida que as camadas vão se aprofundando, mais difícil é a sua recuperação e compreensão, os peritos necessitam utilizar ferramentas específicas para fazer essa recuperação [6].

Toda a análise forense deve ser feita em uma cópia dos dados do computador apreendido, os dados originais devem ficar protegidos em seu estado puro. Em cada camada que faz parte da hierarquia das abstrações que constitui os sistemas de computador, as informações ficam congeladas após serem excluídas, embora as informações excluídas fiquem ambíguas à medida que descemos para os níveis mais baixos de abstração, essas informações ficam muito mais resistentes [4].

A extração é a recuperação de todas as informações que estão presentes na cópia do dispositivo gerada na fase anterior. Há dois procedimentos importantes para a fase de extração, a recuperação de arquivos apagados e indexação de dados, que serão descritos a seguir.

Recuperação de arquivos apagados: Dispositivos de armazenamento retêm mais informações do que as vistas por

usuários comuns, isso ocorre pelo tipo de organização dos dados no interior desses dispositivos. A organização é feita em camadas, a camada superior é a camada visível ao usuário comum, logo abaixo temos os arquivos ocultos, abaixo deles temos os temporários, depois os fragmentados e temos ainda uma camada mais baixa e de maior complexidade, quanto mais camadas descemos mais complexa é a recuperação dos arquivos. O sistema operacional tem um controle de quais espaços estão livres e os que estão ocupados, quando apagamos um arquivo o sistema muda seu estado de ocupado para livre, assim os arquivos continuam lá até que o sistema sobrescreva o arquivo com um arquivo novo. A recuperação de arquivos é feita procurando-se assinaturas de arquivos conhecidas, em toda a área disponível do disco. Após a assinatura ser encontrada busca-se o conteúdo do arquivo, recuperando a informação original.

Indexação de dados: A indexação baseia-se em varrer todos os bits do dispositivo, localizando todas as ocorrências alfanuméricas, organizando de forma que facilite sua recuperação. Esse processo de indexação permite a criação de uma lista que contém cada uma das cadeias e inclui sua localização, facilitando a busca rápida por palavras-chave no conteúdo do dispositivo e permitindo que o procedimento Data Carving seja efetuado de forma mais rápida e muito mais eficaz [3].

Quando se apagar um arquivo o sistema apenas modifica em seu controle, o status do espaço onde se encontrava o arquivo, de utilizado para livre, dessa forma o arquivo continua lá, só não está mais visível, até que o sistema sobrescreva o espaço ou parte dele com outro arquivo. Ao varrer um dispositivo para recuperar seus dados, também é efetuada sua indexação, são localizadas as assinaturas conhecias e também as organiza, para facilitar sua localização e recuperação, é criada uma lista com todas as cadeias encontradas e sua localização possibilitando assim a busca por palavra-chave [6].

C. Análise das Evidências

Uma criteriosa análise das evidencias deve ser feita nos dados extraídos na fase anterior, para isso o perito deve utilizar procedimentos e técnicas forenses para facilitar e agilizar seu trabalho.

Uma análise completa abrange a coleta e o processamento das informações que foram coletadas, quanto mais exatos e completos os dados, melhor e mais interessante será a avaliação. Existem três atributos que podem auxiliar o perito na análise das evidências:

- O atributo atime: faz referência à última data/hora de acesso do arquivo ou diretório.
- O atributo mtime: é alterado com a modificação do conteúdo de um arquivo.
- O atributo ctime: controla a mudança do conteúdo ou as metainformações do arquivo. O atributo ctime também nos dá uma noção de quando o arquivo foi excluído [4].

Esta fase resume-se em examinar as informações obtidas na fase anterior, para distinguir evidências digitais contidas no material obtido da extração, que se correlacionem com o crime investigado. Para o profissional verificar arquivo por arquivo, consumiria muito tempo e tornaria a análise impraticável. Portanto o profissional precisa utilizar procedimentos e técnicas para tornar o processo de análise mais eficiente, entre eles estão: Utilização de Known File Filter; Pesquisa por palavra chave; Navegação pelo sistema de pastas e arquivos; Visualização adequada de arquivos; Utilização de ferramentas de apoio e Virtualização [3].

Para análise das informações recuperadas o profissional forense deve identificar e correlacionar às informações, localizando evidências digitais relacionadas ao crime. Existem procedimentos e técnicas que ajudam o perito nesta fase, o Instituto Nacional de Justiça (NIJ) do Departamento de Justiça dos Estados Unidos juntamente com Instituto Nacional de Padrões e Tecnologia são os mantenedores do projeto Biblioteca Nacional de Referência de Software que proporciona o uso eficiente e eficaz da tecnologia em investigações criminais envolvendo computadores. A busca por palavras-chaves é um recurso eficiente para localização de evidências, tendo como único problema a criptografia, considerando-se que os arquivos estejam criptografados a busca por palavras-chaves não conseguirá localiza-los. O perito deve fazer uma busca nos diretórios pessoais onde normalmente às pessoas guardam seus arquivos. A virtualização pode ser uma alternativa para a utilização de sistemas operacionais específicos [6].

D. Formalização

A etapa final de uma perícia forense é a elaboração de um laudo, que deve conter todos os procedimentos que foram realizados desde a fase inicial na preservação até chegar ao resultado com a obtenção de provas que podem colaborar com a elucidação de um crime, esse laudo deve ser minucioso, e precisa ser claro e objetivo, o perito deve deixar claro o fato ocorrido, para que não fiquem dúvidas sobre as provas encontradas.

A formalização é a última fase da perícia que se resume em elaborar um laudo, determinando o resultado, e exibindo as evidências digitais encontradas em todo o material analisado, o laudo deve conter todas as técnicas utilizadas para preservar o material extrair e analisar seu conteúdo. Evidências importantes devem ser copiadas e anexadas ao laudo [3].

O perito deve redigir um laudo indicando o resultado e exibindo as evidências digitais encontradas no material analisado, e anexando documentos relevantes ao caso [6].

O nome técnico da formalização é substanciação da evidência, que consiste em adequar as evidências em um formato jurídico para apresentá-las [5].

O laudo pericial é um documento técnico-científico, que descreve objetivamente e de forma explícita os procedimentos e metodologia e exames realisados, para a segurança do próprio profissional forense e para que todo o processo forense seja transparente. Os laudos possuem estrutura própria e precisa ser formado pelas seguintes ações:

- Preâmbulo: Contém várias informações de identificação do laudo.
- Histórico: O histórico é opcional ele relata fatos passados que são de proveito para o laudo.

- Material: É descrita em detalhes todas as informações sobre o material examinado.
- Objetivo: Deve destacar de forma concisa os objetivos do laudo pericial.
- Considerações técnicas/periciais: Essas considerações são opcionais, nelas destaca-se o conceito e conhecimentos referentes ao exame pericial que foi realizado, que podem ajudar no entendimento do laudo.
- Exames: Descreve minuciosamente todas as técnicas utilizadas para a preservação do dispositivo, e apresenta em detalhes os passos para recuperar as evidências e os procedimentos realizados no decorrer dos exames.
- Respostas aos quesitos/conclusão: É descrito os resultados com clareza e objetividade, de fácil compreensão, e que não deixe dúvidas ao leitor, sempre que se julgue necessário deve-se fazer referência à seção exame [3].

V. FERRAMENTAS FORENSES DE RECUPERAÇÃO DE ARQUIVOS

Existem diversas ferramentas para extração de dados em dispositivos de armazenamento, entre elas ferramentas de acesso gratuito "Software Livre", de código aberto "Open Source" e de fácil utilização.

Há várias ferramentas forenses que realizam a extração de dados, e a recuperação de arquivos, o Data Carving e a indexação de dados, o perito pode escolher qual ferramenta atende melhor suas necessidades [3].

A. Autopsy Forensic Browser (AFB)

O Autopsy Forensic Browser é um Software Livre e Open Source, de fácil instalação e execução, que gera resultados através de uma interface em HTML de forma íntegra, e oferece várias operações automatizadas.

A ferramenta Autopsy Forensic Browser tem seu código aberto e é gratuita, ela foi desenvolvida por Brian Carrier, e possui uma interface gráfica em HTML, apresenta particularidades sobre dados apagados e estruturas do sistema de arquivo, e o resultado pode ser acessado utilizando um navegador HTML. A ferramenta AFB é classificado como uma interface gráfica do Sleuth Kit. O AFB é de simples execução, após a instalação deve-se executar o binário autopsy que indicará a porta para acesso via browser, o AFB solicita a formação de um novo caso ou a abertura de um caso existente, os casos criados são armazenados como diretórios facilitando a busca por auditorias realizadas com o Autopsy [7].

O Autopsy Forensic Browser é uma ferramenta Open Source que demonstra através de uma interface gráfica os detalhes da partição investigada, foi escrita em Perl e oferece uma interface gráfica para Sleuth Kit em HTML, se assemelha ao gerenciador de arquivos, ela exibe detalhes dos dados removidos e da formação do sistema de arquivos, o acesso ao arquivo gerado é feito através de um browser. O AFB é de fácil compreensão, para sua utilização, basta fazer a instalação e executar o autopsy, informar a porta e acessar via browser [8].

B. Foremost

O Foremost é uma ferramenta executada em linha de comando que recupera arquivos baseado em seus cabeçalhos/assinaturas, rodapés e estrutura de dados internas, como resultado ele cria um diretório para cada extensão de arquivo.

O Foremost foi desenvolvido por Kris Kendall e Jesse Kornblum, agentes do Departamento de Investigações Especiais da Força Aérea dos Estados Unidos, é uma ferramenta que analisa o sistema de arquivos em sua forma bruta, utilizando como base um arquivo que contém uma lista de assinaturas válidas, com a utilização dessas assinaturas é possível recuperar arquivos. Cada assinatura possui seu valor conhecido, bem como o tamanho máximo do arquivo, e verifica-se se o cabeçalho é case-sensitive, também a extensão comum a um tipo específico de arquivo, e o valor que mostra o fim do arquivo como campo opcional [9].

A ferramenta Foremost recupera arquivos utilizando como base cabeçalhos, trechos finais e estruturas de dados internas, os parâmetros serão descritos a seguir: o tamanho do bloco que é utilizado pelo sistema de arquivo, o tipo de arquivo que será procurado, o diretório onde serão armazenados os arquivos recuperados e o nome do arquivo que possui a imagem que será recuperada [10].

VI. MATERIAL E MÉTODOS

Para a viabilidade da pesquisa foi efetuada uma revisão de literatura abrangendo, pesquisa em bibliotecas e sites de publicação acadêmica, os testes com as ferramentas foram efetuados em notebook com hardware incluindo processador Intel core i3-2328M CPU 2.20 Ghz, com 8 G de Memória RAM, com um disco rígido de 500 G e com o sistema operacional Linux Mint 17.

Instalou-se uma máquina virtual com o sistema operacional Deft 7, com 1 G de Memória RAM, e com um disco rígido de 16 G, utilizando o software VirtualBox 4.3.6.

No ambiente virtualizado foram utilizadas as ferramentas Autopsy Forensic Browser 2.24 que é uma ferramenta de interface gráfica e a ferramenta Foremost 1.5.7 que é uma ferramenta de linha de comando. Ambas as ferramentas são livres e open source e são nativas do sistema operacional Deft.

Para os testes de recuperação foi utilizado um dispositivo de armazenamento pen-drive de 2 G de Memória do fabricante Kingston.

O profissional responsável pela perícia deve utilizar um hardware bloqueador de escrita para proteger os dados do dispositivo de armazenamento, em nossa pesquisa essa ferramenta não foi utilizada devido ao seu custo.

As técnicas forenses foram respeitadas em todas as etapas da perícia. E para alcançar os objetivos houve a necessidade de se efetuar quatro diferentes testes. Para efetuar esses testes foi salvo no pen-drive alguns arquivos conforme a figura 1 (exe, pdf, jpg, etc...).

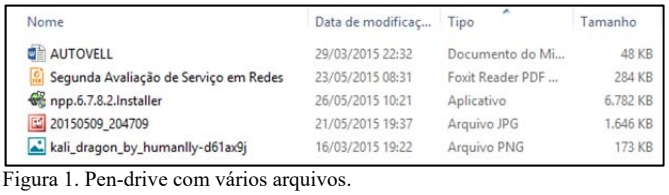

Figura 1. Pen-drive com vários arquivos.

Para cada teste o pen-drive foi montado no Sistema Operacional Deft como somente leitura e foi utilizando o comando dd (ex: # dd if=/dev/sdb1 of=/home/everaldo/Deletados/imagem.img) para gerar uma imagem do pen-drive, todos os testes foram realizados na imagem, que foi submetida às ferramentas de recuperação Autopsy Forensic Browser e Foremost com o propósito de recuperar os arquivos.

Para o procedimento de recuperação utilizando a ferramenta Autopsy Forensic Browser (Figura 2) é necessário seguir os seguintes passos: 1- no menu iniciar do Deft iniciar/ferramentas forenses clique em Autopsy e então será solicitado a senha de super usuário, insira a senha; 2- assim que abrir o browser clique em New Case; 3- insira o nome do caso e o nome do investigador e clique em New Case; 4- clique em Add Host insira o Host Name e clique em Add Host; 5- clique em Add Imagem; em seguida clique em Add Imagem File, insira o Location: a localização da imagem, o type: Disk ou Partition e o Import Method: Symlink e clique em next; 6- clique na opção Calculate: para calcular o hash value, insira o Mount Point ex: C: e File System Type ex: FAT32 e clique em Add; 7- confirme os dados e clique em OK; 8- a página mostra o caso montado, clique em Analyze; 9- é só aguardar para que o Autopsy faça a varredura e mostre na tela do browser os arquivos recuperados.

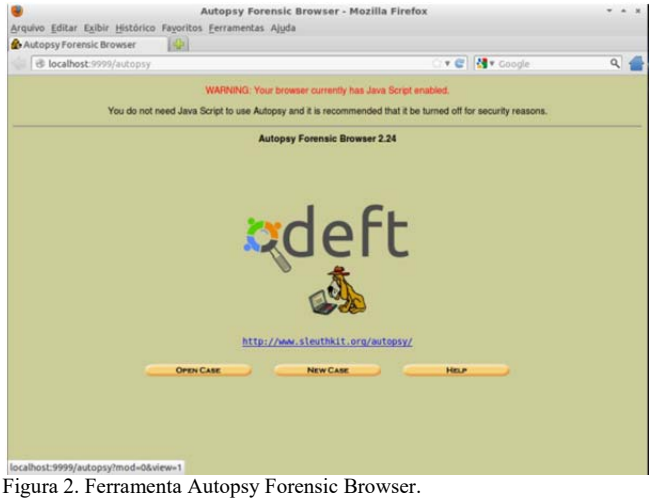

Figura 2. Ferramenta Autopsy Forensic Browser.

Para o procedimento de recuperação utilizando a ferramenta Foremost (Figura 3) é necessário seguir os seguintes passos: 1- no terminal do Deft digite o comando # foremost -Q nome_da_imagem.img; 2- a ferramenta gera um arquivo log.txt e uma pasta chamada output, entre na pasta # cd output; 3- liste os arquivos da pasta # ls; 4- essa pasta contém os arquivos recuperados e um arquivo chamado audit.txt visualize o arquivo # cat audit.txt o conteúdo deste arquivo mosta tudo que o Foremost encontrou durante sua varredura.

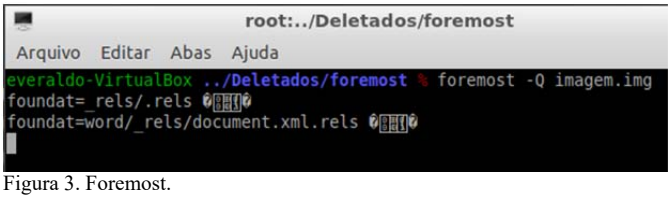

Figura 3. Foremost.

No primeiro teste foram excluídos os arquivos, executado o comando dd e a imagem submetida às ferramentas de recuperação.

Para o segundo teste foi efetuada a formatação rápida do dispositivo esse teste foi dividido em duas etapas que utilizaram sistemas de arquivos diferentes FAT32 e NTFS, para cada etapa foi executado o comando dd e as imagens submetidas às ferramentas de recuperação.

Já no terceiro teste foi efetuada a formatação completa do dispositivo, esse teste também foi dividido em duas etapas que utilizaram sistemas de arquivos diferentes FAT32 e NTFS, para cada etapa foi executado o comando dd e as imagens submetidas às ferramentas de recuperação.

No quarto teste foi utilizado a formatação física, em seguida executado o comando dd e a imagem submetida às ferramentas de recuperação.

Todas as imagens foram copiadas para HD externo 500 GB da fabricante Samsung para fins de cópia de segurança.

Após a realização dos testes foi comparado os resultados obtidos de cada ferramenta, para demonstrar qual ferramenta é a mais indicada à recuperação das informações, após a tentativa de apagá-las utilizando os métodos de exclusão, formatação rápida, formatação completa ou formatação física. Foram avaliados também o tempo de execução de cada teste e compardos se há diferenças significativas entre as ferramentas Autopsy Forensic Browser e Foremost.

VII. RESULTADOS

Através da imagem gerada a partir do pen-drive, foram efetuados quatro tipos de testes com o propósito de recuperar arquivos que foram excluídos, ou que o dispositivo de armazenamento passou pelo processo de formatação rápida, completa, ou física, as imagens foram submetidas às ferramentas Autopsy Forensic Browser e Foremost para recuperar arquivos que o usuário pretendia apagar. Durante os testes determinou-se o tempo de execução e o desempenho das ferramentas.

A tabela I demonstra os tipos de formatação utilizados e o tempo que cada tipo de formatação levou para concluir o processo.

TABELA I
RELAÇÃO ENTRE O TIPO DA FORMATAÇÃO E O TEMPO

Tipo de Formatação	Tempo de execução
Rápida	20 Segundos
Completa	03 Minutos
Física	10 Minutos

A tabela II demonstra os resultados obtidos nos testes, corelacionando o tipo de formatação com a ferramenta de recuperação e seu respectivo tempo de execução.

TABELA II
RESULTADOS OBTIDOS DOS TESTES

5 arquivos inseridos no dispositivo para efetuar os testes				
	Arquivos Recup. Autopsy	Tempo Autopsy	Arquivos Recup. Foremost	Tempo Foremost
Excluídos	5	10 Segundos	5	1 Minuto e 40 Segundos
Formatação Rápida FAT32	0	10 Segundos	5	1 Minuto e 40 Segundos
Formatação Completa FAT32	0	10 Segundos	0	1 Minuto e 10 Segundos
Formatação Rápida NTFS	0	10 Segundos	5	1 Minuto e 40 Segundos
Formatação Completa NTFS	0	10 Segundos	0	1 Minuto e 10 Segundos
Formatação Física	0	10 Segundos	0	1 Minuto e 10 Segundos

VIII. CONCLUSÕES

Com os resutados obtidos nos testes e com a comparação entre eles podemos concluir que a ferramenta Autopsy Forensic Browser é executada em 10% do tempo de execução da ferramenta Foremost quando a varredura encontra arquivos e em 14,3% do tempo de execução da ferramenta Foremost quando a varredura não encontra arquivos, obtendo 100% de recuperação dos arquivos excluídos, mas essa ferramenta não se mostrou eficaz quando o dispositivo de armazenamento passou por qualquer tipo de formatação, já a ferramenta Foremost se mostrou mais lenta mas obteve melhor desempenho 100% dos arquivos recuperados quando excluídos e 100% dos arquivos recuperados quando o dispositivo passou pelo processo de formatação rápida. Ambas as ferramentas não conseguiram recuperar arquivos quando o dispositivo passou pelo processo de formatação completa ou física.

Para que os dados sejam irrecuperáveis pelas ferramentas avaliadas, é necessário que o dispositivo passe pelo processo de formatação completa ou física, assim, verificamos que a formatação completa é mais eficaz devido a apagar 100% dos arquivos em 33% do tempo de execução da formatação física.

As ferramentas se mostraram de fácil e rápida execução podendo contribuir com os profissionais forenses em sua busca por evidencias.

AGRADECIMENTOS

Agradecemos ao corpo docente da FATEC-Bauru pela disseminação dos conhecimentos e em especial ao Mestre Henrique que nos apoiou e nos guiou até nossos objetivos.

REFERÊNCIAS

[1] R. K. Rainer Júnior and C. G. Cegielski. Introdução a Sistemas de Informação: Apoiando e transformando negócios na era da mobilidade. Ed Elsevier, Rio de Janeiro, 2011.

[2] M. Marçula and P. A. Benini Filho. Informática: Conceitos e Aplicações. Ed Érica, São Paulo, 2008.

[3] P. M. S. Eleutério and M. P. Machado. Desvendando a computação forense. Ed Novatec, São Paulo, 2010.

[4] D. Farmer and W. Venema. Perícia Forense Computacional: Teoria e Prática Aplicada. Ed Pearson Prentice Hall, São Paulo, 2007.

[5] A. R. Freitas. "Pericia Forense Aplicada a Informática", Trabalho de Pós-Graduação, "Lato Sensu" em Internet Security, Instituto Brasileiro de Propriedade intelectual, São Paulo, Brasil, 2003. Disponível: http://www.linuxsecurity.com.br/info/general/andrey-freitas.pdf.

[6] R. N. Almeida. "Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais", Monografia, Faculdade de Tecnologia de São Paulo, São Paulo, Brasil, 2011. Disponível: http://www.fatecsp.br/dti/tcc/tcc0035.pdf.

[7] S. V. Oliveira. "Perícia forense em sistemas GNU/Linus", Monografia, Especialização em Segurança de Redes de Computadores, Faculdade Salesiana de Vitória, Vitória, Espirito Santo, Brasil, 2007. Disponível: http://www.multicast.com.br/sergio/arquivos/monografia-pos-seguranca-pericia-forense.pdf.

[8] R. K. M. Galvão. "Forense Computacional com Sleuth kit + the Autopsy Forense Brouser", ICCyber' – I Conferência Internacional de Perícias em Crimes Cibernéticos, Brasília, Brazil, pp. 211-216, set. 2004 Disponível: http://www.alessandrosantos.com.br/emanuel/usp/Computadores_e_sociedadeI/material_seminario/anais-iccyber-dpf-2004.pdf#page=211.

[9] T. R. Cunha. "Remoção Segura de Arquivos em EXT3: técnicas para evitar a recuperação de dados", Monografia, Bacharelado em Ciências da Computação, Universidade de Brasília, Brasília, Distrito Federal, Brasil, 2014 Disponível: http://bdm.unb.br/bitstream/10483/8662/1/2014_ThiagoRodriguesCunha.pdf.

[10] R. Farnese. "Recuperação de Quadros de Arquivos de Vídeo H.264/AVC Corrompidos", Dissertação, Mestrado em Engenharia Elétrica, Universidade de Brasília, Brasília, Distrito Federal, Brasil, 2012. Disponível: http://repositorio.unb.br/bitstream/10482/11231/1/2012_RafaelFarnesel.pdf.

Ligia Maira de Oliveira Campos graduate in Technology in Computer Networks by Bauru School of Technology, Bauru, São Paulo, Brazil. His research interests are Forensic Tools and Computer Forensics.

Everaldo Gomes graduate in Technology in Computer Networks by Bauru School of Technology, Bauru, São Paulo, Brazil. His research interests are Forensic Tools and Computer Forensics.

Henrique Pachioni Martins Masters in Computer Science from Universidade Estadual Paulista (UNESP), Bauru, Brazil. He is a professor of Bauru Technology College (FATEC) their interest in current research includes Computer Networks, Distribuиdos Systems, Cloud Computing are Forensic Tools and Computer Forensics.