EDIÇÃO ESPECIAL DE ANIVERSÁRIO – 7 ANOS

Evidência Digital

Magazine

Edição 05

2011

EDITORIAL

Amigos,

Nesta edição de Comemoração falaremos bastante sobre Forense, há ótimos artigos que valem a pena conferir.

Relacionei também nesta edição o Curso de Pós-graduação Lato Sensu em Perícia Digital da Universidade Católica de Brasília.

Gostaria de agradecer a todos os colaboradores que enviaram seus artigos para a conclusão desta quinta edição e aos participantes do grupo Perícia Forense Aplicada à Informática.

Estou ao seu dispor para ouvir seus comentários e sugestões!

Boa leitura a todos!

Andrey Rodrigues de Freitas
Editor da Revista Evidência Digital

Editor
Andrey R. Freitas

Colaboradores
Andrey R. Freitas
Marcelo Caiado
Luiz Senna
Paulo Barbosa
Fernando Fonseca
Igor Silva
Raffael Vargas
Marcos Bueno
Rhafael Costa

Artigos
Se você deseja escrever artigos para a Revista Evidência Digital envie um e-mail para
periciaforense@yahoo.com.br

Site
http://www.guiatecnico.com.br

Grupo de discussão
http://br.groups.yahoo.com/group/PericiaForense

Investigando Vazamento de Informações e de Propriedade Intelectual

A proteção da informação e um dos temas que mais se ouve falar quando se referencia os principais ativos de uma empresa. Não obstante, constantemente tem sido erroneamente tratada como sinônimo de segurança em tecnologia da informação. O equivoco decorre do fato de que algumas vezes o tratamento da segurança da informação se baseou em uma tomada de decisão onde aspectos não tecnológicos não foram considerados e que áreas afetadas podem não ter sido consultadas na decisão

Na miríade de informações que circulam em uma empresa, e que pode ser realizada de diversas formas diferentes, uma tomada de decisão conjunta da Tecnologia da Informação com as áreas envolvidas, e com o devido respaldo e amparo da alta administração, deve ser a base para a definição de qual informação precisa ser protegida e qual o nível desejado.

Por outro lado, mesmo com a adoção de políticas e todas as devidas salvaguardas possíveis (criptografia, gestão de identidade e acesso – IAM, detecção e filtragem de conteúdo - SCM, prevenção de perda de dados - DLP, etc.), sempre haverá o risco de vazamento de informação confidencial.

Com um número cada vez maior de sítios de Internet dedicados a divulgar informações de propriedade intelectual, a quantidade de localidades a serem monitoradas por empresas que correm o risco de vazamento de informações e divulgação indevida de propriedade intelectual aumenta vertiginosamente. Bloggers, twikers, fórums, comunidades virtuais e páginas da Internet integram uma infinidade de localidades onde podem-se encontrar informações estratégicas que vazaram de uma empresa (Figura 1).

Figura 1 - Exemplos de sites onde se podem encontrar informações confidenciais

Considerando que uma vez disponível na Internet qualquer informação pode ser disseminada rapidamente entre diversas localidades, é fundamental a adoção de um processo que permita

a rápida identificação no instante em que ocorre o vazamento e a publicação de informações confidenciais.

Um procedimento muito bem detalhado, com a alocação de recursos humanos que sejam responsáveis por tal execução e que tenham ciência de todo o ciclo do processo é o ponto mais crítico para uma resposta adequada.

Para a devida contenção, uma estratégia de verificação de vazamento de informações em endereços conhecidos e pesquisas por palavras-chave e pessoas de interesse que seja semanal, diária, de hora em hora ou automática deve ser definida pelo gestor da informação.

A chamada técnica de Google Hacking apresenta-se como uma ferramenta auxiliar nas investigações, e até mesmo na descoberta de vulnerabilidades em diversos sistemas. A utilização de operadores booleanos contribuirá para uma maior precisão no resultado obtido em uma pesquisa na Internet, diminuindo a sobrecarga de páginas a serem inspecionadas. O uso do Google Alerts é também uma alternativa (Figura 2).

As aplicações peer-to-peer (P2P), como por exemplo Limewire, também devem ser consideradas ao se determinar se há algum material confidencial disponível na Internet. Para tal as pesquisas devem considerar o nome da empresa, além daqueles relacionados com a propriedade intelectual. Deve-se observar que a opção de compartilhamento de arquivos deve ser mantida desabilitada.

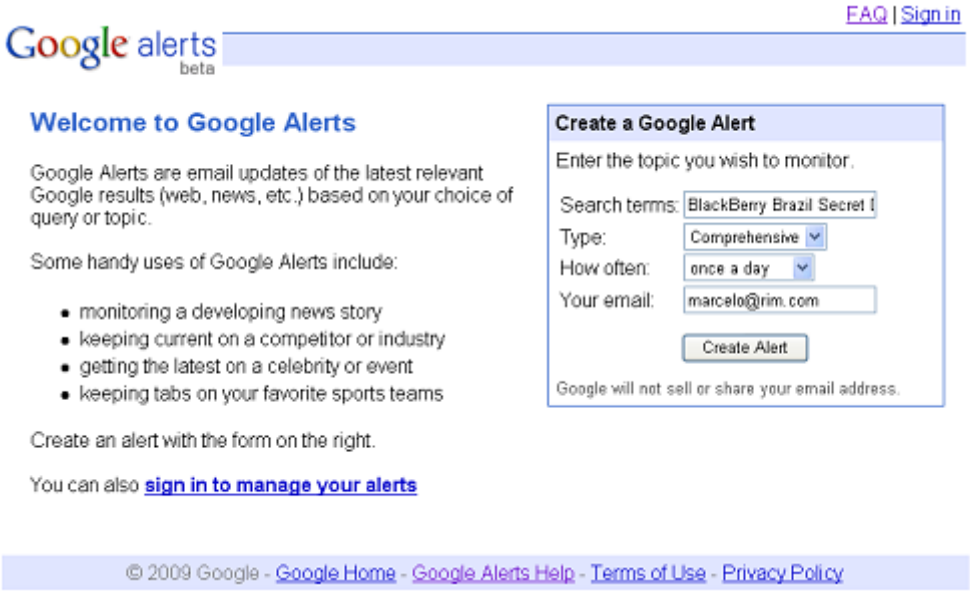


Figura 2 - http://www.google.com/alerts

Addict-o-matic é um sítio de meta-busca que poderá auxiliar no processo de pesquisa em diversos locais ao mesmo tempo, incluindo: Google Blog; Twitter; Youtube; Digg; Delicious Tags; Flickr; Technorati; Wordpress; Wikio; entre mais de 20 fontes diferentes de notícias, blogs, vídeos e imagens (Figura 3).

Para uma monitoração exclusivamente de conteúdo publicado no Twitter, uma alternativa é o uso do http://monitter.com.

Serviços de monitoração focados na proteção da integridade de uma marca ou companhia e de análise de mídias sociais estão sendo oferecidos por diversas empresas e podem auxiliar nessa monitoração. Nesse sentido um estreito canal entre a área de segurança da informação

com a área de comunicação/relações públicas da empresa é fundamental. Infelizmente esses são serviços não muito acessíveis para a maior parte das pequenas e médias empresas.

Uma vez identificada a publicação indevida e a confirmação de que se trata de fato de propriedade intelectual, o primeiro passo é armazenar localmente uma cópia da publicação e/ou arquivo(s). A utilização de programas como SnagIt ou HTTrack permite que sítios inteiros sejam salvos e incluam-se os links existentes. Além disso, o perfil do autor também deve ser armazenado, caso esteja disponível, bem como outras páginas que sejam referenciadas na publicação.

O armazenamento de alguma foto que esteja publicada deve ser realizado de forma que se preservem as características originais da mesma, pois pode haver valiosos metadados associados a imagem. Programas como Microsoft Pro Photo Tools e Irfanview auxiliam na visualização de metadados EXIF (Exchangeable Image File Format), que podem incluir informações como a data e a hora em que foto foi tirada, a marca, o modelo e o numero de serie da câmera utilizada, o programa utilizado na edição da foto, e ate mesmo a localização geográfica (GPS) e o nome do autor da foto, entre diversos outros tags (Figura 3).

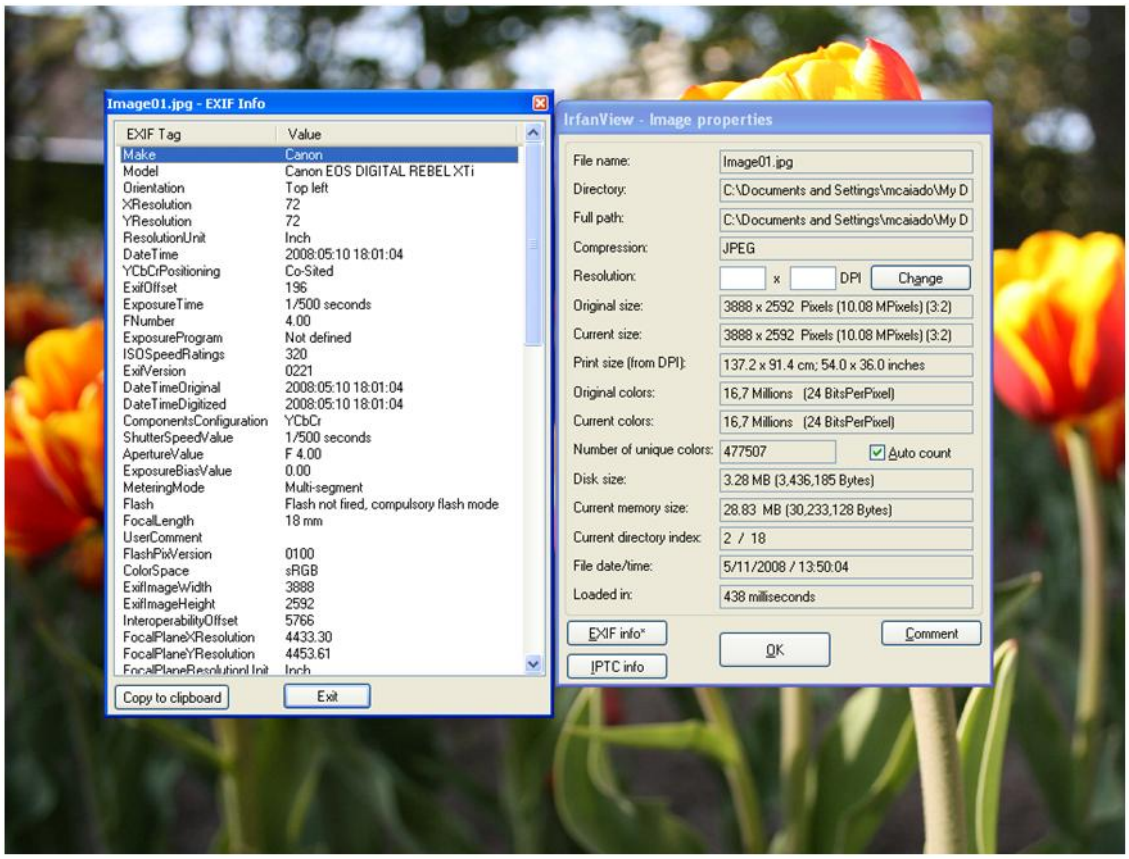


Figura 3 - Informações EXIF armazenadas em uma foto

Outros formatos de metadados como XMP (Extensible Metadata Platform) e IPTC - IMM (International Press Telecommunications Council - Information Interchange Model) também devem ser investigados.

Ademais, deve-se observar a importância de executar um hash nos arquivos salvos, como garantia de sua integridade, o que pode ser realizado com vários programas publicamente disponíveis como HashCalc e Md5summer.

Em muitos casos quando se utiliza um programa de Hash tradicional, não é possível determinar-se uma equivalência exata do arquivo indevidamente publicado com o original, devido ao fato de ter havido alguma modificação no mesmo, desde a remoção de alguma parte de um vídeo ou a alteração em alguma parte no código binário de um programa executável, resultado do efeito avalanche.

Um programa como o SSDeep, que utiliza o conceito de Context Triggered Piecewise Hashes (CTPH), pode auxiliar na identificação de possíveis candidatos a original quando houve alguma alteração neste. Ao contrário dos programas de hash tradicionais, onde em função do efeito avalanche muitas vezes não é possível determinar-se uma equivalência do arquivo indevidamente publicado com o original, o SSDeep permite que arquivos que tenham tido alguma modificação, desde a remoção de alguma parte de um vídeo ou a alteração em alguma parte no código binário de um programa executável, possam ser eleitos como prováveis candidatos.

A utilização do serviço de pesquisa de registros DNS do sítio www.robtex.com também poderá auxiliar na identificação de outros sítios relacionados, os quais porventura tenham republicado a postagem inicial e que podem, até mesmo, auxiliar na identificação do autor da publicação (Figura 4).

Figura 4 – Pesquisa de um registro DNS em www.robtex.com

Finalmente, caberá ao departamento jurídico, que deve ser imediatamente comunicado quando da detecção inicial, decidir se deve ou não realizar uma Ata Notarial da referida publicação; se deverá contactar o autor da publicação e/ou o administrador do sítio para a imediata remoção da página; assim como definir se será dado prosseguimento a quaisquer ações jurídicas que irão depender também da jurisdição da localidade onde se encontra a publicação.

Marcelo Caiado, M.Sc.
CISSP, MCSO

Possui mais de 15 anos de experiência em TI, e mais de 7 anos em Segurança da Informação.

Trabalhou como professor em cursos de graduação e pós-graduação por 6 anos e atuou como palestrante em diversos seminários e conferências.

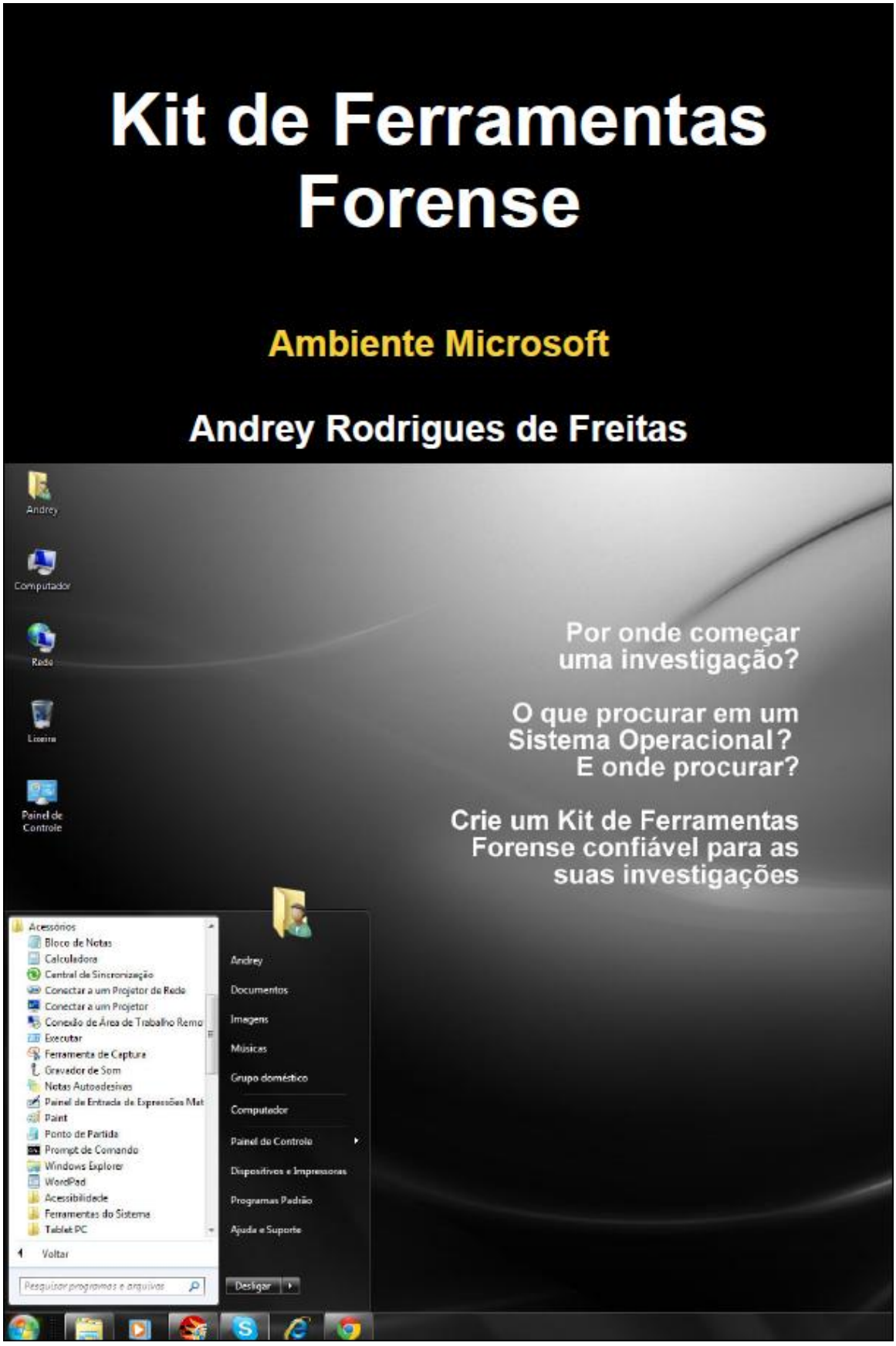
É membro da High Tech Crime Investigation Association – Chapter Ontario e da International Systems Security Association - Chapter Toronto.

Pode ser contactado no email **br2can@gmail.com**

Lançamento do Livro

Kit de Ferramentas Forense

Ambiente Microsoft



Kit de Ferramentas Forense
Ambiente Microsoft

Por onde começar uma Investigação Forense? O que procurar em um Sistema Operacional invadido? Ou melhor, onde procurar? Para responder a estas perguntas dividi este livro em sete tópicos:

Kit de Ferramentas

Conjunto de softwares confiáveis usados na investigação.

Iniciando uma Investigação

Neste tópico estão os passos iniciais de toda investigação.

Investigando o Sistema

Será através deste tópico que você aprenderá a identificar quais processos estão em execução e quais portas estão abertas no SO, a analisar arquivos de logs, a investigar o registro do Windows, compartilhamentos etc.

Investigando os Usuários

Quem está conectado ao sistema neste momento? Quem logou ou tentou logar no computador recentemente? Descubra quem são os usuários que utilizam ou utilizaram o equipamento.

Investigando os Arquivos

Recupere arquivos excluídos, investigue arquivos na lixeira, descubra arquivos temporários, ocultos e impressos.

Investigando os Vestígios de Acesso à Internet

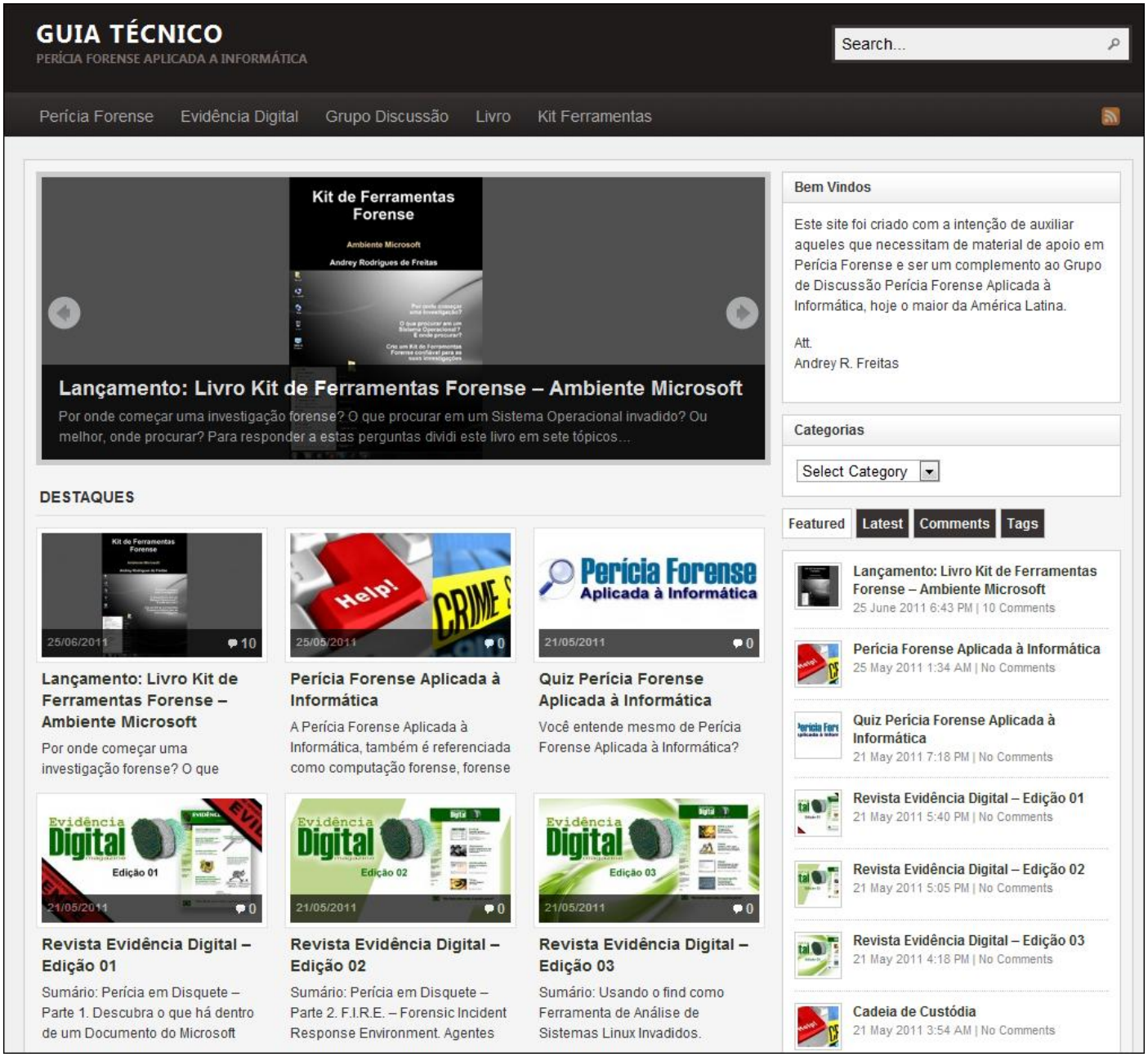
Descubra quais sites foram acessados pelo suspeito, identifique os arquivos temporários da Internet, analise o histórico e o item favoritos do browser.

Finalizando uma Investigação

Neste último grupo estão os passos finais de uma investigação. Capture a data e hora do final da perícia, documente os comandos utilizados e garanta a integridade das evidências.

Sumário

Para mais informações sobre o livro acessem
http://www.guiatecnico.com.br/gt/?p=170



Hoje em dia nunca se ouviu falar tanto em segurança, e principalmente nos meios eletrônicos de segurança da informação. E que informação é esta? São os nossos principais ativos, os principais e mais importantes negócios que possuímos e temos dentro de nossas Empresas. Produtos, documentos, lançamentos, idéias, softwares, hardwares, títulos, nossos Backups e nossa contabilidade.

Nunca houve uma necessidade tão imperiosa de adotarmos uma política de segurança para nossas empresas, e isso abordando todos os seus setores. Desde os mais "simples" como a recepção como ao pessoal de TI (tecnologia da informação), ao pessoal de desenvolvimento de software (programação), ao controle de qualidade.

Devemos lembrar sempre que é pela recepção que as ligações para nossa Empresa são recebidas, e filtradas. Se nossos funcionários; funcionarias não estiverem aptos e treinados e conscientes de fato do perigo que é fornecer esta ou aquela informação ao telefone.

Já temos ai um caminho que por mais simples que aquela informação pareça, ao conhecimento de um engenheiro social (a) ela será um peça para ele (a) formar ou pelo menos, começar a forma o seu plano de "ataque" de "invasão" a política de segurança deve hoje abordar todos os aspectos da área de segurança da informação. E o fator humano continua a ser o fator que mais falha nestes aspectos.

Primeiro hoje é muito importante para nossas Redes, principalmente aquelas que funcionam 7/24, ou seja, 7 (sete) dias por Semana e 24(vinte e quatro horas por dia) serem monitoradas por um conjunto de programas (softwares). Digamos a tríplice coroa da Segurança: 1 – Firewall, 2 – Antivírus 3 – IDS (intrusion detection system (ferramentas de detecção de intrusão). Lembro que se ambas estas ferramentas, este conjunto indispensável não estiver devidamente configurado e atualizado, sem deixar de lado a atualização de Patchs, para o S.O (sistema operacional) seja ele Windows, Linux Mac Os X ou outro. Estaremos cooperando para a nossa própria "destruição".

Windows XP Professional sem SP2 é suicídio, sem atualização é genocídio para a Empresa, e sem se habilitar somente os serviços do sistema indispensáveis e necessários, levando em consideração um número excessivo de portas de comunicação abertas: (65.535) já que já são (sessenta e cinco mil e quinhentas e trinco e cinco portas) temos que levar em consideração que as nossas Redes somente devam responder a ping(s) internos (intranet) e estarem fechadas com o protocolo de ICMP (internet control message protocol) configurado para não responder a ping de fora da Rede interna, ou seja, os que vêm pela Internet.

O administrador de Rede deve tomar o cuidado de fechar portas como: 5631 que pode ser pesquisada pelo PCAnywhare (symantec) e que por ser uma ferramenta comercial, o Firewall não acusará como deveria fazê-lo, a 5632 é te pior, pois ela trabalha com os dois protocolos: TCP/UDP e o mesmo programa pode efetuar um Scan nesta porta.

As portas 5800 e 5900, respectivamente são usadas por outro software bem conhecido e comercial, o VNC, isso pode propiciar ao invasor; vantagens desagradáveis sobre nós. No ótimo livro de Stephen Northcutt: Como detectar invasão em rede – um guia para analistas. O mesmo descreve o perigo de se deixar aberta à porta 161, que segundo o mesmo, e eu confirmo esta informação é um prato para sofrermos algum dos inúmeros tipos de ataque e invasão por parte de Crackers e Script Kiddies, que todos os dias tentam desta ou daquela forma penetrar em nossos sistemas.

Esta porta trabalha com TCP/UDP e deve de fato ser isolada da Internet, a importância mais que vital de se não abrir anexos desconhecidos em nossas caixas postais, mesmo sabendo da origem "idônea" do E-mail, o mesmo vindo com um arquivo anexado. O mesmo deve ser scaneado pelo AV (antivírus) atualizado,

de preferência com a sensibilidade do seu Scanner elevada ao máximo. Mesmo assim somente em Máquinas virtuais devemos abrir anexos, pois existem maneiras de se alterar o tamanho e nome de um arquivo para que ele burle o Antivírus, e o Firewall, e outras ferramentas indispensáveis que devemos todos possuir e atualizar sempre.

Refiro-me aos antispyware e antitrojan que com o Antivírus e o Firewall, nos mantém com certa dose de segurança ao navegarmos na grande rede mundial de computadores e gozarmos de suas imensas Benesses.

Vamos nos manter sempre atentos ao quesito segurança sempre nos atualizando, lendo sobre ele, e mantendo nossas redes de preferência dentro de um perímetro de DMZ (zona desmilitarizada) usar mais de um Firewall e usar roteadores que possuam tecnologia NAT (para mascararem nossos IP(s) da rede interna) para fora dela para que na Internet tenhamos o cuidado de saber lidar com profissionalismo e seriedade que cada vez mais lhe são devidas, desde um Download, Upload, FTP ou mesmo enviar e receber um E-mail, lembremos-nos da Cidade de Tróia. Que aceitou um "presente" que lhe custou sua total destruição. Lembre-se o Backup em fitas DAT, mídia magnética e mesmo CD (s) podem e devem guardar e salvar os nossos principais ativos, principais documentos e mais sigilosos e importantes dados da Empresa.

Luiz Senna
Analista e Consultor de Segurança

http://www.guiatecnico.com.br

A Etologia é a ciência que estuda o comportamento comparado dos animais. Os etólogos estão interessados em poder distinguir quais comportamentos são herdados geneticamente e quais padrões motores são compreendidos por cada comportamento.

Existem muitos exemplos de animais (principalmente primatas) que aprendem a resolver problemas para os quais não tem nenhum conjunto de padrões motores herdados. Eles aprendem. Agem criativamente em seu ambiente.

Por outro lado, existem comportamentos com tal hierarquia que impressionam pela precisão ao acontecerem, e os etólogos experientes já estão tão acostumados a eles que podem prever todo um comportamento quando os primeiros sinais, os primeiros padrões motores, começam a surgir.

Conta-se que Lorenz, um dos iniciadores da Etologia, podia prever se os patos que ele estudava iriam voar mesmo ou estavam apenas "imitando" o movimento de pré-vôo. Cada comportamento tem padrões motores específicos. Alguns comportamentos só disparam em situações determinadas. Um gorila macho Alfa (o chefe do bando) só terá sua autoridade confrontada em contextos bem definidos: como doença ou incapacidade senil.

Entre os animais sociais, porém, são muitos os exemplos de comportamentos baseados no que nós chamamos manipulação. A manipulação e o engodo fazem parte da natureza dos animais sociais. Oferecer ajuda, esconder recursos, descobrir recursos escondidos, fazer alianças (e também falsas alianças) e exercer autoridade são comportamentos biologicamente programados e estão presentes também em nossa espécie por um simples motivo: a sobrevivência.

Talvez seja esse o motivo pelo qual despendemos tanta energia tentando fazer as pessoas viver em sociedade, orientados por conceitos democráticos com o "bem da maioria". Nossas ações precisam de um retorno vantajoso pessoal. Quando uma cultura é criada e utilizada para atrofiar toda e qualquer ferramenta biológica para descobrir o engodo, e.g. acreditar que o outro é bom, e onde a crença substitui a percepção, temos o campo de ação do engenheiro social.

Engenheiro social é qualquer indivíduo que utiliza as facilidades de uma sociedade "ingênua" e orientada por regras para alcançar objetivos pessoais. Ele nos faz acreditar que atua conforme as regras, mas não o faz, o que só percebemos no final do processo, quando já não há mais tempo. Nós substituímos a percepção pela crença.

Aqui entra o principal vilão da história.

Os lingüistas dizem que nossa compreensão não passa disso, nossa compreensão. Ou seja, agimos em toda e qualquer situação com as representações que temos armazenadas em nosso sistema nervoso. Essas representações são ampliadas ou modificadas pela aprendizagem (experiência), quando há necessidade de aprender algo novo, quando as situações não nos desafiam, as velhas informações são úteis e servem.

Se eu digo para um técnico de TI, para um auxiliar de escritório e para um vigilante que eles vão receber treinamento em segurança da informação, muito provavelmente, não necessariamente, o técnico pensará em firewalls, antivírus, roteadores e etc. O auxiliar de escritório em crachás, cadeados nos armários e papel picotado. O segurança, bem, ele pode pensar em anotar nomes, etc.

Todos estão certos, até um ponto. Quando eles fazem sua parte em segurança da informação, eles estão respeitando o princípio sanitário (no sentido manicomial da palavra) da "necessidade de não saber" sobre todas as áreas da empresa. Além daquele ponto... eles estão errados por desrespeitarem o princípio da "necessidade

de saber" dialogar com os outros setores da empresa. Ou seja, saber qual impacto uma ação levada a cabo numa área terá em outras.

Um cenário prático

99% das empresas disponibilizam por telefone informações de setores importantes. Quem atende ao telefone diz o nome do Diretor de TI, Marketing, Financeiro etc. Eles dão o ramal, informam se o gerente está de férias e quando retorna. Existe Diretor Financeiro que dá número de celular de gerente de TI por telefone. Eles não pensam nos riscos, no valor das informações. Como isso é possível? Basta que o engenheiro social crie um cenário (mental) que iluda o funcionário e leve-o acreditar em uma situação como vantajosa para ele (o funcionário).

Imagine o seguinte cenário:

-Engenheiro Social: "Alô.. Quem fala?"
-Vítima: "Com quem quer falar?"
-E S: "É a secretária do Dr. Gilberto?"
-V: "Sim."
-E S: "Oi, Como é mesmo o seu nome?"
-V: "Beatriz."
-E S: "Oi Beatriz, aqui é o Afonso, gerente de TI."
-V: "Oi, tudo bem?"
-E S: "Tudo, O Dr. Gilberto está de férias, não é?"
-V: "Sim."
-E S: "Pois é, ele mencionou que está com um problema no antivírus do computador dele e eu estou super atarefado aqui fazendo a instalação de um servidor novo, sabe o trabalhão que dá..."
-V: "Hmm."
-E S: "Eu estava pensando se você pode passar aqui no cpd e pegar o disquete com o antivírus e instalá-lo, é bem fácil."
-V : "Sei, mas eu não posso sair daqui assim..., você não pode mandar alguém aqui, ou eu mando um boy, ou sei lá...."
-E S: "É, boa idéia, o boy de vocês está por aí?"
-V : "Vou ter que ver."
-E S : "Espera, eu tive uma idéia. É claro, por que não pensei nisso antes?"
-V : "O quê?"
- E S: "Ora, é claro, eu posso te mandar isso por e-mail, então você usa um disquete, a atualização é bem pequena, abra seu e-mail, baixe o programa e grave no disquete. Depois, salva do disquete para o computador do Dr. Gilberto."
-V : "Pode ser."
-E S: "Qual é o seu e-mail?"
-V : "abc@mail.com"
-E S : "Bommm..., Tchau, obrigado viu".
-V : "Que isso, não foi nada."

Claro que foi. E através dessas situações podemos perceber como o investimento em segurança da informação realizado de maneira restrita impossibilita a redução das ameaças de engenharia social. Para essas situações, de que adianta a empresa possuir uma sala-cofre, servidores em cluster ou o mais caro firewall do mercado? Ou alguém duvidaria que um bom engenheiro social não conseguiria descobrir quais as portas de comunicação que são "liberadas" pelo firewall? Podemos ir além: seria o engenheiro social capaz de persuadir o administrador do firewall a abrir alguma dessas portas? Nós acreditamos que sim.

Claro que esses cuidados são muitas vezes necessários. Muitos recursos tecnológicos disponíveis no mercado são extremamente eficientes para o seu propósito. Mas o que ocorre nas empresas é um grande

investimento nesse tipo de controle e nada, ou quase nada, nos cuidados necessários para evitar as práticas de engenharia social.

Um dos modos pelos quais entendemos as mensagens é por pressuposição. Elas criam e reforçam as alucinações que temos sobre o mundo.

Imagine o nosso engenheiro social do cenário anterior percebendo que sua vítima começou pouco cooperativa, utilizando-se de autoridade e lançando mão de uma ferramenta lingüística, ele diz: "Bom, você me manda um e-mail dizendo que não quis instalar o programa para que eu possa mostrar para o Dr. Gilberto quando ele voltar e ver o computador cheio de vírus".

A representação criada com a ajuda do engenheiro social força a pessoa não cooperativa a cooperar.

Veja bem. Mandar um e-mail assumindo que você não fez o que alguém com autoridade pediu, pressupõe que você levará toda a culpa. E "quando o Dr. chegar" pressupõe que ele irá chegar (o que a secretária sabe), e pior, ele achará o computador infectado.

Se a funcionária fosse treinada em técnicas contra engenharia social, o mínimo que ela faria seria transferir a responsabilidade para outra pessoa, alguém para ajudá-la a tomar uma decisão acertada. Para isso ela deve ter aquela sensação peculiar de "algo errado acontecendo". O alarme mental tem que tocar. E isso só ocorre com muito treinamento.

Controle as ameaças

O treinamento é elemento indispensável para evitar que práticas de engenharia social sejam efetivas nas empresas. O ideal é que treinamentos sejam ministrados quando da contratação de funcionários e reforçados periodicamente. Além disso, os treinamentos podem ser organizados de acordo com as funções dos funcionários da empresa, uma vez que o contato com pessoas e o acesso a informações sensíveis são diferentes entre as diversas funções na organização.

Adicionalmente aos treinamentos, diversos outros cuidados podem ser tomados, entre os quais podemos citar:

- Política de Segurança da Informação: padronizando as práticas de segurança necessárias para proteger informações e recursos da organização.
- Classificação de Informações: possibilitando a identificação da sensibilidade de cada informação e viabilizando o tratamento adequado destas, considerando sua criação, armazenamento, transmissão e descarte.
- Processo de desligamento de pessoal: garantindo que seu acesso será negado, tanto para o acesso físico quanto para o lógico.
- Revisão das informações disponíveis (site internet, intranet, etc): reduzindo a possibilidade de que informações sejam utilizadas para forjar uma identidade que será utilizada para buscar a cooperação da pessoa da qual deseja-se obter certa informação.
- Uso de crachá: possibilitando a identificação de pessoas, restringindo sua circulação em ambientes onde informações importantes podem ser facilmente acessíveis.
- Centralização do fornecimento de informações em pessoas especialmente treinadas para identificar e lidar com engenharia social.

Com a aplicação destes cuidados, sua empresa estará apta a gerenciar os riscos relacionados à engenharia social, reconhecidamente a maior das ameaças ao seu negócio.

Paulo Barbosa
prbarbosa@gmail.com

Venha fazer parte você também do único grupo de discussão em português sobre "Perícia Forense Aplicada à Informática"

http://br.groups.yahoo.com/group/PericiaForense/

* Análise de Invasão em Sistemas
* Ferramentas (Software/Hardware)
* Análise de Arquivos de Logs
* Testes de Conhecimentos
* Estudos de Caso
* Cyber Crimes
* Documentos
* Cursos
* Livros...

Por um bit: Explicando o Hash

Tenho percebido em algumas palestras que quando estou explicando conceitos sobre tecnologias como a verificação de integridade de código (Code Integrity Checking) do Windows Vista, verifico que as pessoas que não pertencem à área de segurança não entendem bem o conceito de HASH, por isso pensei em postar uma dica interessante, com um exemplo prático sobre como funcionam os hashes.

Um hash é um número único gerado através de um algoritmo de mão única, ou seja, através de um arquivo se gera o hash mas através do hash não se recompõe o arquivo que o gerou. Este método é muito utilizado para verificar se arquivo e senhas estão íntegros, sua utilização mais comum é em senhas e assinaturas digitais. Em sistemas como Windows e Unix, ao invés de se armazenar a senha do usuário, estes sistemas fazem um hash destas senhas e os armazena em seus bancos de dados.

Quando o sistema precisa validar se a senha que um usuário inserir para acessar o sistema é verdadeira, ele passa a senha digitada pelo mesmo algoritmo e verifica se o resultado foi o mesmo que o armazenado em seu banco de dados.

Uma outra aplicação para o Hash é a conferência de arquivos em programas Peer-to-Peer com o Emule.

Estes programas não conferem se estão lidando com o mesmo arquivo pelos atributos como nome ou tamanho, eles usam o hash para se certificarem que estão buscando blocos do mesmo arquivo em várias fontes.

Uma vez que os computadores só entendem números, cada caractere representado em um documento tem um valor numérico correspondente. Na tabela ASCII (American Standard Code for Information Interchange), a mais comumente utilizada em microcomputadores, a letra "A" é representada para o computador pelo número 65, a letra "B" pelo 66, e assim em diante. No exemplo a seguir utilizaremos um utilitário da Microsoft chamado "Microsoft File Checksum Integrity Checker" para mostrar como um único Bit alterado pode mudar todo o sentido de um arquivo, e como isso gera um Hash completamente diferente.

O primeiro passo para minha demonstração foi criar um arquivo chamado testehash.txt com apenas uma frase: "Lula é o presidente do Brasil". Imaginemos que por alguma ironia do destino, este arquivo teve o bit menos significativo do primeiro byte do texto alterado de 0 para 1, mudando o valor do byte de 76 (01001100) para 77 (01001101). Após este infeliz acidente, a letra "L" virou um "M", e a referência feita ao nome do presidente da república, cargo máximo da nação e reservado a pessoas da mais alta inteligência e capacidade, passa a referenciar um animal geralmente associado à falta de inteligência e teimosia. Vejamos o exemplo abaixo com o arquivo original:

C:\Teste>fciv -sha1 testehash.txt
//
// File Checksum Integrity Verifier version 2.05.
//
bdd7cb36458bb8c0a0f9406bff47107b06abb50d testehash.txt

Agora com o arquivo depois de "corrompido"

C:\Teste>fciv -sha1 testehash.txt
//
// File Checksum Integrity Verifier version 2.05.
//
0b6ca609eefec6e3ec8e74613adb87539ab11e67 testehash.txt

Notem que por um Bit os hashes foram totalmente alterados:

Lula é o presidente do Brasil ☐ bdd7cb36458bb8c0a0f9406bff47107b06abb50d
Mula é o presidente do Brasil ☐0b6ca609eefec6e3ec8e74613adb87539ab11e67

Embora o texto não tenha sofrido uma alteração significativa, vemos uma radical diferença no hash. Este exemplo demonstra que podemos utilizar o hash para verificar se um arquivo foi recebido da forma como deveria, ou se sofreu alguma modificação proposital, pois se um bit for alterado o Hash não será o mesmo.

Este processo vem se mostrando muito útil no processo de assinatura digital e na verificação de alteração dos arquivos do sistema operacional, que quase sempre tem a intenção de se alterar o funcionamento do mesmo para executar uma ação desejada pelo invasor. Este processo é chamado de instalação de um rootkit.

Existem ferramentas como o Tripwire que armazenam o hash de todos arquivos importantes para o sistema operacional em um banco de dados criptografado e comparam diariamente com o hash obtido dos arquivos no momento da comparação, desta forma qualquer modificação nos arquivos será detectada, gerará um alerta e ficará registrada. O Windows Vista faz essa verificação automaticamente, no momento da inicialização.

Uma outra aplicação para o Hash é a conferência de arquivos em programas Peer-to-Peer com o Emule. Estes programas não conferem se estão tratado do mesmo arquivo pelo nome ou tamanho, eles usam o hash para se certificarem que se trata do mesmo arquivo ao buscá-lo de várias fontes

Espero que esta forma "lúdica" tenha demonstrado como funciona o hash. Isso já nos dá uma base para discutir mais a fundo a verificação de integridade de código (Code Integrity Checking) do Windows Vista e outras tecnologias semelhantes.

Referências Bibliográficas

Wikipedia (Tabela ASCII) – http://pt.wikipedia.org/wiki/ASCII

Checksum Integrity Verifier – http://www.microsoft.com/downloads/details.aspx?FamilyID=b3c93558-31b7-47e2-a663-7365c1686c08&DisplayLang=en

Fernando Fonseca
fernando@fernandofonseca.info

Poderíamos escrever centenas de páginas sobre esta função, mas o assunto já ficou bastante cansativo (e muito tecnológico, por tendência).

Vamos fazer diferente, hoje vamos falar um pouco sobre o Ser humano que ocupa esta função. Sim, é um Ser humano e não uma máquina.

Tive um Insight numa noite dessas, quando saia da Pós. Este um pouco mais desenvolvido, mas parecido com um outro que tive há cerca de uns 05 anos atrás.

Tecnologia, Processos, Pessoas. Hmmmm... Pessoa, Ser humano.
O elo mais fraco de Segurança... Por enquanto.

Pensei: Tecnologia, processos, leis, gestão, modelos e outros.

Será que todos ao saírem com seus supostos diplomas, estarão prontos para lidar também com pessoas? E com o conhecimento, competências, comunicação, informação e toda aquela parafernália "política" de uma grande ou ainda uma gigante organização?

Complicada questão? Nem um pouco. Só a ponta de um Iceberg.

Imagine um Ser humano que deve possuir maestria para harmonizar e direcionar os aspectos de segurança em uma organização, ter fluência em qualquer tipo de comunicação, conhecer o negócio e objetivos dela, tecnologias, tendências, lutar com o orçamento (sempre comprometido a usá-lo sabiamente), se relacionar bem com as áreas, conhecer o fator humano, conhecer o humano e suas competências.

Seus colaboradores.
Sim. Ele também gerencia e se relaciona com pessoas a todo o momento.
Papel difícil? Não é difícil porque não apontei todos os itens desta missão.
Poucos itens e um pouco além de Tecnologia, Processos e Pessoas. Mas relaxem.
Nada é impossível. Tenha sempre uma alternativa!
Hoje, a grande maioria dos profissionais que ocupam esta função é oriunda de TI.

Não vejo isto como um mal. Porém não mais me assusto com a atitude de alguns. Afinal, lidaram com 0 e 1 uma boa parte de sua jornada profissional.

Estamos acostumados a presenciar cenas, como o dialogo abaixo:

- Olá? Tem um minuto? (Project Consultant)
- Não. (Security Officer)
- Sabe o projeto XYZ daquela empresa NASA? Precisamos reduzir...
- Não.

Quase uma clean-up rule (Any – Any – Any – DROP).

Um Firewall Officer na frente de um computador?

Não. Somente um Ser humano com algumas faculdades ainda não desenvolvidas lidando com um outro Ser humano. Capacidade de se comunicar, de ouvir.

"Quando não há alternativas, há apenas uma mentalidade fechada."
Peter Drucker – O melhor de Peter Drucker – O Homem

Para balancear conheço (e aplaudo) alguns profissionais que possuem não somente visão ampla, mas são capazes de lidar com todos ou grande maioria dos aspectos que envolvam segurança, negócios, comunicação e conhecimento. Pessoas.

Estes são Polivalentes, na era do conhecimento. Anos Luz da versão anterior.

"As pessoas eficazes procuram primeiro entender.
Só depois é que analisam quem está certo e quem está errado."
Peter Drucker – O melhor de Peter Drucker – O Homem

Intrigado e ao mesmo tempo curioso, comecei a estudar sobre o assunto.

Comecei com uma pergunta básica (e aconselho a quem for seguir, começar do básico).

Quem sou eu?
Com isto, conheça para conhecer outros. O conhecimento gera e traz novos conhecimentos.
Assim iremos alcançar um objetivo comum.
Uma sociedade voltada ao conhecimento em evolução continua.

É evidente que não poderia deixar de aplaudir e parabenizar todos os profissionais, aqueles movidos pelo conhecimento multidisciplinar, que de alguma maneira fazem seu papel diário e estão comprometidos com o crescimento pessoal e de seus semelhantes a sua volta.

Parabéns para a unida InfoSec do País.

E voltando à questão inicial:

Embora todos os itens de uma missão quase impossível, aspectos que para alguns já são visíveis e para outros só imagináveis...

Security Officer é sim, um Ser humano.

Igor Silva
Sr. Information Security Analyst
volcov@gmail.com

Perícia Forense Computacional Metodologias e Ferramentas Periciais

Introdução

Atualmente os setores básicos da sociedade vêm se adequando ao modelo que dizem ser parte de um mundo virtual, mas que não passam de um mundo real com diferentes ferramentas e novos paradigmas de relacionamento humano, que dependem de sistemas computacionais para um funcionamento consistente e confiável.

A conectividade oferecida pela Internet também introduziu uma série de novas facilidades no dia-a-dia das pessoas, como por exemplo: os *games on-line*, transferência de arquivos e a própria *World Wide Web*, permitindo assim acesso a qualquer tipo de informação disponível nos *sites*. Portanto, não é de se espantar o fato de que essa revolução computacional tenha atingido também o mundo do crime.

Nesse artigo, serão discutidas algumas metodologias na fase de aquisição de evidências, até a apresentação judicial, independente do sistema operacional. O objetivo é expor algumas técnicas e aspectos que devem ser considerados durante uma análise forense, a fim de evitar a dependência de elementos de software e metodologias que não sejam livres.

Para isso, está organizado em cinco seções além desta introdução. A seção 2 define uma metodologia para obtenção de evidências com um comentário sobre o profissional forense e suas principais características. Na seção 3 são apresentadas as principais fontes de informação dentro de um computador. A seção 4 apresenta algumas ferramentas periciais utilizadas no mercado. Já na seção 5 são apresentadas as considerações finais e, por fim, tem-se as referências bibliográficas utilizadas.

Forense Computacional

A Forense Computacional é uma área de pesquisa relativamente recente e são poucos os trabalhos sobre este assunto no Brasil, entretanto é crescente a necessidade de desenvolvimento nesse sentido, haja visto que a utilização de computadores em atividades criminosas é cada vez mais comum.

De acordo com Freitas (2006) a Forense Computacional é o ramo da criminalística que compreende a aquisição, prevenção, restauração e análise de evidências computacionais, quer sejam os componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais. A padronização e a quantidade de metodologias na área de Forense Computacional são ainda insuficientes considerando-se a grande demanda de aplicações, de acordo com Ubrich e Valle (2005).

Na Figura 2.1 é apresentado um modelo proposto por Ubrich e Valle (2005), que procede de uma estrutura hierárquica de duas classes multiníveis (Aspectos Legais e Aspectos Técnicos).

Na classe dos Aspectos Legais encontram-se as exigências legais, baseadas na área de Direito, às quais devem estar sujeitos os procedimentos periciais. Já a classe dos Aspectos Técnicos corresponde às questões práticas da área computacional.

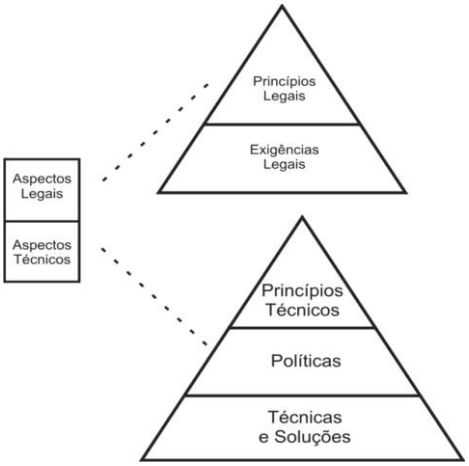


Figura 2.1: Modelo de padronização (UBRICH e VALLE, 2005)

Metodologia Forense para Obtenção de Evidências

Diariamente há diversos tipos de casos de fraudes e crimes onde o meio eletrônico foi em algum momento utilizado para este fim, sendo este tipo de caso chamado, de acordo com Ubrich e Valle (2005), de *CyberCrime*. A missão da perícia forense é a obtenção de provas irrefutáveis, que irão se tornar o elemento chave na decisão de situações jurídicas, tanto na esfera civil quanto criminal.

De acordo com Adams (2000), atualmente já existem padrões metodológicos bem definidos e desenvolvidos pelo SWGDE (*Scientific Working Group on Digital Evidence*), que é o representante norte-americano na *International Organization on Computer Evidence* (IOCE). Tais padrões foram apresentados durante a *International Hi-Tech Crime and Forensics Conference* (IHCFC), realizada em Londres, de 4 a 7 de outubro de 1999.

Esses padrões seguem um único princípio: o de que todas as organizações que lidam com a investigação forense devem manter um alto nível de qualidade a fim de assegurar a confiabilidade e a precisão das evidências. Esse nível de qualidade pode ser atingido através da elaboração de SOPs (*Standard Operating Procedures*), que devem conter os procedimentos para todo tipo de análise conhecida e prever a utilização de técnicas aceitas na comunidade científica internacional, apresentadas a seguir.

Obtenção e Coleta de Dados

Os procedimentos adotados na coleta de dados devem ser formais, seguindo toda uma metodologia e padrões de como se obter provas para apresentação judicial, como um *checkList*, de acordo com as normas internacionais de padronização, citadas acima.

Um exemplo de *checkList* adotado na obtenção e coleta de provas pode ser encontrado no *site* da Comissão Européia (2004).

Identificação

Dentre os vários fatores envolvidos no caso, é extremamente necessário saber separar os fatos dos fatores, que possam vir a influenciar ou não um crime, para estabelecer uma correlação na qual se faz um levantamento das ligações relevantes como datas, nomes de pessoas, autarquias, etc, dentre as quais foi estabelecida a comunicação eletrônica.

Preservação

Um Perito Forense Computacional experiente, de acordo com Kerr (2001), terá de ter certeza de que uma evidência extraída deverá ser adequadamente manuseada e protegida para se assegurar de que nenhuma evidência seja danificada, destruída ou mesmo comprometida

pelos maus procedimentos usados na investigação e que nenhum vírus ou código malicioso seja introduzido em um computador durante a análise forense. Além do mais, qualquer informação sigilosa e privativa que seja inadvertidamente obtida, durante uma análise e que não fizer parte do objetivo da investigação, deverá ser eticamente e legalmente respeitada e não divulgada.

Análise

Na concepção de Kerr (2001), a análise será a pesquisa propriamente dita, onde o investigador se detém especificamente nos elementos relevantes ao caso em questão pois todos os filtros de camadas de informação anteriores já foram transpostos.

Novamente, deve-se sempre ser um profissional atento e cuidadoso em termos da obtenção da chamada "prova legítima", a qual consiste numa demonstração implacável e inquestionável dos rastros e elementos da comunicação entre as partes envolvidas e seu teor, além das datas e trilhas dos segmentos de disco utilizados.

Apresentação

De acordo com Freitas (2006) esta fase é tecnicamente chamada de "substanciação da evidência", pois nela consiste o enquadramento das evidências dentro do formato jurídico, sendo inseridas, pelo juiz ou pelos advogados, na esfera civil ou criminal ou mesmo em ambas. Desta forma, quando se tem a certeza material das evidências, atua-se em conjunto com uma das partes acima descritas para a apresentação das mesmas.

O investigador precisa estar perfeitamente sintonizado com os objetivos de cada etapa metodológica apresentada na seção 2.1, para poder minimizar o tempo e a quantidade de dados que deve desde obter até apresentar, maximizando sua eficiência e eficácia. Isso pôde ser averiguado nesta seção como indispensável para melhores resultados.

O Profissional

Para caracterizar um investigador, também chamado perito, pode-se enfatizar algumas observações importantes sobre sua personalidade e seus princípios. O bom profissional tem de ser antes de tudo uma pessoa de boa conduta, sendo conhecedor dos princípios básicos do direito, de sigilo e privacidade, além de ter conhecimento e entendimento profundo das características de funcionamento de sistemas de arquivos, programas de computador e padrões de comunicação em redes de computadores, noção sobre psicologia dos atacantes, seus perfis de comportamento e motivações que os levam a realizar um ataque.

Com o avanço da tecnologia o profissional deverá ter familiaridade com as ferramentas, técnicas, estratégias e metodologias de ataques conhecidos, inclusive as que não se têm registro de ter ocorrido, mas que já são vistas como uma exploração em potencial de uma determinada vulnerabilidade de um sistema.

Este terá de ter conhecimento das diretivas internas das empresas e instituições envolvidas no processo investigativo, com especial atenção às limitações como diretivas de privacidade, sigilo e escopo ou jurisdição de atuação, sendo uma pessoa que está sempre atualizada com os acontecimentos globais, novas tecnologias, *softwares* e aplicações *hackers*.

Fontes de Informação

A busca de indícios em um sistema computacional inicia-se com uma varredura minuciosa das informações nele contidas, seja em arquivos ou em memória, dados "deletados" ou não, cifrados ou possivelmente danificados.

De acordo com Adams (2000) existem três tipos de espaços, no computador, que podem conter informações valiosas para uma investigação, que serão detalhados no decorrer do trabalho:

- **Espaço de arquivos lógicos:** refere-se aos blocos do disco rígido que, no momento do exame, estão atribuídos a um arquivo ativo ou à estrutura de contabilidade do sistema de arquivos (como as tabelas FAT ou as estruturas *inode*);

- **Espaço sub aproveitado:** espaço formado por blocos do sistema de arquivos parcialmente usados pelo sistema operacional. São listados nesta categoria todos os tipos de resíduo de arquivos, como a memória RAM e os arquivos sub aproveitados;

- **Espaço não-alocado:** qualquer setor não tomado que esteja ou não em uma partição ativa.

Para fins de ilustração, os dados de um disco rígido foram divididos em camadas parecidas com as do modelo de rede OSI (KUROSE e ROSS, 2003). Encontram-se informações com valor de provas em todas essas camadas.

A Tabela 1 apresenta a localização em determinados sistemas operacionais da alocação de evidências nas camadas de arquivos do sistema. Isso ajuda a determinar o tipo de ferramenta a ser usada para extrair as informações.

Camada do Sistema de Arquivos	Localização de Provas em DOS e Windows	Localização de Provas em Linux
Armazenamento de Aplicativos	Arquivos	Arquivos
Classificação de Informações	Diretórios e pastas	Diretórios
Alocação de espaço de armazenamento	FAT, NTFS	Inode e Bitmaps de dados
Formato de Blocos	Clusters	Blocos
Classificação de dados	Partições	Partições
Fisica	Setores Absolutos ou C/H/S	Setores Absolutos

Tabela 1: Camada de armazenamento de arquivos do sistema (FREITAS, 2006)

De acordo com Adams (2000), em alguns casos, a perícia objetiva responder alguns quesitos pré-estabelecidos, como, por exemplo, "descrever o conteúdo das mídias enviadas para o exame", mas muitas são as fontes de informação para uma análise forense em um sistema computacional. Dentre elas, citam-se as listadas a seguir:

Sistemas de Arquivos

Representando a maior fonte de informação para o exame forense, os arquivos de dados e executáveis são analisados para se determinar seu conteúdo e funcionalidade no sistema computacional, sendo procurados indícios por palavras-chave, imagens, dados específicos ou programas utilizados para práticas ilícitas.

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

Arquivos de Logs

Estes também representam um papel importante na análise do sistema de arquivos, pois permitem a reconstituição de fatos que ocorreram no sistema computacional, podendo registrar entre outras informações as atividades usuais e não usuais dos usuários, dos

processos e do sistema, as conexões e atividades de rede, podendo variar de acordo com o sistema operacional e serviços utilizados.

O arquivo de *log* serve para a indicação de ações em um determinado sistema operacional ou de alguma aplicação. Um exemplo de arquivo *log* é o arquivo que contém o histórico dos registros das páginas visitadas por um usuário no acesso a *web*.

Espaços Não Utilizados no Dispositivo de Armazenamento

Estes espaços podem ser caracterizados, na concepção de Freitas (2006) como:

- Espaços não alocados dentro do sistema de arquivos;
- Espaços alocados a arquivos, mas não totalmente utilizados (chamados de *file slacks*)
- Área de dispositivo de armazenamento que não constituem uma partição de disco ou que não contém um sistema de arquivos;
- Arquivos e diretórios excluídos.

Esses espaços podem conter indícios de algum ato ilícito e devem ser investigados.

Arquivos Temporários (*temp*)

Descrito no trabalho de Freitas (2006), alguns programas de processamento, desde o de texto até os que manipulam banco de dados, criam arquivos temporários nos diretórios durante sua execução. Esses arquivos são apagados automaticamente ao final da sessão de trabalho e como podem conter indícios de atos ilícitos deverão ser investigados.

Setor de *Swap*

Segundo Freitas (2006), o gerenciamento de memória do sistema operacional utiliza o setor de *swap* como uma grande área de armazenamento temporário de arquivos, que pode ser descarregados momentaneamente na memória principal, podendo ser tanto um arquivo quanto uma partição inteira do disco. Logo, este setor poderá conter alguma prova de algum ato ilícito e esta deve ser também investigada.

Setor de *Boot*

Este setor trabalha na inicialização do sistema operacional, sendo possível, se modificado, carregar qualquer outro tipo de programa durante a inicialização do computador, de acordo com Freitas (2006). Exemplo: inserção de uma instrução no *boot* que irá inicializar algum tipo de ocorrência maliciosa no sistema operacional. Logo é importante também para o investigador a análise do setor de *boot* do computador periciado.

Memória

A memória contém informações voláteis do sistema, que ainda não foram gravadas em disco. De acordo com Freitas (2006), tais informações podem ser acessadas por meio de dumps da memória ou pela geração de *core files*. Exemplo: *buffer* de impressora, área de transferência de arquivos.

Periféricos

Na concepção de Freitas (2006), são quase todos os dispositivos, implantados ou não, em um computador, que obtém memória, sendo esta temporária ou não. Exemplo: impressoras, pendrives, scanners, etc.

Ferramentas Periciais

Com o advento e desenvolvimento da tecnologia nos últimos anos, as infrações, invasões, pirataria, tentativas de acessos indevidos a organizações ou até mesmo a pessoas comuns vêm se sofisticando e, com isso, há a necessidade do auxílio de ferramentas mais modernas e mais incrementadas para a busca destes infratores.

Com esse grande avanço os peritos forenses computacionais necessitam de uma metodologia de padronização, desde a obtenção de evidências, passando pela padronização de laudos até a apresentação das mesmas perante a justiça, por isso serão apresentadas e exemplificadas a seguir três tipos de ferramentas que podem ser úteis em seu trabalho diário.

Smartwhois

Criada pela Tamasoft, empresa especializada no ramo de segunrança de informação, a ferramenta *SmartWhois* auxilia na verificação de IPs e de domínios na Internet. Para isso, basta digitar a indicação do IP ou domínio da organização desejada e a ferramenta apresenta na tela a localização da empresa correspondente aos dados digitados no sistema, seu endereço, telefone e nome do responsável pelo IP ou pelo domínio em questão.

A Figura 4.1 ilustra a tela de abertura do *SmartWhois*. O usuário indica qual o domínio ou o IP que se deseja investigar (nesse caso "zdnet.com") e a ferramenta retorna todas as informações deste domínio ou IP. É uma ferramenta de muita utilidade quando se deseja, por exemplo, investigar uma determinada correspondência eletrônica que omite os dados do remetente. Para isto basta digitar o endereço do IP do servidor que a ferramenta auxiliará na busca de todos os dados necessários na identificação do remetente.

eMailTracker

Criada e distribuída pela empresa Visualware, a ferramenta *eMailTracker* fornece através de uma entrada de um *e-mail* ou uma lista de *e-mails,* o local de origem, onde fora criado este *e-mail*.

Esta ferramenta também disponibiliza a rota entre as empresas que de alguma forma, utilizaram este *e*-mail e a organização responsável pelo *e-mail*, que será identificada com a apresentação de seu endereço, telefone, dentre outros dados.

Na Figura 4.2 está sendo apresentada à esquerda a rota de um determinado *e-mail* por IPs e a rota do mesmo no mapa mundi, enquanto que à direita está sendo indicada a empresa responsável pelos serviços de *e-mail*. Pode-se utilizar esta ferramenta quando se deseja, por exemplo, investigar se as informações confidenciais de uma suposta organização foram vendidas antes mesmo de chegar "às mãos" da empresa responsável por este serviço. Neste caso, faz-se uma busca da rota por onde este *e-mail* passou, informando quando houve o desvio da informação confidencial.

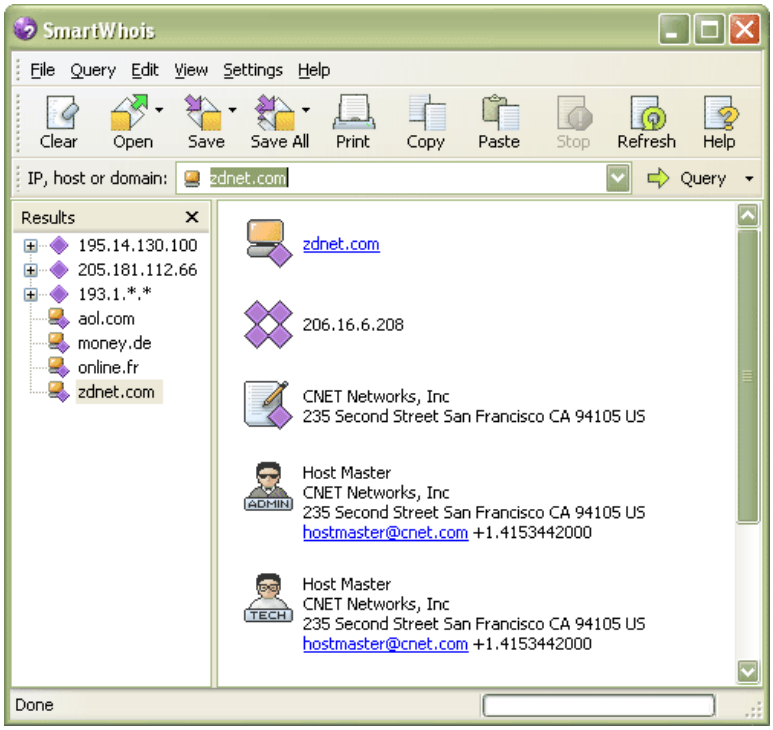


Figura 4.1: Tela principal da ferramenta *SmartWhois* (TAMOSOFT, 2007)

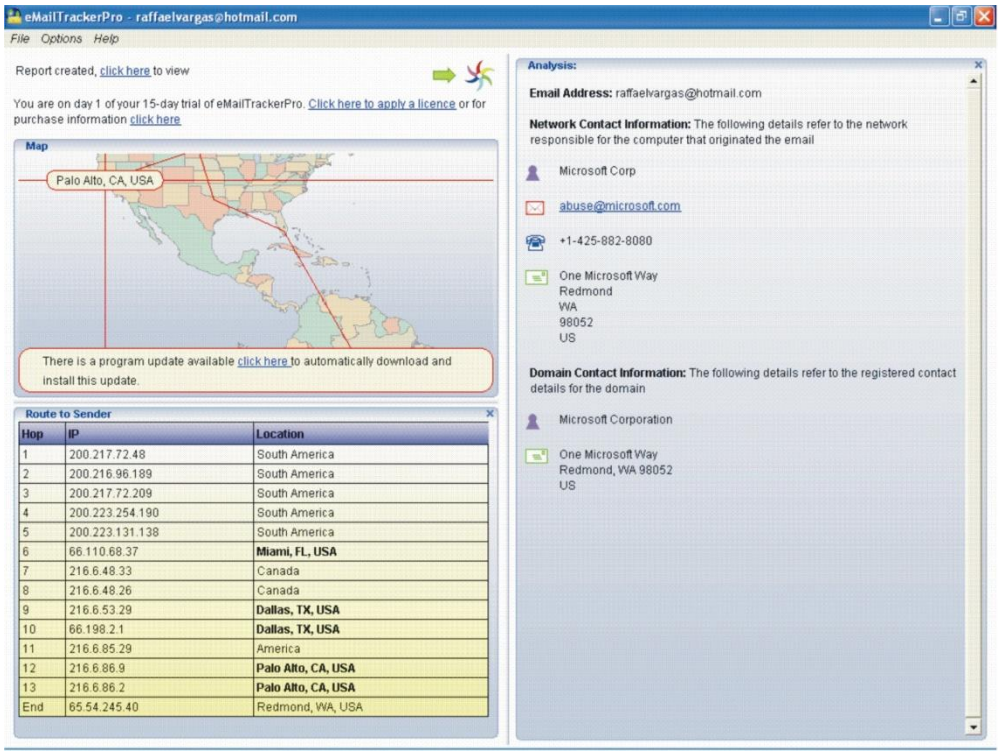


Figura 4.2: Tela Principal da Ferramenta *eMailTracker* com Rota de IPs

EnCase

A ferramenta *EnCase*, criada e patenteada pela empresa Guidance Software, que é diretamente ligada ao setor forense computacional, é uma das ferramentas mais completas no que se refere à perícia forense, pois além de auxiliar na recuperação de arquivos excluídos, padroniza laudos periciais, organiza um banco de dados com as evidências, faz o *encryption* (fornece senhas do arquivo) e o *decryption* ("quebra" as senhas do arquivo) dos arquivos, analisa hardwares, analisa *logs*, analisa formatos e tipos de *e-mails* e fornece uma opção de se manusear a evidência sem danificá-la, além de outras características.

A Figura 4.3 ilustra uma verificação da caixa de entrada de *e-mail*, utilizando métodos de busca e investigação da ferramenta *EnCase* em *e-mails.* Pode-se utilizar esta ferramenta quando se deseja, por exemplo, investigar os dados em um computador que foram excluídos ao se formatar logicamente a máquina.

Nessa situação, a ferramenta pode auxiliar o perito na busca de dados nos setores não utilizados do HD e logo após fazer uma busca em todos os *e-mails* enviados à suposta vítima, podendo com esta ferramenta recuperá-los, mesmo se estiverem em uma área que foi formatada (ANDRADE, 2005).

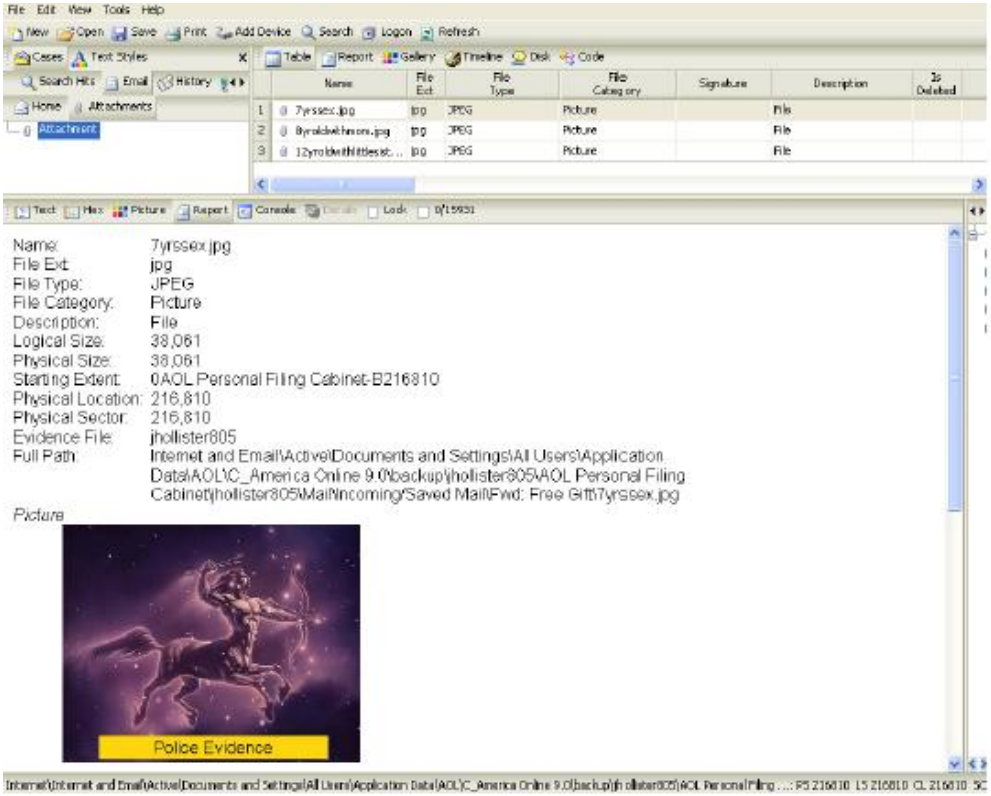


Figura 4.3: Tela do EnCase com visualização dos anexos de *E-mail* (ANDRADE, 2005)

Considerações Finais

A aplicação minuciosa de técnicas investigativas na computação forense é, sem dúvida, muito semelhante às técnicas de perícias investigativas utilizadas em crimes convencionais. De a cordo com uma metodologia criada pela SWGDE é possível conhecer as características do ambiente de trabalho e entender o ambiente forense computacional como a cena de um crime, por isso há a necessidade de seguí-la como forma de aperfeiçoar o trabalho pericial.

A grande abrangência da atividade forense computacional em diversas áreas que envolvem segurança computacional traz complexidade aos trabalhos a serem realizados na investigação de cada caso. A pesquisa necessária em busca de informações a respeito de forense computacional merece especial atenção no que diz respeito a sistemas em plataforma Windows, devido à escassez de informações sobre os detalhes de funcionamento em outros sistemas operacionais.

A compreensão de cada camada de observação em um caso de investigação forense computacional ficou mais clara conforme se deu o desenvolvimento teórico e prático da pesquisa e aplicação de práticas forenses A forense computacional está se fazendo cada vez mais presente e cada vez menos dispensável pelos motivos apresentados neste trabalho sobre o histórico acelerado de crescimento da base

de atividades computacionais nas relações humanas.

A validade técnica e jurídica das metodologias para recuperar dados de computadores envolvidos em incidentes de segurança tem se tornado fundamental, pois os procedimentos têm que ser tecnologicamente robustos para garantir que toda a informação útil como prova seja obtida e também de uma forma a ser legalmente aceita de forma a garantir que nada na evidência original seja alterado, adicionado ou excluído.

Devido à globalização dos crimes digitais é fundamental que sejam feitos, em cada país, esforços constantes a respeito de legislação local, nacional e internacional em conjunto com a padronização de procedimentos, criação e uso de manuais de boas práticas aceitas internacionalmente para a forense computacional.

Referências Bibliográficas

ADAMS, Dwigth Edwans. **Digital Evidence: Standards and Principles**, 2000. Disponível em <http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm> Acessado em: 13. set. 2006.

ANDRADE, Thiago Felipe de. **Perícia Forense Computacional Baseada em Sistema Operacional Windows**. Trabalho de Conclusão de Curso, Jaraguá do Sul, SC, 2005.

COMISSÃO EUROPÉIA. 2004 Disponível em: <http://ec.europa.eu/ civiljustice/evidence/evidence_por_pt.htm>.Acesso em: 03. abr. 2007.

FREITAS, Andrey Rodrigues. **Perícia Forense Aplicada a Informática.** São Paulo. Ed. Brasport, 2006.

KERR, Orin. **Searching and Seizing Computers and Obtaining Eletronic Evidence in Criminal Investigations**. Computer Crime and Intellectual Property Section (CCIPS), 2001.

KUROSE, J.F., ROSS, K. W. **Redes de Computadores e a Internet – Uma Nova Abordagem**. São Paulo: Addison Wesley, 2003.

TAMOSOFT. Disponível em: <http://www.tamos.com/products/smartwhois/>. Acesso em: 03. abr. 2007.

ULBRICH, Henrique César. VALLE, James Della. **Universidade Hacker**. São Paulo, Ed. Digerati, 2005.

VARGAS, Raffael Gomes. **Processos e Padrões em Perícia Forense Aplicado a Informática**. Trabalho de Conclusão de Curso, Bacharelado em Sistemas de Informação, Faculdade Metodista Granbery, Juiz de Fora, Minas Gerais, 2006.

Raffael Gomes Vargas
raffaelvargas@hotmail.com

Universidade Católica de Brasília

Pós-graduação (Especialização) Lato Sensu

Perícia Digital

A Internet no mundo e, principalmente, no Brasil tem se popularizado cada vez mais. A mesma interconectividade que traz tantas facilidades para as pessoas é, por outro lado, utilizada como instrumento para a prática de crimes como ataque a sites, fraudes bancárias, espionagem industrial, plágio, furto de dados, pedofilia, ganhos financeiros ilícitos, terrorismo, disseminação de vírus eletrônico, clonagem de celulares e cartões de crédito, crimes de racismo, entre outros.

Neste cenário, o curso de Perícia Digital nos leva à abertura de importante espaço acadêmico para a compreensão do fenômeno impactante da criminalidade e do terrorismo digital na sociedade pós-moderna, bem como demonstra a necessidade de se ter pessoas com competência para fazer frente a estes tipos de fraudes, com base na ciência da investigação eletrônica. Portanto, o curso de Perícia Digital visa instrumentalizar profissionais para o melhor desempenho na área em questão, promovendo um aporte de conhecimentos, ferramentas e a formação de uma mentalidade na técnica de perícia digital e seus processos.

Grade horária

Disciplinas	Carga Horária
Módulo I (1º Semestre)	**180hs**
o Sistema Operacional	45 hs
o Profissional em Perícia Digital (Ètica)	15 hs
o Fundamentos em Perícia Digital	60 hs
o Segurança em TI	60 hs
Módulo II (2º Semestre)	**180hs**
o Fundamentos Jurídicos em Perícia Digital	15 hs
o Crimes Digitais	45 hs
o Laboratório de Perícia Digital	60 hs
o Análise de Tráfego em Redes TCP/IP	45 hs
o Metodologia da Pesquisa	15 hs
Orientações e bancas de TCC	40 hs
Total	**420hs**

Público Alvo

Graduados e pós-graduados da área de tecnologia, que desejem especializar-se em perícia digital, além de participantes de outras áreas que demonstrem estarem aptos a participarem do curso.

Corpo Docente:

- Esp. Américo Munhoz Junior;
- MSc. Dino Macedo Amaral;
- Esp. João Eriberto Mota Filho;
- MSc. João Paulo Batista Botelho;
- MSc. Laerte Peotta de Melo;
- MSc. Paulo Roberto Corrêa Leão – Coordenador.

Outras Informações:

- Inscrições:
  - Até 20 de julho de 2011

  Vagas limitadas! Garanta já a sua acessando o link http://www.ucb.br/textos/2/357/Inscricoes/?sIT=8

  - Campus II - SGAN 916 - Av. W5 - Asa Norte - Sala A-238 Tels (061) 3448 -7140 ou 3448-7000 -
  - Secretárias: Leonor - leonor@pos.ucb.br e Wanessa wanessap@ucb.br.
- Previsão de Curso:
  - Início: 1ª quinzena de Agosto11
  - Dias de aula: 2ª, 4ª e 6ª (noite) - 19:20 às 2250hs
  - Local: UCB - Campus II - SGAN 916 - Av. W5 - Asa Norte – Lab. B007
- Investimento:
  - Bruto: 18 X R$ 666,68
  - Líquido: desconto de 5%: 18 x R$ 633,35 (para pontualidade
- Contatos:
  - Coordenador: Prof. Paulo Roberto Corrêa Leão - prcleao@ucb.br;
  - Secretárias: Leonor - leonor@pos.ucb.br e Wanessa wanessap@ucb.br; Tels (061) 3448 -7140 ou 3448-7000 Campus II-SGAN 916-Av. W5 -Asa Norte-Sala A-238.

Análise Forense do Espaço de Swap

Antes de entrarmos na discussão a respeito da captura e análise de dados do espaço de swap, vamos descrever brevemente alguns aspectos da forense na memória principal.

Investigação da Memória Principal

Diante do grande fluxo de informações (processos, dados, drivers de dispositivos etc.) armazenadas na memória principal em um curto intervalo de tempo, surgem dificuldades inerentes à obtenção de dados armazenados nesse dispositivo. Não obstante, é uma área importante para a análise forense, pois pode conter diversas informações, como senhas, textos em claro de mensagens cifradas etc. [de Souza Oliveira, 2002].

Um importante ponto a considerar na busca por informações nesse dispositivo é o seu alto caráter de volalitilidade. Segundo [Venema and Farmer, 2004], o "tempo de vida" das informações armazenadas na memória é da ordem de nanossegundos. Por si só, a captura de informações já apresenta um desafio ao investigador, uma vez que as evidências tem de ser capturadas rapidamente. Temos de levar em conta também que a filtragem dos dados presentes na memória é trabalhosa e nem sempre os dados podem estar completos [de Souza Oliveira, 2002].

Uma segunda questão crucial para a análise forense diz respeito à alteração da memória durante a execução de algum procedimento para acessá-la e copiá-la. Se usarmos o programa **dd** para copiar, no Linux, o conteúdo da memória, estaremos modificando-a. Isso porque o programa requer espaço na memória para ser executado, o que já altera pelo menos alguma parte dela. A investigação do conteúdo da memória sem causar-lhe distúrbios é uma tarefa bastante complexa e requer conhecimento altamente especializado [dos Reis, 2003].

A memória principal dos PCs é implementada via dispositivos eletrônicos voláteis, ou seja, só mantém a informação enquanto houver alimentação de energia elétrica. Dado essa característica, o procedimento usual é coletar dados da memória com o sistema nativo ligado, ou seja, trata-se de uma *live analysis*. Vejamos como podemos copiar[1] a memória principal do Linux no próprio sistema operacional:

```
# dd if=/dev/mem of=/memdump bs=1024
```

Algumas análises podem ser feitas na evidência coletada acima. Um exemplo simples e viável é fazer buscas por palavras-chave usando os comandos **grep** e **strings**, conforme abaixo [dos Reis, 2003]:

```
# grep palavra-chave /memdump
# strings -a /memdump | grep palavra-chave
# strings -a /memdump | more
```

No primeiro exemplo, é possível pesquisar palavras-chave no arquivo de *dump* da memória, sendo possível achar endereços e códigos de cabeçalhos HTTP, fragmentos e nomes de imagens etc. Já nos exemplos subseqüentes, podemos pesquisar palavras-chave a partir de cadeias de caracteres extraídas ou simplesmente exibir essas cadeias de caracteres.

Conceitos

[1] O processo de cópia da memória principal também é conhecido como *dump* de memória

O espaço de swap está intrinsecamente relacionado ao esquema de memória virtual adotado por muitos sistemas operacionais. Lembremo-nos que o espaço (ou área) de swap é usado quando a memória principal precisa executar mais processos do que a sua capacidade [Silberschatz et al., 2001]. Esse espaço é alocado no armazenamento auxiliar (disco rígido, por exemplo), adotando a política de armazenar os processos que não estão em execução no momento, liberando espaço na memória principal para aqueles que estão em execução [Scheetz, 2001].

Segundo [Silberschatz et al., 2001], como todo processo para estar em execução deve estar na memória, quando os processos armazenados na área de swap são chamados para executar, eles são levados dessa área para a memória principal. Essa operação é denominada de *swap in*. A situação inversa ocorre quando um processo é trazido da memória principal para a área de swap, operação denominada de *swap out*. A Figura 1 ilustra essas operações.

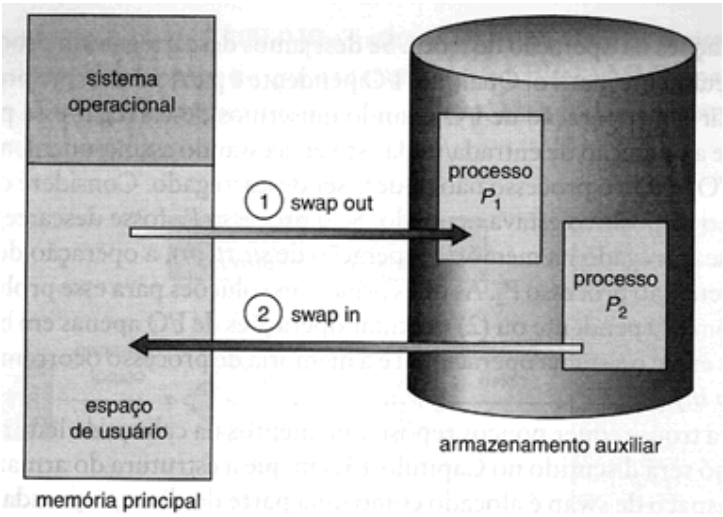


Figura 1: troca de dois processos usando um disco como armazenamento auxiliar para a área de swap [Silberschatz et al., 2001]

Em geral, o armazenamento de swap é implementado de duas maneiras: via arquivo ou via partição. A primeira forma cria um arquivo (localizado no próprio sistema de arquivos nativo), no qual processos são armazenados. Na segunda forma, os processos são armazenados em uma partição destinada unicamente a esse fim. Como exemplo de implementação via arquivo temos o Microsoft Windows, já a implementação via partição podemos citar o Linux (embora possa ser configurado para utilizar arquivo de swap, também, mas não é a configuração padrão).

No espaço de swap podem ser encontrados dados dos mais variados tipos, como: senhas que não chegaram a ser armazenadas no disco rígido, arquivos (completos ou parciais) confidenciais, rascunhos não salvos etc. [Caloyannides, 2004]. Também podem ser encontradas nessa área: dados de processos, de kernel, buffers de impressora, assim como dados ocultados deliberadamente [dos Reis, 2003]. Portanto, analisar a área de swap é uma tarefa importante na busca de dados - possíveis evidências - que provavelmente nunca seriam encontradas no disco.

Análise do Espaço de Swap - Partição de Swap do Linux

Como dissemos, no Linux a opção mais comum é usar o espaço de swap como uma partição específica para tal fim. Mas pode ser usado arquivo de swap (semelhante ao modo feito no Windows), no lugar da partição. No entanto, para se ter um uso mais eficiente da swap no Linux, é recomendado o uso da armazenagem da Swap em partição em lugar do arquivo, pois a partição é otimizada para essa tarefa [Scheetz, 2001].

Para copiar o conteúdo da partição de swap no linux, podemos utilizar o comando **dd** da seguinte forma:

```
# dd if=/dev/hdaX of=/swap/swaplinux bs=1024 count=131070
```

que copiará o conteúdo da partição de swap, localizada em /dev/hdaX - "hdaX" é o número fictício de dispositivo em nosso exemplo - para o arquivo "/swap/swaplinux". Observe que estamos instruindo o dd a copiar 131070 setores de 1024 bytes cada, resultando em 128MB, que é o tamanho da partição de swap (esse valor depende do tamanho da partição de swap configurada no sistema).

Devemos parar nesse momento para fazer algumas considerações importantes com relação ao procedimento de captura do conteúdo da swap no Linux descrito acima. O procedimento é executado com o sistema nativo (Linux) ligado. Quando chamamos a execução do programa dd, ele tem de ser armazenado na memória principal para ser executado, assim como outro processo qualquer. Acontece que podem ocorrer operações de swap in e swap out entre o armazenamento auxiliar e a memória principal, para que o processo dd possa executar.

Conclusão: talvez não consigamos copiar a swap sem causar o mínimo de alteração a ela. Mas isso não quer dizer que a análise será em vão, pois devemos ter em mente que este é um caso de *live analysis*. Devemos procurar minimizar os efeitos da coleta de evidências no sistema em funcionamento, causando o menor distúrbio possível.

Arquivo de Swap do Windows (ou *Pagefile*)

Para poder analisar o arquivo de swap do Windows 2000/XP no Linux, podemos proceder da seguinte forma (obedecendo aos "três As da Forense Computacional – adquirir, autenticar e analisar evidências):

Aquisição - Primeiramente devemos montar a partição (FAT ou NTFS) onde reside o arquivo de swap do Windows em modo somente leitura. No exemplo abaixo, consideramos uma instalação do Windows usando o sistema de arquivos NTFS e alcançável no Linux pelo dispositivo /dev/hda1 (apenas a título de exemplo):

```
# mount -t ntfs -r /dev/hda1 /mnt/hd/C
```

Assim, se montarmos a partição do Windows em /mnt/hd/C, o arquivo de swap deverá estar localizado em /mnt/hd/C/pagefile.sys.

Para adquirirmos efetivamente o arquivo de swap, temos de fazer uma cópia bit-a-bit do seu conteúdo para um arquivo imagem no Linux. Isso pode ser feito via comando **dd**:

```
# dd if=/mnt/hd/C/pagefile.sys of=/swap/pagefile.sys bs=1K
```

Assim, teremos uma cópia idêntica do arquivo de swap do Windows, localizada em /swap/pagefile.sys. Terminada a fase de aquisição da evidência, podemos autenticar sua cópia agora.

Autenticação – Colocada de maneira simples, a autenticação visa garantir que a cópia espelho e a evidência original são idênticas. Logo, devemos verificar se a cópia que obtivemos no passo anterior é autêntica, utilizando algum método confiável.

Uma maneira de verificar a autenticidade de uma cópia espelho é calcular os hashes criptográficos MD5 da cópia e do original. No Linux, podemos fazer isso por meio do comando **md5sum**:

```
# md5sum /mnt/hd/C/pagefile.sys /swap/pagefile.sys > /swap/md5swap
```

Será gerado um hash criptográfico MD5 para o arquivo original de swap e para a cópia espelho. Indicamos para o comando armazenar a saída no arquivo /swap/md5swap. Para

conferirmos a autenticidade da cópia espelho basta verificar em qualquer editor de texto que as duas linhas geradas possuem o mesmo hash criptográfico gerado (veja um exemplo abaixo de dois valores de hash criptográfico MD5 armazenadas no arquivo "md5swap"). Deste modo, concluímos a autenticação da evidência original e de sua cópia espelho.

```
f3db4f45f5adcfc61a562123b7fb214b /mnt/hd/C/pagefile.sys
f3db4f45f5adcfc61a562123b7fb214b /swap/pagefile.sys
```

Análise - A seguir, são descritos alguns exemplos de como podemos analisar a evidência usando comandos comuns do Linux.

1. Pesquisar um padrão de caracteres, usando o comando **grep**. A saída será armazenada em um arquivo denominado "resultgrep". Veja:

```
# grep -a http:// /swap/pagefile.sys > /swap/resultgrep
```

Neste caso, pesquisamos, na cópia da swap, pela existência da cadeia "http://". Abrindo o arquivo "resultgrep" num editor de texto podemos visualizar diversas informações textuais e não-textuais (uma vez que usamos a opção **-a** com o comando para pesquisar). Dentre as informações textuais, podemos destacar alguns itens encontrados que mostram, pelo menos em parte, rastros de atividades do usuário no sistema, como:

- URLs e códigos de status de requisições (401, 200 etc.) de páginas da Web;
- Código-fonte de páginas da Web;
- Código-fonte de scripts (e.g., Java scripts);
- Cookies;
- Requisições de senha e nome de usuário;
- Nomes e partes de arquivos gráficos (gif, jpg etc.);
- Ampla variedade de diversos tipos de informação.

2. No exemplo abaixo, usamos o comando **strings** para salvar o resultado da busca por qualquer cadeia de caracteres (com pelo menos 4 caracteres de texto) no arquivo de texto "resultstrings":

```
# strings /swap/pagefile.sys > resultstrings
```

A análise do conteúdo de cadeias de caracteres fornecidas por **strings** é bastanta trabalhosa, o que pode ser melhorado com o emprego de métodos de busca e análise, como a busca por determinada string relacionada ao contexto de investigação (por exemplo, crimes de pedofilia).

Os arquivos gerados nos dois exemplos acima poderão ter dezenas de megabytes de tamanho, especialmente se o espaço de swap for da ordem de centenas de megabytes.

Monitorando a Swap

No Windows, o software Swapmon[2] (desenvolvido pela Fliptech) realiza o monitoramento da swap. A documentação do software descreve-o como software de análise de memória virtual e apresentar sugestões educativas para uso da memória RAM.O Swapmon mostra o uso da área de swap, quais aplicativos colocam dados na RAM, dentre outras funções interessantes.

Considerações – Antiforense e Privacidade

Devemos ter em mente que, apesar da característica do espaço de swap permitir o armazenamento de dados (e posterior coleta pelo investigador) eventualmente importantes

[2] http://www.fliptech.net/swapmon/

numa análise forense, também existe o outro lado da análise: a antiforense. No caso da análise do espaço de swap, podemos entender a antiforense como a tentativa de eliminar informações da área de armazenamento de swap, o que pode ser feito por meio de procedimentos e ferramentas para tal fim.

Como exemplo de procedimento antiforense, podemos citar a alteração de valores no Registro do Windows para que o arquivo de swap seja sobrescrito com zeros ao desligar o sistema [Caloyannides, 2004]. Essa medida de segurança fornecida pelo Windows 2000/XP não apaga todas as páginas da swap, no entanto, uma vez que algumas ainda estarão em uso pelo sistema.

Em termos de ferramentas, existem diversos programas que fazem a "limpeza" (*wipe*[3], ou remoção permanente de um arquivo ou do seu conteúdo, exclusão segura) do arquivo de swap no Windows [Caloyannides, 2004]. Exemplos: PGP for DOS[4] e BCWipe[5]. No Linux é possível utilizar comandos, como **dd**, de forma a preencher a partição swap (ou arquivo, for o caso) com bits 0 ou randômicos.

Trabalhos futuros

O próximo passo deste trabalho será a implementação de uma ferramenta que automatize vários dos processos descritos acima, como listagem de URLs, cookies, figuras, dentre outros. Também procuraremos desenvolver uma metodologia de recuperação de arquivos, como imagens GIF, JPG etc., observando o cabeçalho e assinatura desses arquivos na área de swap.

Referências Bibliográficas

[Caloyannides, 2004] Caloyannides, M. A. (2004). Privacy Protection and Computer Forensics. Artech House, Norwood, MA, USA, 2nd edition.

[de Souza Oliveira, 2002] de Souza Oliveira, F. (2002). Resposta a incidentes e análise forense para redes baseadas em windows 2000. Master's thesis, Universidade Estadual de Campinas. Disponível em
http://www.las.ic.unicamp.br/paulo/teses/20021121-MSc-Flavio
.Oliveira-Resposta.a.incidentes.e.analise.forense.para.redes
.baseadas.em.Windows.2000.pdf

[dos Reis, 2003] dos Reis, M. A. (2003). Forense computacional e sua aplicação em segurança imunológica. Master's thesis, Universidade Estadual de Campinas. Disponível em
http://www.las.ic.unicamp.br/paulo/teses
/20030226-MSc-Marcelo.Abdalla.dos.Reis-
Forense.computacional.e.sua.aplicacao.em.seguranca.imunologica.pdf.

[Gutmann, 1996] Gutmann, P. (1996). Secure deletion of data from magnetic and solid-state memory. In Sixth USENIX Security Symposium, Focusing on Applications of Cryptography, pages 77{90. USENIX. Disponível em
http://www.usenix.org/publications/library/proceedings
/sec96/full papers/gutmann/index.html.

[Scheetz, 2001] Scheetz, D. (2001). Dwarf's guide to debian gnu/linux. Debian (web site). Disponível em http://people.debian.org/~psg/ddg/dwarfs-debian-guide.html

---

[3] De um modo geral, o *wipping* da área de swap consiste em inserir nela bits randômicos ou seguindo algum padrão um certo número de vezes (o que constitui a chamada *pass*, que também é executada diversas vezes) [Gutmann, 1996]
[4] http://www.pgpi.org/products/pgp/versions/freeware/dos
[5] http://www.jetico.com

[Silberschatz et al., 2001] Silberschatz, A., Galvin, P., and Gagne, G. (2001). Sistemas Operacionais: Conceitos e Aplicações. Elsevier - Campus, Rio de Janeiro, RJ, First edition.

[Venema and Farmer, 2004] Venema, W. and Farmer, D. (2004). Forensic Discovery. Addison Wesley Professional, Boston, MA, USA, first edition.

Marcos Luiz de Paula Bueno
mlpbcc@gmail.com

http://www.guiatecnico.com.br/EvidenciaDigital

Edições 1 e 2

Evidência Digital magazine

Edição 3

Edição 4

PROCEDIMENTOS BÁSICOS PARA REALIZAÇÃO DA PERICIA COMPUTACIONAL FORENSE

Introdução

Nas últimas décadas, a utilização de computadores tornou-se parte integrante da vida das pessoas. Transações bancárias e compras passaram a ser feitas pela internet, informações diversas passaram a ser armazenadas e transmitidas de forma eletrônica, dispositivos digitais passaram a compor quase todo o tipo de equipamento eletrônico. Com o crescimento do terrorismo no mundo, especialistas acreditam que muitas mensagens trafegadas pela web podem esconder informações com planos de atentados e outras mensagens de cunho criminoso. O perito em computação científica deve estar atento ao descarte de imagens aparentemente inofensivas, pois poderá perder informações valiosas em um trabalho pericial. A definição de uma política a ser adotada no caso de um incidente de segurança é essencial para que os danos sejam minimizados. É necessário que haja metodologias para que uma vez descoberta à invasão, seja possível identificar, coletar e manipular evidências sem distorcê-las. Mantendo-se assim, a possibilidade de futuramente adotar-se medidas legais contra o invasor.

A Prática Investigativa da Perícia Forense

Com o surgimento do computador, tornou-se necessária arquitetar uma disciplina forense. Disciplina essa que tenha metodologia e acúmulo de conhecimento necessário para a aquisição, manipulação e análise de evidências. Para deparar com uma evidência é necessário que se faça um exame minucioso na máquina (FREITAS, 2006).

A Perícia forense é uma área relativamente nova e tornou-se uma prática investigativa importante tanto para as empresas quanto para a polícia.

"Perícia forense em sistemas computacionais é o processo de coleta, recuperação, análise e correlacionamento de dados que visa, dentro do possível, reconstruir o curso das ações e recriar cenários completos fidedignos". (FREITAS, 2003).

Análise Pericial

A análise pericial é o método empregado pelo perito para identificar informações preciosas, buscando e extraindo dados relevantes para uma investigação.

Segundo (FREITAS, 2003) a técnica de análise pericial é dividida em duas fases: análise física e análise lógica.

Análise Física

No decorrer da análise física são investigados os dados brutos da mídia de armazenamento. Os dados podem ser analisados por três métodos fundamentais: pesquisa de seqüência, processo de busca e extração de espaço sub-aproveitado e livre de arquivos.

Todas as operações são realizadas na imagem pericial ou na cópia restaurada das provas. (FREITAS, 2003).

Em todo o sistema o primeiro método na análise física é a pesquisa de seqüências. *StringSearch* é a ferramenta mais precisa em se tratando de DOS. Através do deslocamento

de *byte* do inicio do arquivo ela retorna o conteúdo da pesquisa de seqüência. (FREITAS 2003).

O segundo método da análise física é o processo de busca e extração, o programa analisa uma imagem pericial em busca de cabeçalhos dos tipos de arquivos correspondente ao tipo de caso em que se estiver trabalhando. Quando encontra um, retira um número fixo de *byte* a partir do ponto da ocorrência. (RODRIGUES, 2004).

O último processo da análise física é extrair espaço livre ou não alocado e espaço sub-aproveitado.

"O espaço livre é qualquer informação encontrada em um disco rígido que no momento não esteja alocada em um arquivo. O espaço livre pode nunca ter sido alocado ou ser considerado como não-alocado após a exclusão de um arquivo. Portanto, o conteúdo do espaço livre pode ser composto por fragmentos de arquivos excluídos. Para analisar o espaço livre é preciso trabalhar em uma imagem do nível físico." (FREITAS, 2003).

"O espaço sub-aproveitado ocorre quando dados são escritos na mídia de armazenamento em blocos que não preenchem o tamanho de bloco mínimo definido pelo sistema operacional. Esse processo exige uma ferramenta que possa distinguir a estrutura particular de sistema de arquivos em uso." (RODRIGUES, 2004).

Análise Lógica

No decorrer de um exame de arquivos lógicos, o conteúdo de cada partição é pesquisado com um sistema operacional que entenda o sistema de arquivos.

O investigador precisa estar ciente de todas as medidas tomadas na imagem restaurada. É devido a isto que quase nunca se usa diretamente sistemas operacionais mais convenientes, como o *Windows 95/98/NT/2000/XP*. O objetivo básico é proteger as provas contra alterações (FREITAS, 2003).

Prover ou acessar a imagem restaurada a partir de um sistema operacional que entenda nativamente o formato do sistema de arquivos é muito arriscado.

A maneira de efetuar isto é montar cada partição em *Linux*, em modo somente de leitura. O sistema de arquivos montado é então exportado, via Samba, para a rede segura do laboratório, onde os sistemas *Windows* 2000 ou 2003, carregados com visualizadores de arquivos, podem analisar os arquivos. (RODRIGUES, 2004).

Obtenção de Evidências

A missão da perícia forense é a obtenção de provas irrefutáveis, as quais irão se transformar o elemento chave na decisão de situações jurídicas, tanto na esfera civil quanto criminal. Para tanto, é crítico observar uma metodologia estruturada visando à obtenção do sucesso nestes projetos. (FREITAS, 2003)

A rigorosa documentação das atividades é fundamental para que uma análise possa ser aceita, mesmo que o *stress* causado por um incidente de segurança torne mais difícil a atividade de documentar as decisões e ações, que pode prejudicar uma futura ação judicial contra os responsáveis. (RODRIGUES, 2004).

Réplicas: efetuar a duplicação pericial completa é sempre aconselhável para que seja possível a repetição dos processos e a busca da confirmação dos resultados, sem que haja um dano à evidência original, por algum erro do examinador (RODRIGUES, 2004).

Garantia de Integridade: deve haver procedimentos previamente determinados que visem garantir a integridade das evidências coletadas. No mundo virtual a autenticidade e a integridade de uma evidência podem ser verificadas através da utilização de algoritmos de hash criptográfico como o MD5, SHA-1 e o SHA-2. Além disso é possível armazená-las em mídias para somente leitura, como CD-ROMs. (RODRIGUES, 2004).

Ferramentas Confiáveis: não há como garantir a confiabilidade dos resultados obtidos durante uma análise se os programas utilizados não forem idôneos. (RODIGUES, 2004);

Identificação das Evidências

A cada crime que é cometido, gera um tipo de evidência. Para identificar as evidências vai depender da habilidade e da familiaridade que o perito tem com o tipo de crime que foi cometido e dos programas e sistemas operacionais. Para localizar possíveis evidências é aconselhável que siga os passos descritos abaixo:

Procurar por dispositivos de armazenamento (hardwares): laptops, HDs, disquetes, CDs, DVDs, drives Zip/Jaz, memory keys, pendrives, câmeras digitais, MP3 player, fitas DAT, Pocket PC, celulares, dispositivos de backup ou qualquer equipamento que possa armazenar evidências; procurar por informações relacionadas ao caso: anotações, nome de pessoas, datas, nomes, de empresas e instituições e número de telefones, documentos impressos etc. (FREITAS, 2006, p.2-3).

Preservação das Evidências

A regra mais importante na preservação das evidências é não destruir ou alterar as provas. Isso quer dizer que as evidências precisam ser preservadas de tal forma que não haja dúvida alguma de sua veracidade. E para que as evidências não sejam comprometidas, substituídas, ou perdidas, deve-se: (FREITAS, 2006, p.3).

É recomendável criar imagens do sistema investigado, também conhecido como duplicata pericial, e seguir os seguintes procedimentos: se a caso necessitar de uma análise ao vivo, salvar as evidências em disquete e bloqueá-las contra regravação; todas as evidências deverão ser lacradas em sacos e etiquetadas; a etiqueta deverá conter um número para a identificação das evidências, o número de caso, a data e o horário em que a evidência foi coletada, e o nome da pessoa que a está levando para custodia; etiquetar todos os cabos e componentes do computador, para que depois possam ser montados corretamente quando chegar no laboratório; durante o transporte das provas, tomar cuidado com líquidos, umidade, impacto, sujeira, calor excessivo, eletricidade e estática; quando já tiverem sido transportadas, as evidências deverão ser armazenadas e trancadas para evitar a adulteração até o momento em que poderão ser examinadas e analisadas; todas as mudanças feitas durante esta fase deverão ser documentadas e justificadas (Cadeia de custódia) (FREITAS, 2006, p. 3 - 4).

Análise das Evidências

A fase de análise representa o principal objetivo do processo de investigação forense. É a hora em que todo o material coletado e minuciosamente investigado em busca de evidências, proporcionando formular conclusões acerca do incidente que originou a investigação.

A documentação das tarefas realizadas e evidências encontradas, bem como a atualização da cadeia de custódia dos itens analisados, devem ser atividades rotineiras durante a etapa de análise. Outra atividade importante é a correlação das evidências encontradas, possibilitando, entre outras conclusões, definir se realmente houve um incidente de segurança; refazer as atividades do atacante; identificar causas, suspeitos e conseqüências da invasão. Com

base nos resultados obtidos pela investigação. (FREITAS, 2006, p. 4).

Para que seja possível alcançar os objetivos em uma investigação é necessário saber identificar quem fez, quando fez e que dano causou e como foi desenvolvido, mas para atingir os objetivos deve-se conhecer o que está sendo procurado e onde procurar. Ressaltando que as evidências têm a obrigação de ser autentica, exata, completa e precisa.

Apresentação das Evidências

Na fase de apresentação da análise, o perito gera um laudo pericial que é um relatório técnico sobre a investigação, onde são apresentados os fatos, procedimentos, análise e resultado. (FREITAS, 2006, p. 5).

O laudo deve ser claro, conciso, estruturado e sem ambigüidade, de tal forma que não deixe dúvida alguma de sua veracidade; Deverão ser informados os métodos empregados na perícia, incluindo os procedimentos de identificação, preservação e análise, e os software e hardware utilizados;

O laudo pericial deve conter apenas afirmações e conclusões que possam ser aprovadas e demonstradas técnica e cientificamente. (FREITAS, 2006, p. 5)

Considerações Finais

Conseguiu-se alcançar os objetivos propostos neste trabalho que era apresentar os passos básicos e necessários da pericia computacional forense, cujo objetivo é auxiliar os peritos obter, identificar, preservar, analisar e apresentar as evidências.

Os Hackers, vírus, crimes virtuais, fraudes eletrônicas na Internet e abuso do e-mail continuarão a aumentar nos próximos anos. Devido a esses problemas muitas empresas proporcionarão treinamentos na aquisição, na examinação e na utilização apropriada da evidência eletrônica (FREITAS, 2003).

O campo da Perícia Computacional Forense continuará a crescer e se começará a ver empresas com os detetives digitais treinados na equipe de funcionários, a combater não somente ameaças externas e internas, mas também a analisar e preparar procedimentos e aplicações protetoras para a empresa (FREITAS, 2003).

O surgimento de legislação e padrões a serem aplicadas no Brasil referentes à Forense Computacional tornaria menor a chance de laudos sarem inutilizados por falta de experiência dos peritos.

Referências Bibliográficas

FREITAS, Andrey Rodrigues. **Perícia Forense aplicada à Informática.** Disponível em: <http://www.modulo.com.br/pdf/monografia_forense.pdf> Acessado em 10 de outubro de 2007.

FREITAS, Andrey Rodrigues. **Perícia Forense aplicada á Informática Ambiente Microsolft.** Rio de Janeiro: Editora Brasport Livros e Multimídia Ltda. 2006.

GOMES, Ricardo Reis. **Como Colher Provas de um Crime Virtual.** Disponível em: <http://www.modulo.com.br/index.jsp?page=3&catid=7&objid=2459&pagecounter=0&idiom=0> acessado em 18 de outubro de 2007.

MORIMOTO, Carlos. **Como Recuperar Dados de HD'S Defeituosos.** Disponível em <http://www.guiadohardware.net/tutoriais/recuperar-dados/> acessado em 11 de abril de 2008.

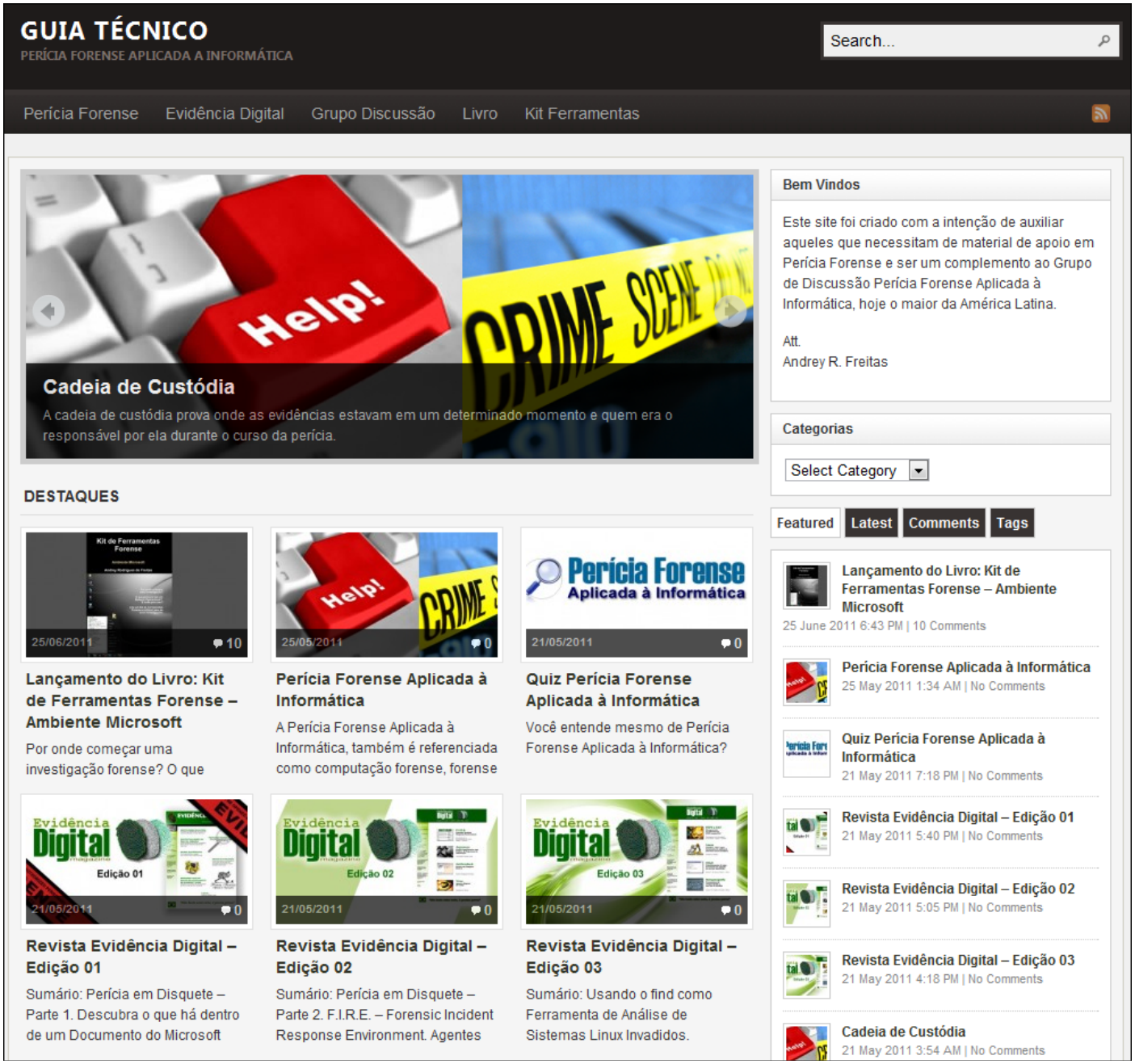
NEUKAMP, Paulo; PEREIRA, Evandro Della Vecchia; FAGUNDES, Leonardo Lemes; LUDWING, Glauco; KONRATH, Marlom. **Forense Computacional Fundamentos, Tecnologias e Desafios Atuais.** 2007 – UNISINOS – RS.

RIBEIRO, Uirá. **Certificação Linux.** Rio de Janeiro: Axcel Books, 2004.

RODRIGUES, Wagner de Paula. **Análise Pericial Em Sistema Operacional Ms-Windows 2000**. Disponível em: <http://www.dc.uel.br/nou-rau/document/?view=169> acessado em 18 de outubro de 2007

TREVENZOLI, Ana Cristina. **Perícia forense computacional – ataques, identificação da autoria, leis e medidas preventivas.** Sorocaba: SENAC 2006.

Rhafael Freitas da Costa
Costa.cfr@gmail.com



http://www.guiatecnico.com.br