Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 22 Issue 2 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

# Use of Techniques and Tools for Investigative Process in Computational Forensic Expertise

By Priscilla Leão de Lima

*Abstract-* Computer forensics investigates and retrieves information about a fact, as well as examining digital evidence that can be decisive in any technological situation. The research will explain techniques that are used during the expertise, ensuring the integrity of the data so that the analysis is not impaired. First, a bibliographic survey will be carried out in search of concepts about data collection and analysis techniques in the for ensic area. The method includes performing procedures such as equipment identification and chain of custody in a simulated environment, in orderto determine the best mechanism for the presented scenario. Finally, the mainsteps and forensic tools were presented for a betterway in which the expert can use to perform the exactan alysis of the crime.

*Palavras-Chaves:* *evidências. investigação. computaçãoforense.*

*GJCST-E Classification:* *DDC Code: 004.62 LCC Code: T58.5*


*Strictly as per the compliance and regulations of:*

# Use of Techniques and Tools for Investigative Process in Computational Forensic Expertise

Priscilla Leão de Lima

*Abstract-* **Computer forensics investigates and retrieves information about a fact, as well as examining digital evidence that can be decisive in any technological situation. The research will explain techniques that are used during the expertise, ensuring the integrity of the data so that the analysis is not impaired. First, a bibliographic survey will be carried out in search of concepts about data collection and analysis techniques in the for ensic area. The method includes performing procedures such as equipment identification and chain of custody in a simulated environment, in orderto determine the best mechanism for the presented scenario. Finally, the mainsteps and forensic tools were presented for a betterway in which the expert can use to perform the exactan alysis of the crime.**

*Palavras-Chaves: evidências. investigação. computaçãoforense.*

## I. Introdução

É indiscutível que os avanços tecnológicos tenham se difundindo em nossa sociedade, porém esse desenvolvimento ampliou crimes ocorridos na Internet, atingindo particulares como também grandes empresas.

Pode-se afirmar que em razão desta situação, foram criadas técnicas para investigação e manipulação de evidencias eletrônicas, como a forense computacional, " é a ciência responsável por adquirir, preservar, identificar, extrair, restaurar e documentar evidências computacionais, processadas eletronicamente e armazenadas em mídias computacionaisǁ (ATÍLIO, 2003 apud SOUSA et al., 2006).

Para este, também há outra interpretação como "Forense Computacional: O estudo de como as pessoas usam o computador para causar danos, ferir e mesmo destruir. " (MOHAY et al., 2003, p. 1)

Em base desse estudo, também possuímos respaldo legal conforme o Código de Processo Penal nos Artigo 170 "Os peritos deverão guardar material suficiente para nova perícia" e Artigo 171 "Nos crimes cometidos com destruição ou rompimento de obstáculo a subtração da coisa, ou por meio de escalada, os peritos, além de descrever os vestígios, indicarão com que instrumentos, por que meios e em que época presumem ter sido o fato praticado". Em que deverá ser feito cópias reservas, caso acontecer algum imprevisto na análise e apresentar todos os detalhes das evidencias para compor seu laudo judicial.

Assim, este trabalho explanará técnicas para melhor manuseio de vestígios em uma análise de perícia forense computacional, para que no final da investigação possa garantir o valor judicial de uma prova eletrônica.

## II. Forense Computacional

Segundo Queiroz e Vargas (2010), a forense computacional é um conjunto de procedimentos e metodologias com a função de investigar e armazenar evidências que possam responder se houve ou não um crime, tendo como base de análise equipamentos de processamento de dados (computadores pessoais, laptops, servidores, estações de trabalho ou outras mídias eletrônicas).

O principal objetivo deste tipo de perícia forense pode ser definido como a coleta de vestígios relacionados ao crime investigado, os quais possibilitem a formulação de conclusões sobre o caso (REIS, 2003).

O intuito é coletar todas as evidências, buscando indícios virtuais com a aquisição, a identificação, a extração e análise de dados que estejam em uma mídia computacional, possibilitando comprovar de uma forma legal em que realmente ocorreu o crime ilícito de acordo com a investigação realizada pelos peritos forenses.

A Computação Forense determina à dinâmica, a materialidade e autoria de ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhe validade probatória em juízo. (ELEUTÉRIO; MACHADO, 2010, p. 16). Portanto, é basicamente uma área nova e está sendo desenvolvida para combater crimes cibernéticos. Com a expansão da internet, está ocorrendo a ampliação de fraudes eletrônicos, para estes casos, a perícia forense é uma ferramenta eficiente para identificação desse delito e assim reduzir riscos.

## III. Processo De Investigação Da Forense Computacional

Segundo Noblett, Pollitt e Presley (2000), para que os resultados da perícia sejam válidos, é necessário que sejam postos em práticas

*Author: ESP (Instituto de Especialização do Amazonas)*
*e-mail: prilima2413@gmail.com*

procedimentos e protocolos (documentados) que garantam assim os requisitos legais e técnicos para a evidência pericial.

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

De acordo com Eleutério e Machado (2001), a Computação Forense tem quatro etapas do processo de computação forenseprincipais:

*Coleta:* Segundo Vargas (2007), os procedimentos adotados, na coleta de dados, devem ser formais, seguindo normas internacionais de padronização e padrões de como se obter provas para apresentação judicial, como um *checklist.*

Obtendo todas as evidências, realizar cópias garantindo sua integridade, etiquetar os vestígios, como colocar adesivos com cores distintas para identificar se o equipamento estava ligado ou não, realizar vídeos ou fotos do cenário, sendo possível verificar quais programas estavam em execução e suas conexões de rede.

Itens que requerem atenção especial durante a documentação, devendo ser fotografados, são (STEEL, 2006):

- Telas do computador, com resolução suficiente para leitura de textos ali presentes, se necessário;
- Conexões de rede, mostrando quaisquer cabos de rede conectados ao computador. As duas pontas do cabo devem ser fotografadas, para o caso em que o perito tenha que provar que o computador estava conectado a algum equipamento específico;
- Conexões de periféricos, para provar que estavam conectados ao computador.

Nesta etapa, pode empregar-se a Forense *Em Vivo*, que dependendo do contexto, podemos encerrar a análise com o desligamento do computador de forma abrupta, o que classicamente é procedimento tomado pelo perito (MELO, 2009). Em que o perito utilizará suas técnicas e procedimentos que possam produzir vestígios na investigação ainda em funcionamento.

Outro fator importante, é verificar na ordem judicial se há restrição de coleta de algum equipamento que não possa ser retirado do lugar do acontecimento do crime. Alguns equipamentos possíveis de fontes de dados são computadores, maquinas fotográficas, pen drives, dispositivos de armazenamento em rede, entre outros.

E para Cansian (2000), é importante sempre fazer a coleta de dados de acordo com a ordem de maior volatilidade para a de menor, dos elementos mais utilizados:

- Registros de memória periférica, cache;
- Memória principal;
- Estado da rede, rotas, interfaces;
- Processos em execução;
- Discos e partições;
- Fitas, disquetes e outros meios magnéticos;
- Em mídias como CD-ROMs e cópias impressas.

Os peritos devem coletar esses dados voláteis o mais rápido possível para não ser perdido nenhum aspecto relacionado ao crime que possam ser de extrema importância para uma das etapas da perícia forense computacional, a análise dos dados.

Segundo BATTULA (2000), Imagem e Espelhamento são técnicas de duplicação/cópia utilizadas na fase de coleta A cópia dos dados é realizada através de ferramentas apropriadas para duplicação de dados, como o utilitário dd (Linux) que é capaz de recolher dados voláteis que estão englobados na memória e replicar dados não voláteis.

Entretanto, as coletas devem ser realizadas minuciosamente para que não ocorra nenhuma falha, resultando erros em sua análise, logo o laudo pericial não estará coerente com a investigação.

*Exame:* identificar, extrair, filtrar e documentar dados relevantes a análise, buscando até aquele não estarão explícitos que serão manipuladas por ferramentas forenses adequadas para perícia digital.

Segundo Kerr (2001, apud VARGAS, 2007, p. 21), um perito forense computacional deve garantir que uma evidência será manuseada e protegida de tal forma que não seja danificada, destruída ou até comprometida. Isso pode se dá, pelo mal uso e escolha dos procedimentos a serem introduzidos.

Para que não seja danificada, pode ser utilizado o HASH(MD5/SHA1/SHA256) que estabelecem a sequência de caracteres de tamanho fixo, certificando que os dados coletados não sofram nenhum dano, garantindo a sua integridade. Como de acordo com Eleutério e Machado (2010): "O que torna esse tipo de função extremamente utilizada para a verificação de integridade de dados computacionais é o fato que uma simples alteração na informação de entrada do algoritmo gerará uma sequência de bits (valor hash) completamente diferente."

Esse artefato consegue assegurar até alguns tipos de arquivos que facilitam a ocultação de dados, evitando sua descoberta, em que uma das técnicas mais conhecida e utilizada sobre este caso é o uso de esteganografia.

O processo de esteganografia consiste em esconder uma informação através de uma mensagem de menor importância, conhecida como mensagem de

cobertura. Após inserir os dados na mensagem de cobertura, obtém-se o chamado estego-objeto, que é uma mensagem inócua que contém secretamente uma mensagem de maior importância (ROCHA, 2004).

Com esses dados contidos nos equipamentos que foram capturados no local do fato ocorrido deve ser registrado toda as informações como data, hora, tamanho, descrições, observações, entre outros, relatando todo período da investigação.

Freitas (2006) lista alguns exemplos de procedimentos para a preservação dos dados, para que estes não sejam comprometidos por qualquer ação:

- Inicialmente, devem-se criar imagens do sistema investigado, para que as potenciais provas possam ser posteriormente analisadas;
- Se o caso necessitar de uma análise ao vivo, salvar as evidências em dispositivos e bloqueá-los contra regravação;
- Todas as evidências deverão ser lacradas em sacos e etiquetadas;
- A etiqueta deverá conter um número para a identificação das evidências, o número do caso, a data e o horário em que a evidência foi coletada e o nome da pessoa que a está levando para a custódia, além do nome de quem coletou essas evidências;
- Etiquetar todos os cabos e componentes do computador, para que, depois, possam ser montados corretamente quando chegar ao laboratório;
- Os HDs deverão ser armazenados em sacos antiestática, para evitar danos e, também, para que os dados não sejam corrompidos;
- Durante o transporte das provas, tomar cuidado com líquidos, umidade, impacto, sujeira, calor excessivo, eletricidade e estática;
- Quando já tiverem sido transportadas, as evidências deverão ser armazenadas e trancadas para evitar a adulteração até o momento em que poderão ser examinadas e analisadas;
- Todas as mudanças feitas durante essa fase deverão ser documentadas e justificadas (cadeia de custódia);

Uma das técnicas para duplicação de uma cópia idêntica dos equipamentos aprendidos é o de imagem e espelhamento. Segundo (ELEUTÉRIO; MACHADO, 2011) relata que essas técnicas, ao serem realizadas através de softwares e equipamentos forenses, garantem uma cópia fiel dos dados e consequentemente a preservação correta do material que foi apreendido.

O espelhamento é uma técnica de duplicação que realiza uma cópia exata e fiel dos dadoscontidos em um dispositivo de armazenamento computacional para outro (ELEUTÉRIO; MACHADO, 2011). Uma reprodução realizada de bit a bit para local de destino almejado, porém esse disco deverá conter o tamanho ideal ou maior para finalizar esta cópia com êxito.

E a imagem também é uma cópia fiel de drivers, sistema operacionais, configurações, entre outros é construída arquivos de imagem de disco, contendo toda base do armazenamento realizado.

De acordo com Eleutério e Machado (2011), a técnica de imagem possui algumas vantagens se comparada com o espelhamento:

- Um dispositivo de destino pode armazenar diversas imagens de disco, se houver capacidade;
- Possibilidade de compactação dos arquivos de imagem; facilidade de replicação das imagens de disco, uma vez que podem ser copiadas por qualquer sistema operacional;
- Eventuais setores defeituosos no dispositivo de destino são tratados pelo sistema operacionais

Recomenda-se utilizar o recurso de bloqueio de escrita para acessar as mídias sem realizar nenhuma modificação no conteúdo. Pode ser feito no software colocando o computador do investigado em somente leitura. E também por hardware, que há vários equipamentos no mercado, com custo baixo, mas também há aqueles mais aprimorados.

Segundo Eleutério e Machado (2001), Os equipamentos EspionForensics e o Forensic Bridge Tableau são os mais utilizados para bloqueio de escrita em discos, já o software ICS Write ProtectCard Reader é o mais utilizado para bloqueio de escrita em cartões de memória.

Posteriormente de realizar estes mecanismos para garantir a integridade, há a extração de todos os dados etapa, que são a extração que irá remover das mídias apreendidas tudo o que for importante para a investigação, recuperando os dados que foi possivelmente excluído intencionalmente pelo suspeito do delito.

De acordo com Eleutério e Machado (2001), Data Carving, que na computação refere-se à recuperação de arquivos apagados, é uma técnica realizada através da localização de assinaturas conhecidas (por exemplo, cabeçalhos que contêm a identificação do tipo de arquivo).

Para organizar os arquivos são indexados os dados, para que em uma busca, sejam localizados rapidamente, podendo ser realizado por palavras-chave no conteúdo do material examinado.

Esta técnica muito eficiente e muito utilizada na etapa de análise é a busca por palavras-chave, sendo essa técnica disponível em muitos softwares de análise de arquivos. (ELEUTÉRIO; MACHADO, 2011).

Com todos esses procedimentos, os peritos são capazes de realizar cópias exatas do que é

pretendido, capturando até dados que possivelmente foram ocultos para camuflar uma evidência.

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

Portanto, é necessário realizar a operação com bastante atenção pois os dados que possivelmente ser úteis para o caso, possam estar em locais imprevisíveis e que o perito deve estar apto para a identificação e recuperação desses dados.

*Analise*: identificar (pessoas, locais e eventos) e a correlacionam, reconstruindo acena a fim de encontrar vestígios com paramentos adequados com o crime investigado.

Segundo Kerr (2001, apud VARGAS, 2007, p. 21), a análise será a pesquisa propriamente dita, em que o investigador pode se deter, especificamente, nos elementos relevantes ao caso em questão, pois todos os filtros de camadas de informação anteriores já foram transpostos.

Na análise, o perito examina os dados que foram coletados, verificando os parâmetros das evidencias interligadas ao crime, utilizando ferramentas adequadas para desvendar o caso.

De acordoEckert (1997), o valor de uma evidência é medido por quatro parâmetros:

- Relevância: que descreve a importância da evidência no contexto ou escopo dos fatos ocorridos;
- Materialidade: que descreve capacidade da evidência em ajudar a reproduzir os fatos ocorridos;
- Credibilidade: que descreve o meio pelo qual a evidência foi obtida;
- Competência: que descreve o nível de validade dos procedimentos científicos empregados na análise e teste da mesma.

Dessa forma, deverão ser aplicadas ferramentas e técnicas que efetuem uma cópia fidedigna dos dados e mantenham a integridade do material apreendido. (ELEUTÉRIO; MACHADO, 2011).

Nesta fase, há grandes chances de ocorrer equívocos durante a análise devidoa grande demanda de dados que nem sempre é evidente, como apresenta CASEY, 2006. Essa é uma fase que além de consumir muito tempo, está muito suscetível a equívocos, pois depende muito da experiência e do conhecimento dos peritos, já que são poucas as ferramentas que realizam esse tipo de análise com precisão.

Outro artefato, é proceder com o equipamento ainda ligado para não que os dados não sejam perdido se o computador reinicie ou for desligado bruscamente. Segundo Bertoglio (2008), a *Live forensics*, ou análise ao vivo, representa a perícia que é feita em um computador ou equipamento ainda em funcionamento.

De acordo comAdelstein (2006, apud BERTOGLIO 2008, p. 31) um desafio para a análise ao vivo é o fato de que o sistema não é estático, arquivos e processos estão sempre mudando. Para que a aquisição dos dados seja realizada corretamente, é adotado um conjunto de melhores práticas que busca melhorar a qualidade das evidências. É importante seguir essas práticas, já que trabalhar com um computador em funcionamento dificulta a coleta de provas, uma vez que qualquer ação pode afetar outros elementos das informações requeridas.

Dessa forma, a analise necessita de conhecimento maior do perito para realizar toda a pesquisa e escolher ferramentas propicias para ter um laudo correto sem cometer nenhuma injustiça, pois é nessa fase que ocorrerá a conclusão do fato que será entregue para o poder judiciário.

*a) Resultados Obtidos*

Basicamente, esta é última etapa da investigação do caso examinado em que irá ser gerado um laudo constando informações necessárias para a apuração do crime. Para Kent e outros (2006, apud PEREIRA et al., 2007) nessa fase, é necessária a organização da documentação necessária para a criação do laudo pericial, sendo necessários alguns procedimentos como: reunir toda a documentação e anotações geradas nas etapas de coleta, exame e análise, incluindo as conclusões obtidas; identificar os fatos que fornecerão suporte as conclusões descritas no laudo pericial;listar as conclusões obtidas; organizar e classificar informações recolhidas para garantir um laudo conciso e inquestionável.

"É importante que a conclusão apresentada no relatório seja imparcial e final, de forma a não favorecer alguma decisão. Por esta razão, a etapa de apresentação é a fase conclusiva da investigação". (PEREIRA *et al.*, 2007).

Com os resultados obtidos durante toda a investigação, é de fundamental importância redigir o laudo, anexando evidências detalhadas encontradas no material examinado e demais documentos encontrados na cena do crime, concluindo toda analise realizada. Porém, esse conteúdo que será adicionado ao relatório, deverá ser organizado em seções para não ocorrer informações dispersas e assim deixar o laudo inexato.

Para Kent *et al.* (2006), o conteúdo do laudo pericial torna-se um documento de fácil interpretação e, para isso, deve ser organizado em seções:

- Finalidade da investigação: explicar claramente os objetivos do laudo;
- autor(es) do relatório: listar todos os autores e co-autores do relatório, incluindo suas especialidades e responsabilidades, durante a investigação;

- Resumo do incidente: síntese explicando o incidente investigado e suas consequências;
- Relação de evidências: relacionar e descrever todos objetos, onde se encontram, estado, como, quando e por quem elas foram adquiridas no decorrer das investigações;
- Detalhes: fornecer uma descrição detalhada de quais evidências foram analisadas, quais os métodos utilizados e quais as conclusões alcançadas, descrevendo os procedimentos e as técnicas adotados, durante a investigação;
- Conclusão: os resultados da investigação devem ser somente descritos, citando especificamente as evidências que comprovem as conclusões. A conclusão deve ser clara e não oferecer dupla interpretação;
- Anexos: todas as documentações devem ser anexadas, ao final do laudo, tais como: diagramas da rede, formulários descritivos dos procedimentos utilizados, formulário de cadeia de custódia e informações gerais sobre as tecnologias envolvidas na investigação;
- Glossário: adicionar um glossário dos termos utilizados no laudo, que poderá esclarecer muitas dúvidas que possam surgir durante a leitura do juiz e/ou dos jurados.

Nessa fase do processo da perícia, é apresentada todo o procedimento produzido durante todo o ciclo para poder ser entregue ao jurídico e assim obter um julgamento dos dados examinados.

De acordo com Freitas (2006), nessa fase ocorre o enquadramento das evidências no formato jurídico, por isso, também, é conhecido como substanciação das evidências, sendo isso feito pelo juiz e/ou advogados na esfera civil ou criminal.

E com todas as evidências recolhidas, o perito descreverá tudo o que foi encontrado, relatando indícios que podem ajudar a desvendar o crime investigado, tornando-se encarregado de realizar o laudo pericial.

Como responsável pelo laudo operitodeveenvolvertodas as pessoas que achar conveniente em sua investigação, de acordo com (REINALDO, 2007)

E segundo Reis e Geus (2004), a elaboração do laudo é o último passo da perícia, neste momento o perito tem a liberdade de descrever o incidente, sendo ele o único responsável pelo documento e todo o seu conteúdo.

Dessa forma, com a conclusão do laudo, os documentos deverão ser armazenados e poderá também ser anexado a mídia com o material coletado. Neste, é necessário conter todas os requisitos que foram solicitados, bem como a descrição das provas e assim ser entregue ao solicitante.

Portanto, é de fundamental importância que o laudo contenha uma linguagem clara para que todas as pessoas que tiverem acesso a esse material possam entender e compreender o que realmente o perito concluiu da investigação.

## IV. Equipe Forense

Para obtenção de um laudo coerente, é necessário a composição de uma equipe preparada e especializada para não ocorrer falhas durante qualquer investigação, do início até sua finalização.

Segundo Ng (2007) diz que a equipe forense deve ter algumas funções como:

- Identificar atividades suspeitas e realizar o processo de investigação;
- Tratar as atividades suspeitas que não foram identificas pela equipe;
- Definir níveis de criticidade e um tempo de *report*para cada um dos eventos;
- Realizar*reports*periódicos a respeito dos processos de investigação;
- Coletar e documentar as evidências encontradas;
- Definir, manter e gerenciar um local para armazenar as evidências;
- Envolver todos os profissionais que podem auxiliar no processo de investigação;
- Realizar atividades de acordo com as políticas da organização e das leis vigentes;
- Seguir a metodologia de análise forense computacional definida e implementada.

Como todo trabalho, é essencial ter uma equipe, em que possa ser dividido as tarefas, mas na perícia essas pessoas contém um maior conhecimento, são especializadas na área forense e assim gerar buscas e analises de evidências mais eficazes.

## V. Obstaculos Durante a Investigação

Segundo REIS, 2003, podem ocorrer muitas dificuldades na coleta e análise de vestígios deixados na máquina utilizada no ato ilícito, sendo que a quantidade de evidências deixadas é inversamente proporcional às habilidades apresentadas pelo criminoso.

Durante a investigação, poderão ocorrer algumas dificuldades que o perito irá enfrentar como a grande quantidade de arquivos, por isso é necessário que os requisitos do laudo estejam bem claros, não deixando sentido genérico. Então, é importante que o a autoridade solicitante busque sempre detalhar o quê procura, descrevendo no máximo de detalhes possível, ou seja, que mostre para a equipe pericial exatamente o quê deve ser buscado, para dessa forma, evitar desperdício de trabalho dos peritos. (ALMEIDA, 2011).

Também há equipamentos que contém senhas,criptografia onde as informações são escritas

em códigos, esteganografia que oculta seu verdadeiro sentido."Esteganografia é uma palavra de origem grega, onde Stegano significa escondido ou secreto e Grafia: escrita ou desenho", conforme Coelho e Bento (2004), entre outros obstáculos e para quebra desses artefatos, uso de fermentas forenses são adequados para estes procedimentos.

Entretanto, um mecanismo que pode ser útil no caso examinado é a engenharia social. De acordo com (SOCIAL-ENGINEER, 2015) engenharia social é um método de ataque, no qual alguém faz uso da persuasão, diversas vezes abusando da ingenuidade ou confiança do usuário, com a finalidade de obter informações que possam ser utilizadas no acesso não autorizado a computadores ou informações. Facilitando o acesso das senhas e o tempo da analise pericial.

## VI. Ferramentas Periciais

Com o advento e disseminação da tecnologia nesses últimos anos, as infracções, invasões, venda e roubo de informações privilegiadas, pirataria, envio de e-mails falsos, tentativas de acessos indevidos à organizações ou até mesmo à pessoas comuns vêm se aumentando cada vez mais e por isso há a necessidade do auxílio de ferramentas mais modernos e incrementada para busca de infractores, além da necessidade de padronização das buscas e apresentação das evidências mais consistentes. (Vargas, 2006)

Em uma perícia, é de extrema importância a utilização de ferramentas que irão auxiliar no desenvolvimento da análise do caso, examinando e resgatando todas as evidências para êxito do laudo investigativo.

De acordo com Eleutério e Machado (2011), as ferramentas que são destaques na etapa de análise são os softwares Encase e o software Forensic Toolkit (FTK), pois eles além de serem uteis em todas as etapas do processo forense computacional, eles ainda têm diversas funcionalidades que são fundamentais para a etapa de analise, como: as buscas por palavra-chave, a navegação adequada pelos arquivos e pastas da base de dados, o KFF, entre outras.

O software ForensicToolKit (FTK) e o software Encase são soluções proprietárias compatíveis com o Windows. Ambas possuem diversas funcionalidades que possibilitam a realização de diversas técnicas para perícia forense computacional. Já como opções para Linux, o autor destaca a utilidade de alguns softwares para a etapa de preservação e coleta: DC3DD e Guymager, e destaca também os sistemas Linux CAINE e FDTK-Ubuntu para mesma finalidade. (ELEUTÉRIO; MACHADO, 2011).

Muitos softwares de computação forense trabalham com indexação de dados, dentre estes, destaca-se o FTK e o Encase. (BATTULA, 2000).

### *a) Encase*

O Encase possui a capacidade de formar o *timeline*(linha do tempo), de forma gráfica. Este recurso ajuda muito a estabelecer a temporalidade dos dados encontrados e mostrar de forma clara as datas relativas aos arquivos encontrados e ou existentes no sistema (COSTA, 2003).

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

De acordo com Christófaro (2006) a ferramenta EnCase da Guidance Software surgiu no cenário da Computação Forense em 1998 nos Estados Unidos, dois anos depois ela se tornaria a principal ferramenta forense. Naquela época, a maioria dos examinadores se utilizavam do prompt dos sistemas operacionais em suas investigações; a proposta de um ambiente compatível com os populares ponteiros e janelas do Windows da Microsoft era ousada, uma vez que na visão dos examinadores forenses o prompt era mais poderoso e ainda oferecia mais opções de controle, além do mais a ferramenta irá ser composta por quatro recursos básicos que permitem sua funcionalidade abrangente. Esses recursos serão vistos a seguir (GUIDANCE, 2007)

- Análise detalhada do sistema: a ferramenta é capaz de descobrir arquivos ocultos e excluídos, detectar rootkits, procurar documentos, identificar processos de invasores, reconstruir atividade de Web e de e-mails, até decodificar certos tipos de criptografia e identificar comunicação não autorizada na rede; – análise paralela: este tópico analisa com rapidez um grande número de computadores ao mesmo tempo, reunindo informações críticas sobre seu estado e conteúdo.
- A análise paralela:é o recurso básico que permite produzir velocidades de pesquisa empresarial e reação a incidentes muito superiores às tecnologias concorrentes;
- Correção: após a identificação de um evento mal-intencionado, a ferramenta auxilia a detê-lo e controlá-lo. Em quase todos os casos de reação a incidentes, é possível ver o problema, mas não fazer algo a respeito ou não fazer nada, ou então, usar ferramentas de terceiros para remediar a situação, o que pode significar a desativação de pelo menos uma parte da rede. Com a ferramenta pode-se documentar o incidente detalhadamente,

acessar os computadores comprometidos e corrigir o problema;

- Integração: a ferramenta é capaz de ser integrada à infra-estrutura de segurança existente na empresa para proporcionar reação a incidentes em tempo real automatizada. Os alertas gerados por tecnologias de monitoração, com os sistemas IDS1 e SIG2, ativam reações automatizadas pela ferramenta, permitindo aos profissionais de segurança reagir a centenas e potencialmente a milhares de alertas por dia, logo após o evento ocorrer.

*b) Accessdata Forensic Toolkit*

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

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

i. *Ftk Imager (Access Data)*

Este programa é extremamente útil para a coleta de dados em local de busca e apreensão, sendo disponibilizado gratuitamente pela empresa AccessData (ACCESSDATA, 2011).

Esta ferramenta possui apena três funcionalidades, para a linha de comando, no entanto, não é um programa de linhas de comando, mas proporcionam em que sejam automatizadas as coletas dos dados. Portanto, as linhas de comando suportadas são (ACCESSDATA, 2011):

- /CreateDirListing – Cria um arquivo de lista de diretório na pasta onde o "FTK Imager" é executado;
- /VerifyImage – verifica uma imagem quando especificado o nome do arquivo e seu caminho;
- /EnableDebuLog – permite acesso ao arquivo FTKImageDebug.log criado na pasta em que o "FTK Imager" é executado.

As ferramentas apresentadas são umas das principais utilizadas em pericia forenses, que auxiliam na recuperação de dados, buscando vestígios para compor uma investigação bem-sucedida.

## VII. Considerações Finais

A forense computacional está sendo propagada cada vez mais em entidades de Justiças devido ao aumento dos crimes cibernéticos. Então, para suprir esses determinados caos, é necessária uma perícia para ser desvendado o crime almejado.

O artigo apresentou as técnicas essências como a coleta, identificação, analise e resultados obtidos em uma perícia digital, bem como algumas ferramentas que poderão contribuir para o trabalho do perito computacional.

Entretanto, pode haver dificuldades durante o período da investigação, devido a falha humana ou até mesmo ausência de evidências. Portanto, é necessária uma equipe forense qualificada, buscando a verdade nos vestígios examinados para a obtenção correta do laudo pericial.

## Referências Bibliográficas


1. BATTULA, B. et al. *Techniques in Computer Forensics:* IJS. V. 3, 2000.
2. BERTOGLIO, B. B. *Análise Forense:* Estudo teórico e prático. Novo Hamburgo, junho de 2008
3. CANSIAN, A. M. *Conceitos para perícia forense computacional.* VI ESCOLA REGIONAL DE INFORMÁTICA DA SBC, 2001, São Carlos, SP. Anais da VI Escola Regional de Informática da SBC. São Carlos, SP: ICMC/USP, 2001. p. 141 - 156.
4. ELEUTÉRIO, P. M. S.; MACHADO, M. P. *Desvenda ndo a computação forense*. São Paulo: Novatec, 2010.
5. GALVÃO, R. K. M. *Introdução à análise forense em redes de computadores:* São Paulo: Novatec, 2013.
6. GALVÃO, R. K. M. *Introdução à análise forense em redes de computadores:* São Paulo: Novatec, 2013.
7. KENT, K. et al. *Guidetointegratingforensictec hniquesintoincident response:* Special publication. Gaithersburg: NIST, 2006.
8. MOHAY, George; ANDERSON, Alison; COLLIE, Byron; DE VEL, Oliver; McKEMMISH, Rod. *Compu ter andIntrusionForensics. edArtechHouse*, 2003.
9. NG, R. *Forense Computacional Corporativa*. Ed. Brasport, Rio de Janeiro, 2007.
10. REINALDO,N.G.(2007). *Forense Computacional Corporativa,* ed. Brasport, 1ª Ed.
11. REIS, M. A. dosGeus. *Forense computacional e sua aplicação em segurança imunológica*. Campinas, SP: 2003
12. REIS, Marcelo Abdalla dos, GEUS, Paulo Lácio de. *Análise Forense de Intrusões em Sistemas Comp utacionais: Técnicas, Procedimentos e Ferr amentas.* Instituto de Computação –Universi dade Estadual de Campinas, 2004, p.54
13. SOUSA, S. R. A.; GOUVEIA, B. J. *Estudo para verif icação da eficiência da aplicação de métodos de*

*análise forense computacional em ambientes Windows*. Rio Verde, dezembro 2006.