REVISTA CIENTÍFICA ELETRÔNICA DE CIÊNCIAS SOCIAIS APLICADAS DA EDUVALE
Publicação científica da Faculdade de Ciências Sociais Aplicadas do Vale de São Lourenço - Jaciara/MT
Ano V, Número 07, novembro de 2012 – Periodicidade Semestral – ISSN 1806-6283

PERÍCIA FORENSE COMPUTACIONAL: METODOLOGIAS, TÉCNICAS E FERRAMENTAS

GONÇALVES, Márcio[1]
AMADIO, Renato Arnaut[2]
GAVILAN, Júlio César[3]
SANTOS, 'Herlones Wuilles dos[4]

RESUMO: Este trabalho apresenta ao leitor a definição de computação forense, os procedimentos realizados em uma investigação de perícia computacional e a solução de crimes na área de informática. A perícia computacional é uma área recente, e que precisa acompanhar o crescimento tecnológico. A perícia computacional traz ao mercado da tecnologia a solução em criminalística, sendo um auxiliar da justiça na coleta de provas, através de evidências digitais, que são coletadas nos equipamentos computacionais suspeitos de serem usados em um delito. Em meios práticos a finalidade da pericia computacional é buscar formas para comprovar um crime de informática, e levar a justiça até o autor do crime. A evidência fornece ao profissional em perícia computacional as informações para a investigação. Será descrito neste trabalho todas as etapas de uma investigação, busca e preservação de evidências, coleta, análise, laudo pericial, e algumas ferramentas existentes que auxiliam o profissional em perícia no trabalho de investigação. Será abordado também a legislação brasileira com relação aos crimes digitais e alguns exemplos de casos reais de crimes de informática que mostram como é solucionado um delito virtual.
PALAVRAS-CHAVE: Perícia Forense, Evidência, investigação, crimes.

[1] Graduado em Sistemas de Informação pela Faculdade de Ciências Sociais Aplicadas do Vale do São Lourenço – EDUVALE.
[2] Especialista em Redes e Teleprocessamento pela UNIC e Bacharel em Ciências da Computação pela UNIPAR. Atualmente professor do Curso de Sistemas de Informação da Faculdade de Ciências Sociais Aplicadas do Vale do São Lourenço – EDUVALE.
[3] Mestre em Ciências da Computação pela Universidade Federal de Santa Catarina e Bacharel em Física Computacional pela Universidade de São Paulo. Atualmente é professor e chefe do departamento do Curso de Sistemas de Informação da Faculdade de Ciências Sociais Aplicadas do Vale do São Lourenço – EDUVALE.
[4] Professor Especialista e Coordenador do Curso de Sistemas de Informação – Faculdade EDUVALE.

INTRODUÇÃO

As Tecnologias da Informação cresceram de uma forma espantosa em um curto espaço de tempo. Na atualidade o computador faz parte da vida de milhões de pessoas no mundo. A massificação do uso da internet e do computador trouxe recursos importantes para a sociedade. Vivemos na sociedade da informação, onde nos tornamos dependentes das informações, e a disseminação das mesmas na internet passou a ser uma ferramenta importante para instituições e empresas.

Hoje as instituições cada vez mais utilizam avanços da tecnologia para melhorias em suas operações e também para um crescimento no potencial de mercado. Hoje podem ser feitas através do computador conectado a internet transações bancárias, vendas, compras, divulgação de serviços e produtos, comunicação, etc. O crime virtual tem crescido a cada dia juntamente com o avanço das tecnologias. Para combater esse tipo de crime, não basta apenas serem usados os métodos de investigação convencionais, para isso é necessário conhecimento das tecnologias computacionais.

Conforme Eleutério e Machado (2011) a Perícia Forense ou Análise Digital Forense é a modalidade de perícia criada para combater os crimes digitais, utilizando análises e métodos na busca de identificar e coletar evidências comprovadas e eficientes.

Neste trabalho será mostrado o conhecimento que o profissional precisa ter para atuar na perícia, e também as metodologias, técnicas e ferramentas utilizadas na Análise Digital Forense, além de contribuir como enriquecimento didático para está área de pesquisa pouco explorada e com poucos profissionais.

DEFINIÇÃO DE COMPUTAÇÃO FORENSE

Segundo Eleutério e Machado (2011) a Computação Forense é a ciência que usa técnicas especializadas, para coletar, preservar e analisar os dados digitais de um computador ou computadores suspeitos de serem utilizados em um crime virtual, sendo assim apresentados para a justiça através de um laudo pericial. Da mesma forma que a perícia convencional, ela trata de buscar evidências para a solução de um crime.

> A Computação Forense é a ciência que, através de técnicas e habilidades especializadas, trata da coleta, preservação e análise de dados eletrônicos em um incidente computacional ou que envolvam a computação como meio de praticá-lo. (ELEUTÉRIO E MACHADO, 2011, p. 31).

De acordo com Eleutério e Machado (2011) para a perícia criminal da polícia, a computação forense envolve o trabalho investigativo e todo o trabalho pericial, para desvendar os crimes cometidos através do uso do computador. Ela pode ser empregada tanto para fins legais como exemplo investigar espionagem industrial, como também para ações disciplinares internas, por exemplo, uso indevido de recursos de uma empresa.

Segundo Santos (2008) a Forense Digital é uma área recente de pesquisa, e necessita de desenvolvimento constante, tendo em vista que as tecnologias da informática evoluem constantemente, e também é evidente que cresce as atividades criminosas praticadas com o computador.

> Uma perícia em um computador suspeito envolve uma série de conhecimentos técnicos e a utilização de ferramentas adequadas para a análise, que é justificado pela necessidade indiscutível de não alterar o sistema que está sendo analisado. (SANTOS, 2008, p. 5).

Profissional da Perícia Forense

É necessário que a equipe ou profissional responsável pela perícia forense, tenham conhecimento de várias tecnologias de informática, podemos citar entre elas: Engenharia de Softwares, Banco de dados, Redes de Computadores, Sistemas Distribuídos, Arquitetura de Computadores, Programação, etc.

> O profissional ou equipe de trabalho, deve-se contar com profissionais que conheçam o máximo possível das tecnologias da informática, procurando capacitar-se para o trabalho de investigação, levantamento e preservação das provas materiais. (ELEUTÉRIO E MACHADO, 2010, p. 14).

De acordo com Vargas (2010) o perito para ser um bom profissional, acima de tudo precisa ter uma boa conduta, precisa conhecer os princípios básicos do direito, sigilo, privacidade, e conhecimento profundo nas tecnologias de informática, e também uma noção sobre psicologia dos criminosos, seu comportamento e motivos para realizarem o ataque.

Legislação

De acordo com Queiroz e Vargas (2010) na atualidade no Brasil, não existem leis específicas para os crimes virtuais, o que existem em termos de leis, são as leis que punem com relação da consequência que o crime virtual trás. São utilizados alguns artigos do código civil, Art. 927, 186, 187 e outros.

Segundo Queiroz e Vargas (2010) As legislações vigentes sobre crimes que são cometidos com o computador não possui nenhuma tipificação própria, então os mesmos crimes são tipificados com a legislação de crimes comuns, onde apenas o resultado do crime é caracterizado a um crime comum, então o meio utilizado pelo autor do crime é ignorado no caso quando é utilizado o computador como meio de praticar o delito.

> O aparecimento da Informática no meio social ocorreu deforma tão rápida e passou a exigir, com a mesma rapidez, soluções que o Direito não estava preparado para resolver. Com isso, a necessidade social aparenta estar desprovida da tutela do direito.(SILVA, 2003, p.31).

Evidência Digital

Segundo o dicionário Aurélio Buarque de Holanda (2012) uma evidência é tudo aquilo que pode ser utilizado para provar que determinada afirmação é verdadeira ou falsa. Existem vários tipos de evidências na criminalística.

> A evidência digital abrange os periféricos e dispositivos ligados à cena do crime, onde podemos coletar e averiguar os dados ali contidos seja em um computador ou em um dispositivo móvel. Entretanto, na busca de uma evidência é importante respeitar a autenticidade dos dados, tentando deixa-los exatamente igual ao momento em que foi coletado na cena do crime. Tais fatores auxiliam na documentação da análise forense e geram novas informações na conclusão de uma perícia computacional (LISITA; MOURA; PINTO, 2009, p.23).

De acordo com Lisita, Moura e Pinto (2009) É dito que evidência digital não deixa de ser um tipo de evidência física, embora ela não seja palpável. Este tipo de evidência é formado por campos magnéticos, campos elétricos e pulsos eletrônicos que podem ser coletados e analisados através de técnicas e ferramentas de perícia digital.

Fontes de Evidências

Com o avanço tecnológico hoje existem vários dispositivos de armazenamento além do computador, tais como: pen drives, CD´s, DVD´s, cartões de memória, mp3, mp4, câmeras digitais, celulares, dentre muitos outros. E todos esses dispositivos podem armazenar dados que possam ser evidências de um crime de informática.

De acordo com Adams (2000) existem três tipos de espaços no computador, que podem conter informações para uma investigação:

- Espaço de arquivos lógicos: refere-se aos blocos do disco rígido que, no momento do exame, estão atribuídos a um arquivo ativo ou à estrutura de contabilidade do sistema de arquivos (como as tabelas FAT);
- Espaço subaproveitado: espaço formado por blocos do sistema de arquivos parcialmente usados pelo sistema operacional. São listados nesta categoria todos os tipos de resíduo de arquivos, como a memória RAM;
- Espaço não alocados: qualquer setor não tomado que esteja ou não em uma partição ativa.

Para Neukamp (2007) o sistema de arquivos de um computador possui vários tipos de dados como: binário, textos, Imagens, áudios, e todos eles precisam ser analisados e identificados com relação a sua funcionalidade dentro do sistema investigado. Quando se sabe a atividade praticada pelo suspeito se torna mais fácil achar indícios através de palavras-chave, imagens ou tipos de programas utilizados por tal atividade.

> Além de alterações, exclusão ou até mesmo inclusão de modificações inesperadas em diretórios, arquivos (especialmente aqueles cujo acesso é restrito) podem caracterizar-se como indícios para uma infração. Exemplo: arquivos do tipo doc, txt, imagens, programas executáveis, aplicações instaladas (exe), dentre outras (FREITAS, 2006, p. 73).

Neukamp (2007) afirma que a memória também é um ponto importante na investigação, nela contém os arquivos voláteis do sistema, que são usados pelos programas que estão em funcionamento, ou os arquivos que ainda não foram salvos no disco rígido. É possível recuperar esses dados através de um processo

conhecido com dump de memória, onde é gravado todo o conteúdo da memória para um arquivo de dump. Analisar a memória significa incluir desse a área de transferência de arquivos até memórias de impressoras (buffer).

CRIMES DE INFORMÁTICA

Definição de Crimes de Informática

Hoje com a massificação da informática e da internet, cada vez mais essa ferramentas fazem parte do cotidiano das pessoas. E com esse avanço surgem também novos desafios para a sociedade, com a mesma rapidez que a tecnologia avança os crimes de informática também evoluem de uma forma espantosa.

> Sergio Marcos Roque conceitua crime de informática como sendo "toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material". (ROQUE, 2007, p. 29).

Segundo Roque (2007), conceitua o crime de informática como:
"[...] toda, conduta, definida pela lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração".

Crimes Cometidos com o Apoio de Computadores

Nessa prática criminosa o computador é utilizado como uma ferramenta de apoio para efetuar o crime virtual. Várias práticas criminosas podem ser realizadas com a ajuda do computador tais como: Falsificação de documentos, venda de produtos proibidos como exemplo os entorpecentes, sonegação fiscal, compra de votos em caso de eleições, e vários outros.

> Como qualquer outra ferramenta (agendas, veículos, telefones celulares etc.), o computador é utilizado apenas como elemento auxiliar para a realização de um crime. Por exemplo, se o crime for um assalto a banco, os criminosos poderiam utilizar o computador para armazenar informações, como horários, mapas, nomes dos funcionários. (ELEUTÉRIO E MACHADO, 2011, p. 17)

Segundo Eleutério e Machado (2011) neste caso o computador é a ferramenta fundamental utilizada para o crime, em outras palavras sem o

computador não seria possível a prática criminosa. Essa forma de crime de informática é diferente da forma anterior de prática que vimos, geralmente são delitos que surgem com o mau uso do computador e da internet, por exemplo, ataques a sites da internet, roubos de informações confidencias, programas maliciosos para roubar senhas, chamados “malwares”, vírus, entre outros.

> O computador é utilizado para a realização de um crime. Por exemplo, se o crime for hacker um site, o criminoso utiliza o computador para invadir e acessar o banco de dados da página, modificando ou mesmo deletando o conteúdo. (ELEUTÉRIO E MACHADO, 2011, p. 17)

Locais do Crime

O local de um crime é o lugar, onde ocorreu ou supostamente ocorreu um determinado crime. No local que podem ser encontradas as evidências que são de suma importância e ajudam a levar a solução de um crime, o conhecido termo quem, como e onde,como afirma COSTA (2011, p. 61)“[...] toda área onde tenha ocorrido qualquer fato que reclame as providencias da polícia”.

> Um local de crime de informática nada mais é do que um local de crime convencional, mas acrescido de equipamentos e dispositivos computacionais que podem ter relação com o delito investigado pelos peritos do caso. (ELEUTÉRIO E MACHADO, 2010, p. 25)

Exemplos de Crimes Digitais

- Crimes Contra a Honra

Segundo Crespo (2011) no código penal brasileiro, os crimes contra a honra estão previstos nos artigos 138, 139 e 140, e estes crimes são extremamente comuns na internet, devido a grande quantidade de usuários que a utilizam. Segundo o código penal os crimes contra a honra são: difamação, calúnia e injúria. Geralmente esse crime é cometido em redes sociais, sites e programas de conversa em tempo real como o MSN.

- Pornografia Infantil

Segundo Rosa (2002) Muitas pessoas confundem pedofilia com pornografia infantil, mas cada termo é um crime diferente do outro. A pedofilia é existe a perversão sexual, o adulto tem contato erótico com a criança ou adolescente, já a pornografia infantil, é a comercialização ou distribuição de fotos pornográficas ou eróticas que envolvam crianças e adolescentes, geralmente é utilizado a internet para esse fim.

- Discriminação

De acordo com Rosa (2002) Este crime bastante comum também na internet principalmente depois do surgimento de sites de relacionamento como: Orkut, Facebook, Blogs.

É um crime relacionado com o preconceito de raça, cor, etnia, religião, nacionalidade, etc. Onde através desses sites são criados até comunidades e grupos racistas, onde muitas vezes até marcam encontros para praticar o mal a pessoas que são discriminadas pelos mesmos.

- Fraudes Bancárias

Segundo Crespo (2011) um crime comum, principalmente com usuários dos chamados Internet Banking, versão do banco para a internet. Os criminosos costumam atrais a atenção dos usuários através de phishingscan (e-mail malicioso), que se aberto instala no computador do usuário um software que copia as senhas das vítimas.

- Invasão

De acordo com Salvadori (2011)a invasão se tornou um crime muito comum nos dias atuais, e o seu poder de prejuízo é muito grande. O criminoso chamado de hacker necessita de um alto conhecimento na informática e nas tecnologias digitais,

por meio deste conhecimento ele invade sites ou sistemas governamentais ou empresariais buscando roubar informações ou até mesmo apagar as mesmas.

- Vírus

De acordo com Salvadori (2011) é um programa criado por pessoas mal intencionadas e com grandes habilidades em tecnologias de informática, capaz de causar danos a um computador. Existem várias formas de um computador ser infectado por um vírus, como através de e-mail, de um dispositivo contaminado e conectado a máquina, etc.

Exemplos de Criminosos

- Hackers

São criminosos virtuais conhecidos por invadirem sistemas, praticam este crime simplesmente para desafiar suas próprias habilidades e conhecimentos. Geralmente invadem sistemas e sites do governo, e de grandes empresas privadas buscando demonstrar suas habilidades mesmo que de forma anônima, apenas para satisfazer-se.

> No mundo digital é adotado o termo hacker para descrever o criminoso que atua neste meio, apesar de não haver um consenso entre autores estes são divididos em vários outros termos de acordo com o tipo de crime cometido por eles. (NOGUEIRA, p. 19, 2001).

- Crackers

De acordo com Assunção (2002) são os Hackers antiéticos, agem como os hackers, mas utilizam o seu conhecimento para penetrar através de invasão sistemas e sites do governo ou privados, e assim furtam as informações confidenciais, trazem prejuízos para as empresas, pessoas, e também adulteram dados e informações.

> Esses sim são os maldosos. Com um alto grau de conhecimento e nenhum respeito, invadem sistemas e podem apenas deixar a sua “marca” ou destruí-los completamente. Geralmente são hackers que querem se vingar

> de algum operador, ou adolescentes querem ser aceitos por grupos hacker,e saem apagando tudo que veem ou mestres da programação que são pagos por empresas para fazerem espionagem industrial. (ASSUNÇÃO, p. 6, 2002).

- Phreakers

São hackers que atuam e são especializados em fraudar sistemas de telecomunicação, com o objetivo de fraudar linhas de telefone fixo e celulares para utilizar-se dos benefícios gratuitamente.

> Maníacos por telefonia. Essa é a maneira ideal de descrever os phreakers. Utilizam programas e equipamentos para que possam utilizar telefones gratuitamente. Alguns phreakers brasileiros são tão avançados que têm acesso direto a centrais de telefonia, podendo ligar ou desligar telefones, assim como apagar contas.(ASSUNÇÃO, p. 7, 2002)

- Wannabeés

Segundo Bezerra (2012) é um criminoso que se intitula como Hacker ou Cracker, mas na verdade não possui habilidades necessárias para receber esse título. Utiliza-se de programas prontos criados por hackers para praticar seus crimes, mas não conhece a fundo as práticas que comete.

- Cyberpunks

Segundo Bezerra (2012) utiliza-se de seus conhecimentos em informática para criar vírus de computador com o objetivo de espionar ou sabotar redes de computadores, e também furtar dados da vítima.

- Wizard

De acordo com(2012) é considerado o mestre dos hackers, possui um grande conhecimento e habilidades variadas, mas nem sempre com má-intenção.

- Lameré

Para Bezerra(2012) é o criminoso que não tem tanta experiência e age baseado em informações encontradas na internet e em livros de hackers, com a ajuda dessas ferramentas ele prática suas invasões em redes de computadores e computadores pessoais que possuem uma frágil segurança.

Apesar de existirem várias definições para se tratar dos criminosos virtuais, a mais utilizada para se chamar os mesmos é Hacker como forma de identificá-lo.

ETAPAS DE INVESTIGAÇÃO

Segundo Reis e Geus (2004) a finalidade da Computação Forense é fazer um processo de investigação, com o objetivo de provar algum fato ocorrido com a maior transparência possível. Para que esse processo de investigação ocorra de uma forma correta, é necessário que o perito responsável pela perícia investigativa de determinado crime trabalhe de uma forma bem cuidadosa com todas as evidências encontradas no local do crime, buscando preservar todos os dados obtidos, para que o laudo da perícia possa ser confiável e aceito pela justiça.

> Na fase de planejamento, tem que se definir a melhor abordagem para a investigação, identificando as principais atividades que precisarão ser executadas, de acordo com as informações obtidas preliminarmente, de modo a aproveitar melhor a coleta de dados. Dar início a criação de uma cadeia de custódia, ou seja, um histórico dos passos tomados na investigação, reunindo informações sobre os procedimentos, pessoas envolvidas e evidências recolhidas. (REIS e GEUS, 2004, p. 54).

1 Coleta

Segundo Newkamp (2007) a coleta de evidências é a primeira parte da perícia computacional, e nessa etapa devem ser identificadas, processadas e documentadas as evidências.

> O processo de identificação, processamento e documentação de possíveis provas, ocorre no primeiro passo de uma investigação criminal, ou seja, durante o processo de coleta de evidências, sendo esta, considerada a mais vital das etapas da investigação. Aoextrair o material de análise é necessário que se tome todos os cuidados possíveis para que não haja perda ou alteração de dados, pois isso trará prejuízos para todos os outros passos do processo, especialmente investigações que tiverem fins judiciais. (NEUKAMP, 2007, p. 26).

2 Exame

No processo de perícia computacional a fase de exame é a mais importante e a fase mais trabalhosa para o profissional. Farmes e Venema (2007) aconselham que deva ser realizada uma cópia de todas as informações coletadas na fase de coleta de dados, para não ocorrer alterações no estado original das evidências, preservando a integridade das provas encontradas.

> O ato de extrair, localizar e filtrar somente as informações que possam contribuir, de forma positiva, em uma investigação ocorre na segunda etapa, denominada “exame de evidências”. Considera-se esta, a etapa mais trabalhosa do processo de investigação criminal, principalmente pela quantidade de diferentes tipos de arquivos existentes (áudio, vídeo, imagem, arquivos criptografados, compactados, etc.) que facilitam o uso de esteganografia, o que exige que o perito esteja ainda mais atento e apto a identificar e recuperar esses dados (FARMER; VENEMA, 2007 p. 41).

3 Análise

De acordo com Queiroz e Vargas (2010) a análise tem como objetivo examinar as informações coletadas em busca de evidências, para que no final do processo possa ser formulada a conclusão referente ao crime que originou a investigação. Na análise deve ser investigado todas as fontes de informação, para que seja possível identificar práticas criminosas por parte do suspeito ou suspeitos.

4 Laudo

Segundo Reis e Geus (2004) o último passo da perícia é a elaboração de um laudo onde o perito tem a liberdade de descrever o incidente, pois ele é o único responsável pelo documento e tudo àquilo que for escrito nele. Não existe um modelo padrão para elaboração de laudo, mas sim orientações para sua confecção, e deve ser feito com a maior clareza para que se torne fácil a sua compreensão.

FERRAMENTAS DE COMPUTAÇÃO FORENSE

Segundo Eleutério e Machado (2011) existem muitas ferramentas no mercado criadas especificamente para Perícia Computacional, algumas delas são para uso específico em uma determinada fase da perícia, já outras possuem um

conjunto de ferramentas que podem ser utilizadas em todas as etapas da investigação computacional.

ForensicToolKit

O ForensicToolKit, ou FTK, foi desenvolvido pela AccessData, e neste software podemos encontrar as principais funcionalidades para a realização de exames forenses em dispositivos de armazenamento de dados. Este aplicativo possui uma suíte com vários recursos que podem ser utilizados em todas as fases de um exame computacional forense.

EnCase

O EnCase é produzido pela empresa Guidance, da mesma forma que o FTK ele possui diversos recursos que ajudam o profissional no seu trabalho de exames de pericia em Computação Forense em dispositivos de armazenamento de dados.

SIFT

SIFT- Sigla de SANS *Investigative Forensic Toolkit*, é uma distribuição Linux préconfigurada para investigações forenses. Criado em parte por Rob Lee´s, atualmente está na versão 2.0 e contém todas as ferramentas necessárias para realizar as quatro etapas da investigação coleta, exame, análise e o resultado.

Backtrack

Desenvolvido na Suíça pela empresa Whax e Auditor SegurityCollection, tem como foco testes de segurança e testes de penetração. Possui mais de 300 ferramentas para testes e análise de vulnerabilidade. Muito usado para encontrar furos em sistemas e sites invadidos por criminosos virtuais.

Caine

O software *Computer Aided Investigative Environment* – Caine foi desenvolvido na Itália tem como objetivo criar um ambiente gráfico amigável ao usuário e auxiliar o investigador digital em todas as quatro fases do trabalho de investigação digital. Uma das vantagens do Caine é criar uma cópia semiautomática do relatório final da investigação realizada. Possui versão para Linux e Windows.

PeriBR

Programa brasileiro para investigação computacional, desenvolvido por alunos de pós-graduação em perícia computacional da Universidade Católica de Brasília. Este software foi baseado no FDTK, da mesma forma pode ser usado nas quatro fases de uma investigação digital.

CASOS REAIS

Caso Sharon Guthrie - EUA

Em 1999 Sharon Guthrie de 54 anos residente em Dakota-EUA, morreu afogada em casa na banheira. A autópsia feita no corpo de Guthrie revelou uma substânca chamada Temazepan, que é usado para o tratamento de pessoas com dificuldades do sono. Seu marido pastor Willian Guthrie, foi quem indicou este remédio para a esposa.

O fato de o marido ter indicado o medicamente não era o bastante para acusá-lo do crime. A polícia então contratou um perito em computação científica,chamado Judd Robbins que fez um exame nos computadores usados pelo pastor na igreja.

Depois de alguns dias de investigação, o perito descobriu que o acusado havia pesquisado na internet sites que ensinam como matar uma pessoa de uma forma eficaz e indolor sem deixar vestígios, inclusive com o uso do medicamento Temazepan. O acusado também havia pesquisado por “acidentes em banheira”, “acidentes domésticos”. Essa prova foi de suma importância para que o júri condenasse o Pastor Guthrie pelo crime.

A perícia estuda os fatos que ocorreram no passado, e neste caso o perito teria que descobrir a pergunta: Quando o acusado acessou os sites? Uma pergunta importante para saber se a pesquisa foi feita antes ou depois do crime.

Analisando este caso, pode ser constatado que uma provável técnica usada foi a restauração dos arquivos de backup do registro de navegação web, que a época era usado o Windows 98.(www.imasters.com.br)

Caso Corretor de Imóveis – Brasil

Um profissional da área de corretagem de imóveis foi condenado por homicídio tendo como meio de prova a sua localização no momento do crime.

A estação rádio-base (Erb) de celular, mostrou que o aparelho do corretor estava próximo ao local do crime, no mesmo horário que aconteceu, o que deu-se contrário ao depoimento do mesmo, que afirmou estar em outro local no memento que aconteceu o crime.O sinal foi recebido pela antena, a partir de onde se encontrava o celular, foi realizado o cálculo da localização. A margem de erro nesse cálculo é de no máximo cem metros.

Entretanto, a prova circunstancial apresentada ajudou a influenciar o júri a condená-lo por seis votos a um, pois o rastreamento de celular se enquadra como prova científica desde que seja autorizado pela justiça.

As informações obtidas foram retiradas dos bancos de dados da operadora de telefonia celular e garantidassua autenticidade. (www.imasters.com.br)

CONSIDERAÇÕES FINAIS

O principal objetivo deste trabalho foi elaborar um estudo sobre Computação Forense. Um assunto instigante e novo no meio tecnológico, mas com uma grande perspectiva de crescimento. É uma área que vem se tornando muito utilizada, devido principalmente ao grande aumento nos crimes envolvendo o meio da informação.

Houve uma grande dificuldade para a elaboração deste trabalho acadêmico devido à escassez de literatura e materiais pertinentes a este assunto, principalmente na língua portuguesa. A falta de material deve-se a ser uma área recente. Através deste estudo pode-se constatar que a computação forense tem

muito que desenvolver e inovar. É necessário muito aperfeiçoamento no que se refere a métodos e tecnologias na obtenção das evidencias necessárias para a solução dos crimes de informática.

Por se tratar de uma área recente existe pouca demanda de profissionais capacitados, que realmente são conhecedores dos procedimentos seguidos pela área cientifica forense, além de existirem poucas ferramentas no mercado em hardware e software forense computacional.

Também há necessidade de se atualizar as leis brasileiras para que os crimes de informática possam ser atendidos de uma forma melhor juridicamente falando. A computação forense só tem o que contribuir para a sociedade no que se refere a garantia de direitos e deveres por parte dos cidadãos.

REFERÊNCIAS

ANDRADE,MariaMargaridade.**Introdução do Trabalho Cientifico** .4.ed. SãoPaulo: Atlas, 2003.

ASSUNÇÃO, Marcos Frávio A. **Guia do Hacker Brasileiro**. 1. ed. Florianópolis: Visual Books, 2002.

BEZERRA, Adonel. **Evitando Hackers:** Controle Seus Sistemas Computacionais Antes Que Alguém o Faça! 1. ed.Rio de Janeiro: Ciência Moderna, 2012.

CERVO, Amado Luiz. **Metodologia científica**. 4. Ed. São Paulo: Makron Books, 1996.

COSTA, Marcelo Antonio Sampaio Lemos. **Computação Forense**: A análise forense no contexto da resposta a incidentes computacionais. 3. ed. Campinas: Millenium, 2011.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 2. ed. São Paulo: Saraiva, 2011.

Disponível em http://imasters.com.br/artigo/4656/gerencia-de-ti/casos-reais-crimes-elucidados-com-ajuda-da-ti acessado em 21 de outubro de 2012.

ELEUTÉRIO, Pedro Monteiro da Silva; ACHADO, Marcio Pereira. **Desvendando a Computação Forense**. 1. Ed. São Paulo: Novatec, 2011.

FARMER, Dan e VENEMA, Wietse. **Pericia Forense Computacional** - Teoria e Pratica Aplicada. 1. ed. EUA: Prentice Hall Brasil, 2007.

FREITAS, Andrey Rodrigues de.**Pericia Forense** - Aplicada A Informatica; 1. ed. Rio de Janeiro: Brasport, 2006.

NEUKAMP, Paulo A. **Forense Computacional:** Fundamentos E Desafios Atuais. 11 Junho de 2007. Universidade do Vale do Rio dos Sinos (UNISINOS). 06 Nov. 2007.

NOGUEIRA, José Helano Matos. **A nova face do crime**. Revista Perícia Federal. Ano III nº 9, julho 2001.

QUEIROZ, Claudemir e VARGAS, Raffael; **Investigação e Perícia ForenseComputacional.** 1. ed. Rio de Janeiro:Brazport, 2010.

REIS, Marcelo Abdalla dos, GEUS, Paulo Lúcio de. **Análise Forense de Intrusões em Sistemas Computacionais**: Técnicas, Procedimentos e Ferramentas. Instituto de Computação - Universidade Estadual de Campinas, 2002.

ROQUE, Sérgio Roque. **Criminalidade Informática – Crimes e Criminosos do Computador**. 1 ed. São Paulo: ADPESP Cultural, 2007.

ROSA, Fabrízio. **Crimes de Informática**. Campinas: 2. ed. Campinas: Bookseller, 2002.

SALVADORI, Fausto. **Crimes Virtuais.** Disponível em http://revistagalileu.globo.com/Revista/Common/0,,EMI110316-17778,00-CRIMES+VIRTUAIS.html

SALVADORI, Fausto. **Crimes Virtuais.** Disponível em http://revistagalileu.globo.com/Revista/Common/0,,EMI110316-17778-2,00-CRIMES+VIRTUAIS.html acessado em 23 de outubro de 2012.

SILVA, Rita de Cássia Lopes. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003.

TOCHETTO, Domingos. **Tratado de perícias criminalísticas.** 2. ed. Campinas: Millenium, 2011.

VARGAS, Raffael Gomes.Perícia Forense Computacional Metodologias e Ferramentas Periciais. Revista Evidencia Digital ed. 03, 2004. Disponível em: http://www.guiatecnico.com.br/EvidenciaDigital/ acessado em 11 de setembro de 2012.