A IMPORTÂNCIA DA PERÍCIA FORENSE COMPUTACIONAL NA INVESTIGAÇÃO DE CRIMES

Lucas Serafim Parizotto
Antonio Lucas Neves
Nicolli Rinaldi Pinheiro

Resumo

Este meta-artigo, ao qual foi confeccionado por meio de pesquisas bibliográficas, tem como objetivo introduzir a necessidade da Perícia Forense Computacional, relacionando-a com a Segurança da Informação e apresentando como a forense computacional tem agilizado de modo geral as investigações criminais, portanto, o trabalho visa focar na importância e deveres de um perito em Forense Computacional apresentando princípios, processos e demais competências.

Palavras-chave: Segurança da Informação, profissão, perícia forense.

Abstract

This meta-article, which was made through bibliographical research, aims to introduce the need for Computer Forensic Expertise, relating it to Information Security and presenting how computer forensics has generally streamlined criminal investigations, therefore, the work aims to focus on the importance and duties of an expert in Computer Forensics, presenting principles, processes and other competences.

Keywords: *Information Security, profession, forensic expertise.*

1. Introdução

A mais de 5000 anos atrás (...), o poder provido da informação foi inicialmente contemplado, quando a tecnologia revolucionaria começou a se desenvolver mesmo que em passos lentos, o que mais tarde introduziria a humanidade em um mundo moderno. Tudo começou com nada mais, nada menos do que o surgimento da própria linguagem escrita, que fundamentalmente se compõe da transmissão e armazenamento de informações. “As palavras são capsulas de suporte de vida para a informação”. (THE STORY OF INFORMATION- ORDER AND DISORDER. DIREÇÃO: NIC STACEY, PRODUÇÃO: BBC. REINO UNIDO, 2012, 1 DVD)

À primeira vista, pode parecer uma questão simples, mas a informação foi um dos conceitos mais difíceis e sutis que a ciência teve que desvendar de forma que, com a descoberta desse sistema, tudo aquilo que poderia ser dito e até mesmo pensado, poderiam ser transformados em símbolos e a informação passou a viver não apenas no cérebro humano, mas também fora dele. Durante 4000 anos a escrita foi a única tecnologia de informação utilizada pelas pessoas. No entanto, o cenário começou a se alterar tendo início durante a grande revolução Industrial do século XIX.

Sendo algo existente por todo o mundo, desde o inicio dos tempos, é correto dizer que as pessoas trocam informações constantemente e seus cérebros estão cheios delas em todos os sentidos.

De acordo com Singh (1999, p.13) em seu livro The Code Book:

> Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, e que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, porque os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação.

E isso permanece até os dias de hoje, ganhando ainda mais destaque com a Era da informação na qual nos situamos, marcada pelo avanço da tecnologia, que para Damásio (2007, p.45), pode ser entendida como sendo a soma de um dispositivo, das suas aplicações, contextos sociais de uso e arranjos sociais e organizacionais que se constituem em seu torno. Consequentemente, essa enxurrada de novas possibilidades traz consigo a oportunidade de praticar atos ilícitos e criminosos, entre as ocorrências mais comuns dos crimes em ambientes virtuais encontram-se a calúnia, difamação e injúria via e-mail, o roubo de informações confidenciais e a remoção de arquivos. Além disso, crimes como pedofilia, fraudes e o tráfico de drogas via Internet também são atos ilícitos constantemente realizados com o apoio de computadores. De maneira que “A convergência entre crimes e tecnologia da informação se torna realidade, e antes dois assuntos que sequer tinham relação hoje estão extremamente integrados” (NG REYNALDO, 2007, p.3).

Conhecidos como cybercrimes ou crimes cybernéticos, ocorrem em um de seus motivos, devido a visão geral de que perante as redes sociais, navegando na internet em si, há uma facilidade maior de anonimato, o que acaba dando toda a liberdade necessária da qual criminosos precisam para cometer seus delitos, portanto, quando ocorrem esses tipos de crimes se faz necessário um profissional que esteja apto a coletar, manipular e examinar as evidencias digitais, reconstruir o passado, constatar a materialidade e apurar a autoria de incidentes cometidos com

o requinte dos bits. Esta é a função da perícia digital ou forense digital, carreira que mescla a formação jurídica com a tecnologia da informação e que é crescente na esfera pública e privada, à medida que conflitos, fraudes, furtos e agressões passam a ser cometidas por intermédio de dispositivos informáticos e telemáticos, de um computador de mesa a um dispositivo móvel celular.

Com o decorrer dos anos é inevitável parar o processo de evolução o qual se encontra o avanço da criminalidade, devido a isso, este Artigo desenvolvido a partir do método de pesquisa qualitativo apoiando-se em técnicas de coleta de dados, tem como objetivo apresentar e explicar de qual maneira a perícia forense computacional atua auxiliando na resolução de crimes, mostrando quais são os métodos e etapas para a conclusão de uma investigação.

2. A Perícia Forense Computacional

Segundo o dicionário Michaelis da Língua Portuguesa, Forense é um termo " 1 Relativo a ou próprio de foro; 2 Relativo à justiça e aos tribunais; judicial." Ainda segundo ele, o termo perícia significa:

> 1 Qualidade de perito; 2 Um conhecimento especial ou uma grande habilidade em uma atividade ou área específica; destreza, mestria, proficiência; 3 JUR Exame de caráter técnico, por pessoa especializada, nomeada pelo juiz, de um fato, estado ou valor de um objeto litigioso, cujos resultados servirão de meio de prova que o juiz precisará conhecer para tomar decisão"

Freitas (2006) diz que a Forense Computacional é o ramo da criminalística que compreende a aquisição, prevenção, restauração e análise de evidências computacionais, quer sejam os componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais. A Perícia Forense Computacional surgiu com o objetivo de suprir as necessidades das instituições legais no que se refere à manipulação das novas formas de evidências eletrônicas. Ela é a ciência que estuda a aquisição, preservação, recuperação e análise de dados que estão em formato eletrônico e armazenados em algum tipo de mídia computacional.

Esse campo de estudo se destaca, pois ao contrário das demais disciplinas forenses, que produzem resultados interpretativos, a forense computacional pode produzir informações diretas, que por sua vez, podem ser decisivas em um dado caso. Isso pode ser notado no exemplo muito simples que se segue: no caso de um assassinato, o legista verifica que há traços de pele em baixo das unhas da vítima. Isso é interpretado como um indício de que houve luta antes da consumação do crime, contudo não passa de uma interpretação. Já no caso de uma perícia em uma máquina suspeita podem ser encontrados arquivos incriminadores como diários e agendas.

Mas vale ressaltar que o perito em forense computacional não atua somente em crimes virtuais, ele pode atuar em todo e qualquer caso dentro ou fora do ambiente virtual, podendo atuar em crimes convencionais que fizeram uso de um computador ou qualquer outro dispositivo eletrônico.

2.1. Computadores utilizados como apoio em crimes convencionais

Estima-se que 90% dos exames forenses realizados na área de informática são para investigações desse tipo de crime, onde o computador é apenas uma ferramenta de auxílio aos criminosos na prática de delitos, como roubos a banco, fraudes, até mesmo assassinatos. Portanto, como mencionado anteriormente a Perícia Forense Computacional se faz necessária também em crimes convencionais.

Por exemplo, na fuga de bandidos de um roubo a banco, tanto o computador, quanto o carro estão relacionados ao modus operandi do crime, ou seja, à forma com a qual é executada o crime. Portanto, em muitos casos, exames forenses nesses objetos são uma prova técnica bastante eficiente e os laudos produzidos tornam-se peças fundamentais para o convencimento do juiz na elaboração da sentença, devido ao fato de que podem ser encontradas evidencias digitais que comprovem o crime, ou evidencie indícios de quem seria o possível autor do mesmo em computadores, celulares etc.

2.2. Computadores utilizados como meio para a realização do crime

Nesta categoria, o computador é usado como ferramenta principal para a realização do ato ilícito, de forma que, o crime não ocorreria se tal dispositivo não existisse, diferente do item anterior onde os dispositivos computacionais apenas serviram de auxilio ao crime de tal maneira na qual o crime poderia ser executado mesmo sem o uso desses dispositivos.

Alguns exemplos de crimes cibernéticos desse tipo são: furto de informações sigilosas, ataques a sites, phishing (maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias), malwares (um software destinado a se infiltrar em um computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações), vírus de computador, cavalos de tróia, worms (Um programa semelhante aos vírus, com a diferença de este ser auto-replicante, ou seja, ele cria cópias funcionais de si mesmo e infecta outros computadores), etc.

3. Evidencias no conceito da Perícia Forense

3.1. Evidencias

O Princípio da Troca de Locard (1877-1966) explica que, qualquer um, ou qualquer coisa, que entra em um local de crime leva consigo algo do local e deixa alguma coisa para trás quando parte. Ou seja, deixa para trás algum vestígio, e no âmbito da computação forense, os vestígios deixados por um crime são digitais, sendo elas as evidencias de um crime. Ainda se tratando das evidencias, o Código de Processo Penal (CPP) determina em seu artigo 158 que: “Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado. ”

Dessa forma, surge a necessidade de um profissional qualificado, que examine vestígios e produza laudos de interesse à justiça na apuração de um delito, conforme definidos nos caputs dos artigos 159 e 160 do CPP, que dizem, respectivamente: “O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.” e “Os peritos elaborarão o laudo pericial, no qual descreverão minuciosamente o que examinar e responderão aos quesitos formulados.”

3.1.1. Evidencia Física

Entende-se por toda evidencia que tem uma forma de um objeto, e que tem como objetivo provar um fato baseado nas suas características. Uso como exemplo as mídias (CD, disquete, DVD), dispositivo USB, papel impresso, computador etc. No caso da forense computacional, é possível extrair evidencias digitais das evidencias físicas, como por exemplo, arquivos existentes em um dispositivo USB ou e câmeras fotográficas.

3.1.2. Evidencia Digital

É toda informação armazenada ou transmitida utilizando uma tecnologia computacional que permita identificar que um determinado fato tenha ocorrido. Este tipo de evidencia, devido ao fato de ser frágil por natureza pode ser facilmente corrompida, alterada ou apagada dependendo de alguns fatores como horários do dispositivo de origem.

Devido às características de uma evidencia digital, é necessário ter alguns cuidados tais como: Testar o procedimento de tratamento da evidencia com o intuito de validar que o mesmo não altere quaisquer propriedades ou informação, documentar a evidencia, realizar cópias pois é imprescindível que a evidencia original seja preservada, também é fundamental que o transporte das evidencias seja planejado para que não haja qualquer interferência ou sofra qualquer dano causados por temperatura ou meios magnéticos por exemplo.

3.2. Período de retenção das evidencias

É importante saber que as evidencias são armazenadas por um período determinado pela legislação vigente do país, isso ocorre pois, um caso concluído pode ser reaberto, e pode ser necessário realizar novas análises nas evidencias.

4. Inicio da Perícia Forense Computacional em investigações

4.1. Procedimentos iniciais

Durante a investigação de um crime, independente se há um computador envolvido, deve-se seguir as normas estabelecidas pela legislação brasileira, mais precisamente o decreto-lei Nº 3.689, de 3 de outubro de 1941. Nesse texto, presente no Código de Processo Penal, está regulamentado a função do Estado de julgar as infrações penais e de aplicar punições a quem as pratica.

Porém, antes de qualquer coisa, é necessário que se tenha uma investigação iniciada após uma denúncia ou suspeita de crime com o intuito de esclarecer a materialidade, a dinâmica e autoria, em outras palavras, o que aconteceu, como aconteceu e quem realizou tal ato ilícito. No geral, os procedimentos básicos executados pela autoridade policial durante a inquirição são: dirigir-se ao local e preservar o estado e a conservação das coisas até a chegada dos peritos criminais; apreender os objetos que tiverem relação com o fato, após liberados pelos peritos; colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias; proceder a reconhecimento de pessoas e coisas.

Para Eleutério e Machado (2011) Computação Forense é uma ciência que obtém, preserva e documenta evidências de dispositivos de armazenamento digital, como computadores, PDAs, câmeras digitais, telefones celulares e vários dispositivos de armazenamento de memória. Esses autores organizam a Computação Forense em 4 etapas principais: Coleta, Exame, Análise e Relatório.

4.1.1. Coleta

O objetivo da primeira etapa é identificar, isolar, etiquetar, registrar e coletar os dados e evidências físicas relacionadas com o incidente que está sendo investigado, enquanto estabelece e mantem a integridade das provas. Eleutério e Machado (2011) explica que é fundamental que

os dados contidos nos dispositivos (mídias digitais e dispositivos de armazenamento) e os dados voláteis (aqueles que constam na memória RAM ou trafegando em rede de computadores), possíveis fontes de evidências digitais, permaneçam coletados e preservados corretamente, de maneira a garantir que os mesmos não sejam alterados. Nessa fase de preservação e coleta será possível buscar elementos (dados, mídias de armazenamento, entre outros) de maneira a consolidar uma base investigativa para as fases seguintes da perícia.

4.1.1.1. Técnicas de imagem e espelhamento

De modo geral, os exames forenses devem ser efetuados em cima de duplicatas idênticas, as quais são obtidas dos materiais originalmente apreendidos e submetidas a exames forenses. Dessa forma, deverão ser aplicadas ferramentas e técnicas que efetuem uma cópia fidedigna dos dados e mantenham a integridade do material apreendido (ELEUTÉRIO E MACHADO, 2011). Imagem e espelhamento são técnicas de duplicação/cópia utilizadas na fase de coleta. 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. A importância e finalidade deste processo são destacadas por Reynaldo (2007, p.69):

> Realizar uma cópia física de dados permite realizar a cópia de todas as informações existentes no dispositivo, inclusive informações anteriores que porventura foram armazenadas no dispositivo e questão, como por exemplo, instalações de sistemas operacionais anteriores, informações apagadas, informações armazenadas em blocos defeituosos e informações armazenadas em espaço não alocados pelo sistema operacional ativo.

Em alguns casos, como quando há um setor danificado em um determinado dispositivo, não será possível trabalhar com a cópia real dos dados, neste caso, a informação precisará ser documentada e o processo de análise feito em cima dos dados recuperados, sendo recomendado realizar várias cópias. Para explicar em exemplo o motivo pelo qual não se trata de uma simples cópia de arquivos, um pen drive é a prova de um crime por alguma razão e serão necessárias várias analises na evidencia física, para extrair evidencias digitais do mesmo, o que pode acabar por danificar o driver original, para isso serão feitas as cópias físicas do pendrive, para que a evidencia original não seja adulterada.

Se durante este processo, não for utilizado uma ferramenta forense especifica para obtenção da imagem, as cópias não terão o resultado satisfatório, pois quando copiamos os arquivos do pendrive, estamos copiando apenas os arquivos ali presentes e não necessariamente os bytes aos quais não são expostos visivelmente, ou seja, vários bytes deste pendrive que estão com arquivos recuperados, ou indícios que podem ser usados como evidencia, não serão aproveitados. Portanto dizemos que essas cópias são feitas bit-a-bit.

4.1.1.2. Hash de dados

Determinado arquivo está sendo compartilhado por torrent, porém, uma das pessoas modifica o seu conteúdo e continua distribuindo-o pela rede. Dessa forma, quem realizar o download desse conteúdo acabaria, no fim, com um arquivo adulterado, podendo estar corrompido ou, até mesmo, escondendo algum tipo de malware. Para garantir a integridade dos dados compartilhados, os clientes de torrent usam um “truque” muito esperto: ao gerar o arquivo original, o software calcula uma sequência única de letras e número e a atribui aos arquivos ou pastas que começarão a ser compartilhados. De modo que, antes daquele conteúdo ser baixado,

o programa utilizado pede a mesma sequência de letras e números para a máquina que está servindo o arquivo: se a sequência estiver diferente, significa que o arquivo foi alterado e que não deve ser baixado. Caso a conferência esteja correta, a transferência é iniciada.

Essa sequência é conhecida como Sequencia Hash, que é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo. Por esse motivo, as funções Hash são conhecidas por resumirem o dado. A principal aplicação dessas funções é a comparação de dados grandes ou secretos.Esse processo é de suma importância na etapa de espelhamento, pois segundo Reynaldo (2007, p. 70):

> Ao se realizar a cópia dos dados, o processo de hash dos dados deve ser executado, a fim de garantir a autenticidade das evidencias analisadas. O processo de hash de dados consiste basicamente no seguinte procedimento: as informações/ evidencias digitais são submetidas a um software que utiliza um algoritmo matemático, resultando em um número que representa aquela informação de forma única .

Esse procedimento garante a autenticidade das evidencias devido ao fato de que, partindo do princípio de que cada arquivo de uma evidencia possuí uma sequencia de hash única, se apenas um bit do mesmo for alterado, a sequencia de hash originada deste arquivo será completamente diferente, de tal maneira que fica possível identificar se alguma evidencia foi ou não adulterada.

4.1.1.3. Coleta de dados voláteis

De acordo com Lillard et al (2010), a fase de coleta de evidências digitais para realizar uma perícia forense computacional é dividida em dois grupos, separados de acordo com a volatilidade dos dados: Grupo post-mortem, a coleta é realizada sobre fontes não voláteis, (que independam de energia para armazenar os dados) e grupo em vida (coleta live), nesse as informações digitais são coletadas em fontes voláteis (armazenagem temporária). Segundo Eleutério e Machado (2011), os principais dispositivos fontes da coleta post-mortem são: CDs, DVDs, cartões de memória, Mídias de armazenamento, discos rígidos (HD). Se tratando de dados voláteis, é correto dizer que são as informações que devem ser verificadas em caso de análise em um computador que esteja ligado, sendo importante mantê-lo ligado para que não haja a perda de informações e para que o processo de analise forense não seja danificado.

Como há a possibilidade da existência de informações importantes, este processo é realizado online, isto é, na evidencia original, mas isso requer certo nível de cautela, para evitar que dados na evidencia não sejam alterados de forma alguma. Podemos citar como exemplo de informações que podem ser coletadas durante esse processo, os usuários logados, processos ativos, conexões e informações de configurações de rede, arquivos abertos, system uptime que são informações sobre o tempo que o computador está ligado (como o boot proposital no computador para encobrir atividades suspeitas), partições, discos e dispositivos USB conectados.

4.1.2. Exame

Nesta fase é necessário identificar e extrair as informações relevantes a partir dos dados coletados utilizando ferramentas e técnicas forenses adequadas. Depois de finalizada a etapa de coleta, a próxima etapa é extrair dados / informações relevantes para uma posterior análise. Nessa etapa, é extraído e avaliado o que pode ser importante para a investigação. Nesse ponto, podem ser encontradas evidências inacessíveis, devido à proteção por senha, criptografia, ou prévia exclusão do dado.

4.1.2.1. Recuperação de arquivos

Durante a fase de exames ocorre a recuperação de arquivos, que é efetuada por meio de softwares específicos, no entanto essa fase pode ocasionar questionamentos do tipo “Como é possível recuperar arquivos apagados? ”. Isso se torna possível pois até mesmo os arquivos apagados da lixeira de um computador não são de fato deletado. Os sistemas operacionais, em geral utilizam uma técnica para remover arquivos com a finalidade de atingir maior performance e velocidade nas operações. Reynaldo (2007, p. 81) destaca que:

> [...] Quando uma operação para apagar um determinado arquivo é solicitada, o sistema operacional remove a sua referência, de forma que o espaço alocado pelo arquivo passe a ser visualizado como espaço livre, ou seja, as informações não são apagadas no momento da operação de deleção.

Para que um arquivo seja removido permanentemente, existem duas formas: Sobrescrever o espaço utilizado pelo arquivo e utilizar uma técnica que sobrescreve os espaços considerados livres. Caso nenhuma das situações ocorra, arquivos apagados podem ser recuperados juntamente com informações de diversas instalações de sistemas operacionais em um mesmo computador. Ou seja, do mesmo jeito que se é possível recuperar arquivos, também é possível recuperar apenas uma parte deles ou até mesmo não conseguir recuperar nada, tudo irá depender do estado de sobreposição de seus bits.

4.1.2.2. Arquivos temporários

Os arquivos temporários costumam ter uma série de informações a respeito das operações realizadas em um computador, normalmente, o sistema operacional utiliza arquivos temporários para gravar uma série de informações que tenham uma vida útil predefinida. Um bom exemplo disso é a instalação de um software qualquer, que normalmente vem compactado. Ao realizar a instalação do mesmo, o sistema operacional descompacta os arquivos, realiza as operações necessárias e instala o software.

4.1.2.3. Indexação de dados e busca binária

A indexação é uma técnica de organização/arrumação de dados. Essa técnica envolve a criação de estruturas de dados associados aos documentos de uma determinada coleção, de forma que possa ser acessado posteriormente com índices, gerando mais velocidade no acesso dessas informações.

Já a busca binária é uma forma interessante de realizar buscas de evidencias utilizando palavras-chave fazendo uso do recurso de busca binária, que realiza pesquisas utilizando strings ASCII e expressões regulares (GREP). Reynaldo (2007, p. 81) menciona que a grande vantagem desse tipo de busca é que ela pode ser realizada em todo sistema e arquivo e também em áreas de disco que são listadas pelo sistema operacional ativo.

4.1.3. Análise

Nesta etapa os dados transformam-se em informações, ou seja, o perito computacional

deve identificar e correlacionar pessoas, locais e eventos, reconstruir as cenas e documentar os fatos. De acordo com Almeida (2011), esta etapa consiste em examinar os dados/informações extraídos da etapa de extração, e em seguida identificar evidências digitais, verificando a relação com o fato apurado.

Após a identificação e avaliação das evidências encontradas no material questionado, é possível responder as perguntas feitas pela autoridade solicitante. Dessa forma, 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 que deve ser buscado, para dessa forma, evitar desperdício de trabalho dos peritos. (ALMEIDA, 2011). aAinda sobre a fase de análise de evidencias Reynaldo (2007, p. 91) complementa que:

> Um fator importante que deve ser levado em consideração é a quantidade de informações existentes versus a ocorrência de um determinado evento. Sempre que possível é interessante delimitar o período que se quer analisar, pois fará com que a quantidade de informações a ser tratada seja reduzida, apesar de existirem casos onde é necessário realizar uma análise detalhada de todas as informações, como, por exemplo, ao adquirir um computador que foi utilizado para realizar crimes e fraudes.

5. Políticas de segurança para melhorar os resultados da perícia forense em computadores e redes.

Políticas são introduzidas de forma que, com base em evidências encontradas durante a investigação forense, possa ser mais fácil identificar o tipo de crime cometido e sua autoria. Neste processo, as seis políticas abaixo são fundamentais (YASINCAC, MANZANO, 2001).

a) Retenção de informação: consiste de copiar e reter aplicação e arquivos de usuários locais e copiar e reter computador e atividade de rede logs, utilizando técnicas apropriadas que garantam a integridade, autenticidade.
b) Planejando a resposta: consiste no estabelecimento de uma equipe forense, estabelecendo um procedimento de resposta de intrusão e formalização do processo de investigação.
c) Formação técnica: isso inclui treinamento de equipe de resposta. Formação da equipe de investigação e de formação para todo o pessoal que utilizam computadores.
d) Acelerar a investigação: inclui nessa política a proibição da criptografia de arquivos pessoais, proibir software de trituração de arquivo. Recomenda-se indexação de dados.
e) Prevenção de todas as atividades anônimas: Exigir data, hora e usuário estampados nos arquivos, usando a autenticação rígida de usuário e mecanismos de controle de acesso rígidos, garantindo que toda atividade seja identificada.
f) Proteger as provas: exercer um controle rígido sobre o acesso administrativo das evidências. Criptografar arquivos de evidências e conexões, aplicando tecnologia de verificação de integridade forte.

Utilizando estas seis políticas, além de haver diminuição de crimes digitais, facilitará o processo investigativo da perícia computacional (YASINCAC, MANZANO, 2001).

6. Ferramentas

A perícia forense necessita ser organizada e cuidadosa para que seus resultados possuam a maior confiabilidade possível, desse jeito é necessário caminhar por quatro etapas das quais são a coleta, extração, análise e apresentação (KENT et. al, 2006). A quantidade de dados extraídos da máquina durante a perícia, pode ser enorme e nem todos são relevantes para a investigação, ou seja, é necessário saber separar os dados importantes daqueles irrelevantes para o resultado (SOUZA, 2015 apud KENT et. al, 2006). Do momento da coleta até a análise dos dados para o veredito final, são utilizadas ferramentas e técnicas no qual auxiliam os investigadores para o processo ser feito de forma assertiva e num menor tempo possível (SOUZA, 2015 apud WEYER, 2011).

Toda investigação forense se inicia com a coleta dos dados do material duvidoso, porém a sua manipulação deve-se por via de regra ser feito apenas com os seus dados copiadas, deixando o material original intacto para impedir a manipulação indevida das provas. Para isso ocorrer, é utilizado técnicas de espelhamento e imagem que tem como propósito a cópia fidedigna dos dados guardados em um dispositivo de armazenamento do computador, um software muito utilizado é o Symantec Norton Ghost que além de realizar essas técnicas também serve como bloqueador de escrita impedindo a manipulação dos dados no momento da cópia (SOUZA, 2015 apud KENT et. al, 2006). Agora mostraremos algumas ferramentas que estão disponibilizadas para realizar as diferentes etapas da investigação forense.

6.1. Forensic Toolkit (FTK)

O FTK é um software forense criada pela Acess Data, onde possui diversas ferramentas para a realização da investigação e muito utilizada por profissionais na área, auxiliando na verificação de arquivos em ambientes NTFS (SOUZA, 2015 apud KENT et. al, 2006). Segundo Dodt (2018) uma das grandes vantagens desse software é a sua agilidade para analisar os dados, por ser multi-core (multiprocessador) sua performance acaba sendo até quatrocentos porcento (400%) superior comparado a outros softwares. Esse software possui diversas ferramentas como a análise de e-mails podendo filtrar palavras e busca de IP, recuperar senhas utilizadas, recuperação de blocos de dados (Data Carving) por tamanho ou tipo de arquivo, Web Viewer que permite o cruzamento de dados enquanto as evidências ainda estão sendo processadas, Cerberus que é um poderoso detector de malware e OCR (Optical Character Recognition) podendo converter imagens para textos legíveis, AFind, HFind, SFind e Hunt.

6.2. Encase

Assim como o FTK, o Encase é um dos softwares mais utilizados para a perícia forense apresentando diversas ferramentas para a investigação, interface clara e de fácil manuseio. Segundo Souza (2015), o Encase é um dos principais softwares para analisar dispositivos de armazenamento, coleta de dados não voláteis (duplicar o conteúdo vindo de HDs), Data Carving, indexação de dados, análise de e-mails e hardwares e fornecimento de senhas de arquivos criptografados. É importante ressaltar que esse software também lhe permite a implementação de novas funções para o ele, tanto que dois peritos brasileiros produziram a ferramenta “NuDetective”, onde realiza uma triagem em imagens coletadas afim de encontrar material pornográfico (CONSTANTINO, 2012).

6.3. Autopsy

O Autopsy é um software que utiliza o Linux para rodar e que diferente dos outros dois acima, é de uso livre (sem custos) ele se apresenta de forma simples e intuitiva de se operar o que gera ganho de tempo para investigar. Reynaldo (2007) explica que o Autopsy se utiliza de diversas ferramentas, permitindo a análise de diversos sistemas de arquivos como NFTS, FAT, Ext2, Ext3, UFS1 e UFS2. Segundo o site (SLEUTHKIT, 2003), o software foi desenhado para ser completo, possuindo diversas ferramentas extras como análise do histórico para saber o momento em que se foi registrado maior tráfico de dados, filtro de Hash onde se marca os arquivos que foram modificados ou não, filtrador de palavras, recuperação de dados, extrair dados de imagens e vídeos entre outros .

6.4. Guymager

Este é um software gratuito, pertencente ao sistema CAINE (Computer Aided Investigative Environment), disponível apenas para a plataforma Linux, é um software como opção para a criação de imagens e cálculo de Hash, muito importante para verificar uma potencial alteração nos arquivos coletados. Existem diversos softwares com o mesmo objetivo do Guymager porém ele pode realizar esta atividade ao fazer comparações e validações de forma nativa dos dados, através da opção de hash. (SILVA & OLIVEIRA, 2014).

7. Crimes Virtuais

Crimes virtuais são delitos praticados através da internet que podem ser enquadrados no Código Penal Brasileiro resultando em punições como pagamento de indenização ou prisão. Os crimes digitais são cada vez mais comuns porque as pessoas cultivam a sensação de que o ambiente virtual é uma terra sem leis. A falta de denúncias também incentiva fortemente o crescimento dos número de golpes virtuais e violência digital (como o cyberbullying).

Muito se fala sobre a carência de um conjunto de normas e sanções jurídicas dedicadas somente para os crimes digitais. Porém, existindo ou não uma legislação específica para este assunto, quando o computador é usado como uma ferramenta para a prática de delitos e violência, estes crimes serão adaptados ao código penal já existente e os agressores e golpistas serão punidos da mesma forma.

7.1. Categorias

Crime Informático significa: "qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados". Essa categoria de crime apresenta algumas características, dentre elas: transnacionalidade – pois não está restrita apenas a uma região do globo - universalidade – trata-se de um fenômeno de massa e não de elite - e ubiqüidade – ou seja, está presente nos setores privados e públicos. (GUIMARÃES E FURLANETO NETO, 2003)

Os crimes informáticos podem ser classificados em virtuais puros, mistos e comuns.

a) Crime virtual puro - compreende em qualquer conduta ilícita, a qual atenta o hardware e/ou software de um computador, ou seja, tanto a parte física quanto

a parte virtual do microcomputador.

b) Crime virtual misto - seria o que utiliza a Internet para realizar a conduta ilícita, e o objetivo é diferente do citado anteriormente. Por exemplo, as transações ilegais de valores de contas correntes.

c) Crime virtual comum - é utilizar a Internet apenas como forma de instrumento para realizar um delito que enquadra no Código Penal, como, por exemplo, distribuição de conteúdo pornográfico infantil por diversos meios, como messengers, e-mail, torrent ou qualquer outra forma de compartilhamento de dados.

8. Casos Reais

A aplicação de tecnologia e computação em investigação forense teve seus primeiros indícios de participação em casos levados para justiça nos anos 70, aumentando ali em diante sua participação, tanto para crimes praticados através da internet, quanto para crimes que não envolvia tecnologia, o que acabou se tornando pauta de discussão em reunião do G7 em Lyon, nos anos 90. Hoje em dia temos inúmeros exemplos de casos em que o investigador de computação forense se fez presente, ocasionando uma grande valorização da profissão e crescimento nessa área de atuação.

8.1. Internacional

US vs Drinkman, Kalinin, Kotov, Rytikov, Smilianets

Em 2013 a justiça americana acusou cinco homens por invasão de sistemas e fraudes em cartões de crédito, que custaram US$ 300 milhões às empresas afetada, o procurador Paul J. Fishman, considera este um dos maiores crimes cibernético da história dos Estados Unidos.

Cerca de 15 empresas entre elas 7-Eleven, JCPenney, JetBlue, Dow Jones e a bolsa de valores Nasdaq foram vítimas entre o período de 2005 a 2012 do grupo de hackers formado por quarto russos e um ucraniano um dos integrantes também foi indiciado separadamente por ter invadido servidores de operações da bolsa Nasdaq, entre 2008 e 2010, e manipulado dados.

Autoridades de New Jersey informaram que cada envolvido tinha uma especialidade: os russos Vladimir Drinkman, de 32 anos, e Alexandr Kalinin, de 26, invadiam redes de computadores, enquanto Roman Kotov, de 32 anos, explorava os dados das redes comprometidas. Eles acobertavam suas atividades em serviços de hospedagem on-line anônimos fornecidos pelo ucraniano Mikhail Rytikov, de 26 anos, e o quinto integrante do grupo, o russo Dmitriy Smilianets, de 29 anos, é acusado de vender os dados roubados e distribuir os lucros.

8.2. Brasil

Operação "Luz na Infância II", 2018.

A Operação "Luz na Infância II", de combate a crimes de exploração sexual contra crianças e adolescentes no ambiente virtual, prendeu 251 pessoas em flagrante, segundo

número atualizado pelo Ministério da Segurança Pública. As prisões foram efetuadas a partir do cumprimento de 579 mandados de busca e apreensão em 24 estados e no Distrito Federal, são homens e mulheres, de diferentes idades e profissões, flagrados cometendo o delito de armazenar, trocar ou produzir conteúdo ligado a pornografia infantil. Entre os presos, segundo o coordenador de Inteligência Cibernética da Senasp, Alessandro Barreto, estão "pessoas acima de qualquer suspeita", como advogados, educadores, servidores públicos, aposentados.

Raul Jungmann, Ministro da segurança pública apresentou a operação como a maior ação do tipo no mundo realizada, em dois meses foram mais de um milhão de arquivos analisado relacionados à pedofilia na internet e em apenas um único dia todos os mandatos foram cumpridos, com participação de 2,6 mil policiais civis.

9. Considerações Finais

A partir deste longo estudo à Perícia Forense, pode-se compreender que o trabalho realizado por um perito é de extrema acuidade, dependendo do seu ponto de vista ele consegue criar resultados o suficiente para condenar aqueles que desprezam a lei visando obter vantagem para si. Com a tecnologia adentrando cada vez mais em nossas casas, no governo e nas grandes empresas isso se torna um chamariz para aqueles que cometem o crime, principalmente tendo a grande vantagem de estarem no anonimato, porém conforme os criminosos se especializam nesse novo ramo existem aqueles para nos defender contra os crimes cibernéticos. Sendo assim, através de diversas técnicas e ferramentas a disposição do criminoso, também existem aquelas que auxiliam o perito forense na identificação e na condenação dessas pessoas que agem de má fé.

Este Artigo teve, portanto, o intuito de explicar melhor como funciona o trabalho de um profissional na área de criminalistica voltado ao mundo cibernético, compreender um pouco sobre as técnicas, o pensamento crítico e a lógica por trás de cada detalhe observado nos casos apresentados, ajudando a criar um pensamento mais acurado sobre os aspectos que envolvem a Segurança da Informação na área da criminalística onde ambas as áreas caminham juntas.

Referências

YASINCAC, A.; MANZANO, Y. Policies to enhance computer and Network Forensics. IEEE. 2001.

DAMÁSIO, Manuel José. Tecnologia e educação: as tecnologias da informação e da comunicação e o processo educativo. Lisboa: Vega, 2007.

DODT, C. Computer Forensics: FKT Forensic Tools [Forense Computacional: Ferramentas Forenses FTK]. Disponível em <https://resources.infosecinstitute.com/category/computerforensics/introduction/commercial-computer-forensics-tools/ftk-forensic-toolkit-overview/#gref>. Acesso em 10 Out. 2022.

CONSTANTINO, Z, D. Técnicas da Computação Forense. 2012.

FURLANETO, N. M.; GUIMARÃES, J. Crimes na Internet: elementos para uma reflexão sobre a ética informacional. Revista CEJ, América do Norte, 720 03 2003.

ELEUTÉRIO, P. M. S; MACHADO, M. Desvendando a Computação Forense. Editora Novatec, 2011.

KENT, K.; CHEVALIER, S. GRANCE, T.; DANG, H. Guide to integrating forensic techniques into incident response [Guia para integrar técnicas forenses na resposta a incidentes]. 2006.

LUCCAS, R. G. O CONTADOR FORENSE NA INVESTIGAÇÃO E NO COMBATE A FRAUDES NO BRASIL: APLICAÇÃO DA TÉCNICA DELPHI. 2013. Dissertação (Congresso de Iniciação Cientifica em Contabilidade) - Universidade de São Paulo.

LILLARD, T. et al. Digital forensics for network, internet and cloud computing: Burlington: Syngress, 2010

NG, R. Forense Computacional Corporativa. Editora Brasport, 2007.

SILVA, V. A.; OLIVEIRA, C. H. D. Análise De Ferramentas Livres Para Perícia Forense Computacional. Caderno de Estudos Tecnológicos, v.2(1), p.110–132. 2014.

SLEUTHKIT. Autopsy [Autópsia], Disponível em <http://www.sleuthkit.org/autopsy/>. Acessado em 19 mai. 2018.

RIBEIRO, A. A. D. Contabilidade e Lavagem de Capitais. 2009. Dissertação (Tese de mestrado) – Centro de Ciências Sociais Aplicadas.

SINGH, SIMON. The code book. Editora Record, 1999.

THE story of Information- Order and Disorder. Direção: Nic Stacey, Produção: BBC. Reino Unido, 2012, 1 DVD

FREITAS, Andrey Rodrigues de. Perícia forense aplicada à informática. Rio de Janeiro: Brasport, 2006.

SILVA, V. A.; OLIVEIRA, C. H. D. Análise De Ferramentas Livres Para Perícia Forense Computacional. Caderno de Estudos Tecnológicos, v.2(1), p.110–132. 2014.