PERÍCIA FORENSE COMPUTACIONAL

GUIMARÃES, Leonys T. – leonys@ig.com.br
Cruz, Benedito Aparecido (Orientador) – Benedito.cruz@gmail.com

RESUMO

A seguinte apresentação conceitua o que é e o trabalho de um perito forense, responsável por examinar, estudar, algumas vezes reconstituir, analisar e identificar provas de um ato criminoso, de vandalismo ou contra a lei.

Serão descritas algumas ferramentas utilizadas por esse profissional, como geralmente é feito um trabalho de investigação, algumas leis que são importantes para o ramo do perito forense de informática e também alguns métodos anti-forense, utilizados para tentar despistar esses peritos.

Palavras Chave: Forense; Informática; Ferramentas; Anti-forense

ABSTRACT

This presentation conceptualizes what is the work of a forensics expert, responsible for examining, studying, sometimes rebuilding, analyzing and identifying evidences of a criminal act, vandalism or against the law.

It will be described some tools used by this professional; how usually is done an investigation work; some important laws for the computing forensics expert's field e also some anti-forensics methods, used to try to outwit this experts.

Keywords: Expert; Forensics; Computing; Tools; Anti-forensics.

INTRODUÇÃO

No cenário "Pericia Forense Computacional"

O **objetivo geral** foi apresentar os principais pontos do trabalho de um perito forense especializado na área de informática.

O objetivo específico foi detalhar a área de atuação desse profissional, a parte burocrática relacionada, as ferramentas utilizadas e como funciona a atuação anti-forense.

O **método científico** de pesquisa utilizado foi revisão bibliográfica de livros e artigos relativos ao tópico em questão e realização de um *survey* dos assuntos considerados relevantes para o tema.

O trabalho foi estruturado em cinco capítulos, sendo que o primeiro conceitua o que faz um forense computacional, o segundo discorre sobre as leis importantes para o ramo da informática, o terceiro faz menção às ferramentas utilizadas por um forense, o quarto diz respeito às praticas e ferramentas anti-forense.

O QUE FAZ UM FORENSE COMPUTACIONAL?

Ele é responsável por estudar as leis referentes a crimes relacionados com informática, examinar locais de crimes, fazer levantamentos de pistas, possibilidades e possíveis meios de ataque, fazer recuperação de dados, rastreamento de rede e armazenamento de informações.

O perito é chamado pela Justiça para oferecer laudos técnicos em processos judiciais, nos quais podem estar envolvidos pessoas físicas, jurídicas e órgãos públicos. O laudo técnico escrito é assinado pessoalmente pelo perito e passa a ser uma das provas que compõem um processo judicial.

Outra coisa que impacta diretamente o trabalho do perito forense computacional é a falta de leis especializadas para esse tipo de crime, delito, ação, o que com certeza acarreta que os profissionais necessitam fundamentalmente ter conhecimento dos artigos descritos no Código de Processo Penal, o que previne que as evidencias apontadas sejam taxadas de alguma maneira ilegais.

Vale ressaltar que o especialista em segurança computacional necessita manter as empresas (clientes) informadas de que as mesmas precisam manter suas

redes atualizadas, sempre com a manutenção em dia, principalmente nas políticas de segurança, a fim de evitar acidentes e incidentes. E, caso esses incidentes aconteçam, é para isso que os profissionais da área de computação forense estarão a postos, podendo colocar em pratica as políticas de segurança com eficiência (desde que atualizadas e documentadas), logo, caso haja material para que possam realizar o trabalho.

LEIS IMPORTANTES PARA O RAMO DA INFORMÁTICA

Todo o processo que envolve pericia forense, computacional ou não, está diretamente ligado ao ramo jurídico, visto que muitas vezes os crimes podem resultar em processos judiciais e prisões, o que implica diretamente ou indiretamente na aplicação do código penal brasileiro.

Como o Brasil é um país extremamente deficiente na área jurídica relacionada a crimes virtuais, geralmente é traçado um paralelo entre com os métodos tradicionais. Isso é feito, pois assim consegue-se comprovar a integridade e o valor judicial da(s) determinada(s) prova(s) virtual(is).

Isso não quer dizer que não existam projetos vigentes que visam a melhoria do processo jurídico brasileiro, relativo à área de crimes virtuais. Todos os dias são criados novos projetos de lei que passam por cada órgão e cada secretaria do Brasil, com o objetivo de tornar sólida e representativa uma área jurídica reservada aos crimes e delitos virtuais.

Vale ressaltar que todo perito forense (computacional ou não) necessita ter conhecimento e compreensão do Código de Processo Penal “Capítulo II - Do Exame do Corpo de Delito, e das Perícias em Geral”, visto que é nessa fração do código que é detalhado todo o processo de investigação, o que obviamente é necessário para qualquer tipo de perito forense.

FERRAMENTAS UTILIZADAS POR UM FORENSE

Devido ao fato da computação ser uma área muitas vezes densa, complexa e trabalhosa, existem vários tipos de ferramentas que pode ser usadas para a verificação/analise/solução de um caso.

É indispensável que o perito possua os conhecimentos mínimos necessário para se fazer uma análise breve e já ter uma idéia dos meios utilizados pelo criminoso. Podem ser esses meios diretos/físicos (ex: tentativa de destruição de HDs) como meios “indiretos”/lógicos (ex: roubo de senha virtual).

Devido a essa multiplicidade de possibilidades, existem ferramentas direcionadas aos mais diversos tipos de análise, como rastreamento de IPs, recuperação de unidades externas, etc. Mas também, existem ferramentas de uso geral, que abrangem não só um, mas vários conceitos na pratica da analise do caso, o que pode tornar mais rápida e eficiente a ação do perito.

Exemplos: CallerIP, RecoverMyFiles, SmartWhoIs, E-mailTracker, Encase, chrootkit, Sleuth Kit, entre outros.

PRATICAS E FERRAMENTAS ANTI-FORENSE

Conforme dito anteriormente, o processo de análise forense consiste em estudar as leis referentes a crimes relacionados com informática, examinar locais de crimes, fazer levantamentos de pistas, possibilidades e possíveis meios de ataque, fazer recuperação de dados, rastreamento de rede e armazenamento de informações entre outras funções.

Mas enquanto os peritos forenses estão se esforçando nessa árdua tarefa de analisar e desvendar os crimes, os atacantes também estão focados fortemente em ocultar, disfarçar, esconder, maquiar e até mesmo apagar seus rastros.

Existem várias práticas e ferramentas utilizadas. Nesse trabalho, serão abordados a utilização de “Rootkits” (um vírus ou trojan, destinado a liberar total acesso na maquina do atacado), “Backdoors” (Função semelhante à dos “Rootkits”.

Aproveitam-se de falhas, brechas e defasagens de segurança no sistema, que permite que os atacantes tenham controle remoto total da maquina da vítima), “Slack Space” (implantação de ameaças em pequenas brechas contidas dentro do sistema, driblando anti-vírus) e a curiosa Esteganografia (Já vem sendo utilizada a mais de dois mil e quinhentos anos. A melhor definição seria algo como “ocultar” uma mensagem dentro de um objeto sendo que essa mensagem não seja visível para qualquer observador.).

RESULTADOS E/OU DISCUSSÃO

Qualquer pessoa pode utilizar esse artigo para pesquisas, consultas, formulação de idéias e/ou ideologias. Mas, ressalto que os profissionais da área de Tecnologia da Informação serão os mais privilegiados, visto que o maior foco desse artigo está ligado diretamente à área de informática e computação.

CONSIDERAÇÕES FINAIS

A partir da apresentação e análise dos dados, observa-se que, com o decorrer do tempo, o índice de crimes envolvendo o ramo digital e virtual cresceu de maneira muito acelerada, tornando necessário a aumento e o aprofundamento de estudos, analises, processos e leis relativos a esse tipo de incidentes.

Outra questão importante diz respeito ao número de profissionais, cursos, certificações e pessoal especializado nessa área, que e infelizmente é um numero pequeno, mas que com toda a certeza tende a aumentar muito em pouco tempo, devido ao crescimento desenfreado de crimes virtuais.

Atrelado às questões acima citadas, podemos frisar que alem de profissionais do ramo investigativo, também existem vários profissionais do ramo jurídico que estão nessa constante luta para ajudar a desenvolver e aumentar o numero de leis relacionadas a processos digitais/virtuais.

Ressaltando que não existiria um bom processo de investigação sem boas ferramentas, sendo que estas, no ramo da informática abrangem todos os patamares relacionados à plataforma digital, desde hardware como HDs, Pendrives

e outros, até softwares, reconhecimento de IPs, rastreamento de e-mails, entre outros.

Conforme todos os pontos selecionados e citados nesse trabalho, conclui-se que o ramo da pericia forense computacional, desde o trabalho de análise até o detalhamento jurídico, está se tornando cada dia mais essencial e mais necessário devido ao crescimento exponencial dos crimes virtuais, cibernéticos e digitais, que vão desde simples “atos maliciosos”, até roubo, assalto, atividades anti-forense e muitos outros.

REFERÊNCIAS BIBLIOGRÁFICAS

AGOSTINHO, Denilson A. “Leis da segurança da informação”, 2004 – Disponível em:

<http://www.inf.ufsc.br/~bosco/ensino/ine5630/Trabalhos%202004-2/artigo-LeisDeSeguranca.pdf>

Acesso em: 03 de março de 2011 às 23h25min.

BARRETO, Gustavo L. “Utilização de técnicas anti-forenses para garantir a confidencialidade”, 2009 – Disponível em:

<http://www.ppgia.pucpr.br/~jamhour/Download/pub/RSS/MTC/referencias/TCC%20-%20Gustavo%20Luis%20Barreto.pdf>

Acesso em: 08 de março de 2011 às 17h15min.

BARWINSKI, Luísa. “O que é rootkit?”, 2009 – Disponível em:

<http://www.tecmundo.com.br/2174-o-que-e-rootkit-.htm>

Acesso em: 07 de março de 2011 às 17h25min.

BUSTAMANTE, Leonardo. “O papel da computação forense para a autoridade policial”, 2006 – Disponível em:

<http://imasters.com.br/artigo/4729/forense/o_papel_da_computacao_forense_para_a_autoridade_policial/>

Acesso em: 25 de abril de 2011 às 23h35min.

BUSTAMANTE, Leonardo. “Introdução a computação forense”, 2006 – Disponível em:

<http://imasters.com.br/artigo/4175/forense/introducao_a_computacao_forense/>

Acesso em: 06 de abril de 2011 às 16h45min.

CARPANEX, Juliana. “Conheça os crimes virtuais mais comuns”, 2006 – Disponível em:

<http://www1.folha.uol.com.br/folha/informatica/ult124u19455.shtml>

Acesso em: 02 de maio de 2011 às 23h10min.

CASA CIVIL - Subchefia para Assuntos Jurídicos. “LEI Nº 9.609 , DE 19 DE FEVEREIRO DE 1998**”** – Disponível em:

<http://www.planalto.gov.br/ccivil/Leis/L9609.htm>

Acesso em: 02 de maio de 2011 às 23h20min.

CONTI, Fatima. “Vírus e Cia, Backdoors”, 2007 – Disponível em:

<http://www.cultura.ufpa.br/dicas/vir/inv-indi.htm>

Acesso em: 21 de abril de 2011 às 22h50min.

CRUZ, Benedito A., Material utilizado na disciplina "Pericia Forense Computacional", 2011 – Disponível em:

<http://www.benecruz.info/moodle/course/view.php?id=9>

Acesso em: 11 de maio de 2011 às 19h15min.

DANTAS, Allan. "Entenda o que é Backdoor", 2010 – Disponível em:

<http://tecnologiajb.com/2010/08/entenda-o-que-e-backdoor/>

Acesso em: 22 de março de 2011 às 19h15min

FARMER, Dan – Perícia Forense Computacional: Teoria e Prática Aplicada, 1ª Edição, 2006, Editora Pearson Prentice Hall.

FREITAS, Audrey Rodrigues de – Perícia Forense Aplicada à Informática, 1ª Edição, 2006, Editora Brasport Livros e Multimídia Ltda.

GETDATA. "Purchase Recover My Files v4" – Disponível em:
<http://www.recovermyfiles.com/data-recovery-software-purchase.php/>
Acesso em: 15 de março de 2011 às 20h30min.

GUIDANCE SOFTWARE. "EnCase Forensic" – Disponível em:
<http://www.guidancesoftware.com/forensic.htm>
Acesso em: 15 de março de 2011 às 22h10min.

HOLPERIN, Marco - **LEOBONS,** Rodrigo. "The @stake Sleuth Kit (TASK)", 2007– Disponível em:
<http://www.gta.ufrj.br/grad/07_1/forense/task.html>
Acesso em: 20 de abril de 2011 às 10h00min.

HOLPERIN, Marco - **LEOBONS,** Rodrigo. "EnCase", 2007 – Disponível em:
<http://www.gta.ufrj.br/grad/07_1/forense/encase.html>
Acesso em: 22 de março de 2011 às 19h40min.

LEITE, Thiago. "Escondendo Arquivos Utilizando ADS", 2007 – Disponível em:
<http://localdomain.wordpress.com/2007/04/30/escondendo-arquivos-utilizando-ads/>
Acesso em: 11 de maio de 2011 às 20h40min.

LUCENA, Jonatas. "Crimes Virtuais" – Disponível em:
<http://www.drjonatas.com.br/crimes-virtuais.php>
Acesso em: 22 de março de 2011 às 20h40min.

MARTINS, Elaine. “Perito Digital: o que ele faz e como consegue recuperar informações perdidas”, 2010 – Disponível em:
<http://www.tecmundo.com.br/3615-perito-digital-o-que-ele-faz-e-como-consegue-recuperar-informacoes-perdidas.htm>
Acesso em: 15 de maio de 2011 às 23h25min.

MARTINS, Elaine. “O que é esteganografia”, 2010 – Disponível em:
<http://www.tecmundo.com.br/3763-o-que-e-esteganografia-.htm>
Acesso em: 19 de abril de 2011 às 23h50min.

MARTINS, Fabrício. “A impunidade na internet está com os dias contados”, 2005 – Disponível em:
<http://www1.folha.uol.com.br/folha/informatica/ult124u18101.shtml>
Acesso em: 21 de maio de 2011 às 22h30min.

MIRABETE, Julio F. “Exame do corpo de delito e pericias em geral”, 2010 – Disponível em:
<http://xoomer.virgilio.it/direitousp/curso/mira20.htm>
Acesso em: 03 de março de 2011 às 23h10min.

MURILO, Nelson. “Chkrootkit”, 2006 – Disponível em:
<http://arquivos.naopod.com.br/files/03-chkrootkit.pdf>
Acesso em: 10 de março de 2011 às 22h40min.

PINHEIRO, José M. S. “Esteganografia digital”, 2005 – Disponível em:
<http://www.projetoderedes.com.br/artigos/artigo_esteganografia_digital.php>
Acesso em: 15 de março de 2011 às 23h20min.

QUEIROZ, Ruy de. “Forense Computacional”, 2010 – Disponível em:
<http://www.cin.ufpe.br/~ruy/crypto/seguranca/Forense_Computacional%28UFPE%29.pdf >

Acesso em: 14 de março de 2011 às 23h20min.

ROSA, André. “Pericia Forense: Recuperar histórico do Firefox com o ff3hr”, 2010 – Disponível em:

<http://vivaolinux.com.br/dica/Pericia-Forense-Recuperar-historico-do-Firefox-com-o-ff3hr/>

Acesso em: 10 de abril de 2011 às 23h00min.

ROSA, André. “Computação Forense: Entendendo uma perícia”, 2010 – Disponível em:

<http://www.vivaolinux.com.br/artigo/Computacao-Forense-Entendendo-uma-pericia>

Acesso em: 14 de março de 2011 às 00h10min.

SILVA, Luís M. “Anti-Análise Forense”, 2006 – Disponível em:

<http://lms.ispgaya.pt/documentacao/anti-analise.forense.pdf>

Acesso em: 02 de maio de 2011 às 22h45min.

SOUZA, Ranieri M. “Computação forense”, 2009 – Disponível em:

<http://blog.segr.com.br/computacao-forense/>

Acesso em: 14 de março de 2011 às 23h50min.

TAMOSOFT. “Product Catalog” – Disponível em:

<http://www.tamos.com/order/index.php?js=1>

Acesso em: 15 de março de 2011 às 21h00min.

TOMÁS, Eliane M. C. “CRIMES INFORMÁTICOS: Legislação brasileira e técnicas de forense computacional aplicadas à essa modalidade de crime”, 2010 – Disponível em:

<http://www.artigos.etc.br/crimes-informaticos-legislacao-brasileira-e-tecnicas-de-forense-computacional-aplicadas-a-essa-modalidade-de-crime.html>

Acesso em: 02 de março de 2011 às 22h00min.

VARGAS, Raffael. “Duplicação forense de discos rígidos”, 2009 – Disponível em: <http://imasters.com.br/artigo/13155/gerencia-de-ti/duplicacao-forense-de-discos-rigidos>

Acesso em: 14 de março de 2011 às 22h00min.

VARGAS, Raffael. “Pericia forense computacional: Ferramentas periciais”, 2007 – Disponível em: <http://imasters.com.br/artigo/6485/forense/pericia_forense_computacional_ferramentas_periciais/>

Acesso em: 09 de março de 2011 às 21h50min.

VISUALWAREl. “CallerIP Pricing Options”– Disponível em: <http://www.callerippro.com/purchase/cip.html>

Acesso em: 15 de março de 2011 às 19h50min.

VISUALWAREl. “EmailTrack Pricing Options”– Disponível em: < http://www.emailtrackerpro.com/purchase/emt.html>

Acesso em: 15 de março de 2011 às 20h20min.