# Métodos de Investigação Com Técnicas Forense em Pericia Computacional

Marco Aurélio Monteiro de Lima - marcoaurelio@gmail.com

Governança nas tecnologias da Informação

Instituto de Pós-Graduação - IPOG

Goiânia, Go, 12 de Março de 2015

***Resumo***

*Este artigo apresenta o estudo da informática forense junto com seus métodos investigativo de perícia computacional e a solução de crimes na área de informática. A perícia computacional é uma área que precisa acompanhar o alto crescimento da informática e da tecnologia. A informática forense consiste no uso de métodos científicos para preservação, validação, coleta, identificação, interpretação, análise, documentação e apresentação de evidência digital válida como prova em juízo. A aplicação desses métodos em sua grande maioria não se dá de maneira simples, uma vez que encontrar uma evidência digital pode ser um trabalho muito lento, complexo e cansativo. Com os discos rígidos atingindo a capacidade de TeraBytes de armazenamento, milhões de arquivos podem ser armazenados em um único dispositivo. Logo a utilização de métodos e técnicas de Computação Forense se torna indispensável para encontrar provas e pistas de um crime*. *Estão presentes neste artigo dados sobre procedimentos e características da informática forense, além de informações sobre crimes computacionais, suas vertentes e alguns casos já ocorridos. Ainda avaliar algumas ferramentas disponíveis no mercado, utilizadas por peritos em investigações.*

## *Palavras-Chave: Informática forense e, Evidência, investigação, crimes.*

## 1. Introdução

Segundo a Fundação Getúlio Vargas de São Paulo (FGV-EAESP), em 2013 o Brasil alcançou um total de 136 milhões de computadores em uso por empresas e usuário com uma média de dois computadores para cada três habitantes do país. As pesquisas indicam que em 2016 haverá mais de 200 milhões, sendo um computador por habitantes. Comparando com os anos anteriores, em 2011 havia 78,2 milhões de computadores em uso no país, em 2012 o número chegou a 85 milhões de computadores, o crescimento esta aumentando em uma velocidade assustadora. Com o avanço da informática mais pessoas estão tendo acesso a tecnologia com mais facilidade*,* consequentemente os crimes cometidos ou utilizando a rede mundial de computadores cresce exponencialmente. Neste âmbito, surge a necessidade de um departamento para investigar crimes cibernéticos, criada então a Informática Forense que é a uma área, que complementa a criminalística, cuja seu principal objetivo e determinar a materialidade e autoria de ilícitos referentes à área de informática, tendo como foco principal identificar e processar evidências digitais em provas materiais de crime.   
A informática forense atua utilizando uma série de conceitos de outras subáreas, como, Engenharia de Software, Banco de Dados, Redes de Computadores, Sistemas Distribuídos, Arquitetura e Organização de Computadores, Programação, entre outras, exigindo um alto conhecimento da parte dos investigadores.

## 2. Definição De Computação Forense

## De acordo com o Departamento de Polícia Técnica (DPT), a definição da informática forense seria: "A informática Forense realiza atividades e perícias relativas aos crimes de informática, como fraudes contra a administração pública, rastreamento de ameaças feitas via Internet, pedofilia, invasão de sistemas, quebra de privacidade de dados e outros. Realiza análise em dispositivos de informática em busca de evidências e provas de crimes. Promove ainda, perícia em crimes contra o consumidor no que diz respeito a hardwares e softwares, recuperação de conteúdo em discos rígidos e mídias de backup relacionados com destruição de provas de crimes.

Segundo Eleutério e Machado a informatica Forense é a ciência que utiliza 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 crimes.

De acordo com Eleutério e Machado 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 a Forense Digital é uma área recente de pesquisa, e necessita de desenvolvimento constante, tendo em vista que a informtica tem uma evoluçao constantemente, e também é evidente que cresce as atividades criminosas praticadas com o computador.

Com o intuito de auxiliar os profissionais a identificar sistemas, sites e criminosos digitais foram criados os exames forenses. Onde os principais são: Exames e procedimentos em locais de crime de informática, Exames em dispositivos de armazenamento computacional, Exames em sítios da Internet, Exames em mensagens eletrônicas e Exames em aparelhos eletrônicos móveis. Segundo o IGP de Santa Catarina:

**Exames e procedimentos em locais de crime de informática:**Seu principal objetivo e mapear, identificar e a preservar de maneira adequada os equipamentos computacionais, com o objetivo de filtrar os melhores materiais apreendido na sena de um crime, para posteriormente ser mais bem explorado em laboratório.

**Exames em dispositivos de armazenamento computacional:**São os exames mais periciais mais comuns na informática forense, pois trabalham na análise arquivos, sistemas e programas instalados em discos rígidos. Os dispositivos mais comuns nesse tipo de exame são os discos rígidos, *pen drives*, cartões de memória, disquetes, CDs, DVDs, Blu-Rays, entre outros. Esses exames são feito em quatro etapas (preservação, extração, análise e formalização) utilizando algumas técnicas, como recuperação de arquivos deletados, quebra de senhas e virtualização. Entre os principais crimes relacionados a este tipo de exame estão a pornografia infanto-juvenil, fraude de documentos e sonegação fiscal.

**Exames em sítios da Internet:** Consistem na verificação e cópia de conteúdo existente na Internet, em sites e servidores remotos dos mais variados serviços. Os principais focos das investigações são em conteúdo relacionado à calúnia, pornografia infanto-juvenil e pirataria. Com intuito de verificar o conteúdo e identificar os responsáveis pela publicação das informações contidas no sítio.

**Exames em mensagens eletrônicas (emails): C**orresponde basicamente à análise do responsável pelo envio de uma mensagem de correio eletrônico criminosa, identificando hora, data, endereço IP e outras informações do remetente da mensagem.

Outro exame que é importante citar:

**Exames em aparelhos eletrônicos móveis:** Com objetivo de extrair os dados desses aparelhos, a fim de recuperar e formalizar as informações armazenadas em suas memórias como lista de contatos, ligações, fotos, mensagens de texto, etc.

**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, Programão, etc.

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.

**2.1.** **Evidências**

É importante conhecer os diferentes tipos de categorias de evidência.

**2.1.1. Evidencia real**

É qualquer evidência que fala por si, sem depender de qualquer outra coisa. Em termos eletrônicos, este pode ser um registro produzido por uma função de auditoria, desde que o log pode ser mostrado para ser livres de contaminação.

**2.1.2. Evidencia testemunhal**

É qualquer evidência fornecida por uma testemunha. Este tipo de evidência é sujeito à confiabilidade percebida da testemunha, mas enquanto uma testemunha é, prova testemunhal confiável considerada pode ser útil e quase tão poderoso como evidencia real. Depoimentos escritos por um testemunho pode ser considerado testemunho, enquanto o autor está disposto a afirmar que a escreveu.·.

**2.1.3. Evidência digital**

São informações armazenada, transmitida ou criada digitalmente possibilitando seu uso em um processo judicial, esse tipo de evidência pode estar dividido em vários tipos como em fotos, vídeo, áudio, arquivos de texto, e-mail, *Website* e etc.

**2.1.2. Requisitos de uma evidencia.**

Para uma evidencia ser valida ela tem que cumprir uma serie de requisitos legais. Podemos destacar cinco como os principais requisitos para uma evidencia ser útil.

**2.1.2.1. Admissível**

Esta é a regra mais básica, a prova deve ser capaz de ser usado em um tribunal ou em outro local. O não cumprimento desta regra é equivalente a não cobrança da prova em primeiro lugar, exceto o custo é mais elevado.

**2.1.2.2 Autêntica**

Se você não pode ligar as evidencias de forma positiva a uma cena de crime, não é possível usar como prova em um tribunal. É prescindível que a evidência relaciona-se com o incidente de forma relevante.

**2.1.2.3. Completa**

Não é o suficiente para coletar evidências de que apenas mostra uma perspectiva do incidente. Apenas a coletar de evidencias que prove as ações do suspeito, mas para ser completo, também é necessário considerar e avaliar todas as evidências disponíveis para os investigadores e reter o que pode contradizer ou não, diminuir a confiabilidade da outras potenciais provas incriminatórias realizada sobre o suspeito. Da mesma forma, é vital para coletar evidência de que elimina suspeitos. Por exemplo, se você pode mostrar que o suspeito estava logado no momento do incidente, você também precisa mostrar quem mais estava logado e demonstrar por que eles não fizeram isso. Isto é chamados elementos de defesa e é uma parte importante para provar uma evidencia.

**2.1.2.4. Confiável**

Os procedimentos de coleta e análise de provas não deve pôr em causa a autenticidade e veracidade da prova.

**2.1.2.5. Crível ou acreditável**

A evidência apresentada deve ser clara e de fácil entender crível por um júri. Não há motivo de apresentar um dump binário de processo de memória se o júri não tem ideia do que isso significa. Da mesma forma, se for apresentado uma versão formatada de fácil entendimento por um júri mostrando a relação com o binário original. Caso contrário, não há nenhuma maneira para o júri identificar a veracidade da evidencia.

## 2.3. Legislação

Ate o ano de 2012 o Brasil não tinha uma lei especifica para informática, a lei 12.737 de 2012, a chamada lei “Carolina Dieckmann” Sancionada em dezembro de 2012, a alteração do Código Penal foi apelidada com o nome da atriz, após fotos em que Carolina Dieckmann aparecia nua terem sido divulgadas na internet.

A nova legislação caracteriza como crime pontos importante da segurança digital, como a invasão de dispositivos (smartphones, PCs, e tablets). Com a nova Lei, quem interromper provedores ou derrubar sites, invadir “dispositivos informáticos”, enviar cavalos de tróia ou acionarem webcams remotamente podem ser enquadrados na nova lei, com uma pena especifica para cada crime cometido que pode ser de três meses a dois anos, a pena pode ser aumentada se resulta prejuízo econômico e se informações confidenciais ou intimas forem divulgadas.

**2.4** **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 informätica também evoluem de uma forma espantosa.

Segundo Roque (2007, p. 25), crime de informática é toda, conduta, definida pela lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material.Nessa prática criminosa o computador é usado como ferramenta de apoio para efetuar o crime virtual. Várias práticas criminosas podem ser realizadas com a ajuda do computador tais como: Falsificaçaoo de documentos, venda de produtos proibidos como exemplo os entorpecentes, sonegação fiscal, compra de votos em caso de eleições, e vários outros.

Segundo Eleutãrio 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.

**2.4.1 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 soluções de um crime, o conhecido termo quem, como e onde, como afirma (KEHDY p. 68) toda área onde tenha ocorrido qualquer fato que reclame as providencias da polícia.

## 3. Ferramentas

O propósito de técnicas forenses aplicadas à mídia digital, é simplesmente para ajudar a prender e processar os autores de um evento e têm carga de testes adequados, resultando em uma condenação, ou, no caso contrário , exonerar os inocentes. Para fazer isso, o pesquisador tem diferentes ferramentas que simplificam a tarefa, devemos ter em mente a grande quantidade de dados para analisar é desafiador, portanto, em geral, depende do interesse, determinação e capacidade do sucesso processo de investigação. O que pode ser conseguido através de computação forense?

* Recuperação de arquivos ocultos, apagados ou corrompidos
* Identificação das rotas, modificações e autoria de documentos e dados
* O acesso a informações protegida ou criptografada, password revelado
* Follow-up transferências de arquivos, e-mails, sessões de bate-papo, as comunicações de rede (internet) e VoIP
* A identificação da origem e destino. Os arquivos de rastreamento A computação em nuvem
* Posicionamento e história de dispositivos de GPS dotado
* Atividade de auditoria em computadores e dispositivos eletrônicos.
* Os testes de penetração e sistema de certificação e segurança de rede
* Estudo de vírus, cavalos de Tróia ... Back Orifice, rootkits. Engenharia Reversa

Para o perito criminal exercer a essa difícil tarefa de encontrar as evidências digitais existe uma série de ferramentas e equipamentos quem foram desenvolvidas. As mais utilizadas são:

**3.1. *Forensic ToolKit***

O *Forensic ToolKit (FTK)* é um conjunto de ferramentas desenvolvida para a investigação forense. Com uma interface intuitiva, ele faz análise de e-mail, exibições de dados personalizáveis e estabilidade, FTK ampliou seu quadro de expansão, com uma gama de funcionalidades.

Com a ferramenta é fácil criar imagens, analisar o registro, conduzir uma investigação, decodificar os arquivos, recuperar senhas de arquivos criptografados, identificar esteganografia e construir relatórios, também recupera senhas, utilizar CPUs ociosos na rede para decriptar arquivos e executar ataques de dicionário. Ela enumera todos os processos em execução, inclusive ocultos por rootkits, e exibe as DLLs associadas. O FTK faz busca seqüencial de memória, permitindo identificar hits na memória e automaticamente os mapeie de volta para um determinado processo.

A ferramenta apresenta outras funcionalidades como a utilização web para conexão com BD, compartilhamento de casos, além das demonstradas, mas este artigo visa apresentar uma nova ferramenta que em breve estarei utilizando.

**3.2. EnCase**

De acordo com Jennifer Higdon, porta-voz para Guidance Software, fabricante de EnCase, o EnCase é uma ferramenta desenvolvida em C++ que oferece um conjunto de ferramenta para informática forense, antes da sua criação eram necessárias um conjunto de ate 15 ferramentas para proporcionar as mesmas funcionalidades. Segundo Raffael Vargas as principais características do EnCase são:

**Processador de Evidência**: Este módulo novo agiliza a capacidade de resposta do caso e a disponibilidade de informações, o que era um problema em casos com tamanho maior. O processador de novas evidências prepara um caso através da realização de tarefas de processamento de chave, tais como a criação de um índice, a análise de hash, a análise de assinaturas, a análise de arquivo protegido, internet e processamento de e-mail, e pesquisando palavras-chave. Além disso, o processador evidencia tem acesso aos novos recursos a seguir:

* Análise do arquivo protegido alimentado por Passware: Este módulo utiliza o Analisador de Criptografia Passware para identificar arquivos criptografados e protegidos por senha.
* Parser Sistema de Informação: Detecta automaticamente o sistema operacional Windows ou Linux em um dispositivo de hardware e extratos de usuários, software e outras informações do sistema valiosos para os utilizadores a rever.
* Suporte para o Windows 7 e artefatos do sistema de arquivos EXT4 incluída.
* Parser de Artefato: Um único módulo que permite analisar de forma abrangente para os arquivos da Lixeira e arquivos de Link, e para analisar o log de transações MFT.
* IM Parser: Localiza e analisa conversas de AOL, MSN, Yahoo! e bate-papo registros no sistema.
* Parsers Event Log: Para Windows, Linux, Unix e sistemas, estes analisadores localizar logs de eventos e informações de login.

**Apresentação de e-mail**: E-mail agora exibe de forma semelhante aos programas familiares como o Microsoft Outlook ou Lotus Notes. Além disso, inclui e-mail EnCase conversas threading e afins, permitindo a revisão das cadeias de conversa.

**Maior escalabilidade com o cache eficiente**: Estruturas compostas do sistema de arquivos, e-mail e outros estão agora armazenadas em cache no disco, reduzindo o tempo e os recursos de sistema necessários para revisar os dados que já foram processados. Isso permite que a escala em toda EnCase grandes conjuntos de dados.

**Relatórios completamente personalizáveis:** Novo sistema de notificação, permite definir todos os aspectos do relatório, incluindo cabeçalhos, rodapés, conteúdo personalizado e formatação. Você também pode criar relatórios de dados de evidência, editar os templates, ou construir relatórios personalizados.

**Aquisição de dados de Smartphone/Tablet integrado:** Os usuários podem agora adquirir dados de smartphones e tablets, como o iPhone, iPad, BlackBerry e dispositivos Android, diretamente do EnCase Forense.

Módulo Suporte incluído: Todos os usuários agora têm acesso EnCase para as seguintes ferramentas:

* EnCase Decryption Suíte, incluindo suporte atualizado para Check Disk Encryption ponto cheio.
* Sistema de Arquivo Virtual
* Emulator de disco físico
* Bloqueador FastBloc SE

**3.3. WinHex**

Conforme o site X-Ways software technology AG. Ter todos os bits do seu computador para alcançar tornou-se uma realidade. WinHex é um editor hexadecimal universal, e também, possivelmente, o mais poderoso utilitário de sistema já criado. Apropriado para a computação forense , recuperação de arquivos , conhecimentos de informática, processamento de dados de segurança de baixo nível. Suas características incluem:

* Disk Editor para FAT12 / 16/32, exFAT, NTFS, ext2 / 3/4, Next3 ®, CDFS, UDF
* Interpretação Built-in de sistemas RAID e discos dinâmicos
* Várias técnicas de recuperação de dados
* Editor da RAM , uma maneira de editar RAM e memória virtual de outros processos
* Intérprete de dados, sabendo 20 tipos de dados
* Estruturas de dados edição utilizando templates
* Concatenar, cortar, juntar, analisar e comparar arquivos
* Funções de busca particularmente flexível e substituir
* Clonagem de disco , com licenciado especialista também em DOS
* Fotos e backups de disco (opcionalmente comprimido ou dividido em 650 arquivos MB)
* Interface de programação (API) e os scripts
* Criptografia AES, checksums, CRC32, resenhas de 256 bits (MD5, SHA-1, ...)
* Apagamento irreversível de dados confidenciais / privado
* Importe todos os formatos da área de transferência
* Conversão formatos: binário, ASCII Hex, Intel Hex, e Motorola S
* Conjunto de caracteres: ANSI ASCII, IBM ASCII, EBCDIC
* Salto instantâneo entre janelas
* Vasta documentação

**3.4. Smartwhois**

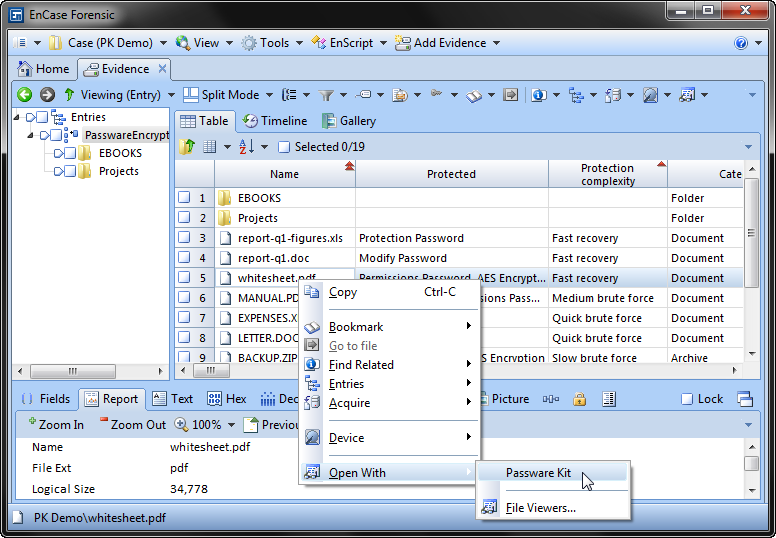
Desenvolvida pela Tamasoft, empresa especializada em segurança de informação, a ferramenta *SmartWhois* auxilia na verificação de IPs e de domínios na Internet. Basta digitar o IP ou domínio que a ferramenta exibe na tela a localização da empresa, o endereço, telefone e o nome do responsável pelo registro do IP ou domínio pesquisado.

O *SmartWhois* e muto utilizado para investigar correspondecias eletronicas que omite as informações do remetente, digitando o ip do servidor a ferramenta busca todos os dados para identificar a origem.

Alem de software existem também equipamentos forenses desenvolvidos para auxiliar na preservação e obtenção das provas, como bloqueadores de escrita de discos e duplicadores forenses, como o Talon, Dossier e Solo 4 (Equipamentos que faz a clonagem de disco rígidos sem o uso de computadores), garantindo a preservação do disco rígido original. Um sistema bastante avançado denominado F.R.E.D, sigla para Forensic Recovery Evidency Device, (www.digitalintelligence.com)tem sido amplamente utilizado. O FRED é uma plataforma modular para aquisição forense, em alta velocidade, de discos IDE, SATA e SCSI. Contando com bloqueadores de escrita e baias onde podem ser conectados os discos rígidos a serem examinados. Uma vez conectados, os discos são copiados com proteção de escrita, de forma a manter a integridade dos dados ali armazenados. A cópia é então analisada com o uso dos softwares acima citados.



Figura 1 - Forensic ToolKit.   
Fonte - http://www.berghel.net/col-edit/digital\_village/aug-06/dv\_8-06

  
Figura 2 – Tela do Software EnCase.  
Fonte- http://www.lostpassword.com/encase

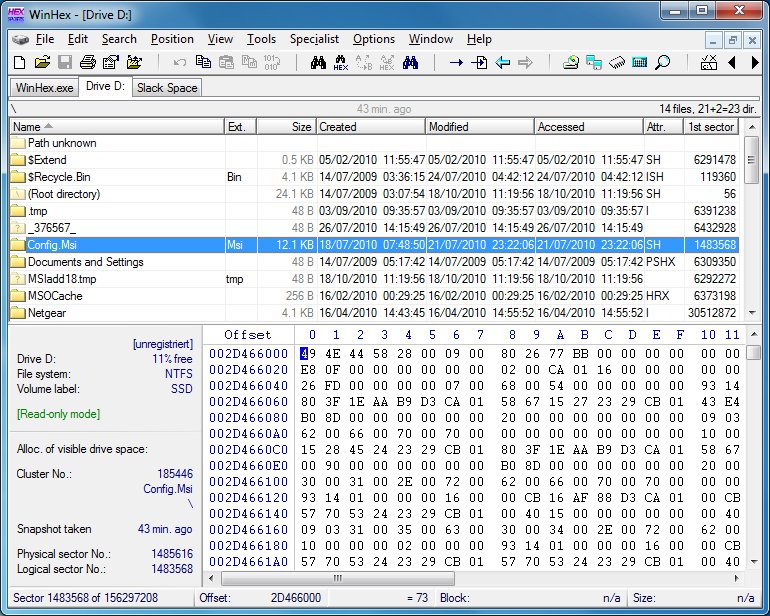
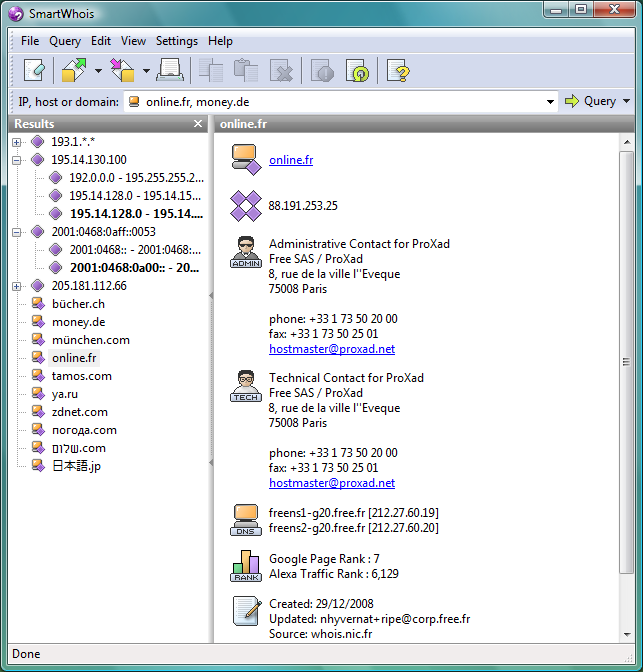


Figura 3 - Tela do WinHex.   
Fonte - http://www.downloadcrew.com/article/14760-winhex



Figura 4 - Talon, Dossier e Solo 4.  
 Fonte- Própria

  
Figura 5 – Tela do Smartwhois.   
Fonte - http://www.tamos.com/products/smartwhois/

## 4. Casos Reais

**4.1. O caso Carolina Dieckmann**

De acordocom o site g1.com.br em 2012, 36 fotos de Carolina Dieckmann nua foram divulgadas na internet. Segundo as investigações quatro pessoas foram detidas como suspeitos de terem roubado as fotos íntimas do computador de Carolina Dieckmann. O primeiro suspeito encontrado foi Diego Fernando Cruz, de 25 anos, que teria sido o primeiro a divulgar as fotos na internet, os outros três rapazes estão entre os suspeitos. Um deles é menor de idade e teria sido o autor das ligações para chantagear a atriz, com o pedido de R$ 10 mil para que as fotos não fossem publicadas.

Um grupo especializado da Delegacia de Repressão aos Crimes de Informática (DRCI) da Polícia Civil do Rio usou programas de contra-espionagem para chegar aos suspeitos. De acordo com a investigação, o roubo teria começado com um e-mail usado como isca (spam), que ao ser aberto liberou uma porta para a instalação de um programa que permitiu aos hackers entrarem no computador da atriz.

**4.2. Um dos primeiros casos de Computação Forense**

De acordo com Thiago S. Mosqueiro em 1988 Sally Weiner, casado com Harry Weiner, é sequestrada e liga a mando do sequestrador para negociar o resgate. Seu marido entrou em contato com a polícia local e o FBI, que tomaram controle do caso. Eles já sabiam de antemão que o telefonema foi, na verdade, uma reprodução de uma fita gravada algum tempo antes. No telefonema, Sally mandou Harry pegar uma bolsa, que deveria estar próxima ao carro dele, contendo informações que ele deveria seguir à risca. Esta bolsa deveria ser entregue com o dinheiro do resgate. Na bolsa, havia um bilhete com instruções impressas.

Harry foi ao local combinado, junto com um policial. Ficaram no local por algunas horas,como os sequestradores nao apareceram. Harry e os policiais voltaram para casa. No dia seguinte, um grupo da FBI realizou uma busca pelo local onde o resgate deveria ocorrer e encontraram, um segundo bilhete. Este segundo bilhete direcionaria Harry por um caminho até um terceiro bilhete, que o mandaria até uma igreja abandonada não muito longe dali. Na igreja, cessavam as pistas.

Dois dias após o contato, um domingo, o corpo de Sally foi encontrado. Os investigadores concluiram que os sequestrador não procurava simplesmente por dinheiro.

O principal suspeito era Copenhefer dono de uma loja ao lado do banco onde Harry trabalhava, pois os padrões dos bilhetes usado pelo sequestrador eram muito parecido com os anucios na vitrine da loja.

Com tudo as provas encontradas foram todas circunstanciais, O especialista Al Johnson e sua equipe passaram a procurar, manualmente, por fragmentos de algum arquivo que pudesse ajudar no caso. Um disco com capacidade de 20Mb a equipe levou 33 dias para analisar por completo. Mas ao final, eles encontraram pedaços de um documento muito oportuno, nome do arquivo era The Plan (o plano). Era um documento em que Copenhefer escrevera tudo o que planejava fazer, inclusive o que deveria ter ocorrido na noite do resgate. Assim como suspeitavam os policiais e o FBI, Sally já estaria morta antes mesmo do resgate e toda aquela brincadeira dos bilhetes era uma armadilha para tentar assasinar também Harry Weiner. Por fim, conseguiram ainda encontrar um motivo para o assassinato: um empréstimo negado a Copenhefer por Harry.

**4.3. Caso Sharon Guthrie - EUA**

Em maio de 1999 o corpo de Sharon Guthrie, de 54 anos,e encontrado na banheira de sua casa em Dakota, EUA. A autópsia revelou que Sharon morreu afogada, e tambem foi encontrada em seu corpo vestigios de Temazepan, uma droga usada para auxiliar o sono. Seu marido, o pastor Willian Guthrie, foi quem indicou o medicamento a sua esposa.

O fato de Willian ter arientado a esposa usar o temazepan nao era prova suficiente para o encrimina-lo, com isso, Judd Robbins foi contratado pela policia para examinar os computadores utilizados pelo pastor na igreja.

Após alguns dias de análise, foi descoberto que o acusado tinha pesquisado na internet sites que explicavam como matar de forma eficaz e indolor incluindo o uso do Temazepan. Repetidas consultas como “acidentes na banheira” e “acidentes domésticos” também foram identificadas no histórico do computador usado por Guthrie. Esse fato foi essencial para o júri considerar Willian Guthrie como culpado

## 5. Conclusão

O principal objetivo deste artigo foi elaborar um estudo sobre Informática Forense. Um assunto novo no meio tecnológico, mas com uma grande potencial de crescimento, uma área que vem se tornando muito utilizada, devido ao grande avanço da tecnologia. Nos últimos anos os crimes relacionados com informática se espalham rapidamente, muitas empresas têm sido alvos de ataque com grande prejuízo financeiro, bem como sua imagem denegrida. Com o aumento nos crimes cibernéticos o mercado corporativo busca por segurança, focando na prevenção, controle e diagnóstico, de situações como por exemplo: crackers, vírus, fraudes internet, e-mail abusivo, pedofilia entre outros, somando tudo com novas tecnologias e insatisfação pessoal, gera novas entradas de acesso aos sistemas computacionais, lógicos ou físicos.

Devido à grande procura o mercado de perícia em sistemas computacionais caminha para um grande crescimento nos próximos anos, não somente combatendo ameaças externas e internas, mas criando um ambiente e mecanismo de prevenção, ou seja, ter toda uma estrutura corporativa totalmente proativa antecipando e identificando possíveis falhas. Com isso é possível avaliar as fraquezas para uma melhor resposta a incidentes, bem como para auditoria a sistemas computacionais, não sendo aqui, de forma alguma esgotado o processo de aprendizagem e de estudo de métodos e procedimentos para se atingir os objetivos de forma cada vez mais eficaz.

Antigamente a solução de crimes era obtida através de impressões digitais, relatórios de toxicologia, análise de rastro, documentos em papel e outros meios tradicionais. Levando em consideração que ainda hoje essas provas são essenciais para a resolução de muitos crimes, a tecnologia adicionou outro nível com a evidência digital. Constantemente mais informações podem ser adquiridas com a análise de um computador que o de uma impressão digital. A história inteira de um crime pode ser desvendada com a recuperação de um arquivo que pensaram ter sido apagado.

## 6.Referências

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. Desvendando a Computação Forense. São Paulo: Novatec Editora, Jan/2011 (ISBN: 978-85-7522-260-7).

Eoghan Casey-Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Disponivel em http://goo.gl/P4pOiv Acessado em 01/2015

FREITAS, Andrey Rodrigues de.Pericia Forense - Aplicada A Informatica; 1. ed. Rio

de Janeiro: Brasport, 2006.

Globo. Suspeitos do roubo das fotos de Carolina Dieckmann são descobertos. Disponível em http://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html acessado em 12/2014

Instituto De Criminalística De Santa Catarina - Informática Forense. Disponível em http://www.igp.sc.gov.br/index.php?option=com\_content&view=article&id=112&Itemid=128. Acessado em 02/2015

Instituto de Criminalística Do Paraná (ICPR)- Informática Forense Disponível em http://www.ic.pr.gov.br/modules/conteudo/conteudo.php?conteudo=27 Acessado em 11/2014

KEHDY, Carlos. Munição. **Elementos de Criminalística**. 3. ed., São Paulo: Sugestões Literárias, 1968.

Matthew Braid - Collecting Electronic Evidence After a System Compromise. Disponível em https://www.auscert.org.au/download.html?f=22 acessado em 02/2015

Raffael Vargas. Conhecendo o EnCase Forensic v7. Disponivel em http://imasters.com.br/artigo/21358/gerencia-de-ti/conhecendo-o-encase-forensic-v7/ Acessado em 11/2014

Rômulo Lachi-Exceções À Inadmissibilidade Das Provas Ilícitas No Processo Penal Brasileiro. Disnponivel em http://www.unigran.br/revista\_juridica/ed\_anteriores/22/artigos/artigo07.pdf acessado em 01/2015

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

Thiago S. Mosqueiro. Um dos primeiros casos de Computação Forense .Disponivel em http://legauss.blogspot.com.br/2009/01/um-dos-primeiros-casos-de-computao.html acessado em 12/2014

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 02/2015.

Warren G. Kruse II , Jay G. Heiser. *Computer Forensics: Incident Response Essentials.* Editora Addison Wesley. Edição: 1 ( ISBN-10: 0201707195*)*

X-Ways software technology AG, WinHex: Computer Forensics & Data Recovery Software,

Hex Editor & Disk Editor. Disponivel em [http://www.x-ways.net/winhex/index-m.html. acessado em 01/2015](http://www.x-ways.net/winhex/index-m.html.%20acessado%20em%2001/2015).