Computação Forense no Brasil

Ivan Leoni V. Boas[1], **Leonardo Rodrigo de Sousa**[1], **Lucas Tiense Blazzi**[1], **Thiago Marcelo Passos**[1]

[1] Instituto de Matemática e Computação
Universidade Federal de Itajubá (UNIFEI) – Itajubá, MG – Brazil

Abstract. *Cybercrimes have strong impacts not only on Brazilian society as in the world. Added to that, the illegitimate computer acts has been increasing more and more in recent years and, therefore, it is necessary to investigation and production of evidence to combat such crimes. To help such problems the important area of computer forensics systematically proves the execution of collection, examination, analysis and reporting processes for authorities law enforcement agencies in order to discover such computer crimes. Highlighting the process of examination that must be carried out according to the environment in which the crime is committed in order to better analysis and more accurate conclusions about the evidence.*

Resumo. *Os Crimes cibernéticos têm gerado fortes impactos não somente na sociedade brasileira como no mundo. Somado a isso, os atos infomáticos ilegais vem aumentado cada vez mais nos ultimos anos e, por isso, é necessario a investigação e a produção de provas para combater tais crimes. Como ajuda a tais problemas a importante área da computação forense provê sistematicamnte a execução de processos de coleta, exame, análise e relatório para autoridades legais a fim de solucionar os crimes informáticos. Em destaque o processo de exame que deve ser realizado conforme o meio que o crime é acometido para melhor análise e conclusões mais certerias acerca das evidências.*

1. Introdução

Devido ao grande avanço tecnológico e a dependência de empresas e pessoas quanto aos diversos equipamentos como notebooks, tablets, celulares, computadores, relógios inteligentes, entre outros, e, ainda sobre os sistemas informatizados e a internet, os crimes também evoluíram paralelamente, tomando esses mesmos equipamentos como uma ferramenta para cometer atos ilícitos, uma vez que, uma grande desvantagem que a evolução tecnológica traz consigo são os crimes. A percepção de obter uma vantagem monetária, de forma ilegal, enganando outros usuários e invadindo sistemas organizacionais, sejam eles públicos ou privados, tem fortemente originado os crimes digitais e principalmente as fraudes digitais que se apresentam uma realidade crescente não apenas na sociedade brasileira como mundial.

Com o desenvolvimento da tecnologia e uso massivo da internet, de forma nem sempre segura, houve por consequência um aumento de crimes cibernéticos e para realizar a investigação de tais atos faz-se o uso da Ciência Forense, que conforme [Garrido and Giovanelli 2009] é o conjunto de métodos e técnicas científicas que são aplicadas na resolução de diveros crimes e assuntos legais (cíveis, administrativos e penais) contemplando inúmeras áreas do saber (física, química, biologia, entre outras). A area criminal da Ciência Forense visa elucidar os problemas do ato criminoso, como a

identificação dos envolvidos na ação ilegal, sejam eles autores ou vítimas, e também das ferramentas de TI que foram utilizados para o cometer tal crime. A partir do uso e para a identitificação e análise dos dispositivos informaticos de um crime surgiu a Computação Forense (computação forense), que é um dos ramos da Ciência Forense, que abarca os estudos realizados pela perícia digital, objetivando a investigar e ajudar na solucionação de crimes, através da coleta de informações digitais dos dispositivos para determinar a causa dos ilícitos que se relacionam diretamente com a TI. Para isso, se utiliza a identificação e a análise minuciosa dos dados e das evidências digitais espalhadas pelo crime, que são solucionadas, conforme [da Silva Eleutério and Machado 2011], através de métodos científicos de análises quantitativas e qualitativas. Resumidamente [Melo 2009] define computação forense como uma área da Ciência da Computação que se desenvolve gradualmente para atender à demanda oriunda da Criminalística, e também como uma parte da Criminalística que se apropria de fundamentos da Ciência da Computação, ou seja, a intercecção da area da criminalistica com a computação formam a computação forense. Assim a computação forense não está relacionada apenas a soluções de crimes digitais e fraudes (como, por exemplo, clonagem de cartões e roubo de dados pessoais), mas também na busca de provas e evidências para solução de qualquer tipo de crime que esteja relacionado à área de informática. Portanto, cabe à computação forense identificar e manipular as evidências que possam ser usadas como provas consistentes de um crime, incluindo a devida coleta de informações digitais dos dispositivos.

Encontrar evidencias que são ocultas as pessoas comuns e que visam a identificação e a preservação de todas as provas necessárias para resolução do ato ilegal é fundamental para solução de um crime e cabe a sua devida realizaçao por peritos qualificados. Estes especialistas conseguem rastrear e analisar todo tipo de informação coletada a partir de qualquer dispositivo que possa conter informações importantes. Entretanto, eles possuem habilidades, aptidões e métodos específicos para encontrar rastros maliciosos, mesmo que sejam sutis, e também, a capacidade de verificar a tentativa de adulteração dos dados para tentar apagar vestígios que liguem os fatos como, por exemplo, averiguações de documentos digitais fraudados e alterações de data e hora em vídeos.

Uma das razões para o aumento dos crimes cibernéticos é a falsa sensação de impunidade que se tem, no qual os indivíduos cometem crimes acreditando que ao consumar as transgressões da lei por estarem a longa distância e que os instrumentos utilizados para as práticas do ilícito não fornecem algum tipo de identificação, porém a computação forense está desmistificando cada vez mais esse errôneo conceito.

2. Crimes Cibernéticos

Com o advento da internet no Brasil e no mundo, os malfeitores também aperfeiçoaram os crimes e as invasões aos computadores e sistemas. Somado a isso conseguiram adaptar os tradicionais delitos realizando a sua migração do mundo real para o virtual. Os criminosos cometem os mais variados tipos de imoralidades e crimes cibernéticos como o uso da rede para assediar pessoas, discrimina-las, vender produtos ilegais, bem como realizar injúria, calúnia e difamação, pedofilia, espionagem, apologia ao crime, estelionato, roubo de identidade e até terrorismo. Conforme [da Silva 2015] o crime cibernético é qualquer crime que seja realizado com o uso de dispositivos informáticos e de rede de transmissão de dados para delinquir alguem e no campo jurídico a conduta por lesar um outrem é dada como culpável. Somado a isso, conforme [da Silva Filho] o crime cibernético já

é o terceiro que mais causa prejuízo financeiro ao mundo depois do narcotráfico e da falsificação de marcas e de propriedade intelectual.

Os crimes podem ser classificados segundo [da Silva Filho] com a forma de como os equipamentos computacionais são utilizados para o cometimento de um crime: Sendo classificado como ferramenta de apoio à prática de delitos convencionais ou como condição necessária para a existência. Onde no primeiro caso o computador é um mero instrumento facilitador para os crimes, ou seja, são delitos que podem ser cometidos sem necessariamente o uso de computadores. Para [Costa 2004] este tipo de crime pode ser classificado quanto à sua essência de impuro por serem realizados por meio do computador, mas por ser considerado já um crime tradicional, porém que atualmente se faz uso de algum equipamento ou tecnologia, e, por isso deixa algum vestígio digital. Como exemplos têm-se os crimes contra a honra, crime de ameaça, furto, apropriação indébita, violação de direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, incitação ou apologia ao crime ou ao criminoso, jogos de azar, estelionato, pedofilia, crime de divulgação do nazismo, pornografia infantil, entre outros. Como exemplo mais específico deste tipo se enquadra o crime de corrupção passiva, onde para haver corrupção o agente não precisa de um computador, mas provavelmente as atitudes ilícitas podem deixar rastros digitais que podem ser utilizadas como provas no campo penal como os e-mails trocados entre os parceiros do crime, planilhas e demais documentos digitais que possam materializar o fato criminoso.

No segundo caso o computador é visto como peça fundamental da ação criminosa onde se enquadra os crimes de informática propriamente ditos segundo [Costa 2004, da Silva Filho], ou seja, sem o computador tais crimes não existiriam, pois são peças imprescindíveis para o cometimento do crime. Neste caso se enquadra também os crimes em que o computador é visto como alvo. [Costa 2004] ainda classifica este tipo de crime na essência de puro pelo uso direto da TI para sua ocorrência, ou seja, o autor do fato age com o objetivo de atacar, de forma virtual ou física, programas, redes, sistemas e unidades de armazenamento de dados. Como exemplos deste tipo apresentam-se os crimes de invasão, contaminação por vírus, uso de ransomware, sabotagem do sistema, destruição ou modificação do conteúdo do banco de dados, furto de informação e senhas, furto de propriedade intelectual, vandalismo cibernético, acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo de fora da empresa, entre outros.

Para os crimes tradicionais já existem no Brasil leis específicas sobre, porém a legislação não aborda todos os crimes e principalmente têm se uma maior ausência de leis para os crimes em que o computador é indispensável para seu cometimento, mas não só no Brasil como também internacionalmente, por se tratar de uma temática global, o ambiente virtual e sua constante expansão impõe um grande desafio não somente aos legisladores para conceituar, tipificar e criminalizar as práticas delituosas cometidas no âmbito virtual, mas como também para os profissionais de computação forense que devem constantemente se aperfeiçoar, atualizar e descobrir novas técnicas para combater e identificar para além dos crimes já existentes, como também serem capazes de prever as futuras e possíveis ameaças às pessoas e as corporações.

3. Legislação no Brasil e normas técnicas

Para que um profissional atue na área forense no Brasil, não é necessário que exista alguma titulação ou certificação específica. Também não é taxativo o uso de normas, regimentos ou procedimentos específicos[Velho 2016].

Contudo, para a aceitação de provas perante o Código de Processo Penal, é exigido que o perito oficial de um caso tenha curso superior e adote métodos reconhecidos pela comunidade científica. Se tratando da parte da Justiça, é necessário o uso de regramentos para se aplicar em um caso concreto, de forma a evitar interpretações rasas e datadas. O Direito Digital abrange o Direito Codificado (leis), o Direito Costumeiro (sobre costumes e julgados), princípios e normas de autorregulamentação (Regulamento Técnico)[Velho 2016].

Para a Computação Forense, os profissionais encontram vasto conteúdo de normas oficiais, normas técnicas e procedimentos operacionais, mantidas por entidades nacionais, regionais e internacionais, como a Associação Brasileira de Criminalística, a Sociedade Brasileira de Ciências Forenses, a AMN-Mercosul, a International Society of Forensic Computer Examiners, ISO, etc. O uso desses documentos existentes varia para cada contexto, sendo que a escolha deve levar em conta qual possui a melhor aplicação[Velho 2016].

É importante diferenciar o Regulamento Técnico de normas e procedimentos. O Regulamento Técnico é um documento normativo e de uso obrigatório, emitido por autoridades competentes. As normas e procedimentos seguem o regulamento técnico, porém sintetizam conhecimentos científicos, tecnológicos e práticos usados por grupos de trabalhos de especialistas. Normas e procedimentos são abertos para a comunidade e não são de aplicação obrigatória, a menos quando exigido por ato jurídico[Velho 2016].

3.1. Procedimento Operacional Padrão

Os Procedimentos Operacionais Padrão (POP) buscam padronizar e minimizar riscos na execução de tarefas. No Brasil, a Secretaria Nacional de Segurança Pública publicou em 2013 o documento "Procedimento Operacional Padrão Perícia Criminal", um documento que traz padronização na perícia criminal em todo o território nacional, onde aborda quatro POP's computacionais[SENASP 2013]:

1. Exame Pericial de Mídia e Armazenamento Computacional: orienta os exames sobre dados armazenados em mídias computacionais (HDs, pendrives, etc).
2. Exame Pericial de Equipamento Computacional Portátil e de Telefonia Móvel: guia para exames de dispositivos portáteis (tablets, celulares, etc).
3. Exame Pericial de Local de Informática: orienta exames sobre locais de informática ou que demandem análise de vestígios em um local de informática.
4. Exame Pericial de Local de Internet: orienta a investigação de crimes ocorridos com auxílio da internet.

4. Ciência Forense e Processos da computação forense

O trabalho da Forense é examinar vestígios relacionados a um crime, utilizando de métodos científicos e aplicando as ciências à matéria ou problemas legais, cíveis, penais ou mesmo administrativos [Garrido and Giovanelli 2009]. É uma área interdisciplinar, que envolve o estudo de artefatos de diferentes naturezas, a fim de formalizar uma evidência.

Desde o começo da Revolução Científica, no século XVI, e da evolução da medicina (ocidental) existem evidências do interesse do uso de métodos científicos no estudo material dos vestígios, dando origem à medicina legal [Garrido and Giovanelli 2009]. Entre os séculos XIX e XX foi estudado e proposto um modelo de classificação pessoal baseado em impressões digitais, o Sistema Galton-Henry [Prestes 2011]. O uso da Ciência Forense não é algo atual, apesar de estar em constante evolução.

Com a presença constante da tecnologia em diversas áreas da sociedade, com o fenômeno da Computação Ubíqua, não é surpresa o fato de termos um novo ambiente e contexto de estudo para a Ciência Forense: "A Computação Forense é a ramificação da Criminalística que tem como objetivo a análise de vestígios cibernéticos, englobando os elementos que os orbitam." [Velho 2016].

Um modelo simples de processo da computação forense, proposto por [Kent et al. 2006], afirma que o processo ocorre em quatro etapas: a coleta, o exame, a análise e o relatório.

4.1. Coleta de dados

Durante a coleta de dados são identificados os dados relacionados a um evento específico. Esses dados serão etiquetados, registrados e coletados.

A identificação das possíveis fontes de dados computacionais começa pelo mais óbvio, mídias de armazenamento (e os dispositivos que as possuem). Assim, o mais comum no cenário atual seria a análise de computadores, notebooks e celulares. Mídias de armazenamento externas também são uma fonte comum de dados. Em uma abordagem mais profunda, pode ser necessário recolher dados de empresas terceiras, como uma provedora de serviço de internet, dados do aplicativo de antivírus, do firewall, do S.O, dados de periféricos usados. A fonte de dados analisada depende do contexto de trabalho, mas é importante ter ciência de quais existem possibilidade de coleta.

Após a identificação das fontes de dados, é necessário realizar a coleta. A coleta de dados passa por 3 passos:

1. Plano de aquisição de dados: O primeiro passo diz respeito ao planejamento realizado na aquisição dos dados, uma vez que eles vêm de múltiplas fontes. Assim sendo necessário classificar os dados quanto ao seu valor (o que varia para cada contexto), sua volatilidade (dados mais voláteis têm maior prioridade de aquisição) e a quantidade de esforço necessário para a aquisição de dados.
2. Coleta de dados: A aquisição de dados ocorre através de ferramentas forenses seguras, coletando os dados voláteis e duplicando as fontes de dados não-voláteis e protegendo as fontes não-voláteis originais. A coleta pode ocorrer fisicamente ou através da rede, quando não é possível acesso físico.
3. Verificação de integridade: Após a aquisição de dados, é essencial que se prove a integridade dos mesmos, para ser possível o uso legal das informações. A verificação de integridade faz o uso de ferramentas para calcular o resumo da mensagem dos dados originais e copiados e comparar os resumos para garantir que sejam iguais.

Alguns passos complementares são importantes para uso legal e são aconselhados a serem gerados por uma pessoa qualificada. Uma descrição de procedimento, detalhando

passos e ferramentas é essencial para replicação de testes que possam confirmar os resultados apresentados. Fotos e prints podem ser usados na documentação do ambiente e do sistema. Também é necessário registrar os responsáveis pela realização de cada procedimento.

4.2. Exames executados em perícia forense digital

Durante o processo de exames a equipe forense digital precisa realizar exames direcionados ao escopo do problema que está atuando, principalmente de acordo com o meio utilizado no contexto do crime, podendo ele variar, sendo que para cada um desses meios temos ferramentas comuns que ajudam no processo de análise.

De modo geral, temos onze exames em meios diferentes comumente aplicados em processos de análise forense no Brasil, sendo eles: Exames em mídias de armazenamento, Exames em locais de internet, Exames em redes de computadores, Exames em imagens digitais, Exames relacionados a pornografia infanto-juvenil, Exames em computação embarcada, Exames em equipamentos portáteis, Exames em computação na nuvem, Exames em detecção de intrusão, Exames em malwares e Exames em dados criptografados.

Nas subseções seguintes serão detalhados os exames em alguns dos meios comumente inseridos no cotidiano de usuários brasileiros. A intenção é abordar melhor o processo de exame através do meio em busca de dados relevantes para a análise e confirmação de evidência[Velho 2016].

4.2.1. Exames em mídias de armazenamento

No processo de exames em mídias de armazenamento o objetivo é extrair dos dispositivos, informações que sejam relevantes ao fato que está sendo investigado. Dado as questões legais e as regras do processo forense, temos a necessidade de um passo a passo que mantenha a integridade do conteúdo analisado, e para isso é proposto o seguinte fluxo de etapas: preservação, extração dos dados, análise e apresentação (laudos)[Velho 2016].

Na etapa de preservação temos a necessidade de documentação das características do dispositivo coletado (fabricante, modelo, descrição física...) e replicação dele, evitando a manipulação da mídia real, sendo a análise conduzida na cópia do dispositivo para evitar problemas relacionados a danificação do real. Para essa etapa temos a utilização dos chamados equipamentos de duplicação forense (equipamentos especializados que clonam o dispositivo, protegendo a mídia original de possíveis escritas no processo de conexão).

Após a documentação e duplicação da mídia, se inicia o processo de extração dos dados na mídia cópia. O processo de extração busca identificar arquivos fragmentados, removidos ou ativos que possam possuir relevância no escopo da análise. Para isso os arquivos são avaliados em nível de metadados, identificados de acordo com seu tipo pela sua assinatura (magic number) que revela o tipo original do arquivo (ex: txt, jpg, docx), permitindo que os peritos identifiquem possíveis processos de esteganografia que escondam um determinado conteúdo. Além disso, também é executado o processo conhecido como File Carving, que seria o inverso do citado anteriormente, nesse caso o perito conhece os possíveis magic numbers e busca no dispositivo por trechos hexadecimais referentes a esse magic number, podendo assim, extrair arquivos ocultos e corrompidos por essas identificações associadas a limitações de cabeçalho e rodapé[B. 2005].

Por fim, com todos os objetos identificados no processo de extração dos dados, é iniciado o processo de análise. Nessa etapa serão buscadas evidências e provas que envolvem um determinado fato apurado. Assim o perito faz a redução da mídia, excluindo arquivos considerados irrelevantes para o escopo, como softwares conhecidos, aplicativos, drivers e jogos, reduzindo o volume de dados que será analisado, para isso as hashs dos arquivos conhecidos são confrontadas com as hashs dos arquivos existentes (presentes na base NSRL da NIST, que possui mais de 40 milhões de hashes de arquivos conhecidos), evitando que processos de esteganografia escondam uma informação em um arquivo considerado comum ludibriando o perito[Velho 2016]. Com o escopo limitado o perito realiza a busca por palavras-chave de modo automatizado através de mecanismos de indexação e busca, além de realizar também a busca em tempo real por meio de comandos como o grep, permitindo que ele isole conteúdos de seu interesse.

Durante essas etapas abordadas anteriormente, o perito manteve a constante documentação de seus processos, inclusive com horários de atuação, e realizou o levantamento das partes interessantes para o foco da análise, assim, a partir disso, ele faz a construção de laudos, que são os documentos finais referentes a análise realizada em conformidade legal com o processo de perícia.

4.2.2. Exames em locais de internet

No processo de exames em locais de internet temos a buscas de evidências em ambientes que utilizam da internet para funcionamento, podendo ser servidores, e-mails, páginas web, servidores dns, aplicativos de chat, redes sociais, navegadores e redes TOR. A exploração desses ambientes se dá de acordo com o escopo que o crime se encontra, sendo na maioria das vezes as redes sociais sempre presentes como ferramenta de exploração. Assim, o primeiro passo para esse exame é a identificação do meio utilizado pelo criminoso, sendo que esse meio determinará a abordagem a ser seguida[Velho 2016].

O email é um dos meios utilizados, sendo muito comum para a aplicação de golpes e utilização para comunicação relacionada ao crime. Nessa análise é importante validar os cabeçalhos do email, já que eles irão conter o caminho que a mensagem percorreu, podendo extrair informações de origem e destino em nível de IP, para caso necessário, solicitar quebra de sigilo ao devido provedor. Nesse caso também é possível solicitar a interceptação de dados telemáticos, semelhante a interceptação de dados telefônicos, porém nesse caso se tem uma conta espelho para qual as mensagens de um alvo são direcionadas, ocorrendo o monitoramento em tempo real.

Outro tipo de meio comum para aplicação de golpes são as paginas web, muito usual para roubo de identidade. Esse tipo de análise pode ter como objetivo a investigação de seu teor, como em casos de conteúdo ilícito (racismo, tráfico de drogas, venda de armas, exploração sexual de menores), o que necessita da validação do material e identificação de responsáveis. O primeiro passo nesse caso é a análise offline, onde o conteúdo do website é copiado com o objetivo de preservar as informações de um determinado horário (utilizando wget ou Wayback Machine). Com o objeto clonado é realizada a identificação de possíveis temas ilícitos que poderão levar ao processo de investigação dos responsáveis. Nesses cenários muitas vezes também é cruzar informações de domínio do website, sendo utilizado o whois para verificação de informações do dono do domínio,

facilitando o processo de requisição de acesso a registros armazenados nos provedores de acesso a rede (quebra de sigilo)[P. M. S. 2011].

Um facilitador para as investigações são as redes sociais, dado a publicação da vida pessoal em massa pelos usuários, possuindo grande valor para apuração de crimes e identificação de suspeitos. A exploração das redes sociais pode se dar em tres escopos, no caso de ocorrer sua utilização como apoio ao crime (estelionatos e tráfico), utilização como meio do crime (distribuição de malware e compartilhamento de pornografia infantil) ou verificação de perfil de suspeitos. Nos três casos, o objetivo do perito é identificar vestígios cibernéticos nas redes, como publicações, mensagens privadas e compartilhamento de arquivos. O importante nesse processo é a identificação dos envolvidos (id do perfil da rede) com informações adicionais como timeline, timestamp, dispositivo, locais, amigos, fotos, grupos, curtidas, registro de atividades, localização de mensagens, todos eles variando de acordo com a rede social em que se atua. No caso da investigação ocorrer em um dispositivo que utilizou uma rede social, é possível utilizar ferramentas como Facebook Forensic Toolkit e Twitter Forensic Toolkit, que contribuirão para identificação de vestígios[L. 2011].

Para a busca de vestígios no dispositivo, também é utilizada a exploração de dados de navegação dos usuários, presentes nos navegadores. Nesse caso temos a busca de dados em cookies, histórico de navegação, cache, localização em disco, existindo métodos específicos para acesso aos dados de acordo com o navegador utilizado e sua respectiva versão.

No caso de ser identificado um anonimizador de navegação um passo anterior deve ser tomado pelo perito. No caso da utilização de proxies é possível solicitar a quebra de sigilo aos provedores, já que eles mantêm informação de fluxo de comunicação de seus usuários, podendo conter o IP da pessoa envolvida, ele se aplica para o caso da utilização de VPNs. No caso da identificação de utilização da rede TOR / Deep Web, existe a impossibilidade de mapeamento da origem das mensagens pela arquitetura de nós de entrada, trânsito e saída da rede TOR, nesse caso os peritos buscam por alvos que possuem vulnerabilidades no navegador TOR, identificação de origem por metadados em arquivos, captura de características de navegador utilizado, resolução, idioma, fuso-horário[Velho 2016].

4.2.3. Exames em redes de computadores

A análise de redes de computadores consiste na tentativa de encontrar logs nos diversos recursos de infraestrutura de redes, muitas vezes se analisando o tráfego da rede buscando recuperação de dados trafegados nos protocolos de rede, identificação de fontes de ataques por engenharia reversa, busca de atividades de usuários, identificação de ataques a servidores. As buscas são executadas de acordo com o objeto analisado, sendo esses recursos abordados nos seguintes parágrafos[Velho 2016].

No caso de switches temos a o mapeamento entre o endereço físico (MAC) e a porta física do switch, sendo essa informação buscada na tabela CAM, com a identificação dessa porta é possível localizar fisicamente o equipamento com o endereço encontrado. No caso de roteadores o perito tenta descobrir o caminho de um tráfego de rede do usuário

através da tabela de roteamento, fazendo o mapeamento entre os endereços da rede e a porta física do roteador.

No caso de servidores de autenticação, como Active Directory e LDAP temos a identificação de atividades de autenticação nos logs do sistema, sendo encontrados dados de endereço, horário, origem e tentativas de conexão, que servem para identificar DoS por exemplo. Em servidores proxy o perito tem a preocupação de encontrar atividades de um determinado usuário, como sites acessados em determinados horários, já que ele armazena os logs de todas as ações dos usuários no servidor. Podendo o perito encontrar ações de descumprimento de políticas e distribuição de malwares, por exemplo[Sherri 2012].

Em servidores DHCP é possível cruzar os endereços físicos (MAC) com o endereço IP de determinado equipamento, podendo associar um ataque identificado anteriormente provindo de um IP específico com o endereço físico mapeado pelo DHCP.

Outro sistema muitas vezes utilizado são os sistemas de detecção e prevenção de intrusão e firewalls, que por realizar o monitoramento (passivo e ativo) de tráfego de rede e identificarem padrões relacionados a ataques conhecidos, fornecem dados relevantes para peritos no processo de análise para identificar a origem de ataques.

Em servidores de DNS temos o armazenamento de logs referentes a IP de origem de requisição, hostname alvo e horário da requisição, que permite ao perito mapear um histórico de atividades relacionados a um determinado IP, além de permitir a identificação de computadores infectados por malwares que se comunicam por servidores acessados via DNS[Sherri 2012].

Por fim, em servidores de aplicação pode se encontrar registros de log de atividades de usuário como IP origem, método HTTP, url, resposta da requisição, horário e navegado. A partir disso, é possível mapear possíveis ataques realizados, já que seus padrões são conhecidos como no caso de ataques de injeção SQL, DDoS, LFI, RFI.

Essas buscas citadas anteriormente muitas vezes utilizam de ferramentas específicas para as atividades se destacando: Wireshark, TCPDump, NetworkMiner, XPlico, DSniff, Snort.

4.2.4. Exames em malwares

Dado a quantidade de dispositivos infectados e o aumento de incidentes de segurança e crimes cibernéticos associados a distribuição e uso de malwares, viu-se a necessidade de um exame detalhado desse tipo de ameaça, no caso da computação forense a análise tem três principais objetivos: analisar um software suspeito já utilizado, analisar ataques que utilizam malwares como elemento principal, e analisar malwares como elemento secundário para aquisição de informações criadas pelo malware (spywares / keyloggers)[Velho 2016].

Para o processo de exame em malware alguns tipos de análise são utilizados, sendo eles: análise estática, análise dinâmica, análise post-mortem e avaliação de utilização de antianálise.

Na análise estática envolve a análise do código sem a execução do malware, identificando elementos do código fonte que possam determinar seu funcionamento, localização

de métodos de comunicação na rede e disassembling. Esse processo é conhecido como engenharia reversa e é feito através de um disassembler, que desmonta o código para ser analisado em nível de instrução (linguagem assembly).

Na análise dinâmica temos o estudo do software em execução, verificando quais são os impactos e as atividades do malware no sistema, avaliando desde os sistemas de arquivos até o tráfego na rede, esse processo utiliza de debuggers que examinam as instruções aplicadas pelo malware em tempo de execução.

Na análise post-mortem, temos a investigação de vestígios gerados pelo malware após a execução em um sistema, buscando informações a partir de logs dos sistemas atingidos.

Por fim, também é executado a análise de aplicação de antianálise no malware, sendo a antianálise uma técnica para prevenir e dificultar o processo de análise dos peritos. Algumas dessas implementações envolvem a capacidade de detecção de uma execução em máquina virtual, modificando o comportamento nesse cenário, empacotamento de arquivos sendo combinados por um código de descompressão para execução, que dificulta a análise, e a ofuscação que modifica a estrutura do código para torná-lo menos compreensível[M 2011].

4.2.5. Exames em dados criptografados

Muitas vezes é comum os peritos se depararem com dados criptografados, que podem estar nos dados de tráfego de rede como em mídias de armazenamento que precisam ser analisados. Os procedimentos nesse caso são voltados para o aumento da probabilidade de encontrar as senhas ou chaves necessárias para o acesso dos conteúdos, sendo que em alguns países existem Leis de Divulgação de Chaves que podem obrigar o fornecimento desses dados[Velho 2016].

Para o acesso aos dados, os peritos precisam realizar o processo de decifragem através de métodos conhecidos, como: recuperação direta, pré-computado, dicionários, força bruta, métodos probabilísticos.

No processo de recuperação direta tem-se a exploração de vulnerabilidades conhecidas nos algoritmos criptográficos utilizados, facilmente encontrados em cifras de substituição e XOR, além disso, nesse cenário também são procurados dados no dispositivo, que pode possuir a senhas armazenadas.

No método criptografado tem-se tabelas que mapeiam um texto claro e seu texto cifrado, sendo possível encontrar o texto cifrado nesse mapeamento, essas tabelas são conhecidas com Rainbow Tables e são comumente utilizadas para quebra de hashs.

No método de força bruta tem-se a busca exaustiva de combinações que possam gerar a chave ou senha para determinado acesso, sendo considerado um método ineficiente que é aplicável no cenário de cenas pequenas ou comuns.

A utilização de dicionários nada mais é que um método de força bruta mais sofisticado, onde se tem a possibilidade de quebra de senha a partir de n tentativas de inserção de textos que estão contidos em um arquivo (dicionário) com cada possibilidade em uma linha do arquivo, normalmente esse dicionário é alimentado por palavras comuns e se-

nhas já vazadas na internet, podendo ser gerado especificamente para o usuário alvo dado o conhecimento de informações pessoais do alvo[Eoghan 2002].

Por fim, tem-se a possibilidade de aplicação de métodos probabilísticos, nesse método existe a geração de expressões e combinações por meio de análise de padrões em senhas conhecidas do próprio alvo para geração de senhas prováveis a partir do treinamento de gramática do algoritmo.

4.3. Análise de dados

Com a extração dos dados concluída, é hora de analisar as informações e tirar conclusões em cima dos dados. Esse processo utiliza uma abordagem metódica para extrair conclusões adequadas ou definir que não é possível ter uma conclusão acerca dos dados.

A análise deve conectar pessoas, lugares, eventos e objetos de um modo que faça sentido para o caso. Com a presença de múltiplas fontes de dados, a análise deve englobar a informação de modo geral, porque ela é parte de um todo, mas está distribuída. Por exemplo, um log de um sistema de detecção de intrusão à rede pode ligar o evento a um host, o log do host liga o evento a um usuário, detalhando quais foram as ações praticadas.

4.4. Relatórios

A fase final desse processo abordado da computação forense é o relatório, que consiste na preparação e na apresentação formal dos resultados da análise. A geração de relatórios deve ser adequada com o seu objetivo de uso. Relatórios usados em processos criminais, devem ser detalhados e técnicos, mas permitir que pessoas fora da área tecnológica entendam o objeto estudado e onde se quer chegar com aquela análise. Além disso, os relatórios têm que seguir as normas de redação oficial, devendo ser impessoais, claros, concisos e formais [Velho 2016].

4.4.1. Laudo Pericial

O Laudo Pericial é um dos possíveis relatórios formais usados em processos. Ele é obrigatoriamente feito por um perito oficial. Segundo o Código de Processo Civil, Artigo 473 [Senado Federal 2015], o laudo pericial deve conter: I - a exposição do objeto da perícia; II - a análise técnica ou científica realizada pelo perito; III- a indicação do método utilizado, esclarecendo-o e demonstrando ser predominantemente aceito pelos especialistas da área do conhecimento da qual se originou; IV - resposta conclusiva a todos os quesitos apresentados pelo juiz, pelas partes e pelo órgão do Ministério Público.

O laudo tem uma estrutura padronizada sugerida, definida pelo Procedimento Operacional Padrão Perícia Criminal [SENASP 2013], composta por **Preâmbulo**: traz as informações relativas ao exame pericial, como os órgãos requerentes, tipo de exame, perito designado, etc; **Histórico (opcional)**: relata dados para compreensão dos fatos, da dinâmica e autoria dos atos realizados; **Objetivo**: Explicita os objetivos da perícia, podendo relatar os requisitos dos exames realizados; **Exame**: É mostrado as técnicas e métodos utilizados no exame e o caminho usado para fundamentar as conclusões (observação do ambiente, hipótese sobre vestígio, experimento de verificação de hipótese, lei científica que comprove os resultados, teoria que explica as questões levantadas); **Considerações técnico periciais (opcional)**: é a parte do laudo que o perito pode fazer

considerações sobre os vestígios e fatos e discutir sobre objetivos, detalhar as descobertas e sintetizar todo o trabalho científico, além de sugerir exames complementares; **Conclusão e resposta aos quesitos**: é definido se os resultados foram conclusivos ou não e apresentar um ponto final objetivo para o documento; **Anexos (opcional)**: Documentação anexa que complementa o laudo.

4.4.2. Parecer Técnico

Segundo [Velho 2016], o parecer técnico não precisa ser realizado por um perito oficial, como o laudo pericial, porém segue um padrão de conteúdo semelhante. O parecer técnico é feito por um especialista na área, com formação adequada. A estrutura do parecer técnico apresenta o histórico, o objetivo, a descrição do material analisado, os procedimentos preliminares, análises técnico periciais (os 3 últimos se assemelham com a fase de exame do laudo pericial), a conclusão e os anexos, se necessários.

4.5. Integridade e judicialização da prova

O Código de Processo Civil garante o direito do uso de todos meios legais, moralmente legítimos como prova de fato, assim como garante o direito da impugnação da exatidão destes meios (Código de Processo Civil, Artigos 369 E 255)[Senado Federal 2015].

Porém, para que possua valor legal, a prova precisa apresentar dois fundamentos essenciais: autenticidade e integridade. A autenticidade é a certeza da autoria e a integridade é certeza da não alteração (propositalou involuntária)[Velho 2016].

Complementando a autenticidade e integridade há a cadeia de custódia, formada pela documentação que comprove cronologia e controle de acesso do vestígio, sendo possível determinar as ações realizadas com o objeto de investigação por determinada pessoa ou entidade[Velho 2016].

Dados particulares, da posse de terceiros precisam de ordem judicial na coleta, para que sejam consideradas lícitas. Provas digitais tendem a possuir um tempo de vida curto e esperar que uma ordem judicial seja expedida pode prejudicar ou impossibilitar a obtenção da prova. Assim, a obtenção de ordens de busca e apreensão ou inspeções costumam ter um caráter de urgência e ocorrerem de forma mais rápida do que o usual, devido à sua natureza[Velho 2016].

5. A importancia da computação forense

A evolução da internet permitiu a conexão entre as pessoas de diversas partes do mundo de forma rápida, acelerando a troca de informações entre elas e consequentemente vários benefícios a sociedade em geral, porém juntamente com os benefícios, houve o advento dos crimes cibernéticos, ou seja, as práticas ilegais e criminosas envolvendo a internet. Como em qualquer área, os crimes podem deixar vestígios, e no ambiente da informática, esses vestígios podem ser analisados por profissionais específicos, como os peritos criminais em informática, auditores de sistemas, profissionais de TI entre outros. O ramo da legislação que investiga os vestígios e os crimes cibernéticos é chamada de computação forense. A computação forense pode ser considerada a junção da ciência da computação com o ramo do direito, nesse âmbito é considerado a análise de qualquer dispositivo eletrônico para a

análise de crimes, podendo ser o dispositivo um computador, celular, dispositivos de armazenamento como pen-drives e discos rígidos, ou até mesmo informações como dados de um GPS. Atualmente a computação forense se tornou uma das formas mais eficientes de combate ao crime cibernético, visto que a internet gera um ambiente que passa a sensação de impunidade e a falta de autenticidade das ações, a computação forense atua identificando os vestígios dos crimes cibernéticos e consequentemente os responsáveis pela ação.

6. Problemas da computação forense

Apesar de ser muito importante para a análise crimes digitais, a computação forense apresenta alguns problemas relacionados tanto a quantidade de dados que são processados por uma máquina, quanto pela falta de profissionais capacitados a atuar no ramo do direito e da computação. Devido o rápido desenvolvimento dos sistemas computacionais, maiores quantidades de informações podem ser armazenadas, processadas e transferidas de um sistema a outro, portanto um período de tempo considerável deve ser destinado a análise dessas informações e somente com as ferramentas específicas é possível essa análise, visto que a utilização de pessoas poderia aumentar significativamente esse tempo. Além disso, o Brasil não possui uma legislação específica sobre crimes eletrônicos, dificultando a execução de penas rígidas para crimes cibernéticos. Outro ponto que pode ser citado é o aumento de dispositivos com acesso a internet com o avanço do 5G e consequentemente a evolução do IOT, devido a esse alto número a diversidade de pontos de acesso aos criminosos pode dificultar a análise dos resquícios dos crimes. Apesar de todos esses problemas, a maior dificuldade encontrada pela computação forense é a transformação dos dados encontrados nos sistemas computacionais em provas aceitas pela justiça, e para isso é necessário uma série de procedimentos rigorosos garantindo a validade das provas, portanto para o resultado de provas concretas os responsáveis pela investigação deve ter um conhecimento tanto na área da computação, quanto na área do direito e esses profissionais estão cada vez mais em escassez no mercado.

7. Futuro da computação forense

Segundo dados divulgados pelo grupo Mz, os ataques cibernéticos cresceram no primeiro semestre de 2021 cerca de 220% em comparação com o mesmo período de 2020, esse aumento se deu devido ao crescimento do trabalho remoto em tempos de pandemia e a possibilidade de acessar dados confidenciais em ambientes não controlados. Ao analisar esses dados, pode-se inferir que a computação forense tem e continuará a ter uma grande importância também no cenário empresarial, onde atuará como ferramenta essencial a identificação de responsáveis por vazamentos de dados sensíveis, tentativas de invasões, e roubo de informações. Portanto o crescimento da demanda por profissionais especializados também será um fato, e consequentemente o problema da falta de pessoas será acentuado. De acordo com a Associação Brasileira de Criminalística (ABC), a perícia criminal estadual trabalha hoje com um déficit de pessoal estimado em 30 mil peritos, e ainda segundo o estudo da ABC o Brasil tem hoje cerca de 6,5 mil peritos e o número mínimo recomendado pelas nações unidas seria de 1 perito para cada 5 mil habitantes, então o número mínimo de peritos criminais que precisaria ter seria de 38 mil peritos.

8. Conclusão

O desenvolvimento humano e tecnológico não pode se estagnar mesmo que atualmente os crimes cibernéticos tenham se mostrado cada vez mais em alta. A evolução trás consigo grandes benefícios à humanidade, mas como efeito negativo, atos ilícitos têm crescido paralelamente no Brasil. A solução de enfrentamento está na computação forense que contempla a criminalística e a computação afim de ser a grande aliada no combate aos crimes cibernéticos e informáticos.

A sociedade brasileira ainda sofre por não haver leis existentes para todos atos imorais cometidos por cibercrimiosos, e no que tange a área forense um perito deve além de possuir competências e habilidades adotar métodos científicos e seguir rigorosamente regramentos, além de atentar para procedimentos operacionais padrões a fim de atender a justiça e o código penal. Além disso, o processo da computação forense inclui 4 etapas fundamentais que devem ser devidamente executadas para possuir valor legal. Eles são a coleta, o exame, a análise e o relatório. Todos estes processos são complementares e quando realizados de forma correta produzirão um relatório eficiente para solucionar moralmente diversos tipos de atos ilegais. Em destaque especial para o processo de exames que devem ser realizados sempre de acordo com o meio tecnológico que é utilizado para cometer atos ilícitos, pois cada meio utilizará uma ferramenta mais especifica e apropriada para ajudar na análise final.

A computação forense, portanto, desempenha um importante papel na investigação e solução, acusando com provas criminalmente ou absolvendo, e, para além de combater crimes a computação forense ajuda diretamente na prevenção de possíveis delitos que poderiam vir a ser cometidos e até mesmo contribuindo na evolução e melhorias de sistemas perante as falhas que podem ser encontradas na fase de exame.

Referências

B., C. (2005). *File System Forensic Analysis*. Addison Wesley Professional, 1th edition.

Costa, A. M. (2004). Crime informÁtico. In EMERJ, editor, *REVISTA DA EMERJ*, page 24/40. V.7, N.28.

da Silva, P. S. (2015). *Direito e crime cibernético: Análise da competência em razão do lugar no julgamento de ações penais*. Editora Vestnik, 1th edition.

da Silva Eleutério, P. M. and Machado, M. P. (2011). *Desvendando a Computação Forense*. Novatec Editora, 1th edition.

da Silva Filho, W. L. Crimes cibernéticos e computação forense. Novatec Editora.

Eoghan, C. (2002). *Practical approaches to recovering encrypted digital evidence*. International Journal of Digital Evidence, 1th edition.

Garrido, R. G. and Giovanelli, A. (2009). Criminalística: origens, evolução e descaminhos. In *Cadernos de Ciências Sociais Aplicadas*, number 5/6, pages 46–60, Vitória da Conquista-BA.

Kent, K., Chevalier, S., and Grance, T. (2006). Guide to integrating forensic techniques into incident.

L., D. (2011). *Digital forensics for legal professional - Understanding digital evidence from the warrant to the courtroom*. Elsevier, 1th edition.

M, L. (2011). *Malware analyst's cookbook*. Wiley, 1th edition.

Melo, S. (2009). *Computação Forense com Software Livre*. Alta Books, 1th edition.

P. M. S., E. (2011). *Desvendando a Computação Forense*. Novatec, 1th edition.

Prestes, Á. N. (2011). Sistema de reconhecimento de impressões digitais.

Senado Federal (2015). Código de processo civil.

SENASP (2013). Procedimento operacional padrão perícia criminal.

Sherri, D. (2012). *Network Forensics: Tracking Hackers through Cyberspace*. Prentice Hall, 1th edition.

Velho, J. A. (2016). *Tratado de computação forense*. Milennium Editora, 1th edition.