Faculdade de Tecnologia de Americana

Curso Superior de Tecnologia em Segurança da Informação

PERÍCIA FORENSE COMPUTACIONAL

Adriana Aparecida Muniz da Costa

Americana, SP

2012

Faculdade de Tecnologia de Americana

Curso Superior de Tecnologia em Segurança da Informação

PERÍCIA FORENSE COMPUTACIONAL

ADRIANA APARECIDA MUNIZ DA COSTA

muniz.dry@gmail.com

Trabalho de Conclusão de Curso apresentado à Banca Examinadora, como exigência parcial para obtenção de título de Graduação do Curso de Segurança da Informação, da Faculdade de Tecnologia de Americana, sob a orientação do Prof. Rogério Nunes Freitas.

Americana, SP

2012

FICHA CATALOGRÁFICA elaborada pela

BIBLIOTECA – FATEC Americana – CEETPS

C87p	Costa, Adriana Aparecida Muniz da Perícia forense computacional. / Adriana Aparecida Muniz da Costa. – Americana: 2012. 48f. Monografia (Graduação em Análise de Sistemas e Tecnologia da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza. Orientador: Prof. Rogério Nunes de Freitas 1.Segurança em sistemas de informação 2. Direito de informática I. Freitas, Rogério Nunes de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana. CDU: 681.518.5 34:681.3

Bibliotecária responsável Ana Valquiria Niaradi – CRB-8 região 6203

Americana - São Paulo - Brasil

JUNHO 2012

BANCA EXAMINADORA

_____

Rogério Nunes de Freitas

_____

Carlos Henrique Sarro

_____

José William Pinto Gomes

AGRADECIMENTOS

Agradeço a Deus, a quem devo minha vida, por me guiar e sempre estar ao meu lado e nunca me deixar desistir mesmo sabendo que a jornada seria difícil, pela oportunidade de estudar e concluir o ensino superior.

Agradeço aos meus pais por todas as lições ensinadas durante a minha vida, pelo apoio e incentivo no início e decorrer do curso.

Ao meu esposo pela paciência e por me dar força nos meus momentos de cansaço. Aos professores que contribuíram com meu aprendizado.

Agradeço ao Professor Rogério Nunes de Freitas pelo auxílio, paciência, empenho e profissionalismo durante as orientações.

Em especial a minha amiga Regina de Sousa Braz pela dedicação e apoio na construção deste trabalho.

A todos que, direta ou indiretamente, contribuíram para a realização deste trabalho.

DEDICATÓRIA

Dedico este trabalho as pessoas que me incentivaram, mostrando que com fé, conseguimos realizar todos os nossos objetivos.

Aos meus amigos e meus pais que me apoiaram durante essa jornada.

Ao meu esposo por me compreender nos momentos de ausência. A todos que estão na busca pelo conhecimento buscando crescer profissionalmente e adquirir conhecimento.

EPÍGRAFE

“A felicidade não está na partida e nem na chegada, mas na travessia”.

Guimarães Rosa

RESUMO

A seguinte apresentação conceitua segurança da informação, o que é crime digital, a perícia forense computacional, bem como suas vantagens, seu crescimento ao longo do tempo, também será abordado o trabalho de um perito forense, como este profissional busca as provas e evidências para desvendar crimes quando se tratado de crimes cibernéticos e auxiliado pelas questões tecnológicas, quais os requisitos que o mesmo precisa ter para a realização deste trabalho. Também serão mostradas algumas ferramentas utilizadas por profissionais para desvendar os crimes cibernéticos. Serão apresentadas algumas leis nesse aspecto.

Palavras Chave: Segurança da informação, perícia forense e Evidências digitais.

ABSTRACT

The following presentation is about the concept of information security, what is a digital crime, the forensic expertise on computers, its advantages and growning, a forensic specialist, how this professional searches for clues and evidences to find a solution for a cybercrime and helped by tecnology and what are the exigency to do this job. We will present you some tools used by professionals to find solutions for the cybercrimes. Some laws will be presented to you too.

Keywords: Information Security, forensic, Digital Evidence.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1. INTRODUÇÃO

“A desconfiança é a mãe da segurança.”
Madeleine Scudéry

Os computadores estão cada vez mais presentes em nosso cotidiano, com isso a tecnologia está crescendo de forma extremamente extensa. As pessoas se tornaram “escravas” da mesma, deixando, muitas vezes de sair de casa, pois muitas de suas necessidades são superadas nas próprias residências pelo fato de utilizarem desta tecnologia. Nós usamos o computador para pagar contas, comprar produtos e serviços e também como forma de entretenimento, “[...] milhões de cidadãos comuns atualmente estão usando as redes para executar operações bancárias, fazer compras e arquivar sua devolução de impostos, a segurança das redes está despontando no horizonte como um problema potencial”, (TANENBAUM, 2003). Com o crescimento tecnológico também cresce, infelizmente, os índices criminais, pois muitas pessoas utilizam os computadores e as redes para cometer crimes, o chamado crime digital que será discutido no terceiro capítulo. “Fazer compras pela internet, por exemplo, pode ser um desafio, visto que o mundo virtual permite uma série de golpes e os problemas são frequentes”, (Oficina da net, 2012).

O aumento da criminalidade não ocorre apenas por questões éticas e psicológicas do criminoso e tampouco pelo crescimento urbano, mas sim porque os infratores da lei estão muito bem informados e equipados com relação a questões tecnológicas e algumas vezes estes até fazem parte dos profissionais da área de segurança da informação e com isto sabem como, quando e porque agir e quais são as fraquezas de alguns sistemas tecnológicos.

A falta de softwares específicos, que fornecem, ou deveriam fornecer segurança da informação ajudam no rompimento da proteção que as empresas e os usuários em geral deveriam ter das suas informações. Além da falta desses softwares há também a fragilidade e facilidade de encontrar um meio de destruir a sua proteção, tornando esses softwares inúteis para a proteção dos dados que são roubados pela rede, dados como senhas, número de contas, cartões e outras informações sigilosas. Também devemos analisar que vários criminosos utilizam

recursos de criptografia como métodos anti-forense com o objetivo de retardar e até mesmo impedir a investigação de um equipamento.

Para conseguir o acesso a informações sigilosas de usuários de computadores e rede, o fraudador utiliza-se de programas e também algumas ferramentas com código malicioso que são instaladas nos computadores das vítimas, que reflete o elo mais fraco numa transação financeira online.

Entretanto a tecnologia, embora utilizada por fraudadores para encontrar os pontos fracos de sistemas e roubar o que lhes interessam, ou muitas vezes, apenas destruir o que acham não ter serventia para si causando um caos na vida dos verdadeiros donos dessa informação, auxilia em estudos criminalísticos, o que chamamos de *Pericia Forense Computacional.*

O objetivo principal deste trabalho é mostrar a relação que a perícia possui com a área de segurança da informação, os crimes que muitas pessoas cometem por desrespeitar as leis, o conhecimento necessário para atuar como perito criminal, a seriedade do trabalho deste profissional e ainda algumas ferramentas utilizadas no trabalho pericial.

No segundo capítulo será apresentada uma pequena introdução sobre segurança da informação, definição de ameaças, vulnerabilidades e riscos que podem colocar a segurança das empresas e também de usuários domésticos em perigo.

O terceiro capítulo é dedicado a definir crimes digitais, seu crescimento e alguns exemplos de infrações cometidas através do uso da internet. O quarto e quinto capítulo são inteiramente destinados à montagem teórica que engloba toda a contextualização e definição do tema perícia forense computacional, bem como a legislação utilizada para tratar dos casos envolvendo crimes digitais.

O sexto capítulo é destinado à apresentação de algumas ferramentas que são utilizadas por peritos para localizar arquivos destruídos para que os responsáveis pelos crimes sejam punidos. Por fim o último capítulo é destinado à conclusão obtida ao final da construção do trabalho.

2. SEGURANÇA DA INFORMAÇÃO

“A segurança é semelhante a uma corrente: sua resistência será igual à resistência de seu elo mais frágil.”

Edson Fontes

“A informação, independente do seu formato, é um dos maiores patrimônios de uma organização moderna, sendo vital para quaisquer níveis hierárquicos e dentro de qualquer instituição que deseja manter-se competitiva no mercado”, (MOREIRA, 2008). Em consequência disto, ela deve estar bem protegida, principalmente porque as empresas estão cada vez mais conectadas por redes e muitos recursos são utilizados online.

Fontes (2006) define segurança da informação como uma corrente formada por vários elos. A robustez desse processo será igual à resistência de seu elo mais frágil.

Figura 1 - Elo mais fraco (PEIXOTO, 2006).

A segurança da informação é um assunto que vem crescendo muito nos últimos tempos, seguindo o ritmo do crescimento referente à tecnologia, pois segurança da informação e tecnologia são assuntos que devem ser abordados em conjunto, especialmente quando a tecnologia é utilizada para romper com a segurança de muitos programas e usar informações pessoais ou de empresas para um crescimento ilegal.

De acordo com Sêmola (2003), segurança da informação pode ser definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

A segurança da informação é uma ferramenta essencial quando falamos de crescimento de negócios dentro de uma organização, visto que os dados sigilosos devem ser protegidos de forma que garanta o futuro promissor da empresa. Entretanto, é comum ouvirmos que muitas empresas ainda acham desnecessários os gastos ocasionados pela prevenção da perda dos dados, porém o número de empresas que pensam desta forma está diminuindo muito por já terem passado por momentos difíceis ao perderem dados que deveriam estar guardados a sete chaves ou por conhecerem alguém que passou por isso.

Há ainda aquelas que pensam que a necessidade de cuidar da informação deve partir apenas do departamento de Tecnologia da Informação (TI). Outro fator que contribui com a perda de informações é a falta de capacitação e conhecimento dos profissionais da empresa em relação ao tema.

Segundo Fontes (2006), na seção introdutória de sua obra, "Segurança da informação: o usuário faz a diferença", o tema segurança da informação tem se tornado cada vez mais conhecido na medida em que:

- As organizações possuem suas informações processadas e armazenadas no ambiente computacional;
- As organizações dependem do ambiente computacional para realizarem seus negócios; e
- O acesso à informação no ambiente computacional está disponível a todos os colaboradores da organização.

Para garantir a segurança da informação é necessário um conjunto de fatores que devem incluir políticas e procedimentos a serem tomados em caso de problemas com a informação, estes procedimentos podem ser encontrados no plano de contingência se a empresa possui-lo. “Divulgar as responsabilidades dos usuários é uma tarefa que as organizações têm executado por meio de campanhas internas, palestras ou de literatura [...]”, (FONTES, 2006).

É importante salientar que estes fatores devem ser implementados, monitorados, analisados criticamente e sempre que necessário, alterados visando a melhoria que garanta os objetivos da empresa.

2.1. Ameaças

Ameaça pode ser definida como alguma violação em um sistema ou informação.

Uma definição mais abrangente; ameaças são: “Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perda de confidencialidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização”, (SEMOLA, 2003). Portanto, vulnerabilidades não causam problemas à segurança, elas representam o meio para o causador dos problemas.

As ameaças à rede de computadores ou a um sistema podem vir de agentes maliciosos, os chamados crackers, entretanto, não são apenas estes que ameaçam a nossa rede, muitas vezes as ameaças podem surgir dos próprios usuários e funcionários da empresa; empregados demitidos, muitas vezes provocam ataques aos sistemas computacionais da empresa como forma de vingança; “Os registros policiais mostram que a maioria dos ataques não é perpetrada por estranhos que grampeiam uma linha telefônica, mas por pessoas ressentidas com a organização a que pertencem”, (TANENBAUM, 2003).

Segundo a (ABNT NBR ISO/IEC 17799, 2005), em sua seção introdutória “As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação”.

No parágrafo anterior são citados alguns tipos de ameaças segundo a ABNT, entretanto algumas delas e outras podem ser consideradas crimes como veremos no capítulo III Crimes digitais, sua definição.

Algumas das principais ameaças às redes de computadores são:

- Destruição de Informação ou de outros recursos;
- Modificação ou deturpação da informação;
- Roubo, remoção ou perda de informação ou outros recursos;
- Revelação de informação;
- Interrupção de serviços.

Muitos dos problemas relacionados à segurança de redes são causados, intencionalmente, por pessoas maliciosas que têm o objetivo de conseguir vantagens para si ou para outrem. Alguns invasores estão listados na Tabela 1:

Tabela 1 - Algumas pessoas que podem causar problemas de segurança e os motivos para fazê-lo (TANENBAUM, 2003).

Adversário	**Objetivo**
Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas
Cracker	Testar o sistema de segurança de alguém; roubar dados
Representante de vendas	Tentar representar toda a Europa e não apenas Andorra
Executivo	Descobrir a estratégia de marketing do concorrente
Ex-funcionário	Vingar-se por ter sido demitido
Contador	Desviar dinheiro de uma empresa
Corretor de valores	Negar uma promessa feita a um cliente através de uma mensagem de correio eletrônico
Vigarista	Roubar número de cartões de crédito e vendê-los
Espião	Descobrir segredos militares ou de um inimigo
Terrorista	Roubar segredos de armas bacteriológicas

As ameaças podem ainda ser intencionais ou acidentais. Ameaças acidentais são aquelas onde não houve a intenção, ou seja, não foram premeditadas, já as ameaças intencionais são aquelas que são premeditadas, onde houve a intenção de violar a segurança da informação para conseguir vantagem para si ou outrem.

2.2. Vulnerabilidades

Todo ativo de uma organização está sujeito a alguma vulnerabilidades, podendo esta ser em maior ou menor escala.

“Nenhuma área ou instalação de T.I. será cem por cento invulneráveis a fatores naturais ou ações feitas pela mão do homem [...] os processos e sistemas de informações podem apresentar vulnerabilidades que, se exploradas, poderão comprometer a segurança”, (FERREIRA; ARAÚJO, 2008, p. 189).

> ***Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. (MITNICK; SIMON, 2003, p. 3).***

Para Sêmola (2003), as vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou condição favorável, que são as ameaças.

“Quando grandes quantidades de dados são armazenados sob formato eletrônico, ficam vulneráveis a muito mais tipos de ameaças do que quando estão em formato manual”, (LAUDON, 2004).

Nas empresas, a maioria das informações é armazenada em computadores, isso torna seus dados muito mais vulneráveis.

2.3. Riscos

“O risco é apenas uma forma de representar a probabilidade de algo acontecer. Trata-se de uma possibilidade. Portanto, pode ocorrer ou não”, (DAWEL, 2005).

“A constante avaliação de riscos de T.I. e de ativos críticos de informação na organização irá permitir uma evolução constante e um aprimoramento em termos de controles mais eficazes, inteligentes, com custos adequados e alinhados ao apetite de riscos da empresa”, (FERREIRA; ARAÚJO, 2008, p. 195).

Para evitar os riscos que as empresas estão expostas é necessário fazer uma análise de riscos, esta deve conter os incidentes e falhas de segurança, bem como a possibilidade dos mesmos ocorrerem, e quais seriam os impactos e perdas caso esses incidentes ocorram. Esta análise possibilita a aplicação de controladores nos pontos com maior probabilidade de riscos e que necessitam de investimento em segurança.

> ***Os resultados dessa avaliação ajudarão a direcionar e determinar ações gerenciais e prioridades mais adequadas para um gerenciamento dos riscos de segurança da informação e a selecionar os controles a serem implementados para a proteção contra estes riscos. Pode ser necessário que o processo de avaliação de riscos e seleção de controles seja executado um determinado número de vezes para proteger as diferentes partes da organização ou sistemas de informação isolados. (FOCO SECURITY, 2006).***

"O objetivo da segurança da informação é aprender a lidar e conviver com o risco e não eliminá-lo completamente, o que na maioria das vezes é impossível." (DAWEL, 2005).

A Tabela 2 indica a preocupação que as organizações possuem em relação às ameaças, bem como a prioridade de cada uma delas.

Tabela 2 - Quadro indicando a prioridade de ameaças e riscos para a organização. (adaptado (FONTES, 2011)).

Administração do risco	
Organizações=>	**Prioridade**
Roubo de informações por concorrente desleal ou por criminosos que podem vender esta informação	1
Vazamento de informação por erro, descuido/negligência	2
Contingência que indisponibiliza o ambiente de tecnologia.	3
Invasão do ambiente de tecnologia por criminosos externos	4
Vírus e demais códigos maliciosos	5
Incapacidade de responder questionamento da justiça sobre uso e guarda da informação	6
Fraude realizada por usuário interno	7
Falha em sistema aplicativo	8

Segundo pesquisa realizada por Fontes em 2011 com empresas de diversos setores e como mostrado na tabela acima, o roubo é a ameaça que mais preocupa as organizações, pois ele afeta diretamente os objetivos de negócio da empresa.

"Em segundo lugar está a preocupação com o sigilo das informações, nenhuma empresa quer que seus dados sejam acessados por pessoas não autorizadas e de má fé. Já em ultimo lugar ficou a falha em sistema aplicativo, o que

indica que a proteção técnica é considerada mais eficiente do que as proteções contra ações de erro e má fé das pessoas.” (FONTES, 2011).

Quando falamos em segurança da informação logo vêm em mente os fatores abaixo:

- Confidencialidade: quando a informação só está disponível para aqueles devidamente autorizados;
- Disponibilidade: os recursos e serviços do sistema devem estar disponíveis sempre que necessário;
- Integridade: diz-se quando a informação não é destruída ou corrompida.

3. CRIME DIGITAL

“Nossa segurança está em risco quando a parede de nosso vizinho está em chamas.”
Horácio

Neste capítulo será apresentado a definição de crimes digitais, alguns tipos desses crimes e como eles vêm crescendo nos últimos anos.

Para entendermos melhor a forense computacional é importante pensarmos o que é realmente um crime cibernético, o que leva a ocorrê-lo e suas consequências, pois se tratando de segurança da informação e quando envolvem redes de computadores tudo gira em torno do tal crime cibernético.

“Com o aumento do uso da tecnologia, se tornou comum possuirmos um grande número de informações em formato eletrônico, com isso surgiu o interesse dos criminosos que tem conhecimento de que informação é poder, desta forma nasceram os crimes eletrônicos ou crimes cibernéticos”, (TAVARES PERÍCIAS, 2012). Os ataques cibernéticos ocorrem por falhas nas redes de computadores. Esses ataques tem sido a maior preocupação dos analistas de todo o mundo, pois não ocorrem somente no Brasil, mas no mundo inteiro.

“Vários países, já estão atentos à segurança cibernética. Nos Estados Unidos, o presidente Barack Obama lançou recentemente o prospecto Cybersecurity com várias medidas prioritárias, incluindo a criação de um comando Cibernético nas Forças Armadas americanas”, (REVISTA BRASILEIRA DE INTELIGÊNCIA, 2011).

Complementando a guerra cibernética é um conjunto de ações utilizadas por um indivíduo ou grupo de indivíduos que usam os computadores ou rede de computadores para criar uma guerra no ciberespaço, retirando de operação serviços importante como a internet, energia e outros ou simplesmente para propagarem pragas por diversão, pelo simples fato de serem reconhecidos ou para roubo de informações. Com a informatização mundial os crimes realizados de próprio punho estão sendo substituídos pelo crime cibernético, pois este se torna menos arriscado para o criminoso.

Através de dados obtidos pelo Centro de Atendimento a Incidentes de Segurança (CAIS) é possível perceber o aumento da quantidade de incidentes de segurança no decorrer de anos, e também no decorrer de meses como apresentado na Figura 2 e Figura 3:

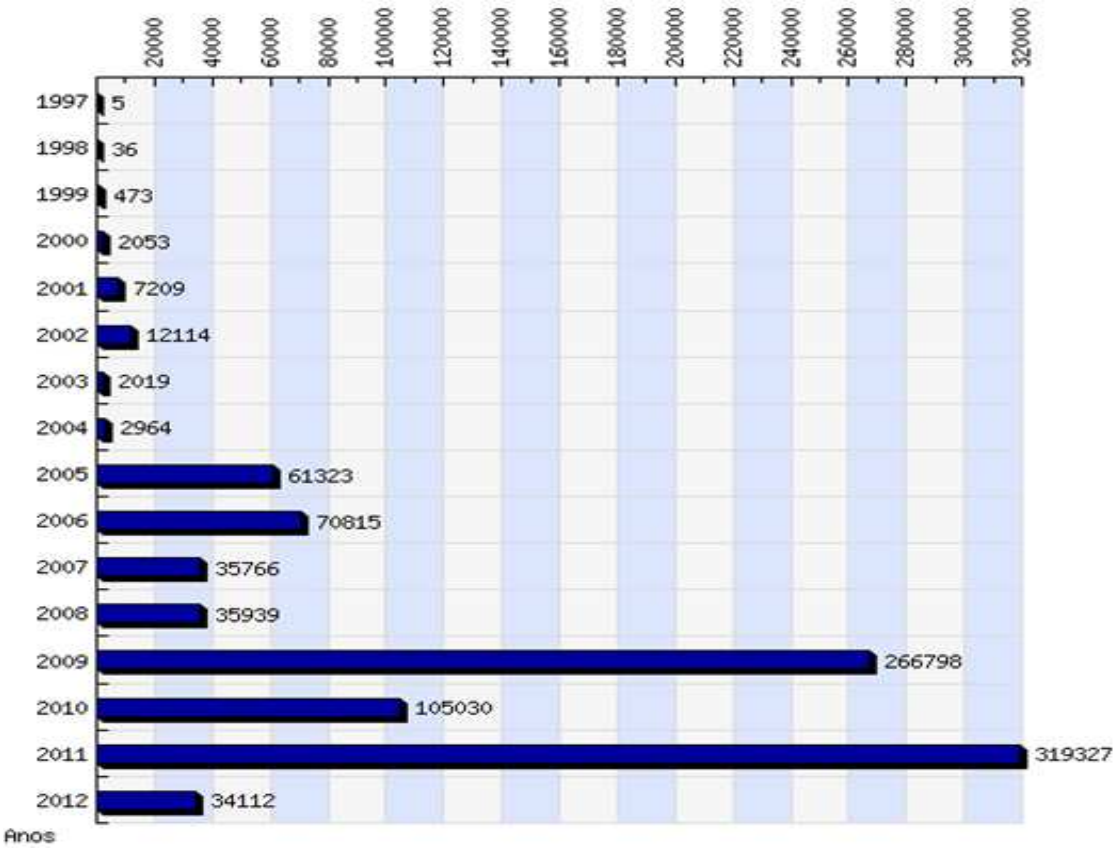

Figura 2 - Número de incidentes por ano registrado pelo CAIS (RNP, 2012).

O gráfico mostra um aumento relevante no ano de 2011 comparado ao de 2010. Já em 2012, apesar de estarmos no primeiro semestre, o índice é maior que o índice referente a 2010 e se fizermos uma média é bem semelhante ao ano de 2011. Entretanto, não podemos confiar apenas nas estatísticas apresentadas visto que muitos dados não são reportados. Com os índices aumentando há a necessidade de mais profissionais na área de forense para desvendar tantos crimes de informática, o que infelizmente não tem por diversos motivos como profissionais não qualificados.

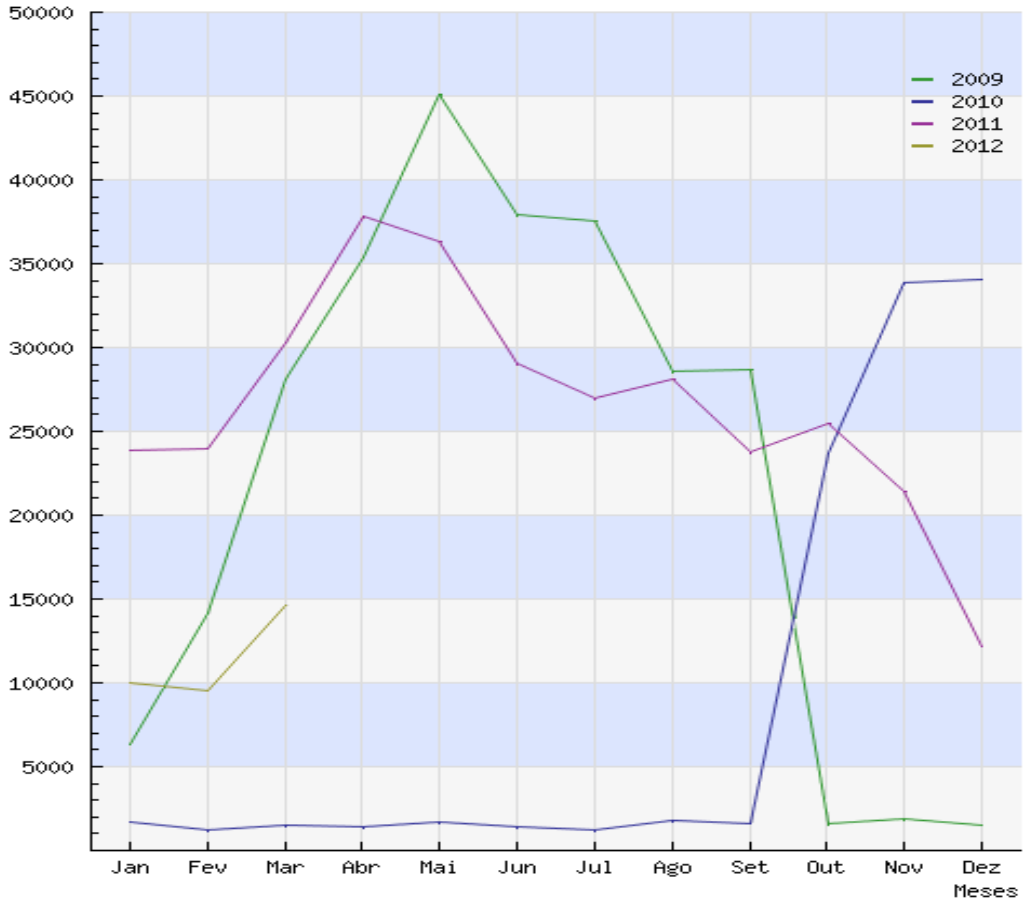

Figura 3 - Número de incidentes por mês registrado pelo cais (RNP, 2012).

Além dos crimes cibernéticos estarem crescendo de forma desordenada também está crescendo a habilidade e conhecimento de criminosos que a cada dia deixam menos rastros dificultando o trabalho do perito.

Quando falamos em crimes digitais, pensamos em alguns tipos de crimes como a pedofilia, criação e disseminação de vírus, fraude, porém a qualificação desse tipo de crime vai muito mais além; desde atitudes que achamos ser mais inocente como comentários maldosos por email, o envio de mensagens falsas a roubo de senhas e invasão de sistemas que também podem ser caracterizados como delitos digitais. Isso mostra que muitas pessoas podem cometer delitos sem se aperceberem disso, ou seja, podem mandar emails com comentários maldosos ou mensagens falsas.

São muitos os tipos de crimes digitais que encontramos, entre eles, roubo, chantagem, difamação, calúnia, a distribuição de material obsceno, transgressão de propriedade intelectual, disseminação de vírus, pedofilia, extorsão, fraudes

financeiras, grampo, falsificação de documentos, pirataria digital, violações aos Direitos Humanos fundamentais, enfim são inúmeros os crimes que são praticados com o uso das redes de computadores, esses crimes estão crescendo cada vez mais. Veja na Tabela 3 algumas infrações realizadas, através da internet:

Tabela 3 - Infrações puníveis pelos termos da Lei (FERREIRA; ARAÚJO, 2008, p. 156).

Infrações puníveis pelos termos da Lei		
Encaminhar para várias pessoas mensagens contendo um boato eletrônico	Difamação	Artigo 139 do Código Penal
Enviar uma mensagem para terceiros com informação considerada confidencial	Divulgação de segredo	Artigo 153 do Código Penal
Enviar um vírus que comprometa equipamento ou conteúdo de terceiros	Dano	Artigo 163 do Código Penal
Copiar um conteúdo e não mencionar a fonte, baixar arquivos de mídia (MP3, MPEG, entre outros) que não possua controle de direitos autorais	Violação ao direito autoral	Artigo 184 do Código Penal
Enviar mensagem de correio eletrônico com remetente falso (spam)	Falsa identidade	Artigo 307 do Código Penal
Fazer cadastro com nome ou informações falsas em páginas diversas na internet	Inserção de dados falsos em sistemas de informações	Artigo 313-A do Código Penal
Entrar em rede corporativa e alterar informações (mesmo que com uso de um software) sem autorização prévia	Adulterar dados em sistemas de informações	Artigo 313-B do Código Penal
Participar de jogos de azar via internet (exemplo Cassino online)	Jogo de azar	Artigo 50 da Lei de Contravenções Penais
Ver ou enviar fotos de crianças e menores de 18 anos nus, através da internet	Pedofilia	Artigo 247 da Lei 8.069/90 “Estatuto da Criança e do Adolescente”

Usar logomarca de empresa em mensagem de correio eletrônico, documentos, propostas ou contratos sem autorização do titular, no todo ou em parte, ou imitá-la de modo que possa induzir a confusão.	Crime contra a propriedade industrial	Artigo 195 da Lei 9.279/96
Uso de mecanismos (softwares ou ferramentas diversas) para coleta de informações sem autorização prévia	Interceptação de comunicações de informática	Artigo 10 da Lei 9.296/96
Usar cópia de software sem ter a licença para tanto	Crimes contra Software “Pirataria”	Artigo 12 da Lei 9.609/98

A Tabela aponta apenas alguns crimes que são mais ocorridos com o uso da internet, todavia existem inúmeros outros que são cometidos em qualquer lugar do mundo.

4. FORENSE COMPUTACIONAL

“Em forense Digital, a excelência não é uma opção, é uma necessidade operacional.”

Raffael Vargas

No presente Capítulo, serão apresentadas algumas características pertinentes à forense computacional. Também serão apresentados conceitos que tenham relação com a forense, o Trabalho do perito e a vantagem de ser um perito.

Forense Computacional é um ramo relativamente novo que está se desenvolvendo pelo fato da necessidade de atuar no combate aos crimes eletrônicos. “É a aplicação de conhecimentos em informática e técnicas de investigação com a finalidade de obtenção de evidências”, (FREITAS, 2006). A forense computacional refere-se aos métodos para análise, preservação, documentação e obtenção de provas para reuni-las e reconstruir o cenário no momento do delito para que assim o mesmo possa ser solucionado. Foi criada com o objetivo de suprir as necessidades das instituições legais no que se refere à manipulação das novas formas de evidências eletrônicas. “Na criminalística a Computação Forense trata o incidente computacional na esfera penal, determinando causas, meios, autoria e consequências”, (PAULA, 2012).

A forense computacional usa métodos científicos para reconstruir as ações que são usadas em cyber crimes, para então poder chegar a uma decisão judicial. Como já foi dito no parágrafo acima, a forense computacional é um ramo novo, entretanto ela é recente quando falamos no seu envolvimento tecnológico, pois há algum tempo já são observáveis muitos casos de aplicação de métodos científicos para fins de comprovação de fraudes e reconstrução de evento. Segundo Eckert (1997 apud BUENO 2007, p 23), foi a partir da segunda metade do século XIX que a ciência foi primeiramente empregada para auxiliar o avanço de investigações legais.

Ao começar a usar a ciência para solucionar os crimes as autoridades legais obtiveram maior validade nos resultados de uma investigação forense. Então houve a necessidade de criar uma técnica igualmente eficiente no que tange a tecnologia, então desenvolveu-se a perícia forense computacional. Dentro do conceito Forense encontramos os termos “local de crime e vestígios” que serão explicados a seguir.

4.1. Local de crime

Local de crime é caracterizado como qualquer local onde haja vestígios relacionados ao delito. O local de crime não é, necessariamente, um local físico, podendo o mesmo ser um local remoto como nos casos dos crimes digitais. Entretanto os procedimentos de preservação do local são os mesmos, ou seja, garantir à integridade de ambas as evidências, evidências físicas e digitais. Componentes, como teclado, mouse, armazenamento removível mídia e outros itens podem ter evidência física, assim como impressões digitais, DNA etc. Todas as evidências devem ser preservadas, ou seja, garantir que não sejam comprometidas durante documentação.

Antes de iniciar uma perícia é interessante fotografar o ambiente e o dispositivo que será periciado para que, posteriormente, possa ser comprovado como o objeto foi encontrado. “Um exemplo cabível é a captura e perícia de máquinas ligadas, pois, nesse caso, o ambiente em questão que deve ser fotografado são as telas do computador [...]”, (QUEIROZ; VARGAS, 2010, p. 46).

Figura 4 - Local de crime (BEZERRA; LUCAS, 2010, p. 11).

4.2. Vestígios

Vestígio é tudo o que for encontrado na cena do crime que possa ter relação com o que venha a ser investigado, desde objetos até pequenas marcas deixadas no local, ou seja, são elementos que após ter sido estudado por peritos possam vir a se transformar em provas. “Só depois de examinar adequadamente saberemos se o vestígio está ou não relacionado ao evento periciado.” (SENASP/MJ, 2012).

> ***Onde quer que ele (autor) ande, o que quer que ele toque ou deixe, até mesmo inconscientemente, servirá como testemunho silencioso contra ele. Não impressões papilares e de calçados somente, mas, seus cabelos, as fibras das suas roupas, os vidros que ele quebre, as marcas de ferramentas que ele produza, o sangue ou sêmen que ele deposite. Todos estes e outros transformam-se em testemunhas contra ele. Isto porque evidências físicas não podem estar equivocadas, não perjuram contra si mesma. (SENASP/MJ, 2009).***

Hildebrand no trecho acima reforça o dito popular de que não há crime perfeito. Mesmo se houver tentativas de despistar o perito com o uso de pistas falsas ou ocultação de provas sempre haverá brechas deixadas pelo autor e que nas mãos de profissionais altamente qualificados se tornarão provas para desvendar o crime.

Figura 5 - HD dentro de saco de evidência (GALVÃO, 2009).

4.3. Fases de uma investigação Forense

Na investigação criminal é preciso tomar cuidado com os resultados obtidos após uma perícia, pois laudos que não forem feitos cuidadosamente poderão acarretar problemas para pessoas inocentes. Portanto, os peritos seguem rigorosamente as leis e há necessidade de seguir cronogramas com algumas fases que não podem ser deixadas para trás. Abaixo segue as fases que devem ser seguidas visando um resultado positivo.

- Coleta de dados: Os dados são coletados para uma futura avaliação, esta coleta deve sempre preservar a integridade dos dados. “As evidências precisam ser preservadas de tal forma que não haja dúvida alguma de sua veracidade", (FREITAS, 2006). Posteriormente os equipamentos são identificados. Computadores Pessoais, Notebooks, CDs e DVDs, Cartões de memória Pen-drives, Máquinas fotográficas, Celulares, etc, podem ser identificados como possíveis fontes de dados em uma investigação forense. Depois de identificados, eles devem ser devidamente embalados e etiquetados. Um computador é coletado como um tipo de evidência física durante a fase de investigação da cena do crime físico;
- Exame dos dados: nessa fase são utilizadas algumas ferramentas apropriadas para cada tipo de dado. Porém é utilizada apenas uma amostra da evidência afim de não destruir a prova de um crime;
- Análise das informações: nessa etapa serão analisadas as amostras dos dados encontrados na fase anterior;
- Interpretação dos resultados: é a ultima fase, porém não a menos importante, pois é gerado um relatório com todas as partes anteriores descritas minuciosamente e ao fim deve conter os resultados obtidos através das fases. Os Laudos devem conter:
  - Finalidade da Investigação;
  - Autor (es) do Laudo (peritos envolvidos);
  - Resumo do caso/incidente;
  - Relação de evidências analisadas e seus detalhes;
  - Conclusão;
  - Anexos;

- Glossário.

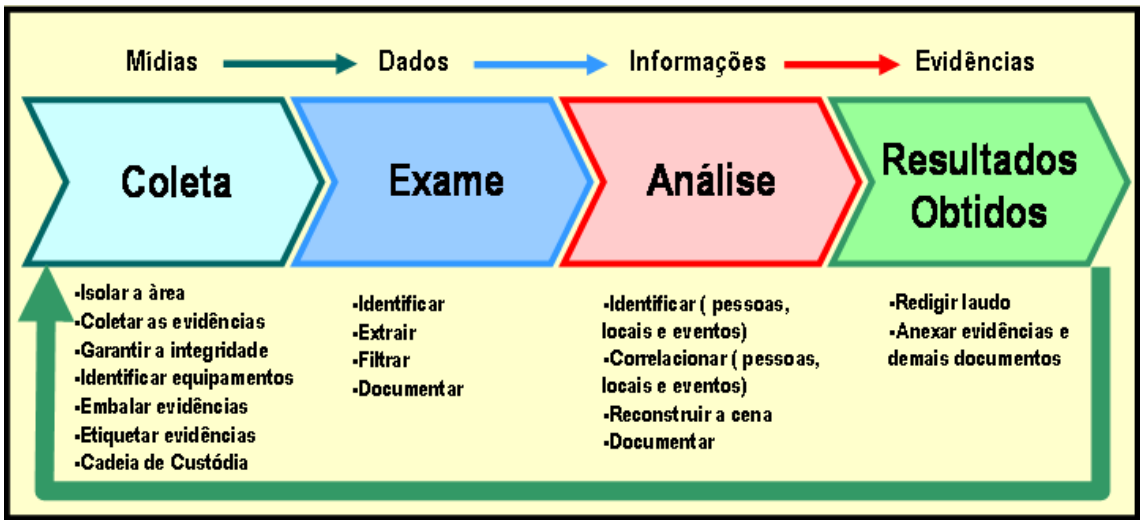

Figura 6 - Ciclo da Investigação Computacional Forense (Forense Computacional: Processo de Investigação, 2012).

Para a aquisição dos dados, o perito deve utilizar um processo composto por três etapas:

1. Identificar a ordem em que os dados devem ser coletados.

Os dados devem ser coletados seguindo a ordem de volatilidade, pois se o sistema for desligado essas informações serão perdidas. Assim sendo, o perito deve coletar imediatamente esse tipo de dados.

A Tabela 4 apresenta a expectativa de vida de alguns dados:

Tabela 4 - O ciclo de vida esperado dos dados (FARMER; VENEMA, 2007, p. 6).

Tipos de dados	**Tempo de vida**
Registradores, memória periférica, cachês etc.	Nanossegundos
Memória principal	Dez nanossegundos
Estado da rede	Milissegundos
Processos em execução	Segundos
Discos	Minutos
Disquetes, mídia de backup etc.	Anos
CD-ROMs, impressões etc.	Dezenas de anos

2. Copiar os dados: “A análise forense de um sistema envolve um ciclo de coleta de dados e processamento das informações coletadas. Quanto mais precisos e completos os dados, melhor e mais abrangente a avaliação pode ser. Os dados originais permanecem protegidos em um estado puro; qualquer analise deve ser realizada em uma cópia dos dados do computador”, (FARMER; VENEMA, 2007, p. 5).

3. Garantir e preservar a integridade dos dados: o perito deve garantir que aqueles dados que já foram coletados sejam preservados, pois do contrário eles poderão ser invalidados perante a justiça.

4.4. Perito

Identificar autores de crimes, muitas das vezes pela internet através de algumas evidências é um trabalho difícil que visa grande desempenho e profissionalismo. Essa dificuldade se dá pelo fato de que as evidências estão ocultas na rede mundial de computadores, onde de qualquer lugar do mundo, podem ser acessadas e a qualquer momento.

O perito é um profissional que deve ser muito bem treinado, especializado em encontrar evidências, ou seja, as provas técnicas ou periciais dos crimes para esclarecimento do mesmo em determinado processo judicial. Para isso, o profissional deve estar capacitado para atuar com competência, pois é um serviço que exige muita técnica e responsabilidade. Os peritos não devem invadir sistemas para analisar dados sem ordem judicial, pois invasão de privacidade também é crime. “O perito forense computacional se enquadra em uma pessoa que tem no seu perfil profissional as características necessárias para dar respostas à justiça enquanto observador e perscrutador de fatos e ações criminosas reais e/ou virtuais que podem levar à descrição e identificação referente a vítimas ou ao criminoso, tendo em mente tão somente a solução dos casos em que estejam envolvidos e para os quais tenham sido solicitados”, (QUEIROZ; VARGAS, 2010, p. 9).

A função do perito, de modo geral é estudar o corpo ou objeto envolvido no delito. Para isso ele refaz os mecanismos do crime utilizando os objetos e evidências encontradas no local do delito. Faz exames laboratoriais utilizando uma pequena quantidade de amostra das evidências, para não destruir as provas que poderão ser pedidas futuramente.

O perito pode atuar em diversas áreas, entre elas a de informática. O perito responsável em solucionar problemas com relação à tecnologia, ou seja, todo tipo de crime correlacionado a informática como roubo no meio eletrônico, quebra de senhas e de sigilo eletrônico lidam com pessoas de todo o tipo que sabem o que estão fazendo e não costumam deixar rastros.

Segundo (QUEIROZ; VARGAS, 2010, p. 15), a obrigação do perito computacional forense é entender a sua importância no processo de resolução e desencadeamento de respostas para os mais tipos de crimes que envolvam a informática. Dentre muitas de suas funções, ele avalia e determina se as empresas estão ou não utilizando softwares legais no desenvolvimento de sistemas eletrônicos, atua na resolução de crimes envolvendo pedofilia, espionagem, além de produzir laudos de crimes como roubo, fraude e extorsão envolvendo o uso da rede de computadores.

É importante destacar que, independentemente da área de atuação o perito é responsável em partes para que a decisão judicial seja válida e fundamentada nas provas encontradas no local do crime.

Ele deve conseguir comprovar a autenticidade dos resultados obtidos em determinada análise forense, caso contrário o processo pode ser contestado durante sua aplicação em um processo criminal.

A área de perícia forense é uma área recente, por isso não existem muitos profissionais experientes atuando no mercado. Certificações são mais difíceis ainda de se encontrar. Além do conhecimento, o perito deve apresentar comprovação em currículo, tanto de títulos em universidades quanto em conhecimentos prévios adquiridos por meio de experiência no mercado de trabalho.

4.5. Vantagens de ser um perito

Como foi dito acima as certificações na área de perícia forense são difíceis de encontrar, entretanto não é impossível, o que torna o profissional dessa área que possua o conhecimento adequado e certificações um grande profissional e com verdadeiras oportunidades para uma ascensão profissional.

Quem desejar atuar como perito em computação forense deve ter experiência em áreas especificas como redes, segurança da informação e direito, ele deve ter

conhecimento entre muitas outras coisas, nos artigos descritos no Código de Processo Penal.

O perito presta serviços para a Justiça justamente porque é uma pessoa honrada, isso lhe dá muitas vantagens como possuir fé pública. Além de a profissão ser dinâmica, pois, todos os dias, a todo o momento, ocorrem novos tipos de crimes e são necessárias novas técnicas para desvendá-los. A área de perícia, principalmente no que diz respeito à informática é uma área com grande expansão e poucos profissionais qualificados, ou seja, com certeza não faltarão boas oportunidades para os profissionais que decidirem se especializar no assunto para os próximos anos.

De acordo com (Queiroz; Vargas, 2010, p. 12) abaixo estão alguns dos requisitos para o perfil profissional de um perito:

- Formação superior em tecnologia e domínio tecnológico;
- Possuir especialização;
- Possuir grande interesse pela área de perícia forense digital;
- Conhecimento das leis que envolvam crimes praticados com o auxilio da internet e do computador;
- Ser proficiente em língua estrangeira, especialmente o inglês;
- Conhecimento sobre os termos da linguagem do direito.

5. LEGISLAÇÃO

"O dever de um perito é dizer a verdade; no entanto, para isso é necessário: primeiro saber encontrá-la e, depois querer dizê-la. O primeiro é um problema científico, o segundo é um problema moral."

Nerio Rojas

Neste capítulo, serão apresentadas as leis que rodeiam a perícia forense computacional, pois o perito deve atuar sempre ao resguardo dessas leis.

Embora ainda não haja leis específicas sobre os crimes digitais, são aplicadas as leis existentes que podem ser também interpretadas para o meio digital. Abaixo encontram-se algumas leis que podem ser utilizadas para punir os criminosos digitais.

5.1. CÓDIGO PROCESSUAL CIVIL – CPC

Seção II

Do Perito

Art. 145. Quando a prova do fato depender de conhecimento técnico ou científico, o juiz será assistido por perito, segundo o disposto no art. 421.

§ 1º Os peritos serão escolhidos entre profissionais de nível universitário, devidamente inscritos no órgão de classe competente, respeitado o disposto no Capítulo Vl, seção Vll, deste Código. *(Parágrafo acrescentado pela Lei nº 7.270, de 10.12.1984).*

§ 2º Os peritos comprovarão sua especialidade na matéria sobre que deverão opinar, mediante certidão do órgão profissional em que estiverem inscritos. *(Parágrafo acrescentado pela Lei nº 7.270, de 10.12.1984).*

§ 3º Nas localidades onde não houver profissionais qualificados que preencham os requisitos dos parágrafos anteriores, a indicação dos peritos será de livre escolha do juiz. *(Parágrafo acrescentado pela Lei nº 7.270, de 10.12.1984)*.

5.2. CÓDIGO PENAL

INDUZIMENTO, INSTIGAÇÃO OU AUXÍLIO A SUICÍDIO.

Art. 122 - Induzir ou instigar alguém a suicidar-se ou prestar-lhe auxílio para que o faça.

Pena - reclusão, de 2 (dois) a 6 (seis) anos, se o suicídio se consuma; ou reclusão, de 1 (um) a 3 (três) anos, se da tentativa de suicídio resulta lesão corporal de natureza grave.

Exemplo: falar num chat, blog ou comunidade que alguém deve se matar ou sugerir como fazê-lo. (PONTOLDIO, ROSSI, 2010).

CALÚNIA

Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime.

Pena - detenção, de 6 (seis) meses a 2 (dois) anos, e multa.

Exemplo: afirmar em chat que alguém cometeu algum crime. (PONTOLDIO, ROSSI, 2010).

DIFAMAÇÃO

Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação.

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Exemplo: Infração: encaminhar um boato eletrônico para várias pessoas. (PONTOLDIO, ROSSI, 2010).

INJÚRIA

Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.

Exemplo: enviar e-mail para alguém, xingando-a (gorda, feia, desonesta...) (PONTOLDIO, ROSSI, 2010).

AMEAÇA

Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave.

Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.

Exemplo: enviar e-mail dizendo que vai fazer algo contra a pessoa. (PONTOLDIO, ROSSI, 2010).

DIVULGAÇÃO DE SEGREDO

Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem.

Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.

Exemplo: repassar e-mail com informação considerada confidencial. (PONTOLDIO, ROSSI, 2010).

DANO

Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia.

Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.

Exemplo: enviar vírus, por e-mail, que destrua equipamento ou conteúdo. (PONTOLDIO, ROSSI, 2010).

VIOLAÇÃO DE DIREITO AUTORAL

Art. 184 - Violar direitos de autor e os que lhe são conexos.

Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa. Exemplo: copiar conteúdo para blog e não mencionar a fonte, baixar MP3 que não tenha controle. (PONTOLDIO, ROSSI, 2010).

ULTRAJE A CULTO E IMPEDIMENTO OU PERTURBAÇÃO DE ATO A ELE RELATIVO

Art. 208 - Escarnecer de alguém publicamente, por motivo de crença ou função religiosa; impedir ou perturbar cerimônia ou prática de culto religioso; vilipendiar publicamente ato ou objeto de culto religioso:

Pena - detenção, de 1 (um) mês a 1 (um) ano, ou multa.

Exemplo: criar uma comunidade on-line (no Orkut, por exemplo) que fale sobre religiões e seus praticantes. (PONTOLDIO, ROSSI, 2010).

ATO OBSCENO

Art. 233 - Praticar ato obsceno em lugar público, ou aberto ou exposto ao público:

Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa.

Exemplo: adotar foto com gestos obscenos em comunidade on-line. (PONTOLDIO, ROSSI, 2010).

FALSA IDENTIDADE

Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:

Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa, se o fato não constitui elemento de crime mais grave.

Exemplo: fazer cadastro com nome falso em uma loja virtual. (PONTOLDIO, ROSSI, 2010).

6. FERRAMENTAS UTILIZADAS PARA DESVENDAR CRIMES DIGITAIS

“A melhor inteligência militar é atacar as estratégias dos inimigos, em seguida atacar suas alianças, depois atacar seus soldados em seu próprio campo.”

Sun Tzu

(A Arte da Guerra)

Apesar de a segurança de sistemas estar sendo cada vez mais utilizada pelas empresas, para um criminoso “cracker” existem inúmeras possibilidades de invasão de um sistema eletrônico, pois o mesmo estuda cada passo que será tomado para que a ação tenha êxito. Em muitos casos, os criminosos ficam meses estudando a fragilidade dos sistemas de determinada empresa até conseguirem encontrar um ponto fraco para atacar.

Como já mencionado anteriormente, o papel de um perito é desvendar os crimes muitas vezes reconstituindo a cena do mesmo, este é um trabalho complicado e que exige muita responsabilidade e para tal o perito forense conta com o auxilio de algumas ferramentas necessárias para verificação, análise e posteriormente desvendar eventuais crimes digitais.

Inicialmente, o perito deve fazer uma breve análise e ter alguma idéia de como o criminoso obteve os resultados pretendidos, quais foram os meios utilizados pelo mesmo. A partir de então o perito contará com ferramentas que o ajudará a descobrir a autoria dos crimes. Utilizadas para diagnosticar e recuperar dados, abaixo serão apresentadas algumas dessas ferramentas utilizadas por um perito para auxiliar em sua tarefa.

6.1. Caller Ip

É uma ferramenta que faz o monitoramento, a entrada, saída e invasão de IPs.

Com a finalidade de encontrar o possível responsável pela ação ocorrida, “A ferramenta *CallerIp* auxilia na indicação de entradas, saídas e invasões de IP na máquina em questão, informando qual o IP que está conectado ou tentando se conectar”, (VARGAS, 2007). É uma ferramenta interessante para o trabalho pericial, pois indica a posição geográfica onde se localiza o dono do endereço IP responsável pela invasão, ou seja, a ferramenta faz o rastreamento de onde vem o IP

responsável pela invasão e aponta direto no mapa mundi a sua localização com endereço e telefone. Como podemos ver na figura abaixo ao lado direito é mostrado os IPs que estavam em maior evidência de ataque e quando clicamos sobre o mesmo é mostrado ao lado do mapa informações relacionadas a esse.

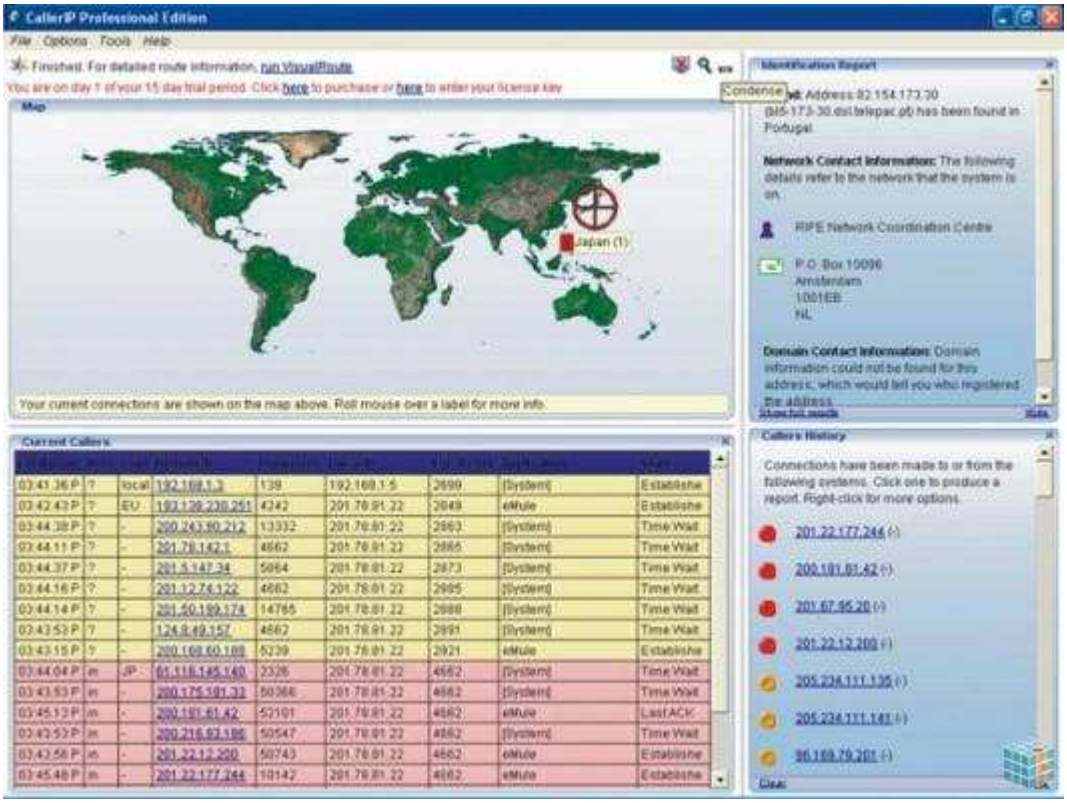

Figura 7 - Tela Principal da Ferramenta *CallerIp* (VARGAS, 2007).

6.2. RecoverMyFiles

Trata-se de um software destinado a plataforma Windows. É um tipo de ferramenta que recupera dados deletados ou formatados.

“É um programa que permite recuperar facilmente arquivos apagados acidentalmente, ou não, do Windows”, (VARGAS, 2007).

Figura 8 – *RecoverMyFiles* (VARGAS, 2007).

O *RecoverMyFiles* recupera desde documentos, músicas, fotografias, vídeos, emails, cartões de máquinas fotográficas, USB, disquetes, como também ficheiros depois de um erro de partição ou falha de disco rígido ou ainda discos rígidos formatados ou outras unidades de armazenamento.

6.3. EnCase

É uma ferramenta bem completa utilizada pelos peritos para atividades em geral, pois abrange muitos recursos gráficos voltados para a recuperação de dados perdidos ou apagados no computador apreendido, protegendo os dados contra escrita, não realizando alterações nos discos originais, pois o *EnCase* não opera na mídia original ou discos espelhados, ele monta as *Evidence Files* como discos virtuais protegidos contra escritas, o que é muito importante para o trabalho do perito, na preservação do local do crime. O *encase* realiza padronização de laudos; “[...] analisa hardwares, logs, emails, fornece uma opção de manusear evidências sem danificá-las, além de outras”, (BORGES et al, 2010); pode fazer a encriptação bem como a decriptação de dados, caso necessário.

Figura 9 – *Encase* (*EnCase Forensic*, 2012)

6.4. Helix

Helix é uma ferramenta de uso gratuito criada em 2005, dedicada a investigação computacional. Segundo (Queiroz; Vargas, 2010, p. 47) uma ótima vantagem desta ferramenta é que ela funciona sem maiores complicações, tanto no sistema Operacional Windows como no Linux, facilitando o trabalho do perito. Outra vantagem é que esta ferramenta é gratuita e há a possibilidade de escolha de idioma.

Esta ferramenta realiza várias etapas importantes na investigação, tais como “recuperar arquivos danificados ou excluídos, buscar senhas em programas de mensagens instantâneas e sites, obter histórico de sites visitados, informações detalhadas de quando uma porta USB foi utilizada e por que tipo de periférico”, (BORGES et al, 2010). Também realiza listagem de processos, análise de memória, recuperação de logins e senhas, além de realizar várias etapas importantes na investigação.

A ferramenta é executada a partir de um CD que pode ser executado tanto com o computador ligado como também ao ligar o computador.

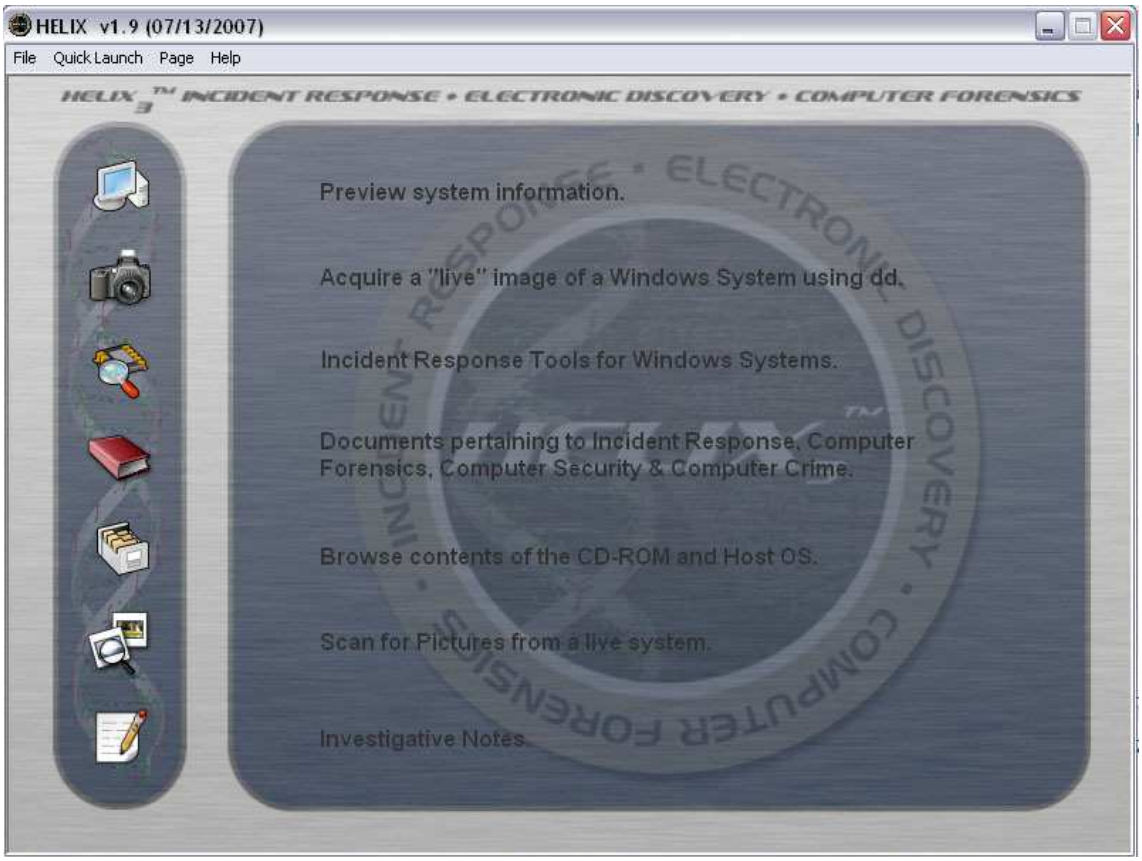

Figura 10 - Ferramenta *Helix* (BORGES et al, 2010).

Com a utilização das ferramentas que foram apresentadas neste capítulo, entre outras, o perito profissional buscará identificar a autoria dos crimes. As ferramentas, com certeza, ajudam o trabalho do profissional além de garantir a integridade da análise desenvolvida durante o processo de investigação.

7. CONCLUSÃO

Nos dias atuais, a Segurança da informação nas organizações não pode ser deixada para segundo plano, visto que empresas perdem muito dinheiro devido a problemas relacionados com a tecnologia. Com certeza o assunto segurança da informação e os assuntos correlacionados serão cada vez mais abordados em temas de trabalho como este. De um lado as instituições investem em tecnologia visando um aumento na segurança e integridade de informações e do outro lado os fraudadores descobrem maneiras de quebrar essa segurança e usufruir das informações conseguidas para ganhar dinheiro ou simplesmente para divertir-se causando estragos dentro das organizações.

A perícia forense computacional deve ser levada mais a sério dentro do termo Segurança da Informação e deve ser um assunto mais abordado dentro dos cursos relacionados, pois a investigação forense tem total relação com a segurança da informação além de ser fundamental para que haja justiça e os crimes realizados através do uso do computador possa ser tratado e julgado de forma justa e os autores paguem pelo delito que cometeram.

Foram apresentados alguns crimes que são cometidos pela internet, estes que cresceram e ainda estão crescendo devido ao fato de os bandidos se sentirem mais protegidos, pois o bandido não expõe seu rosto e tampouco sofre o risco de ser baleado pela polícia. Com o grande aumento dos crimes digitais a área de perícia forense necessita de mais profissionais, pois infelizmente há escassez de mão de obra qualificada no mercado.

O trabalho também visou mostrar a importância do perito e como o mesmo deve estar sempre atualizado na questão de segurança das organizações. Algumas ferramentas que são utilizadas por eles, estas que podem, muitas vezes, ser utilizadas no dia-a-dia do usuário doméstico quando estes desejar recuperar documentos que foram apagados por engano. Mostrou que a identificação da autoria é possível de ser realizada, mas ainda não é uma tarefa simples, principalmente porque ainda há falta de leis especificas para tratar os casos de informática.

Buscou trazer o conhecimento, tanto para profissionais de segurança da informação quanto ao público em geral e mostrar a importância que a perícia forense computacional tem e terá futuramente na sociedade devido ao fato de estarmos

cada vez mais interligados pela rede de computadores e dependente do sistema de informação digital.

Espero que este trabalho sirva de incentivo para futuras pesquisas sobre a área, especialmente sobre as técnicas e ferramentas de forense computacional.

8. REFERÊNCIAS BIBLIOGRÁFICAS

_____. Referências: NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

ABNT NBR ISO/IEC 17799/ago-2005 - Tecnologia da Informação - Técnicas de segurança: Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas. ABNT. Rio de Janeiro, 2005. Disponível em: <http://pt.scribd.com/doc/2449992/Abnt-Nbr-Isoiec-17799-Tecnologia-da-Informacao-Tecnicas-de-Seguranca-Codigo-de-Pratica-para-a-Gestao-da-Seguranca-da-Informacao>.

BEZZERRA, Aline; LUCAS, Marcos. Genética Forense, 2010. Disponível em: <http://pt.scribd.com/doc/44659886/Genetica-Forense>. Acesso em 08 de maio de 2012.

BORGES, Cássio Henrique. et al. Informática Forense. Ferramentas mais utilizadas na perícia forense computacional, 2010. Disponível em: <http://informaticauniaraxa.blogspot.com.br/>. Acesso em 02 de maio de 2012.

BUENO, Marcos Luiz de Paula. Monografia - Forense Computacional: Técnicas e Ferramentas, Departamento de Ciência da Computação, Campus Catalão, UFG, Catalão, Brasil, 2007. 117 p.

CÓDIGO PENAL. Disponível em: <http://cartilha.cert.br/conceitos/sec1.html>. Acesso em 30 de abril de 2012.

CÓDIGO DE PROCESSO CIVIL. Disponível em: <http://www.soleis.com.br >. Acesso em 30/04/2012.

CÓDIGO PROCESSUAL CIVIL. Seja Perito Judicial. Legislação: Como ser perito judicial. Disponível em: <http://www.manualdepericias.com.br/advogadosindice.asp>. Acesso em 30 de abril de 2012.

DAWEL, George. A Segurança da Informação nas Empresas: Ampliando Horizontes Além da Tecnologia. RIO DE JANEIRO: Ciência Moderna, 2005. 117p.

ENCASE FORENSIC, 2012. Disponível em: <http://data-recovery-software.findthebest.com/l/13/EnCase-Forensic>. Acesso em 06 de junho de 2012.

FARMER, Dan; VENEMA, Wietse. Perícia Forense Computacional: Teoria e prática aplicada. São Paulo: Pearson Prentice Hall, 2007. 190 p.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio Tadeu de. Política de Segurança da Informação: Guia Prático para Elaboração e Implementação. Rio de janeiro: Editora Ciência Moderna Ltda., 2008 – 2ª edição. 259 p.

FOCO SECURITY. Apresentação Foco Security, 2006. Disponível em: < http://www.focosecurity.com.br/apresentacao_foco_security.pdf > Acesso em 02 de maio de 2012.

FONTES, Edison Luiz Gonçalves. Política de segurança da informação: uma contribuição para o estabelecimento de um padrão mínimo. – Centro Estadual de Educação Tecnológica Paula Souza, 2011. Disponível em: <http://www.centropaulasouza.sp.gov.br/Posgraduacao/Trabalhos/Dissertacoes/formacao-tecnologica/2011/edison-luiz-goncalves-fontes.pdf>. Acesso em 29 de abril de 2012.

FONTES, Edson. Segurança da informação: o usuário faz a diferença. São Paulo: Saraiva, 2006. 173 p.

FORENSE COMPUTACIONAL: Processo de Investigação, 2012. Disponível em: <https://sites.google.com/a/cristiantm.com.br/forense/forense-computacional/processo-de-investigacao>. Acesso em 16 de maio de 2012.

FREITAS, Andrey Rodrigues de. Perícia Forense aplicada à informática. Rio de Janeiro: Brasport, 2006. 216 p.

GALVÃO, Ricardo Kleber M. Perícia Forense Computacional. Rio de Janeiro, 2009. Disponível em: < http://www.cefetrn.br/~rk/seginfo2009_2_rk.pdf>. Acesso em: 18 de abril de 2012.

LAUDON, Kenneth C. Sistemas de informações gerenciais: administrando a empresa digital. São Paulo: Pearson Prentice Hall, 2004. 561p.

MITNICK, Kevin D.; SIMON, William L. A arte de enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. Tradução: Kátia Aparecida Roque. São Paulo: Pearson Education, 2003. 284 p.

MOREIRA, Ademilson. A importância da segurança da informação, 2008. Disponível em:<http://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao>. Acesso em 19 de março de 2012.

OFICINA DA NET. Aprenda a se proteger de golpes virtuais, 2012. Disponível em: <http://www.oficinadanet.com.br/artigo/seguranca/aprenda-a-se-proteger-de-golpes-virtuais>. Acesso em 19 de março de 2012.

PAULA, Sidney de. Perícia Forense, 2012. Disponível em: <http://www.peritodeinformatica.com/>. Acesso em 30 de abril de 2012.

PEIXOTO, Mário César Pintaudi. Engenharia Social e Segurança da Informação na Gestão Corporativa. Rio de Janeiro: Brasport, 2006. 132 p.

PONTOLDIO, Erich; ROSSI, Pedro Kilikian; PONTOLDIO, Carol Del Santo. Crimes na internet - Talvez você infrinja regras sem saber, 2010. Disponível em: <http://www.30epoucosanos.com/2010/08/crimes-na-internet-talvez-voce-infrinja.html>. Acesso em 30 de maio de 2012.

QUEIROZ, Claudemir; VARGAS, Raffael. Investigação e Perícia Forense Computacional: certificações, Leis processuais e estudo de caso. Rio de Janeiro: Brasport, 2010. 134 p.

REVISTA BRASILEIRA DE INTELIGÊNCIA. Agência Brasileira de Inteligência. – n. 6 (abr. 2011) – Brasília: Abin, 2005. P16-104. Disponível em: <http://www.abin.gov.br/modules/mastop_publish/files/files_4e3ae31e2c097.pdf>. Acesso em 18 de abril de 2012.

RNP - Rede Nacional de Pesquisa. Disponível em: <http://www.rnp.br/cais/estatisticas/index.php> Atualizado em 19/04/2012. Acesso em 20 de abril de 12.

SEMOLA, Marcos. Gestão de segurança da informação: uma visão executiva. Rio de Janeiro: Elsevier, 2003. 156 p.

SENASP/MJ. Secretaria Nacional de Segurança Pública. Curso Preservação de local de crime – Módulo 1 - Última atualização em 09/07/2009. Disponível em:<http://www.ebah.com.br/content/ABAAABpP0AB/preservacao-local-crime-completo>. Acesso em 27 de março de 2012.

SENASP/MJ. Secretaria Nacional de Segurança Pública. Curso Preservação de local de crime – Módulo 1. Disponível em: <http://ead.senasp.gov.br/default.asp> Acesso em 30 de março de 2012.

TANENBAUM, Andrew S. Redes de Computadores. Tradução Vanderberg D. de Souza. Rio de janeiro: Elsevier, 2003 – 17ª reimpressão.945 p.

TAVARES PERÍCIAS. Crimes de computador, 2012. Disponível em: <http://ww1.tavarespericias.com/index.php?option=com_content&view=article&id=59&Itemid=68/>. Acesso em 19 de março de 2012.

VARGAS, Raffael. Perícia Forense Computacional - Ferramentas Periciais, 2007. Disponível em <http://imasters.com.br/artigo/6485/gerencia-de-ti/pericia-forense-computacional-ferramentas-periciais>. Acesso em 16 de maio de 2012.