Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

PERICIA FORENSE COMPUTACIONAL

LEONYS TADDEO GUIMARÃES

Americana, SP
2011

Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

PERICIA FORENSE COMPUTACIONAL

LEONYS TADDEO GUIMARÃES
leonys@ig.com.br

Trabalho de Conclusão de Curso apresentado à Banca Examinadora, como exigência parcial para obtenção de título de Graduação do Curso de Segurança da Informação, Habilitação em Segurança da Informação, da Faculdade de Tecnologia de Americana, sob a orientação do Prof. Benedito Aparecido Cruz.

Americana, SP
2011

Americana - São Paulo - Brasil
JUNHO 2011

BANCA EXAMINADORA

Benedito Aparecido Cruz

Rogério Nunes de Freitas

Irineu Ambrozano Filho

AGRADECIMENTOS

Meu principal agradecimento vai para uma pessoa que ajudou muito no meu engrandecimento profissional e acadêmico, meu orientador, Professor Benedito Cruz, que dentre tantas aulas de protocolos de rede, banco de dados, perícia forense e etc., apesar da complexidade e da quantidade de matéria, nunca deixou de dar uma aula descontraída e com uma didática incrível, que sempre cativou todos os alunos. Partilhador do mesmo gosto musical, sempre me lembrarei das conversas sobre musica que tivemos tal qual a disposição e o animo que era demonstrado tanto em conversas descontraídas, quanto em conversas relativas à matéria. Muito obrigado por tudo professor, devido ao fato do Sr. ser quem é, garanto que nunca me veio outra pessoa à cabeça para ser meu orientador.

DEDICATÓRIA

Gostaria de agradecer primeiramente a toda a minha família. Todo o apoio, o encorajamento e a confiança que me foi depositado para chegar onde estou hoje, desde meu ensino infantil, passando pelo fundamental e médio, até chegar ao final de meu curso de ensino superior. Segundo, aos tão dedicados e competentes professores que muitas vezes se empenham tanto quanto os alunos para realizarem suas funções sempre com muita maestria e profissionalismo. E não poderia deixar de mencionar, meus amigos que, junto com a família, sempre foram meu porto-seguro, minha fonte de companheirismo, compreensão, ajuda, risadas e trabalho de equipe.

Aos professores da FATEC Americana:

Os anos passam... O conhecimento é acumulado, algum conhecimento esquecido, outros ultrapassados, mas os valores são eternos e a lembrança de alguns mestres permanece.
Somos frutos de algum mestre, seja ele professor, pai ou mãe, pois todos são mediadores. Todo pai é um pouco mestre e todo professor é um pouco pai!
Obrigada, Mestres
Obrigada, Professores

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: Perito; 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.

LISTA DE SIGLAS

IP – “Internet Protocol”

HD - "Hard Disk"

RMF - "Recover My Files"

SWI - "Smart Who Is"

T@SK - "The @stake Sleuth Kit"

PC - "Personal Computer"

IDS - "Intrusion Detection System"

ADS - "Alternate Data Streams"

HTML - "Hyper Text Markup Language"

LSB - "Least Significant Bit"

LISTA DE FIGURAS

SUMÁRIO

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.

Com base nas informações conseguidas a partir dos estudos realizados nos capítulos anteriores, o capítulo cinco se reserva às considerações finais.

1 O QUE FAZ UM FORENSE COMPUTACIONAL?

Atualmente, nos deparamos com uma onda que cresce exponencialmente, tratando-se do quesito digital. Pessoas, empresas, fábricas, tudo está cada vez mais dependente da informática. Gerenciar uma empresa, por menor que seja, sem a informática, hoje é praticamente impossível, pois o mundo em si está extremamente envolto e dependente dos meios digitais.

Infelizmente, como sabemos, quanto mais a informática é usada, maiores são as tentativas de deturpar, roubar, extraviar informações, o que preocupa a todos os usuários desse universo digital. Mas uma coisa é fato: conforme aumenta o uso da tecnologia digital, aumenta também o numero de indivíduos mal-intencionados. Diversos crimes têm surgido nesse meio e muitos afetados não tem tido o resultado esperado em troca.

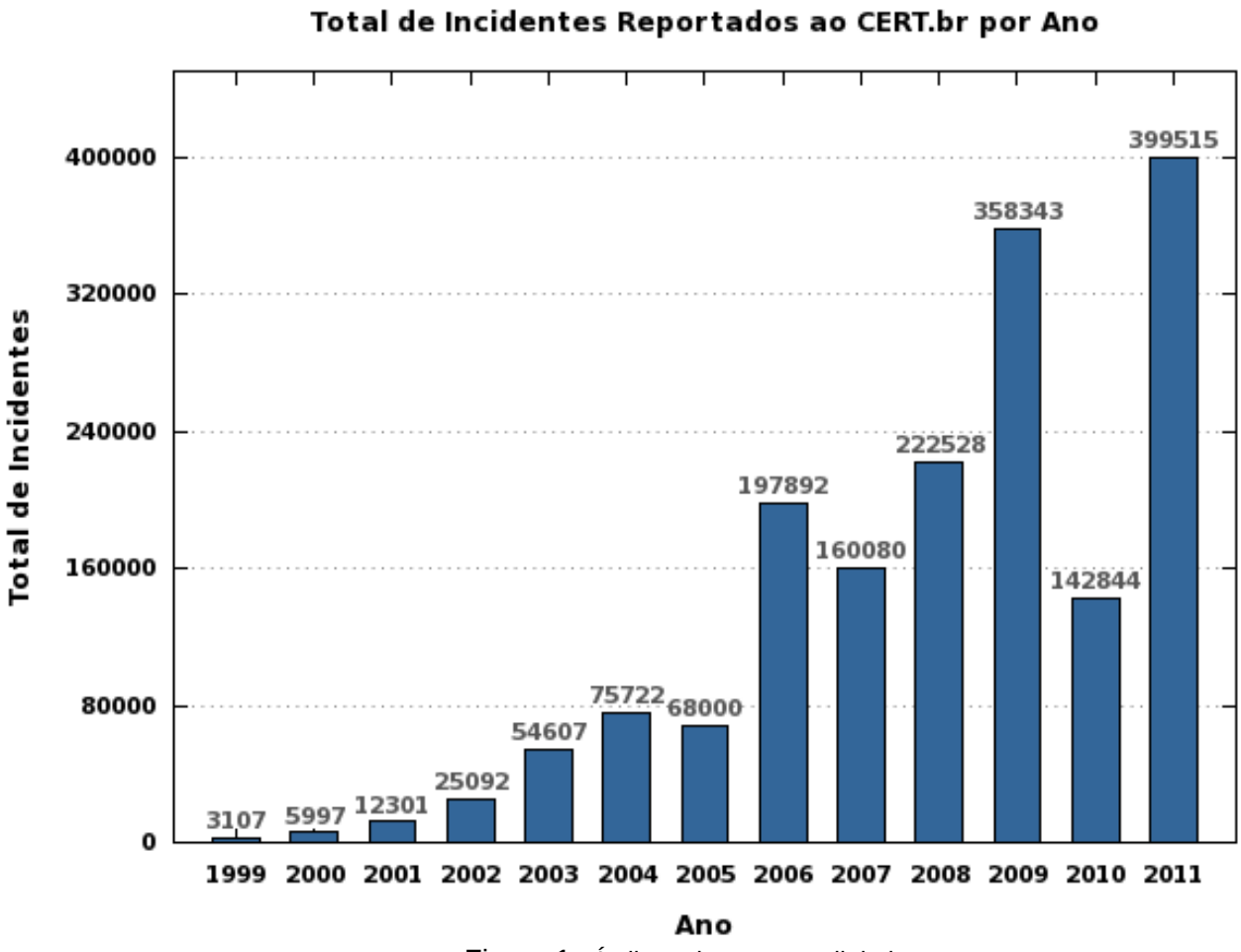

Figura 1 - Índices de ataques digitais
Fonte: http://newspressrelease.files.wordpress.com/2010/06/estatistica-cert-br.png?w=510&h=382

Considera-se “resultado esperado” qualquer tipo de punição contra os atacantes. Cadeia, reformatório, trabalho voluntário ou outro tipo de atividade. Muitas vezes, como dito anteriormente, nenhuma dessas ações acabam tornando-se realidade, algumas vezes por não existir nenhuma lei que ajude efetivamente a determinar a gravidade desses crimes e algumas vezes porque os criminosos simplesmente não conseguem ser encontrados.

Por essa crescente necessidade, surgiu o profissional conhecido por perito 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.

Essa ainda é uma prática muito nova no Brasil. Ainda estamos apenas no começo das especializações e dos estudos na ciência forense aplicada ao ambiente computacional. Pode-se lembrar que essa pratica já é seguida nos Estados Unidos e em alguns lugares da Europa há algum tempo. Mas como já foi dito, esse crescente e desenfreado uso dos recursos digitais aumenta cada vez mais a procura e a busca por esse tipo de profissional, o que também abrange, claro, o Brasil.

O Instituto de Computação da Unicamp identificou o conceito como "a ciência que estuda a aquisição, preservação, recuperação e análise de dados que estão em formato eletrônico e armazenados em algum tipo de mídia computacional".

Devido a essa área ser uma área recente, não existem muitos profissionais experientes no mercado, tampouco com certificações específicas, o que torna qualquer tipo de experiência, por menor que seja, um diferencial que pode ser decisivo para a aceitação em uma vaga nessa área.

Certificações então são mais difíceis ainda de se encontrar, principalmente por serem recentes, o que as torna praticamente um ingresso garantido para um emprego baseado nessa área.

É imprescindível que um profissional que queira tornar-se um perito em computação forense tenha experiência em áreas especificas como redes, segurança da informação e direito. Talvez mais importante que a especialização técnica seja a integridade desse profissional como cidadão e como profissional, visto que ele lidará com informações valiosas e secretas na maior parte de suas atividades.

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[1]. 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.

Também é interessante sempre alertar/informar os usuários para fazerem o possível para evitar complicações, sempre ficarem atentos a atentados digitais e sempre optarem por empresas que tenham boas e atualizadas políticas de segurança da informação, sempre as seguindo à risca.

---

[1] Nota:
Acidente: Acontecimento fortuito, geralmente lamentável, infeliz; desastre
Incidente: Evento não desejado, o qual ocorre circunstancias ligeiramente diferentes no qual poderia haver resultado em lesões para as pessoas, danos à propriedade ou perdas no processo

No caso de um incidente, os profissionais forenses poderão atuar com boas ferramentas e com maestria para resolver o problema, o que garante que os problemas sejam resolvidos na maioria das vezes.

1.1 Crimes virtuais mais comuns

- Pedofilia

Um caso muito popular e muito combatido atualmente, a pedofilia acontece quando o criminoso expõe e disponibiliza material (imagens e vídeos) com conteúdo pornográfico que vai desde nudez até atos sexuais envolvendo menores de idade.

- Aviltação e Vilipendiação

Casos onde comete crime a pessoa que publica informações caluniosas e mentirosas sobre outra pessoa ou corporação, visando prejudicá-la e difamá-la. Lembrando que esse tipo de crime virtual se tornou muito popular após o estouro dos sites de relacionamento virtual. Estouro esse que começou com o Orkut a praticamente uma década e que se expandiu para Tumblr, Twitter, Facebook, entre outros.

- Discriminação

Crime também muito praticado na vida não-virtual, a discriminação consiste em difamar, insultar e desrespeitar raças, etnias, religiões, cor e também praticas de xenofobia. Também se tornou muito mais comum após o surgimento das grandes redes de relacionamento.

- Roubo de Identidade

Os atacantes utilizam técnicas reais (ex: engenharia social) ou virtuais (ex: keyloggers) para se apoderarem de dados pessoais das vitimas, para realizar compras virtuais, transações bancárias e qualquer outra pratica que possa vir a beneficiá-los utilizando os dados de outras pessoas. Os praticantes desse ato estão

sujeitos a responder por estelionato, furto devido a fraude, extravio de dados, quebra de sigilo bancário e formação de quadrilha.

- Ameaças

Qualquer tipo de ameaça que possa vir a indiciar algum mal para o mencionado. Se existe alguma declaração de ameaça publicada virtualmente, ela é usada automaticamente como prova, caso realmente venha acontecer algo com a pessoa/instituição mencionada.

- Espionagem corporativa

Dados de empresas e corporações estão sujeitos a extravios todos os dias, até porque, existem inúmeras maneiras desse extravio ocorrer. Pendrives, HDs externos, cartões de memória e até mesmo e-mails. A tecnologia facilita muito esse tipo de ação, até porque um simples pendrive com um peso insignificante pode equivaler a muitas pastas de documentos.

2 LEIS IMPORTANTES PARA O RAMO DA INFORMATICA

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.

2.1 Processo Litigioso

O processo Litigioso é quando o caso envolve conflito de interesses entre o estado e o administrado.

Dentro desse conflito, o estado possui a função de tomar parte, porém, também possui a função de Julgador, tornando o Juiz uma entidade imparcial, mediadora, que não tomará lado de nenhumas as partes.

- Envolve sentença judicial
- Crimes

● Ressarcimento de danos

● Culpabilidade (família)

2.2 Processo Não-Litigioso

Ao contrário do processo Litigioso, o processo Não-Litigioso não impõe interesses entre o estado e o administrado.

Esses, com certeza, são os casos que ocorrem com maior freqüência.

● Não envolve sentença judicial

● Empresas (preservação da marca)

● Residências (privacidade)

2.3 Exemplo de uma lei aplicada a TI

“LEI Nº 9.609 , DE 19 DE FEVEREIRO DE 1998.

Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.

CAPÍTULO II

DA PROTEÇÃO AOS DIREITOS DE AUTOR E DO REGISTRO

Art. 2º O regime de proteção à propriedade intelectual de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no País, observado o disposto nesta Lei.

§ 1º Não se aplicam ao programa de computador as disposições relativas aos direitos morais, ressalvado, a qualquer tempo, o direito do autor de reivindicar a paternidade do programa de computador e o direito do autor de opor-se a alterações não-autorizadas, quando estas impliquem deformação, mutilação ou outra modificação do programa de computador, que prejudiquem a sua honra ou a sua reputação.

§ 2º Fica assegurada a tutela dos direitos relativos a programa de computador pelo prazo de cinqüenta anos, contados a partir de 1º de janeiro do ano subseqüente ao da sua publicação ou, na ausência desta, da sua criação.

§ 3º A proteção aos direitos de que trata esta Lei independe de registro.

§ 4º Os direitos atribuídos por esta Lei ficam assegurados aos estrangeiros domiciliados no exterior, desde que o país de origem do programa conceda, aos brasileiros e estrangeiros domiciliados no Brasil, direitos equivalentes.

§ 5º Inclui-se dentre os direitos assegurados por esta Lei e pela legislação de direitos autorais e conexos vigentes no País aquele direito exclusivo de autorizar ou proibir o aluguel comercial, não sendo esse direito exaurível pela venda, licença ou outra forma de transferência da cópia do programa.

§ 6º O disposto no parágrafo anterior não se aplica aos casos em que o programa em si não seja objeto essencial do aluguel.

Art. 3º Os programas de computador poderão, a critério do titular, ser registrados em órgão ou entidade a ser designado por ato do Poder Executivo, por iniciativa do Ministério responsável pela política de ciência e tecnologia. (Regulamento)

§ 1º O pedido de registro estabelecido neste artigo deverá conter, pelo menos, as seguintes informações:

I - os dados referentes ao autor do programa de computador e ao titular, se distinto do autor, sejam pessoas físicas ou jurídicas;

II - a identificação e descrição funcional do programa de computador; e

III - os trechos do programa e outros dados que se considerar suficientes para identificá-lo e caracterizar sua originalidade, ressalvando-se os direitos de terceiros e a responsabilidade do Governo.

§ 2º As informações referidas no inciso III do parágrafo anterior são de caráter sigiloso, não podendo ser reveladas, salvo por ordem judicial ou a requerimento do próprio titular.

Art. 4º Salvo estipulação em contrário, pertencerão exclusivamente ao empregador, contratante de serviços ou órgão público, os direitos relativos ao programa de computador, desenvolvido e elaborado durante a vigência de contrato ou de vínculo estatutário, expressamente destinado à pesquisa e desenvolvimento, ou em que a atividade do empregado, contratado de serviço ou servidor seja prevista, ou ainda, que decorra da própria natureza dos encargos concernentes a esses vínculos.

§ 1º Ressalvado ajuste em contrário, a compensação do trabalho ou serviço prestado limitar-se-á à remuneração ou ao salário convencionado.

§ 2º Pertencerão, com exclusividade, ao empregado, contratado de serviço ou servidor os direitos concernentes a programa de computador gerado sem relação com o contrato de trabalho, prestação de serviços ou vínculo estatutário, e sem a utilização de recursos, informações tecnológicas, segredos industriais e de negócios, materiais, instalações ou equipamentos do empregador, da empresa ou entidade com a qual o empregador mantenha contrato de prestação de serviços ou assemelhados, do contratante de serviços ou órgão público.

§ 3º O tratamento previsto neste artigo será aplicado nos casos em que o programa de computador for desenvolvido por bolsistas, estagiários e assemelhados.

Art. 5º Os direitos sobre as derivações autorizadas pelo titular dos direitos de programa de computador, inclusive sua exploração econômica, pertencerão à pessoa autorizada que as fizer, salvo estipulação contratual em contrário.

Art. 6º Não constituem ofensa aos direitos do titular de programa de computador:

I - a reprodução, em um só exemplar, de cópia legitimamente adquirida, desde que se destine à cópia de salvaguarda ou armazenamento eletrônico, hipótese em que o exemplar original servirá de salvaguarda;

II - a citação parcial do programa, para fins didáticos, desde que identificados o programa e o titular dos direitos respectivos;

III - a ocorrência de semelhança de programa a outro, preexistente, quando se der por força das características funcionais de sua aplicação, da observância de preceitos normativos e técnicos, ou de limitação de forma alternativa para a sua expressão;

IV - a integração de um programa, mantendo-se suas características essenciais, a um sistema aplicativo ou operacional, tecnicamente indispensável às necessidades do usuário, desde que para o uso exclusivo de quem a promoveu.

CAPÍTULO III

DAS GARANTIAS AOS USUÁRIOS DE PROGRAMA DE COMPUTADOR

Art. 7º O contrato de licença de uso de programa de computador, o documento fiscal correspondente, os suportes físicos do programa ou as respectivas embalagens deverão consignar, de forma facilmente legível pelo usuário, o prazo de validade técnica da versão comercializada.

Art. 8º Aquele que comercializar programa de computador, quer seja titular dos direitos do programa, quer seja titular dos direitos de comercialização, fica obrigado, no território nacional, durante o prazo de validade técnica da respectiva versão, a assegurar aos respectivos usuários a prestação de serviços técnicos complementares relativos ao adequado funcionamento do programa, consideradas as suas especificações.

Parágrafo único. A obrigação persistirá no caso de retirada de circulação comercial do programa de computador durante o prazo de validade, salvo justa indenização de eventuais prejuízos causados a terceiros.

CAPÍTULO IV

DOS CONTRATOS DE LICENÇA DE USO, DE COMERCIALIZAÇÃO E DE TRANSFERÊNCIA DE TECNOLOGIA

Art. 9º O uso de programa de computador no País será objeto de contrato de licença.

Parágrafo único. Na hipótese de eventual inexistência do contrato referido no caput deste artigo, o documento fiscal relativo à aquisição ou licenciamento de cópia servirá para comprovação da regularidade do seu uso.

Art. 10. Os atos e contratos de licença de direitos de comercialização referentes a programas de computador de origem externa deverão fixar, quanto aos tributos e encargos exigíveis, a responsabilidade pelos respectivos pagamentos e estabelecerão a remuneração do titular dos direitos de programa de computador residente ou domiciliado no exterior.

§ 1º Serão nulas as cláusulas que:

I - limitem a produção, a distribuição ou a comercialização, em violação às disposições normativas em vigor;

II - eximam qualquer dos contratantes das responsabilidades por eventuais ações de terceiros, decorrentes de vícios, defeitos ou violação de direitos de autor.

§ 2º O remetente do correspondente valor em moeda estrangeira, em pagamento da remuneração de que se trata, conservará em seu poder, pelo prazo de cinco anos, todos os documentos necessários à comprovação da licitude das remessas e da sua conformidade ao caput deste artigo.

Art. 11. Nos casos de transferência de tecnologia de programa de computador, o Instituto Nacional da Propriedade Industrial fará o registro dos respectivos contratos, para que produzam efeitos em relação a terceiros.

Parágrafo único. Para o registro de que trata este artigo, é obrigatória a entrega, por parte do fornecedor ao receptor de tecnologia, da documentação completa, em especial do código-fonte comentado, memorial descritivo, especificações funcionais internas, diagramas, fluxogramas e outros dados técnicos necessários à absorção da tecnologia.

CAPÍTULO V

DAS INFRAÇÕES E DAS PENALIDADES

Art. 12. Violar direitos de autor de programa de computador:

Pena - Detenção de seis meses a dois anos ou multa.

§ 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:

Pena - Reclusão de um a quatro anos e multa.

§ 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

§ 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:

I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;

II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.

§ 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

Art. 13. A ação penal e as diligências preliminares de busca e apreensão, nos casos de violação de direito de autor de programa de computador, serão precedidas de vistoria, podendo o juiz ordenar a apreensão das cópias produzidas ou comercializadas com violação de direito de autor, suas versões e derivações, em poder do infrator ou de quem as esteja expondo, mantendo em depósito, reproduzindo ou comercializando.

Art. 14. Independentemente da ação penal, o prejudicado poderá intentar ação para proibir ao infrator a prática do ato incriminado, com cominação de pena pecuniária para o caso de transgressão do preceito.

§ 1º A ação de abstenção de prática de ato poderá ser cumulada com a de perdas e danos pelos prejuízos decorrentes da infração.

§ 2º Independentemente de ação cautelar preparatória, o juiz poderá conceder medida liminar proibindo ao infrator a prática do ato incriminado, nos termos deste artigo.

§ 3º Nos procedimentos cíveis, as medidas cautelares de busca e apreensão observarão o disposto no artigo anterior.

§ 4º Na hipótese de serem apresentadas, em juízo, para a defesa dos interesses de qualquer das partes, informações que se caracterizem como confidenciais, deverá o juiz determinar que o processo prossiga em segredo de justiça, vedado o uso de tais informações também à outra parte para outras finalidades.

§ 5º Será responsabilizado por perdas e danos aquele que requerer e promover as medidas previstas neste e nos arts. 12 e 13, agindo de má-fé ou por espírito de emulação, capricho ou erro grosseiro, nos termos dos arts. 16, 17 e 18 do Código de Processo Civil.” [2]

[2] Nota:
*Trecho extraído do acervo virtual da casa civil da Presidência da República [**CASA,** José I.]*

3 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.

3.1 CallerIP

*Preço da licença: Varia de um usuário: $34.95 + $48.95 (manutenção anual) até cinqüenta usuários: $400 + $560 (manutenção anual) [**VISUALWARE**]*

O CallerIP trata-se de uma ferramenta que monitora entradas, saídas, e tentativas de invasões de IP do sistema em pauta. Uma das partes mais interessantes desse software é “localizador”. Trata-se de um pequeno mapa mundi exibido no topo da tela, quando o IP de provável atacante é detectado, a própria ferramenta faz o rastreamento de onde vem esse IP e aponta direto no mapa mundi. Além disso, o sistema também disponibiliza alguns dados muitas vezes valiosos, como um e-mail utilizado por esse IP e telefone. Diz-se que esses dados são “muitas vezes” valiosos pois nem sempre os mesmos estão corretos. Além desses recursos, o CallerIP também disponibiliza os dados mas simples (mas não menos importantes): hora do recebimento/envio, se trata-se de uma entrada ou saída, país de destino, porta, IP local, aplicação utilizada e o estado da conexão (estabelecida, fechada, ou ainda tentando se conectar).

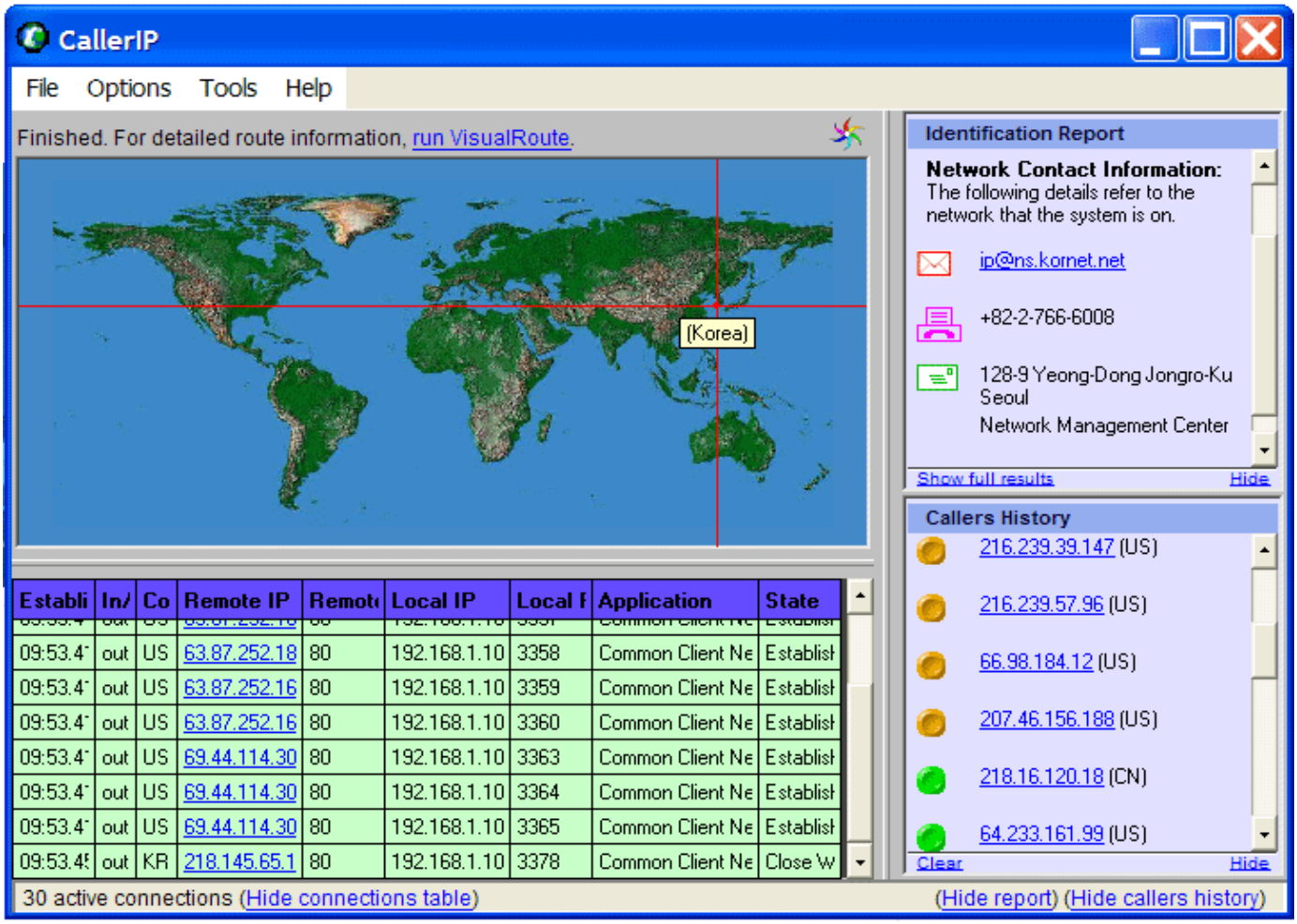

Figura 2 -– Utilização da ferramenta CallerIP
Fonte: http://www.pcdistrict.com/modules/productcatalog/product_images/52764-CallerIP.gif

3.2 RecoverMyFiles

Preço da licença: Standard: $69.95; Professional $99.95 e Technician $299.90.

*Respectivas taxas de manutenção anuais: $19.95; $29.95 e $99.95 [**GETDATA**]*

O RecoverMyFiles (RMF) trata-se de um software destinado à plataformas Windows. De uso bastante intuitivo, o RMF consegue recuperar facilmente arquivos que foram apagados, seja acidentalmente ou não.

A aplicação disponibiliza um filtro que ajuda muito nas buscas/recuperações de arquivos. Pode-se configurar o filtro para encontrar dados em uma determinada extensão, também é possível selecionar a partição que será analisada. Através desses critérios do filtro, o RMF consegue fazer uma busca eficaz, direta e focada.

A figura a seguir está apresentando a tela da aplicação RecoverMyFiles recuperando os dados apagados de uma determinada partição de um HD, que foram deletados acidentalmente ou não de suas supostas pastas, sendo acionado anteriormente a opção de demonstrar somente as pastas deletadas à esquerda e à direita os arquivos destas pastas.

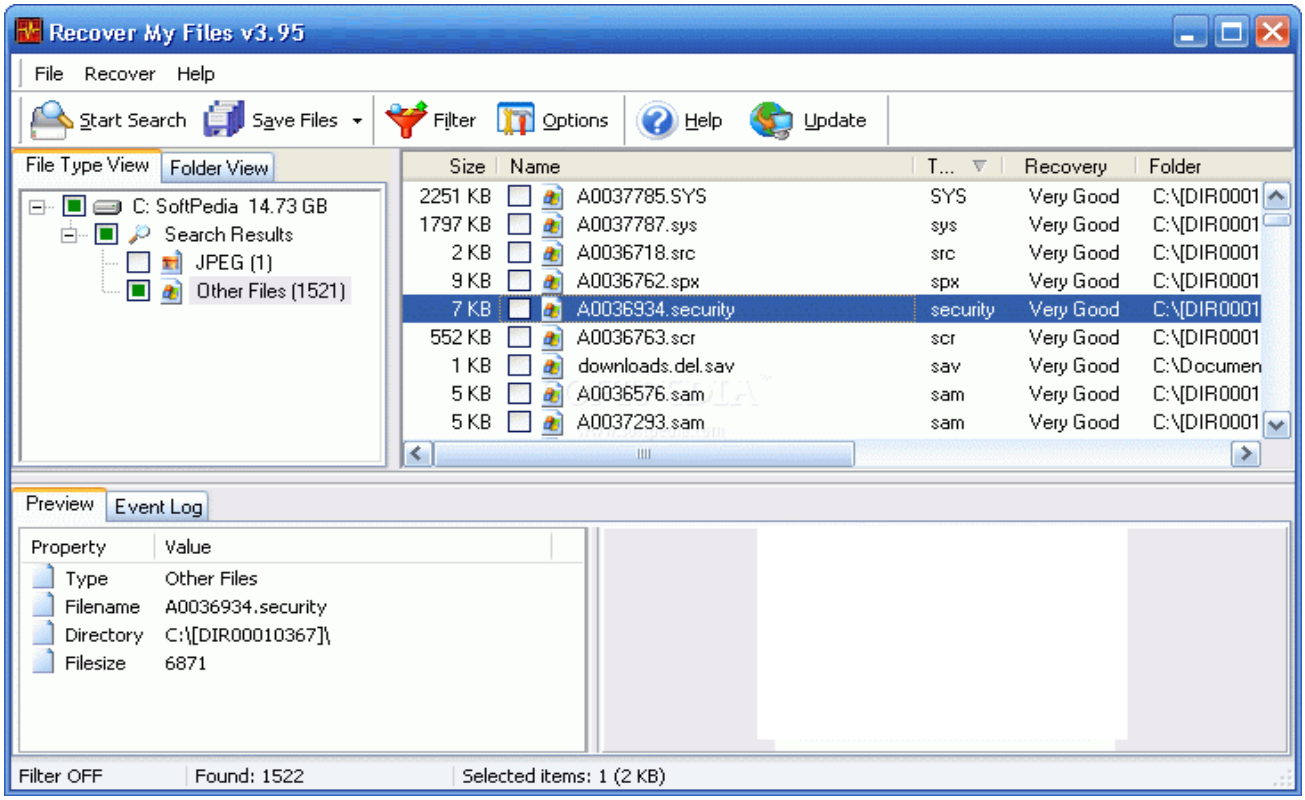

Figura 3 - Utilização da ferramenta RecoverMyFiles
http://i1-news.softpedia-static.com/images/reviews/large/RecoverMyFiles_007-large.png

3.3 SmartWhoIs

*Preço da licença: Um usuário: $39.00; Cinco usuários $195.00; Dez usurários $399.00. [**TAMOSOFT**]*

O software SmartWhoIs (SWI) possui uma funcionalidade quase idêntica ao CallerIP, mas a diferença é que existe um foco maior no domínio da internet.

Após a coleta dos dados, a aplicação consegue disponibilizar dados como endereço, telefone, responsável pelo IP ou pelo domínio em questão, ou seja, praticamente todos os dados mais relevantes de uma determinada organização buscada.

“Exemplo: foi recebido por uma vítima um e-mail chantageando-a, mas este e-mail não contém dados suficientes para informar o remetente, contém somente o IP de domínio do servidor de onde foi enviado este e-mail.

*“O perito pode então, com o auxílio desta ferramenta, verificar o IP de domínio em questão e entrar em contato com o responsável, para poder reaver, mediante pedido judicial a quebra de sigilo de e-mail do mesmo, para poder verificar quem foi que enviou esse e-mail, podendo dar um direcionamento à investigação;” [**VARGAS**, Raffael]*

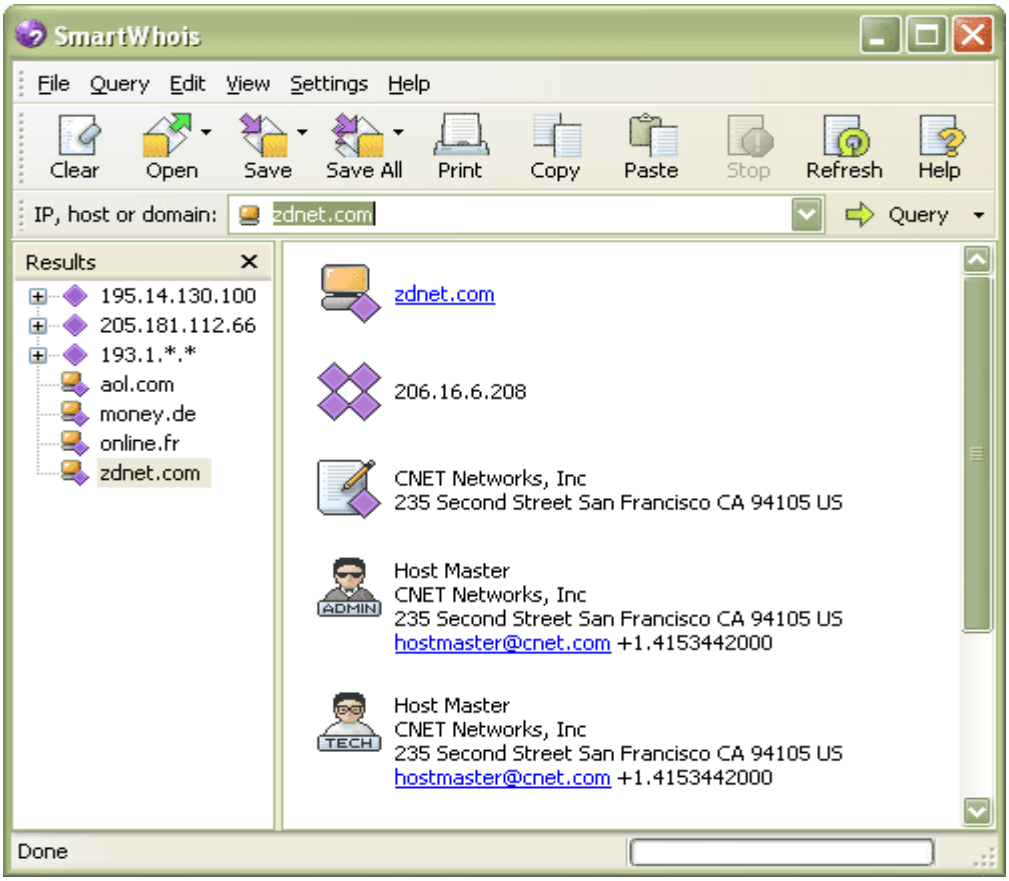

Figura 4 - Utilização da ferramenta SmartWhoIs
Fonte: http://www.logitheque.com/imggif/smartwhois_17987.gif

3.4 E-mailTracker

Preço da licença: (Versão Standard) Varia de um usuário: $29.45 + $41.90 (manutenção anual) até dez usuários: $210 + $294 (manutenção anual).

*(Versão Advanced) Varia de um usuário: $49.95 + $67.95 (manutenção anual) até dez usuários: $300 + $395 (manutenção anual) [**VISUALWARE**]*

Essa aplicação disponibiliza dados a partir de um e-mail ou uma determinada lista de e-mails como o local de origem do e-mail, a rota e a organização em vigor, disponibilizando dados como endereço, telefone, e-mail, entre outros.

*"Exemplo: houve a informação de que o e-mail e informações confidenciais de uma suposta organização foram vendidos antes do mesmo chegar as mãos da empresa responsável por este serviço. Neste caso é utilizada esta ferramenta para fazer uma busca na rota por onde este e-mail passou, informando quando houve o desvio da informação confidencial." [**VARGAS**, Raffael]*

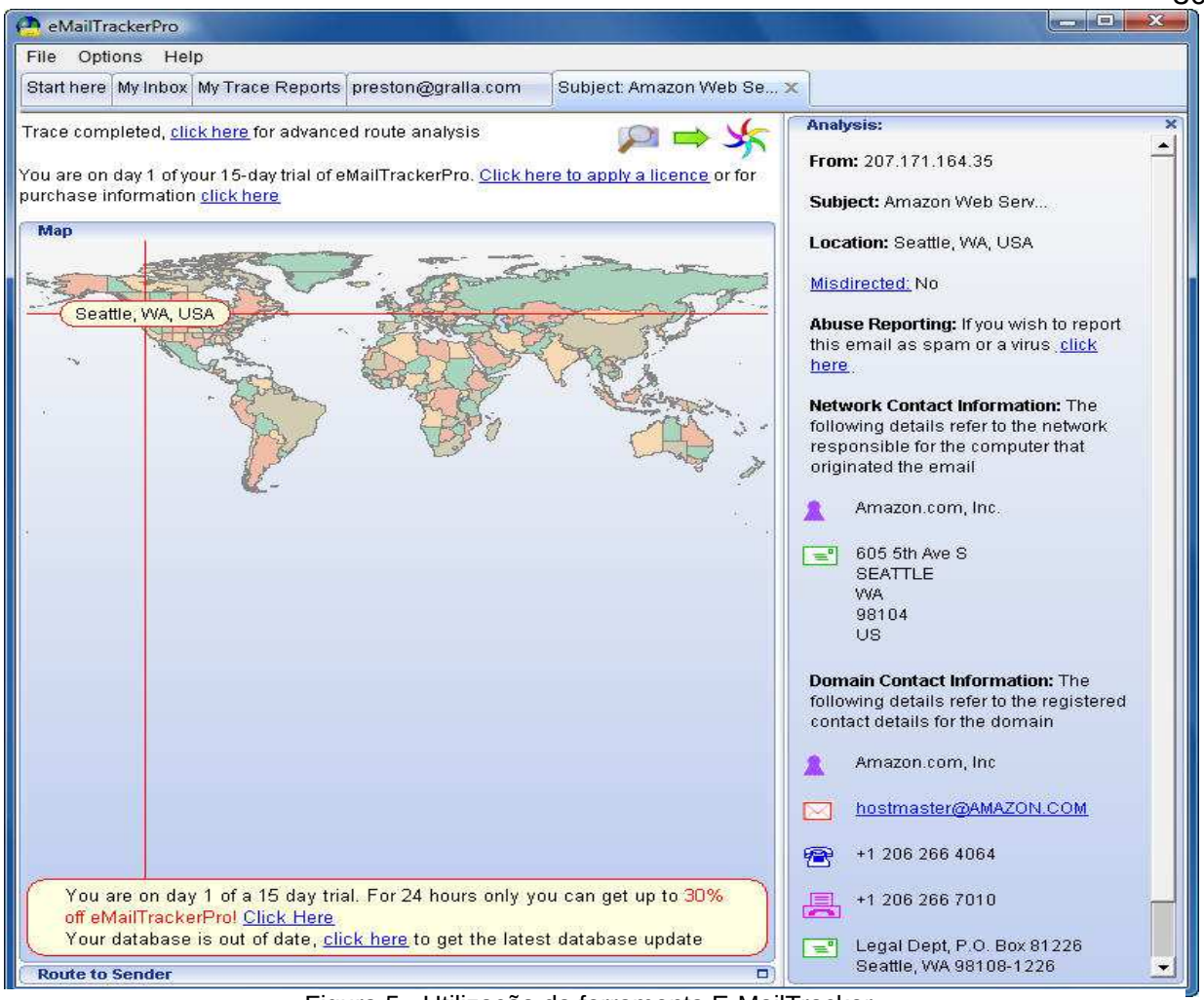

Figura 5 - Utilização da ferramenta E-MailTracker
Fonte: http://idg.bg/test/pcw/2009/1/10/8159-Image8.jpg

3.5 EnCase

*Preço da licença: Aproximadamente $3000 [**GUIDANCE SOFTWARE**]*

No começo do tópico, foi dito que existem softwares forenses para atividades especificas e softwares para atividades em geral. O EnCase com certeza é o melhor exemplo para se citar no quesito de “software geral”. A ferramenta é super completa e fornece vários serviços indispensáveis.

A ferramenta não realiza apenas a recuperação de dados apagados, mas também elabora e padroniza laudos periciais, dispõe organizadamente todas as evidências em um banco de dados, pode fazer a encriptação tal qual a decriptação de dados, faz a análise de hardwares, logs, e-mails, diversos formatos de arquivos.

Além de todos esses fatores, o EnCase também possui um sistema que permite que seja feito o manuseamento das evidências sem risco de danificá-las.

“Ele é baseado em sistemas Windows. O ambiente Windows não é considerado apropriado por muitos profissionais da área para a prática forense, uma vez que ele rotineiramente altera os dados e escreve no disco rígido sempre que é acessado. Mas, o EnCase não opera na mídia original ou discos espelhados, ele monta os Evidence Files como discos virtuais protegidos contra escritas. Então, o EnCase (não o sistema operacional) reconstrói o sistema de arquivos contido em cada Evidence File, permitindo ao investigador visualizar, ordenar e analisar os dados, através de uma interface gráfica.”

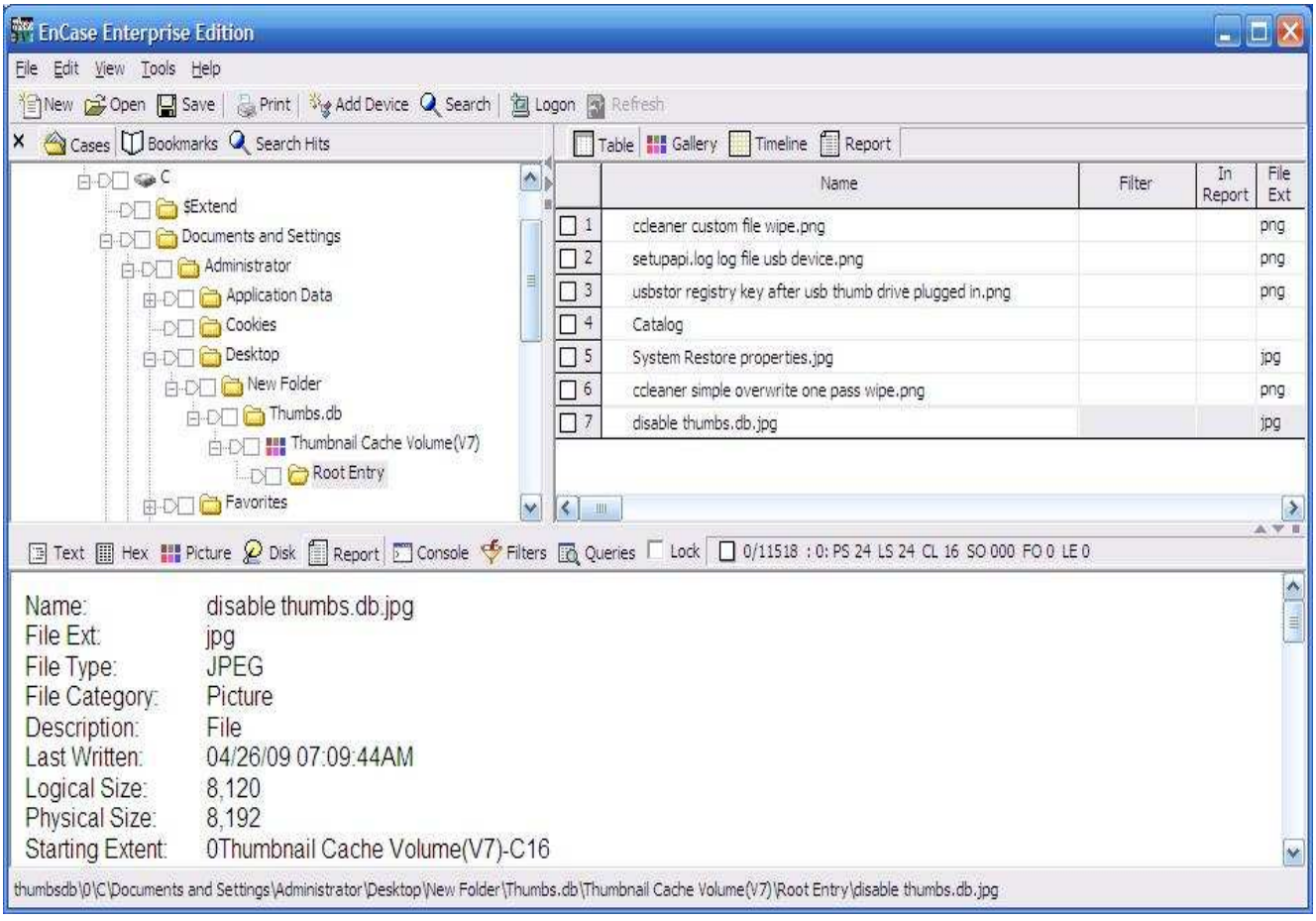

Figura 6 – Utilização da ferramenta Encase
Fonte: http://www.anti-forensics.com/wp-content/uploads/2009/04/encase-thumbsdb-view-file-structure.jpg

3.6 chrootkit

Preço da licença: Software livre

O chrootkit foi desenvolvido em meados de 1997, com a motivação de que os servidores de inúmeras empresas apresentavam os mesmos sinais de invasão, logo, eram encontrados vários vestígios similares.

Essa ferramenta foi desenvolvida visando fácil compreensão e utilização. Assim, a mesma apresenta facilidade na sua instalação. Possui facilidade de compreensão, o que pode ajudar em futuras contribuições alem do fato de ter sido desenvolvido em ferramentas consideradas simples (Posix Shell e C ANSI).

É uma ferramenta de simples portabilidade que faz uma busca local por rootkit instalado e trabalha em tempo real podendo analisar programas em uso, portas e serviços ativos e alguns (Loadable Kernel Module) que estão rodando.

O chrootkit procura por Módulos de kernel maliciosos, cargas binárias corrompidas, pastas e até mesmo processos não confiáveis.

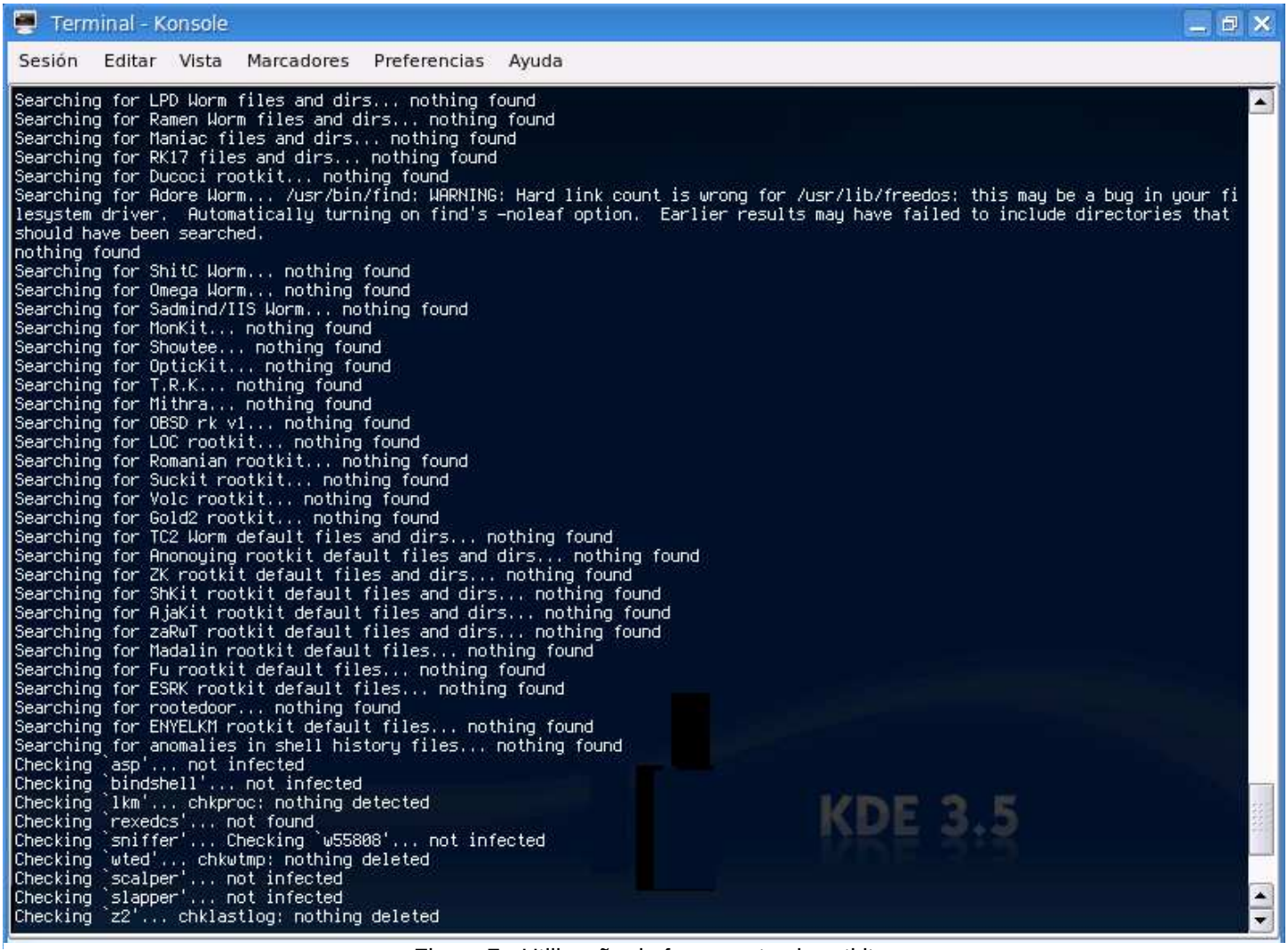

Figura 7 - Utilização da ferramenta chrootkit
http://img.photobucket.com/albums/v63/umaranjum/Feburary/Chkrootkit_en_Linux.png

3.7 Sleuth Kit

Preço da licença: Software livre

Anteriormente conhecido por T@SK - The @stake Sleuth Kit, ele analisa sistemas de arquivos NTFS, FAT, UFS, EXT2 e EXT3.

“Característica marcante é a não-dependência de plataforma. As ferramentas do Sleuth Kit são organizadas em uma abordagem de camadas e o nome de cada programa em uma mesma camada inicia-se com a mesma letra, facilitando a identificação de sua função. Essas camadas incluem o sistema de arquivos como um todo: o conteúdo dos arquivos, as estruturas de dados do sistema de arquivos (inodes, por exemplo) e a interface de interação humana (nomes dos arquivos).”

Segue uma descrição básica dos componentes do Sleuth Kit:

• dcalc: Calcula a posição dos dados existentes numa imagem encontrados no espaço não alocado (obtidos com o dls). É útil quando uma evidência é encontrada no espaço não alocado;

• dcat: Extrai o conteúdo de uma unidade de dados;

• dls: Lista os detalhes sobre unidades de dados, podendo extrair o espaço não alocado ao sistema de arquivos;

• dstat: permite visualizar informações sobre um determinado bloco de dados (incluindo o numero do grupo e se o bloco encontra-se alocado);

• ffind: Encontra nomes de arquivos alocados ou não que apontam para uma determinada estutura de dados;

• fls: Lista nomes de arquivos alocados e apagados de um diretório;

• fsstat: permite visualizar informações detalhadas sobre um sistema de arquivos;

• icat: Extrai unidades de dados de um arquivo, indicado pelo inode (no lugar do nome do arquivo);

• ifind: Encontra a estrutura de metadados cujo nome de arquivo aponta para ela ou a estrutura de metadados que aponta para uma unidade de dados;

• ils: Lista a estrutura e o conteúdo de metadados;

• istat:Mostra estatísticas e detalhes sobre uma estrutura de metadados em um formato de fácil leitura;

• sha1: computa a assinatura criptográfica de um fluxo de bits qualquer.

4 PRÁTICAS 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”, “Backdoors”, “Slack Space” e a curiosa Esteganografia.

4.1 Rootkits

O termo “Root” é usado quando o usuário possui o controle completo da maquina. Logo, o termo “Kit” nos faz entender logo de cara que essa ameaça trata-se de algo como um vírus ou um trojan, destinado a liberar total acesso na maquina do atacado. Esses arquivos são escondidos nos sistemas operacionais de modo que os atacantes possam manusear livremente a maquina do atacado.

No Windows: São infectadas as tarefas e os processos de memória. Isso impede que alguns programas funcionem, visto que o RootKit visa que o sistema não encontre os arquivos necessários para que aquele determinado programa funcione, gerando vários erros.

No Linux/Unix: A infecção ocorre de outra maneira. O Rootkit substitui uma determinada programação de uma “file list”, o que o acaba deixando “escondido” dentro do sistema. Desconhecendo a infecção, o arquivo ficará lá camuflado, permitindo que o atacante use-o da maneira que quiser para acessar a maquina do atacado.

As medidas de prevenção e eliminação são bastante conhecidas, visto que também são aplicadas para vírus, trojans, entre outras ameaças.

Os “RootKits” podem ser proliferados via e-mail, sites mal-intencionados (por exemplo sites “falsos” que copiam o layout de outros sites legítimos) . Abrir um arquivo ou um link infectado pode acarretar várias injúrias como roubo de informações, acesso a arquivos da maquina, etc.

Manter um bom Firewall e um bom antivírus instalados também são medidas básicas, porem de grande ajuda, visto que por vezes elas podem barrar algumas invasões. Anti-Spams também são muito úteis.

Alguns “RootKits” já são detectados pelos antivírus, por isso, foi desenvolvida uma nova forma de infecção. A que ataca diretamente falhas no sistema. Isso acarreta que manter seu sistema operacional sempre atualizado também é uma ótima medida de prevenção.

4.2 Backdoors

Os “backdoors” tem um 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.

Após a infiltração de um “backdoor” o atacante passa a ter controle de inúmeras operações do sistema, como reiniciar o equipamento, ter controle do drive de CD/DVD, ativar periféricos como webcams e microfones, sem que o usuário saiba, conectar-se a outras maquinas que estiverem conectadas na mesma rede que o computador infectado e até mesmo formatar partições.

“O backdoor se caracteriza pelo vírus que contamina a máquina através de um programa e a deixa exposta para uma futura invasão do cracker por acesso remoto. Em muitos casos a utilização do backdoor se faz através de vírus chamados cavalo de tróia. A forma mais comum de você encontrar um cavalo de tróia é pelo seu e-mail, no qual possui aquela mensagem padrão “Olhe as nossas fotos” ao

baixar você pode ter sido infectado sua máquina com um cavalo de tróia que instalará um backdoor."

*Os cavalos de tróia nomeados backdoors levam essa nomenclatura porque após estar no computador da futura vítima facilitam as invasão do pc por uso da internet por portas de rede, dizem que as mais comuns são as portas 3333, 666, 888." [**DANTAS**, Allan]*

Como com os "Rootkits", as medidas de prevenção e eliminação de backdoors também são bastante conhecidas.

Antivírus recentes e atualizados já estão aptos a detectar backdoors, mas sempre devemos recorrer também à utilização de IDS (Intrusion Detection System) e claro, o bom e velho firewall que muitas vezes protege vários "buracos" do sistema, além de fechar portas para possíveis invasões.

4.3 Slack Space

Uma das técnicas mais sagazes, o "Slack Space" trata-se de uma brecha encontrada no final de um cluster de blocos de arquivos dentro do disco. Os dados contidos no disco são compostos por vários clusters de blocos, e entre eles existe esse "espaço". A partir disso que o nome "Slack Space" torna-se bastante sugestivo, pois "Space" imutavelmente significa "espaço", porém o termo "Slack" possui vários sentidos, mas nesse caso, creio que o mais condizente é o termo "folga". Daí é possível compilarmos o termo "Espaço de folga", que logo é interpretado como uma brecha.

Utilizando determinados programas específicos, esse espaço é utilizado pelo atacante para ocultar arquivos. Lembrando que esses arquivos são guardados em blocos considerados "inutilizados" (corrompidos, por exemplo), o que os torna extremamente difíceis de serem encontrados por softwares de busca (desde simples anti-virus até softwares destinados à analise forense).

A maior parte dos softwares de busca não rastreia essas "folgas", o que tornam as informações lá contidas "indetectáveis".

O espaço livre utilizável nos blocos é muito pequeno, por isso, o atacante deve utilizar de ferramentas que possam “fundir” todos os bits, com o objetivo de torná-los um fluxo de informação grande o bastante para que sejam armazenados os arquivos (podendo fazer ligação com “Rootkits”, “Backdoors”, “Sniffers”, vírus, trojans, entre outros tipos de ameaças.).

Dentro do sistema de arquivo NTFS, existem alocações de espaço denominadas ADS (Alternate Data Streams). Presente desde a versão Windows NT 4.0 até as versões mais atuais, o ADS do sistema NTFS permite que dados possam ser inseridos em arquivos já existentes, mas, de uma maneira que comandos de listagem de conteúdo (como o “dir”) não os exibam. Assim sendo, o ADS também entra no conceito de “Slack Space”.

4.4 Esteganografia

Sento talvez a técnica mais curiosa abordada nesse capítulo, esteganografia é uma palavra que vêm do grego. Significa “Escrita Oculta”. 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.

Na área da informática, esses objetos podem ser arquivos de áudio, texto, imagens, HTML, entre outros. São utilizados os bits menos relevantes desses arquivos para executar a esteganografia (técnica conhecida como LSB (Least Significant Bit)). Podem ser ocultados dados como mensagens normais, textos criptografados, anagramas ou até mesmo imagens. Lembrando que a esteganografia é bem mais difícil de ser detectada e desvendada do que arquivos criptografados.

Em arquivos de áudio, por exemplo, quando ouvimos um ruído estranho, podemos estar diante de um caso de esteganografia. A pessoa que esteganografou

o arquivo pode ter inserido uma frase normal, uma frase invertida, ou qualquer outro tipo de informação que possa ser transmitida através de áudio.

“A forma mais comum de esconder informações ainda é através de imagens. Arquivos digitais, de maneira geral, possuem áreas não utilizadas, ocupáveis por informação adicional. Uma imagem é formada por um conjunto de pixels de 8 bits cada um. O pixel é a unidade básica de programação de cor em um display de computador ou em um arquivo de imagem. A cor específica que um pixel descreve é uma mistura dos três componentes do espectro de cores – vermelho verde e azul.

*A idéia é que, alterando-se o bit menos significativo não ocorrem mudanças perceptíveis na imagem. Assim é possível codificar em uma imagem uma seqüência de dígitos binários que contenham um texto usando apenas o bit menos significativo de cada componente (canal) da cor dos pixels.” [**PINHEIRO**, José M. S]*

5 CONSIDERAÇÕES FINAIS

> “Um belo dia, hoje será o passado, e falarão numa grande época e nos heróis anônimos que criaram a História. Gostaria que todo mundo soubesse que não há heróis anônimos. Eles eram pessoas e tinham nomes, tinham rostos, desejos e esperanças e a dor do último de entre os últimos não era menos do que a dor do primeiro cujo nome há de ficar”.
>
> (Testamento sob Força – Júlio Fuchik – ed. Brasil Debates, 1980)

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.

6 REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Citação: NBR-10520/ago - 2002. Rio de Janeiro: ABNT, 2002.

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.